FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Evaluation von Methoden zur Abwehr von SPIT in VoIP

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Wirtschaftsinformatik

eingereicht von

Michael Krieber
Matrikelnummer 0525434

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung
Betreuer/in: Thomas Grechenig

Wien, 29.09.2010

(Unterschrift Verfasser/in)

(Unterschrift Betreuer/in)

Forschungsgruppe für Industrial Software (INSO)
Institut für Rechnergestützte Automation (E183)
Fakultät für Informatik
Technische Universität Wien

Diplomarbeit

Evaluation von Methoden zur Abwehr von SPIT in VoIP

Autor:
Krieber Michael
Gersthoferstrafle 28/7 1180 Wien

Betreuer:
Thomas Grechenig

Wien, 14. Oktober 2010

Inhaltsverzeichnis

Zusammenfassung

Voice over IP (VoIP) ist eine häufiger werdende Art der Kommunikation im Alltag. Eines der am meisten störenden und aus dem E-Mail-Bereich bekannten Probleme ist SPAM. Im Bereich von VoIP wird SPAM als SPAM over Internet Telephony oder kurz SPIT bezeichnet. Die vorliegende Arbeit beschreibt Möglichkeiten und eventuelle Lösungsansätze zur Bewältigung dieses Problems.

Im Zuge der Arbeit wurden ausgewählte Abwehrmethoden von SPIT analysiert. Die Analyse zeigte auf, dass es grundlegend zwei verschiedene Kategorien von Abwehrtechniken gibt. Einerseits werden geeignete Filterlisten (z.B. Whitelists oder Blacklists) gepflegt, die unerwünschte Anrufe von Voice SPAMmern verhindern sollen. Andererseits wird ein Prinzip verfolgt, das automatisiert das Verhaltensmuster von Anrufern analysiert, um einen Abwehrschutz zu erzeugen.

Zur Analyse der SPIT-Problematik wurde in dieser Arbeit eine Evaluierung und Bewertung der verschiedenen Methoden zur Abwehr von SPIT auf Basis von zwölf Bewertungskriterien vorgenommen. Ergebnis dieser Evaluierung ist eine Reihung der einzelnen Methoden, auf Basis derer man einzelne Abwehrmethoden für den Einsatz in der Praxis auswählen kann. Es hat sich gezeigt, dass Methoden, die auf Listen basieren, derzeit besser geeignet sind, SPIT auf eine einfache und verlässliche Weise abzuwehren als Methoden, die das Verhalten der Kommunikationsteilnehmer berücksichtigen.

Abstract

Voice over IP (VoIP) is getting much more often used to communicate in today's daily routines. One of the most annoying and known problems in this area is SPAM. In the field of VoIP, the technical term for SPAM is SPAM over Internet Telephony or just SPIT. This master's thesis exploits the potential threats and possible solutions to treat with this problems.

In the course of this work different defense methods were selected and analyzed. It shows, that there exist two main categories of such techniques. The first category are miscellaneous filter lists (e.g. whitelists or blacklists) which should avoid callers of voice SPAMmers. The other method is to automatically analyze the behavior pattern of callers to create a strong defense mechanism.

During the work of this thesis an evaluation and ranking of several methods to defense SPIT on base of twelve criterias were carried out. The result of this evaluation is a ranking of these methods on which in practice decisions to deploy of one of this methods can base. Currently methods that use lists are more effective to defense SPIT than methods analyzing behavior.

Danksagung

Als allererstes möchte ich mich bei den beiden Personen bedanken, die mir diese Diplomarbeit ermöglicht haben und mir eine große Unterstützung in fachlicher und konzeptioneller Richtung waren, Herr Univ.Prof. DI Dr. Thomas Grechenig und Herr Dipl.-Ing. Florian Fankhauser von der Forschungsgruppe INSO.

Eine weitere sehr starke Stütze meine ganze Studienzeit hindurch war mir meine Mutter Marie-Luise. Durch ihre hilfreichen und motivierenden Worte konnte sie mir immer wieder, wenn ich in einem Tief war, neue Motivation und neue Kraft spenden, was mich weiter in Richtung Abschluss meines Studiums gebracht hat. Weiteres möchte ich auch meiner restlichen Familie danken, welche mir die Möglichkeit geboten hat, dieses Studium zu absolvieren. Vielen Dank!

Ein weiterer treuer Begleiter ist mein guter Freund und Studienkollege Markus Freudenthaler. Kennengelernt haben wir uns im ersten Semester und seitdem haben wir einen erfolgreichen gemeinsamen Weg durch unser Studium beschritten. Vor allem durch unsere sehr gut funktionierende Teamwork, aber auch durch den ständig herrschenden Konkurrenzkampf um die besten Noten und den schnellsten Studienfortschritt, haben wir uns gegenseitig immer neue Motivation und Kraft geschenkt, um dieses Studium abzuschließen. Vielen Dank, Markus!

Großen Dank möchte ich ebenfalls meinen beiden Arbeitgebebern CSC Austria und ST-Security aussprechen. CSC hat es mir ermöglicht, trotz Berufstätigkeit meine Termine auf der Universität wahrzunehmen. Des Weiteren unterstützte mich meine Firma in der Hinsicht, mir genügend freie Zeit für Klausuren, Termine und schlussendlich für die Fertigstellung meiner Diplomarbeit zu Verfügung zu stellen. Weiters möchte ich auch meinem zweiten Arbeitgeber ST-Security danken, welcher immer Verständnis dafür hatte, dass ich an gewissen Wochenenden Zeit für die Fertigstellung meiner Arbeit gebraucht habe und der Firma so nicht zur Verfügung stand. Vielen Dank!

Letzten Endes möchte ich mich auch bei all meinen Freunden bedanken, die

mich während meines gesamten Studiums sowie bei der Ausarbeitung meiner Diplomarbeit motiviert und gestützt haben. Gemeinsam mit ihnen war es mir möglich, eine schöne, aufregende und lehrreiche Zeit an der Universität zu verbringen. Besonders hervorheben möchte ich hier Markus Freudenthaler, Oliver Selinger und Roland Ladengruber, mit denen ich während meiner Studienzeit den meisten Kontakt hatte. Vielen Dank!

Kapitel 1

Einleitung

Im Kapitel Einleitung werden die Ziele der Masterarbeit „Evaluation von Methoden zur Abwehr von SPIT in VoIP“ erläutert und beschrieben.

1.1 Zielsetzung der Arbeit

Voice over IP (VoIP) ist eine häufiger werdende Art der Kommunikation im Alltag.
Besonders häufig findet VoIP im Bereich von Firmentelefonnetzen Anwendung, aber auch im privaten Bereich wird diese Technologie immer beliebter. Doch durch ihren immer häufiger werdenden Einsatz ergeben sich neue Arten von Problemen und Sicherheitsrisiken. Eines der am meisten störenden und aus dem E-Mail-Bereich bekannten Problemen ist SPAM (siehe Kapitel 4). [Kha08a]

Im Bereich von VoIP wird SPAM als SPAM over Internet Telephony oder kurz SPIT (siehe Kapitel 5) bezeichnet. Oft tritt SPIT in Form von automatisiertem Telefonmarketing auf. Hierbei werden dem Betroffenen durch automatische Computersysteme unzählige Sprachnachrichten pro Minute gesendet. So kommt es vor, dass diese Art von Anrufen jederzeit eingehen und der Benutzer mit ungewollten, oftmals störenden Werbeansagen belästigt wird. Es gibt zwar schon einige Ansätze und Lösungsmöglichkeiten, um diese Art der Unterbrechnungen und Störungen zu vermeiden, allerdings noch keine konsolidierte Möglichkeit welche diese Probleme zur Gänze verhindert. [Kun08]r Ziel der Arbeit ist es, diese Methoden zu erheben und zu evaluieren.

Das fachliche Ziel dieser Arbeit ist es, den zukünftig zu erwartenden Problemen im Bereich von SPIT entgegenzuwirken bzw. auf Gefahren aufmerksam zu machen. Im Verlauf der Zeit hat sich das Thema SPAM vor allem im Umfeld der IT, auf E-Mails bezogen, als deutlicher Störfaktor erwiesen. Enorme Mengen an SPAM-Mails (siehe Kapitel 4) werden erzeugt und teilweise auch

im privaten Bereich versendet. Im Bereich des E-Mail-Versands gibt es schon sehr gute Schutzmechanismen, welche sich über Jahre hinweg etabliert haben und einen guten Umgang mit SPAM weitestgehend ermöglichen. Anders ist dies jedoch im noch jungen Bereich von VoIP. Die Erwartungen bzgl. SPAM lehnen sich an die Erfahrungen im E-Mail-Bereich an. [Kun08] Darum ist es aus wissenschaftlicher, aber auch aus wirtschaftlicher Sicht sehr wichtig, entsprechende Methoden zu finden, diese zu vergleichen und zu evaluieren. Primär wird durch die Einsatzmöglichkeit die Sicherheit solcher Dienste gesteigert. Sekundär dient diese Arbeit einer allgemeinen Aufklärung bezüglich der Gefahren, die VoIP mit sich bringen kann.

1.2 Aufbau der Arbeit

Zu Beginn wurde das Augenmerk auf das Thema IT-Security gelegt. Die Grundlagen der IT-Security bilden eine Einleitung in die Grundbegriffe und Thematik der IT-Security. Darauf aufbauend, bildet das Kapitel Grundlagen von Voice over IP einen detaillierten Einblick in das Thema VoIP, in dem Inhalte wie die Geschichte von VoIP bis hin zur technischen Übertragung behandelt werden.

Ein weiteres Kapitel wurde dem Thema SPAM gewidmet. Dieses Kapitel erklärt dessen Problematik näher und gibt einen umfangreichen Überblick über die verschiedenen Arten von SPAM.

Anschließend bildet das Kapitel SPAM over Internet Telephony eine Einleitung in die Thematik von SPIT. Darauf aufbauend bilden Kapitel 6, Methoden zur Abwehr von SPIT und Kapitel 7, Evaluation von Methoden zur Abwehr von SPIT, die beiden Kernpunkte dieser Diplomarbeit.

In Kapitel 6 werden verschiedene aktuelle Methoden zur Abwehr von SPIT im Detail untersucht und beschrieben. Im Kapitel 7 werden die Methoden aus Kapitel 6 durch verschiedene Bewertungskriterien zuerst einzeln evaluiert und anschließend miteinander verglichen.

Ergebnis dieser Evaluierung ist ein Vergleich der vorgestellten Methoden im Bezug auf Sinnhaftigkeit, Einsetzbarkeit und Effektivität. Weitere Ziele sind die technischen Details dieser Methoden mit Hinweisen auf entsprechende Schwachpunkte in VoIP-Netzwerken zu evaluieren. Im Anschluss wird im Kapitel 8 eine Zusammenfassung der gesamten Arbeit geliefert, sowie im Kapitel 9 ein Ausblick auf eventuelle zukünftige Methoden und Aussichten präsentiert.

1.3 Methodik

Die Masterarbeit Evaluation von Methoden zur Abwehr von SPIT in VoIP basiert großteils auf einer theoretischen Ausarbeitung, die sich auf aktuelle Literatur stützt.
Das methodische Vorgehen bei der Verfassung dieser Arbeit basiert auf dem Einlesen in die entsprechende Fachliteratur, welche in der ersten Phase zur Bearbeitung der Basisthemen Security, VoIP und SPIT dient und in der darauffolgenden Phase der Masterarbeit Fachwissen zum Thema Abwehrmethoden von SPIT liefert. Das Ergebnis dieser Fachrecherche ist ein tiefer Einblick in das Thema VoIP und die aktuellsten technischen Möglichkeiten zur Abwehr von SPIT. Aufbauend auf dem Wissen aus Grundlagen und Fachliteratur kann ein Vergleich bzw. eine Bewertung und Auswahl der Methoden vorgenommen werden.

Kapitel 2

Grundlagen der IT-Security

Im zweiten Kapitel werden allgemeine Punkte wie die Grundbegriffe der IT-Security, die verschiedenen Sicherheitsziele, welche aus dem Grundschutzkatalog abgeleitet werden, sowie Schutzbedarf, Spannungsfelder und Bedrohungs- bzw. Risikoanalysen behandelt. Dieses Kapitel dient als Grundlage für alle weiteren Kapitel.

Es wird kurz erläutert, was Security im Bezug auf das Internet bedeutet. Des weiteren soll eine klare Abgrenzung der Teilgebiete aus dem Bereich IT-Security erreicht werden, wobei das Kerninteresse auf Internetsecurity liegt.

2.1 Betrachtung unterschiedlicher Sicherheitsziele

Aus der Sicht des Bundesamtes für Sicherheit in der Informationstechnik in Deutschland (BSI) werden folgende Sicherheitsziele (security objectives) angeführt: [BSI10]

- Integrität (integrity)
- Verfügbarkeit (availability)
- Vertraulichkeit (privacy, confidentiality)
- Authentizität (authenticity)
- Nicht-Abstreitbarkeit (non-repudiation)
- Verbindlichkeit (commitment, liability)
- Zuverlässigkeit (reliability, dependability)

2.1.1 Integrität

Unter der Integrität (integrity) von Informationen versteht man die Vollständigkeit und Korrektheit (Unversehrtheit) der übertragenen Nachricht auf Sender- und Empfängerseite. Das bedeutet, es wird davon ausgegangen, dass der Inhalt der Nachricht bei der Übertragung unverändert bleibt. Die Integrität von Nachrichten kann man durch verschiedenste Methoden wie z.B. Hash-Verfahren, message authentificeation codes oder digitale Signaturen kontrollieren. [BSI09b]
Möglich wird dies dadurch, dass diese Verfahren direkt mit den Inhalten der Nachrichten verknüpft sind. Auswirkungen, welche durch mangelhafte Integrität verursacht werden, sind zum Beispiel Fehlbuchungen, falsche Lieferungen oder fehlerhafte Produktionen. Seit den letzten Jahren wird dem Faktor Verlust an Authentizität als Teilbereich der Integrität ein höherer Stellenwert zugesprochen. [BSI09c] Auswirkungen in diesem Teilbereich sind beispielsweise Bestellungen und Zahlungsanweisungen, welche an falsche Personen ausgestellt werden. So kann es zur Fälschung digitaler Identitäten kommen. [BSI09b], [Bun10]

2.1.2 Verfügbarkeit

Mit der Verfügbarkeit (availability) einer IT-Landschaft wird die Eigenschaft des Systems, innerhalb eines bestimmten Zeitraums mit einer bestimmten Wahrscheinlichkeit die vom eingesetzten System erwarteten Anforderungen zu erfüllen, bezeichnet. Oftmals wird die Verfügbarkeit als Qualitätsmerkmal herangezogen. [BSI09b], [Bun10]

2.1.3 Vertraulichkeit

Um eine sichere und effektive Datenverarbeitung zu gewähren, kommt dem Faktor Vertraulichkeit (confidentiality) ein sehr hoher Stellenwert zu. In der IT versteht man unter vertraulich, dass die zu verarbeitenden Daten und Informationen nur für berechtigte Personen verfügbar sind. Nicht autorisierten Personen wird hingegen der Zugang zu diesen Informationen verwehrt. [BSI09b]

2.1.4 Authentizität

Unter der Authentizität (authenticity) versteht man die Echtheit, Zuverlässigkeit, Rechtsverbindlichkeit, Unveränderbarkeit und Glaubwürdigkeit einer Mitteilung. Sie ist in vielen Fällen nach heutiger Rechtsauffassung nur bei originaler Mitteilung, z.B. Direktkommunikation oder Schriftgut mit originaler oder digitaler Unterschrift der zur Abgabe von schriftlichen Willenserklärungen autorisierten Personen gewährleistet. [Rec99]

Durch Authentizität wird sichergestellt, dass eine Nachricht tatsächlich von demjenigen Sender stammt, der sich auch als Absender ausgibt.
Signaturen werden zur Sicherung der Authentizität und Integrität von Daten sowie von Entitäten auf der Basis zugrunde liegender kryptographischer Mechanismen eingesetzt. In entsprechende technische, organisatorische und rechtliche Rahmenbedingungen in Form von Zertifizierungsinfrastrukturen eingebettet, ermöglichen Signaturen die Realisierung einer definierten Verbindlichkeit der über öffentliche oder private Netze übertragenen Informationen, aber auch der in Archivierungssystemen bereitgestellten Daten. [BSI09b], [Inf10]

2.1.5 Nicht-Abstreitbarkeit

Das Hauptaugenmerk der Nicht-Abstreitbarkeit (non-repudiation) ist es, die Nachweisbarkeit gegenüber Dritten sicherzustellen. Der Fokus liegt auf der Gewährleistung, dass versandte und empfangene Daten nicht abgestritten werden können. [BSI09b]

Grundsätzlich werden zwei Unterteilungen getroffen:

1. Nichtabstreitbarkeit der Herkunft: Es soll verhindert werden, dass der Absender von elektronischen Daten und Informationen das Absenden einer Nachricht bestreiten kann. Nichtabstreitbarkeit der Herkunft beinhaltet die Authentizität.

2. Nichtabstreitbarkeit des Erhalts: Es soll verhindert werden, dass der Empfänger von elektronischen Daten und Informationen den Empfang einer Nachricht bestreiten kann.

[BSI09b], [Ren00]

2.1.6 Verbindlichkeit

Unter dem Begriff Verbindlichkeit (commitment, liability) versteht man eine Zusammenfassung der Sicherheitsziele Authentizität und Nicht-Abstreitbarkeit der Zustellung. Das bedeutet, dass bei der Übertragung von elektronischen Daten und Informationen der Sender und Empfänger einer Nachricht ihre Identität bewiesen haben und den Empfang sowie das Absenden nicht in Abrede stellen können.
[Bun10]

2.1.7 Zuverlässigkeit

Microsoft hat sechs Merkmale festgelegt, anhand derer sich die Zuverlässigkeit eines Systems messen lässt. Dieses Qualitätsmerkmal beinhalten im Wesentlichen eine Kombination aus Verfügbarkeit und Integrität.

1. ausfallsicher
   Das System kann dem Benutzer auch dann Dienste anbieten, wenn eine interne oder externe Unterbrechung stattfindet. (Verfügbarkeit)

2. wiederherstellbar
   Das System kann nach einer benutzer- oder systembedingten Unterbrechung mittels Instrumentation und Diagnose problemlos wieder ohne Datenverlust in seinen ursprünglichen Zustand zurückgeführt werden. (Verfügbarkeit)

3. kontrolliert
   Das System erfüllt im Bedarfsfall immer korrekt und rasch die Anforderungen an den gewünschten Dienst. (Integrität, Verfügbarkeit)

4. unterbrechungsfrei
   Erforderliche Änderungen und Aktualisierungen unterbrechen die Betriebsbereitschaft des Systems nicht. (Verfügbarkeit)

5. produktionsbereit
   Das System weist bereits bei der Auslieferung nur ein Minimum an Fehlern auf, sodass nur eine begrenzte Zahl an vorhersehbaren Aktualisierungen nötig ist. (Verfügbarkeit)

6. berechenbar
   Das System funktioniert wie erwartet bzw. wie versprochen, und was früher funktioniert hat, funktioniert auch jetzt. (Integrität, Verfügbarkeit)

[Mic05]

2.2 Schutzbedarf

Daten und Informationen sind heutzutage Teil der wichtigsten Güter, die ein Unternehmen oder eine Behörde besitzen. Somit ist es unerlässlich, diese Werte auch bestmöglich zu schützen. Ein Teil der verfügbaren Informationen, welche sich digitalisieren lassen, werden mittels der Informationstechnologie persistent gespeichert. Informationen, welche nicht ausreichend geschützt werden, stellen einen wesentlichen Risikofaktor für das Unternehmen dar. Oftmals können diese Risikofaktoren sich auch existenzbedrohend auswirken. Grundlegenden Informationsschutz erreicht man schon mithilfe relativ geringer Maßnahmen. [BSI09b]

Das BSI [BSI09b] bietet mit dem IT-Grundschutz einen Leitfaden, um jene wichtigen Informationen eines Betriebes ausreichend schützen zu können, welche einen Schutzbedarf bis hin zur Schutzkategorie Mittel besitzen.

Alle Schutzkategorien über dem Schutzbedarf Hoch werden mit speziellen Maßnahmen abgedeckt. Dargestellte Schutzkategorien werden im Laufe des Kapitels noch näher behandelt. Das BSI bietet eine Kombination aus IT-Grundschutz-Vorgehensweisen und IT-Grundschutzkatalogen an, welche die Voraussetzungen für den Einsatz in verschiedensten Umgebungen darstellen.

Der Einsatz von elektronischer Datenverarbeitung ist im heutigen Alltag weder aus beruflicher noch privater Sicht wegzudenken. Datenverarbeitung erfolgt in der modernen Welt nicht nur lokal, sondern global, über die ganze Welt verteilt.

Die meisten Behörden- und Unternehmensziele können nur bei ordnungsgemäßem und sicherem IT-Einsatz erreicht werden.
Schutzbedarf ist nicht quantifizierbar und wird daher zum Beispiel in drei Kategorien eingeteilt: [BSI09g]

1. Normal

   Die Schadensauswirkungen sind begrenzt und überschaubar.

2. Hoch

   Die Schadensauswirkungen können beträchtlich sein.

3. Sehr hoch

   Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Es ist es aber sehr wichtig, sich nicht nur allein auf die technische Sicherheit von IT-Systemen zu konzentrieren, da Informationssicherheit nicht nur eine Frage der Technik ist, sondern auch sehr stark von den organisatorischen und personellen Rahmenbedingungen abhängt. Weitere Bedingungen sind der richtige Umgang mit zu schützenden Daten, die Sicherheit von Betriebsumgebungen, die Verlässlichkeit von Dienstleistungen, usw.

Wie schon erläutert, sind die Informations- und auch die immer stärker werdende Kommunikationstechnik wesentliche Teile unserer heutigen Kultur. Der Stellenwert dieser Technologien steigt zunehmend an. Im Speziellen sind nachfolgende Entwicklungen auffallend und von Bedeutung:

- Vernetzung:
  Das Phänomen der Vernetzung wurde in den letzten Jahren durch das Internet, VoIP und ähnliche Techniken immer mehr vorangetrieben. Es ist state of the art, nicht mehr lokal gebunden und isoliert zu sein, sondern mit anderen Rechnern und Menschen weltweit zu kommunizieren. Die gemeinsame Vernetzung ermöglicht zum Beispiel den Zugriff auf

verteilte Ressourcen, den Zugriff auf gemeinsame Datenbestände oder die weltweite Kommunikation via Internet. Vernetzung ist die Voraussetzung, internationale Kooperationen zu erleichtern.

- IT-Verarbeitung und Durchdringung
  Im heutigen Alltag fällt es oftmals nicht auf, dass viele Bereiche von der IT beeinflusst werden. Durch den Fortschritt von Technik und Technologie ist es möglich, Hardware und andere Komponenten immer kleiner zu gestalten und somit in sehr viele Lebenslagen und Situationen zu integrieren, ohne dass diese merklich auffallen. Beispiel dafür ist das Mobiltelefon, welches inzwischen ein integraler Bestandteil unserer Gesellschaft ist. Des Weiteren werden hier alle Sensoren und Techniken im Auto angesprochen, um auf veränderte Umwelt- und Umgebungsbedingungen zu reagieren.

- Schwindende Netzgrenzen
  Bis vor kurzem ließen sich Geschäftsprozesse und Anwendungen eindeutig auf die IT-Systeme und die Kommunikationsstrecken dazwischen begrenzen. Ein Beispiel dafür ist Global Software Development (GSD). GSD ist eine Art von Softwareentwicklung, in der Teams nicht lokal zusammen arbeiten, sondern geografisch getrennt sind. Die Teams befinden sich oftmals an mehreren verschiedenen, auf der ganzen Welt verteilten Orten. In vielen Fällen werden die Teams derselben Institution angehören, sie können aber auch zum Beispiel verschiedenen Organisationen angehören, die ein Projekt zusammen bearbeiten, oder eine weitere Möglichkeit wäre, dass man Teile eines Projektes durch outsourcing ausgelagert hat. Die geografische Trennung der Entwicklerteams kann von 50 Meter bis hin zu tausenden Kilometer Entfernung gehen. Nachfolgende Abbildung 2.1 auf Seite 18 von GSD soll sinnbildlich zeigen, dass die Entwicklung eines Projektes global verteilt sein kann, sodass z.B. die Anforderungsanalyse in Amerika geschieht, die späteren Tests aber in Asien durchgeführt werden.

  [fI10]

2.3 IT-Grundschutzkataloge

Da der IT-Grundschutz nach BSI, einer deutschen Institution, auch international sehr großes Ansehen genießt, werden alle Unterlagen auch in digitaler Form in englischer Sprache angeboten.
Inhalt der IT-Grundschutzkataloge ist eine detaillierte Beschreibung von Standard-Sicherheitsmaßnahmen, welche in allen IT-Systemen, die den Schutzbedarf Normal nicht übersteigen, eingesetzt werden können. [BSI09f]

Unter Anderem beinhalten diese Maßnahmen Folgendes:

- Maßnahmen für Standardgeschäftsprozesse, Anwendungen und IT-Systeme, bei denen der Schutzbedarf als Normal eingestuft wird.
- Eine Spezifikation der Gefährdungslagen von IT-Systemen
- Eine Beschreibung der Maßnahmen als Hilfe zur Umsetzung
- Eine Übersicht über Prozesse zur Erreichung und Aufrechterhaltung eines bestimmten Sicherheitsniveaus. Des Weiteren sind Prozesse beschrieben, die eine Ermittlung des derzeitigen Sicherheitsniveaus ermöglichen.

Dieses Ermittlungsverfahren basiert auf einem Ist-Soll-Vergleich und wird in den BSI-Standards 100-1, 100-2 und 100-3, IT-Grundschutz, detailliert beschrieben. [BSI09d]

Aufbau der IT-Grundschutzkataloge

Die Grundaufgaben der Grundschutzkataloge werden in einem Informationssystem verwaltet. Als Informationssystem bezeichnet man ein System, welches die Planungs- sowie Lenkungsaufgaben beschreibt, die notwendig sind, um Informationsprozesse aufzubauen und umzusetzen. Informationssysteme werden oftmals als IS-Management bezeichnet. Ein IS-Management wird heutzutage als Grundlage für jedes funktionierende Sicherheitssystem angesehen. Der BSI-Standard beschreibt ein IS-Management in seinen Funktionen und Leistungsumfängen und bezeichnet dieses System als „BSI-Standard 100-1 Managementsystem für Informationssicherheit“ (ISMS).
[BSI09g], [BSI09b], [BSI09f]
Aufbauend auf das oben genannte IS-Management nach BSI werden die IT-Grundschutzkataloge aus Bausteinen zusammengesetzt. Diese geben die Gliederung und Struktur vor. Inhaltlich wird beschrieben, wie ein funktionierendes IS-Management eingerichtet und konfiguriert bzw. laufend weiterentwickelt wird, um einen sicheren Betrieb zu ermöglichen.

Bausteine

Wie erläutert werden die Grundschutzkataloge in Bausteine unterteilt. Bausteine selbst haben eine kurze Beschreibung der jeweiligen Komponenten, IT-Systeme und Vorgehensweisen zum Inhalt. Des Weiteren finden sich hier Informationen zur Gefährdungslage und Maßnahmenempfehlungen wieder. Bausteine werden nach dem Schichtenmodell wie folgt katalogisiert:

- B 1: übergreifende Aspekte der Informationssicherheit
- B 2: Sicherheit der Infrastruktur

- B 3: Sicherheit der IT-Systeme
- B 4: Sicherheit im Netz
- B 5: Sicherheit in Anwendungen

[BSI09f]

Im Teilbereich Gefährdungskataloge werden die Gefahren beschrieben, welche in den einzelnen Bausteinen unter dem Punkt Gefährdungslage aufgezählt werden:

- G 1: Höhere Gewalt
- G 2: Organisatorische Mängel
- G 3: Menschliche Fehlhandlungen
- G 4: Technisches Versagen
- G 5: Vorsätzliche Handlungen

[BSI09f]

Der Teilbereich Maßnahmenkataloge beschreibt den Unterpunkt Sicherheitsmaßnahmen aus den Bausteinen der IT-Grundschutzkataloge. Die Einteilung erfolgt in sechs Unterpunkte:

- M 1: Infrastruktur
- M 2: Organisation
- M 3: Personal
- M 4: Hard- und Software
- M 5: Kommunikation
- M 6: Notfallvorsorge

[BSI09f]

Um den Aufbau eines effektiven Sicherheitsprozesses zu gewährleisten, muss eine gewisse Anzahl von Aktionen vonstatten gehen. Dazu geben die IT-Grundschutz-Vorgehensweise (BSI-Standard 100-2) [BSI09d], aber auch die IT-Grundschutzkataloge hilfreiche Hinweise, um eine theoretische und praktische Umsetzung dieser Prozesse zu ermöglichen. Des Weiteren finden sich

Lösungsansätze, die Informationssicherheit betreffend, in diesem Aufbau wieder. Beispiele dafür sind Sicherheitskonzeption, Revision oder Zertifizierungen. [BSI09a] Die Anwendungsweise des IT-Grundschutzes ist je nach Verwendungszweck unterschiedlich. In Abbildung 2.2 auf Seite 18 ist die grundsätzliche Vorgehensweise beim Aufbau des IT-Grundschutzes schematisch dargestellt. Abbildung 2.2 auf Seite 18 kann ferner als eine Art Aktionsplan verstanden werden, welcher alle wesentlichen Schritte beinhaltet, um einen ordentlichen Sicherheitsprozess zu erzeugen. Ziel ist es, mit diesem Aktionsplan ein entsprechendes Sicherheitsniveau zu erreichen bzw. im Weiteren aufrecht zu erhalten. Der Aktionsplan teilt sich in vier Abschnitte ein:

1. Initiierung des Sicherheitsprozesses:

   Darunter fällt unter anderem die Übernahme der Verantwortung durch die Führungsebene. Weitere Punkte sind die Planung und Spezifikation des Sicherheitsprozesses, die Erstellung einer Leitlinie für die Informationssicherheit und Aufbau und Strukturierung des Informationsmanagements und der Organisationsstruktur. Ein wesentlicher Punkt ist die Bereitstellung der benötigten Ressourcen aus den Bereichen Human Ressources, Finance Ressources und Time Ressources. Ziel muss es sein, alle beteiligten Mitarbeiter in den Sicherheitsprozess einzubinden.

2. Erstellung einer Sicherheitskonzeption

3. Umsetzung der Sicherheitskonzeption und Realisierung der entwickelten Sicherheitsmaßnahmen

4. Aufrechterhaltung der Informationssicherheit im Betrieb und ständige Verbesserung

[BSI09a]
Für weiterführende Informationen, wird auf [BSI09e] verwiesen.

Weitere Informationen zu Anwendung und Gebrauch von Grundschutzkatalogen sind dem Grundschutz nach BSI zu entnehmen [BSI09f].

2.4 Ablauf eines Angriffs

Das Ablaufszenario eines Angriffs auf IT-Infrastrukturen unterteilt sich grundsätzlich in drei Phasen welche in diesem Abschnitt basierend auf [Wes07] beschrieben werden.

Phase I
Sammeln von Informationen über das spezielle Netzwerk. Diese Information dient als Basis für den späteren Angriff. Phase I erstreckt sich oft über

Abbildung 2.1: Globale Software Entwicklung [Gsd10]

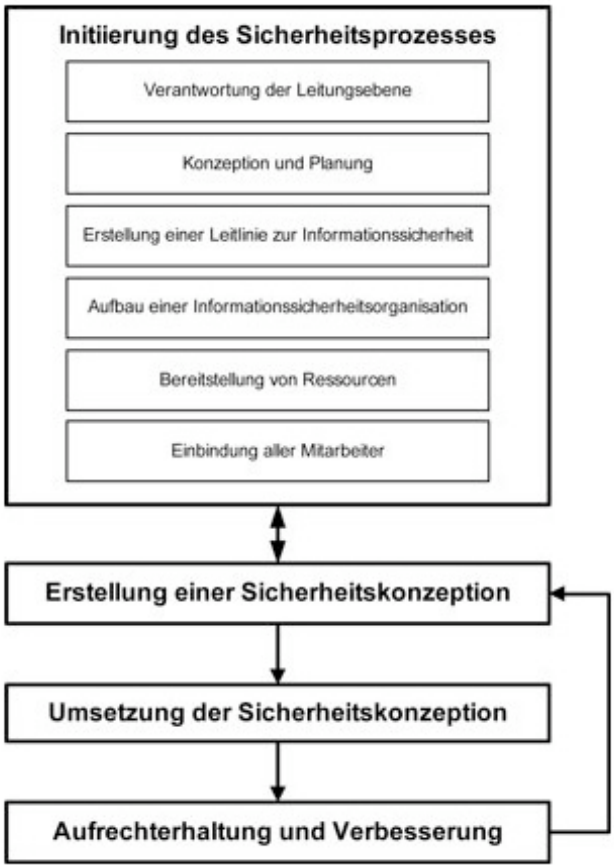


Abbildung 2.2: BSI-Standard 100-2 [BSI09a]

mehrere Monate und kann bis zu 90 Prozent der Zeit aller drei Phasen in Anspruch nehmen. Nach dem Sammeln der Basisinformationen konzentriert sich der Hacker auf das Ausspionieren offener Ports sowie anderer offener, nicht gesicherter Dienste des zu attackierenden Hosts.

