

Contents

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

1. Editorial

Patches – Fluch oder Segen?

Ich muss gestehen, dass ich mich seit der Veröffentlichung im Besitz einer Xbox von Microsoft befinde. Und dies obschon ich mich nicht wirklich zum bekennenden Microsoft-Lager zählen würde. Die Konsole hat mich in erster Linie in Punkto Hardware und Netzwerkfähigkeit überzeugt [Ruef 2003] – Unzählige Stunden habe ich mich schon, zum Leidwesen meiner Freundin, mit der Konsole vergnügt (Sie spielt zwar auch zwischendurch und sogar nicht selten besser als ich!).

Letzte Woche habe ich mir das Fun-Rennspiel „Burnout 3 - Takedown“ aus dem Hause Electronic Arts (<http://www.ea.com>), ein vor allem bezüglich Sportspielen (z.B. FIFA Football) sehr bekannter Game-Publisher, geholt.

Schon nach wenigen Stunden viel mir auf, wie sehr dieses Spiel ernstzunehmende Entwicklungsmängel aufweist. Dies fing schon bei der fehlerhaften Spracherkennung an (das Spiel läuft auf Französisch, obwohl ich meine

Konsole auf Englisch eingestellt habe). Ebenso ist die Möglichkeit der Joypad-Vibration zwar im Menu vorhanden und aktivierbar – Das Pad bleibt aber stumm, unabhängig von der gewählten Einstellung. Auch und ganz besonders das Online-Spiel bereitete mir Kopfschmerzen: Verbindungsabbrüche en masse, Server, die sich nicht starten lassen und nicht nachvollziehbare Probleme bei der Sprachübertragung trüben den Spielspass ungemain. („Hallo, kannst Du mich hören?“)

Ich war jedoch nicht der einzige, der sich über derlei Fehler, die eindeutig auf Schwächen in der Entwicklung zurückzuführen sind, aufregt. In den jeweiligen Foren, in denen ich meinem Unmut Luft gemacht habe, fand ich überwiegend Zustimmung von Leuten, die die gegenwärtige Lage ebenfalls nicht akzeptieren wollen [Ruef 2004].

Nur wenige Tage nach dem Erscheinen des Spiels hat Electronic Arts nun Patches angekündigt, die zu einer Behebung der besagten Mängel beitragen sollen (einige Dinge müssen scheinbar serverseitig gelöst werden). Zwar ist dieser Aufwand nach einer Herausgabe des Produkts lobenswert, doch hätte ich mir viel lieber ein schon bei der Veröffentlichung „fertiggestelltes“ Spiel gefreut.



Der Konsolen-Markt nimmt immer mehr Züge der PC-Industrie an. Halbfertige Software wird auf den Kunden losgelassen, da man sie ja sowieso später mittels Patches und Service Packs nachbessern kann. Die Benutzer werden so zu hilflosen Beta-Testern degradiert, die sich für teures Geld über fehlerhafte Lösungen ärgern dürfen.

Klar, mein Beispiel zielt in erster Linie auf den Bereich der Spielekonsolen ab. Doch im Software- und Security-Bereich sind Patches schon lange zu einem wichtigen Bestandteil im Lebenszyklus eines Produkts geworden.

Irgendwie haben Patches also immer einen faden Beigeschmack – Und wir haben die Problematik des Testings vor der Installation der Bugfixes auf produktiven Systemen noch gar nicht miteinbezogen. Müsste ich spontan ein Wort bezüglich Patches assoziieren, ich würde wohl „Fluch“ wählen.

Und wahrhaftig gefährlich und mühsam wird es spätestens dann, wenn voraussichtlich mit IPv6 der vernetzte Haushalt Einzug halten wird. Viel Spass, wenn sich Ihr Kühlschrank oder die Alarmanlage aufgrund eines Bugs alle paar Stunden von selber abschaltet. Aber das ist ja gar nicht so schlimm, denn der erste Patch, der folgt sogleich...

Für die Hersteller wäre es also, um den Kunden nicht nur kurzfristig für sich gewinnen zu können, ebenso wichtig, Qualitätsstandards einzuhalten und weitsichtig zu denken. Erweiterte Protokollierungen, um dadurch ein umfassendes Log-Management realisieren zu können, wäre ein im Betrieb und Sicherheitsbereich bestimmt gerne gesehenes Feature. Doch das schnelle Geld ist verlockender weder zufriedene Kunden, auch wenn das wirtschaftlich gesehen nicht wirklich optimal erscheint.

Dem Kunden bleibt so dann nur noch die Möglichkeit, den Herstellern Druck zu machen. Dies kann leider nur durch entsprechende Fehlerbenachrichtigungen und der Drohung des Boykotts geschehen. Dies bedeutet jedoch Mehraufwand, den nur die wenigsten Anwender auf sich nehmen wollen. Viele meinen nämlich, dass das entweder so hingenommen werden sollte oder in Zukunft wahrscheinlich alles besser wird. Das kann und will ich so jedoch nicht akzeptieren!

Marc Ruef <maru@scip.ch>
Security Consultant
Zürich, 18. September 2004

2. scip AG Informationen

2.1 Attack Tool Kit

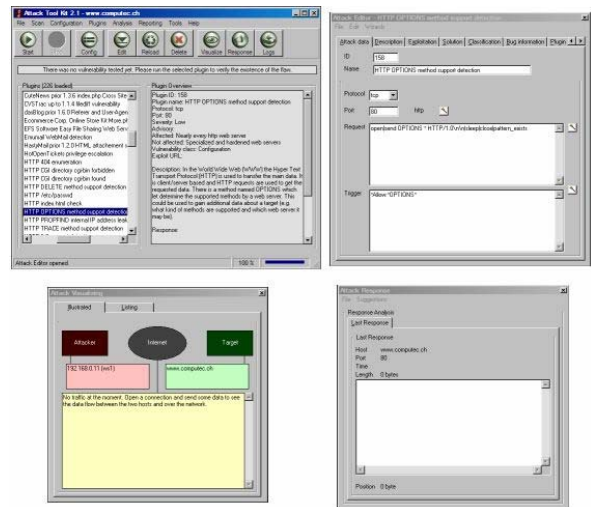
Die Version 2.1 des [Attack Tool Kit](#) ist nun fertiggestellt und zum Download freigegeben.

Die durch Herrn Marc Ruef, Security Consultant der scip AG, programmierte Software, erlaubt dem Anwender die konkrete Nachprüfung gefundener Schwachstellen (z.B. durch Nessus). Dank der Integration des Attack Tool Kit - Attack Editors, können eigene Checks erstellt oder auch

scip monthly Security Summary
Marc Ruef & Simon Zumstein
scip_mss-19_09_2004-1.doc



bestehende Routinen den jeweiligen Gegebenheiten der zu überprüfenden Infrastruktur angepasst werden.



Auch aus diesem Grund ist, bei scip AG Penetration Test oder Security Audits, das Attack Tool Kit ein fester Bestandteil des Testprozederes.

Die Güte des Programmes hat sich seit seiner erstmaligen Veröffentlichung [scip 2004] enorm erhöht. So dass das Programm, in seiner neusten Version, gar durch unsere Mitbewerber angewandt wird!

Ebenfalls die Fachpresse (z.B. [Heise](#)) wurde, selbstständig, auf das Attack Tool Kit aufmerksam und vergibt Höchstnoten.

Detailliertere Informationen finden Sie auf der Projektwebseite: [Attack Tool Kit](#).

2.2 Workshops

September 2004

23.09.2004

[Intrusion Prevention](#) [IPVE03]

Das scip AG Workshop-Portfolio finden Sie auf unserer Firmenwebseite <http://www.scip.ch>.

