Secorvo Security News
Mai 2005

Dirk Fox, Stefan Gora, Stefan Kelm, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 5, 4. Jhrg. 2005
Stand 25. Mai 2005

ISSN 1613-4311

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

Inhalt

Editorial: Spieglein, Spieglein ...

Der Traum von biometrischen Identifikationssystemen, die uns von der Not befreien, unser Gedächtnis mit Myriaden ständig wechselnder User-IDs, Passwörter und PINs zu quälen, ist viel älter, als so manche Science Fiction-Verfilmung uns glauben machen will. Schon unter den von den Gebrüdern Grimm tradierten klassischen Märchen findet sie sich: „Schneewittchen und die sieben Zwerge“ kommt zwar ohne Elektrizität und fließendes Wasser aus, wäre aber ohne Biometrie nicht denkbar.

In der Gestalt des Spiegels der Königin erwacht sie zum vollen Leistungsumfang. Nicht nur erkennt der seine Herrin eindeutig an Stimme und Gesicht, sondern er gibt auch bereitwillig Auskunft über biometrische Merkmale Dritter – wie der Schönheit Schneewittchens. Mehr noch: Selbst den Aufenthaltsort Schneewittchens kennt er (dank RFID?) und gibt ihn Preis, er weiß sogar um ihren aktuellen Gesundheitszustand. Ganz zu schweigen von der fortschrittlichen natürlichsprachlichen Benutzerschnittstelle...

Vielleicht ist es Zeit, Schneewittchen neu zu interpretieren. Denn das Märchen zeigt in drastischer Klarheit, was durch die Vernetzung biometrischer und personenbezogener Daten möglich ist. Der Zauberspiegel, der zweifellos eine sehr effektive Durchführung von Schönheitswettbewerben ermöglichen würde, wird in der Hand der Königin zum Mordwerkzeug. Wir erinnern uns: Jede Technik öffnet auch dem Missbrauch Tür und Tor – nicht nur in Herrscherhand.

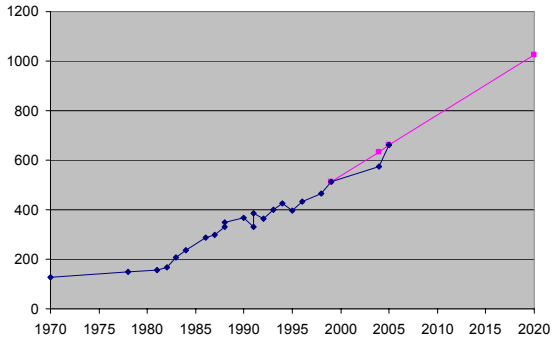
Dabei lassen sich biometrische und andere Identifikationssysteme auch so gestalten, dass eine Erfassung und Auswertung biometrischer Daten sowie der Aufenthaltsinformation nicht oder nur in kontrolliertem Umfang möglich ist. Dazu gehören die Einhaltung von Löschfristen, eine bedachte Technikgestaltung – vor allem aber der politische Wille, die Freiheit nicht um ihrer selbst Willen abzuschaffen.

„Spieglein, Spieglein an der Wand, wie lebenswert ist die Zukunft in diesem Land?“

1 Security News

1.1 RSA-200 faktorisiert

Am 09.05.2005 meldete die Bonner Forschungsgruppe von Prof. Jens Franke die erfolgreiche Faktorisierung der RSA-Challenge „RSA-200“ (Modullänge: 663 bit). Knapp 17 Monate hatte die Faktorisierung durch die Gruppe um Bahr, Böhm, Franke, Kleinjung, Montgomery und te Riele gedauert; der Rechenaufwand lag bei umgerechnet etwa 120.000 MIPS-Jahren. Für die Faktorisierung der Challenge „RSA-576“ Ende 2003, die auch auf das Konto dieser Forschergruppe ging, hatte sie „nur“ ca. 13.200 MIPS-Jahre benötigt (SSN 5/2004).



Grafik: Faktorisierungsprognose [BoFT 02]

Diese jüngste Faktorisierung entspricht fast exakt der Secorvo-Vorhersage aus dem Jahr 2001 – damals haben wir für 2005 die Faktorisierung eines 660 bit langen Moduls prognostiziert. Hält die Prognose, dann ist die Faktorisierung eines RSA-Moduls der Länge 1.024 bit in 15 Jahren zu erwarten.

1.2 Cross-Zertifikats-Report

Die Verknüpfung von Public-Key-Infrastrukturen (PKI) über Cross-Zertifikate oder Bridge-CAs ist in der Praxis noch immer nicht zufrieden stellend gelöst. Insbesondere Standard-Anwendungen wie Browser und E-Mail-Clients zeigen beim Umgang mit den entsprechenden Zertifikaten auch heute noch ein eher „holpriges“ Verhalten.