Phase II
In dieser Phase wird eine Art „passives Ausspionieren“ betrieben. Diese Phase gliedert sich in zwei Teilschritte. Im ersten Schritt sammelt der Angreifer Informationen über sein Ziel, ohne Kontakt aufzunehmen, was ein Sammeln legaler Daten darstellt. Trotzdem werden die so erhaltenen Daten zu einem Zweck gesammelt, der in späterer Folge zu einer verbotenen Tat führt. Diese Informationen werden aus Quellen, wie zum Beispiel nachfolgend dargestellt, bezogen:

- allgemeine Informationen, welche man einer Homepage entnehmen kann
- Informationen aus Foren
- Informationen, die durch eine Online-Suchmaschine gewonnen werden
- Stellenangebote und interne Dokumente
- soziale Kontakte

Phase III
Diese Phase wird auch als „aktives Ausspionieren“ bezeichnet. Aktive Versuche, Information zu beschaffen, werden meistens in Logdateien festgehalten und können somit nachverfolgt werden.

Kapitel 3

Grundlagen von Voice over IP

Mit Voice over IP wird allgemein die auf dem Internet basierende Telefonie mittels TCP/IP-Protokoll bezeichnet.

Andere Begriffe für VoIP Kommunikation sind:

- IP-Telefonie
- LAN-Telefonie
- SIP-Telefonie
- Voipen [Dud09]
- Internettelefonie

3.1 Rechtliche Rahmenbedingungen

Rechtliche Rahmenbedingungen spielen auch im Bereich von VoIP eine wesentliche Rolle. Auch mit Maßnahmen der IT-Security müssen solche Rahmenbedingungen sichergestellt und von der VoIP-Infrastruktur unterstützt werden.

Telekommunikationsrecht
Das Telekommunikationsrecht ist in Österreich auf das österreichische Gesetz abgestimmt. Damit man die wesentlichen Kernbereiche des Gesetzes, die im Zusammenhang mit VoIP-Regulierungen von Bedeutung sind, identifizieren kann, wurden vorerst die wichtigsten und traditionellsten Normen zusammengefasst:

"Die zentrale Rechtsvorschrift des Telekommunikationsrechts in Österreich ist das Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 TKG 2003), BGBl I 2003/70 idF BGBl I

2004/178 und 2005/133. Das TKG 2003 ist in seiner Stammfassung am 20. August 2003 in Kraft getreten."[Rec03]

Zunächst werden die gesetzlich im Telekommunikationsgesetz 2003 verankerten geltenden Richtlinien der Telekommunikation betrachtet.

Wettbewerbsregulierung
Grund des Telekommunikationsgesetzes 2003, welches mit 19. August 2003 das Vorgängergesetz in Form eines Bundesgesetzes abgelöst hat, war die Übereinstimmung mit den Richtlinien der Wettbewerbsförderungen. [Rec03]

Grundkonzept ist die sog. asymmetrische Regulierung, wonach besondere Gesetzespflichten für Unternehmen mit beträchtlicher Marktmacht bestehen. Diese besagen, dass Wettbewerbern der Zugang zu Netzeinrichtungen und Netzfunktionen gewährt werden muss. [Rec03]

VoIP-Regulierung bezogen auf die Gesetzeslage in Österreich
Für den Betrieb von VoIP-Diensten am österreichischen Markt und demnach österreichischen Gesetzen unterliegend wird Folgendes festgehalten: Die Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH) hat im dritten Quartal 2004 ein Dokument entworfen [Rtr04], welches vorläufige regulatorische Einstufungen von öffentlichen VoIP-Diensten vornimmt. In diesem Dokument werden drei Klassen von Diensten im Bereich VoIP unterschieden. Entscheidungskriterien waren vor allem, ob auch öffentliche Anschlüsse via VoIP erreichbar sind oder nicht. Jene Dienste, die Funktionalität im öffentlichen Telefonnetz bieten, will die RTR-GmbH als öffentlichen Telefondienst im Sinne des §3 Z 16 TKG 2003 eingestuft wissen, für welchen die oben kurz dargestellten Betriebsauflagen gelten.

Ein Punkt, der weitestgehend unerörtert scheint, ist die Frage der Wettbewerbsregulierung im Hinblick auf das konkurrierende Verhalten zwischen Festnetz und Internettelefonie. Dieses Konkurrenzverhalten hat allerdings größte Auswirkungen auf den gesamten Wirtschaftszweig und bedarf einer Klärung. Die künftige Markt- und mit ihr einhergehend die weitere Rechtsentwicklung darf daher mit Spannung erwartet werden. [Rtr06]

Die asymmetrische Regulierung ist des Weiteren von grundlegender Bedeutung für die Regulierungsbehörde, die für Endgeltkontrollen zuständig ist. Zur Beurteilung, ob einem Unternehmen beträchtliche Marktmacht zukommt oder nicht, nahm die Telekommunikationsmärkteverordnung 2003 eine Unterscheidung in 16 verschiedene Märkte vor, die sich hauptsächlich auf das öffentliche Telefonnetz beziehen. Ausnahmen bilden §3 Z 16 TKG 2003. [Rtr03] [Rec03]

Betriebsauflagen
Anbieter von Telefondiensten, welche diese der Öffentlichkeit zugänglich machen und somit am Markt teilnehmen, müssen eine Allgemeingenehmigung vorweisen. Diese Genehmigung ist entsprechend § 15 TKG 2003 zu beantragen.

Öffentliche Telekommunikationsanbieter sind laut §20 TKG 2003 dazu angehalten, die Erreichbarkeit von Notrufnummern samt Identifikation des anrufenden Anschlusses zu garantieren. Bezogen auf nationale Ebenen ist gemäß §5 Abs. 1 der Kommunikationsparameter-, Entgelt-, und Mehrwertdiensteverordnung Transport und Weitergabe der Rufnummer des Anrufers zwischen allen an der Verbindung beteiligten öffentlichen Kommunikationsnetzen verpflichtend vorgeschrieben. Weitere Bestimmungen und Verordnungen regeln die Überwachung des Fernemeldeverkehrs in Ausnahmefällen, die Gewährleistung des Kommunikationsgeheimnisses, usw. [Rtr06]

Überwachung von Internetinhalten
Artikel 8 der Europäischen Menschenrechtskonvention (EMRK) schützt das Privat- und Familienleben sowie auch die private Korrespondenz. [Bun07] Dies umfasst auch den Schutz von privater Korrespondenz am Arbeitsplatz. Der EMRK wurde ein Fall vorgelegt, in dem eine Mitarbeiterin einer öffentlichen Schule vonseiten des Direktors in Hinblick auf ihre private Nutzung von Internet, E-Mail und Telefon überwacht wurde. Nicht nur wurden Aufzeichnungen über die einzelnen E-Mails, die besuchten Webseiten und die getätigten Telefonate geführt, es wurde auch nachträglich Personen, mit denen die Mitarbeiterin Kontakt aufgenommen hatte, angerufen und zum Inhalt der Gespräche befragt. Eine Entscheidung des Gerichtshof sagt, dass Privatkontakte am Arbeitsplatz nicht prinzipiell erlaubt und vom Schutz des Artikels 8 EMRK umfasst werden. Es kommt auf eine Abwägung zwischen den Interessen des Überwachten und den Interessen des Arbeitgebers an. [Bla04]

Lauschangriff
Die Genehmigung für einen solchen Angriff ist bei der Staatsanwaltschaft zu beantragen und von der Rechtskammer zu legitimieren. Eine Ausnahme bildet hier ein Lauschangriff bei gegenwärtigen schwerwiegenden Freiheitsentziehungen. Dies ist besonders oft bei Geiselnahmen der Fall. [Wie03]

Unterschieden wird hier zwischen dem großen und dem kleinen Lauschangriff. Als Voraussetzung für den großen Lauschangriff gilt, dass das mögliche Mindeststrafmaß eine zehnjährige Freiheitsstrafe übersteigt. [Wie03]

Remote Forensic Software
Die Remote Forensic Software oder so genannte Online-Durchsuchung (Polizeitrojaner) ist ein aktuelles Thema im Bereich der digitalen Strafverfolgung. Ziel von derartiger Software ist es, der Polizei den Zugriff auf die lokale Festplatte sämtlicher Computer über ein Netzwerk wie beispielsweise das Internet zu ermöglichen. Dies soll vor allem dazu dienen, geplante Verbrechen schon vorzeitig erkennen zu können und entsprechende Maßnahmen dagegen einzuleiten. Die rechtliche Situation in Österreich für diese Thematik sieht derzeit wie folgt aus: Die Durchsuchung von Rechnern ist derzeit im Rahmen von Hausdurchsuchungen bereits möglich. Eine Hausdurchsuchung stellt allerdings einen schweren Eingriff in die Privatsphäre eines Menschen dar. Aus diesem Grund gelten für derartige Durchsuchungen besondere Auflagen wie z.B. die richterliche Anordnung. Des Weiteren darf eine solche Durchsuchung nur jene Bereiche umfassen, welche tatsächlich dem Verdächtigen zugeordnet werden können. Ebenso müssen Gegenstände oder Personen, nach denen gesucht wird,genau bezeichnet werden. §139 StPO. [Rec10] Es ist daher nicht zulässig, einfach eine Durchsuchung des Eigentums einer Person durchzuführen, in der Hoffnung, belastendes Material zu finden. Bei Hausdurchsuchungen weiss die betroffene Person in der Regel bescheid und kann die Durchsuchung abwenden, indem die betroffenen Gegenstände freiwillig ausgehändigt werden. Trotz strenger Auflagen und Regeln finden immer wieder ungerechtfertigte Durchsuchungen statt, welche durch §303 StGB [Rec74] , der eine spezielle Strafdrohung gegen Beamte vorsieht, eingeschränkt werden sollen. [DAT07], [Bun07].

Alle eben genannten Voraussetzungen treffen auf den Polizeitrojaner nicht zu. Eine derartige Software würde ohne Kenntnis des Verdächtigen einen Zugriff auf den Rechner ermöglichen (inkl. VoIP). Ein weiteres Problem ist, dass der betroffenen Person kein Rechtsmittel zur Verfügung steht, um wie bei der Hausdurchsuchung die geforderten Daten herauszugeben, um eine Durchsuchung abwenden zu können. Es ist außerdem nicht gewährleistet, dass der von der Polizei infizierte Computer von der verdächtigten Person überhaupt genutzt wird. Der Eingriff in die Grundrechte Dritter ist aufgrund der Tatsache, dass ein Rechner oft von mehreren Personen verwendet wird, fast nicht auszuschließen. Des Weiteren gibt es auch einen strafrechtlichen Hintergrund zu beachten. Die Entwicklung und der Einsatz eines Trojaners könnte in Österreich nur durch das Verstoßen gegen §126c StGB [Rec74] erfolgen, worin jede Verwendung eines Programms, welches zum Ausspähen und zur Nutzung von Sicherheitslücken bestimmt ist, unter Strafe gestellt ist. Nach dem Datenschutzrecht §14 DSG [Rec00] sind alle Verarbeiter von personenbezogenen Daten verpflichtet, dem Stand der Technik entsprechende Sicherheitsvorkehrungen zu treffen, um mögliche Angriffe wie beispielsweise die von Trojanern zu verhindern. Das betrifft in diesem Fall natürlich auch Internet Service Provider, welche Webserver oder Mailboxen bereitstellen.

Ein gezieltes Offenhalten von Hintertüren für z.B. den Polizeitrojaner würde zwangsläufig auch zahlreiche andere nicht verdächtige Personen betreffen. Diese könnten unter Berufung auf diese fehlenden Sicherheitsbestimmungen Strafverfahren einleiten.

Abgesehen von den rechtlichen Aspekten gibt es auch einige technische Schwierigkeiten, die überwunden werden müssen, wie beispielsweise unterschiedliche Betriebssysteme, Firewalls und Verschlüsselungsalgorithmen. Ein wichtiger Punkt, der nicht unbeachtet bleiben darf, ist die Gefahr, dass nicht verhindert werden kann, dass sich Kriminelle über den Polizeitrojaner Zugang zu Fremdsystemen verschaffen.

3.2 Grundlegende Aspekte der Geschichte der Telefonie

Der Abschnitt Grundlegende Aspekte der Geschichte der Telefonie bildet lediglich einen Auszug aus der Geschichte der Telefonie.

Im Jahre 1880 wurde das Telefon als die Innovation des Jahrhunderts angepriesen.

Da Kommunikation als eines der Grundbedürfnisse des Menschen gilt, hat sich in der menschlichen Evolution allein die Art der Informationsweitergabe geändert. Mit dem Telefon hat sich eine Technologie in unserem Leben festgesetzt, welche schon seit Jahrzehnten fixer Bestandteil unserer Kultur ist. Es wird als normal angesehen, dass man in wenigen Sekunden mit Personen auf der ganzen Welt in Verbindung treten kann.

Betrachtet man die Anfänge der Telefonie, so wurden die Gespräche noch händisch vom Personal am Amt vermittelt. Das bedeutet, die Verbindung zwischen den zwei Parteien wurde durch eine Person im Amt durch Setzen von Metallstöpseln ermöglicht.

Die eigentliche geschichtliche Entwicklung des Telefons begann aber schon zwanzig Jahre vor dem Aufkommen in Österreich. Ein deutscher Physiker names Phillip Reis entwickelte 1861 das erste funktionsfähige Gerät zur Übertragung von Signalen. Es war möglich, auf elektrischem Wege Musik, Sprache und dergleichen zu übertragen und wiederzugeben.

Von der Festnetztelefonie geleitet, ging die Motivation in Richtung Ferngespräche quer durch die ganze Welt. Im Jahr 1867 machte Alexander Graham Bell eine Entwicklung, die bei der menschliche Sprache eine Membran vibrieren ließ. Durch die erzeugten Vibrationen entstanden in einer Drahtspule

Stromschwankungen, welche nach der Übertragung zu einem anderen Gerät wieder in menschliche Sprache umgewandelt werden konnten.
Über diese Entwicklung wurde ein Patent ausgesprochen und im Jahre 1860 wurde mit demselben Gerät eine Verbindung zwischen Boston und Cambridge aufgebaut und somit das erste Ferngespräch der Welt geführt.

Im Juni des Jahres 1881 erteilte das k.k. Handelsministerium der Wiener Privat-Telegraphen-Gesellschaft eine Concession zum Betrieb von Telefonanlagen. Die Netzabdeckung erschein zwar aus heutiger Sicht wenig beeindruckend, denn die Telefonanlagen durften lediglich in einem Umkreis von fünfzehn Kilometern rund um den Wiener Stephansturm (sic) betrieben werden. Schon drei Monate später jedoch wurde der Betrieb der Telefonanlagen auf ganz Wien ausgeweitet, im Dezember 1881 konnte in der Wiener Friedrichstraße die erste Telefonzentrale Österreichs eröffnet werden. Mit 154 Teilnehmern, darunter Zeitungen, Großunternehmern und Banken, wurde der Netzbetrieb gestartet. [Aus09]

Im Jahre 1910 kamen schließlich die ersten Telefone, die mit einer Wählscheibe und einem Hörer ausgestattet waren, auf den Markt. Zugleich bereitete die Post- und Telegraphenverwaltung mit der Umstellung der Verbindungen innerhalb eines Ortes vom handvermittelten Dienst auf Selbstwählverkehr eine kleine Revolution vor. Nun konnten die Teilnehmer erstmals ihre Gesprächspartner innerhalb eines Ortes direkt und ohne Vermittlungshilfe erreichen.

In Österreich nahm die Anzahl der Anschlüsse beispielsweise zwischen 1891 mit zuerst 440 Anschlüssen und dann im Jahr 1895 mit bereits 19.000 Anschlüssen rasant zu. [Aus09]

Das Festnetz wurde im englischen als Public Switched Telephone Network (PSTN) bezeichnet. Der Begriff PSTN wird auch in der Deutschen Sprache benutzt.

Ein weiterer Schritt in der steten Weiterentwicklung der Telefonie war die drahtlose Kommunikation mittels mobiler Telefone. Die Entwicklung dieser ersten mobilen Telefone liegt in etwa 60 Jahre zurück. Unter Mobiltelefon verstand man damals ein etwa zwischen 15 und 20 kg schweres Telefon, welches im Auto zum Einsatz kam. Die Kosten für dieses Telefon lagen in etwa der Höhe der Kosten für einen VW Käfer, den man in diesen Jahren um ca. 5.000DM erstehen konnte. Das bedeutet, die Entwicklung der Mobiltelefonie war von sehr großen und schweren Geräten geprägt. Zweiter negativer Faktor waren die horrenden Kosten für die Endgeräte bzw. für die laufenden Kosten der Telefonate. Das bedeutete, zu den Anfängen des mobilen Zeitalter ein Mobiltelefon zu besitzen, blieb den reichen Unternehmern und Politikern vorbehalten. Die ersten Ansätze einer mit der heutigen Situation vergleich-

baren mobilen Telefonie wurden zwischen 1980 und 1990 erbracht, indem in Deutschland die ersten gut ausgebauten Handynetze installiert wurden und mobile Endgeräte in einer Gewichtsklasse von ca. ein kg zu finden waren. Mit fortlaufender Entwicklung wurden die Endgeräte leichter, kleiner und zugleich leistungsfähiger. Parallel zu dieser Entwicklung standen Ausbau und Aufbau von Mobilnetzen weltweit.

[Kle10]

3.3 Einführung in Voice over IP (VoIP)

Die Thematik der Internettelephonie ist ein weiterer Meilenstein der Telekommunikation. Diese Art der Technologie ist nicht neu und etablierte Telefongesellschaften können sich seit etwa zehn Jahren auf die kommende Umstellung vorbereiten. Vom Prinzip her basiert jede IP-Telefonie auf den Internetprotokollen Internet Protocol (IP), Transmission Control Protocol (TCP) / User Datagram Protocol (UDP). Im Abschnitt 3.4 Technik wird die nähere Funktionsweise erläutert. VoIP hat auch eine große Bedeutung in der System- bzw. Netzwerk-internen Übertragung, jedoch ist SPIT nur für den Endkunden relevant. [Bad09]

Diese Punkte und der Fakt, dass man in Firmen die gleiche Infrastruktur zur Datenübertragung und zur Telefonie nutzen wollte, brachte den Durchbruch für VoIP. Frühere Technologien wie Frequenzbänder hatten den gravierenden Nachteil, dass Daten und Telefonie nicht dieselben Übertragungsrechte hatten, was eine Benachteiligung eines der beiden gewünschten Dienste mit sich brachte. Herkömmliche Telefonie war davor immer kanalorientiert gewesen. Im Bereich von VoIP spricht man von einer Paketorientierung im Bezug auf die Verbindung.

Eine paketorientierte Übertragung von Sprache nutzt Leitungskapazitäten gezielter aus als die bisherige Methode einer Reservierung der gesamten Leitung. Des Weiteren besteht ein Vorteil durch die Kombination von Sprach- und Datenübertragung bei der Erzeugung und Entwicklung des Übertragungsmediums und daraus resultiert ebenfalls eine erweiterte Flexibilität beim Einsatz von VoIP. Eine Überlegenheit von VoIP gegenüber der herkömmlichen Telefonie ist deshalb gegeben. [Gmb05]

Allgemein bedeutet dies, dass jeder immer erreichbar ist (Konferenzschaltungen sind möglich). Einzige Einschränkung ist derzeit die verfügbare Bandbreite, was sich in den letzen Jahren aber auch immer mehr gebessert hat und bald vernachlässigbar sein wird. Die Verrechnung erfolgt in den meisten Fällen nach dem Datenvolumen, es kann aber auch eine zeitliche Verrechnung erfolgen.

Um Internettelefonie zu verwirklichen, sind einige Voraussetzungen notwendig. Zentraler Punkt ist das Digitalisieren analoger Sprache.

Nicht unwesentlich ist die Sicherheit bei der Datenübertragung. Oftmals besteht die Notwendigkeit, Daten verschlüsselt zu übertragen. In VoIP ist diese Notwendigkeit mittels Secure Real-Time Transport Protocol (SRTP) [Nor04] umgesetzt. In der Praxis kommt diese Möglichkeit allerdings sehr selten zum Einsatz, da sie die meisten VoIP- Anbieter nicht unterstützen. Um Daten paketorientiert übertragen zu können, muss man diese so transformieren, dass sie in IP-Pakete umgewandelt werden. Eine der wesentlichen Herausforderung ist es, die Daten wieder zeitrichtig zusammenzusetzen und analog auszugeben. [Fal08] [Ala08]

Vorteile bei VoIP

- interne Kommunikation via Intranet ohne Gesprächsgebühren
- günstige Anlagenvernetzung durch VPN bzw. Internet
- Internet und Telefonie in einem Medium
- Ortsungebundenheit gegenüber der Festnetztelefonie
- Kostenersparnis bei Ferngesprächen.
- Erweiterbarkeit durch z.B. Zusatzservices, etc. leichter möglich
- unified messaging: Unified Messaging bietet die Möglichkeit, verschiedene Nachrichten-Systeme zentral durch eine einziges Interface zu verwalten. [Ban10]
- Unabhängige Komplettlösung (Internetanschluss vorausgesetzt)
- Prozessoptimierung durch Computer Telephony Integration (CTI) [Inc10]

Nachteile bei VoIP

- Sicherheit: Höheres Sicherheitsrisiko durch die Anbindung an das Internet
- Qualitäts-Defizit: Die Audioqualität hängt von der jeweiligen Verbindungsqualität ab und ist oftmals schwankend, ebenfalls abhängig von der Qualität der Hardware
- Zuverlässigkeits-Defizit: Leitungsausfall bzw. Hardware-/Softwaredefekte

- Stromabhängigkeit: Selbst bei einem regionalen Stromausfall kann man mit einem einfachen herkömmlichen Telefon in der Regel telefonieren, da dessen Stromversorgung über das Festnetz erfolgt. Die VoIP-Anwendung ist dagegen aufgrund der beteiligten Geräte von der häuslichen Stromversorgung abhängig.
- Notrufe: Wegen der Stromabhängigkeit nicht mehr uneingeschränkt möglich
- Strom-Kosten: Wesentlich höher als bei analoger Telefonie, da mehrere Geräte in Betrieb sein müssen
- höheres SPAM/SPIT-Aufkommen aufgrund der günstigeren Kosten (siehe Kapitel SPAM over Internet Telephony)

[Ala08], [Bro09], [Inf08]

3.4 Technik

Voice over IP-Gespräche sind durch einen kontinuierlichen Datenstrom gekennzeichnet, wie das auch bei herkömmlichen analogen Telefonaten der Fall ist. Es erfolgt eine Aufteilung der Datenmenge in einzelne Pakete, welche beim potentiellen Empfänger wieder zusammengesetzt werden. Die Aufteilung in komprimierte Pakete übernimmt ein sogenannter VoIP-Router. Ein Pufferspeicher staut die Pakete auf und leitet diese anschließend an einen Decoder weiter, welcher aus den Datenpaketen eine Tonwiedergabe erzeugen kann. Durch die Pufferfunktion können Schwankungen (Jitter) ausgeglichen werden. Zu Störungen bei den Sprachübertragungen kommt es genau dann, wenn der Jitter die gepufferte Datenmenge übersteigt. Durch die Pufferung ist auch eine Grundverzögerung (delay) gegeben. Dieser Delay ist mit früheren Ferngesprächen vergleichbar. Ein wichtiger Begriff im Bereich von VoIP ist der Begriff Audio, dieser umfasst alle Tonausgaben wie z.B. Sprache, Musik, Geräusch. In der Realität werden aber die Begriffe Audio und Sprache oftmals gleichgesetzt, der Unterschied besteht aber darin, dass Sprache nur einen kleinen Frequenzbereich nutzt, um Informationen zu übertragen. Dieser Bereich liegt bei wenigen Hertz und geht bis zu einer Grenze von ca. 10 kHz. [Jun08] Die Übertragung analoger Signale liegt im Bereich von 300 Hz bis hin zu 3,4 kHz. [Jun08] Durch diese Einschränkungen eignen sich manche Kodierungsverfahren nicht zur Übertragung von Musik oder Ähnlichem. [Col07b], [Sin06], [Lob05], [Nam05]

Nachfolgende Abbildung 3.1 auf Seite 30 liefert eine Darstellung, wie Sprache via VoIP vom Sender zum Empfänger übertragen wird. Der Sender bringt mit der natürlichen Sprache Schallwellen in Bewegung, welche durch einen

Analog-/Digital-Wandler (A/D-Wandler) in digitale Signale verwandelt werden. Nach erfolgreicher Kompression werden die digitalen Signale in einzelne Pakete aufgeteilt. Nach der Übertragung über ein IP-Netz befindet sich an der Gegenstelle ein sogenannter De-Jitter-Buffer, der die Aufgabe hat, die gesamten Datenpakete, welche eine gewisse Verzögerung aufweisen könnten, zusammenzufassen. Der Dekodierer wandelt die Pakete wieder in eine digitale Signalkette um, welche von einen Digital-/Analog-Wandler (D/A-Wandler) in menschliche Sprache umgewandelt werden:

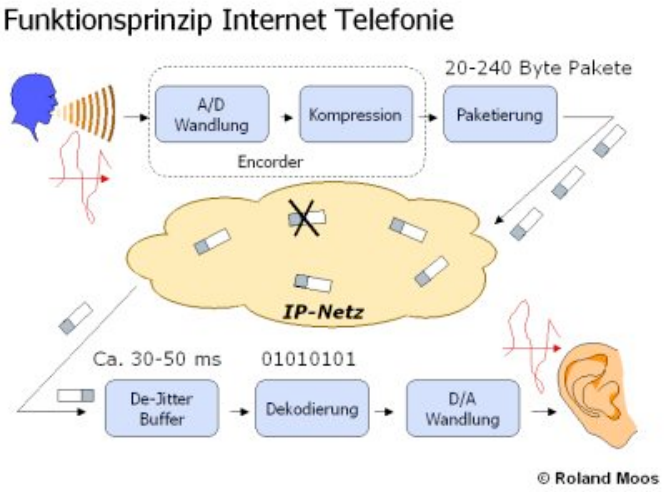


Abbildung 3.1: Funktionsprinzip VoIP [Krö10]

Echos entstehen, wenn Reflexionen einer Schallwelle so stark verzögert werden, dass Sie diesen Schall als separates Hörereignis wahrnehmen. Als Echoschwelle wird die Verzögerung eines reflektierten Schalls bezeichnet, um separat wahrgenommen zu werden. Sie ist abhängig von der Schallcharakteristik und kann zwischen 100 ms (bei Klicks) und mehreren Sekunden (bei langsamer Orcherstermusik) liegen.

Unterhalb der Echoschwelle werden Reflexionen als Nachhall bzw. Hall wahrgenommen.

ENUM

Um an die IP-Telefonadressen zu gelangen, kann ein VoIP-User auf das globale Onlineverzeichnis Telephone Number Mapping (ENUM) zugreifen. An dieser Stelle werden alle Adressen diverser VoIP-Anbieter vereinheitlicht aufgelistet. Nähere Details folgen im Verlauf dieses Abschnittes. ENUM bezeichnet ein Protokoll, welches im Standard RFC 3761 [Lam05] der Internet Engineering Task Force (IETF) spezifiziert ist (früher RFC 2915) [Lam05]. Jede Telefonnummer, welche in ein Domain Name System (DNS) System überführt werden soll, muss zuerst in eine eindeutige Domain überführt werden. Um dieses Problem zu lösen, wurde eine neue Top-Level-Domain eingeführt, welche als e164.arpa definiert wurde. Laut Spezifikation RFC 3761 verwendet das DNS-System spezielle Einträge, um auf einzelne Telefonadressen zuzugreifen. Diese werden als Naming Authority Pointer (NAPTR) bezeichnet. Es besteht die Möglichkeit, für jede ENUM-Domain mehrere NAPTR-Verweise und für jede Adresse genau einen NAPTR-Verweis zu erstellen. Des Weiteren ist eine Priorisierung möglich. [Enu10]

Wenn ein Benutzer über sein Endgerät bzw. über seinen VoIP-Provider einen anderen VoIP-Teilnehmer mit ENUM-registrierter Rufnummer anwählt und selbst eine ENUM-Nummer unterstützt, kann mittels des ENUM-Protokolls die Rufnummer der Gegenstelle bis zum NAPTR-Verweis aufgelöst werden. Dieser Verweis enthält meist in Form einer Session Initiation Protocol (SIP)- oder E-Mail-Adresse eine weitere Kommunikationsadresse. Nach Erhalt dieser Kommunikationsadresse wird in der Regel via SIP eine Verbindung zum NAPTR-Verweis aufgebaut. Sollte eine Verbindung nach Anwahl des ersten Eintrages nicht möglich sein, gibt es individuelle Lösungen, wie damit umgegangen wird. Eine Möglichkeit ist, eine Rufumleitung einzurichten, eine weitere denkbare Möglichkeit ist die Anwahl einer Festnetznummer, wobei eine Prüfung von ENUM auf eine vorhandene SIP-Adresse vorangeht. Sollte dies der Fall sein, kann statt des PSTN das im Allgemeinen günstigere VoIP genutzt werden. [Enu10][Lam05]

Die Abbildung 3.2 auf Seite 32 stellt dar, wie ein Teilnehmer eine Verbindung zu einer ENUM-registrierten Rufnummer aufbaut. Der Teilnehmer unterstützt selber ENUM (ENUM-Lookup). Die erste Anfrage mittels des ENUM-Protokolls richtet sich an ein Service, welches Auskunft über die Position des entsprechenden DNS-Servers mit dem richtigen Eintrag erteilt. Die Rufnummer wird nun bist zum NAPTR-Eintrag über den DNS-Server aufgelöst. Dieser liefert eine SIP-/ E-Mail-Adresse oder Ähnliches als Antwort. Im nächsten Schritt wird mittels des SIP eine Verbindung zum NAPTR-Eintrag aufgebaut.[Enu10], [Lam05]

Somit zeigt sich, das ENUM die Verbindung zweier Welten, Internet und PSTN, darstellt.

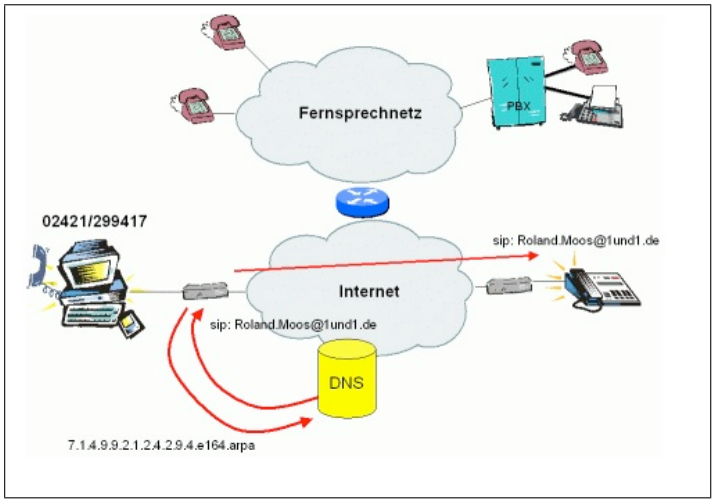


Abbildung 3.2: ENUM [Lam05]

Proxy

Der Begriff Proxy stammt vom englischen Wort proxy representative ab und bedeutet Stellvertretung. Unter einem Proxy versteht man allgemein eine Schnittstelle zur Kommunikation in Netzwerken. Ein Proxy übernimmt die Aufgaben eines Vermittlers, der Anfragen entgegennimmt und über eigene Adressen des Proxys selbst zur gewünschten Gegenstelle verbindet.

Die Vorteile beim Einsatz eines Proxys sind mehr Sicherheit, höhere Performance und oftmals auch bessere Administration. Ein weiterer Vorteil ist das Ausmerzen von Inkompabilitäten in Netzwerken, welche durch einen Proxy als Verbindungsglied beseitigt werden. Der Unterschied zu einer herkömmlichen Adressweiterleitung, wie es mit NAT geschieht, ist, dass der Proxy-Server (dedicated proxy) die Kommunikation selber leitet und aktiv in die Kommunikation eingreifen kann.

Weitere Aufgaben, welche von einem Proxy erledigt werden können, sind:

- Schnittstellte zwischen privatem Netzwerk und dem Internet (Intranet)

- Schutz des eigentlichen Servers

  Die Verwendung eines Proxys ermöglicht eine höhere Angriffssicherheit, da die Komplexität eines Proxys geringer ist als die eines Servers, andererseits besitzen Proxys eine Abstraktionsschicht, weitere Steuerbarkeit und sind meist zentral gehalten.