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 Mozilla bis 1.7.3, Firefox bis 1.0PR und Thunderbird bis 0.8 lange Links ohne ASCII Pufferüberlauf
- 3.2 Microsoft verschiedene Produkte JPEG GDI+ Parsing Pufferüberlauf
- 3.3 Microsoft Office WordPerfect Converter Pufferüberlauf
- 3.4 Squid bis 2.5.STABLE6 clientAbortBody() Denial of service
- 3.5 Apache bis 2.0.50 mod_ssl SSL-Verbindung abrechnen Denial of Service
- 3.6 MIT Kerberos V5 1.2.2 bis 1.3.4 ASN.1 BER Denial of Service
- 3.7 MIT Kerberos V5 1.2.8 bis 1.3.4 krb524d krb5_free_ticket() doppeltes Speicher freigeben Programmcode ausführen
- 3.8 MIT Kerberos V5 bis 1.3.1 krb5_rd_cred() doppeltes Speicher freigeben Programmcode ausführen
- 3.9 MIT Kerberos V5 bis 1.3.4 KDC doppeltes Speicher freigeben Programmcode ausführen
- 3.10 Samba bis 2.2.11 FindNextPrintChangeNotify() bevor FindFirstPrintChangeNotify() Denial of Service
- 3.11 Cisco IOS bis 12.0(3) Telnet spezielle TCP-Verbindung Denial of Service
- 3.12 Cisco Secure Access Control Server bis 3.2(3) Web-Interface schwache Authentisierung
- 3.13 Symantec verschiedene Firewall-Produkte ISAKMPd unbekannt Denial of Service
- 3.14 Netscape Network Security Services Library SSL2 Hello-Nachrichten Pufferüberlauf
- 3.15 Verschiedene Webbrowser iframe rekursives Laden Denial of Service
- 3.16 KDE Konqueror bis 3.2.3 Cross Domain Cookie Injection

3.1 Mozilla bis 1.7.3, Firefox bis 1.0PR

und Thunderbird bis 0.8 lange Links ohne ASCII Pufferüberlauf

Einstufung: **kritisch**
 Remote: Ja
 Datum: 14.09.2004
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=838>

Das Mozilla-Projekt versucht open-source Webbrowser zur Verfügung zu stellen. Der Mozilla Webbrowser bzw. seine Ableger erlangten seit der Veröffentlichung der ersten offiziellen Versionen immer mehr Akzeptanz, kann jedoch in Punkto Marktanteile mit den anderen Grössen des Genres noch nicht mithalten. Im Bugzilla Bug 256316 wird eine von Mats Palmgren und Gael Delalleau ausgemachte Pufferüberlauf-Schwachstelle festgehalten. Überlange Links, die Non-ASCII Zeichen enthalten, können zur Ausführung beliebigen Programmcodes führen. Um die Schwachstelle zu analysieren wurde ein entsprechender proof-of-concept Exploit im Initial-Posting umgesetzt. Die Schwachstelle wurde in Mozilla 1.7.3, Firefox 1.0PR und Thunderbird 0.8 behoben. Als Workaround wird empfohlen, auf das Folgen von Links unbekannter Herkunft zu verzichten.

Expertenmeinung:

Ein Angriff auf einen Webbrowser über manipulierende Links ist natürlich ein Honigschlecken für jeden Angreifer. Da Links die Hauptfunktion des Web-Browsers ermöglichen, ist es deshalb fragwürdig, wie sich da ein solch schwerwiegender Fehler einschleichen konnte. Es scheint deshalb unbestritten, dass dieser Bug in gewisser Masse Geschichte geschrieben hat.

3.2 Microsoft verschiedene Produkte JPEG GDI+ Parsing Pufferüberlauf

Einstufung: **sehr kritisch**
 Remote: Ja
 Datum: 14.09.2004
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=833>

Microsoft ist der weltweit grösste Softwarehersteller mit Hauptsitz in Redmond, einem Vorort von Seattle (US-Bundesstaat Washington). Das Unternehmen wurde 1975 von Bill Gates und Paul Allen gegründet [<http://de.wikipedia.org/wiki/Microsoft>]. Der Hersteller gibt in seinem Microsoft Security Bulletin MS04-028 eine schwerwiegende Pufferüberlauf-Schwachstelle in Gdiplus.dll bekannt. Diese DLL wird für das Interpretieren und Darstellen von JPEG-Dateien genutzt. Ein Angreifer kann mittels einem korrupten JPEG-

Bild über Software, die diese Bibliothek ansteuert, beliebigen Programmcode ausführen lassen. Es ist bisher nicht genau bekannt, ob dabei die Rechte des eingeloggten Benutzers oder diejenigen des Systems vom Angreifer geerbt werden. Heise berichtet von Benutzer-Rechten. Eine Reihe von Microsoft-Produkten machen von der besagten DLL-Gebrauch, wie zum Beispiel Microsoft Windows XP und Server 2003, Office 2003 und XP, Internet Explorer 6, Visio 2002 und 2003, Visual Studio .NET 2002 und 2003 sowie andere unbekanntere Microsoft-Produkte. Microsoft hat für alle verwundbaren Komponenten Patches zur Verfügung gestellt. Anwender können diese über die Links in den Bulletins beziehen oder über den Windows-Update-Dienst installieren. Unter <http://support.microsoft.com/default.aspx?scid=k b;EN-US;873374> hat Microsoft ein Tool bereitgestellt, mit dessen Hilfe die Schwachstelle identifiziert und direkt ein Bugfixing im System umgesetzt werden kann. In Bezug auf das ebenfalls betroffene Microsoft Outlook wird angeraten, Emails lediglich als Plaintext anzeigen zu lassen; also auf den Einsatz einer HTML- bzw. RTF-Darstellung zu verzichten. Digital signierte Emails werden bei Outlook aber auch in dieser Einstellung weiterhin im Original-Format, also unter Umständen als HTML oder RTF, angezeigt. Nicht betroffen sind unter anderem Windows 98, NT, 2000 und Windows XP mit Service Pack 2 sowie der Internet Explorer 5.01 und 5.5. Die Installation des Service Pack 2 von Microsoft Windows XP wird also für die Unternehmen erstmals wirklich erforderlich.

Expertenmeinung:

Eine wahrhaftig kritische Schwachstelle, da der Pufferüberlauf nahezu jedes moderne Windows-System betrifft. Die Interpretation von JPEG-Bildern ist üblich, mitunter auch über HTML im Mail-Verkehr. Spammer und Wurm-Entwickler werden wohl in den kommenden Tagen entsprechende Exploits entwickelt haben, um die Schwachstelle für ihre Zwecke ausnutzen zu können. Grossflächige Kompromittierungen von Systemen wird die Folge sein. Gegenmassnahmen sind unverzüglich umzusetzen, um verheerende Ausmasse an Schäden wie im Falle des Blaster-Wurms zu verhindern.

3.3 Microsoft Office WordPerfect Converter Pufferüberlauf

Einstufung: **kritisch**
 Remote: Indirekt
 Datum: 14.09.2004
 scip DB: [http://www.scip.ch/cgi-](http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=832)

[bin/smss/showadvf.pl?id=832](http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=832)

Microsoft Office ist eine sehr populäre kommerzielle Office-Suite der bekannten Firma aus Redmond. Teil dieses Pakets sind beispielsweise die Textverarbeitung Word, die Tabellenkalkulation Excel und die Datenbank Access. Die jeweiligen Komponenten sind in der Lage Dateien des Konkurrenzprodukts WordPerfect für eine Weiterverarbeitung zu konvertieren. Microsoft berichtet nun in ihrem Security Bulletin MS04-027 von einem Pufferüberlauf im besagten Converter, der beim Öffnen eines korrupten Dokuments das Ausführen beliebigen Programmcodes mit den Rechten des gegenwärtigen Benutzers ausführen lässt. Von der Schwachstelle betroffen sind alle Microsoft- bzw. Office-Elemente, die den besagten Converter mitführen oder ansteuern. Für die jeweiligen Produkte hat Microsoft dedizierte Patches zum Download bereitgestellt. Im Advisory von Microsoft werden ebenfalls einige Workarounds vorgetragen. So wird empfohlen, keine WordPerfect-Dateien auf verwundbaren Systemen zu öffnen. Bestenfalls sollte man den Converter über die Software-Installation der Systemsteuerung entfernen (Office Shared Feature). Sodann könne man auf ein alternatives Produkt für das Konvertieren von WordPerfect-Dateien zurückgreifen.

Expertenmeinung:

Die Schwachstelle ansich wäre nichts besonderes, wenn nicht die sehr gerne in allen Bereichen eingesetzte Office-Suite von Microsoft betroffen wäre. Die Möglichkeit eines Pufferüberlaufs könnte durchaus für Viren-Programmierer interessant sein, die diese Facette für das Umsetzen und Erweitern ihres Codes einsetzen wollen. Das Erscheinen eines Wurms, der den besagten Pufferüberlauf ausnutzt, ist nur noch eine Frage der Zeit. Unternehmen und auch Privatpersonen täten gut daran, sich mit der Umsetzung der vorgeschlagenen Gegenmassnahmen auseinanderzusetzen.

