Früherkennung von verdeckten Kanälen in VoIP-Kommunikation

Christian Krätzer, Jana Dittmann
Arbeitsgruppe Multimedia and Security
Fakultät für Informatik
Otto-von-Guericke Universität Magdeburg, Germany

1. Einleitung

Der potentielle Schaden, der durch den Einsatz einer Maßnahme zur geheimen Kommunikation, wie sie die Steganographie darstellt, droht, liegt vor allem im Bereich der unautorisierten Übermittlung von vertraulichen Daten. Die Nutzung von steganographischen Maßnahmen zur Sicherung der Geheimhaltung von Kommunikationskanälen zielt oft darauf ab, bestehende Kommunikationsbeschränkungen zu umgehen ohne dass einem möglichen Beobachter die Existenz einer geheimen Kommunikation bewusst wird.
Ein Kommunikationsprotokoll wie VoIP (Voice over IP), das sich zur Zeit einer stark wachsenden Beliebtheit erfreut, eignet sich hervorragend als Träger für steganographisch versteckte Nachrichten. Dabei dient ein VoIP-Telefonat als Trägermedium (Cover) für einen nicht wahrnehmbaren zweiten Kommunikationskanal, der beim Abhören des Telefonates unentdeckt bleiben würde.
Um die Umgehung bestehender Kommunikationsbeschränkungen (wie z.B. die Weitergabe von Firmengeheimnissen an Dritte) über diesen Kanal nachzuweisen oder zu verhindern, bedarf es eines entsprechenden Frühwarnsystems für die Erkennung von steganographischen Kanälen in solchen Verbindungen.
In diesem Paper wird, nach einer Einführung in die Grundlagen der Steganographie in Abschnitt 2, ein entsprechendes prototypisches Frühwarnsystem mit ersten Testergebnissen vorgestellt. Abschließend werden, basierend auf den präsentierten Ergebnissen, Schlussfolgerungen für weitere Forschungen auf diesem Gebiet gezogen.

2. Steganographie

Die Steganographie ist die Kunst und Wissenschaft der verborgenen Speicherung oder Übermittlung von Informationen. Dabei stammt das Wort „Steganographie“ aus dem Altgriechischen (στεγανός γράφειν [1]) und heißt übersetzt „verdeckt Schreiben“. Sie wird oft definiert als „Die Kunst der versteckten Kommunikation durch das Verbergen von Nachrichten in scheinbar harmlosen Objekten. Dabei ist die Existenz der steganographischen Nachricht nicht ersichtlich.“ [2]. Somit ist Sinn und Zweck die Tarnung von Informationen. Die Sicherheit einer geheimen steganographischen Botschaft liegt also darin, dass einem Betrachter (dem Angreifer) die Existenz einer solchen nicht auffällt. Detaillierte Beschreibungen des allgemeinen steganographischen Szenarios finden sich unter anderem in [3] und [4].

Steganographie als Maßnahme der Kryptographie („Der Wissenschaft der Sicherung von Nachrichten“ [2]) einzuordnen ist falsch, da beide Wissenschaften vollkommen verschiedene Ansätze haben, um eine Nachricht dem Empfänger sicher zukommen zu lassen [5]. Im Gegensatz zur Kryptographie, bei der eine Botschaft verschlüsselt wird, versucht die Steganographie, eine Botschaft im Cover-Objekt zu verstecken. Dennoch sind Steganographie und Kryptographie als eng verwandte Wissenschaften zu sehen, welche oft auch in Kombination auftreten.
Eine weitere Wissenschaft, der die Steganographie verwandt ist, sind die digitalen Wasserzeichen. Da verschiedene Einsatzszenarien für digitale Wasserzeichen existieren (wie z.B. die Integritätssicherung von Daten oder die Authentifizierung von Medienobjekten) ist es schwierig, in der Literatur eine allumfassende Definition für diese Information Hiding Technologie zu finden (siehe dazu [2]). Details zu unterschiedlichen Einsatzszenarien, den Kerncharakteristiken von digitalen Wasserzeichen und deren Anwendung sind unter anderem in [6] zu finden. Einige Wasserzeichenapplikationen bedienen sich derselben Methoden wie steganographische Algorithmen [2]. Daher lassen sich Applikationen aus beiden Wissenschaften auch anhand der Primärcharakteristiken Transparenz, Robustheit und Kapazität sowie anhand von Sekundärcharakteristiken wie der Komplexität evaluieren [7]. Unterschieden werden Beide allerdings immer durch ihre Intention. Diese ist das Markieren von Objekten bei digitalen Wasserzeichen und die versteckte Kommunikation bei der Steganographie.