- Datenaufbereitung

  Proxy-Server können gewisse Applikationsfunktionen ausführen, wie zum Beispiel das Umwandeln in standardisierte Formate

- Protokollierung

  Verbindungen werden mitprotokolliert und sind somit nachvollziehbar

[Ste98b]

SIP-Kommunikation in VoIP

Jeder Dienst basiert auf seinen eigenen Protokollen. Beispielsweise arbeitet ein Browser üblicherweise mittels Hypertext Transfer Protocol (HTTP) , ein Server verwendet zur Übertragung von Dateien das File Transfer Protocol (FTP) oder Mailservices verwenden zum Beispiel das Post Office Protocol (POP3) bzw. Simple Mail Transfer Protocol (SMTP). Auch bei VoIP wird oft das Protokoll SIP zum Verbindungsaufbau genutzt. Eine Ausnahme bildet das VoIP-Tool Skype [Lim10], welches auf einem eigenen Protokoll basiert.

SIP hat die Aufgabe den Gesprächsaufbau (Signalisierung) durchzuführen. SIP kann man sich als eine Art eindeutige Adresse im Internet vorstellen. Das bedeutet, dass eine SIP-Adresse einer E-Mail-Adresse sehr ähnlich ist. Eine SIP-Adresse besteht im Grunde aus drei Teilen:

Protokoll-Bezeichner, Username, Domain

Ein Beispiel für eine SIP-Adresse ist: sip:user@domain.at (wenn bei ENUM registriert)

Hauptaufgabe des SIP-Protokolls ist es, den Rufaufbau zwischen zwei Teilnehmern durchzuführen und diese Kommunikationssitzung bei Beendigung wieder ordentlich zu schließen.
[Joh01]
Nach der Anrufsignalisierung durch das SIP-Protokoll ist das Session Description Protocol (SDP) für die Gesprächsmodalitäten wie

1. Sprachcodec
2. Videoübertragung
3. Übertragungsprotokoll

zuständig.

Die Aufteilung der Datenströme und die Übertragung der Sprachdaten wird durch das so genannte Real-Time Transport Protocol (RTP) übernommen, welches die einzelnen Datenpakete an das User Datagram Protocol (UDP) weiter gibt. UDP, welches ähnliche Zwecke wie das Transmission Control Protocol (TCP) erfüllt, hat die Aufgabe, die einzelnen Datenpakete zu übertragen. UDP verlangt im Gegensatz zu TCP unter anderem keine Empfangsbestätigung. Das bedeutet, dass ein Paket, welches verloren geht, nicht neu angefordert wird, was wiederum Datenverkehr und Verzögerungen einspart, was sich sehr positiv auf eine VoIP-Übertragung auswirkt.

3.5 Sicherheit

In diesem Abschnitt werden allgemein die Sicherheit und der Schutz von VoIP-Netzen beschrieben. Beim Begriff Sicherheit und Schutz werden in diesem Abschnitt zum einen die rechtlichen und gesetzliche Sicherheitsbestimmungen, sowie die möglichen Sicherheitsrisiken in Kommunikationsnetzen näher erläutert und zum anderen technische Aspekte sowie die technischen Möglichkeiten, die geboten werden, um VoIP zu sichern, näher behandelt.

Unter den Begriffen Sicherheit und Schutz aus rechtlich-gesetzlicher Sicht werden vor allem Aspekte wie

- Intimsphäre und Schutz von persönlichen Daten
- Datenschutz,

aus technischer Sicht werden Aspekte wie

- VoIP-Angriffe
- Datensicherheit und Datensicherung bei VoIP

näher betrachtet.
[Jin07], [Jud08], [Wei09], [Nin09]
Im Bereich der Datensicherheit und des Datenschutzes sind, wie im Abschnitt 2.1 erwähnt, die drei Begriffe Vertraulichkeit, Integrität und Verfügbarkeit maßgeblich.

3.5.1 VoIP-Angriffe

Neben SPIT gibt es noch zahlreiche weitere Angriffe, welche auf VoIP-Systeme verübt werden können. Dieser Abschnitt gibt einen kurzen Überblick, welche Gefahren für VoIP-Systeme bestehen und welche Auswirkungen diese zur Folge haben.

Nachfolgend werden Methoden, welche unter dem Begriff Casing the Establishment zusammengefasst werden, näher behandelt. Mit diesem Begriff werden Angriffe bezeichnet, welche dem Angreifer Informationen bezüglich seines Opfers liefern. [Col06]

1. Footprinting

   Footprinting bezeichnet das Sammeln von Randinformationen über ein ausgewähltes Ziel. Zu diesen Randinformationen zählen unter anderem Informationen über eingesetzte Firewalls bzw. IDS-Systeme, Wissen über Netzwerkressourcen, aber auch allgemeine Informationen über die

Firmenstruktur. Als Footprinting wird die Beschaffung von allgemeinen Informationen über das Angriffsziel bezeichnet. Als Angriffsziel dient meist ein VoIP-System. Zu diesen sogenannten Randinformationen zählen zum Beispiel Informationen über verwendete Firewalls, Wissen über die allgemeine Firmenstruktur, Informationen über die verfügbaren Netzwerkressourcen, usw. Diese Art von Informationen zählen zu beliebten Angriffszielen im Bereich des Hackens. Im Umfeld von Cyber-Kriminalität gehen Hacker bei der Beschaffung von diesen Informationen nicht wahllos vor, sondern nach einem bestimmten Schema (siehe Abschnitt 2.4).

Die Phasen I und II unterscheiden sich bei VoIP-Angriffen nicht wesentlich von anderen Angriffen. In der Phase III werden bei Angriffen auf VoIP beispielsweise nachfolgend genannte Methoden angewandt: [Col07a]

- DNS-Lookup:
  Mittels DNS-Lookup (Domain Name System Lookup) werden IP-Adressen bzw. Domains eines bestimmten Computers mittels DNS herausgefunden. Das bedeutet man kann aus IP-Adresse den Domainnamen oder aus Domainnamen die IP-Adresse herausfinden. [Col06]
- Zone Transfer-Namen und IP-Adressen:
  Zone Transfer-Namen und IP-Adressen werden in sogenannten Zonen zusammengefasst und auf einem DNS-Server hinterlegt. Mehrere zusammengehörige DNS-Server halten sich immer gegenseitig aktuell, indem sie diese Daten austauschen. Diese Daten können somit, wenn sie noch dazu unverschlüsselt vorhanden sind, unter Umständen abgefangen werden und liefern geschützte Informationen.
- Ping Sweep:
  Hiermit wird eine Technik bezeichnet, welche dazu verwendet wird, um einen bestimmten Bereich von IP-Adressen zu ermitteln, welche auf so genannte „live hosts“ verweisen.[Teo08]
- Fingerprinting:
  Die oben genannten Verfahren werden allesamt im Rahmen des Footprintings eingesetzt. Hier versucht der Angreifer, zu entdecken, welches Betriebssystem einem Host zugrunde liegt. Diese Information verschafft dem Angreifer das Wissen über spezifische Schwachstellen des Betriebsystems.

Nach Phase III hat ein potentieller Angreifer alle nötigen Informationen gesammelt, um sich ein ungefähres Bild vom Zielrechner machen zu können.

2. Scanning
   Unter dem Begriff Scanning versteht man Remote-scan-Methoden, mit welchen man potentielle aktive VoIP-Geräte im Netzwerk ausfindig machen kann. Verwendet werden herkömmliche Techniken wie UDP, TCP, Simple Network Management Protocol (SNMP) oder Internet Control Message Protocol (ICMP) Scanning. Hierbei erhält der Angreifer keine Sicherheit, ob das eventuelle gefundene Gerät wirklich ein VoIP-Gerät ist.

3. Enumeration
   Hierbei versucht der Angreifer, eine Liste von VoIP-Endgeräten zu erstellen. VoIP-Endgeräte sind so genannte Softphones, Hardphones, Proxies und alle weiteren Geräte, die das SIP zum Aufbau einer Kommunikation nutzen. Ausfindig machen kann man solche Geräte über einen SIP-Scan, der auf das SIP-Protokoll angelegt wird.

4. Network Eavesdropping:
   Unter diesen Begriff fallen alle Angriffe, welche das Abhören von VoIP-Sitzungen betreffen. Mögliche Techniken sind harvesting, call pattern tracking, TFTP file snooping oder auch man-in-the-middle. Alle Techniken haben eine Gemeinsamkeit: Sie dienen dazu, Informationen aus dem Datenverkehr zu bekommen.

Der DoS-Angriff (Denial of Service Angriff) wird zum überlasten eines VoIP-Netzwerks benutzt:
Unter DoS versteht man Angriffe, welche das Zerstören bzw. Unterbrechen des VoIP Services zum Ziel haben. Dies erreicht man z.B. mittels „Invite-Flooding“. Deshalb ist es sehr wichtig über Qualität und Auslastung der VoIP-Umgebung Bescheid zu wissen bzw. diese messen zu können. Weitere Möglichkeiten für Angriffsziele eines DoS-Angriffs sind Services wie DNS oder Dynamic Host Configuration Protocol (DHCP). [Ver06], [Col06]

Neben DoS-Angriffen sind auch Angriffe, die direkt gegen das SIP bzw. RTP Protokoll gerichtet sind, möglich:

1. Fuzzing VoIP:

   Dieser Begriff ist auch bekannt als robustness testing oder functional protocol testing. Fuzzing ist eine eigene Technik, welche zum Testen von Software entwickelt wurde. Das Prinzip von Fuzzing besteht darin, zufällige Daten zu generieren und diese über eine Schnittstelle an das Zielsystem zu übermitteln. Tools, welche auch Fuzzer genannt werden, sind im Internet in großer Vielfalt erhältlich. Fuzzer sind allerdings nicht auf Dateien beschränkt, sondern es gibt sie auch für Netzwerkdienste. Somit eignen sich solche Fuzzer auch dazu, ein VoIP-System

anzugreifen, indem fehlerhafte oder zufällig erzeugte Datenpakete gesendet werden und so das System zum Absturz gebracht wird. [Fes10]

2. Signal- und Medien-Manipulation:

   Diese Art von Angriff zielt darauf ab, dass man SIP- oder RTP-Signale manipuliert und somit den ursprünglichen Aufbau des Protokolls zerstören bzw. verändern und ausnutzen kann. Diese Angriffsart ist leicht auszuführen und richtet beträchtlichen Schaden an. [Col06]

3. Anrufunterbrechung:

   Das Weiterleiten einer „Beendigungs-Nachricht“ beendet ein aktives Gespräch. Der Angreifer hat sich nun diese Eigenschaft zunutze gemacht, um VoIP-Systeme zu bedrohen. Wichtigste Voraussetzung, um diesen Angriff zu tätigen, ist, die Call-IDs des aktiven Gespräches zu ermitteln. Somit besteht die Möglichkeit für den Angreifer, ein aktives Gespräch zu beenden. Eine weitere Möglichkeit, einen Anruf ungewollt zu beenden, ist die sogenannte Cancel-Methode. Hierzu wird ein Script verwendet, welches ein Socket öffnet und den gesamten Nachrichtenverkehr analysiert. Sobald eine Invite-Nachricht entdeckt wird, sendet das Script eine Cancel-Nachricht mit derselben Call-ID, welche in der Invite-Nachricht abgefangen wurde. Der eben beschriebene Vorgang wird in Abbildung 3.3 dargestellt: [Ver06]

3.5.2 Sicherheitsmaßnahmen bei VoIP

Die Motivation zur Absicherung von VoIP-Systemen kommt aus unterschiedlichen Quellen. Einerseits möchten zum Beispiel Anwender im allgemeinen nicht, dass Dritte unberechtigt ihre Gespräche mithören können, andererseits sind zum Beispiel Firmen gesetzlich dazu verpflichtet, ein gewisses Sicherheitsniveau einzuhalten. Kommerzielle Anbieter haben auch das Ziel, dass beispielsweise die Verfügbarkeit ihres Service hoch ist. Daher müssen angemessene technische und organisatorische Maßnahmen getroffen werden, die eine sichere und datenschutzgerechte Nutzung einer VoIP-Infrastruktur ermöglichen. Weiters muss bzw. sollte eine entsprechende Verschlüsselungsmethode verwendet werden, die den Anforderungen der jeweiligen Infrastruktur genüge tut. Ein wesentlicher Faktor wird auch die Weiterentwicklung und Ausbesserung von bestehenden Mängeln in Protokollen und Software sein.

Es wird empfohlen, offene und standardisierte Lösungen zum Einsatz zu bringen und die verwendeten Protokolle offenzulegen, da man so ein Produkt nützt, das weniger Mängel aufweist.
Im Bereich von Datenschutz und VoIP ist es auch sehr wichtig, sich vorab mit den Gefahren und Einschränkungen gegenüber PSTN zu informieren und

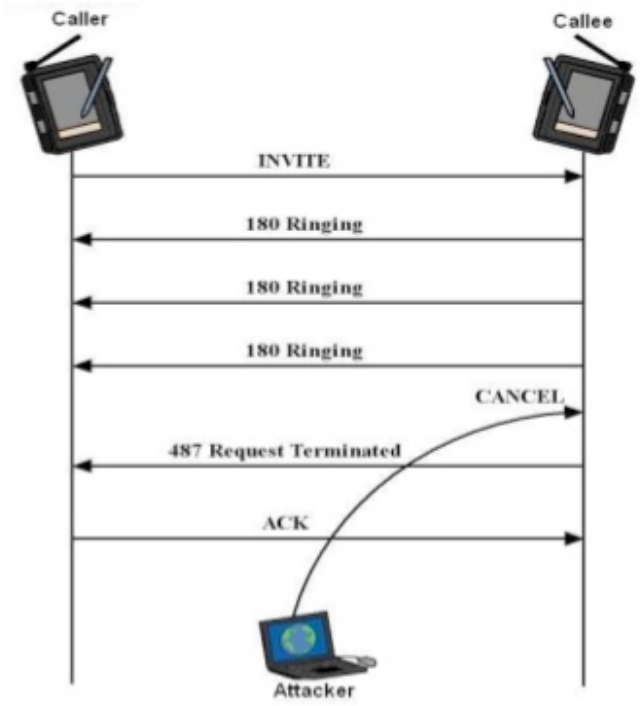


Abbildung 3.3: Call Interrupt (Cancel Methode) [Ver06]

die datenschutzrechtlichen Vorschriften, welche es auch für analoge Telefonie gibt, weiterhin zu beachten. Open-Source-Software bietet unter Umständen einen Sicherheitsgewinn, da aufgrund des Open-Source-Konzepts eine genauere Überprüfung der Quellen und damit der Software auf Sicherheitsprobleme stattfindet. [iACG01], [Han07]

VoIP verwendet ein ähnliches Sicherheitsschichten-Konzept, das auch zur Absicherung von anderen Systemen in der IT verwendet wird.

- Rechteverwaltung (policies)
- Physikalische Sicherheit (physical security)
- Netzwerksicherheit (IP, UDP, TCP, etc.) (network security)
- Supporting Service Security (Webserver, Datenbanken, DHCP)
- Betriebssystemsicherheit (OS security)
- Anwendungssicherheit (application security)

[Col06]

Nachfolgende Abbildung 3.4 auf Seite 41 zeigt die einzelnen Schichten des Sicherheitskonzeptes bei VoIP und stellt die Zuordnung einiger beispielhafter Angriffsmöglichkeiten zu den einzelnen Schichten dar.

Durch Abbildung 3.4 auf Seite 41 wird deutlich, dass nur ein Sicherheitskonzept auf allen Ebenen Schutz gegen eine Angriffsgefahr auf das Netzwerk bieten kann. [Col07a] Weitere Informationen zu den einzelnen genannten Angriffen finden sich in: [Col06], [Lis06], [Cas01], [Lak01]

Unterschiedliche IT-Sicherheitsmaßnahmen existieren, um Angriffe auf VoIP-Systeme abzuwehren. Nachfolgende Methoden helfen beispielsweise das Sicherheitsniveau im Bezug auf die Vertraulichkeit zu erhöhen.

[Col07a], [Col06]

- Firewalls:

  Firewalls schützen das Netz vor ungewollten Eingriffen von außen. Es tritt ein Zielkonflikt auf, wenn man den Anforderungen flüssiger Sprachübertragung und sicherer Übertragung gerecht werden will. Sprache muss im Gegensatz zu anderen Daten verzögerungsfrei übertragen werden, somit bleibt nur sehr wenig Zeit, um die Sprachdaten zu prüfen. Die Firewalls werden auf Ebene der Application-Layer eingesetzt und haben den Zweck, jedes Sprachpaket auf seinen ordnungsgemäßen Zustand zu überprüfen.

- SRTP:

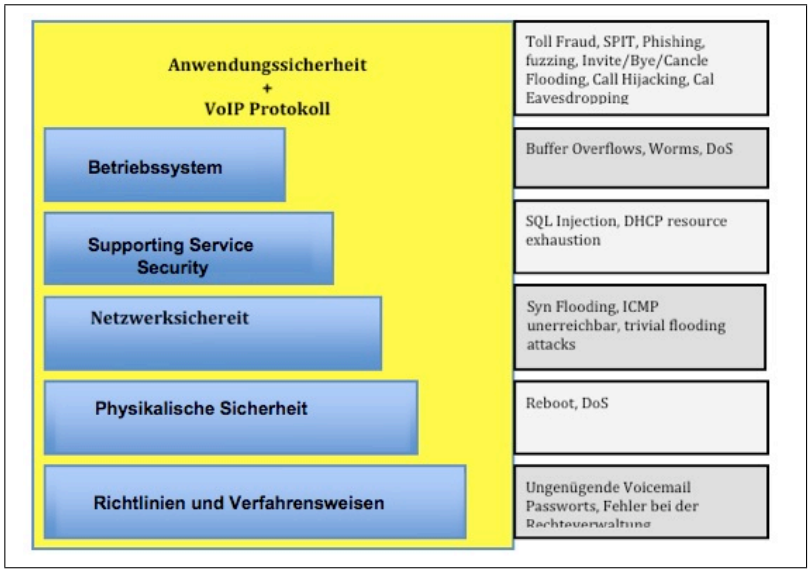


Abbildung 3.4: Sicherheitsschichten und Angriffe, nach [Col07a]

Als SRTP wird das Secure Real-Time Transport Protocol bezeichnet. Dieses Protokol ermöglicht eine Verschlüsselung der zu übertragenden Daten und kann somit die Möglichkeiten des Abhörens einschränken.

- VPN:

  Das Virtual Private Network (VPN) bewirkt ebenfalls eine Absicherung gegen das Mithören durch Dritte, und zwar durch das Aufbauen eines Tunnels zwischen den Anwendern, wo die Daten durchgeschleust werden. Typisch ist diese Art des Schutzes bei VoIP im Bankensektor, da dort vorhandene Sicherheitsmaßnahmen für Transaktionen bestehen, aber es kann auch der Sprachverkehr mitübertragen werden. [Lip07]

- Drahtlose Verschlüsselung:

  Wenn Endgeräte via WLAN eingebunden werden, ist es zweckmäßig, falls nicht SRTP verwendet wird, eine Verschlüsselungsmaßnahme wie z.B. WPA2 zu verwenden.

Kapitel 4

SPAM

In diesem Kapitel wird ein Überblick über das Thema SPAM im Allgemeinen gegeben werden und es erfolgt eine Aufteilung in die verschiedenen Kategorien von SPAM, welche individuell behandelt werden. SPAM ist ein globales Problem und macht vor keinem Land halt, nachfolgende Abbildung 4.3 auf Seite 43 zeigt die zwölf Länder mit dem höchsten SPAM-Versand im Jahr 2009:

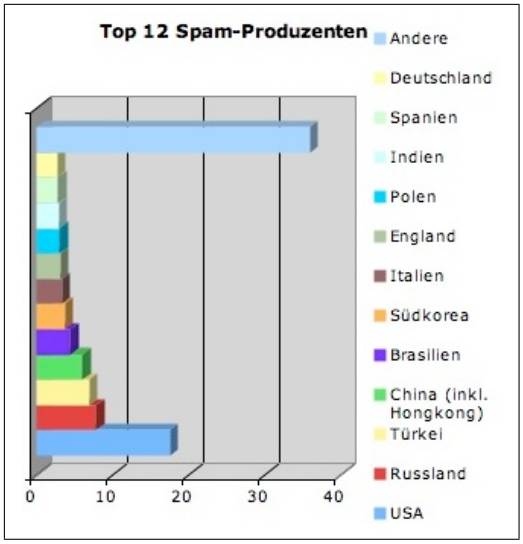


Abbildung 4.1: Herkunft von SPAM 2009, Top 12, nach [Plc09]

Im Vergleich dazu zeigt Abbildung 4.2 auf Seite 43 eine Statistik für das Jahr 2010. Es ist auffällig, dass sich die Entwicklung des SPAM-Aufkommens der zwölf größten SPAM-Produzenten vom Jahr 2009 auf 2010 dramatisch verändert hat. Das Aufkommen von SPAM hat sich in einigen Ländern deutlich erhöht, andere Länder wiederum wie z.B. Deutschland, fallen aus der Statistik für 2010 heraus:

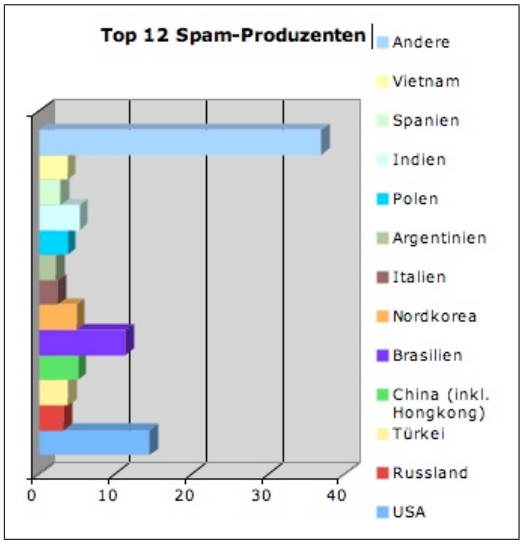
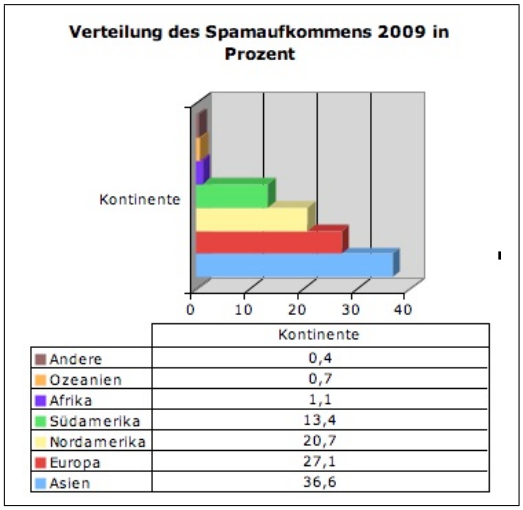


Abbildung 4.2: Herkunft von SPAM 2010, Top 12, nach [Plc10]

Um einen globalen Überblick über die Entwicklung des SPAM-Aufkommens zu bekommen, wird nachfolgend ein Vergleich der Statistiken, nach Kontinenten geordnet, zwischen den Jahren 2009 und 2010 getätigt.

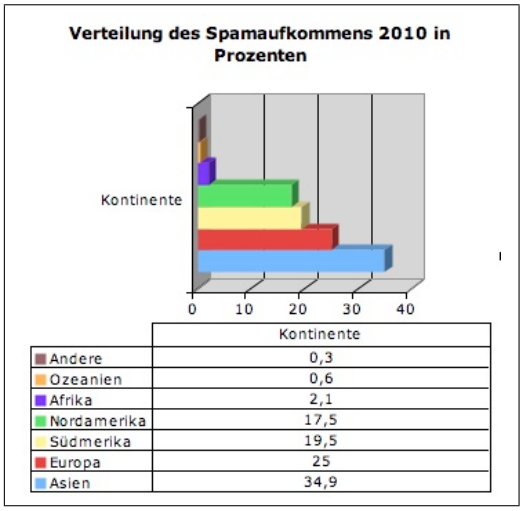
Abbildung 4.3 zeigt eine Übersicht, wie sich SPAM im Jahr 2009 prozentmäßig über alle Kontinente verteilt hat: [Plc09]



	Kontinente
Andere	0,4
Ozeanien	0,7
Afrika	1,1
Südamerika	13,4
Nordamerika	20,7
Europa	27,1
Asien	36,6

Abbildung 4.3: Herkunft von SPAM pro Kontinent, nach [Plc09]

Im Vergleich dazu zeigt Abbildung 4.4 auf Seite 44 die Entwicklung des SPAM-Aufkommens pro Kontinent von 2009 auf 2010:



	Kontinente
Andere	0,3
Ozeanien	0,6
Afrika	2,1
Nordamerika	17,5
Südmerika	19,5
Europa	25
Asien	34,9

Abbildung 4.4: Herkunft von SPAM pro Kontinent, nach [Plc09]

Auffallend ist, dass die globale Verteilung des SPAM-Aufkommens nahezu gleich bleibt, mit Ausnahme von Südamerika, welches einen hohen Anstieg zu verzeichnen hatte.

[Plc09], [Red09]

4.1 SPAM-Störfaktor im Internet

Das Wort SPAM wurde erstmals im Jahr 1936 erwähnt, als es als Markenname für ein Dosenfleisch Bekanntheit erlangte. Gerüchten nach zu urteilen, konnten Soldaten zu der Zeit das Dosenfleisch der Marke SPAM einfach nicht mehr essen und so entstand eine Redensart. SPAM als Begriff galt damals als ein Synonym für eine unnötig häufige Verwendung und Wiederholung. Dadurch entstand der Englische SPAM-Sketch von Monty Python's Flying Circus. In den Cafes im Film konnte man in allen Gerichten das Wort SPAM lesen.

Unter dem Begriff SPAM versteht man heute einen Sammelbegriff für zahlreiche Formen von Nachrichten, wobei der Inhalt meist Werbeinformationen sind, die an Benutzer versendet werden. Die ursprüngliche Form der Verbreitung waren E-Mails. Der Begriff SPAM ist heutzutage aber nicht mehr nur an dieses Verbreitungsmedium gebunden. Bei SPAM in Form von E-Mails spricht man auch von Junk-E-Mails, was übersetzt so viel wie „Mist-E-Mails" bedeutet. Junk-E-Mails zeichnen sich oft durch sehr geringen Inhalt aus. Der Vorgang des Versendens wird als SPAMming bezeichnet und ist meist an mehrere, oft auch unzählige Personen gleichzeitig gerichtet. Der Sender solcher Informationen wird als SPAMmer betitelt.

Sinn und Zweck von SPAM ist es, durch Versenden einer großen Anzahl von Werbe-Mails auf sich aufmerksam zu machen, wobei beim Konsumenten zuerst das Interesse geweckt werden kann, aber nach Empfang einer größeren Anzahl dieser Mails meist das Gegenteil erreicht wird, da der Verbraucher diese Art von Werbung im Endeffekt als Belästigung empfindet. [Red09]
Der Inhalt von SPAM stammt aus verschiedenen Branchen, nachfolgende Abbildung 4.5 zeigt die Verteilung der einzelnen Bereiche:

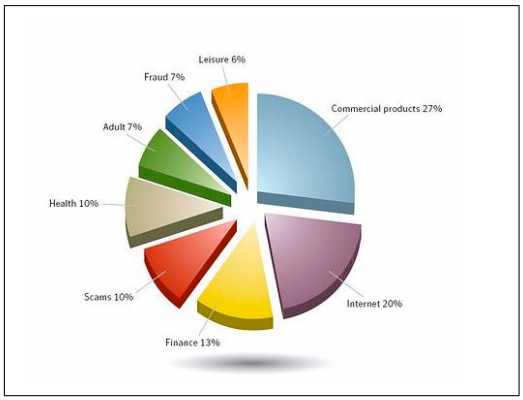


Abbildung 4.5: Aufteilung von SPAM nach Inhalten in der zweiten Jahreshälfte 2007 [Red09]

Durch das Versenden von SPAM-Mails fallen Kosten an, welche nicht immer vom eigentlichen Versender getragen werden. Oftmals werden die Kosten mit diversen Tricks auf andere Personen übertragen.

Botnets werden als Werkzeug verwendet, um Sicherheitslücken auszunützen. Der Begriff Botnet teilt sich in zwei Teile:

1. Bot
   Unter Bot versteht man ein Programm, welches selbstständig wiederholende Prozesse abarbeitet. Bots gibt es zu gutartigen und bösartigen Zwecken. Der Missbrauch von Bots geht z.B. in die Richtung, dass automatisch E-Mail-Adressen zu Werbezwecken gesammelt werden.

2. Net
   Der Begriff Net drückt aus, dass es sich nicht um einen einzelnen Bot handelt, sondern um eine Gruppe von Software-Bots.

Software-Bots werden oftmals auch ohne das Wissen der Betroffenen auf vernetzen Rechnern installiert. Im Bereich von SPAM haben Botnets die Aufgabe, von den Hostrechnern, auf welchen sie installiert sind, aus eine große Menge an E-Mails zu versenden. Es ergibt sich nun der Fall, dass eine

große Anzahl von gleichen E-Mails von verschiedenen Rechnern versendet werden. [Can09]

Durch den Einsatz von Botnets wurde es möglich, eine große Menge an SPAM Mails günstig zu versenden und hat so das SPAMming sehr beliebt gemacht - es wurde zu einem ernsthaftem Problem. SPAM wird von fast allen Internetbenutzern abgelehnt und als schwerer Missbrauch angesehen. SPAMmer können in vielen Staaten rechtlich belangt werden.

Gesetzlich wird in Österreich die Regelung bezüglich SPAM im Telekommunikationsgesetz 2003(TKG) §107 und TKG 2003 §109 Abs. 1 Punkt 19 und 20 verwaltet:

§ 107

- (1) Anrufe - einschließlich das Senden von Fernkopien - zu Werbezwecken ohne vorherige Einwilligung des Teilnehmers sind unzulässig. Der Einwilligung des Teilnehmers steht die Einwilligung einer Person, die vom Teilnehmer zur Benützung seines Anschlusses ermächtigt wurde, gleich. Die erteilte Einwilligung kann jederzeit widerrufen werden; der Widerruf der Einwilligung hat auf ein Vertragsverhältnis mit dem Adressaten der Einwilligung keinen Einfluss.
- (2) Die Zusendung einer elektronischen Post – einschließlich SMS – ist ohne vorherige Einwilligung des Empfängers unzulässig, wenn

  1. die Zusendung zu Zwecken der Direktwerbung erfolgt oder

  2. an mehr als 50 Empfänger gerichtet ist.

- (3) Eine vorherige Zustimmung für elektronische Post gemäß Abs. 2 ist dann nicht notwendig, wenn

  1. der Absender die Kontaktinformation für die Nachricht im Zusammenhang mit dem Verkauf oder einer Dienstleistung an seine Kunden erhalten hat und

  2. diese Nachricht zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen erfolgt und

  3. der Kunde klar und deutlich die Möglichkeit erhalten hat, eine solche Nutzung der elektronischen Kontaktinformation von vornherein bei deren Erhebung und zusätzlich bei jeder Übertragung kostenfrei und problemlos abzulehnen und

  4. der Empfänger die Zusendung nicht von vornherein, insbesondere nicht durch Eintragung in die in §7 Abs. 2 E-Commerce-Gesetz genannte Liste, abgelehnt hat.

- (4) entfallen (durch die Novelle BGBl. I Nr. 133/2005)
- (5) Die Zusendung elektronischer Post zu Zwecken der Direktwerbung ist jedenfalls unzulässig, wenn die Identität des Absenders, in dessen Auftrag die Nachricht übermittelt wird, verschleiert oder verheimlicht wird oder bei der keine authentische Adresse vorhanden ist, an die der Empfänger eine Aufforderung zur Einstellung solcher Nachrichten richten kann.
- (6) Wurden Verwaltungsübertretungen nach Absatz 1, 2 oder 5 nicht im Inland begangen, gelten sie als an jenem Ort begangen, an dem der Anruf den Anschluss des Teilnehmers erreicht.

[Sch03]

§ 109

(1) Eine Verwaltungsübertretung begeht und ist mit einer Geldstrafe bis zu 4.000 Euro zu bestrafen, wer
19. entgegen §107 Abs. 1 Anrufe zu Werbezwecken tätigt;
20. entgegen §107 Abs. 2 oder 5 elektronische Post zusendet;
[Sch03]

4.2 Arten von SPAM

Der Begriff SPAM bezieht bzw. beschränkt sich in der heutigen Zeit nicht mehr nur auf E-Mails oder sonstige Postings, sondern hat eine sehr große Vielfalt in seinen Verbreitungsmöglichkeiten gefunden. Man spricht hierbei zwar nicht mehr von SPAM, sondern es wurden Begriffe gebildet wie SPIT, Blog-SPAM, usw. Somit dient der Begriff SPAM als Dachbegriff für den Werbeinhalt, jedoch gibt er nicht das Verbreitungsmedium an. Im Abschnitt Arten von SPAM wird aufgezeigt, dass es verschiedene Varianten von SPAM gibt. Diese Informationen sollen einerseits zeigen, dass SPAM ein Problem darstellt und andererseits helfen, wie man mit SPAM umgeht. Teilweise können durch diese Erfahrungen unter Umständen Mechanismen zur Abwehr für SPIT abgeleitet werden.