3.4 Squid bis 2.5.STABLE6 clientAbortBody() Denial of service

Einstufung: **kritisch**
 Remote: Ja
 Datum: 13.09.2004
 scip DB: [http://www.scip.ch/cgi-](http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=828)

Squid ist ein open-source Projekt, das einen freien und hochskalierbaren Proxy für Unix-Systeme zur Verfügung stellt. Es werden Protokolle wie HTTP und FTP sowie

Funktionalitäten wie SSL-Unterstützung, Cache-Hierarchien und Zugriffskontrolllisten bereitgestellt. d3thStaR weist in seinem kurzen und technischen Advisory auf eine Denial of Service-Möglichkeit bezüglich Null-Pointer in der Funktion `clientAbortBody()` hin. Der Angriff kann durch eine korrupte Webseite umgesetzt werden. Zur Verifizierung der Schwachstelle kann das Attack Tool Kit Plugin 218 herangezogen werden [<http://www.computec.ch/projekte/atk/>]. Für die Squid Versionen 2.5.STABLE5 und STABLE6 wurden entsprechende Patches herausgegeben.

Expertenmeinung:

Ein interessanter Angriff, der er von Extern über einen regulären Datenstream ausgeführt werden kann, was relativ selten ist. Popularität wird der Angriff eher weniger erreichen - So wird er voraussichtlich eher im Zusammenhang mit anderen, konstruktiven und grösser angelegten Attacken im Verbund genutzt werden.

3.5 Apache bis 2.0.50 mod_ssl SSL-Verbindung abbrechen Denial of Service

Einstufung: **kritisch**

Remote: Ja

Datum: 09.01.2004

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=821>

Apache ist ein populärer, freier open-source Webserver, der für viele verschiedene Plattformen erhältlich ist. Red Hat berichtet in ihrem Advisory RHSA-2004:349-10 von einer Denial of Service-Schwachstelle im für SSL zuständigen Modul `mod_ssl`. Wird eine etablierte SSL-Verbindung an einem bestimmten Punkt abgebrochen, könne das Modul in einen unendlichen Loop verfallen. Ein Angreifer könnte so Ressourcen aufbrauchen und das System so zum Absturz bringen. Es sind keine genauen technischen Details oder ein Exploit zur Schwachstelle bekannt. Zur Verifizierung der Schwachstelle kann das Attack Tool Kit Plugin 137 herangezogen werden [<http://www.computec.ch/projekte/atk/>]. Red Hat hat Patches für die betroffene Schwachstelle herausgegeben. Das Apache Team selbst und andere Linux Distributoren werden voraussichtlich in den kommenden Tagen diesem Beispiel folgen.

Expertenmeinung:

Der Apache Webserver ist einer der populärsten, weshalb diese Schwachstelle grundsätzlich ein hohes Mass an Interesse geweckt hat. Limitierend ist beim Angriff natürlich, dass dieser

nur über SSL umgesetzt werden kann und er lediglich destruktiver Natur ist. Dies wird aber Skript-Kiddies nicht davon abhalten nach dem Erscheinen eines entsprechenden Exploits flächendeckende Scans und Angriffe anzustreben. Das Umsetzen von Gegenmassnahmen erscheint daher bei exponierten Systemen als dringend.

3.6 MIT Kerberos V5 1.2.2 bis 1.3.4 ASN.1 BER Denial of Service

Einstufung: **kritisch**

Remote: Ja

Datum: 31.08.2004

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=818>

Kerberos ist ein etabliertes System zur sicheren Authentisierung von Benutzern und Systemen. Auf praktisch allen wichtigeren Plattformen sind entsprechende Implementierungen gegenwärtig. Wie das MIT meldet, existiert eine Programmierschwachstelle in MIT Kerberos V5 1.2.8 bis 1.3.4. Durch das fehlerhafte mehrfache freigeben von Speicher (engl. freeing) durch die Decoding-Funktion von ASN.1 für BER kann ein nicht authentisierter Benutzer mittels korruptem Paket verwundbaren System zum Absturz bringen. Cisco informiert seine Kunden in einem eigenen Advisory über das Kerberos-Problem. Demnach sind nur die VPN-Konzentratoren der 3000er-Serie betroffen. Produkte mit IOS und Cisco's PIX sind nicht verwundbar, da sie nicht auf der MIT-Implementierung basieren. Es sind bisher keine technischen Details zur Schwachstelle oder ein Exploit bekannt. Das MIT hat einen Patch für die betroffene Kerberos-Version herausgegeben. Der Fehler wird in den kommenden Versionen nicht mehr vorhanden sein. Zusätzlich sollte mittels durchdachtem Zonenkonzept und Firewalling der unerwünschte Zugriff auf den Kerberos-Dienst verhindert werden.

Expertenmeinung:

Die gleichzeitig in Kerberos5 publizierten Schwachstellen haben mit Sicherheit das Interesse potentieller Angreifer geweckt. Nicht nur Skript-Kiddies werden die produktiven Lücken für ihre Zwecke ausnutzen wollen. Sobald ein Exploit die Runde macht, muss mit einer Vielzahl an Scans und Angriffsversuchen gerechnet werden. Exponierte Systeme gilt es deshalb unverzüglich zu schützen.

3.7 MIT Kerberos V5 1.2.8 bis 1.3.4 krb524d krb5_free_ticket() doppeltes Speicher freigeben

Programmcode ausführen

Einstufung: **kritisch**
 Remote: Ja
 Datum: 31.08.2004
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=817>

Kerberos ist ein etabliertes System zur sicheren Authentisierung von Benutzern und Systemen. Auf praktisch allen wichtigeren Plattformen sind entsprechende Implementierungen gegenwärtig. Wie das MIT meldet, existiert eine Programmierschwachstelle in MIT Kerberos V5 1.2.8 bis 1.3.4. Durch das fehlerhafte mehrfache freigeben von Speicher (engl. freeing) durch die Funktion `krb5_free_ticket()` kann ein nicht authentisierter Benutzer Programmcode auf einem verwundbaren System mit den Rechten von Kerberos ausführen. Das Erlangen erweiterter Rechte ist die Folge. Cisco informiert seine Kunden in einem eigenen Advisory über das Kerberos-Problem. Demnach sind nur die VPN-Konzentratoren der 3000er-Serie betroffen. Produkte mit IOS und Cisco's PIX sind nicht verwundbar, da sie nicht auf der MIT-Implementierung basieren. Es sind bisher keine technischen Details zur Schwachstelle oder ein Exploit bekannt. Das MIT hat einen Patch für die betroffene Kerberos-Version herausgegeben. Der Fehler wird in den kommenden Versionen nicht mehr vorhanden sein. Zusätzlich sollte mittels durchdachtem Zonenkonzept und Firewalling der unerwünschte Zugriff auf den Kerberos-Dienst verhindert werden.

Expertenmeinung:

Die gleichzeitig in Kerberos5 publizierten Schwachstellen haben mit Sicherheit das Interesse potentieller Angreifer geweckt. Nicht nur Skript-Kiddies werden die produktiven Lücken für ihre Zwecke ausnutzen wollen. Sobald ein Exploit die Runde macht, muss mit einer Vielzahl an Scans und Angriffsversuchen gerechnet werden. Exponierte Systeme gilt es deshalb unverzüglich zu schützen.

3.8 MIT Kerberos V5 bis 1.3.1 `krb5_rd_cred()` doppeltes Speicher freigeben Programmcode ausführen

Einstufung: **kritisch**
 Remote: Ja
 Datum: 31.08.2004
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=816>

Kerberos ist ein etabliertes System zur sicheren Authentisierung von Benutzern und Systemen.

