Secorvo Security News
Dezember 2005

Dirk Fox, Stefan Gora, Stefan Kelm,
Hans-Joachim Knobloch, Kai Jendrian

Secorvo Security Consulting GmbH

Nr. 12, 4. Jhrg. 2005
Stand 22. Dezember 2005

ISSN 1613-4311

http://www.secorvo-security-news.de

Inhalt

Editorial: War es Prometheus?

Genug, ich traue den Geschenken nicht,
Die mir von solchen Freunden kommen!
Auf ein Kamin zu stellen, nun, dazu
Ist diese Büchse schön genug; gib immer her!
Christoph Martin Wieland, „Pandora“ (1779)

Vor über 200 Jahren geschrieben, und doch merkwürdig aktuell: Dies könnte das einleitende Zitat in der umstrittenen BlackBerry-Studie des BSI sein. Pandoras Büchse als Symbol für das unbekannte Gerät, die „Closed Source“-Software, die, einmal geöffnet, Übles über die Welt bringt.

Tatsächlich lässt sich das Bild auf praktisch jedes IT-System anwenden, das wir heute einsetzen. Kennen wir die Software? Wissen wir wirklich, was Prozessor und Hardwarekomponenten tun? Schließlich gibt es zahlreiche Möglichkeiten, ein Sicherheitssystem unbemerkt zu penetrieren: Manipulation der Schlüsselgenerierung, Erweiterungen des Kommunikationsprotokolls, oder, ganz perfide, verdeckte Informationskanäle wie vermeintliches „Padding“ zum Auffüllen der Datenpakete in Normlänge.

Erwiesenermaßen lässt sich nicht beweisen, dass ein IT-System nicht mehr als das Gewünschte leistet. Wir sind daher angewiesen auf Audits, im besten Fall eine Zertifizierung nach international anerkannten Standards wie den Common Criteria. Nur: Auch eine solche Zertifizierung zeigt lediglich, dass es in einer konkreten Version keine Hintertür gab – mit jedem Versionswechsel, ja mit jeder Neuübersetzung des Codes kann sich das ändern, bei Vorsatz ohnehin. Lernen wir also von Hesiod:

Erstens: Es ist gar nicht ausgemacht, dass Pandora die Büchse geöffnet hat – womöglich war es ihr Schwager Prometheus oder Epimetheus, ihr Gatte. Mit Verdächtigungen sollte man also vorsichtig sein.

Zweitens: Inzwischen gilt als erwiesen, dass es gar keine Büchse war, sondern ein Krug – ein Übersetzungsfehler. Dem geschriebenen Wort sollte man demnach lieber nicht automatisch trauen.

Und drittens: Dem Krug ist auch *Ελπίς*, die Hoffnung, entwichen. Immerhin bleibt uns die.

1 Security News

1.1 ETSI on the Road

Vom 16.01. bis 19.01.2006 macht das European Telecommunications Standards Institute (ETSI) im Rahmen einer ICT-Roadshow durch mehrere europäische Länder in Deutschland Station und bietet vier Informationsveranstaltungen zu seinen Standardisierungsaktivitäten im Bereich Informations- und Kommunikationstechnik an.

Hochrangige deutsche ETSI-Vertreter werden über die Gremienarbeit referieren und die Vorteile von Standards für beteiligte Unternehmen beleuchten. Ziel der Roadshow ist es – neben der Präsentation aktueller Entwicklungen – vor allem, neue Mitglieder und aktive Teilnehmer für die ETSI-Gremien zu gewinnen – also eine gute Gelegenheit zur Kontaktaufnahme für alle, die ETSI-Standards nutzen, z. B. im Mobilfunk oder bei elektronischen Signaturen.

1.2 Schwachstellenauktion

Anfang Dezember versuchte ein Anbieter Informationen zu einer noch nicht veröffentlichten Excel-Schwachstelle via eBay zu versteigern. Die Auktion wurde angeblich auf Betreiben von Microsoft vorzeitig abgebrochen. Offensichtlich wollte der Anbieter die teilweise langwierige Behebung von Schwachstellen bei Microsoft kritisieren. Microsoft-Mitarbeitern wollte er bei Nennung des Rabatt-Codes „LINUXRULZ“ Vergünstigungen einräumen...

Tatsächlich hätte uns diese Auktion eine Vorstellung vom (Markt-) Wert einer Sicherheitslücke in einer verbreiteten Software liefern können – nicht uninteressant.

Dennoch: Schwachstellen sollten immer unmittelbar und zuerst, vor allem auch bedingungslos dem betroffenen Hersteller zur Verfügung gestellt werden. Über Probleme hierbei berichteten wir allerdings bereits in den SSN 09/2004.