4.2.1 E-Mail SPAM

E-Mails als Kommunikationsmittel erfreuen sich heutzutage einer sehr großen Beliebtheit. Für viele Millionen Menschen ist dies eine einfache, bequeme und noch dazu kosteneffiziente Art, zu kommunizieren. E-Mails stellen dem Benutzer die Möglichkeit zur Verfügung, kostenlos eine unzählige Anzahl von

Nachrichten zu versenden. Nachrichten können vom Kilobyte-Bereich bis hin zu mehreren Megabytes reichen. Der generellen Verwendung von E-Mails liegen folgende Zahlen und Statistiken zugrunde: Laut Pew Internet and American Life Project data, Stand April 2009, bezogen auf den US-amerikanischen Markt, sind 90 Prozent der Internetbenutzer auch potentielle Benutzer von E-Mail-Diensten. Weiters wurde erhoben, dass 57 Prozent davon die Tätigkeit, E-Mails zu senden bzw. zu empfangen, als eine alltägliche Aufgabe ansehen.

Im Mai 2009 hat das Marktforschungsunternehmen The Radicati Group geschätzt, dass der derzeigtige Stand von 1,4 Milliarden E-Mail-Benutzern im Jahr 2013 auf 1,9 Milliarden Benutzer steigen wird. Selbiges Marktforschungsunternehmen gibt an, dass im Jahr 2009 pro Tag etwa 247 Millarden E-Mails versendet wurden. [Pty09]

Anhand dieser Statistiken, welche auf den amerikanischen bzw. europäischen Markt bezogen sind, sieht man die große Verwendung von E-Mails. Nicht außer Acht zu lassen ist der Fakt, dass der asiatische Markt, was Technik und Technologie betrifft, stark im Wachsen ist. Dies bedeutet, dass es zu einem sehr großem Anstieg dieser Zahlen kommen wird, ausgelöst durch die Wirtschaftszentren China und Indien. [Pty09]

Im Jahr 2009 betrug der SPAM-Anteil im E-Mail-Traffic durchschnittlich 85,2 Prozent. [Nam10] Der enorme Anstieg von versendeten E-Mails und die immer stärker werdenden Probleme von SPAM-Mails lassen erahnen, dass das Problem von SPAM in den nächsten Jahren drastisch ansteigen wird.

Ein weiteres Problem von SPAM ist die Verbreitung von Viren und Internet-Würmern. SPAMmer sind meist Organisationen, welche durch diese Art der Werbung Geld erwirtschaften. Die größte Anzahl (80 Prozent) von SPAM-Mails gehen laut [Plc10] von den USA, Südkorea und China aus, wie auch in den Abbildungen 4.3 auf Seite 43 und 4.4 auf Seite 44 ersichtlich ist.

4.2.2 SPAM over Mobile Phones

Der nachfolgende Abschnitt SPAM over Mobile Phones (SPOM) bezieht sich auf eine Studie und Analyse des asiatischen Marktes [Ham09] und kann auf andere Märkte teilweise übertragen werden.

Als Definition von SPOM wurden für die Studie folgende Einschränkungen getroffen:

- Nachrichten, die zu einem Anruf auffordern
- Nachrichten, welche zu einem kostenflichtigen Zusatzdienst auffordern

- Nachrichten, welche die Grundeinstellungen verändern
- Nachrichten mit kommerziellem Hintergrund (Kaufaufforderung, Angebote, etc.)
- Nachrichten, welche Informationen über Privatsphäre fordern

[Ham09]

Miteingeschlossen sind Nachrichten von Mobilfunkbetreibern (Mobile Network Operators (MNO)).

Die erste Frage der Analyse bezog sich darauf, ob ein Benutzer SPOM erhalten hat, was 80 Prozent der Befragten (95 Prozent unter 30 Jahre) mit JA beantworteten.

Die zweite Frage nach der Anzahl der SPAM Nachrichten auf das Mobiltelefon, wird mittels Abbildung 4.6 beantwortet. Abbildung 4.6 zeigt eine Tabelle, welche den Erhalt von SPOM-Nachrichten in drei Kategorien einteilt: null, eins bis zehn und größer als zehn Nachrichten im letzten Jahr. Weiters wird unterschieden, ob die Nachrichten vom Netzbetreiber, einem Drittanbieter von SMS oder ähnlichen Fremdanbieter stammen. Bei den Zahlen der Abbildung 4.6 wird die subjektive Wahrnehmung der Empfänger dargestellt. Eventuelle Filter von Seiten der Anbieter wurden nicht berücksichtigt: [Ham09]

	0	1-10	>10
MNO messages	3.1%	76.7%	20.2%
3rd party messages	42.3%	51.9%	5.9%
Misleading mssages with premium number	64.7%	31.8%	3.5%

Abbildung 4.6: Herkunft und Menge von SPOM [Ham09]

Es ist auffallend, dass die größte Anzahl der Nachrichten der letzten Jahre, welche als SPAM empfunden werden, zwischen null und zehn liegen. Durch diese Abbildung wird klar, dass dem Thema SPOM keine sehr große Bedeutung zugewiesen werden muss, da die Verbreitung sehr gering ist.

SMS mit Werbebotschaften haben aus zwei Gründen keinen großen Zulauf:

1. die meisten MNOs lehnen dies aus rechtlichen und politischen Gründen ab
2. die Kosten pro SMS sind zu hoch für die Versender

[Ham09]

4.2.3 Multi User Dungeons SPAM

Im eigentlichen Sinn bedeutet Multi User Dungeons SPAM (MUD) eine Überflutung von text-basierten Inferfaces mit eigenen Botschaften. Die geschichtliche Herkunft des Ausdrucks Multi User Dungeons stammt aus dem Ende der 80er Jahre. Damals wurden Rollenspiele auf Textbasis damit bezeichnet. Häufig wurden diese Spiele aber als Chat-Räume genutzt. Die Verbindung zu den Spielen erfolgte über Telnet-Protokolle. Die einfachen Chat-Räume brachten es mit sich, dass jeder Benutzer, der sich im selben Raum befand, auch alle Mitteilungen der anderen Benutzer empfing. Als diese so genannten MUDS noch weite Verbreitung im WWW fanden, nutzten so genannte Provokateure, welche in Fachkreisen oft auch als Trolle bezeichnet wurden, diese Schwäche aus, indem sie eigenen Nachrichten durch selbstgeschriebene Makros mehrere hunderte Male in das System schickten. Dieses Verhalten hatte zur Folge, dass jegliche Kommunikation zwischen den anderen Teilnehmern unmöglich wurde. Das Verhalten wurde in Anlehnung an den oben beschriebenen Monty-Python-Sketch, in dem sich die Wikinger ähnlich verhalten, als SPAMming bezeichnet. Heute finden MUDs kaum noch Anwendung.

[Sch07]

4.2.4 Usenet-SPAM

Unter Usenet-SPAM versteht man üblicherweise die Verbreitung von ein und demselben Beitrag in großer Anzahl in Newsgruppen. Miteinbezogen werden auch Einträge, welche sich nur in geringem Ausmaß unterscheiden, wobei der Inhalt völlig nebensächlich ist.

Allgemein gibt es zwei Arten von Usenet-SPAM:

- Excessive Multi-Posting (EMP):

Es werden 1:1-Kopien in großer Anzahl in dieselbe Newsgruppe gestellt.

- Excessive Cross-Posting (ECP):

Ein und derselbe Artikel wird in vielen verschiedenen Newsgruppen veröffentlicht.

Rein technisch gesehen liegt der Unterschied zwischen EMP und ECP darin, dass bei Cross-Posting nur eine Kopie der Nachricht am Newsserver vorliegt, beim Multi-Posting aber liegen mehrere Kopien am Server vor. Aus dieser Eigenschaft heraus ergibt sich, dass Multi-Posting viel mehr Speicher und eine höhere Übertragungszeit braucht als Cross-Posting. Somit sind auch die Richtlinien, was den Übergang zwischen gesetzlich erlaubten Verbreiten von Nachrichten und gesetzlich verbotenem SPAM betrifft, viel enger gesetzt.

Um die Grenzwerte nicht umgehen zu können, misst man eine Kombination (Gleiches gilt für das wiederholte Posten nach kurzer Zeit) aus Cross-Post und Multi-Post innerhalb einer definierten Zeitspanne.

Diese Art von SPAM wird heute weltweit aus Newsforen automatisch entfernt. Der Absender von Usenet-SPAM wird per Mail davon in Kenntnis gesetzt und es wird ein öffentlich zugängliches Protokoll darüber erstellt. Auf Österreich bezogen werden besondere Regeln angewandt, welche unter [Dau09] `http://www.dbai.tuwien.ac.at/user/usenetat/cancel.html` zu finden sind. [Dau09], [Sca06]
Weitere Informationen zur Entwicklung des Internets: [Zem01]

4.2.5 Suchmaschinen- oder Index-SPAM

Unter Suchmaschinen-SPAMming versteht man den Einsatz von Organisationen, Unternehmungen oder auch einzelnen Personen, um die Suchmaschinen-Position der eigenen Webseite zu verbessern. Sinn davon ist es, den Bekanntheitsgrad und die Trefferquote der Seite zu steigern. Jeder Suchmaschinen-Index, auch die Indizes der großen und bekannten Suchmaschinen, beinhalten Seiten, welche gegen die Richtlinien der jeweiligen Suchmaschine verstoßen, um durch Tricks die eigene Reihung zu verbessern. Optimierungsmaßnahmen von Suchmaschinen gehen grundsätzlich in zwei Richtungen.

- Ethnische Optimierung: Webinhalte werden so ausgerichtet, dass sie nicht gegen die jeweiligen Richtlinien der Suchmaschine verstoßen. Unter Richtlinien versteht man eigene Regeln, so genannte Guidelines, welche größere Suchmaschinen vorgeben. Diese Guidlines enthalten Punkte, die beim Erzeugen von Webseiten beachtet werden sollten, damit diese bei der jeweiligen Suchmaschine größtmögliche Beachtung finden, zum Beispiel `http://www.google.com/support/webmasters/bin/answer.py?hl=de&answer=3560Punkte9`
- Suchmaschinen-SPAMming: Hiermit werden alle Maßnahmen zusammengefasst, welche es zum Ziel haben, die Suchmaschine zu täuschen und somit gegen die Richtlinien zu verstoßen.

[Wu07], [Höv09]

Suchmaschinen-SPAMmer greifen zu dieser Möglichkeit, da es unter normalen Umständen und den Richtlinien entsprechend sehr schwierig ist, eine Vielzahl von Begriffen gezielten Inhalten zuzuführen. Mithilfe von SPAMming können tausende Begriffe mit automatischen Inhalten verknüpft werden.

Wege, um Suchmaschinen-SPAMming zu betreiben, welche in dieser Arbeit behandelt werden:

- Keyword Stuffing/Hidden Text: Unzählige Seiten, welche Suchwörter beinhalten [Höv09]
- Doorway Pages: Eine Doorway Page ist eine Seite, welche auf einen bestimmten Suchbegriff abzielt, aber keine Inhalte aufweist und meist automatisch auf eine andere Seite weiterleitet. [Höv09]
- Cloaking: Bei dieser Art von SPAM wird der Suchmaschine eine andere Website vorgespielt als die, die der menschliche Besucher sieht. [Höv09]
- Link-SPAMming: Hier wird das Ranking der Webseite durch die Verlinkung von Webseiten beeinflusst. [Höv09] Am einfachsten zeigt sich dies anhand eines Beispiels: Der beispielhafte Link zur fiktiven Seite `http://www.masterarbeit-SPIT.invalid` mit dem Linktext "TU Wien" ist dazu geeignet, das Ranking der Seite `http://www.masterarbeit-SPIT.invalid` für den Suchbegriff TU Wien zu verbessern.
- Content Pages: Wenn die Möglichkeit nicht besteht, den eigentlichen Inhalt einer Webseite zu ändern, werden andere Seiten erstellt, welche suchmaschinenoptimierte Inhalte besitzen und diese den eigentlichen Webseiten hinzugefügt. [Höv09]

4.2.6 Link- oder Blog-SPAM

Blog-SPAM ist eine Art von SPAMmen, bei der SPAMmer unzählige Einträge in öffentliche Blogs posten, die wiederum einen Link zu eine Webseite beinhalten. Ein Beispiel dafür ist die fiktive Seite `http://www.masterarbeit-SPIT.invalid`: „Hallo, das ist ein Beispiel für Blog-SPAM. Nähere Informationen finden sie unter `www.masterarbeit-SPIT.invalid`." Ziel solcher Einträge ist es, durch die Link-Popularität das Google-Ranking zu erhöhen. Vom Prinzip her ist Blog-SPAM mit Guestbook-SPAM zu vergleichen. Durch ein Update des Google-Algorithmus im Jahr 2004 hat diese Art von SPAM aber an Bedeutung und Effizienz verloren. Es gibt allerdings Mechanismen, welche alle Sicherheitsmaßnahmen in Blogs durchbrechen und vollautomatisch Registrierungen durchführen, um dann Nachrichten versenden zu können, was wiederum die Anzahl der Links auf einer Seite erhöht. Links, welche in den Registrierungen angegeben sind, werden von den meisten Suchmaschinen allerdings nicht berücksichtigt.

4.2.7 Social Bookmark-SPAM

Der Begriff Social Bookmark hat sich erst seit dem Entstehen des Web 2.0 ergeben. Als Social Bookmarks werden Webseiten bezeichnet, welche einen

Online-Service zur Verfügung stellen, der ungefähr den bekannten Bookmarks (Lesezeichen) von herkömmlichen Internetbrowsern entspricht. Der Vorteil von Bookmarks, welche online verfügbar sind ist, dass sie von jedem mit dem Internet verbundenen Computer aus abrufbar sind. Weitere Vorteile liegen darin, dass man auf diesen Social Bookmark Webseiten auch die eigenen Lesezeichen mit anderen Benutzer teilen und austauschen kann. Da das Internet eine der schnellsten wachsenden und sich ändernden Technologien ist, welche die aktuelle Wirtschaftslage, aber vor allem das Verhalten der Menschen beeinflusst, verändert sich auch der Zweig der Social Bookmarks (Beispiel Facebook als Plattform für Social Bookmarks). [Ker06] Nachfolgende Abbildung 4.7 auf Seite 53 zeigt aktuelle Plattformen für Social Bookmarks.

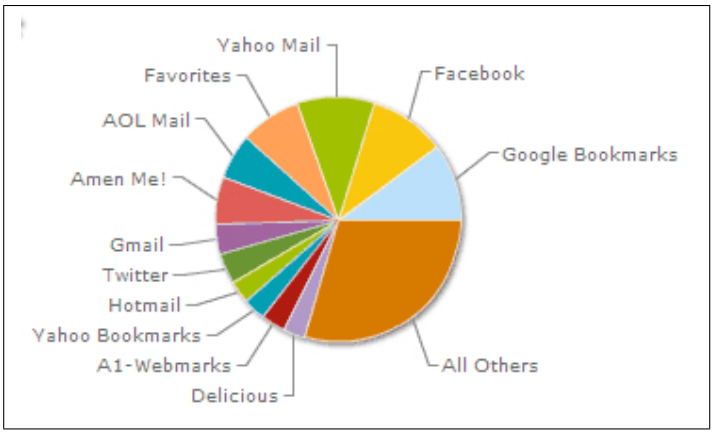


Abbildung 4.7: Social Bookmarking im Jahr 2010 [Wil10]

Durch den hohen Bekanntheitsgrad dieser Plattformen ebenso wie durch die hohe Nutzung und Frequentierung, wurde auch SPAM im Bezug auf diese Services zum Thema. Das Schlagwort Social Bookmarking-SPAM wurde zu einem tragenden Begriff im WWW. Personen, welche es sich zum Ziel gesetzt haben, Social Bookmarking-SPAM zu erzeugen, versuchen durch das Hinzufügen von Links mehr Zugriffe auf ihre eigenen Seiten zu erlangen. Solche Links werden in der Welt des Internets als Backlinks bezeichnet. Nach längeren Beobachtungen wurde diese Art von Missbrauch ersichtlich und die meisten Social Bookmarking Plattformen haben das Attribut rel=’nofollow’ zu ihren ausgehenden Links hinzugefügt. Das Attribut nofollow ist ein optionaler Teil eines Hyperlinks, welcher die Suchmaschine anweist, diese sogenannten Rückverweise bei der zur Berechnung der Linkpopularität nicht zu berücksichtigen. Das bedeutet, die Grundidee des Social Bookmarking-SPAMs hat keine Wirkung mehr (nicht alle Suchmaschinen berücksichtigen dieses Attribut). So kann der Missbrauch von Bookmarks eingeschränkt werden. [Ker06]

4.2.8 Wiki-SPAM

Wiki-SPAM verfolgt ähnliche Ziele wie die zuletzt vorgestellten SPAM-Arten wie zum Beispiel Social Bookmarking-SPAM, Link-SPAM, Blog-SPAM, usw. Kernziel ist es, durch das Hinzufügen von Hyperlinks, welche auf eigene, meist kommerzielle Seiten verweisen, eine höhere Bewertung der Seiten in den Suchmaschinen zu erlangen. Das funktioniert deshalb, weil die meisten Suchmaschinen das Teilkriterium Linkpopularität verwenden. Das bedeutet, je öfter ein Link im WWW zu finden ist bzw. geklickt wird, desto höher ist sein Rating bei den Suchmaschinen. Wiki-Seiten versuchen diesen Umstand ebenfalls durch das Hinzufügen des Attributs rel="nofollow", beschrieben im Abschnitt Social Bookmark-SPAM, beim Hyperlink zu verhindern.

Kapitel 5

SPAM over Internet Telephony

Das Kapitel SPAM over Internet Telephony (SPIT) stellt die Einleitung in den Kernbereich dieser Masterarbeit dar und gibt einen Überblick bezüglich der Charakteristiken, der Arten und des Einsatzes von SPIT.

5.1 SPIT im Detail

Das Wort SPIT stammt aus dem englischsprachigen Raum und bedeutet soviel wie „spucken“. An Bedeutung gewonnen hat dieses Thema, da sich die Kosten für Internettelefonie zu einem sehr niedrigen Niveau entwickelt haben. Dies hatte zum einen zur Folge, dass eine breite Masse an Privat- wie auch Firmenbenutzern diese Technologie nutzen und somit eine sehr breite Schicht an Endbenutzern erreicht werden kann und zum anderen bietet sich ein solcher Markt für Telefon-SPAMs an, da die Kosten für den SPAM-Verbreiter sehr gering sind. SPAM-Verbreiter werden auch als SPITter, SPAMmer, usw. bezeichnet.

In der Literatur findet man einige gängige Definitionen von SPIT.

Unter SPIT versteht man

- eine Art von SPAM, welche via VoIP übertragen wird
- Telefon-SPAM über Internet-Telefonie
- unerwünschte Werbebotschaften aus oft unseriösen Quellen und Organisationen
- massenweise Übertragung unerwünschter Anrufe
- massenweise unerwünschte Verbindungsaufbauversuche, mit dem Ziel, eine Voice-, Video- oder Instant Messenger(IM)-Session aufzubauen

[Kha08a]

Diese Definitionen haben allesamt das gemeinsame Problem, dass sie entweder zu allgemein bzw. zu spezifisch sind oder sie nicht alle Teilbereiche von SPIT abdecken. Basierend auf [Kha08a] kann folgende Definition verwendet werden: Das Ziel eines SPIT Angreifers ist es, eine Kommunikationsverbindung mit möglichst vielen Endbenutzern aufzubauen, um so eine Nachricht an möglichst viele Empfänger zu verteilen.

Erreicht wird das Ziel durch folgende drei Schritte, welche in Abbildung 5.1 auf Seite 57 grafisch dargestellt und beschrieben werden:

1. Beschaffen von Informationen
2. Aufbau einer Verbindung zu den Zielen
3. Versenden der Nachrichten an die Ziele

[Kha08a]

Beschaffen von Informationen
Diese Phase hat das Ziel, eine möglichst große Anzahl von Kontaktadressen zu sammeln. Dies passiert meist über einen Angriff auf das im Kapitel 3 - Grundlagen von VoIP, Abschnitt Technik, beschriebene ENUM. Wie schon erläutert, verwaltet ENUM Telefonnummern und dazugehörige Kommunikationsadressen.

Aufbau einer Verbindung zu den Zielen
Nachdem der Angreifer eine große Anzahl an Kontaktadressen gesammelt hat, kann damit begonnen werden, Verbindungen aufzubauen. (siehe Abschnitt 3.4 - SIP - Kommunikation in VoIP) Es gibt zwei Möglichkeiten, eine Verbindung aufzubauen. Der Voice-SPAMmer kann eine Verbindung mit einer Invite-Nachricht über einen Proxy beginnen, was auch als SPIT via Proxy bezeichnet wird oder er beginnt eine Verbindung mittels eines direkten Aufruf ohne Proxy, was als Direct IP-SPITting bezeichnet wird. Beide Arten unterscheiden sich in zwei Dingen, zum einen in der Art der SIP-Adresse und zum anderen muss beim direkten Angriff kein Account vorhanden sein, sehr wohl aber beim Proxy SPITting (Siehe Kapitel 3)

Versenden der Nachrichten an die Ziele

Der letze Schritt eines SPIT-Prozesses ist das Senden der Nachrichten, nachdem die Verbindung aufgebaut wurde (siehe RTP Kapitel 3 Abschnitt Technik)

Welche Nachrichten gesendet werden, hängt davon ab, welche Art von Angriff der SPITter bezweckt (siehe Abschnitt 5.2).
[Kun08], [Kha08a], [Ewa07]

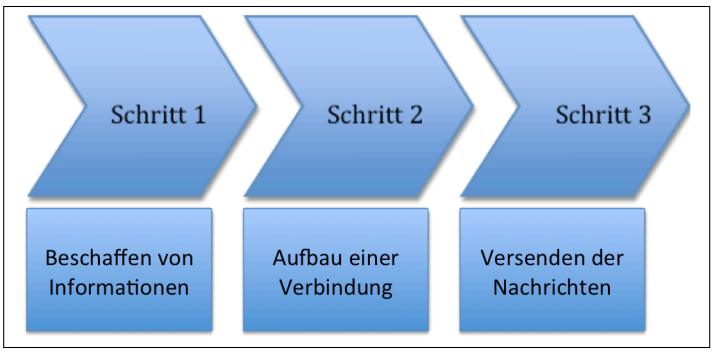


Abbildung 5.1: Drei Phasen eines SPIT-Angriffs nach [Kha08b]

Der wesentlichste dieser drei Punkte ist der Aufbau der Verbindung. Hier ist es von enormer Wichtigkeit, dass möglichst viele Verbindungen aufgebaut werden, um eine größtmögliche Anzahl von Usern zu erreichen.

Ein Beispiel, wie ein SPIT-Angriff vor sich gehen kann:
Durch ein Tool names SPITter [Col06] Kapitel 14, welches von David Endler und Mark Collier entwickelt wurde, kann man SPAM in das bekannte Open-Source VoIP-System Asterisk einspielen. Das entwickelte Tool ist für die selbe Plattform (Unix-Derivate), auf der auch Asterisk aufsetzt, entwickelt worden. Dieses Tool bedient sich eines zur Verfügung gestellten ASCII-Files, welches alle notwendigen Informationen beinhaltet, um einen Rufaufbau zu charakterisieren. Aus diesem File werden separate Anruffiles, welche von Asterisk genutzt werden können, erzeugt und im /tmp-Ordner des VoIP-Systems abgelegt. Später werden diese temporär abgelegten Files in den ausgehende Spool-Ordner des Asterisk-Systems abgelegt (/var/spool/asterisk/outgoing/). Asterisk selber beobachtet diesen Ordner und nutzt sofort nach Erzeugen eines neuen Files die gefundenen Informationen, um einen neuen Anruf zu tätigen. [Nic07] Das enwickelte SPITter-Tool muss mindestens ein Call-File zur Verfügung stellen, jedoch ist eine Obergrenze nur durch den zur Verfügung gestellten Speicherplatz begrenzt. Der Typ des erzeugten Files ist belanglos, da die Informationen auf ASCII-Basis gelesen werden, jedoch ist es von Vorteil, einen ausdrucksstarken Typ zu wählen, wie z.B. .call, .voip, etc... . Jedes nun vom SPITter Tool erzeugte File hat diesen Typ in Form von SPITterCallZUFALLSNUMMER.call. [Col06]

Ein Beispiel File dafür ist auf [Kem02] zu finden.

Eine freie Applikation aus dem WWW nennt sich TeleYapper (`http://`

nerdvittles.com/index.php?p=113). TeleYapper ist ein Asterisk Messaging Broadcast System. Dieses Tool ermöglicht ebenfalls das Einspielen von SPIT-Nachrichten in ein VoIP-System. Für den privaten Gebrauch wird TeleYapper gemeinsam mit trixbox [Fon10] genutzt. Trixbox ging im Mai 2006 aus dem Projekt Asterisk@Home [Gil06] hervor.

Die Funktionsweise des Tools zeigt, dass es aus einer SQL-Datenbank besteht, in welcher Anrufgruppen definiert werden. Dazugehörig werden Audionachrichten in der Datenbank abgelegt. Dieses Tool erkennt auch nicht angenommene Anrufe und kann diese zu einem späteren Zeitpunkt erneut absetzen. [Col06]

Ein weiteres Testanruf-Tool haben Forscher des Frauenhofer Institutes entwickelt. Basierend auf dem frei verfügbaren Tool SIPp haben die Entwickler den SIP XML Scenario Maker (SXSM) enwickelt. Dieser simuliert SPIT-Anrufe und produziert SPIT nach definierten Kriterien. Des Weiteren ist es möglich, diese Nachrichten zu versenden und die Rückmeldungen zu speichern. Zweck ist es, Angriffe zu simulieren und eine Erfolgsbilanz der Verteidigung abzubilden. [Kha08a]

5.2 SPIT-Verfahren

Laut [Waa06] werden werden drei Arten von Angriffsszenarien unterschieden:

1. Call Centres
   Hierbei nimmt ein Computer die Verbindung zu einer Adresse aus der Liste auf und leitet den Anruf nach erfolgreicher Annahme zu einem Callagent aus einem Callcenter weiter, welcher dann mit der angerufenen Person Kontakt aufnimmt. [Waa06]

2. Calling Bots
   Diese Art von SPIT arbeitet eine Liste von Anruferinformationen ab und nach jeder erfolgreichen Kontaktaufnahme wird eine vorher aufgezeichnete Nachricht abgespielt. [Bro09], [Waa06]

3. Ringtone SPIT
   VoIP-Endgeräte, welche über eine Vorkonfiguration verfügen, akzeptieren einen speziellen SIP-Header [Cor06], welcher eine Alert-Info als Inhalt hat. Diese Alarminformation hat unter anderem eine URL als Inhalt, welche auf ein vorher aufgezeichnetes Audiofile zeigt, das sich im Internet befindet. Es wird schon ersichtlich, dass sich hier eine Schwachstelle befindet, die von SPITtern ausgenutzt wird, indem sie diese Alert Informationen verändern und auf eine eigens aufgezeichnete Werbeinformation verweisen welche darauf abzielt die Angerufenen zum Rückruf einer meist teuren Mehrwertnummer zu bewegen.

Eine Abwandlung dieser Methode ist es, dass der Angreifer nur das Telefon des Betroffenen läuten lassen will. In diesem Fall werden keine Mediadateien mitgesendet und jede aufgebaute Session wird sofort wieder geschlossen. Somit läutet das Telefon und keine Nachrichten werden übermittelt. Das hat störende und unangenehme Auswirkungen auf die Benutzer von VoIP-Systemen. [Waa06]

Kapitel 6

Methoden der Abwehr von SPIT

Durch das immer häufigere Auftreten von SPAM im Bereich von VoIP besteht die Notwendigkeit, Gegenmaßnahmen zu treffen.

Solche Gegenmaßnahmen kann man nach Rosenberg und Jennings [Ewa07] in folgende Kategorien unterteilen:

- Non-intrusive methods (Methoden ohne Interaktionen von Anrufer oder Angerufenen)
  Die Grundlage dafür ist ein Austausch und eine Analyse der signalisierenden Nachrichten. Diese Art von Methoden werden auch non-interaction methods genannt, setzen keine Hürden für den Anrufer. Die Effektivität dieser Methoden ist begrenzt. Darunter fallen Methoden wie blacklists, call patterns, call rates, usw...

- Caller interaction methods (Methoden mit Interaktion des Anrufers)
  Hierbei werden dem Anrufer gewisse Hürden in den Weg gelegt. Dieser muss vor der erfolgreichen Verbindung einen Kontrollabschnitt überwinden. Diese Methoden basieren auf der Analyse von Aktionen und deren Reaktionen.

- Callee interaction Methods (Methoden mit Interaktion des Angerufenen)
  Diese Methoden basieren auf dem Prinzip, dass der Benutzer vor Verbindungsannahme gefragt wird, ob er den Anruf akzeptiert.

Die grobe Einteilung in Non-intrusive, Caller interaction und Callee interaction kann durch das Referenzmodell zum Schutz vor SPIT [Sch08] nochmals detaillierter vorgenommen werden. Die Unterteilung erfolgt in fünf sogenannte Stages, welche in Abbildung 6.1 auf Seite 64 ersichtlich sind:

1. Stage 1: Non-intrusive methods [Sch08]

   Stage 1 entspricht nach Rosenberg und Jennings [Ewa07] dem Teilbereich Non-intrusive methods.

   Darunter fallen Abwehrmechanismen wie

   - Blacklists
     Liste mit gesperrten Benutzern
   - Whitelists
     Liste der zugelassenen Benutzern
   - Circle of Trust
     Circles of Trust sind Lösungen, welche auf der Verarbeitung von vertrauenswürdigen Netzwerken basieren
   - Pattern Lösungen
     Pattern Lösungen analysieren den Anrufer anhand eines gewissen Verhaltensmusters

2. Stage 2: Caller interaction methods [Sch08]

   Stage 2 entspricht nach Rosenberg und Jennings [Ewa07] dem Teilbereich Caller interaction methods

   Unter dieser Kategorie von Methoden finden sich Lösungen wie

   - Greylisting
     Greylisting ist eine Methode, bei der der erste Anruf eines Teilnehmers abgewiesen wird, mit der Aufforderung, den Anruf nach einer gewissen Zeitspanne zu wiederholen. Sollte dies der Fall sein, wurde der Greylisting-Prozess bestanden.
   - Computational Puzzle
     Das Prinzip hinter dieser Art der Abwehr von SPIT ist es, dass man dem Anruferterminal vor dem Gespräch eine ressourcenkonsumierende Aufgabe gibt, da SPIT-Generatoren in einer bestimmten Zeit nur eine limitierte Anzahl an Anrufen abarbeiten können. Allerdings kann dieser Schutzmechanismus durch die Verwendung von Botnets umgangen werden.
   - Sender Check
     Die Idee dahinter basiert auf einer Methode, die feststellt, ob der Anrufer einen gültigen Sender in seiner Domain darstellt.
   - Turing Test
     Der englische Mathematiker Alan Turing befasste sich bereits im Jahre 1950 in seiner Ausarbeitung „Computing machinery and intelligence“ mit der Problematik der künstlichen Intelligenz (KI).

> Die grundsätzliche Fragestellung der Arbeit war es, ob eine Maschine jemals in der Lage sei, menschlich zu denken. Um dies zu testen, schlägt er eine empirische Testfolge vor, welche nach ihm benannt wurde.
> [Lug97]
>
> Grundidee dieser Testfolge ist es, dass ein menschlicher Richter im Mittelpunkt einer dialogbasierten Kommunikation steht. Einerseits kommuniziert der Richter über ein Terminal mit einer anderen Maschine und andererseits kommuniziert der Richter über ein Terminal mit einem Menschen. Aufgabe des Richters ist es nun, nach erfolgter Kommunikation, wobei Mensch sowie Maschine über die Aufgabe des Richters informiert sind, zu entscheiden, wer von den zwei Parteien nun der Mensch und wer die Maschine ist.
> [Lug97]

3. Stage 3: Feedback before call [Sch08]

   Stage 3 gehört nach Rosenberg und Jennings [Ewa07] zum Teilbereich der Callee interaction Methods.

   Methoden dieser Kategorie benötigen eine Aktion des Benutzers bei Eingang von SPIT.

   - Consent-based communication
     Das Prinzip dahinter lautet, dass Benutzer A Anrufer B beim ersten Kontakt zuerst autorisieren muss, bevor ein Kontakt hergestellt werden kann.