Auf praktisch allen wichtigeren Plattformen sind entsprechende Implementierungen gegenwärtig. Wie das MIT meldet, existiert eine Programmierschwachstelle in MIT Kerberos V5 bis 1.3.4. Durch das fehlerhafte mehrfache freigeben von Speicher (engl. freeing) durch die Funktion `krb5_rd_cred()` kann ein nicht authentisierter Benutzer Programmcode auf einem verwundbaren System mit den Rechten von Kerberos ausführen. Das Erlangen erweiterter Rechte ist die Folge. Cisco informiert seine Kunden in einem eigenen Advisory über das Kerberos-Problem. Demnach sind nur die VPN-Konzentratoren der 3000er-Serie betroffen. Produkte mit IOS und Cisco's PIX sind nicht verwundbar, da sie nicht auf der MIT-Implementierung basieren. Es sind bisher keine technischen Details zur Schwachstelle oder ein Exploit bekannt. Das MIT hat einen Patch für die betroffene Kerberos-Version herausgegeben. Der Fehler wird in den kommenden Versionen nicht mehr vorhanden sein. Zusätzlich sollte mittels durchdachtem Zonenkonzept und Firewalling der unerwünschte Zugriff auf den Kerberos-Dienst verhindert werden.

Expertenmeinung:

Die gleichzeitig in Kerberos5 publizierten Schwachstellen haben mit Sicherheit das Interesse potentieller Angreifer geweckt. Nicht nur Skript-Kiddies werden die produktiven Lücken für ihre Zwecke ausnutzen wollen. Sobald ein Exploit die Runde macht, muss mit einer Vielzahl an Scans und Angriffsversuchen gerechnet werden. Exponierte Systeme gilt es deshalb unverzüglich zu schützen.

3.9 MIT Kerberos V5 bis 1.3.4 KDC doppeltes Speicher freigeben Programmcode ausführen

Einstufung: **kritisch**
 Remote: Ja
 Datum: 31.08.2004
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=815>

Kerberos ist ein etabliertes System zur sicheren Authentisierung von Benutzern und Systemen. Auf praktisch allen wichtigeren Plattformen sind entsprechende Implementierungen gegenwärtig. Wie das MIT meldet, existiert eine Programmierschwachstelle in MIT Kerberos V5 bis 1.3.4. Durch das fehlerhafte mehrfache freigeben von Speicher (engl. freeing) kann ein nicht authentisierter Benutzer Programmcode auf einem verwundbaren System mit den Rechten von Kerberos ausführen. Das Erlangen erweiterter Rechte ist die Folge. Cisco informiert

seine Kunden in einem eigenen Advisory über das Kerberos-Problem. Demnach sind nur die VPN-Konzentratoren der 3000er-Serie betroffen. Produkte mit IOS und Cisco's PIX sind nicht verwundbar, da sie nicht auf der MIT-Implementierung basieren. Es sind bisher keine technischen Details zur Schwachstelle oder ein Exploit bekannt. Das MIT hat einen Patch für die betroffene Kerberos-Version herausgegeben. Der Fehler wird in den kommenden Versionen nicht mehr vorhanden sein. Zusätzlich sollte mittels durchdachtem Zonenkonzept und Firewalling der unerwünschte Zugriff auf den Kerberos-Dienst verhindert werden.

Expertenmeinung:

Die gleichzeitig in Kerberos5 publizierten Schwachstellen haben mit Sicherheit das Interesse potentieller Angreifer geweckt. Nicht nur Skript-Kiddies werden die produktiven Lücken für ihre Zwecke ausnutzen wollen. Sobald ein Exploit die Runde macht, muss mit einer Vielzahl an Scans und Angriffsversuchen gerechnet werden. Exponierte Systeme gilt es deshalb unverzüglich zu schützen.

3.10 Samba bis 2.2.11

FindNextPrintChangeNotify() bevor FindFirstPrintChangeNotify() Denial of Service

Einstufung: **kritisch**
Remote: Ja
Datum: 08.12.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=813>

Samba ist eine freiverfügbare Applikation für das Freigeben von Ressourcen (Datei- und Druckerfreigabe). Wie das Samba Team nun in den Release-Notes für die neue Version 2.2.11 vermerkt hat, existiert in den vorangehenden Versionen eine Denial of Service-Schwachstelle. Dieser tritt dann ein, wenn beim Wechsel eines Druckers zuerst FindNextPrintChangeNotify() ohne ein vorangehendes FindFirstPrintChangeNotify() ausgeführt wird. Wie gemeldet wurde, kann diese Schwachstelle mitunter auch versehentlich durch Microsoft Windows XP mit installiertem Service Pack 2 initiiert werden. Die Schwachstelle wurde von Seiten Samba in 2.2.11 behoben. Ein Firewall-System sollte die Datei- und Druckerfreigabe lediglich in einem geschützten LAN erlauben.

Expertenmeinung:

Diese Schwachstelle ist unschön und wird sicher die Administratoren einiger Netzwerke in Anspruch nehmen. Das Risiko ist aber dennoch

relativ gering, da Samba-Zugriffe meistens nur in LANs möglich sind, hierbei lediglich eine Denial of Service gegen den smbD umgesetzt werden kann und noch keine Exploits erschienen sind.

3.11 Cisco IOS bis 12.0(3) Telnet spezielle TCP-Verbindung Denial of Service

Einstufung: **kritisch**
Remote: Ja
Datum: 27.08.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=812>

Die Firma Cisco hat sich einen Namen mit ihren Netzwerkelementen - Switches und Router - gemacht. Internet Operating System (IOS) wird die Firmware von Cisco-Routern genannt. Wie Cisco in ihrem Dokument 61671 bekannt gibt, existiert eine Denial of Service-Schwachstelle in der Behandlung spezieller TCP-Kommunikationen zu bzw. über Telnet. Vom Angriff betroffen sind sodann Management-Verbindungen auf den Telnet, RSH und SSH. Es sind keine technischen Details oder ein Exploit zur Schwachstelle bekannt. Cisco gibt in ihrem Advisory bekannt, dass noch kein Fix existiert, jedoch an diesem gearbeitet werde. Als Workaround gilt es Zugriffe auf verwundbare Ports zu blockieren. Alternativ kann der Telnet-Server auch gleich gänzlich auf einem verwundbaren System deaktiviert werden.

Expertenmeinung:

Die Vielzahl der in Cisco-Produkten in den letzten Tagen gefundenen Schwachstellen, die zum Teil kritischer Natur sind, sind irgendwie beängstigend. Gerade ein einfach auszunutzender Fehler wie dieser wird den Skript-Kiddies und Mochtegern-Hackern in den kommenden Wochen ein bisschen Spass bescheren. Entsprechende Angriffe, vor allem in topologisch flachen und nur unzureichend mittels Firewalls geschützten LANs von KMUs, werden sicher vermehrt auftreten. Das Anstreben und Umsetzen der gegebenen Schutzmassnahmen ist deshalb unverzüglich anzuraten.

3.12 Cisco Secure Access Control Server bis 3.2(3) Web-Interface schwache Authentisierung

Einstufung: **kritisch**
Remote: Ja
Datum: 25.08.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=810>

Der Cisco Secure Access Control Server für Windows (ACS Windows) und die Cisco Secure Access Control Server Solution Engine (ACS Solution Engine) ermöglichen Authentisierung, Authorisierung und Accounting (AAA) von Netzwerkgeräten wie Cisco PIX und Router in einem Netzwerk. Cisco gibt in ihrer Meldung 61603 fünf verschiedene mehr oder weniger kritische Schwachstellen in der besagten Lösung bekannt. Die unter der Bug-ID CSCef05950 geführte betrifft das web-basierte Interface names CSAdmin, das standardmässig über den TCP-Port 2002 angesprochen werden kann [<http://www.cisco.com/pcgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef05950>]. Wird ein Benutzer authentisiert, wird die Verbindung über einen kurzlebigen Port geführt. Den weiteren Verlauf der authentisierten Sitzung wird lediglich über die Quell-IP-Adresse des authentisierten Benutzers getätigt. Ein Angreifer könnte mittels Portscanning und IP-Spoofing also eine authentisierte Sitzung übernehmen. Die Schwachstelle betrifft Cisco Secure Access Control Server bis 3.2(3) und wurde durch einen entsprechenden Fix, der nur für registrierte Cisco-Benutzer zugänglich ist, behoben.

Expertenmeinung:

Die Vielzahl der in Cisco-Produkten in den letzten Tagen gefundenen Schwachstellen, die zum Teil kritischer Natur sind, sind irgendwie beängstigend. Gerade ein einfach auszunutzender Fehler wie dieser wird den Skript-Kiddies und Möchtegern-Hackern in den kommenden Wochen ein bisschen Spass bescheren. Entsprechende Angriffe, vor allem in topologisch flachen und nur unzureichend mittels Firewalls geschützten LANs von KMUs, werden sicher vermehrt auftreten. Das Anstreben und Umsetzen der gegebenen Schutzmassnahmen ist deshalb unverzüglich anzuraten.