1.3 Generationenproblem?

Am 08.11.2005 veröffentlichte eine Gruppe um den u.a. durch seine Angriffe auf den Clipper-Abhörchip bekannten Sicherheitsexperten Matt Blaze eine Sicherheitsanalyse von in den USA verwendeten Abhörgeräten für analoge Telefongespräche. Grundlage der Analyse waren ausschließlich öffentlich zugängliche Informationen und auf dem freien Markt erworbene Geräte.

Ergebnis: Verdächtige, die befürchten, abgehört zu werden, können durch das Senden von Signalisierungstönen die Aufzeichnungen über von ihnen geführte Telefongespräche manipulieren, teilweise sogar die Aufzeichnung vorzeitig abschalten. Das alles erinnert fatal an das Blue-Boxing, mit dem Captain Crunch vor mehr als 30 Jahren die Abrechnung von Gesprächen über AT&T deaktivieren konnte.

Die Frage drängt sich auf: Wie kann man heutigen Systemdesignern genug über Angriffe und Konzepte der Vergangenheit beibringen, damit sie nicht ständig altbekannte Schwachstellen in neuer Form wiederbeleben?

1.4 OpenCA goes OpenXPKI

Viele Jahre gab es bei der Frage nach geeigneter Software für den Betrieb einer eigenen PKI nur die Auswahl zwischen sehr teuren kommerziellen Produkten, der ins Microsoft Betriebssystem integrierten, teilweise rudimentären PKI und sehr aufwändigen „Bastellösungen“, bestehend aus frei verfügbaren OpenSource-Paketen und selbst entwickelten Skripten. Bereits 1998 versuchte deshalb das OpenCA-Projekt durch den Aufbau einer OpenSource-Toolbox samt graphischer Oberfläche dieses Problem zu adressieren. Mangels Ressourcen konnte sich OpenCA dennoch nie zu einer produktionsreifen Lösung entwickeln.

In den vergangenen beiden Jahren jedoch wurde OpenCA an vielen Stellen erheblich weiterentwickelt. Seit dem 09.12.2005 wird die Toolbox nun unter dem Namen OpenXPKI neu entworfen und fortgeführt. Open-

XPKI ist – vor allem im universitären Umfeld – bereits in vielen Organisationen im Einsatz: Beispielweise basieren auch die neuen Dienste der DFN-PKI auf OpenXPKI, wie am 18.10.2005 vorgestellt.

Fazit: Wieder einmal schafft es die „Open-Source-Szene“, eine ernst zu nehmende Alternative zu kommerziellen Produkten zu entwickeln.

1.5 Happy New Year, Sober!

Es gibt wenig, worauf man sich heutzutage noch verlassen kann. Aber ein Bekannter bleibt uns zumindest auch noch im neuen Jahr erhalten: der Sober-Wurm. Mitarbeitern des Herstellers F-Secure ist es gelungen, den Update-Mechanismus des Wurms zu entschlüsseln. Dabei entdeckten sie, dass ab 05.01.2006 mit einer neuen Sober-Angriffswelle zu rechnen ist.

1.6 W2K3 SP1 CC EAL4+

Was in der Überschrift aussieht wie ein Geekcode, bedeutet: Am 14.12.2006 gab Microsoft bekannt, dass Windows 2003 und XP in verschiedenen Versionen – jeweils mit Service Pack 1 bzw. 2 und ganz bestimmten Kombinationen von Hotfixes – sowie die Certificate Services von Windows 2003 nach Common Criteria (CC) mit Evaluation Assurance Level (EAL) 4+ zertifiziert wurden.

Neben der Angabe der Prüftiefe mit dem Marketing-wirksamen EAL-Wert ist bei einer CC-Evaluierung stets zu beachten, welcher Funktionsumfang denn geprüft wurde (siehe SSN 2/2005). Und hier steckt – wie bei vergleichbaren Evaluierungen anderer Betriebssysteme (u.a. Solaris, SuSE Linux, AIX) auch – der Pferdefuß: Einmal mehr wurde das Controlled Access Protection Profile (CAPP) angewandt, das keine besonderen Anforderungen an die Netzwerksicherheit stellt. Wörtlich heißt es da: „Any other systems [...] are assumed to be under the same management control”. Mit anderen Worten: Schon ein Internet-Anschluss verstößt gegen die der Zertifizierung zu Grunde liegenden Annahmen.

An zwei Stellen geht Microsoft löblicherweise über CAPP/EAL4 hinaus: Zum einen wurde neben den Grundanforderungen der CC auch der Umgang mit Schwachstellen (Flaw Remediation) mit geprüft. Zum anderen wurden die Certificate Services nach dem vom NIST speziell für PKI entwickelten Protection Profile CIMC evaluiert.