In [8] ist ein Überblick über 87 verschiedene steganographische Tools gegeben. Diese werden im Rahmen einer grundlegenden Klassifikation beschrieben und vielgenutzte Prinzipien bei der Einbettung in verschiedene Medien werden im Detail betrachtet. Natürlich sind die 87 dort betrachteten Applikationen nur die Spitze eines Eisberges was die Zahl aktuell implementierter und genutzter steganographischer Verfahren angeht. Allerdings zeigt dieser Überblick doch gut die große Varianz an genutzten Möglichkeiten zum Verstecken von Kommunikationskanälen und das breite Spektrum an Medientypen und Protokollen, die als Cover für eine steganographische Einbettung genutzt werden.
Andere Publikationen wie z.B. [9], [10], [11], [12], [13], [14] und [15] beschäftigen sich gezielt mit der Nutzung einzelner Protokolle (unter anderem TCP/IP, WLAN und VoIP) als Cover für die Einbettung von steganographischen Nachrichten, wobei sie zum Teil unterschiedliche Arten an steganographischen Kommunikationsszenarien (aktive und passive [15]) betrachten. Alle diese Publikationen gelangen zur gleichen Erkenntnis: ein Steganographieverfahren gilt genau dann als sicher, wenn nach Anwendung des Verfahrens keinerlei Rückschlüsse Dritter darauf zu ziehen sind, ob im vorliegenden Medium eine Nachricht verborgen wurde oder nicht. Hier ergibt sich nun der Ansatzpunkt für die Steganalysis.

3. Steganalysis und Frühwarnsysteme für VoIP Steganographie

Steganalysis (oder auch Stegoanalysis) ist nach [2] die „Kunst des Entdeckens und Entschlüsselns von Nachrichten, die mit Mitteln der Steganographie verborgen wurden." Dabei lassen sich über diese Definition hinaus weitere Ziele für die Steganalysis ableiten. Diese sind:

- Das Entdecken geheimer (steganographischer) Kommunikationskanäle,
- Das Entschlüsseln steganographisch übertragener Nachrichten,
- Die Identifikation der an der steganographischen Kommunikation beteiligten Kommunikationspartner,
- Die Identifikation von Einbettzeitpunkt und –dauer, sowie des Einbettortes.

Werden durch eine Steganalyseapplikation (in Form eines Frühwarnsystems für Steganographie) zur Laufzeit obige Ziele umgesetzt, so werden damit eventuell auch über Detektieren einer Einbettung hinausgehende Gegenmaßnahmen wie das Mitlesen der geheimen Nachricht sowie das Stören, Unterbrechen oder Unterbinden von steganographischen Kanälen ermöglicht.