3.13 Symantec verschiedene Firewall-Produkte ISAKMPd unbekanntes Denial of Service

Einstufung: **kritisch**

Remote: Ja

Datum: 24.08.2004

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=804>

Die Firma Symantec ist Herausgeber einiger kommerzieller Firewalling-, Gateway- und VPN-Lösungen. Wie der Hersteller in einzelnen Advisories bekannt gibt, existiert eine nicht näher beschriebene Denial of Service-Schwachstelle im ISAKMPd der Produkte Symantec Enterprise Firewall (SEF) 7.x, Symantec VelociRaptor 1.5,

Symantec Gateway Security 1.x und 2.x sowie Symantec Enterprise VPN 7.x. Ein Angreifer kann vermutlich von remote ein entsprechendes System zum Absturz bringen. Handelt es sich um einen Pufferüberlauf, wäre gar theoretisch das Ausführen beliebigen Programmcodes möglich. Symantec hat Patches für die betroffenen Lösungen herausgegeben.

Expertenmeinung:

Die dedizierten Firewall-Lösungen von Symantec sind vor allem im professionellen Umfeld sehr beliebt. Die ehemals unter dem Namen Symantec Raptor geführte Firewall machte sich vor allem im Bereich des Application-Firewallings einen sehr guten Namen. Eine Vielzahl an Angreifern wird daher ein erhöhtes Interesse für diese Schwachstelle hegen, weshalb in den kommenden Wochen mit dem Erscheinen eines entsprechenden Exploits zu rechnen ist. Vor allem in Umgebungen, in denen ein betroffenes Symantec-Element als Perimeter-Schutz gegen das Internet verwendet wird, sollten unverzüglich Gegenmassnahmen umgesetzt werden.

3.14 Netscape Network Security Services Library SSL2 Hello-Nachrichten Pufferüberlauf

Einstufung: **kritisch**

Remote: Ja

Datum: 23.08.2004

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=803>

Die Netscape Network Security Services Library ist eine gern genutzte Bibliothek für das Umsetzen von SSL-geschützten Verbindungen. Unterstützt werden sowohl SSL1 als auch SSL2. ISS X-Force hat in ihrem Alert 180 (Netscape NSS Library Remote Compromise) einen Pufferüberlauf bei der Verarbeitung von Hello-Nachrichten bei SSL2-Kommunikationen publiziert. Einem Angreifer ist es dadurch möglich, noch vor der entsprechenden Authentisierung eine Denial of Service oder gar beliebigen Programmcode auf dem Server-System auszuführen. Die ganze Bandbreite der professionellen Netscape-Server [<http://secunia.com/advisories/12379/>] aber auch Produkte anderer Firmen, die auf die Bibliothek zurückgreifen (z.B. Sun One/iPlanet [<http://secunia.com/advisories/12378/>]), sind betroffen. Der erfolgreiche Angriff ist aber explizit nur bei Version 2 von SSH möglich. Diese ist beispielsweise beim betroffenen Sun-Produkt standardmässig nicht aktiviert. Netscape hat einen Patch für die besagte Library herausgegeben. ISS weist in ihrem Bulletin

darauf hin, dass ihre Sicherheitslösungen RealSecure Network Sensor und Proventia mit den aktuellsten Updates vor dem Angriff schützen können. Determinieren lässt sich die Schwachstelle ebenfalls mit dem Internet Scanner 7.0 mit XPU 7.35 vom 25. August 2004 (Check namens "SSLv2-Client-Hello-BO").

Expertenmeinung:

Ein sehr interessanter Angriff, weil er eine Reihe professioneller Produkte betrifft und zudem remote ausgenutzt werden kann. Entsprechend ist es nur eine Frage der Zeit, bis erste Exploits die Runde machen werden. In den kommenden Tagen werden Angreifer alles daran setzen, solche für ihre Vorteile umsetzen zu können. Für die Administratoren verwundbarer Systeme heisst dies, so schnell wie möglich den entsprechenden Patch einsetzen oder eine alternative Gegenmassnahme anstreben.

3.15 Verschiedene Webbrowser iframe rekursives Laden Denial of Service

Einstufung: **kritisch**

Remote: Ja

Datum: 24.08.2004

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=801>

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. Opera ist ein freier Webbrowser, der seit den letzten Jahren den beiden Branchenriesen Microsoft Internet Explorer (MS IEX) und Netscape Navigator den Marktanteil streitig macht. Das Mozilla-Projekt versucht einen open-source Webbrowser zur Verfügung zu stellen. Der Mozilla Webbrowser erlangte seit der Veröffentlichung der ersten offiziellen Versionen immer mehr Akzeptanz, kann jedoch in Punkto Marktanteile mit den anderen Grössen des Genres noch nicht ganz mithalten. In einem knappen Posting auf Bugtraq wird eine Denial of Service-Schwachstelle in diesen drei Webbrowsern vorgetragen. Durch das rekursive Laden von C:\Windows\system32\ über ein iframe ist es möglich, die CPU-Auslastung auf 100 % zu treiben. Opera gibt zudem fortwährend die Fehlermeldung "The address type is unknown or unsupported" aus, so dass ein normales Weiterarbeiten gänzlich verhindert wird. In dem Posting ist ein Link zu einem proof-of-concept Exploit enthalten. Es ist damit zu rechnen, dass die jeweiligen Browser-Hersteller mit Bugfixes oder Upgrades reagieren werden. Als Workaround sollten zwischenzeitlich nicht verwundbare Alternativen eingesetzt werden.

Expertenmeinung:

Derlei Denial of Service-Attacken sind sowohl in ihrer Umsetzung als auch in ihrem Ziel sehr primitiv. Es ist nun eine Philosophie-Frage, ob Schwachstellen dieser Art genau deshalb nicht vorkommen dürfen oder ob sie als Kavaliersdelikt der Entwickler angesehen werden müssen. Rekursive Angriffe sind mühsam zu verhindern, aber nicht unmöglich. Es bleibt also zu hoffen, dass sich die Entwickler einen Ruck geben und sich dieser unangenehmen Problematik annehmen.

3.16 KDE Konqueror bis 3.2.3 Cross Domain Cookie Injection

Einstufung: **kritisch**

Remote: Ja

Datum: 23.08.2004

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=800>

Konqueror ist ein immer populärer werdender grafischer Webbrowser für den allseits beliebten KDE Window Manager. KDE ist die standardmässig installierte grafische Oberfläche bei so mancher Linux-Distribution (z.B. SuSE). Durch einen Designfehler ist es einem Angreifer, der Informationen über bestehende Cookies hat, eben solche von anderen Domains auszulesen oder zu überschreiben. Davon betroffen sind länderspezifische Secondary Top-Level-Domains mit mehr als zwei Zeichen (z.B. .plc.uk). Die Domänen .com, .net, .mil, .org, .gov, .edu und .int sind für diesen Angriff grundsätzlich nicht anfällig. Von der Schwachstelle betroffen ist KDE Konqueror bis 3.2.3 - Patches für die betroffenen Versionen sowie eine aktualisierte Konqueror-Version stehen zum Download bereit.

Expertenmeinung:

Dieses Problem ist grundsätzlich nicht neu, denn so hatten schon eine Vielzahl anderer Browser mit diesem zu kämpfen. Beispielsweise ist auch der Netscape Navigator in seinen frühen Versionen gegen derlei Angriffe auf Cookies verwundbar. Es verwundert daher umso mehr, dass das KDE Team sich der Risiken nicht bewusst war und entsprechende Vorsichtsmassnahmen umgesetzt hat.

4. Interview

4.1 Interview mit Uwe Velten – Leiter Produkte- und Softwareentwicklung – bei der Firma abylonsoft

Interviewer: Marc Ruef <maru@scip.ch>

scip AG: Hallo Uwe. Danke, dass Du Dir die Zeit fuer ein Interview mit mir nimmst.

Uwe Velten: Hi Marc, no Problem. Hoffe, Du bist von meinen Antworten nicht zu sehr enttäuscht.

Auf logosec.de hast Du einige Publikationen zum Thema Chipkarten aufliegen. Wie siehst Du die Zukunft der kleinen Plastikkarten?