Diesem Problem sind die DFN-CERT Services GmbH und SURFnet in der Studie “PKI-Linking-Report: Connecting Public-Key-Infrastructures” nachgegangen, die am 26.04.2005 veröffentlicht wurde. Darin ist dokumentiert, wie unterschiedliche PKI-Anwendungen mit Cross-Zertifikaten etc. in der Praxis umgehen – und wo sie scheitern. Untersucht wurden Outlook Express, Outlook, Mozilla, Thunderbird, KMail, Internet Explorer, Mozilla, Firefox, Opera und Konqueror.

1.3 BSI-Antispam-Leitfaden

Spam ist schon lange nicht mehr nur eine Belästigung: Durch den Missbrauch zur Verbreitung von Phishing-Mails und Schadprogrammen ist Spam auch ein Sicherheitsproblem. Am 12.05.2005 stellte das BSI eine „Antispam-Strategien – Unerwünschte E-Mails erkennen und abwehren“ betitelte Studie zu diesem Thema vor. Die Untersuchung widmet sich dem Thema in großer Ausführlichkeit: Neben technischen Problemen und Lösungsvorschlägen werden auch die (vor allem finanziellen) Hintergründe organisierter Spammer diskutiert.

1.4 Phishing exposed

Phishing-Angriffe, in denen über Massen-E-Mails, die vorgeblich z. B. von Ebay oder einer Bank stammen, versucht wird, die Empfänger auf eine gefälschte Webseite zu locken und zur Eingabe vertraulicher Daten wie Passwörter, PINs oder TANs zu verleiten, nehmen nicht nur bedenklich zu, sondern werden auch immer perfider.

Dem Honeynet-Projekt ist es jetzt gelungen, hinter die virtuellen Kulissen einiger Phishing-Angriffe zu schauen. So konnten „Phisher“ dazu gebracht werden, Köder-Rechner (Honeypots) zu hacken und von dort ihre Angriffe (Aufsetzen gefälschter Webseiten, Verschicken von Massen-E-Mails, etc.) durchzuführen. Die Phisher wurden dabei mehrere Monate lang beobachtet. Dabei konnten drei generelle Angriffsmuster identifiziert werden. Ein am 16.05.2005 veröffentlichtes White Paper beschreibt die Details dieser Live-Analyse: Vieles weist darauf hin, dass zunächst automatisierte Angriffs-Tools verwendet

werden, um Hintertüren in einem System zu installieren. Über diese werden anschließend die Phishing-Attacken initiiert. Offenbar sind die Angreifer dabei sehr gut organisiert: So wurden Phishing-Archive mit gefälschten Webseiten vieler großer Online-Anbieter entdeckt. Erschreckend ist die Beobachtung, dass sehr viele Privatnutzer den Phishern auf den Leim gehen und auf deren gefälschte Webseiten zugreifen.

1.5 Hash-Workshop

Als Reaktion auf die jüngsten kryptoanalytischen Erfolge beim SHA-1 (SSN 02/2005) hat die Computer Security Division des NIST am 28.04.2005 einen Workshop zu kryptographischen Hashfunktionen ausgeschrieben (31.10.-01.11.2005). Interessierte sind aufgefordert, bis zum 15.07.2005 Vorschläge für Präsentationen einzureichen. Nähere Informationen finden sich auf der Workshop-Webseite.

1.6 PIV-Standards

Zur Umsetzung der Homeland Security Presidential Directive 12 vom 27.08.2004 wurde am 25.02.2005 vom NIST mit FIPS 201 ein Standard für eine einheitliche Personal Identity Verification (PIV) von Federal Employees und Contractors verabschiedet. Darin sind sowohl die grundsätzlichen Anforderungen an Identity-Cards als auch – sehr detailliert – die physisch-technischen Merkmale festgelegt, darunter die Abmessungen, Mechanismen (Foto, Barcode, Chip, Unterschriftsfeld, Magnetstreifen, Bedruckung) und Daten (z. B. biometrische Merkmale).

Der am 25.04.2005 publizierte NIST Special Report SP 800-78 enthält die Spezifikation der für PIV-Karten gemäß FIPS 201 zugelassenen kryptographischen Algorithmen und Schlüssellängen, vergleichbar der Algorithmenempfehlung des BSI für qualifizierte digitale Signaturen. Empfohlen werden darin bis Ende 2008/2010 RSA (ab 1024 bit), ECDSA (Kurven nach FIPS 186-3, ab 224 bit), TripleDES und AES (ab 128 bit) und als Hashfunktion SHA-1, SHA-224 oder SHA-256.

1.7 LAND unter

Am 17.05.2005 wurde auf der Bugtraq-Mailingliste die Anfälligkeit aktueller Windows-Systeme für LAND-Attacken gemeldet. Dieser Denial-of-Service Angriff wurde 1997 erstmalig veröffentlicht und eine entsprechende Schwachstelle bei Windows 95 geschlossen. Anfang 2005 wurde bei aktuellen Windows-Systemen erneut eine LAND-Anfälligkeit festgestellt. Die von Microsoft veröffentlichten Sicherheitspatches vom April sollten sie beheben; offenbar wirkt der Patch aber nicht bei Einsatz von IPv6. Wenn aber selbst die Patches vor Verbreitung nicht besser getestet werden als die Originalsoftware – was bleibt dann noch?