Generell kann Steganalysis auf verschiedene Art und Weisen umgesetzt werden. Je nach Art der steganographischen Kommunikation (aktiv oder passiv [15]) kann z.B. in einem Szenario mit passiver Steganographie eine verteilte Analyse unter Nutzung des Vergleiches der Coverströme den größten Teil der oben identifizierten Ziele (nicht notwendiger Weise die Entschlüsselung der übertragenen Nachricht) erreichen (siehe [16]).
Eine weitere Maßnahme der Steganographie ist die Suche nach Signaturen, wie sie bestimmte steganographische Tools wie zum Beispiel PGE [17], JSteg [18], Camouflage [19] oder Hide4PGP [17] in den Steganogrammen hinterlassen.
In [1] werden Angriffe auf steganographische Systeme vorgestellt, die in diesem Kontext mit Steganalysis gleichzusetzen sind. Dabei wird besonders auf die Bedeutung wahrnehmungsgestützter Steganalysis eingegangen. Grundlage für diese Analysemethode ist die menschliche Fähigkeit, Veränderungen an bekannten Strukturen auch ohne direkten Vergleich mit dem Original erkennen zu können.
Alle drei bisher vorgestellten Analysemethoden sind mit starken Einschränkungen versehen (Zugang zu Daten an verschiedenen Stellen des Kommunikationsweges in der verteilten Analyse, Existenz einer bekannten Applikationssignatur in der Signaturerkennung und die geringe Durchsatzrate / Genauigkeit in der wahrnehmungsgestützten Steganalysis), daher muss für eine mögliche Nutzung in einen steganographischen Frühwarnsystem ein weiterer Weg aufgezeigt werden, der frei von diesen Einschränkungen ist: die statistische Kanalanalyse.

In der statistischen Kanalanalyse werden Merkmale erhoben, um das charakteristische statistische Verhalten eines Kommunikationskanals über einen Zeitraum zu protokollieren. Damit wird das

„Normalverhalten“ dieses Kanals bestimmt. Ziel dieses Steganalyseansatzes ist es nun, die Kanalcharakteristiken zu finden, die bei einer steganographischen Einbettung in diesen Kanal verändert werden, um durch die Überwachung dieser Charakteristiken die Einbettung detektieren zu können. [1] und [20] demonstrieren die Anwendung dieser Analysemethode unter Nutzung von Statistiken erster und zweiter Ordnung sowie χ^2 Tests für die Einbettung in Bilddateien.
Im Folgenden wird die mögliche Anwendung der statistischen Kanalanalyse am Beispiel der Steganalyse in einem VoIP Kommunikationssystem näher betrachtet. Dazu wird zuerst nach [15] folgendes Kommunikationsszenario angenommen: Zwei Kommunikationspartner (Alice und Bob) kommunizieren mittels einer VoIP-Kommunikationsapplikation miteinander wie in Abbildung 1 dargestellt.

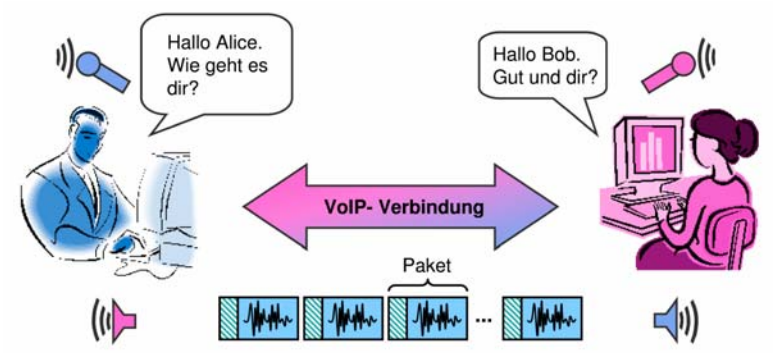

Abbildung 1 – VoIP-Kommunikation [13]

Dieses Kommunikationsszenario wird nun, wie in Abbildung 2 dargestellt, mittels passiver Steganographie um einen versteckten Kommunikationskanal erweitert. Das Resultat davon ist ein Kommunikationssystem, in dem zwei unterschiedliche Kommunikationskanäle an einem Punkt existieren, an dem für einem Betrachter (Angreifer C in Abbildung 2) nur ein Kanal (in unserem Falle die VoIP-Kommunikation) offensichtlich ist. Der zweite Kanal ist nach den Grundforderungen an ein steganographisches System nicht direkt wahrnehmbar für den Betrachter (siehe dazu auch [4]).