Im Prinzip sind Chipkarten eine feine Sache, die schon heute hilfreiche Dienste im Bereich der Authentifizierung, Bezahlung oder Speicherung von Daten bieten. Jedoch wird die Plastikkarte mit Chip noch einen harten Weg vor sich haben, um sich auch im Privatbereich durchzusetzen. Teilweise werden mittlerweile in Ostdeutschland aus Kostengründen EC-Karten wieder ohne Chip und nur noch mit Magnetstreifen ausgegeben. Auch die Geldkartenfunktion der EC-Karte war ein Flop. Leider gab es auch Unstimmigkeiten zwischen Industrie und Staat, wer letztendlich für eine flächendeckende Einführung einer Zertifikatschipkarte zu sorgen hat. Die seit Jahren angepriesene Bürgerkarte hat sich aufgrund von leeren Staatskassen und sicherlich fehlenden Anwendungen nicht durchgesetzt. Mittlerweile sitzt auch bei den Banken das Geld nicht mehr so locker, sodass auch hier zahlreiche Projekte zur Einführung von Zertifikatschipkarten (beispielsweise für HBCI-Banking) stark reduziert oder sogar ganz eingestellt wurden. Ferner wird entgegen meiner früheren Vermutungen, immer noch nicht jeder PC mit einem Chipkartenleser ausliefert. Vermutlich sehen die Hersteller wegen der unterschiedlichen USB-Devices hier auch nicht mehr den Bedarf für den Consumermarkt. Gerade bei USB-Token hat sich ein breites Angebot mit alternativen zur Chipkarte etabliert, wie beispielsweise die Firma Aladdin mit Ihren eToken Pro zeigt. Plastikkarten werden inzwischen nur noch überwiegend bei von Krankenkassen und Kundenkarten a la Payback & Co eingesetzt. Deren Vorteil für die Menschheit sehe ich allerdings eher als gering. Nur die Marktforschung und Werbeindustrie werden hieraus Ihren Nutzen ziehen. Wenn

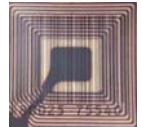


dieser Bereich noch weiter ausgebaut oder sogar mit anderen Systemen, wie Bankkarte oder Handy vernetzt wird, dann ist es nicht mehr weit zum gläsernen Kunden. Da sehe ich doch eher die Bürgerkarte oder den elektronischen Personalausweis als sinnvolle Einsatzmöglichkeit für Chipkarten, wenn auch hier der Datenschutz einen hohen Stellenwert haben sollte.

RFID

(<http://www.heise.de/tr/aktuell/meldung/49197>) ist ein heiss diskutiertes Thema. Sind die Risiken fuer die Privatsphaere der Nutzer existent oder reagieren die Datenschuetzer zu sensibel?

Viele neue Techniken können sowohl zum Vor- als auch zum Nachteil der Nutzer eingesetzt werden. Beispielsweise kann Schießpulver zum zivilen Sprengen und für Gewehrpatronen eingesetzt werden oder mithilfe der Gentechnik könnten Erbkrankheiten eliminiert werden, aber es können auch spezielle Erreger für die Kriegsführung entwickelt werden. Dies ist bei RFID genauso der Fall. Die Öffentlichkeit muss sicherlich ein wachsames Auge auf die Verwendung dieser Technik werfen, damit nicht alle theoretischen Einsatzmöglichkeiten durchgeführt werden. Bei einer Implantation von RFID-Chips unter die Haut von Menschen oder Tieren für deren Authentifizierung würden wir George Orwells Phantasie aus 1984 sicherlich schon recht nahe kommen. Gegen einen Einsatz dieser Technik im Logistikbereich ist dagegen sicherlich nichts einzuwenden. Jedoch zeigt die Geschichte, dass alle Errungenschaften auch immer gegen die Menschen eingesetzt werden und so sehe ich das auf Dauer auch beim RFID-Chip.



Wie ist Deine Einstellung zur akademischen Laufbahn im Bereich der Informatik? Findest Du, dass alle guten Informatiker grundsätzlich Universitäts- bzw. Hochschulabgaenger sind?

Nein auf keinen Fall. Ich habe damals neben der Elektrotechnik auch ein Informatik-Studium angefangen. Allerdings habe ich schon bald gemerkt, dass das Studium nichts mit der Realität zu tun hat (kann sicherlich nicht verallgemeinert werden). Der Stoff war meiner Meinung viel zu theoretisch und kaum praxisbezogen. Außerdem wurden allgemeine abstrakte Programmiersprachen unterrichtet, die in den 70er und 80er verwendet wurden, heute aber keinerlei Nutzen mehr besitzen, außer

vielleicht einen pädagogischen. Die besten Programmierer sind eh die Autodidakten, wie man an der Großzahl guter Softwareentwickler aus Osteuropa, China oder Indien sieht. Wenn wir für unsere Firma einen Entwickler suchen, so spielt es keine Rolle, ob dieser nur einen Hauptschulabschluss oder ein Studium auf einem beliebigen Segment besitzt. Gerade im Bereich Informatik sind das persönliche Interesse an dem Gebiet und die Herausforderung wichtiger, als ein gutes akademisches Zeugnis.

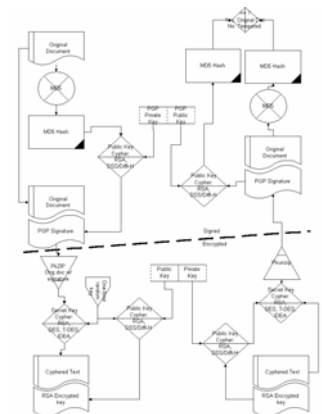
Simon Sing schreibt in seinem Bestseller "The Code Book", dass der erste Weltkrieg der Krieg der Chemiker war (Gas), der zweite Weltkrieg der Krieg der Physiker (Atombombe) war und der dritte Weltkrieg der Krieg der Mathematiker (Kryptologie) sein wird. Teilst Du diese Voraussicht?

Auch der 2. Weltkrieg wurde bereits durch die Entschlüsselung der Chiffriermaschine Enigma entscheidend beeinflusst. In einem möglichen 3. Weltkrieg würde die Kryptographie und Kryptonanalyse sicherlich einen wesentlichen kriegsentscheidenden Punkt ausmachen. Eine Kostprobe auf den Krieg von morgen haben wir ja bereits im Balkan, Afghanistan oder Irak bekommen. Militärische Auseinandersetzungen sind heute vollkommen technisiert und der einzelne Soldat nur noch ein Punkt auf dem Bildschirm. Unsere selbsternannte Weltpolizei setzt ausschließlich auf technologische Kriegsführung, auch wenn allein mit Technik sich sicherlich kein Krieg gewinnen lässt. Guerillataktik wird nicht mehr nur in dunkelnden Gassen geführt, sondern verlagert sich stärker als bisher auf das Internet. Pläne, Taktiken und Absprachen werden über verschlüsselte Kommunikationskanäle im Internet ausgetauscht. Besonders aus diesem Grund wollen einige Staaten (voran die USA) die kryptografischen Verfahren kontrollieren und die Kontrolle darüber nicht aus den Händen verlieren. Die moderne Kriegsführung basiert auf einer gut ausgebauten kommunikativen Infrastruktur, die damit auch für Angreifer immer interessanter wird.

Der Einsatz von PGP (Pretty Good Privacy) haelt sich trotz der phaenomenalen Technologie in Grenzen. Was sind Deines Erachtens die Gruende fuer das Ausbleiben flaechendeckender Popularitaet dieser Loesung?