4. Stage 4: Feedback during call [Sch08]

   Stage 4 gehört nach Rosenberg und Jennings [Ewa07] zum Teilbereich der Callee interaction Methods.

   Methoden dieser Kategorie zielen darauf ab, dass der Benutzer den Anruf annimmt und während des Gesprächs wird der SPIT-Überprüfungs-Prozess gestartet.

   - Content filtering
     Anhand des Inhalts wird entschieden, ob es sich um einen SPIT-Anruf handelt.

5. Stage 5: Feedback after call [Sch08]

Stage 5 gehört nach Rosenberg und Jennings [Ewa07] zum Teilbereich der Callee interaction Methods.

Methoden dieser Kategorie zielen darauf ab, dass der Benutzer selber Feedback zu den entgegengenommenen Anrufen abgibt.

- Reputation System
  Das Ziel ist es, eine Bewertung zu einen Kontakt hinzuzufügen, um später erkennen zu können, ob dieser ein SPIT-Verhalten aufweist.
- Limited-use adresses
  Diese Maßnahme bedingt, dass man, sobald eine SPAM-Nachricht eingeht, seine Adresse verändert.
- Payments at risk
  Entspricht einem Pfandsystem bei Anrufen.
  - Beispiel: Cost for Telephony (siehe Abschnitt 6.2)
- Legal action
  Idee dahinter sind gesetzliche Verordnungen, welche SPIT verbieten.

[Sch08]

6.1 Methoden zur Abwehr von SPIT in VoIP - Allgemein

Gegenmaßnahmen im Bereich SPIT sollen den Problemen, welche ähnlich den bekannten Problemen im Bereich E-Mail sind, entgegenwirken. Eine Gegenüberstellung von SPIT und SPAM zeigt einige Unterschiede auf. Der Bereich der elektronischen, schriftlichen Nachrichten bringt den Vorteil mit sich, dass die versendeten Nachrichten schon vor dem Empfang bekannt sind. Das bedeutet, dass der Inhalt einer Nachricht bereits zum Zeitpunkt der Übertragung vollständig spezifiziert sein muss. Des Weiteren kann der Empfänger einer E-Mail frei entscheiden, ob er diese Nachricht annehmen will. Im Gegensatz dazu ist das im Bereich SPIT nicht der Fall. VoIP-Inhalte sind erst zu dem Zeitpunkt bekannt, wenn eine VoIP-Verbindung angenommen wird. [Kha08a]

Das bedeutet, dass die Methoden, welche bei E-Mail-SPAM-Filter eingesetzt werden, nur teilweise oder überhaupt nicht auf den Bereich VoIP angewendet werden können. Derzeitige Varianten von Methoden zur Abwehr beziehungsweise zur Identifizierung von SPIT basieren im Wesentlichen auf sogenannten Blacklists bzw. Whitelists. Weitere Möglichkeiten, welche eingesetzt werden, um SPIT zu verhindern, werden durch Turing Tests realisiert. Diese Art

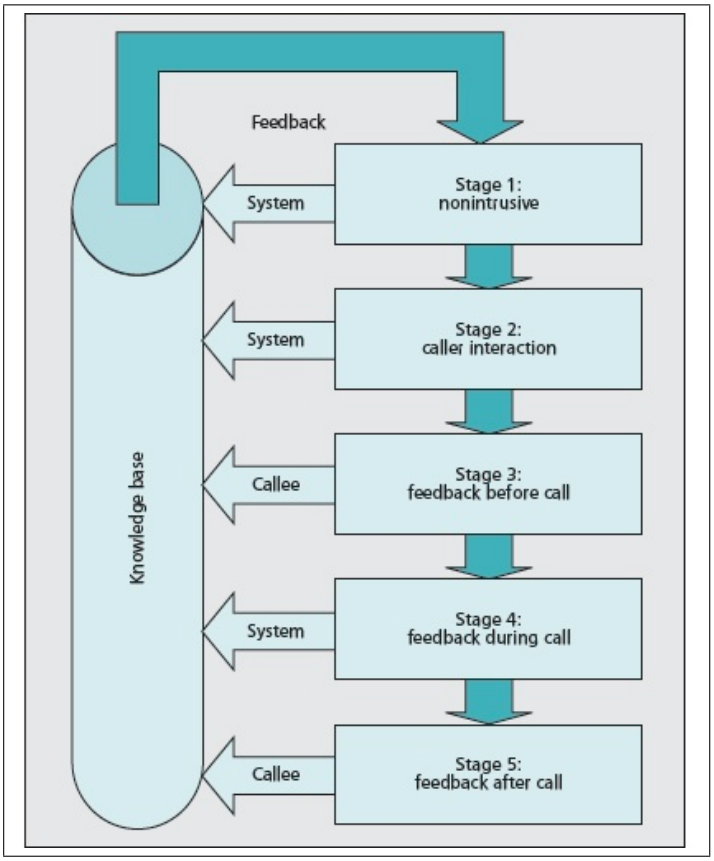


Abbildung 6.1: Referenzmodell zur Abwehr von SPIT, nach [Sch08]

von Tests zielen darauf ab, die Entscheidung zu treffen, ob der Anrufer ein Mensch oder ein Computersystem ist. Weitere Verfahren, welche angewendet werden, legen ihren Schwerpunkt auf soziale Netzwerke bzw. die Verwendung von Buddy-lists. Eine weitere Methode, um SPIT entgegenwirken zu können ist, die Identität eines Anrufers als Voraussetzung einer Kommunikation anzusehen. Dieses Verfahren wird zur Zeit von der Internet Engineering Task Force (IETF) standardisiert. [Eur07]

Der Nachteil einiger dieser Verfahren ist es, dass zur Identifizierung dieser Anrufe auf Parameter zurückgegriffen wird, welche auf den Anrufdaten des Absenders basieren. Diese Parameter können durch einen Anrufer gezielt manipuliert werden. Weiters sind viele dieser Verfahren sehr unflexibel im Bezug auf schnelle Veränderungen des SPIT-Senders. [Eur07]

In den nachfolgenden Unterpunkten werden einzelne ausgewählte SPIT-Abwehrmechanismen im Detail untersucht und beschrieben.

6.2 Cost for Telephony

Ein durchaus erfolgsversprechender Ansatz welcher in [Moe06] näher beschrieben wird, um sich vor SPIT zu schützen, ist es, Kosten vom Anrufer einzufordern, sollte es sich um einen SPAM-Anrufer handeln. Diese Vorgehensweise steht somit im Gegensatz zur ursprünglichen Philosophie von VoIP, kostengünstiges Telefonieren zu ermöglichen. Diese Art des Schutzes hat den Vorteil, dass eine größere Zahl von SPAM-Anrufern damit ausgegrenzt werden kann, da ein teures kostenbehaftetes System unerwünschte Werbeanrufe für den SPAMmer teuer und somit unattraktiver macht.

Des Weiteren ergibt sich der Vorteil, dass unbekannte Anrufer, von denen ein Teil Nicht-SPAM-Anrufer sind, durch die entstehenden Kosten trotzdem die Möglichkeit haben, eine Verbindung mit dem gewünschten Gesprächspartner aufzubauen. Somit kann diese Art des Schutzes für den Teil der nicht bekannten Anrufer genutzt werden. Eine mögliche Realisierung dieses Ansatzes wäre es, den unbekannten VoIP-Anrufer auf ein herkömmliches PSTN-Netz weiterzuverweisen, damit Kosten für den Anrufer entstehen. [Waa06]

Eine weitere Realisierung in diesem Bereich ist der Ansatz, eine Art Pfandsystem beim ersten Anruf aufzubauen. Die Grundidee besteht darin, dass man jedem Anrufer vor dem eigentlichen Verbindungsaufbau, beim ersten Verbindungsversuch, einen Pfand hinterlegen lässt. Wenn sich herausstellt, dass der Anrufer kein SPAM verbreitet, wird der Pfand nach Beendigung wieder rücküberwiesen.

Probleme im Bezug auf diese Idee bestehen darin, dass man eine eigene Infrastruktur für die Transaktionen aufbauen muss, was eine hohe Komplexität beinhaltet und mit sehr hohen Kosten verbunden ist. Diese Kosten müssen mit relativ hohen Transaktionsgebühren eingehoben werden, was eine Gebühr von ca. 15 Prozent für den Hin- und Rückweg ausmachen würde. Ein weiteres Problem bei weltweiter Nutzung stellen die unterschiedlichen Währungen dar. Um diese Idee umzusetzen, muss eine Einheitswährung beziehungsweise ein anderes Verrechnungssystem eingeführt werden. [Tur07]

Im Bezug auf den Pfand und die globale Nutzung tritt ein weiteres Problem auf. Weltweit ist die Verteilung von Hab und Gut sehr unterschiedlich. Es muss also eine Höhe des Pfandes bestimmt werden, welche eine weltweite Akzeptanz findet, zum Beispiel 0,01 Euro. Die Einführung eines Pfandsystems spricht auch gegen die Philosophie von SIP, Komplexität sowie Monopolisierung zu verhindern. [Tur07]

Nachfolgende Abbildung 6.2 zeigt das Prinzip eines Pfandsystems im Bereich VoIP. Wie schon in diesem Abschnitt dargestellt, wird ein Pfand im Vorhinein hinterlegt, zum Beispiel 0,01 Euro und im Falle eines SPIT-Anrufes wird der Pfand einbehalten, im Falle eines Nicht-SPIT-Anrufes wird ein gewisser Betrag, zum Beispiel 0,8 Cent, an den Anrufer zurückgesendet (Betrag abzüglich der ca. 15 Prozent Transaktionskosten). Der Rest wird als Transaktionsgebühr einbehalten.

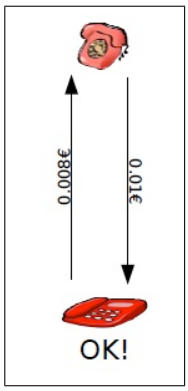


Abbildung 6.2: Pfand als Methode zur Abwehr von SPIT [Tur07]

6.3 Whitelists

Unter einer Whitelist, welche näher unter [Det07] erläutert wird, versteht man eine Sammlung von Kontakten und Teilnehmern, deren Anrufe nicht abgewiesen oder blockiert werden sollen. Das bedeutet, Anrufe von Kontakten, welche in dieser Liste aufgenommen wurden, werden durchgeleitet, jene

Kontakte, die nicht in dieser Liste aufscheinen, werden blockiert.

Prinzipiell werden Whitelists unterteilt in

- private Whitelists
- erweiterte/importierte Whitelists

Erstere werden von den VoIP-Benutzern selber gepflegt und gewartet. Der Nachteil, welcher sich durch die Verwendung von privaten Whitelists, auch Buddylists genannt,ergibt, ist, dass auch jene Kontaktgruppen, welche nicht in der Liste erfasst wurden und keine SPIT-Nachrichten verteilen, nicht mit dem Benutzer in Kontakt treten können.

Im Gegensatz dazu stehen die erweiterten beziehungsweise importierten Whitelists. Der Ansatz dieser Filtermethode geht in Richtung vertrauenswürdiger Netzwerke. Abbildung 6.3 zeigt einen möglichen Zusammenhang zwischen einzelnen Whitelists, welche durch das Telefonsymbol angedeutet werden:

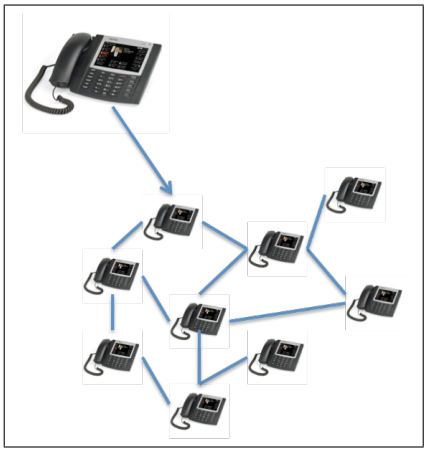


Abbildung 6.3: Whitelist Netzwerk nach [Tur07]

Als Grundlage dient die Idee von Pretty Good Privacy (PGP). PGP kommt unter anderem auch bei der Signatur von Nachrichten zum Einsatz. Eine Signatur dient zum Nachweis der Echtheit einer Nachricht.

Die erweiterte Whitelist wird veröffentlicht, mit anderen Whitelists von vertrauenswürdigen Teilnehmern verknüpft und das unter Berücksichtigung der Vertrauenspriorität. Als Ergebnis erhält man ein Netzwerk von vertrauenswürdigen Whitelists. Kann ein ankommender Anruf anhand der eigenen Whitelist nicht zugeordnet werden, so wird ein Abgleich mit den Whitelists des Netzwerks gemacht und eine Entscheidung getroffen.

Dieses Konzept liefert den Vorteil, dass die Anzahl der vertrauenswürdigen Kontakte im Gegensatz zur Anzahl der Kontakte aus der eigenen Whitelist wesentlich größer ist. Das Risiko, dass Kontakte, welche noch auf keiner Whitelist vermerkt sind, blockiert werden, bleibt allerdings weiterhin bestehen und wird durch diese Art der Filterung nur minimiert. Ein weiteres Restrisiko besteht darin, dass eine der Whitelists aus dem Netzwerk manipuliert wird und somit das Vertrauen im Netzwerk gebrochen wird. Somit besteht die Möglichkeit, SPIT auch in einem vertrauenswürdigen Netzwerk zu verbreiten. [Det07]

Nachfolgende Abbildung 6.4 zeigt, dass der eigentliche Benutzer eine große Anzahl von vertrauenswürdigen Whitelists in seinem Netzwerk hat. Einer dieser vertrauenswürdigen Partner besitzt allerdings einen Kontakt, beziehungsweise eine Verbindung zu einem nicht-vertrauenswürdigen Kontakt, welcher wiederum eine Menge nicht-vertrauenswürdiger Kontakte besitzt. Beim Vergleich der Identität eines Anrufers im vertrauenswürdigen Netzwerk entsteht so eine Stelle im Netzwerk, welche einen Vertrauensbruch darstellt und die Möglichkeit bietet, eventuelle SPIT-Nachrichten in das Netzwerk einzuschleusen.

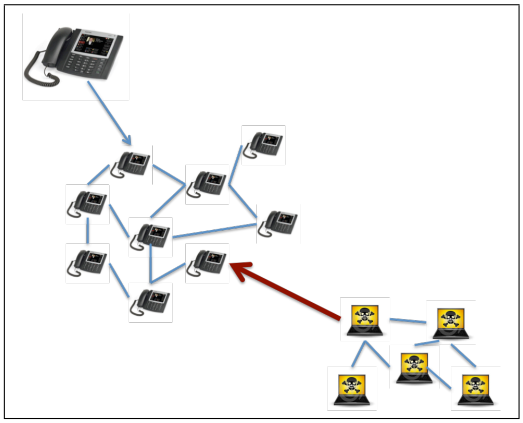


Abbildung 6.4: Whitelist Vertrauensbruch nach [Tur07]

6.4 Blacklists

Blacklists, welche näher unter [Ber09] erläutert werden, sind eine sehr verbreitete Methode, um SPAM im Bereich von E-Mails zu verhindern. Im Gegensatz zu den Whitelists, welche Listen der zugelassenen Benutzer darstellen, beinhalten Blacklists eine Liste der unerwünschten, nicht zugelassenen Kontakte. Viele der Anbieter wie GMX, GMail, usw. bieten die Möglichkeit, eine Blacklist zu führen. Durch den bekannten Erfolg von Blacklists im Bereich von E-Mail ist es naheliegend, dieses Konzept auch im Bereich VoIP

zur Abwehr von SPIT einzusetzen. Somit wurde das Prinzip von Blacklists aus dem Bereich der E-Mails als eine Art Referenz herangezogen, um diese im Bereich VoIP zu verwirklichen. [Ber09]

Grundsätzlich kann davon ausgegangen werden, dass eine IP-Adresse, die als E-Mail-SPAMmer klassifiziert und vermerkt wurde, ebenfalls im Bereich VoIP als SPIT-Verbreiter tätig sein wird. [Ber09] Somit kann eine große Anzahl von möglichen SPIT-Verbreitern ausgeschlossen werden, indem auch bei VoIP Blacklists-Service unter Verwendung von DNS verwendet werden. In [Ber09] wird die Funktionsweise von Blacklists bei VoIP dargestellt. Es wurde ein Modul SpitAssassin entwickelt, welches die Abfrage von Blacklists bei VoIP einbindet.

Blacklists-Service unter Verwendung von DNS
Blacklists kommen bei sehr großen Unternehmungen, Nonprofit-Organisationen und Providern zum Einsatz. Diese Unternehmungen speichern alle IP-Adressen oder oftmals sogar IP-Netzwerke, welche potentielle SPAM-Verbreiter darstellen. Die Länge der Listen und die Zeit, wie lange eine IP-Adresse auf der gesperrten Liste aufscheint, unterscheidet sich von Unternehmen zu Unternehmen. Es gibt weder Regeln, wie eine IP-Adresse hinzugefügt wird, noch, wie lange diese aufscheint. Dass bedeutet, eine Standardisierung ist nicht gegeben. [Ber09]

Blacklists weisen als Gemeinsamkeit die Technik einer Abfrage von IP-Adressen auf. Blacklists werden als DNS-Server verwirklicht, welche nahezu in Echtzeit abgefragt werden können. Ein Realtime-DNSBL (RT-DNSBL) wird dazu verwendet, um IP-Adressen von Simple Mail Transfer Protocol (SMTP)-Servern zu speichern.

Nachdem eine Veränderung der SPAM-Herkunft von SMTP-Servern hin zu Botnets beobachtbar war, wurden in den DNSBL-Servern nunmehr die IP-Adressen dieser Botnet Hosts verwaltet. Botnets sind Personalcomputer, welche durch einen Trojaner von einem Hacker remote kontrolliert werden können und dazu verwendet werden, um SPIT oder SPAM zu versenden. Trojaner werden dazu verwendet, dass ein Hacker seine eigenen Dienste auf einem fremden Rechner in Anspruch nehmen kann. So kann ein bereits infizierter Rechner in einem Botnet durch die Wiederverwendung und einem Update der Botnet-Infrasturktur gleichzeitig für die Verbreitung von SPAM und SPIT verwendet werden. [Ber09]

Aus SMTP-Protokoll und SIP-Protokoll resultiert ein gemeinsames Problem: Es ist sehr leicht möglich, den Header dieser Nachrichten zu verändern. Somit wird der Sender einer SPAM-Nachricht versteckt. Im Bereich von Blacklists ist der Received-Header, welcher bei jedem weitergeleiteten Transportser-

vice angehängt wird, von großem Interesse. Dieser Header beinhaltet den Hostnamen bzw. die IP-Adresse vom Host des Senders sowie vom Host des Empfängers.

Um eine Abfrage auf einen DNSBL-Server zu starten, wird die IP-Adresse des sendenden Hosts verwendet. Diese wird rückwärts als eine Art virtueller Host zu den Adressen des DNSBL-Servers hinzugefügt. Ist die Adresse zum Beispiel w.x.y.z und der DNSBL-Server blacklist.at, so wird vom suchenden Mail-Server ein DNS-Lookup nach dem Namen z.y.x.w.blacklist.at verwendet.

Diese DNS-Anfrage liefert eine virtuelle IP-Adresse, zum Beispiel 127.0.0.1, wenn die IP-Adresse w.x.y.z bereits auf dieser Blacklist vorhanden ist. Sollte dies nicht der Fall sein, wird vom DNSBL-Server ein Antwortcode-Name-Error geliefert.

Wie im oberen Teil schon erläutert, ist es wahrscheinlich, dass ein Host, der SPAM verbreitet, auch SPIT verbreiten wird, im Gegensatz zu einem Host, der noch nicht auf einer Blacklist angeführt ist. Somit kann man mit dem Ansatz vorgehen, dass man die E-Mail-Blacklists nach den IP-Adressen bzw. Hostnamen durchsucht, welche man aus dem SIP und dem Session Session Description Protocol (SDP, IETF RFC 4566 [Per10]) erhält. Um nun an diese Informationen zu gelangen, gibt es verschiedene Möglichkeiten, die nachfolgend genannt werden: [Ber09]

- Via Headers
  Ein Via Header dient der Rückverfolgung des Nachrichtenweges in SIP-Protokollen. Proxy-Server, bei denen eine SIP-Nachricht durchläuft, haben die Aufgabe, eine Nachricht an diesen Header anzuknüpfen. Als Information der Nachricht werden Protokollinformationen, gefolgt von einem Leerzeichen und Proxynamen mit Port, falls gegeben, hinzugefügt.

  [Joh01]

- Contact Header
  Der Contact Header muss vorhanden sein und beinhaltet die URI-Informationen. Die Informatioen des ContactHeaders sind nicht so wertvoll wie die Informationen des Via Headers, da im eigentlichen INVITE-Dialog ein Anruf auch ohne korrekte URI-Informationen vonstatten gehen kann. Das bedeutet, es kann nicht sichergestellt werden, dass man die gewünschten Informationen bzw. die richtigen Informationen aus dem Contact Header erhält.

- SDP-Message
  In einer SDP-Nachricht sind die IP-Adressinformationen im c= Feld untergebracht. Dieses Feld beinhaltet die Informationen bezüglich der Verbindungsherstellung für den Audiostream. Diese IP-Adresse macht dann Sinn, wenn es sich um einen SPIT-Verbreiter handelt, der menschlicher Natur ist und einen Dialog mit dem Angerufenen herstellen möchte. Sollte die SPIT-Nachricht eine nichtmenschliche Quelle besitzen, das bedeutet zum Beispiel, dass die Nachricht eine vorher aufgezeichnete Botschaft sein kann, dann kann diese Information gefälscht sein.

- Source-IP
  Diese Information kann dazu verwendet werden, um sie gegen bereits vorhandene Blacklists abzugleichen, da diese IP einen richtigen Wert besitzen muss, um zum Beispiel einen Invite-Dialog erfolgreich zu starten.

Im Vergleich zu E-Mail, wo man nur den Received Header dazu verwendet, um einen Vergleich im DNSBL-Server zu starten, wird ersichtlich, dass das SIP- bzw. SDP-Protokoll mehrere Möglichkeiten eröffnet, um IP-Adressinformationen zu erhalten. Das hat zum Resultat, dass die Effektivität von Blacklists im Bereich SPIT höher ausfällt als im Bereich SPAM. Sollte man nicht an die IP-Adresse direkt gelangen, sondern als Ergebnis einen Hostnamen erhalten, so muss ein DNS-Lookup erzeugt werden, um den Hostnamen aufzulösen. [Ber09]

SpitAssassin

SpitAssassin ist ein Teilbereich bzw. ein Ableger von SPAMAssassin, welcher unter eine Apache Lizenz [Ber09] steht. SPAMAssasin ist eine Perl-Applikation, welche dazu benutzt werden kann, um eingehende E-Mails zu analysieren. Hier werden zahlreiche Tests benutzt, wie zum Beispiel:

- Static content filter:

  Dieser benutzt regular expressions, um typische Worte in E-Mails zu erkennen.

- Hash-Checksummen:

  Es werden Hash-Checksummen über den Inhalt der Mail erzeugt und mit einer Remote-Datenbank verglichen.

- Bayesian filter:

  Eingehende E-Mail Inhalte werden mit bereits erhaltenen, alten E-Mail-Inhalten verglichen.

- DNSBL:

  DNSBLs um IP-Adressen abzufragen, welche im Received:-Header angezeigt werden.

[Ber09]

Um eine entsprechende Performance zu erreichen, wird ein SPAMAssassin als daemon gestartet, welcher im Hintergrund läuft und auf eingehende Verbindungen, welche per default auf Port 783 laufen, wartet. Wenn eine E-Mail-Nachricht eingeht, so wird diese automatisch vom E-Mail-System zum SPAMAssassin-Client spac weitergeleitet. Nach Analyse dieser Mail erhält der sogenannte SPAMc eine Antwortmail mit demselben Inhalt und einem erweiterten Header. Der erweiterte Header enthält neben optionalen Informationen auch eine SPAM-probability-score, welche die Wahrscheinlichkeit angibt, dass diese Nachricht eine SPAM-Nachricht ist.

Da die oben angeführten Punkte größtenteils auch sehr wertvoll im Bereich von VoIP sind, gibt es den Ansatz, SPAMAssassin zu erweitern. Die Erweiterung und gleichzeitige Umbenennung in SpitAssassin sieht eine Zusammenarbeit mit dem OpenSIPS vor, um SIP-Header analysieren und verändern zu können. [Ber09]

OpenSIPS, ehemals OpenSER, ist eine Serveranwendung im Bereich von VoIP. Im Speziellen nimmt OpenSIPS die Position einer Vermittlungsgegenstelle ein, welche auf dem SIP-Protokoll basiert.
[Ope10]

Durch die Entwicklung eines Moduls namens SPIT.so von der TU Wien und dem Telecommunications Research Center Vienna wurde die Verbindung zwischen OpenSIPS und dem SPAMAssasin Client SPAMc möglich. Als zweiter Schritt war es notwendig, die Analysen an das SIP-Protokoll anzupassen. [Ber09]

Im Detail sieht die Verbindung zwischen nun mehr SpitAssasin und OpenSIPS wie folgt aus: Das Modul SPIT.so wird in das Konfigurationsfile namens openser.cfg geladen. Jede der ankommenden Anfragen wird nun wie folgt gefiltert:

loadmodule “spit.so“

if ((method == “INVITE“){
sl_send_reply(“100“, “Trying“);

spit_check(“127.0.0.1“);

}
[Ber09]

Ist erkennbar, dass dieser Request ein Missbrauch im Sinne von SPIT sein könnte, wird ein 100 Trying als Antwort gesendet. Diese Verzögerung wird benötigt, da SpitAssassin durch seine hohe Komplexität eine Verzögerung auslöst, die somit bereinigt wird. Die Methode SPIT_check verbindet den Request mit der SPAMc-Komponente. Als Parameter wird der Hostname des SpitAssasin Servers angegeben. SPAMc eröffnet einen Verbindung zum Host von SpitAssassin, wodurch eine Analyse des Requests und eine SPIT-Wahrscheinlichkeit errechnet werden. Die SPIT_check-Methode erweitert den Header der SIP-Nachricht durch XSPAM: xxx/yyy, wobei xxx der errechnete Wert für die SPIT-Wahrscheinlichkeit ist und yyy der vordefinierte Grenzwert. Je höher der errechnete Wert ist, desto höher die Wahrscheinlichkeit, dass es sich bei dieser Nachricht um eine SPIT-Nachricht handelt. Wenn der definierte Grenzbereich durch den errechneten Wert überschritten wird, so wird der Empfänger vor Empfang des Anrufes durch eine entsprechende Warnung informiert. [Ber09]

Nachfolgende Abbildung 6.5 auf Seite 74 zeigt die Zusammenarbeit und den Ablauf von OpenSER bzw. OpenSIPS und SpitAssassin in Kombination mit mehreren DNSBL-Servern. Es erfolgt, wie schon beschrieben, eine Anfrage an OpenSER, dieser reicht die Anfrage weiter zu SpitAssassin. Hier wird der Header analysiert und es erfolgt ein Abgleich mit den DNSBL-Servern. Nach Errechnung der Wahrscheinlichkeit für einen SPIT-Anruf wird entschieden, ob der Anruf durchgeleitet oder abgewiesen wird. Zum Tragen kommen die Signale 180 Ringing, 200 OK und das ACK (ACKnowledgement), welches Signale zur Bestätigung darstellen.

6.5 Statistische Blacklists

Statistische Blacklists (statistical blacklists), welche näher unter [Sis08] bzw. [Ber09] erläutert werden, gehören zur Kategorie der Blacklists. Eine Besonderheit an den statistischen Blacklists ist es, dass diese von Telefonanbietern und Ähnlichem erzeugt werden. Unternehmungen wie Telefonanbieter haben einen Überblick über das Verhalten ihrer Kunden.

Eine Studie [Sis08] im Jahr 2008, welche das Telefonierverhalten von 8.700 Franzosen untersuchte, kam zu folgenden Ergebnissen:

Die durchschnittliche Anzahl an Anrufen, die ein Teilnehmer der Studie an

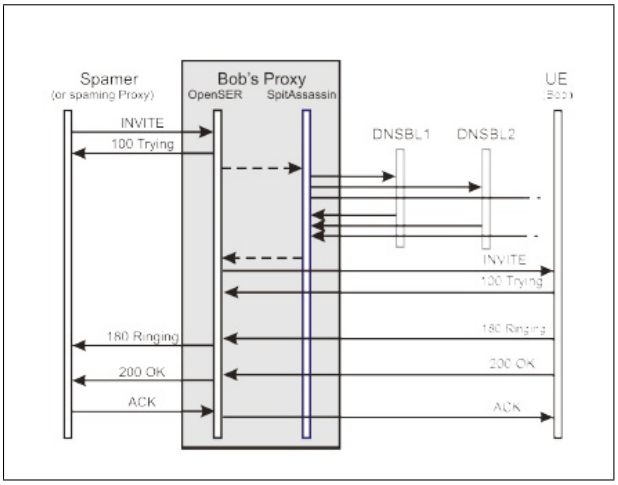


Abbildung 6.5: OpenSER in Kombination mit SpitAssasin [Ber09]

einem Arbeitstag tätigte, lag bei 2,5 Anrufen. Die maximale Anzahl an Anrufen wurde mit 20 pro Tag ermittelt. Naürlich kann dieser Rahmen vor allem im Teenageralter oder auch bei besonderer Verwendung, wie zum Beispiel für Telefonmarketing, gesprengt werden. Abbildung 6.6 zeigt das Telefonverhalten eines durchschnittlichen Teilnehmers dieser Studie. Die maximale Anzahl der Anrufe pro Monat (x-Achse) liegt hier bei zirka 500 Anrufen. Die y-Achse zeigt die Verteilung der Personen, die an der Studie teilgenommen haben.

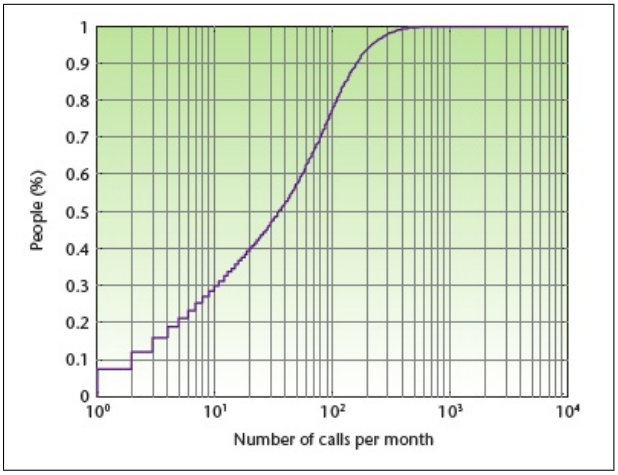


Abbildung 6.6: Durchschnittliche Anzahl der Anrufe pro Monat [Sis08]

An der Studie besonders hervorzuheben ist, dass mehr als die Hälfte der untersuchten Teilnehmer auf eine maximale Anzahl von 40 Anrufen im Monat kamen. Weiters hat diese Studie ergeben, dass die Hälfte der Teilnehmer

dieser Studie zirka drei Stunden im Monat telefonieren. Dies verdeutlicht Abbildung 6.7. Die x-Achse zeigt die durchschnittliche Gesprächsdauer pro Person pro Monat in Sekunden (3 Stunden = 10.000 Sekunden). Die y-Achse zeigt die Verteilung der Personen, die an der Studie teilgenommen haben.

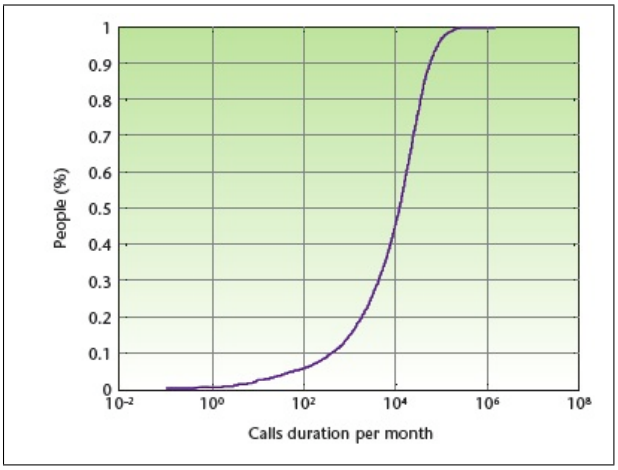


Abbildung 6.7: Durchschnittliche Dauer aller Gespräche pro Monat [Sis08]

Letze Besonderheit, welche durch diese Studie zum Vorschein kommt, ist, dass 90 Prozent der Teilnehmer ihre Gespräche wiederum mit Personen aus demselben Land tätigen, wie in Abbildung 6.8 auf Seite 75 ersichtlich ist. Somit lässt diese Studie einen Rückschluss auf das Telefonierverhalten in anderen Ländern zu:

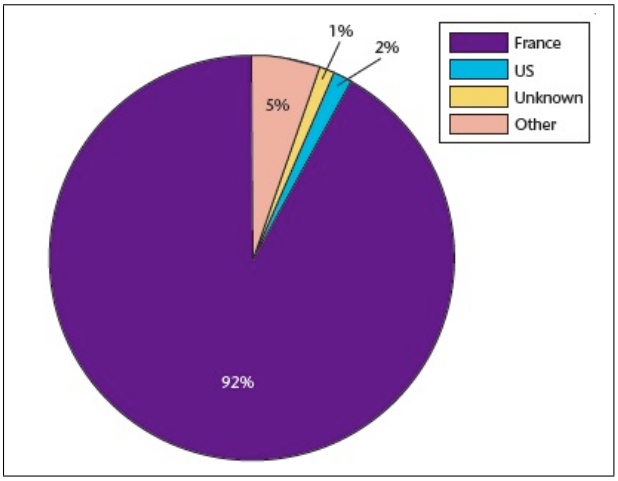


Abbildung 6.8: Lokale Verteilung der Anrufe für die Periode von einen Monat [Sis08]

Durch diese Charakteristiken kann ein SPIT-Verbreiter durch folgende

Punkte erkannt werden:

- hunderte Anrufe pro Tag
- Anrufe von sehr kurzer Dauer
- sehr viele Anrufe in fremde Länder
- Anrufe, die die durchschnittliche Gesamtanrufdauer von drei Stunden pro Monat bei weitem übertreffen

Sollte nun eine Benutzer unter eine oder sogar mehrere Kriterien fallen, so kann das ein Hinweis auf das Aufkommen von SPIT sein.