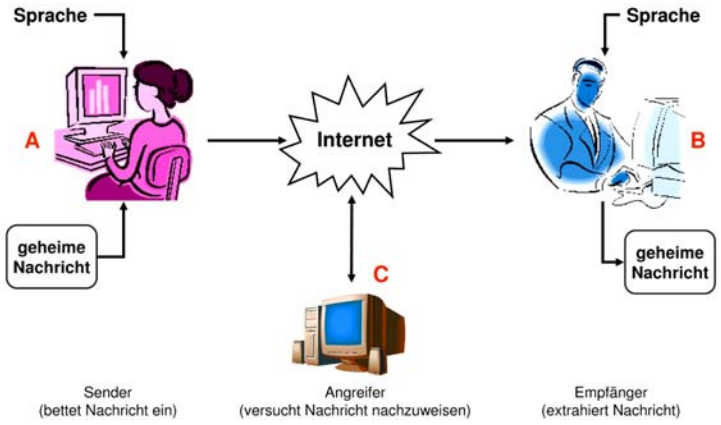

Abbildung 2 – VoIP-Kommunikation mit steganographischem Seitenkanal [13]

Das hier vorgestellte VoIP-Kommunikationssystem mit aktiver Steganographie ist in [13] detailliert beschrieben und formalisiert. Dort finden sich auch Details zur Implementierung.

Für die Steganalyse in diesem Kommunikationsszenario wurde an der Otto-von-Guericke Universität Magdeburg ein eigenes Tool namens Steganalyzer [21] entwickelt, welches als Sensor im Netzwerk agieren kann und für die, in VoIP-Verbindungen übertragenen, Audiodaten statistische Merkmale erster Ordnung erhebt. Dabei werden zurzeit folgende statistischen Merkmale für Fenster mit wählbarer Größe und Überlappung bestimmt:

- Varianz (ein Streuungsmaß welches die Abweichung der Werte von ihrem Mittelwert angibt)
- Kovarianz (eine Maßzahl für den Zusammenhang zweier statistischer Merkmale. Sie ist positiv wenn beide Merkmale einen linearen Zusammenhang besitzen und negativ bei gegensinnigem

linearen Zusammenhang. Bei einer Kovarianz gleich Null besteht keinerlei Zusammenhang.)
- Entropie (Maß für die Menge an Zufallsinformationen, die in einer Informationsfolge steckt)
- Least Significant Bit (LSB) Verhältnis (Verhältnis zwischen Nullen und Einsen im niederwertigsten Bit eines Samples)
- LSB Wechselrate (von Nullen und Einsen) (Wechselrate zwischen Nullen und Einsen im niederwertigsten Bit eines Samples)
- Mittelwert
- Median (Wert an der Grenzstelle zwischen zwei gleich großen Hälften einer in diesem Fall geordneten Zahlenfolge)

Zusätzlich dazu wird die Häufigkeit für eine folgende Null bei Mustern definierbarer Länge berechnet. Um die Aussagekraft der unter Einbeziehung der Merkmale erhobenen Statistiken zu erhöhen, ist es möglich, eine Vorverarbeitung der untersuchten Audiodaten vorzunehmen. Dabei bestehen die folgenden Möglichkeiten:

- Umwandlung der Audiosamples in rein positive Werte, um möglicherweise zu Verhindern, dass sich die positiven und negativen Samplewerte innerhalb der Statistikberechnungen ausnullen
- Reduzierung jedes Samplewertes auf ein Intervall von Bits, um den Wertebereich, der durch den Steganographieeinsatz verändert werden kann, einzugrenzen und somit die Genauigkeit der Statistiken zu erhöhen
- Erstellung der Fenster linear über die Audiodaten oder unter Berücksichtigung der einzelnen Kanäle, um mehrere Möglichkeiten der Einbettung nachvollziehen zu können
- Auslöschung digitaler Ruhe, also Nichtbetrachtung der Bereiche, in denen das Audiofile wahrscheinlich keinerlei Informationen enthält, da anzunehmen ist, dass hier dann auch vorsichtshalber keine Steganographie angewendet wurde

Zusätzlich zu den möglichen Vorverarbeitungsschritten bietet der Steganalyzer auch Möglichkeiten der Nachverarbeitung der bestimmten Merkmalsvektoren. Diese umfassen bisher:

- Die Wichtung der Vektorelemente der Merkmalsvektoren,
- Die Normalisierung der Vektoren,
- Die Konvertierung der Vektoren in das Inputformat einer Support Vector Machine (SVM_light [22]).