Bei der asymmetrischen Verschlüsselung handelt es sich um eine wirklich ausgereifte und meiner Meinung nach überlegene Technik. Aus

diesem Grund haben wir mit unserer Softwarefirma abylonsoft (www.abylonsoft.de) bisher voll auf die RSA-Verschlüsselung nach dem PKCS-Standard auf Basic von X.509 Zertifikaten gesetzt. Wir versuchen diese Technik in unsere Softwarelösungen (z. B. im Paket 'abylon protection manager (apm)') so anwenderfreundlich wie möglich umzusetzen. Der Vorteil der asymmetrischen Verschlüsselung mit einem Öffentlichen Schlüssel (PublicKey) und einem Privaten Schlüssel (Private Key) ist leider auch deren Nachteil. Nur die wenigsten Anwender verstehen wirklich die Technik und können sich vorstellen, dass etwas wieder entschlüsselt werden kann, ohne das Verschlüsselungspasswort zu kennen. Die mathematischen Hintergründe sind leider nur für einen geringen Teil der Bevölkerung verständlich. Zudem wurde für viele Firmen die Einführung diese Technik uninteressant, weil die Regierung bei der Einführung des Signaturgesetzes sehr lange Zeit gelassen hat. Schließlich waren die Auflagen, beispielsweise für Trustcenter, so umfangreich, dass sich ein wirtschaftlicher Betrieb nicht lohnte. Die wenigen verbliebenen Trustcenter müssen entweder die Technik so teuer anbieten, dass es sich für den Normalanwender nicht rechnet, oder es wird wie bei der Genossenschaft



DATEV nur geschlossenen Gruppen angeboten. Ein weiter Hindernisgrund für die Technik ist, dass bei Kartenlesern, Chipkarten und Software häufig auf individuelle Insellösungen gesetzt wird, die untereinander nicht oder nur eingeschränkt kompatibel sind. Anfangs fanden wir PGP auch extrem unübersichtlich und nicht gut zu bedienen. Während unserer eigenen Entwicklung ist uns aufgefallen, dass eine einfache Umsetzung scheinbar nicht möglich ist und der breite Markt diese Technik nie verstehen wird. Aus diesem Grund haben auch wir uns inzwischen entschlossen, auf einfache symmetrische Verfahren auszuweichen.

Setzt Du PGP regelmaessig - vor allem in Deinem Mailverkehr - ein? Auf Deinen Webseiten konnte ich jedenfalls keinen Public-Key finden. Falls Du auf PGP verzichtest, was sind Deine Beweggruende?

Ich setze zur Verschlüsselung meiner Emails

natürlich vorwiegend unsere eigene Software (abylon protection manager (apm)) ein. Ich hatte mir vor einigen Jahren PGP eingehend angesehen, fand aber die Handhabung viel zu umständlich. Dies war auch der ursprüngliche Beweggrund, eine eigene Lösung ausschließlich auf allgemeine Standards zu entwickeln. Ferner denke ich, dass auf dem Verschlüsselungssektor nicht wieder ein ähnlicher Fehler wie bei den Betriebssystemen gemacht werden sollte. Ich denke, der Kunde sollte seinen Wünschen entsprechend zwischen zahlreichen Produkten von unterschiedlichen Herstellern wählen können und auch ein recht auf Interkompatibilität zwischen den Produkten haben. Es sollte selbstverständlich sein, dass eine mit PGP verschlüsselte oder signierte Email auch mit jedem anderen Programm entschlüsselt bzw. verifiziert werden kann. Hier sind meiner Meinung nach vor allem die Hersteller gefordert, sich mehr an definierte Standards zu halten.

IPsec und die erweiterten Sicherheitsmechanismen in IPv6 versprechen eine nachhaltige Verbesserung der Sicherheit des Internets. Was muss in Deinen Augen geschehen, damit diese zu neuen Defacto-Standards werden? Werden die Sicherheitsprobleme des Netzes dann wirklich zu einem Grossteil behoben sein?

Ich bin nicht bis ins letzte Detail über IPv6 und IPsec informiert und kann zu Deiner Frage mehr oder weniger nur oberflächlich antworten. Wenn ich mich richtig erinnere, bietet IPv6 mit 128 Bit einen bedeutend größeren Adressraum und vor allem die feste Implementierung von IPsec. IPsec wiederum ist unter der Transportschicht realisiert und sollte daher für Programme transparent sein. Dabei werden zwei Arten der Übertragung angeboten, einmal der Transportmodus mit der Paketverschlüsselung und dann das Tunneling, wobei das komplette Paket mit Header verschlüsselt wird. Dabei handelt es sich sicherlich um die logische Weiterentwicklung von IPv4, die sich über kurz oder lang durchsetzen wird. Ein grundlegendes Problem für die Verbreitung ist sicherlich das mangelnde Interesse von Systemadministratoren die Netze zu sichern bzw. auf neue Techniken zu setzen. Verständlich ist auch, dass heute niemand weiss, ob sich eine aufwendige Administration wirklich lohnt.

<http://home.t-online.de/home/TschiTschi/ipsec.htm>
http://www.viatec.at/install/papers/IPv6_und_IPsec.pdf
<http://www.ipv6-net.org>

Sind Klartext-Kommunikationen in Netzwerken (z.B. SMTP oder POP3/IMAP4) Deiner Ansicht nach ueberhaupt noch zeitgemass?

Meiner Meinung reagieren viele Leute viel zu neurotisch bei diesem Thema. Nicht jede private Email muss wirklich verschlüsselt übertragen werden. Es werden ja auch weiterhin Postkarten versendet. Kurzum ist die Masse der täglich übertragenen Klartextbotschaften so umfangreich, dass es den einzelnen sicher kaum treffen wird. Anders sieht es jedoch in Unternehmen und Universitäten aus, wo geheime Unterlagen und Forschungsergebnisse heute noch unverschlüsselt übertragen werden. In Deutschland scheint man von Industriespionage noch nicht so viel mitbekommen zu haben und unterschätzt hier sicherlich die Gefahr. SMTP oder POP3/IMAP4 sind und bleiben für die meisten Anwender eine einfache wenn auch risikobehaftete Alternative. Für Unternehmen und Universitäten halte ich die Protokolle jedoch nicht mehr für sinnvoll und kann diesen nur empfehlen, den Mehraufwand für eine beispielsweise S/MIME bzw. PGP verschlüsselte Übertragung zu wählen.

End-zu-End Verschlüsselungen im Kommunikationsbereich sind vor allem in Hochsicherheits-Umgebungen ein Thema. Was macht denn fuer Dich eine gute kryptografische Loesung aus?

Jeder sollte ein Recht auf Privatsphäre besitzen und damit das Recht mit anderen Menschen unbeobachtet von Dritten zu kommunizieren. Die Kryptografie sollte in diesem Fall ein einfach verständliches, schnelles, sicheres und effektives Instrument für die Umsetzung sein. Als Nutzer möchte ich wirklich von der Tastatur bis zum Bildschirm meines Gegenübers die Gewährleistung haben, dass wir unter uns sind. Leider ist das bei der Komplexibilität der Systeme und Programme nicht gewährleistet. Was bringt mir die hochgradigste verschlüsselte Email, wenn ein Trojaner oder mein Betriebssystem auf einem anderen Kanal die Botschaft unverschlüsselt an Dritte übermittelt? Was hilft mir als Unternehmer eine verschlüsselte Übertragung mit einem Algorithmus, der von staatlicher Seite kontrolliert wird? In den USA wird Werkspionage in Unternehmen staatlich explizit zum wohlwollen der USA unterstützt. Ein gutes Verfahren sollte sicherlich Open - Source sein, wie es bei PGP mal der Fall war und auch zwar von der Tastatur



bis zur Ausgabe ohne staatliche Kontrolle.

Globaler Terrorismus ist fuer die westlichen Laender spaetestens seit den Anschlaegen des 11. September ein hochbrisantes Thema. Viele Staaten schraenken aus Angst der fehlenden Kontrolle die Erlaubnis des Nutzens kryptografischer Mechanismen ein. Ist dies eine annehmbare Entwicklung und falls Nein, welche alternativen Loesungswege gaebe es?

Ich beobachte die Entwicklung der weltweiten staatlichen Überwachung mit Sorge. Der 11. September ist sicherlich eine Tragödie, aber rechtfertigt dies wirklich jeden unbescholtenden Menschen zu überwachen? Die Regierungen machen es sich einfach zu leicht, wenn Sie den totalen Überwachungsstaat einrichten wollen, um dem Terrorismus zu begegnen. Ich denke, dass das Schlagwort Terrorismus von allen Regierungen nur dazu genutzt wird, um grundsätzliche Menschenrechte einzuschränken bzw. auszuhebeln. Die Terroristen verfügen inzwischen eh über genügend Mittel sich auf Dauer unabhängig sichere Kommunikationsmöglichkeiten aufzubauen, sodass ein kryptografisches Gesetz nur die Unschuldigen trifft. Eine direkte alternative Lösung kann hier sicherlich niemand geben – evtl. sollte anstelle von Misstrauen einfach mal wieder mehr gegenseitige Toleranz und Vertrauen eintreten. Menschen, die solche Anschläge machen, handeln aus einer absoluten für uns nicht nachvollziehbaren Verzweiflung und Angst. Eine unverschlüsselte Kommunikation zwischen allen Beteiligten würde hier vielleicht mehr helfen.