1.7 Softies und Saboteure

Eine am 21.12.2005 auf Deutsch veröffentlichte Studie wertet in sechs verschiedenen europäischen Ländern erstellte Umfragen zur Gefährdung der IT-Sicherheit durch interne Mitarbeiter aus. Die Studie wurde im Auftrag von McAfee erstellt, was angesichts eines Produktportfolios, das sich besonders dem Schutz gegen „Gefahren von innen“ widmet, wenig verwundert.

Die Zahlen werden aber auch all denen eine Hilfe sein, die Maßnahmen in den Bereichen Security Awareness oder interne Sicherheit begründen müssen und sich dabei nicht auf hinter vorgehaltener Hand gemunkelte Beispiele und Mutmaßungen verlassen wollen.

Bei der Klassifikation der internen Gefahren waren die Autoren humorvoll-kreativ: es wird nach fahrlässigen „Sicherheits-Softies“, verspielten „Gadget-Freaks“, Umnutzung durch „Illegale“ (im englischen Original der Studie: „Squatter“ – Systembesetzer) und vorsätzlichen „Saboteuren“ unterschieden.

1.8 Sandkastensicherheit

Auch in einem Sandkasten kann hin und wieder etwas passieren, was von den Erbauern so nicht vorhergesehen wurde. Das ist mit Kindern auf dem Spielplatz im realen Leben ähnlich wie bei Software in einer virtuellen Maschine.

Am 21.12.2005 wurde auf [Full-Disclosure] von Tim Shelton auf eine Schwachstelle in den meisten VMWare-Versionen (außer ESX-Server) hingewiesen. Durch einen Fehler in der NAT Implementierung wird ein Nutzer des Gastsystems in die Lage

versetzt, Kommandos auf dem Wirtssystem auszuführen.

Das Konzept der virtuellen Maschinen ist nicht nur aus Verfügbarkeitsgründen ein wertvoller Schritt in Richtung erhöhter Sicherheit. Auch wenn dies der erste nachgewiesene Einbruch in das Hostsystem ist, darf man sich allerdings nicht in der trügerischen Sicherheit wähnen, dass diese Maschinen in allen Fällen wasserdicht sind. Sehr kritische Systeme sind daher nach wie vor auf einer eigenen (Hardware-) Plattform besser aufgehoben. Bei der Mehrzahl der Systeme dürften die Vorteile der Virtualisierung die Risiken aber überwiegen.

2 Secorvo News

2.1 Secorvo College aktuell

Für den „Jahrgang 2006“ wurde das bewährte Seminar Public Key Infrastrukturen um einen (optional buchbaren) vierten Tag erweitert, an dem die an den vorangegangenen Tagen vermittelten Grundlagen und Erfahrungen aus zahlreichen PKI-Projekten in Workshop-Form in die Praxis umgesetzt werden können. Es findet erstmals vom 07.-10.02.2006 statt.

Der Workshop-Tag kann auch separat oder zusammen mit dem dritten Seminartag, der fortgeschrittene PKI-Fragestellungen adressiert, gebucht werden.

Weitere Seminarthemen und Termine von Secorvo College finden Sie unter http://www.secorvo.de/college

2.2 Externer DSB

Für mehrere Unternehmen hat Secorvo bereits die Funktion des externen Datenschutzbeauftragten übernommen. Mit Karin Schuler, Volker Hammer und Dirk Fox stehen jetzt drei erfahrene Datenschutzexperten für diese Aufgabenstellung zur Verfügung. Eine detaillierte Leistungsbeschreibung kann unter info@secorvo.de angefordert werden.

3 Veranstaltungshinweise

Dezember 2005	
24.12.	Heiligabend
Januar 2006	
16.-19.01.	ETSI ICT Roadshow (Vier Veranstaltungen in Bonn, Mainz, Ulm, München)
24.-26.01.	IT-Sicherheit heute – Angriffe, Konzepte, Lösungen (Secorvo College, Karlsruhe)
30.-31.01.	Net-ID 2006 – Identity, Trust, Privacy & Security (COMPUTAS, Berlin)
Februar 2006	
07.-10.02.	PKI (Secorvo College, Karlsruhe)
14.-15.02.	Inside Windows Security (Secorvo College, Karlsruhe)
20.-21.02.	IT-Governance (COMPUTAS, Berlin)
20.-23.02.	Sicherheit 2006 (Gesellschaft für Informatik, Magdeburg)
28.02.-03.03.	Black Hat Europe 2006 (Black Hat, Amsterdam)
März 2006	
01.-02.03.	DFN-CERT-Workshop (DFN-CERT, Hamburg)
27.-28.03.	DuD 2006 (COMPUTAS, Berlin)
28.-29.03.	D-A-CH Security 2006 (Universität Klagenfurt)

Aktuelle Veranstaltungsübersicht:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de