Testresultate für die Nutzung des Steganalyzers als Netzwerksensor in einem aktiven Steganographieszenario (wie oben beschrieben) sind in [13] zu finden. Dort wird vor allem die statistische Änderung der betrachteten Merkmale zum Einbettzeitpunkt untersucht. Erste Testresultate für den Einsatz des Steganalyzers in einem passiven Steganographieszenario werden in [16] beschrieben. In diesem Dokument wird der Einsatz als Sensor sowohl für eine verteilte Analyse unter Nutzung des Vergleiches der Coverströme diskutiert, also auch im Rahmen eines SVM (Support Vector Machine; hier SVM_light [22]) basierten Frühwarnsystems. Die Testresultate für den implementierten Prototypen eines Steganographiedetektors zeigten, dass eine automatische Detektion eines in die VoIP-Kommunikation eingebetteten steganographischen Kanals unter Nutzung des Steganalyzers als Sensor prinzipiell möglich ist. Allerdings musste ebenfalls festgestellt werden, dass die bisher erhobenen statistischen Merkmale für eine zuverlässige Klassifizierung des untersuchten Signals nicht ausreichen. Zusätzliche Merkmale zur Verbesserung der Detektionsrate müssen erhoben werden.

4. Zusammenfassung und Ausblick

Erste Testergebnisse zeigen, dass das in diesem Paper vorgestellte Frühwarnsystem für VoIP Steganography mit dem Steganalyzer als (Netzwerk-)Sensor in der Lage ist die Existenz eines steganographischen Kanals unter bestimmten Bedingungen zu detektieren. Allerdings implizieren die Ergebnisse in [13], dass die bisher erhobenen und genutzten statistischen Merkmale nicht ausreichend sind für einen zuverlässigen Einsatz innerhalb eines Frühwarnsystems. Für die Auswahl weiterer Merkmale für diesen Zweck sollten die in [13] und [14] gewonnenen Erkenntnisse bezüglich der Kontextabhängigkeit der statistischen Einbettung mit in Betracht gezogen werden. Aus diesen Publikationen ist ersichtlich, dass im Durchschnitt die Einbettung in Sprachdaten eine niedrigere Transparenz hat als die Einbettung in Musikdaten. Da VoIP-Kommunikationssysteme in der Regel auf die Übertragung von menschlicher Sprache hin optimiert sind (da dies den Großteil der übermittelten

Daten ausmacht) sollten für das weitere Vorgehen vorrangig sprachbezogene Merkmale, wie sie aus der Sprechererkennung bekannt sind, betrachtet werden.
Generell ist mit dem vorgestellten System ein guter Grundstein für ein Frühwarnsystem für die Erkennung von steganographischen Kanälen in VoIP-Kommunikationen gelegt. Dieses erweiterbare System trägt unter anderem der zunehmenden Nutzerakzeptanz von VoIP-Telefonieanwendungen und der guten Eignung eines VoIP-Kommunikationskanals für die Steganographie Rechnung.

Acknowledgements:

The work about classification of steganographic techniques described in this paper has been supported in part by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT. The information in this document is provided as is, and no guarantee or warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Effort for development of the Steganalyzer is partially sponsored by the Air Force Office of Scientific Research, Air Force Materiel Command, USAF, under grant number FA8655-04-1-3010. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Air Force Office of Scientific Research or the U.S. Government.