Gibt es irgendwelche Publikationen, die Du zum Thema Kryptoanalyse empfehlen kannst?

Gute schriftliche Publikationen gibt es leider kaum noch welche. Zum Thema Kryptographie kann ich das Buch „Angewandte Kryptographie“ von Bruce Schneider empfehlen. Prinzipiell suche ich die Informationen Online im Internet, was jedoch durch ständig wachsende kommerzieller Anbieter immer schwieriger wird. Im Internet kann ich ansonsten den „Krypto & Privacy Webring“ (<http://www.webring.de>) empfehlen.

Wie hoch schaezt Du die kryptologische Staerke der NSA und vergleichbarer staatlicher bzw. militaerischer Organisationen ein? Haettest Du die Moeglichkeit bei der NSA zu arbeiten, wuerdest Du diese Chance wahrnehmen?

Die NSA hat sicherlich für uns kaum vorstellbare Möglichkeiten, kryptographische Verfahren zu kontrollieren und auch zu knacken. Es ist schon beunruhigend, dass solche einzelnen Institutionen über solche Machtinstrumentarien verfügen. Kryptographie unterliegt dem Waffenkontrollgesetz, dass nicht anderes heißt, als das es sich hier für das Militär um potentielle Waffen mit den entsprechenden Gefahren handelt. Solche Mittel gehören nicht exklusiv in die Hände einzelner Organisationen wie beispielsweise der NSA. Wenn ich die Möglichkeit zur Arbeit bei der NSA hätte, würde ich diese vermutlich annehmen. Mich würde vor allem die wirklichen Ziele dieser Organisation interessieren und davon würde auch meine weitere Bereitschaft zur Arbeit abhängen. Ein wirklich unabhängiges und ehrliches Urteil über Menschen oder Organisationen kann man nur in der Kommunikation mit diesen fällen und nicht basierend auf Gerüchte.

Du schreibst auf logosec.de zum Thema Hashalgorithmen folgendes: "Ein eher deutscher Alleingang ist das RipeMD160-Verfahren. Dieser Algorithmus ist wohl auch recht sicher, weil es fuer potentielle Hacker keinen Anlass gibt, diesen zu knacken." Vertrittst Du daher die Meinung, dass die Popularitaet einer Loesung das Interesse der Angreifer fuer diese weckt?

Die Popularität einer Lösung ist direkt proportional des Einsatzes bzw. deren Verbreitung. Dies bedeutet, dass weit verbreitete Systeme wie beispielsweise das Microsoft Betriebssystem Windows für Angreifer das größte Angebot beinhalten. Aufgrund der großen Verbreitung von Windows, konzentrieren sich die Angreifer auch eher auf dieses Betriebssystem, obwohl meiner Meinung Linux bestimmt ähnliche Schwachstellen bietet. So komplexe Systeme lassen sich einfach nicht mehr sicher umsetzen. Linux ist nicht annähernd so weit verbreitet wie Windows und wenn ich ein Hacker auf der Suche nach Opfern wäre, würde ich mich auch auf Windows stürzen. Bei Verschlüsselungsverfahren und Hashalgorithmen ist dies genauso der Fall. Ich bin jedoch gegen Insellösung, nur weil diese vielleicht weniger begehrt für einen Angriff sind. Allgemeingültige Standards, die möglichst

geringe Schwachstelle aufweisen, sollten die Lösung der Wahl sein. Die fortlaufenden und ständig durch Medien bekannt gegebenen Angriffe bieten für den Anwender zudem einen Vorteil, weil er so deutlich sensibler mit seinen Daten umgeht und nicht blindlings irgendwelchen Versprechungen vertraut. Ferner helfen so die Angreifer auch den Herstellern, Ihre Systeme Stück für Stück sicherer zu machen.

Wie wir alle Wissen hat die IT-Branche nach dem grossen Boom eine lange Durtstrecke erfahren. War und ist der Kryptologie-Bereich ebenfalls davon betroffen oder verhaelt sich dieser im Gegensatz gaenzlich Asynchron/Asymmetrisch?

Die Gründung unserer Firma abylonsoft erfolgt im Jahre 2001 und seitdem sind wir im Bereich Verschlüsselung und Computersicherheit tätig. Nach der Hype im Jahre 2000 haben auch wir die starke Kaufzurückhaltung von Firmen erlebt. Die Durststrecke konnten wir aufgrund von mehreren kleinen Aufträgen gut überstehen. Ab diesem Jahr merken wir jedoch den Aufwärtstrend, die Verkaufszahlen steigen stetig. Wir konnten auf jeden Fall keinen gegensätzlichen Verlauf beobachten, wie vielleicht im Bereich der Virensoftware. Allerdings bleibt das Kaufverhalten in Deutschland dem europäischen Ausland gegenüber deutlich zurück.

Der Streit um die Patentierbarkeit von Software ist Mittelpunkt gegenwaertiger Diskussionen in der Politik. Welche Auswirkungen haben Patente und wie stehst Du geschlossenen Loesungen (vor allem auf dem Kryptografie-Bereich) gegenueber? Wie empfindest Du Patentierungen in den Bereichen Mathematik und Kryptologie?

Ich bin absolut gegen eine Patentierbarkeit von Software, welche sich prinzipiell nur große Firmen leisten. Einzelentwickler und kleine Firmen werden dadurch benachteiligt und wirkliche Innovationen bleiben damit eher der breiten Masse verschlossen. Zusätzlich bedeuten Patente eine neue Belastung für den Entwickler, der sich neben der eigentlichen Programmierung auch mit Patentfragen auseinandersetzen muss.

Wuerdest Du es so pauschalisieren, dass Du grundsaeztlich keine geschlossenen Loesungen aus Amerika anwenden wuerdest?

Ich beurteile eine Software nicht danach, ob sie

OpenSource oder eine geschlossene Lösung ist, sonder eher nach der Stabilität, dem Funktionsumfang und der Verbreitung. Leider geht es bei OpenSource Projekten häufig drunter und drüber (siehe beispielsweise Netscape) und es kommt nicht so viel rum wie bei zu bezahlenden Lösungen. Allerdings habe auch ich meine Bedenken bei gewissen Anwendungen aus den USA, dennoch gibt es häufig keine vernünftige Alternative. Nach wie vor gelten die USA als Nummer ein von Softwareprodukten und andere Länder und Hersteller bekommen kaum einen Fuß auf dem Markt. Sicherlich sollte der Nutzer vor allem kryptografische Software und Betriebssysteme aus den USA mit Vorsicht begegnen. Ein pauschalisiertes Nein würde ich nicht aussprechen, weil die Entscheidung immer beim Kunden liegen muss.

Was faellt Dir zum Stichwort "Quantenkryptografie" ein? Was denkst Du, wie wird sich eine handfeste Entwicklung in diesem Bereich auf die Informatik- und Telekommunikations-Bereiche auswirken?

Mit dem Thema habe ich mich nur einmal kurz befasst und kann nicht allzu viel dazu sagen. Die Quantenkryptografie ist sicherlich noch weit von kommerziellem Einsatz entfernt und ich habe wirklich keine Ahnung, ob und wie sich die Entwicklung im Bereich Informatik- und Telekommunikation auswirken wird.

Ich moechte mich fuer das unterhaltsame Interview bedanken und wuensche Dir und Deinem Unternehmen noch viel Glueck fuer die Zukunft.

Danke, auch Dir wünsche ich weiterhin viel Erfolg in Deinem Berufsleben und vor allem, das Du Deine Internetseite Computec.ch auch weiterhin mit so viel Hingabe pflegst. (Unsere Logosec-Seite ist aus Zeitgründen leider ein wenig verweist)

6. Literaturverzeichnis

Ruef, Marc, März 2003, Die TCP/IP-Implementierung der Xbox,

http://www.computec.ch/dokumente/windows/tcp-ip-implementierung_der_xbox/index.html

Ruef, Marc, 13. September 2004, Die kleinen Fehler von Burnout 3,

<http://www.areaforen.de/arealive/viewtopic.php?t=6151>

scip AG, 2004, scip monthly Security Summary, Ausgabe 19. März 2004, Attack Tool Kit,

http://www.scip.ch/publikationen/smss/scip_mss-19_03_2004-1.pdf, <http://www.scip.ch>,

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