Das bedeutet, es werden verschiedene statistische Methoden verwendet, die aufgrund der Herkunft und des Verhaltens der Benutzer Beurteilungen erstellen. Spricht die Statistik für einen SPIT-Sender, so wird dieser auf die Blacklist gesetzt. Viele dieser Blacklists behalten es sich vor, den Benutzer durch ein akzeptables Verhalten wieder von der Liste zu streichen. [Sis08] [Ber09]

6.6 Greylists

Greylists, welche näher unter [Han06] erläutert werden, verfolgen eine ähnliche Idee wie Blacklists und Whitelists. Das Verhalten dieser Listen hängt von den Verhalten der Anrufer ab. Zunächst wird beim ersten Anruf eines unbekannten Anrufers der Anruf abgewiesen, ohne dass das Telefon beim eigentlichen Benutzer geläutet hat. Die Annahme ist nun, dass ein Benutzer mit legitimen Interesse an einem Gespräch innerhalb eines definierten Zeitraums einen neuen Anrufversuch startet. Dieser zweite und jeder weitere Anruf mit dieser Anschlusskennung wird sofort durchgestellt. Dieses Verfahren beinhaltet natürlich das Risiko, dass es SPIT-Maschinen gibt, welche sich diesem Abwehrmechanismus anpassen können und gezielt darauf reagieren. [Han06]

6.7 Voice Menu Interaction

Ein Fachbegriff, welcher mit Voice Menu, welches näher unter [Tur07] erläutert wird, in Verbindung steht, ist CAPTCHA. [Tur07] Diese Abkürzung steht für Completely automated public Turing test to tell computers and humans apart. Bekannt ist diese Art von Tests aus dem Web-Bereich, wo man zur Bestätigung eine vorgegebene Zeichenfolge eingeben muss, die zum Beispiel in Abbildung 6.9 auf Seite 77 ersichtlich ist. Dies dient dazu, um eine automatisierte Verarbeitung dieses Prozesses zu verhindern.

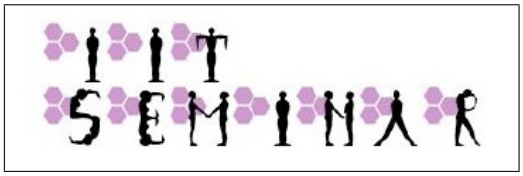


Abbildung 6.9: Visuelles CAPTCHA [Tur07]

Im Bereich von SPIT kommt eine auditive Version zum Einsatz. Beim ersten Kontakt wird der potentielle Anrufer auf einen Voice Menu-Server umgeleitet. Dort werden ähnlich der visuellen Variante auditive Tests durchgeführt, welche nur von Menschen erkannt werden können. Beispiele dafür könnten eventuell Rechenaufgaben oder ähnliche für Menschen sehr einfache Fragen sein. Abbildung 6.10 zeigt einen beispielhaften Aufbau für die Verwendung eines Voice Menu Servers. In einer SIP-Verbindung wird der Anrufer als User Agent Client (UAC) und der Angerufene als User Agent Server (UAS) bezeichnet: [Joh01]

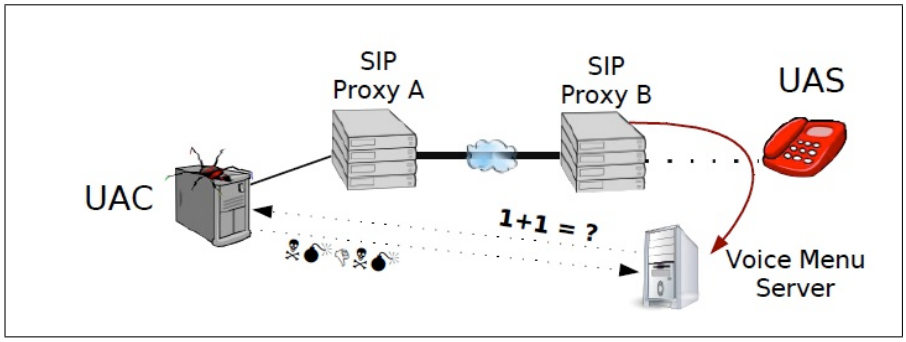


Abbildung 6.10: Einbindung eines Voice Menu Servers [Tur07]

Das Ziel von solchen CAPTCHAs ist es, dass man es dem SPIT-Verbreiter möglichst schwer macht, eine automatisierte Distribution seiner Nachrichten durchzuführen. Weites sollen dem SPIT-Verbreiter durch den Einsatz dieser Verfahren möglichst hohe indirekte Kosten entstehen. Allerdings hat dieses Verfahren auch einige Nachteile, welche in vier Punkten zusammengefasst sind.

- Problem 1: Störfaktor
  Probleme, welche dieses Verfahren mit sich bringt, sind, dass diese Umleitung und Befragung vor dem eigentlichen Telefonat für Anrufer sehr störend sind. Das bedeutet, dieses Verfahren sollte nur angewendet werden, wenn andere mögliche Verfahren nicht zum gewünschten Erfolg führen.

- Problem 2: Vielsprachigkeit
  Ein weiteres Problem ist die Vielsprachigkeit im Bereich der globalen Kommunikation von VoIP. Das hat zur Folge, dass der Voice Menu-Server viele Sprachen anbieten muss.

- Problem 3: Personen mit Beeinträchtigung
  Ein eventuelles Problem durch den Einsatz dieser Methode ergibt sich für die Verwendung von VoIP-Diensten für Personen mit körperlichen oder geistigen Beeinträchtigungen, welche diesen Filterprozess unter Umständen nur beschränkt überwinden können.

- Problem 4: Umgehungsmöglichkeit
  SPIT-Verbreiter können dieses Verfahren durch das Anwerben von billigst Arbeitskräften umgehen. Eine Bezahlung von 60 Cent/Stunde ist keine Seltenheit.

Somit zeigt sich, dass dieses Verfahren in der Praxis nur beschränkt einsetzbar ist. [Tur07]

6.8 User Behavior-Analysis

Die User Behavior-Analysis, welche näher unter [Bha09] erläutert wird, geht auf das Verhalten der Benutzer ein. Dieser Technik zugrunde liegt der Fakt, dass sich das Verhalten von SPIT-Verbreitern signifikant vom Verhalten herkömmlicher Benutzer unterscheidet. Dies kann man auf das Einkommengetriebene Verhalten der Voice-SPAMmer zurückführen. Im Gegensatz zu den meisten verwendeten Verfahren zur Abwehr von SPIT hat diese Methode den Vorteil, dass sie einfach, schnell und effektiv ist.

Das hierzu verwendete Schema um SPIT aufzufinden, nennt sich User-behavior-aware-anti-SPIT-technique. Diese Technik besteht aus einer Filterung bezogen auf das Benutzerverhalten, welches auf Routerebene vonstatten gehen kann und einem sogenannten Adaptive training data selection algorithmus.

Abbildung 6.11 auf Seite 79 zeigt eine SIP-Architektur. Es ist ersichtlich, dass alle VoIP-Geräte an einem Punkt, nämlich an den Routern, gebündelt und über das IP-Netzwerk übertragen werden. [Bha09]

Nachfolgend wird Schritt für Schritt erklärt, wie dieses Verfahren SPIT entgegenwirkt.

Ein erstes Ziel ist es, das Verhalten der Benutzer zu erfassen. Dafür muss eine Technik gefunden werden, in der man das Verhalten und die Interaktionen von Voice-SPAMmern und validen Benutzern studiert, analysiert und beobachtet.

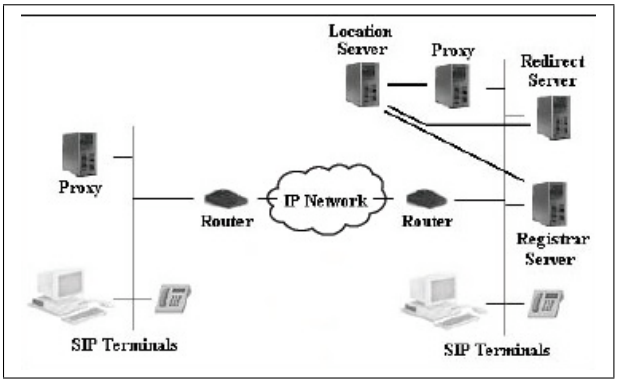


Abbildung 6.11: SIP Architektur [Bha09]

Dazu werden drei Methoden angewendet:

- Interaktionsverhalten (interaction behavior)
  Das Verhalten von Voice-SPAMmern und validen Benutzern unterscheidet sich schon dadurch, dass ein Anwender Anrufe tätigt und entgegennimmt. Bei Voice SPAMmern ist es sehr auffällig, dass diese sehr viele Anrufe tätigen, allerdings wenige bis keine Anrufe entgegennnehmen. Offensichtlich kann schon ein kleiner Anteil an eingehenden und ausgehenden Anrufstatistiken ausreichen, um einen Voice-SPAMmer von einem validen Anrufer abzugrenzen.

- historisches Verhalten (historical behavior)
  Ein anderer Ansatzpunkt zur Beobachtung ist die Analyse von historischem Verhalten. Legitime Benutzer von VoIP tätigen normalerweise Anrufe zu ihren gelisteten Kontakten und rufen für gewöhnlich eine Nummer öfter als einmal an. Im Gegensatz dazu ruft ein SPAMmer viele verschiedene Nummern an, wiederholte Anrufe werden meist vermieden.

- soziales Verhalten (social behavior)
  Ein legitimer Benutzer nimmt normalerweise Kontakt zu Teilnehmern aus seiner Buddylist auf. Im Gegensatz dazu nimmt ein SPAMmer Kontakt zu unzähligen Teilnehmern auf, welche nicht in seiner Buddylist aufgelistet sind. Das bedeutet, eine hohe Anzahl von Anrufen zu verschiedenen Benutzern und die Gesamtanzahl von Benutzern, welche keine Rückrufe getätigt haben, sind Indizien für einen potentiellen Voice-SPAMmer.

  [Bha09]

Der nächste Schritt nach den Beobachtungen des Verhaltens der Benutzer ist die Identifikation der SPIT-Verbreiter. Dazu werden bei der User-behavior-aware-anti-SPIT-technique drei Kennzahlen verwendet:

- Interaktionskennzahl (IR)
  Summe der beantworteten Anrufe/Summe der gewählten Anrufe
- historische Kennzahl (HR)
  Anzahl der wiedergewählten Kontakte/Anzahl der unterschiedlichen Anrufe
- soziale Kennzahl (SR)
  Anzahl der unbekannten angewählten Kontakte/gesamte Anzahl von angewählten Kontakten

[Bha09]

Zweiter angeführter Punkt bei dieser Methode ist der Selektionsalgorithmus. Die User-behavior-aware-anti-SPIT-technique unterscheidet die Qualifikation eines Anrufers abhängig von den Trainingsdaten S. Das bedeutet wiederum, dass zum Beispiel die Gesamtanzahl von Anrufen zuerst beobachtet und analysiert wurde, bevor der Filterprozess vonstatten geht. Durch eine zu ungenaue oder zu kurze Beobachtung und somit schlechte Analyse kann es zu einer Fehleinschätzung kommen, welche den Filterprozess verschlechtern würde. Das hätte zur Folge, dass entweder Kontakte geblockt werden, welche akzeptiert werden müssten und umgekehrt. Das Ziel muss es also sein, die sogenannten false positive (zu Unrecht blockierte Kontakte) zu minimieren und die sogenannten false negative (Kontakte, die nicht geblockt wurden, aber SPIT beinhalten) zu vermindern. [Bha09]

Um diese Ziele zu erreichen, benötigt man einen Algorithmus, der die Größe der Trainingsdaten anpassen kann. Dieser Algorithmus nennt sich Adaptive training data selection. Dieser Algorithmus schätzt die Anzahl der Trainingsdaten. Solche Schätzungen können iterativ wiederholt werden, um die gewünschten false positive und false negative Rate zu erreichen. Abbildung 6.12 zeigt den Ablauf des Algorithmus:

Wenn es nun der Fall ist, dass die false positive-Rate die Erwartung übersteigt, so hat das den Grund, dass die Größe der Trainingsdaten zu klein ist, um legitime Benutzer von SPAMmern genau zu unterscheiden. Um diesem Fall entgegenzuwirken, wird die Größe der Trainingsdaten exponentiell angehoben und nach jeder Erhöhung eine neue Messung der false positiv-Rate durchgeführt. Dies geht solange vonstatten, bis die gewünschte Rate der false positives erreicht beziehungsweise unterschritten wird.

Nach diesem Teilprozess wird die false negative Rate mit den Zielvorgaben verglichen. Die Größe der Trainingsdaten wird dann linear vermindert, falls

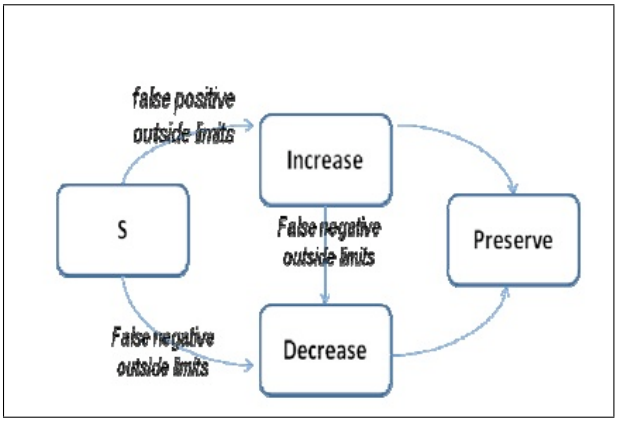


Abbildung 6.12: Ablauf des Selektionsalgorithmus [Bha09]

die aktuelle false negative Rate größer als die Zielvorgabe ist. Sollte sich an den Zielparametern der false positive-Rate etwas ändern, wird der vorherige Wert wiederhergestellt.

Die vorgestellte Methode wurde durch Testdaten mit zehn Prozent SPAM in einer Simulation bewertet. Die Performance Metriken waren [Bha09]

- false positive-rate
  Prozentsatz der validen Anrufe, welche fehlerhafterweise ausgeschlossen wurden
- false negative-rate
  Prozentsatz der SPAM-Anrufe, welche fehlerhafterweise akzeptiert wurden
- Exaktheit
  Beschreibt die Effektivität von korrekt klassifizierten validen Anrufen und SPAM-Anrufen. Die Exaktheit wird laut Abbildung 6.13 auf Seite 81 berechnet:

$$1/2 \times \left(\frac{korrekt\ klassifizierte\ valide\ Anrufe}{Gesamtanzahl\ valider\ Anrufe} + \frac{korrektklassifizierte\ SPAM\ Anrufe}{Gesamtanzahl\ SPAM\ Anrufe} \right)$$

Abbildung 6.13: Formel zur Berechnung der Effektivität [Bha09]

Abbildung 6.14 auf Seite 82 zeigt, dass am Anfang einer Testreihe erst wenige Daten bekannt sind und somit der SPIT-Schutz sehr gering ist. Nach einer gewissen Zeit steigert das System durch die automatische Anpassung die Effektivität und erreicht am Ende einen effektiven SPIT-Schutz von 96 Prozent.

Nachfolgende Abbildung 6.15 auf Seite 82 zeigt den Vergleich von Router-Level-Implementierung und User-Level-Implementierung. Es ist ersichtlich,

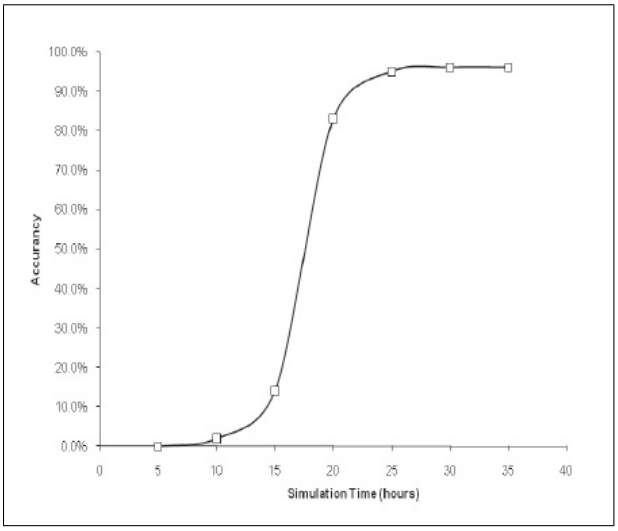


Abbildung 6.14: Maximale Effektivität [Bha09]

dass bei einer Anrufintensität von 30 Anrufen pro Stunde die Router-Level-Implementierung die maximale Effektivität in der halben Zeit im Vergleich zur User-Level-Implementierung erreicht.

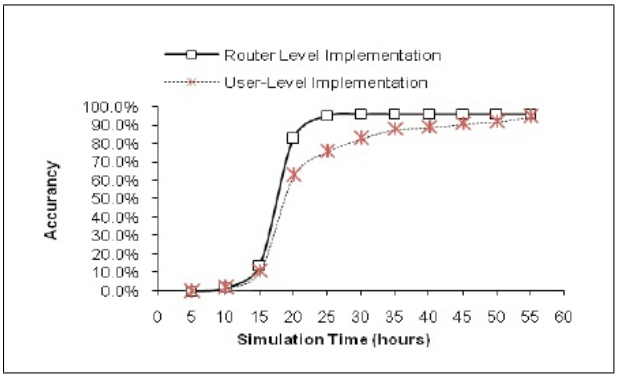


Abbildung 6.15: Router-Level-Implementierung vs. User-Level-Implementierung [Bha09]

Abbildung 6.16 auf Seite 83 zeigt, dass 80 Prozent der Anrufer bei einer Intensität von 45 Anrufen/Stunde innerhalb von zwölf Stunden klassifiziert werden können. Des Weiteren ist ersichtlich, dass bei einer Intensität von 60 Anrufen/Stunde eine Klassifikation in derselben Zeit möglich ist. Während bei einer Intensität von zehn beziehungsweise 30 Anrufern/Stunde eine maximale Klassifikation von zehn Prozent in derselben Zeit erreicht werden kann. Das bedeutet, wenn ein SPAMmer in kurzer Zeit sehr viele Sprachnachrichten versendet, reagiert diese Technik wesentlich effektiver und schneller als bei geringerer Intensität.

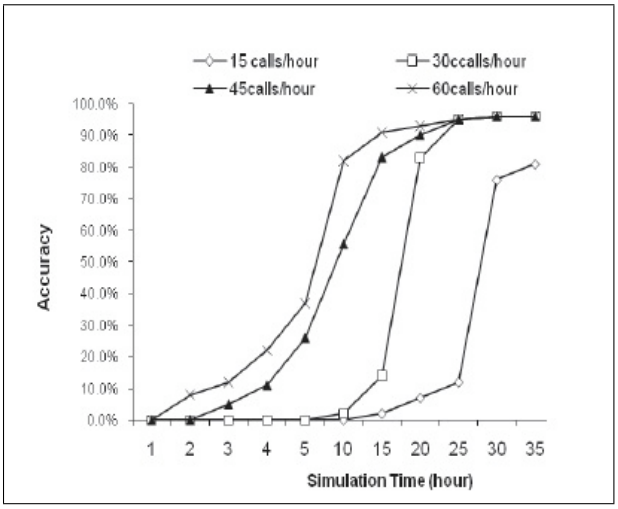


Abbildung 6.16: Variierende Anrufintensität [Bha09]

Somit zeigt sich, dass diese Technik ein sehr hohes Potential aufweist, um Systeme vor SPIT zu schützen.

6.9 Checking Human Communication Patterns

Der Methode Checking Human Communication Patterns zugrunde liegt der sehr innovative Lösungsansatz (nähere Informationen unter [Ewa07]), dass man SPIT-Anrufe durch den Vergleich von versteckten Turing Tests (siehe Kapitel 6 State 2 bzw. Abschnitt 6.9 Hidden Turing Tests) mit human communication patterns durchführt. [Ewa07]

Der Fokus dieser Methode liegt, wie schon erläutert, auf der Anwendung und dem Vergleich von Benutzerinteraktionen durch den Einsatz von Turing Tests. Man muss annehmen, dass SPAMmer in der Lage sind, falsche Signalnachrichten zu senden und somit non-intrusive Methoden zu überwinden. Somit erreicht man einen höheren Schutz durch die Anwendung von caller interaction Methoden.

Man versucht mittels des Turing Tests herauszufinden, ob der Anrufer ein Mensch ist oder ein Computer aus einem Botnet. Natürlich besteht auch die Möglichkeit, dass aktuelle Software mit der notwendigen Technik ausgerüstet ist, sodass eine Unterscheidung des Verhaltens von Maschine beziehungsweise Software und Mensch sehr schwierig ist. Dazu sind allerdings Aufwände wie KI, welche noch in der Entwicklungsphase stecken, notwendig, und man kann davon ausgehen, dass diese Aufwände den Wert, den ein SPIT-Verbreiter sich erwartet, übertreffen und somit nicht eingesetzt werden. [Ewa07]

Der klassische Turing Test besteht aus einer Ansammlung von verschiedenen Fragen, die beantwortet werden müssen, um den Test zu bestehen. Bezogen auf VoIP ruft das bei einem Anrufer Ärger hervor, da er nicht vor jedem Gespräch eine Menge von Fragen beantworten will. Somit muss man diese Art der Testung in den Hintergrund verlegen, man spricht von 'hidden Turing tests'. [Ewa07]

Für die aktuelle Methode wird eine Gruppe von Turing Tests verwendet, welche als Basis human communication patterns verwendet. Vorab muss geklärt werden, was ein human communication pattern eigentlich ist: [Ewa07]

Human Communication Pattern

Human communication patterns wurden sehr genau studiert und es konnten gewisse basis patterns abgeleitet werden. Die International Telecommunication Union (ITU-T) und Hammer et al. benutzen ein einfaches Kommunikationsmodell mit vier Zuständen: [Ewa07]

- M (mutual silence)
  beide Teilnehmenr sind still
- A, B
  einer der beiden Teilnehmer spricht
- D (double talk)
  beide Teilnehmer sprechen

Abbildung 6.17 auf Seite 85 zeigt die vier Zustände M, A, B, D, wie sie obenstehend beschrieben wurden[1]:

Es hat sich gezeigt, dass eine typische Kommunikation nicht sehr lange im Zustand D verweilt. Wieviel Zeit genau man bei einer Kommunikation im Zustand D bleibt, hängt sehr viel von der kulturellen Herkunft der beiden Teilnehmer ab. Im Durchschnitt hat die ITU [Ewa07] für die englische, italienische und japanische Kultur 6,59 Prozent der Zeit einer Kommunikation für den Zustand D mit einer durchschnittlichen Länge von 0,23 Sekunden errechnet. [Ewa07]

Das zeigt, dass der Zustand D sehr selten und wenn, dann sehr kurz, in einer Kommunikation auftritt.

Eine valide Kommunikation (start pattern) zwischen zwei Gesprächspartnern

[1] In der Originalquelle steht rechts unten State "B". Dies muss jedoch tatsächlich State "D" heißen, wie in Abbildung 6.17 geändert wurde.

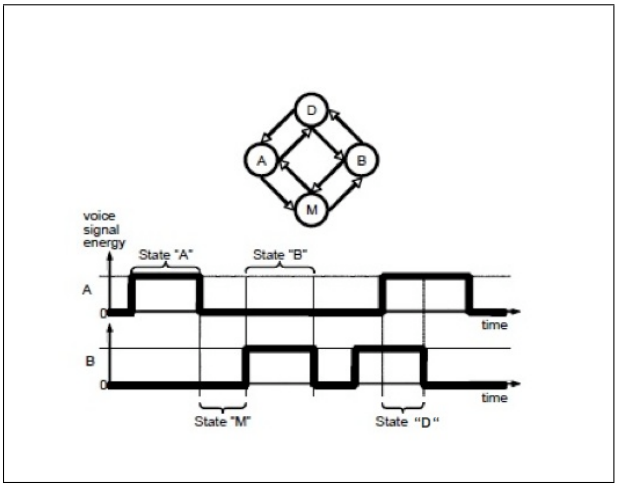


Abbildung 6.17: Vier Zustände von Communication Patterns, nach [Ewa07]

hat folgenden Ablauf, welcher in Abbildung 6.18 auf Seite 85 übersichtlich dargestellt wird:

Das Telefon läutet, der Teilnehmer hebt ab und grüßt beziehungsweise stellt sich vor. Im zweiten Schritt spricht der Anrufer und antwortet beziehungsweise stellt er sich vor. Zwischen diesen beiden Schritten erfolgt normalerweise keine Unterbrechung durch einen anderen Zustand. Zustand D in diesem Abschnitt einer Kommunikation ist untypisch. [Ewa07]

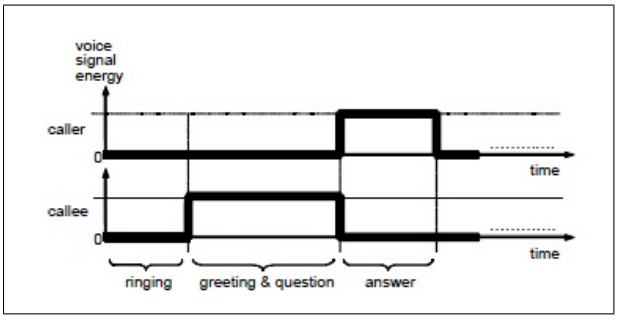


Abbildung 6.18: Start einer Kommunikation nach dem Start Pattern [Ewa07]

Nach Festlegung der Definition eines Turing Tests und der Bestimmung von communication patterns wird das Prinzip von Hidden Truning Tests näher erläutert.

Hidden Turing Tests

Die Grundidee von Hidden Turing Tests ist es, einen solchen Test durch-

zuführen, ohne dass die Teilnehmer etwas davon mitbekommen. Es werden also genau die eben dargestellten communication patterns im Hintergrund der Kommunikation überprüft und keine expliziten Fragen gestellt. Der zentrale Ansatz geht dahin, dass man die Kommunikation auf einen Bruch des Start Patterns untersucht. Somit unterteilt sich der Hidden Turing Test in zwei Schritte:

1. Silence Checking (verpflichtend):

   In dieser Testphase wird die Stimmenergie des Anrufers und die Einhaltung der vorgestellten communication patterns untersucht. Es wird vor allem auf den oben genannten Bruch des Start Patterns geachtet. Einige Ausnahmen, welche bei der Analyse der Call Patterns beachtet werden müssen, sind:

   - lauter Hintergrund des Anrufers
   - Übertragungsprobleme
   - kulturelle Unterschiede

   Unter Berücksichtigung dieser Einschränkungen kann die Umsetzung dieser ersten Phase durch den Einsatz einer automatischen Anrufannahmestelle erfolgen, welche zum Beispiel einen Begrüßungstext abspielt. Ein Trick, der auch angewendet werden kann, ist statt des Abspielens einer Begrüßung wiederum ein eingehendes Anrufsignal zurückzugeben. Ein menschlicher Teilnehmer würde dies erkennen und sein Sprachmuster anpassen, ganz im Gegensatz zu einem maschinellen Teilnehmer, der ungeachtet der Reaktion des Benutzers seine Aktionen fortführen würde.

   [Ewa07]

2. Answer Length Checking (optional)

   Dieser optionale zweite Schritt wird dann eingesetzt, wenn silence checking kein klares Ergebnis gebracht hat. Hier wird der communication pattern nach der Begrüßung untersucht. Umgesetzt kann dieser Test werden, indem wiederum eine Anrufannahmestelle zum Einsatz kommt, welche nach dem Begrüßungstext eine Frage stellt, welche vom Anrufer nach einer kurzen Pause umgehend und kurz beantwortet werden kann. Dies kann zum Beispiel die Frage nach dem Namen des Anrufers sein, bekommt man darauf eine sehr lange Antwort, kann mit hoher Wahrscheinlichkeit davon ausgegangen werden, dass eine SPIT-Nachricht eingeht, welche geblockt wird.

   [Ewa07]

6.10 SPIT-AL

SPIT-AL steht für SPIT-Abwehrlösung (nähere Informationen unter [Waa06]). SPIT-AL ist ein deutsches Projekt mit den Projektpartnern TNG – The Net Generation AG in Kiel (Internet- und Telekommunikationsprovider) und dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (durch das ULD-i) [Uld06] und wurde ursprünglich als Diplomarbeit an der Technischen Universität Dresden geschrieben. SPIT-AL ist eine Kombination aus mehreren Abwehrlösungen. Nachfolgend werden die Leistungsmerkmale, die Gesamtarchitektur und die Einsatzbereiche beschrieben:

Grundprinzip des SPIT-AL-Konzeptes ist es, dass dieses System die Anrufe stellvertretend für den Benutzer entgegennimmt. Der entgegengenommene Anruf wird aufgrund seiner Metadaten, welche aus

- Identität des Anrufers
- Herkunft des Anrufers
- eventuellem Zeitpunkt des Anrufs

bestehen und den Präferenzen (Kriterien) des Angerufenen bewertet. Da es das Ziel ist, eine Bewertung vor der eigentlichen Störung, das bedeutet vor Eingehen des Anrufes beim Angerufenen, zu erhalten, wird auf einen inhaltliche Überprüfung des Gespräches verzichtet. Aufgrund dieser Bewertung entscheidet das System, wie es mit dem Anruf weiter umgeht.

Von der Systemarchitektur her ist SPIT-AL so ausgelegt, dass diese perfekt in eine bestehende Telekommunikationsinfrastruktur integriert werden kann. Die Anbindung an ein herkömmliches PSTN- beziehungsweise ISDN-Netz oder an einen VoIP-Anbieter geschieht mit externen Komponenten, welche von der SPIT-AL unabhängig sind. Somit ist der Betreiber der jeweiligen Telefonanlage dafür verantwortlich, dass jeder Teilnehmer, der seine Gespräche durch diese Abwehrlösung filtern will, auch daran teilnehmen kann. Wenn man weitere Funktionen wie zum Beispiel statistische Filterungen miteinbeziehen will, sind engere Verbindungen mit der Infrastruktur des Betreibers notwendig. Als Basis für die SPIT-AL dient eine Telefonanlage wie Asterisk. [Waa06]

Die SPIT-AL gliedert sich in mehrere Untersysteme (siehe Abbildung 6.19 auf Seite 88):

- Application-Softswitch
  Dieses Subsystem übernimmt die Aufgabe, dass es gezielt die abgestuften Maßnahmen je nach Teilnehmer umsetzt. Als Hilfskomponente

verwendet der Application-Softswitch Dienste eines Voice-Servers. Die Entscheidung, wie das Routing erfolgt, wird von einem Management-Server getroffen.

- Voice-Server
  Die Aufgabe des Voice-Servers ist es, den Application-Softwarswitch durch Funktionen wie Sprachmenüs oder benutzerdefinierte, beziehungsweise vorinstallierte Ansagen, Sprachboxen und dergleichen zu unterstützen.

- Webinterface
  Dient zur Wartung und Einstellung von SPIT-AL

- Management-Server
  Die Aufgabe des Management-Servers ist es, die Routing-Aufgaben des Application-Softswitch zu steuern. Hierzu nimmt er die empfangenen Metadaten von diesem entgegen und liefert die Steuerinformation als Antwort zurück. Des Weiteren erfolgt die Individualisierung der Einstellungen auf diesem Subsystem.

- Datenspeicher
  Daten, welche der Management-Sever abspeichert, werden im Datenspeicher abgelegt.