Literatur:

[1] Westfeld, Pfitzmann: *Attacks on Steganographic Systems*. S. 61–76 in Andreas Pfitzmann (Hrsg.): Information Hiding. Third International Workshop, IH'99, Dresden, Germany, September/October, 1999, Proceedings, LNCS 1768, Springer-Verlag Berlin Heidelberg 2000.

[2] Cox, Bloom, Miller: *Digital Watermarking, Principles & Practice*, Morgan Kaufmann, 2001.

[3] Johnson, Duric, Jajodia: *Information Hiding*, Kluwer Academic Publishers, 2001.

[4] Katzenbeisser, Petitcolas: *Information Hiding*, Artech House, 2000.

[5] Schneier: *Secrets & Lies*, Wiley & Sons, 2000.

[6] Dittmann, *Digitale Wasserzeichen*, Springer Xpert.press, ISBN 3-540-66661-3, 2000.

[7] Fridrich: Applications of data hiding in digital images, Tutorial for the ISPACS 1998 conference in Melburne, Australia, 1998.

[8] Dittmann, Kraetzer (eds.): ECRYPT *D.WVL.10, Audio Benchmarking Tools and Steganalysis*, ECRYPT Public Report, Feb. 2006.

[9] Kundur, Ahsan: *Practical Internet Steganography: Data Hiding in IP*, Proceedings of Workshop on Multimedia, December 2002.

[10] Singh: *Whispers on the Wire - Network Based Covert Channels*, Proceedings of the Symposium on Security for Asia Network (SyScAN'05), Bangkok, Thailand, 1st and 2nd of September 2005.

[11] Murdoch, Lewis: *Embedding Covert Channels into TCP/IP,* University of Cambridge, Information Hiding Workshop 2005.

[12] Szczypiorski: HICCUPS*: Hidden Communication System for Corrupted Networks*, The 10th International Multi-Conference on Advanced Computer Systems ACS 2003, http://krzysiek.tele.pw.edu.pl/pdf/acs2003-hiccups.pdf, 22.-24. Oktober 2003.

[13] Vogel, Dittmann, Hillert, Kraetzer: *Design und Evaluierung von Steganographie für Voice-over-IP*, Sicherheit 2006 GI FB Sicherheit, GI Proceedings, Magdeburg, Germany, Feb 2006.

[14] Krätzer, Dittmann, Vogel, Hillert: *Design and Evaluation of Steganography for Voice-over-IP*, Proceedings of the IEEE International Symposium on Circuits and Systems (ICSAS 2006), Kos, Griechenland, May 21-24, 2006.

[15] Dittmann, Hesse, Hillert: *Steganography and steganalysis in voice over IP scenarios : operational aspects and first experiences with a new steganalysis tool set*, In: Delp, Edward J. (Hrsg.); Wong, Ping W. (Hrsg.): Security, steganography, and watermarking of multimedia contents VII (Electronic imaging science and technology San Jose, California, USA, 17-20 January 2005) ; Bellingham, Wash. : SPIE, 2005, pp. 607 - 618, ISBN 0-8194-5654-3, 2005.

[16] Heutling: *Verteilte Steganographie und Steganalysis in VoIP Szenarien*, Diplomarbeit, Otto-von-Guericke Universität Magdeburg, Germany, Mai 2006.

[17] *PGE, Hide4PGP*, http://www.rugeley.demon.co.uk/security/

[18] *JSteg*, ftp://ftp.funet.fi/pub/crypt/steganography/

[19] *Camouflage*, http://camouflage.unfiction.com/

[20] Böhme, Westfeld: *Exploiting Preserved Statistics for Steganalysis,* S. 82-96 in Jessica Fridrich (Hrsg.): Information Hiding. 6th International Workshop, IH 2004 Toronto, Canada, May 23-25, 2004, Revised Papers, LNCS 3200, Springer-Verlag Berlin Heidelberg 2004.

[21] *Steganalyzer*, Internal Documentation, AG Multimedia and Security, Otto-von-Guericke Universität Magdeburg, Germany.

[22] *SVM Light*, http://svmlight.joachims.org/