1.8 „Roo“ v1.0 erschienen

Am 17.05.2005 veröffentlichte das Honeynet-Projekt die Version 1.0 der kostenlosen Software „Honeywall CDROM Roo“. Dabei handelt es sich um eine auf Fedora basierende, sehr mächtige Tool-Sammlung, die es erlaubt, ein Honeynet der neuesten Generation sehr leicht aufzusetzen und zu administrieren, sowie potentielle Angriffsversuche auf das Honeynet effizient zu analysieren.

Stefan Kelm von Secorvo war während der mehrwöchigen Beta-Testphase intensiv an der Honeywall-Entwicklung beteiligt: Eine entsprechende Testumgebung wurde mehrere Wochen betrieben und Angriffe beobachtet. Die Ergebnisse dieser Testphase werden in Bälde als Secorvo White Paper veröffentlicht.

1.9 Firefox strikes back

Brian Livingston berichtet in seinem Newsletter vom 12.05.2005 von einem neuen Sicherheitsvergleich zwischen Internet Explorer und Firefox. Darin wurde nicht einfach die Anzahl der schwer wiegenden Schwachstellen verglichen, sondern die Zahl der Tage im Jahr 2004, an denen ein Browser mindestens eine ungepatchte, schwere Schwachstelle aufwies. Danach besaß die jeweils aktuelle Version des IE im Jahr 2004 an nur sieben Tagen keine

bekannten Schwachstellen. An 200 Tagen kursierten bereits Exploits (Angriffscode), ohne dass ein geeigneter Patch für den IE verfügbar war – bei Firefox kam dies nicht ein einziges Mal vor. Damit hat die Open-Source Community eindrucksvoll ihre hohe Reaktionsgeschwindigkeit bewiesen.

2 Secorvo News

2.1 Secorvo College aktuell

Wie sorge ich systematisch für Informationssicherheit im Unternehmen? Welche „Best Practices" gibt es, und was fordern die wichtigsten Standards? Antworten auf diese Schlüsselfragen gibt das zwei- bis fünftägige Seminar „Information Security Management von A(udit) bis Z(ertifizierung)" am **13.-14./17.06.2005**.

2.2 Toll Collect auf Midvision

Anlässlich der IT-Mittelstandsmesse „Midvision 2005" (Neue Messe Karlsruhe, 08.-09.06.2005) wird die Karlsruher IT-Sicherheitsinitiative am Abend des **08.06.2005** gemeinsam mit CAS und Cyberforum ein besonderes Event gestalten, in dessen Rahmen der Datenschutzbeauftragte von Toll Collect, Herr Reinhard Fraenkel, über Entwicklung und Umsetzung des Datenschutzkonzepts bei Toll Collect berichten wird. Programm und Anmeldung zu diesem Event mit anschließendem Buffet finden Sie auf der Webseite der KA-IT-Si.

2.3 Security Awareness Symposium 2005

Auf dem diesjährigen dritten „Security Awareness Symposium" am **21.-22.06.2005** in Karlsruhe, das sich in den beiden vergangenen Jahren als Plattform für den Erfahrungsaustausch über Sensibilisierungsmaßnahmen etabliert hat, werden unter anderem die Kampagnen von Bosch, DAK, Novartis und SAP präsentiert. Das aktuelle Programm und ein Anmeldeformular finden sich unter http://www.security-awareness-symposium.de/.

3 Veranstaltungshinweise

Mai 2005	
31.05. -02.06.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
Juni 2005	
01.-02.06.	Einführung in die Praxis des DSB (Euroforum, Wiesbaden)
06.-07.06.	IT-Risk Management 2005 (COMPUTAS, Karlsruhe)
08.06.	Datenschutz bei Toll Collect (KA-IT-SI/Midvision, Karlsruhe)
13.-14.06.	IT-Security Management (Secorvo College, Karlsruhe)
13.-17.06.	Information Security Management (Secorvo College, Karlsruhe)
14.-15.06.	Einführung in die Praxis des DSB (Euroforum, Berlin)
21.-22.06.	Security Awareness Symposium (Secorvo, Karlsruhe)
26.06.- 01.07.	17th Annual Computer Security Incident Handling Conference (FIRST, Singapore)
Juli 2005	
05.-07.07	Western European Workshop on Research in Cryptography (WEWoRC, Leuven-Heverlee)
27.-28.07.	Black Hat Briefings (Black Hat USA, Las Vegas)
29.-31.07.	Defcon 13 (Defcon, Las Vegas)

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

Abonnement des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news")

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