[Waa06]

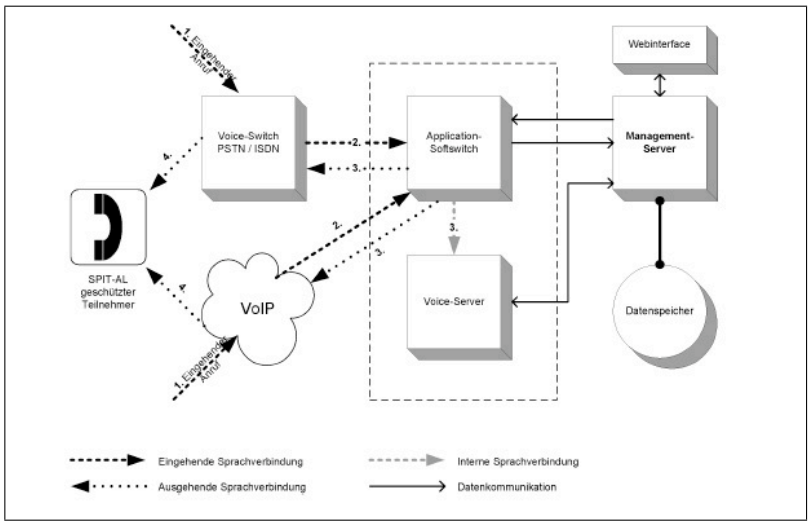


Abbildung 6.19: Zusammenwirkung des SPIT-AL-Systems [Waa06]

Das Management-System errechnet aus den Metadaten, welche oben dargestellt wurden, eine Punktzahl, die von den benutzerdefinierten Einstellungen abhängig ist. [Waa06]

Wie schon erläutert, bewertet SPIT-AL anhand von Kriterien die eingehenden Anrufe. Diese dienen dazu, einen Anruf einstufen zu können und eine Bewertung bezüglich der Wahrscheinlichkeit im Bezug auf SPIT abgeben zu können. Die Bewertung hat eine Punktezahl als Resultat und wird dem aus dem Management-System errechneten Bereich zugewiesen. Jedes Kriterium errechnet eine eigene Punktezahl, welche am Ende unter gewissen Operationen (Addition, Gewichtung, usw.) zu einer Gesamtpunktezahl gerechnet wird. Einige dieser Kriterien werden im Folgenden etwas näher betrachtet: [Waa06]

- Herkunft des Anrufers
  Ein Anruf kann von den verschiedensten Quellen ausgehen. Je nach Quelle ist die Wahrscheinlichkeit eines Voice-SPAMmers unterschiedlich hoch. Mögliche Quellen sind:

  - Telefonnetz (PSTN)
    Hier kann davon ausgegangen werden, dass es sich nicht um SPIT-Nachrichten handelt, da dies ein zu großer Aufwand wäre.
  - große VoIP-Anbieter
    Hier kann ebenfalls davon ausgegangen werden, dass Anrufer, welche einen Großanbieter als Quelle besitzen, einer gewissen Reglementierung, wie zum Beispiel den AGBs, die zum Beispiel das Versenden von SPIT verbieten, unterliegen.
  - private Anschlüsse/Einwahlanschlüsse
    Hier besteht die größte Gefahr, dass der Anrufer eine SPIT-Nachricht versendet.

- private Whitelist
  Eine private Whitelist wird auch in jeder SPIT-AL geführt und gepflegt. Was eine Whitelist ist und wie diese verwendet wird, wird im Abschnitt 6.3 - Whitelists beschrieben.

- Importierte Whitelists
  Jeder Benutzer kann bei der SPIT-AL festlegen, ob er seine eigenen Whitelists publizieren will und somit anderen Benutzern die Möglichkeit gibt, diese zu importieren, beziehungsweise hat jeder Benutzer selbst die Möglichkeit, eine öffentliche Whitelist zu importieren.

  Eine genaue Beschreibung dieser Whitelists erfolgt im Abschnitt 6.3 - Whitelists.

- private Blacklists
  So wie jeder Benutzer in seiner SPIT-AL Whitelists pflegt, geschieht dies auch mit Blacklists.

Eine genaue Beschreibung von Blacklists erfolgt im Abschnitt 6.4 - Blacklists.

- statistische Blacklists
  Die SPIT-AL kann aus allen bisher getätigten Anrufen Statistiken erstellen und bewerten.

  Eine genaue Beschreibung von statistischen Blacklists erfolgt im Abschnitt 6.5 - Statistische Blacklists.

Die aus den Metadaten errechneten Punkte werden zu den errechneten Punkten der Kriterien durch den Management-Server zu einer Gesamtsumme addiert. Nach Errechnung dieser Punktezahl wird in den Benutzereinstellungen nachgeschaut, welche Maßnahme der Benutzer für den Bereich, in dem sich die Punktezahl befindet, angibt. Per default sind die Maßnahmen

- Akzeptieren
  Anrufe, welche nach dieser Maßnahme behandelt werden, werden zum Benutzer geleitet. Somit kommt ein Gespräch ohne Verzögerung zustande. Diese Maßnahme greift zum Beispiel bei Aufscheinen auf einer Whitelist.

- Ablehnen
  Dem Anrufer wird ein Besetzt-Zeichen signalisiert, sodass er den gewünschte Teilnehmer nicht erreichen kann. Dieser Fall tritt zum Beispiel ein, wenn der Anrufer auf einer Blacklist aufscheint.

- Weiterleiten
  Es erfolgt eine Weiterleitung zu einem vorher bestimmten dritten Anschluss. Der dritte Anschluss kann weitere Maßnahmen beinhalten oder auch auf einer Anrufbox enden.

[Waa06]

Weitere Maßnahmen, welche standardmäßig nicht installiert sind, jedoch als Erweiterung hinzugefügt werden können, sind:

- Greylisting
  Eine temporäre Ablehnung erfolgt, wie sie im Abschnitt 6.6 - Greylisting beschrieben wird.

- Alternativer Kontakt
  Der Anrufer wird zum Voice-Server weitergeleitet, welcher eine Sprachnachricht abspielt, auf der dem Anrufer erklärt wird, wie er mit dem Benutzer in Kontakt treten kann.

- Voice-Menu
  Der Anrufer kommt zu einem Voice-Menu, welches im Abschnitt 6.7 - Voice-Menu-Interaction beschrieben wird.

- Voicebox
  Der Anrufer wird sofort zu einer Voicebox, die sich auf dem Voice-Server befindet, weitergeleitet, wo er dann eine Sprachnachricht hinterlassen kann.

[Waa06]

SPIT-AL bietet weitere Möglichkeiten, wie zum Beispiel die Aufnahme von Gesprächspartnern in deren Black- und Whitelists während des Gesprächs. Des Weiteren werden die Metadaten aller bisherigen eingegangenen Gespräche aufgezeichnet und vorab bewertet. Der Benutzer kann diese dann selbstständig im Webinterface weiterverarbeiten. SPIT-AL führt beim Eingang eines Anrufers, der ebenfalls die SPIT-AL-Lösung verwendet, eine sofortige Aufnahme in die Whitelist durch. Diese und weitere Möglichkeiten sollen dem Benutzer die Verwendung des Lösungskonzeptes vereinfachen. [Waa06] [Uld06]

SPIT-AL hat zwei Nachteile:

1. Unterdrückung der Identität
   Im Bereich der Telefonie gibt es die Möglichkeit, einen Anruf auf inkognito zu setzen. Das bedeutet, der zu erreichende Partner kann nicht feststellen, wer diesen Anruf tätigt. Dies vermindert die Effektivität der Bewertungskriterien Blacklists und Whitelists.

2. Verifikation der Identität
   Eine Identifikation des Absenders ist im Bereich VoIP zur Zeit noch nicht standardisiert und somit ist es sehr einfach, einen gefälschten Absender anzugeben. Dies hat wiederum auf die Effektivität der Bewertungskriterien von Blacklists und Whitelists Auswirkungen.

[Waa06] [Uld06]

Kapitel 7

Evaluierung von SPIT-Abwehr-Methoden

Im Kapitel Evaluierung von SPIT-Abwehr-Methoden werden zunächst die einzelnen Bewertungskriterien näher vorgestellt und beschrieben. Im darauffolgenden Teilbereich werden die einzelnen Methoden aus dem Kapitel Methoden zur Abwehr von SPIT im Bezug auf diese Kriterien untersucht.

7.1 Bewertungskriterien im Bezug auf SPIT

In diesem Teilbereich wurden im Zuge einer Diskussion an der TU Wien, mit der Forschungsgruppe für Industrial Software (INSO), zwölf Bewertungskriterien erarbeitet, welche dazu dienen, Methoden zur Abwehr von SPIT zu bewerten. Die Kategorie der Methoden sind grundlegend verschieden und gehen vom Zeitpunkt der Erkennung über den Installationsort bis hin zum technischen Reifegrad. Im Vordergrund der Kriterien liegt die Effektivität und nicht die Effizienz der einzelnen Methoden.

Die einzelnen Kriterien weisen verschiedene Prioritäten auf, welche im Zuge der Diskussionsrunde beziehungsweise durch Betrachtung von allgemeinen Informationen aus Wirtschaft und der Informatik, hergeleitet wurden. Die Wichtigkeit der einzelnen Kriterien wird in drei Stufen unterteilt, welche sich in einem Bereich von:

1. Wenig (maximal 4 Punkte)
2. Mittel (maximal 6 Punkte)
3. Hoch (maximal 10 Punkte)

bewegen. Der Bereich 0 - 10 Punkte wurde gewählt, da dieser Wertebereich zusätzlich eine feinere Untergliederung der einzelnen Stufen erlaubt. Des weiteren wird gezeigt, dass der Unterschied zwischen einem Kriterium mit einer

niedrigen Wichtigkeit und einem Kriterium mit mittlerer Wichtigkeit geringer ist, als der Unterschied zwischen einem wichtigen Kriterium und einem Kriterium mit hoher Wichtigkeit.

Einige der Merkmale weisen keine Priorisierung auf, da diese nur zum informativen Zwecke, nicht aber für die Bewertung dargestellt werden. Das ist deshalb der Fall, da einige dieser Punkte keine direkte Auswirkung auf die Effektivität der Methoden aufweisen, aber es von Seiten der Evaluierung von Interesse ist, diese Informationen darzustellen. Dargestellt werden diese Zusatzinformationen am Ende des Kapitel 7 in einer zusammenfassenden Tabelle. Durch die Vielseitigkeit der möglichen Evaluationsbereiche, ist es nicht möglich, alle Punkte zu erfassen und die gewählten Punkte stellen nur einen Überblick dar. Zum einen resultiert dies aus dem Umfang der möglichen Bereiche und zum anderen ist es teilweise nicht möglich Kriterien, wie zum Beispiel den Kostenfaktor einer Methode, zu erheben, da viele Methoden noch in der Entwicklungsphase sind und eine Kostenerhebung oftmals nicht möglich, beziehungsweise zu dieser Zeit der Entwicklung nicht seriös ist.

Je nach Priorität kann eine Methode für ein Kriterium, abhängig vom Grad der Erfüllung bzw. dem Zutreffen des Unterscheidungsmerkmales des Kriteriums der Methode, eine maximale Punktzahl erreichen. Ausgeschlossen davon, sind Kriterien, welche informativ und völlig wertfrei erhoben werden.

Da jedes Kriterium verschiedene Unterscheidungs- und Bewertungsmerkmale aufweist, wird eine individuelle Unterteilung und Bewertung pro Kriterium erstellt. Die Auswahl der Punkte für die interne Unterteilung entspricht einer Verteilung über den Gültigkeitsbereich des Kriteriums und wird durch allgemeine Informationen aus Wirtschaft und Technik gewichtet.

Um eine spätere Wertung der einzelnen Methoden zu ermöglichen, wird in der Evaluierung pro Methode eine Gesamtpunktezahl ermittelt, welche eine spätere Gesamtreihung der Methode ermöglicht.

7.1.1 Zeitpunkt der Erkennung

Der Zeitpunkt der Erkennung stellt jenes Kriterium dar, welches zeigt, ob ein Voice-SPAMmer

- vor einem Telefonat
- während eines Telefonates
- nach dem Telefonat

erkannt werden kann.

Dieses Kriterium hat vor allem Auswirkungen auf den Komfort der Methode. Methoden, welche eine Erkennung ohne eine Belästigung im Vorfeld erkennen, bringen einen Anstieg des Komforts, wobei hingegen Methoden, welche erst nach einer möglichen Belästigung aktiv werden, eine Verringerung des Komforts bringen. Da aber auch Methoden die nach und während eines Telefonats eine Erkennung liefern funktionieren, wird die Priorität dieser Methoden als Mittel eingestuft.

Priorität: Mittel (maximal 6 Punkte)

Bewertung:

- Vor einem Telefonat (6 Punkte)
- Während eines Telefonates (3 Punkte)
- Nach dem Telefonat (1 Punkt)

7.1.2 Technischer Reifegrad

Die Reife eines Produktes oder eines Konzepts ist von maßgeblicher Bedeutung. Ist ein Produkt im Zustand eines Konzeptes, so ist eine Umsetzung noch nicht erfolgt, und die Methode hat noch keine Relevanz für die Praxis. Die Relevanz einer Abwehrmethode steigt nach einer ersten Umsetzung in der Forschungsphase und findet ihren Höhepunkt, wenn sich die Methode zu einer Technik entwickelt hat, welche Marktreife besitzt. Der technische Reifegrad wird in folgende vier Abstufungen unterteilt:

- Konzept
- Forschung
- Testversionen
- Marktreife

Viele der vorgestellten Methoden befinden sich noch in der Konzept- bzw. Forschungsphase und werden erst in naher Zukunft zu Testversionen bzw. Marktreife übergeleitet werden. Um eine Unterteilung zu finden, welche die Wichtigkeit des Kriteriums, bezogen auf die Methode abbildet, wurden Methoden, welche noch in der Konzept bzw. Forschungsphase waren, mit einer niedrigen Punktezahl abgebildet und Methoden die zum Teil im Einsatz sind mit einer höheren Punktezahl abgebildet. Die Vergabe der Punkte resultiert daraus, dass auch Methoden, welche zum heutigen Zeitpunkt in einer nicht ausgereiften Phase befinden, geforderte Funktionalitäten zum Schutz vor SPIT erfüllen.

Priorität: Hoch (maximal 10 Punkte)

Bewertung: Der technische Reifegrad wird in folgende vier Abstufungen unterteilt:

- Konzept (2 Punkte)
- Forschung (4 Punkte)
- Testversionen (8 Punkte)
- Marktreife (10 Punkte)

7.1.3 Komplexität vs. Effektivität

Dieses Merkmal beschreibt den Zusammenhang zwischen Kostenabschätzung, Nutzen, Verwendung und Aufwand. Das bedeutet, mit dieser Kennzahl ermittelt man eine Kompromissmethode. Das Verhältnis von Komplexität und Effektivität wird durch die Abstufung in:

- Niedrig
- Mittel
- Hoch

dargestellt. Im Idealfall bietet einen Methode hohen Nutzen kombiniert mit breiter Verwendungsmöglichkeit und einem geringen Aufwand. Die Priorität der Methode ist im Bereich Mittel, da die Ansprüche vor dem Einsatz einer Methode sehr unterschiedlich sein können und man somit nicht immer eine Kompromissmethode zum Einsatz bringen kann. Die Unterteilung der Punkte in Niedrig 1 Mittel 3 und Hoch 6 ergibt sich daraus, dass man, wenn man die Anforderungen außer acht lässt und die Methoden nur nach dem Verhältnis Komplexität zu Effektivität beurteilt, eine Methode mit hoher Effektivität und niedriger Komplexität einer Methode mit niedriger Effektivität und hoher Komplexität vorzieht und somit besser bewertet.

Priorität: Mittel (maximal 6 Punkte)

Bewertung:

- Niedrig (1 Punkt)
- Mittel (3 Punkte)
- Hoch (6 Punkte)

7.1.4 Benutzerkreis

Das Bewertungsmerkmal Benutzerkreis beschreibt im eigentlichen zwei verschiedene Möglichkeiten. Zum einen, einen abgeschlossenen Benutzerkreis, welcher darauf abzielt, dass diese Art von Benutzer zum Beispiel aus dem selben Sprachraum kommen oder aus einer bestimmten Gruppe (Personen mit Behinderungen, alte Personen) stammen bzw. überhaupt benutzerspezifisch definierten Gruppen unterliegen. Zum anderen gibt es universelle Lösungen, welche keine Einschränkungen mit sich bringen. Somit unterteilt sich dieses Kriterium in

- abgeschlossen
- offen

Die Bewertung in diesem Bereich ergibt eine höhere Wertung für offene Lösungen, da diese universeller eingesetzt werden können und weniger Hindernissen ausgesetzt sind.

Priorität: Niedrig (maximal 4 Punkte)

Bewertung:

- abgeschlossen (2 Punkte)
- offen (4 Punkte)

7.1.5 Komfortabilität

Die Komfortabilität einer Methode beziehungsweise der Komfort der Anwendung einer Methode spielen eine maßgebliche Rolle für die Verwendung. Einfache, logische Methoden ohne großen administrativen Aufwand (Wartung, Installation, etc.) werden bevorzugt bewertet. Eine Unterteilung des Komforts in die Unterstufen

- Gering
- Mittel
- Hoch

wird durch das Betrachten des Funktionsablaufes der einzelnen Methoden erreicht. Aus dieser Betrachtung ergibt sich, dass Methoden, welche einen geringen Komfort haben, eine niedrige Priorität erhalten und Methoden, welche einen hohen Komfort besitzen, eine hohe Priorität erhalten, weil die Motivation eines Einsatzes solcher Abwehrlösungen höher ist, je leichter und einfacher die Bedienung und Wartung einer solchen Lösung ist.

Priorität: Hoch (maximal 10 Punkte)

Bewertung:

- Gering (2 Punkte)
- Mittel (5 Punkte)
- Hoch (10 Punkte)

7.1.6 Effektivität

Die Effektivität der Methoden wird durch zwei Punkte definiert. Zum Ersten das Verhältnis von false positives zu false negatives und dessen Entwicklung und zum Zweiten durch die Möglichkeiten zur Umgehung dieser Methode. Die Bewertung dafür untergliedert sich in:

- Gering (viele false positives, viele false negatives, umgehbar)
- Mittel (false positives-, false negatives-Rate verbessert sich, schwer umgehbar)
- Hoch (Keine false positives, keine false negatives, nicht umgehbar)

Mit Hilfe dieser drei Punkte soll ein grober Überblick über die Effektivität einer Methode gegeben werden.

Priorität: Hoch (maximal 10 Punkte)

Bewertung:

- Gering (2 Punkte)
- Mittel (5 Punkte)
- Hoch (10 Punkte)

7.1.7 Individualisierung

Der Punkt Individualisierung oder auch Customization genannt, beschreibt, ob diese Methode die Möglichkeit bietet, individuelle Anpassungen des Verhaltens vorzunehmen.

Priorität: Niedrig (maximal 4 Punkte)

Bewertung:

- Ja (4 Punkte)
- Nein (0 Punkte)

7.1.8 Anwendungsbereich

Der Anwendungsbereich von Abwehrlösungen unterscheidet sich grundsätzlich in zwei Bereiche:

1. Privat
2. Business

Unterschieden werden diese beiden Bereiche deshalb, da die Wichtigkeit bzw. die Ausfallsicherheit im Businessbereich wesentlich höher ist, als im privaten Bereich. Des weiteren hat man im Durchschnitt im Bussinesbereich mit einer deutlich höheren Datenmenge zu rechnen. Zusammenfassend gesagt, im Businessbereich wird eine professionelle Lösung, welche über Supportmöglichkeit verfügt verlangt, wobei im privaten Bereich oftmals Semi-professionelle Anwendungen zum Einsatz kommen können. Da dieses Kriterium allerdings nur von informativer Bedeutung ist, werden keine Punkte vergeben. Abgebildet wird dieses Kriterium am Ende des Kapitel 7 in der zusammenfassenden Tabelle mittels einer eigenen Spalte Anwendungsbereich.

Bewertung:

- Privat geeignet
- Business geeignet

7.1.9 Aufnahmemechanismen

Eine interessante Unterscheidung ist die Art der Aufnahme bzw. die Detektion eines Voice-SPAMmers. Die Möglichkeiten gehen von manueller Detektion bis hin zu automatischer Detektion. Bei dieser Betrachtung steht die Effektivität und nicht die Effizienz einer Methode im Vordergrund. Unterscheiden kann man durch eine grobe Kategorisierung folgende Punkte:

- Keine Aufnahme
  Der Benutzer wird in keine persistente Liste aufgenommen und muss jedes Mal neu analysiert werden.
- Manuell
  Der Benutzer muss den Voice-SPAMmer manuell vermerken.
- Automatisch bei Aufkommen
  Der Voice-SPAMmer wird automatisch beim ersten Auftreten vermerkt.
- Lernphase
  Das System braucht eine gewisse Zeit um Voice-SPAMmer zu erkennen, dies funktioniert jedoch voll automatisch.

- Analysephase
  Vor dem ersten Aufkommen werden bestimmte Daten analysiert und der Voice-SPAMmer vermerkt.

Da diese Varianten von Aufnahmemechanismen weder Vor- noch Nachteile mit sich bringen, werden diese wertfrei behandelt und es erfolgt keine Priorisierung bzw. Bewertung.

7.1.10 Barrierefreiheit

Methoden zur Abwehr von SPIT müssen so konstruiert werden, dass auch eingeschränkte Personen weiter mit diesem System arbeiten können. Vor allem in öffentlichen Institutionen, welche durch das W3C (`www.w3.org`) Vorgaben und Richtlinien für eine behindertengerechte Verwendung beachten und einhalten müssen, kommt dieses Kriterium zum tragen. Die Unterteilung erfolgt in:

- Ja
- Nein

Da die Priorität für manche Anwendungsfälle in denen Barrierefreiheit von Bedeutung ist anders aussieht, als in Fällen, wo Barrierefreiheit keinen hohen Stellenwert besitzt, wird dieses Kriterium als wertfrei eingestuft und in der zusammenfassenden Tabelle am Ende des Kapitel 7 aufgezeigt.

7.1.11 Nachhaltigkeit

Der Begriff Nachhaltigkeit beschreibt, ob ein Anrufer durch die Filterung einer Methode als Voice-SPAMmer identifiziert wird und den Status Voice-SPAMmer auf Dauer behält, oder ob dem Benutzer die Möglichkeit gegeben wird, durch sein Verhalten bzw. gewisse Aktivitäten, seinen Status zu ändern. Unterschieden wird somit in:

- dauerhaft
- befristet

Da diese Unterteilung wertfrei ist, wird keine Priorität und Bewertung dafür abgegeben.

7.1.12 Installationsort

Der Installationsort einer Lösung kann theoretisch auf drei Positionen im System erfolgen:

1. Empfängerseitig

2. Senderseitig
3. Zentraler Punkt (Router)

Die Praxis zeigt, dass eine Installation auf der Sender-Seite nicht zum Einsatz kommt. Das hat den Grund, dass ein potentieller SPIT-Verbreiter durch den Einsatz einer Abwehrlösung seine eigenen Ziele zunichte machen würde. Somit kommt in der Praxis eine Zentrale- oder Empfängerseitige Lösung zum Einsatz.

Da diese Unterteilung wertfrei ist, wird keine Priorität und Bewertung dafür abgegeben.

7.2 Evaluierung und Auswertung aktueller Methoden zur Abwehr von SPIT

Im Abschnitt Evaluierung und Auswertung aktueller Methoden zur Abwehr von SPIT werden die Methoden aus dem Kapitel 6 Methoden zur Abwehr von SPIT herangezogen und mit den Kriterien aus dem Abschnitt 7.1 Bewertungskriterien im Bezug auf SPIT bewertet und evaluiert.

7.2.1 Cost for Telephony

Die Cost for Telephony Methode (Abschnitt 6.2) ist derzeit in der Konzeptphase. Die Frage der Erkennung kann man so nicht beantworten, da ein potentieller Voice SPAMmer im Normalfall darauf verzichten wird, den Pfand für das Gespräch zu bezahlen, da sonst der Vorteil der günstigen Werbung verloren geht. Der Kostenfaktor dieses Konzeptes ist sehr hoch, da für eine Realisierung eine komplette eigene Infrastruktur zur Transaktionsübertragung errichtet werden müsste. Diese Infrastruktur müsste an alle Länder und Währungen in der richtigen Höhe angepasst sein. Des weiteren fallen pro Transaktion Gebühren in der Höhe von zirka 15 Prozent an, welche wiederum die Vorteile einer günstigen Kommunikation schmälern würden. Cost for Telephony wäre eine sehr wirksame Methode um Voice SPAM zu verhindern, bringt allerdings sehr viele Nachteile mit sich. Durch das Erreichen von 27 Punkten von möglichen 60 Punkten erreicht die Methode rund 45 Prozent der möglichen Gesamtpunkte.

Kriterien	**Anmerkung**	**Priorität (max. Punkte)**	**Punkte**
Zeitpunkt der Erkennung	Vor dem Anruf	Mittel (max. 6 Punkte)	6 Punkte
Technischer Reifegrad	Konzept	Hoch (max. 10 Punkte)	4 Punkte
Komplexität vs. Effektivität	Effektiv, aber sehr komplexe Implementierung	Mittel (max. 6 Punkte)	3 Punkte
Benutzerkreis	Offener Benutzerkreis	Niedrig (max. 4 Punkte)	4 Punkte
Komfortabilität	Mittel, durch Transaktionsverwaltung	Hoch (max. 10 Punkte)	5 Punkte
Effektivität	Nur durch hohe Kosten umgehbar	Hoch (max. 10 Punkte)	5 Punkte
Individualisierung	Nein	Niedrig (max. 4 Punkte)	0 Punkte
Gesamt		**60 Punkte**	**27 Punkte**

Tabelle 7.1: Bewertung Cost for Telephony

7.2.2 Whitelists

Whitelists (Abschnitt 6.3) sind eine bekannte und derzeit schon eingesetzte Methode zur Abwehr von SPIT. Des weiteren haben sich Whitelists auch früher schon im Bereich von SPAM etabliert. Eine Erkennung vor einem störenden Anruf ist möglich, jedoch ist es nicht möglich, mit unbekannten Anrufern eine Verbindung aufzunehmen. Diese Art der Filterung weist eine niedrige Komplexität auf und wirkt trotzdem sehr effektiv. Von den Kosten her werden solche Systeme oftmals gratis angeboten bzw. sind diese in vielen VoIP Systemen bereits integriert. Die Aufnahme in diese Whitelist erfolgt entweder manuell oder auch über automatisierte Systeme, welche nach bestimmten Kriterien entscheiden, ob ein Kontakt aufgenommen wird oder nicht. Durch das Erreichen von 43 Punkten von möglichen 60 Punkten erreicht die Methode rund 72 Prozent der Gesamtpunktezahl.

Kriterien	**Anmerkung**	**Priorität (max. Punkte)**	**Punkte**
Zeitpunkt der Erkennung	Vor dem Anruf	Mittel (max. 6 Punkte)	6 Punkte
Technischer Reifegrad	Bereits in Verwendung	Hoch (max. 10 Punkte)	10 Punkte
Komplexität vs. Effektivität	Einfaches, effektives System	Mittel (max. 6 Punkte)	6 Punkte
Benutzerkreis	Definierte Gruppen	Niedrig (max. 4 Punkte)	2 Punkte
Komfortabilität	Einfache Bedienung	Hoch (max. 10 Punkte)	10 Punkte
Effektivität	Keine false negatives, aber evtl. false positives	Hoch (max. 10 Punkte)	5 Punkte
Individualisierung	Ja	Niedrig (max. 4 Punkte)	4 Punkte
Gesamt		**60 Punkte**	**43 Punkte**

Tabelle 7.2: Bewertung Whitelists

7.2.3 Blacklists

Blacklists (Abschnitt 6.4) sind eine etablierte Art der SPAM und SPIT Filterung. Diese Art der Methoden basiert auf einer einfachen Technik der Filterung welche wenig kostenintensiv ist und oftmals schon bei fertigen VoIP-Lösungen mit angeboten wird. Durch die Verwendung von Blacklists bleibt der Benutzerkreis offen, Nachteile welche sich ergeben sind, dass sich neue, noch nicht bekannte Kontakte erst nach der Kontaktaufnahme als SPAM herausstellen können. Das bedeutet die Effektivität dieser Methode im Vergleich zu Whitelists ist geringer, jedoch wird der gravierende Nachteil, dass nur Anrufe von bekannten Anrufern empfangen werden können, behoben. Blacklists werden im Bereich SPAM und SPIT schon seit längerer Zeit eingesetzt. Durch das erreichen von 42 Punkten von möglichen 60 Punkten erreicht diese Methode 70 Prozent der Gesamtpunktezahl.

Kriterien	**Anmerkung**	**Priorität (max. Punkte)**	**Punkte**
Zeitpunkt der Erkennung	Vor dem Anruf	Mittel (max. 6 Punkte)	6 Punkte
Technischer Reifegrad	Marktreife (in Verwendung)	Hoch (max. 10 Punkte)	10 Punkte
Komplexität vs. Effektivität	Filtert nur Kontakte der Liste	Mittel (max. 6 Punkte)	3 Punkte
Benutzerkreis	Offen, verhindert nur eine Gruppe von Kontakten	Niedrig (max. 4 Punkte)	4 Punkte
Komfortabilität	Einfache Administration	Hoch (max. 10 Punkte)	10 Punkte
Effektivität	Mittel, neue SPIT Kontakte noch nicht erfasst	Hoch (max. 10 Punkte)	5 Punkte
Individualisierung	Ja	Niedrig (max. 4 Punkte)	4 Punkte
Gesamt		**60 Punkte**	**42 Punkte**

Tabelle 7.3: Bewertung Blacklists

7.2.4 Statistische Blacklists

Statistische Blacklists (Abschnitt 6.5) bilden eine Erweiterung der schon erläuterten Blacklists. Sie ermöglichen es durch statistische Daten automatisch neue Kontakte zur Blacklist hinzuzufügen, was einen Komfortabilitätsvorteil mit sich bringt. Die Beschaffung dieser Daten ist relativ komplex und umständlich. Eine Administration an zentraler Stelle ist notwendig. Somit verlagert sich der Installationsort auch zum Teil auf einen zentralen Punkt, was den Vorteil mit sich bringt, dass die eigentliche Blacklistanwendung in einen komplexen zentralen Teil und einen einfachen Filterteil geteilt wird, was zur Folge hat, dass die Performance der Anwendung nicht leidet (evtl. mobiler Einsatz möglich, schnell, etc.) Durch das Erreichen von 47 Punkten von möglichen 60 Punkten erreicht die Methode 78 Prozent der Gesamtpunktezahl.

Kriterien	**Anmerkung**	**Priorität (max. Punkte)**	**Punkte**
Zeitpunkt der Erkennung	Vor dem Anruf	Mittel (max. 6 Punkte)	6 Punkte
Technischer Reifegrad	Marktreife (in Verwendung)	Hoch (max. 10 Punkte)	10 Punkte
Komplexität vs. Effektivität	Aufnahmemechanismen sind komplexer	Mittel (max. 6 Punkte)	3 Punkte
Benutzerkreis	Offen	Niedrig (max. 4 Punkte)	4 Punkte
Komfortabilität	Automatische Aufnahme von SPIT Kontakten	Hoch (max. 10 Punkte)	10 Punkte
Effektivität	Effektiver als Blacklists	Hoch (max. 10 Punkte)	10 Punkte
Individualisierung	Manuell + Statistikadministration	Niedrig (max. 4 Punkte)	4 Punkte
Gesamt		**60 Punkte**	**47 Punkte**

Tabelle 7.4: Bewertung Statistische Blacklists

7.2.5 Greylists

Greylists (Abschnitt 6.6) verfolgen ein ähnliches Ziel wie Blacklists bzw. Whitelists mit dem Unterschied der Aufnahme in die Listen. Durch das selbe Grundprinzip entsteht ein sehr effektives Verfahren, welches kostenfrei verfügbar ist. Durch den Einsatz von Black- oder Whitlists weist dieses Verfahren eine niedrige Komplexität auf. Durch die Abweisung des ersten Anrufversuchs kann davon ausgegangen werden, dass die SPIT Erkennung vor dem eigentlichen Anruf geschieht. Eine Individualisierung ist durch das manuelle Hinzufügen von Kontakten möglich. Durch das Erreichen von 43 Punkten von möglichen 60 Punkten erreicht die Methode 72 Prozent der Gesamtpunktezahl.

Kriterien	**Anmerkung**	**Priorität (maximale Punkte)**	**erreichte Punkte**
Zeitpunkt der Erkennung	Vor dem Anruf	Mittel (maximal 6 Punkte)	6 Punkte
Technischer Reifegrad	Testphase	Hoch (maximal 10 Punkte)	8 Punkte
Komplexität vs. Effektivität	Niedrig	Mittel (maximal 6 Punkte)	6 Punkte
Benutzerkreis	Offen	Niedrig (maximal 4 Punkte)	4 Punkte
Komfortabilität	Hoch	Hoch (maximal 10 Punkte)	10 Punkte
Effektivität	Mittel	Hoch (maximal 10 Punkte)	5 Punkte
Individualisierung	Ja	Niedrig (maximal 4 Punkte)	4 Punkte
Gesamt		**60 Punkte**	**43 Punkte**

Tabelle 7.5: Bewertung Greylists

7.2.6 Voice Menu Interaciton

Voice Menu Interaction (Abschnitt 6.7) bietet die Möglichkeit, dass ein Anrufer erst eine manuelle Tätigkeit ausführen muss, um sich als korrekter Anrufer zu identifizieren. Der Zeitpunkt der Erkennung liegt wiederum vor dem eigentlichen Eingang des Anrufs. Effektivität und Komplexität stehen in einem ausgewogenen Verhältnis. Die Komfortabilität für den Anrufer ist nicht mehr gegeben und daher als gering einzustufen. Es kann davon ausgegangen werden, dass sich die Effektivität solcher Systeme ähnlich der Effektiviät von CAPTCHAs im Bereich des Internets verhält und wird daher als hoch eingestuft. Eine technische Realisierung beziehungsweise die Verwendung dieser Lösung wird allerdings auf Grund der Nachteile nicht zu erwarten sein. Durch das Erreichen von 27 Punkten von möglichen 60 Punkten erreicht die Methode 45 Prozent der Gesamtpunktezahl.

Kriterien	**Anmerkung**	**Priorität (maximale Punkte)**	**erreichte Punkte**
Zeitpunkt der Erkennung	Vor dem Anruf	Mittel (maximal 6 Punkte)	6 Punkte
Technischer Reifegrad	Konzept	Hoch (maximal 10 Punkte)	2 Punkte
Komplexität vs. Effektivität	Mittel	Mittel (maximal 6 Punkte)	3 Punkte
Benutzerkreis	Offen	Niedrig (maximal 4 Punkte)	4 Punkte
Komfortabilität	Gering	Hoch (maximal 10 Punkte)	2 Punkte
Effektivität	Hoch	Hoch (maximal 10 Punkte)	10 Punkte
Individualisierung	Nein	Niedrig (maximal 4 Punkte)	0 Punkte
Gesamt		**60 Punkte**	**27 Punkte**

Tabelle 7.6: Bewertung Voice Menu Interaction

7.2.7 User Behavior-Analysis

Die User Behavior-Analysis (Abschnitt 6.8) basiert auf der Auswertung des Verhaltens eines Benutzers. Die in der Forschungsphase befindliche Methode weist somit eine hohe Komplexität auf. Durch die Analyse des Gesprächverhaltens ergibt sich ein offener Benutzerkreis. Die Komfortabilität liegt im Bereich mittel, da es zu unerwünschten Anrufen kommen kann, welche allerdings in weiterer Folge erkannt werden. Eine Individualisierung ist defacto nicht möglich. Durch das Erreichen von 25 Punkten von möglichen 60 Punkten erreicht die Methode 42 Prozent der Gesamtpunktezahl.

Kriterien	**Anmerkung**	**Priorität (maximale Punkte)**	**erreichte Punkte**
Zeitpunkt der Erkennung	Nach dem Anruf	Mittel (maximal 6 Punkte)	1 Punkt
Technischer Reifegrad	Forschung	Hoch (maximal 10 Punkte)	2 Punkte
Komplexität vs. Effektivität	Mittel	Mittel (maximal 6 Punkte)	3 Punkte
Benutzerkreis	Offen	Niedrig (maximal 4 Punkte)	4 Punkte
Komfortabilität	Mittel	Hoch (maximal 10 Punkte)	5 Punkte
Effektivität	Hoch	Hoch (maximal 10 Punkte)	10 Punkte
Individualisierung	Nein	Niedrig (maximal 4 Punkte)	0 Punkte
Gesamt		**60 Punkte**	**25 Punkte**

Tabelle 7.7: Bewertung User Behavior-Analysis

7.2.8 Checking Human Communication Patterns

Da das Checking Human Communication Patterns Verfahren (Abschnitt 6.9) auf dem Prinzip der Anrufmuster Erkennung basiert, liegt die Phase der Erkennung während des Gespräches bzw. mittels Erweiterungen vor dem Gespräch. Das Verfahren setzt eine sehr komplexe Lösung voraus, welche eine effektive Lösung bietet. Der Benutzerkreis ist durch das Verwenden von Patternlösungen abhängig von dem Sprachverhalten gewisser Personengruppen und Nationalitäten. Die Komfortabilität ist dadurch, dass keine Interaktion stattfinden muss, als hoch einzustufen. Eine Individualisierung ist nicht möglich. Der technische Reifegrad liegt im Bereich Konzept bzw. der Forschungsphase. Durch das Erreichen von 30 Punkten von möglichen 60 Punkten erreicht die Methode 50 Prozent der Gesamtpunktezahl.

Kriterien	**Anmerkung**	**Priorität (maximale Punkte)**	**erreichte Punkte**
Zeitpunkt der Erkennung	Während des Anrufs	Mittel (maximal 6 Punkte)	3 Punkte
Technischer Reifegrad	Konzept- Forschungsphase	Hoch (maximal 10 Punkte)	2 Punkte
Komplexität vs. Effektivität	Mittel	Mittel (maximal 6 Punkte)	3 Punkte
Benutzerkreis	Geschlossen	Niedrig (maximal 4 Punkte)	2 Punkte
Komfortabilität	Hoch	Hoch (maximal 10 Punkte)	10 Punkte
Effektivität	Hoch	Hoch (maximal 10 Punkte)	10 Punkte
Individualisierung	Nein	Niedrig (maximal 4 Punkte)	0 Punkte
Gesamt		**60 Punkte**	**30 Punkte**

Tabelle 7.8: Bewertung Checking Human Communication Patterns

7.2.9 SPIT-AL

SPIT-AL (Abschnitt 6.10) ist eine Kombination von Abwehrmechanismen. Durch diese Kombination ist eine höhere Komplexität des Systems gegeben. Dieses Verfahren wurde in Deutschland realisiert und kommt teilweise auch zum Einsatz. Der Benutzerkreis wird durch die Kombination von Lösungen offen gehalten. Eine effektive und individualisierbare Lösung ist das Endergebnis dieses Lösungsansatzes. Durch das Erreichen von 47 Punkten von möglichen 60 Punkten erreicht die Methode 78 Prozent der Gesamtpunktezahl.

Kriterien	**Anmerkung**	**Priorität (maximale Punkte)**	**erreichte Punkte**
Zeitpunkt der Erkennung	Vor dem Anruf	Mittel (maximal 6 Punkte)	6 Punkte
Technischer Reifegrad	Marktreife	Hoch (maximal 10 Punkte)	10 Punkte
Komplexität vs. Effektivität	Mittel	Mittel (maximal 6 Punkte)	3 Punkte
Benutzerkreis	Offen	Niedrig (maximal 4 Punkte)	4 Punkte
Komfortabilität	Hoch	Hoch (maximal 10 Punkte)	10 Punkte
Effektivität	Hoch	Hoch (maximal 10 Punkte)	10 Punkte
Individualisierung	Ja	Niedrig (maximal 4 Punkte)	4 Punkte
Gesamt		**60 Punkte**	**47 Punkte**

Tabelle 7.9: Bewertung SPIT-AL

7.2.10 Zusammenfassung der Evaluierung

Nachfolgende Tabellen zeigen einen zusammenfassenden Überblick der Evaluation der einzelnen Methoden. Des Weiteren werden alle als wertfrei beschriebenen Kriterien dargestellt. Schlussendlich dient die Tabelle 7.11 zur Übersicht über die Reihung der einzelnen Methoden nach den errechneten Punkten der Evaluation.

Folgende Legende entspricht den Spaltenüberschriften der Tabelle 7.10

BFR := Barrierefreiheit
NACH := Nachhaltigkeit
ANW := Anwendungsbereich
AUF := Aufnahmemethode
INST := Installationsort

Methode	**ANW**	**NACH**	**INST**	**BFR**	**AUF**
Cost for Telephony	Business	Befristet	Zentral	Ja	Automatisch
Whitelists	Privat/Business	Befristet	Zentral/Empf.	Ja	Manuell
Blacklists	Privat/Business	Befristet	Zentral/Empf.	Ja	Manuell
Statistische Blacklists	Business	Befristet	Zentral	Ja	Auto./Man.
Greylists	Business	Befristet	Zentral	Ja	Automatisch
Voice Menu Interaction	Business	Dauerhaft	Zentral	Nein	Keine Aufnahme
User Behavior-Analysis	Business	Befristet	Zentral	Ja	Automatisch
Human Communication Patterns	Business	Dauerhaft	Zentral	Nein	Keine Aufnahme
SPIT-AL	Business	Befristet	Zentral	Ja	Auto./Man.

Tabelle 7.10: Wertfreie Zusatzkriterien

Durch die Bewertung hat jede Methode einen Prozentsatz der Gesamtpunkte bzw. eine gewisse Punktezahl der Gesamtpunkte erreicht, welche nun in einer Reihung gelistet werden. Somit wird ersichtlich, welche Methode statistisch gesehen die beste Kombination aus den herangezogenen Kriterien bietet.

Rang	**Methode**	**Prozentsatz der Gesamtpunkte**	**erreichte Punkte**
1	SPIT-AL	78%	47 Punkte
2	Statistische Blacklists	78%	47 Punkte
3	Whitelists	72%	43 Punkte
4	Greylists	72%	43 Punkte
5	Blacklists	70%	42 Punkte
6	Checking Human Communication Patterns	50%	30 Punkte
7	Cost for Telephony	45%	27 Punkte
8	Voice Menu Interaction	45%	27 Punkte
9	User Behavior-Analysis	42%	25 Punkte

Tabelle 7.11: Methoden Ranking

Es ist nun ersichtlich, dass es sehr große Unterschiede zwischen den einzelnen Methoden gibt. Von den erreichten Punkten her bewegt sich die schlechteste Methode bei 25 Punkten und die beste Methode bei 47 von möglichen 60 Punkten. Die Wahl der richtigen Methode kann allerdings nicht anhand der Tabelle pauschal abgelesen werden, sondern muss mittels eines Auswahlverfahrens, welches die Eigenheiten der jeweiligen Methoden unter Berücksichtigung der Anforderungen mit einbezieht, gewählt werden.

Kapitel 8

Ausblick und Conclusio

Das Thema SPAM hat sowohl im Bereich von E-Mail und VoIP als auch in vielen anderen Bereichen der elektronischen Kommunikation einen sehr hohen Stellenwert. Basierend auf der langjährigen Erfahrung mit SPAM im Bereich von E-Mail ist mit einer ähnlichen, wenn nicht sogar unangenehmeren Entwicklung von SPAM im Bereich von VoIP (SPIT) zu rechnen. Die Begründung dieser Einschätzung stammt zum einen aus den bisherigen Erfahrungen im Bereich VoIP und zum anderen lässt die rasante Entwicklung und Verbreitung von VoIP-Systemen diese Schlussfolgerung zu.

Im Bereich von SPIT haben sich drei verschiedene Szenarien von Angriffen gezeigt. Dies sind Call Centres, Calling Bots und Ringtone SPIT. Den ersten zwei Methoden kommt eine wesentlich höhere Bedeutung zu, da diese den eigentlichen Zweck eines Voice SPAMmers - das Verbreiten kostengünstiger Werbung - erfüllen. Diese treten somit häufiger auf als der Ringtone SPIT, welcher eine störende Wirkung zur Folge hat und teilweise darauf abzielt die Angerufenen zum Rückruf einer meist teuren Mehrwertnummer zu bewegen.

Im Zuge der Arbeit wurden ausgewählte Abwehrmethoden von SPIT analysiert. Die Analyse zeigte auf, dass es grundlegend zwei verschiedene Kategorien von Abwehrtechniken gibt. Einerseits werden geeignete Filterlisten (z.B. Whitelists oder Blacklists) gepflegt, die unerwünschte Anrufe von Voice SPAMmern verhindern sollen. Andererseits wird ein Prinzip verfolgt, welches automatisiert das Verhaltensmuster von Anrufern analysiert, um einen Abwehrschutz zu erzeugen.

Zur Analyse der SPIT-Problematik wurde in dieser Arbeit eine Evaluierung und Bewertung der verschiedenen Methoden zur Abwehr von SPIT auf Basis von zwölf Bewertungskriterien vorgenommen. Ergebnis der Evaluierung ist eine Reihung der einzelnen Methoden, auf Basis derer man einzelne Ab-

wehrmethoden für den Einsatz in der Praxis auswählen kann. Es hat sich gezeigt, dass Methoden, welche auf Listen basieren, derzeit besser geeignet sind SPIT auf eine einfache und verlässliche Weise abzuwehren als Methoden, welche das Verhalten der Kommunikationsteilnehmer berücksichtigen. Viele Abwehrmethoden gegen SPIT, wie zum Beispiel Statistical Blacklists oder SPIT-AL, bestehen aus einer Kombination von Abwehrmethoden und führen so zu einem effektiveren Schutz vor SPIT. Diese Methoden liegen bei der abschließenden Evaluierung im Spitzenfeld, weisen allerdings eine höhere Komplexität auf.

Viele der in der Diplomarbeit vorgestellten Methoden befinden sich derzeit auch noch in der Konzept- oder Forschungsphase. Das bedeutet, dass diese Lösungen erst zukünftig zur Marktreife gebracht werden. Die Entwicklungsgeschwindigkeit in diesem Bereich hat sich als sehr schnell herausgestellt. Da dieses Thema voraussichtlich immer mehr an Bedeutung gewinnen wird, ist zu erwarten, dass in den nächsten Jahren viel Forschungs- und Entwicklungsarbeit durchgeführt wird und Lösungen ausgearbeitet werden, die sowohl effektiv als auch einfach zu verwenden sind. Die Ergebnisse dieser Diplomarbeit können für solche weitergehende Forschungen eine Basis darstellen, da sie zeigen in welchen Aspekten Maßnahmen gegen SPIT noch Verbesserungspotenzial haben.

Tabellenverzeichnis

Abbildungsverzeichnis

Literaturverzeichnis

[Ala08] M. Alakhras. Voice over IP (VoIP). Communications, Computers and Applications, 2008. MIC-CCA 2008. Mosharaka International Conference on, August - Oktober 2008.

[Aus09] Telekom Austria. Geschichte Telefonie. "http://www.stadt-wien.at/index.php?id=telekommunikation-telefon", 2009.

[Bad09] A. Badach. *Voice over IP - Die Technik. Grundlagen, Protokolle, Anwendungen, Migration, Sicherheit.* Hanser Fachbuch, Jänner 2009.

[Ban10] C.M. Banner. Understanding Unified Messaging. *IT Professional*, 12(1):40 –45, Jänner - Februar 2010.

[Ber09] M. Hirschbichler; C. Egger; O. Pasteka; A. Berger. Using E-Mail SPAM DNS Blacklists for Qualifying the SPAM-over-Internet-Telephony Probability of a SIP Call. In *Digital Society, 2009. ICDS '09. Third International Conference on*, Jänner - Juli 2009.

[Bha09] Y. Bai; X. Su; B. Bhargava. Adaptive Voice Spam Control with User Behavior Analysis. *High Performance Computing and Communications, 10th IEEE International Conference on*, 0:354–361, 2009.

[Bla04] R. Blanpain. *Use and Monitoring of E-mail, Intranet and Internet Facilities at Work:Law and Practice: 27 (Studies in Employment and Social Policy) (Gebundene Ausgabe).* Kluwer Law International, 2004.

[Bro09] M. Brownlow. Email and webmail statistics. "http://www.email-marketing-reports.com/metrics/email-statistics.htm", Oktober 2009.

[BSI09a] BSI. BSI Anwendungsweisen der IT-Grundschutz-Kataloge. "https://www.bsi.bund.de/cln_174/ContentBSI/

grundschutz/kataloge/allgemein/einstieg/01001.html#1_4", 2009.

[BSI09b] BSI. BSI Begriffsdefinitionen. "https://www.bsi.bund.de/cln_183/sid_C6E2892F31C8991A1AAD7D06780EC8A8/ContentBSI/grundschutz/kataloge/glossar/04.html", 2009.

[BSI09c] BSI. BSI IT-Grundschutz - Basis für Informationssicherheit. "https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzKataloge/Inhalt/Allgemeines/Einstiegskapitel/einstiegskapitel_node.html", 2009.

[BSI09d] BSI. BSI IT-Grundschutz-Standards. "https://www.bsi.bund.de/ContentBSI/Publikationen/BSI_Standard/it_grundschutzstandards.html", 2009.

[BSI09e] BSI. BSI Umsetzung IT-Grundschutz. "https://www.bsi.bund.de/cln_174/ContentBSI/grundschutz/kataloge/baust/b01/b01000.html", 2009.

[BSI09f] BSI. IT-Grundschutz-Kataloge. "https://www.bsi.bund.de/cln_174/DE/Themen/weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html", 2009.

[BSI09g] BSI. Schutzbedarfskategorien. "https://www.bsi.bund.de/cln_156/DE/Themen/weitereThemen/WebkursITGrundschutz/Schutzbedarfsfeststellung/Schutzbedarfskategorien/schutzbedarfskategorien_node.html", 2009.

[BSI10] BSI. BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS). "https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1001.pdf?__blob=publicationFile", 2010.

[Bun07] Bundeskanzleramt. Bundesrecht: Gesamte Rechtsvorschrift für Europäische Menschenrechtskonvention. "http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000308", November 2007.

[Bun10] Bundesverwaltungsamt. Glossar. "http://www.bit.bund.de/nn_373372/BIT/DE/Zentrale__Dienste/DVDV/Glossar/Functions/glossar,lv2=373502.html", 2010.

[Can09] P. Sroufe; S. Phithakkitnukoon; R. Dantu; J. Cangussu. Email Shape Analysis for Spam Botnet Detection. In *Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE*, Oktober - Dezember 2009.

[Cas01] S. Cass. Anatomy of malice [computer viruses]. *Spectrum, IEEE*, November 2001.

[Col06] D. Endler; M. Collier. *Hacking Exposed VoIP- Voice Over IP Security Secrets Solutions*, volume 539. McGraw-Hill Osborne Media, 2006.

[Col07a] D. Endler; M. Collier. Exploiting Voice over IP Networks. Foliensammlung bei RSA Conference 2007, 2007.

[Col07b] D. Endler; M. Collier. Hacking exposed. "`http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Endler.pdf`", November 2007.

[Cor06] Nokia Corp. SIP Alert Header. "`http://sofia-sip.sourceforge.net/refdocs/sip/group__sip__alert__info.html`", 2006.

[DAT07] ARGE DATEN. Hysterie, Versagen und Polizeitrojaner. "`http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=91782erl`", Dezember 2007.

[Dau09] W. Dautermann. Usenet TU Wien. dbai TU Wien, Dezember 2009.

[Det07] E. Eren; K. Detken. *VoIP Security. Konzepte und Lösungen für sichere VoIP-Kommunikation.* Hanser Fachbuchverlag, 2007.

[Dud09] Dudenredaktion. *Duden - Voipen*, volume 1216. DUDEN VERLAG, Juli 2009.

[Enu10] Enum.at. ENUM und Voice over IP (VoIP). "`http://www.enum.at/ENUM-und-VoIP.375.0.html`", 2010.

[Eur07] NEC Europe. Verfahren zur Identifizierung von uerwünschten Telefonanrufen. "`http://www.patent-de.com/20071122/DE102006023924A1.html`", November 2007.

[Ewa07] J. Quittek; S. Niccolini; S. Tartarelli; M. Stiemerling; M. Brunner; T. Ewald. Detecting SPIT Calls by Checking Human Communication Patterns. In *Communications, 2007. ICC '07. IEEE International Conference on*, 2007.

[Fal08] S. Fries; R. Falk. *Voice Security.* VDE VERLAG, 2008.

[Fes10] H. Abdelnur; R. State; O. Festor. Advanced fuzzing in the VoIP spaces. *Journal in Computer Virology*, 6:57–64, 2010.

[fI10] Bundesverwaltungsamt Bundesstelle für Informationstechnik. Glossar. "http://www.bit.bund.de/nn_373372/BIT/DE/Zentrale__Dienste/DVDV/Glossar/Functions/glossar,lv2=373502.html", 2010.

[Fon10] Fonality. Trixbox. "http://www.trixbox.org", 2010.

[Gil06] A. Gillis. Asterisk@Home. "http://asteriskathome.sourceforge.net/", 2006.

[Gmb05] Berlecon GmbH. VoIP fuer Unternehmen - Nutzenpotenziale und Strategien jenseits des Hype. "http://www.berlecon.de/research/index.php?we_objectID=240", August 2005.

[Gsd10] Gsd. Globale software develoment. "http://www.karl-steinbuch-stipendium.de/uploads/RTEmagicC_verteilteentwicklung.jpg.jpg", 2010.

[Ham09] T. Brodt; J. Lan; S. Binti; S. Hameed. The services and application of mnos regarding mobile spam in southeast asia: Survey and discussion. *IEEE 2009*, 2009.

[Han06] H. Waack; J. Möller; M. Hansen; M. Hansen. Abwehr von Spam over Internet Telephony (SPIT-AL). "http://www.spit-abwehr.de/Whitepaper_SPITAL_20060310.pdf", Jänner 2006.

[Han07] M. Hansen. Voice over IP. "https://www.datenschutzzentrum.de/vortraege/20070320-hansen-voip-cebit-heise.pdf", 2007.

[Höv09] M. Hövener. Suchmaschinen Spam Teil 2. "http://www.contentmanager.de/magazin/artikel_1075_suchmaschinen_spam_praxis.html", Dezember 2009.

[iACG01] innominate AG; Colibri GmbH. Open-Source-Software Ein Leitfaden für kleine und mittlere Unternehmen. "http://oss-broschuere.berlios.de/broschuere/broschuere-de.html#N3275", März 2001.

[Inc10] Bitpipe Inc. Definition CTI. "http://www.bitpipe.com/tlist/CTI-%28Computer-Telephony-Integration%29.html", 2010.

[Inf08] Düvel Informationssysteme. Das Internetportal für Voice over IP. "http://www.voip-sip.de/faq/voip-faq-artikel-36-rubrik-2.htm", 2008.

[Inf10] Gesellschaft Für Informatik. Fachgruppe Biometrik und elektronische Signaturen. "http://www1.gi-ev.de/fachbereiche/sicherheit/fg/biosig/", Februar 2010.

[Jin07] D. Butcher; L. Xiangyang; G. Jinhua. Security Challenge and Defense in VoIP Infrastructures. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, 37(6):1152 –1162, November 2007.

[Joh01] A. B. Johnston. *Sip: Understanding the Session Initiation Protocol*, volume 228. Artech House Publishers, Jänner 2001.

[Jud08] W. Yang; P. Judge. Visor: Voip security using reputation. In *Communications, 2008. ICC '08. IEEE International Conference on*, 19-23 2008.

[Jun08] C. Jung. *Ansatz für eine Migration zu Voice over IP (VoIP): Unter Berücksichtigung der CISCO SYSTEMS AVVID (R)-Lösung.* Grin Verlag, Juni 2008.

[Kem02] S. Wintermeyer; P. Kempgen. Asterisk - Call Files. "`http://www.das-asterisk-buch.de/2.1/call-file.html`", November 2002.

[Ker06] D.R. Millen; J. Feinberg; B. Kerr. Dogear: Social bookmarking in the enterprise. In *CHI '06: Proceedings of the SIGCHI conference on Human Factors in computing systems*, New York, NY, USA, 2006. ACM.

[Kha08a] A. Schmidt; N. Knutze; R. Khayari. Spam over Internet Telephony and how to deal with it. In HS. Venter; MM. Eloff; JHP. Eloff; L. Labuschagne, editor, *Proceedings of the ISSA 2008 Innovative Minds Conference*, Juli 2008.

[Kha08b] R. Khayari. Spam over internet telephony and how to deal with it. Master's thesis, TU Darmstadt, Juli 2008.

[Kle10] G. Klemens. *The Cellphone: The History and Technology of the Gadget That Changed the World.* McFarland and Company, August 2010.

[Krö10] T. Kröner. VoIP - Voice over IP. "`http://www.voip-information.de/voip-voice-over-ip.html`", 2010.

[Kun08] R. Khayari; N. Kuntze. Angriff der Sprachcomputer. "`http://www.sit.fraunhofer.de/pressedownloads/pressemitteilungen/20080723.jsp`", Juli 2008.

[Lak01] SR. Subramanya; N. Lakshminarasimhan. Computer viruses. *Potentials, IEEE*, Oktober 2001.

[Lam05] G. Kambourakis; D. Geneiatakis; S. Gritzalis; T. Dagiuklas; C. Lambrinoudakis. Security and privacy issues towards ENUM protocol. Dezember 2005.

[Lim10] Skype Limited. Skype. "`http://www.skype.com`", 2010.

[Lip07] M. Lipp. *VPN - Virtuelle Private Netzwerke: Aufbau und Sicherheit*. Addison-Wesley, September 2007.

[Lis06] E. Skoudis; T. Liston. *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses*. Prentice Hall, Jänner 2006.

[Lob05] M. Lobeck. *Internet-Telefonie - VoIP für Alle*. Karl Hanser Verlag, 2005.

[Lug97] G. Luger. *Artificial Intelligence: Structures and Strategies for Complex Problem Solving*. Addison Wesley, 1997.

[Mic05] Microsoft. Die 6 Merkmale der Zuverlässigkeit. "`http://www.microsoft.com/germany/sicherheit/twc/Reliabilityattributes.mspx`", Mai 2005.

[Moe06] M. Hansen; M. Hansen; J. Moeller. Developing a Legally Compliant Reachability Management System as a Countermeasure against SPIT. Third Annual VoIP Security Workshop, Juni 2006.

[Nam05] N. Thanthry; R. Pendse; K. Namuduri. Voice over IP security and law enforcement. In *Security Technology, 2005. CCST '05. 39th Annual 2005 International Carnahan Conference on*, 11-14 2005.

[Nam10] D. Gudkova; E. Bondarenko; M. Namestnikova. Kaspersky Security Bulletin 2009. "`http://www.kaspersky.com/de/downloads/pdf/kaspersky_security_bulletin_2009.pdf`", Februar 2010.

[Nic07] M. Falomi; R. Garroppo; S. Niccolini. Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE. In *Simulation and Optimization of SPIT Detection Frameworks*. NEC Eur. Ltd., Heidelberg;, November 2007.

[Nin09] S. Liancheng; J. Ning. Research on Security Mechanisms of SIP-Based VoIP System. In *Hybrid Intelligent Systems, 2009. HIS '09. Ninth International Conference on*, volume 2, 12-14 2009.

[Nor04] M. Baugher; D. McGrew; M. Naslund; E. Carrara; K. Norrman. The Secure Real-time Transport Protocol (SRTP). "`http://www.ietf.org/rfc/rfc3711.txt`", März 2004.

[Ope10] OpenSIPS. Open SIP Server. "`http://www.opensips.org/`", 2010.

[Per10] M. Handley; V. Jacobson; C. Perkins. Sessinon Description Protocol. "`http://www.ietf.org/rfc/rfc4566.txt`", 2010.

[Plc09] Sophos Plc. Security threat report: 2009. Security threat report, 2009.

[Plc10] Sophos Plc. Security threat report: 2010. Security threat report, 2010.

[Pty09] Hitwise Pty. Yahoo! Mail More than One Third of Yahoo! Traffic. "http://weblogs.hitwise.com/us-heather-hopkins/2009/03/yahoo_mail_more_than_one_third.html", Dezember 2009.

[Rec74] Bundeskanzleramt Rechtsinformationssystem. Bundesrecht: Gesamte Rechtsvorschrift für Strafgesetzbuch. "http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296&ShowPrintPreview=True", 1974.

[Rec99] Bundeskanzleramt Rechtsinformationssystem. Signaturgesetz. "http://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40095845/NOR40095845.html", 1999.

[Rec00] Bundeskanzleramt Rechtsinformationssystem. Bundesrecht: Gesamte Rechtsvorschrift für Datenschutzgesetz 2000. "http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597", 2000.

[Rec03] Bundeskanzleramt Rechtsinformationssystem. Telekommunikationsgesetz 2003. "http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20002849", 2003.

[Rec10] Bundeskanzleramt Rechtsinformationssystem. Bundesrecht: Gesamte Rechtsvorschrift für Strafprozeßordnung 1975. "http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002326", 2010.

[Red09] B. Reder. Die Spam-E-Mail feiert ihren 30. Geburtstag. "http://www.networkcomputing.de/die-spam-e-mail-feiert-ihren-30-geburtstag/", Dezember 2009.

[Ren00] U. Rödig; S. Fischer; C. Rensing. *Open Internet Security*. Springer, 2000.

[Rtr03] Rtr. Telekommunikationsmärkte Verordnung 2003. "http://www.rtr.at/de/tk/TKMVO2003", 2003.

[Rtr04] Rtr. Richtlinien für Anbieter von VoIP Diensten. "`http://www.rtr.at/de/tk/RichtlinienVoIP`", 2004.

[Rtr06] Rtr. Voice over IP Grundlagen, Regulierung und erste Erfahrungen. "`http://www.rtr.at/de/komp/KonsultationVoIP`", 2006.

[Sca06] D. Cook; J. Hartnett; K. Manderson; J. Scanlan. Catching spam before it arrives: domain specific dynamic blacklists. In *ACSW Frontiers '06: Proceedings of the 2006 Australasian workshops on Grid computing and e-research*, Darlinghurst, Australia, Australia, 2006. Australian Computer Society, Inc.

[Sch03] F. Schmidbauer. Die österreichische Rechtslage zur E-Mail-Werbung. "`http://www.internet4jurists.at/e-mail/oe1a.htm`", Juni 2003.

[Sch07] C. Schreiber. *Identitätsarbeit in Multi-User-Dungeons: Funktionsweise von MUDs und mögliche Auswirkungen auf die Persönlichkeit des Spielers*. Grin Verlag, November 2007.

[Sch08] J. Quittek; S. Niccolini; S. Tartarelli; R. Schlegel. On Spam over Internet Telephony (SPIT) Prevention. *IEEE Communications Magazine*, August 2008.

[Sin06] H. Sinnreich. *Internet Communications Using SIP: Delivering VoIP and Multimedia Services with Session Initiation Protocol*. Wiley, 2006.

[Sis08] B. Mathieu; S. Niccolini; D. Sisalem. SDRS: A Voice-over-IP Spam Detection and Reaction System. *Security and Privacy, IEEE*, 6(6):52 –59, November - Dezember 2008.

[Ste98a] S. Fischer; A. Seinacker; R. Bertram; R. Steinmetz. *Open Security*. Springer, 1998.

[Ste98b] D. Johnson; A. Ruth; J. Michael Stewart. *MCSE Crash Test Proxy Server 2*. Mitp-Verlag, 1st edition, April 1998.

[Teo08] L. Teo. Port Scans and Ping Sweeps Explained. *Linux J.*, 2008.

[Tur07] M. Turino. SPIT Spam over Internet Telephony. "`http://www.net2.uni-tuebingen.de/fileadmin/RI/teaching/seminar_mobil/ss07/abgabe/slides-turino.pdf`", 2007.

[Uld06] Datenschutz Initiative Uld. SPIT-AL Rechtskonforme Abwehr von SPAM over Internet Telephony (SPIT). "`http://www.spit-abwehr.de/SPIT-AL-BvD-20060317-JM.pdf`", 2006.

[Ver06] G. Me; D. Verdone. An overview of some techniques to exploit VoIP over WLAN. In *Digital Telecommunications, 2006. ICDT '06. International Conference on*, 2006.

[Waa06] M. Hansen; M. Hansen; J. Möller; T. Rohwer; C. Tolkmit; H. Waack. Third Annual VOIP Security Workshop. In *Developing a Legally Compliant Reachability Management System as a Countermeasure against SPIT*, Juni 2006.

[Wei09] Q. Zhaoyang; Y. Wei. The Design of an Active VoIP Security Defense Model Based on Dynamic Self-Adaptive Diffluence. In *Environmental Science and Information Application Technology, 2009. ESIAT 2009. International Conference on*, volume 1, 4-5 2009.

[Wes07] C. Westbrook. *Netzwerksicherheit: Hacking für Administratoren - Angriffe erkennen und Schutzmaßnahmen verstärken.* Books on Demand GmbH, 2007.

[Wie03] E. Wiederin. *Privatsphäre und Überwachungsstaat.* MANZ'sche Wien, Juli 2003.

[Wil10] R. F. Wilson. E-Mail + Social Bookmarking = Instant Rankings. "`http://www.wilsonweb.com/linking/wilson-email-addthis.htm`", Jänner 2010.

[Wu07] B. Wu. *Finding and fighting search engine spam.* PhD thesis, Lehigh University, Bethlehem, PA, USA, 2007.

[Zem01] H. Zemanek. *Vom Mailüfterl zum Internet: Geschichte, Perspektiven und Kritik der Informationstechnik.* Picus-Verl., Februar 2001.

URLs zuletzt geprüft am: 18.08.2010