Secorvo Security News
April 2003

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

Secorvo Security Consulting GmbH

Nr. 4, 2. Jhrg. 2003
Stand 25. April 2003

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

Inhalt

Editorial: Am Zopf aus dem Sumpf

Was dem einen der Lösungsweg, ist dem anderen eine Vermeidungsstrategie: Die Zurückführung eines Problems auf ein anderes. Mathematiker lösen mit dieser Methode komplexe Herausforderungen: Sie formulieren eine Problemstellung so um, dass sie auf eine andere, bereits gelöste, zurückgeführt werden kann. Die Entwickler von Sicherheitslösungen beherrschen diese Technik auch. Allerdings erwischen sie, so scheint es, dabei häufiger ungelöste Probleme, auf die sie die Fragestellung zurückführen.

Ein klassisches Beispiel ist die Erzeugung digitaler Signaturen. Theoretisch mag die Signatur unfälschbar sein. Tatsächlich ist sie aber immer nur so sicher wie der geheime Signierschlüssel: Kann ein Angreifer ihn in Erfahrung bringen, ist die Sicherheit perdu. Also speichert man ihn auf einer Smartcard – und führt das Problem damit auf den Schutz der PIN zurück. Die kann ein Angreifer jedoch oft leicht gewinnen, wie Forscher der Universität Bonn 2001 am Beispiel des Signtrust-Clients „eTrust“ anschaulich vorführten [Cremers, Spalka, Langweg 2001].

Ein anderes Beispiel ist die Jahrzehnte alte Vision eines sicheren Betriebssystems: Integer muss es sein und Veränderungen durch nicht autorisierte Programme verhindern. Allein durch Signieren der Software lässt sich das Problem jedoch nicht lösen – sondern bestenfalls auf die Authentizität des Prüfschlüssels verschieben. Die von Compaq, HP, IBM, Intel und Microsoft gegründete Trusted Computing Platform Alliance (TCPA) versucht es nun mit der Einführung einer Hardware-Verankerung von Schlüsseln und Zufallsgeneratoren.

Vor allzu kühnen Hoffnungen sei allerdings gewarnt. Denn die Angriffe auf die Xbox zeigen: Auch Hardware ist modifizierbar. Und noch sind wir alle keine Barone, die sich mit beherztem Griff an den eigenen Zopf aus dem Sumpf ziehen können.

1 Security News

1.1 TCPA in der Kritik

Gleich an mehreren Fronten kam die Trusted Computing Platform Alliance (TCPA) in den vergangenen Wochen unter Beschuss: Die Datenschutzbeauftragten des Bundes und der Länder äußerten ihre Skepsis, dass die TCPA Architektur zur Aushebelung des Datenschutzes missbraucht werden könnte und fordern die vollständige und ausschließliche Kontrolle der Anwender über ihre mit TCPA geschützten Systeme. In dieselbe Richtung zielen die vier Forderungen, die der Chaos Computer Club anlässlich der CeBIT an die TCPA stellte. Und Protect Privacy e.V. hat für die Kritiker ein Web-Forum etabliert.

Auf technischer Ebene wurde Anfang April der Sicherheitsmechanismus der Microsoft Xbox – von vielen als Testlauf für mögliche TCPA Mechanismen angesehen – ausgehebelt: durch einen Buffer Overflow im Spiel „007 Agent Under Fire“ ist es sogar ohne Hardware-Eingriff möglich, Linux auf der Xbox zu starten.

Bei aller Skepsis und negativen Schlagzeilen darf jedoch nicht übersehen werden, dass TCPA oder vergleichbare Architekturen – fehlerfrei und datenschutzkonform umgesetzt – einen wichtigen Schritt zu mehr Sicherheit darstellen können.

1.2 Signaturbündnis geht an den Start

Fast sechs Jahre nach Inkrafttreten des ersten Signaturgesetzes in Deutschland haben Staat und Wirtschaft am 03.04.2003 das „Bündnis für elektronische Signaturen“ gegründet.

Das von der Bundesregierung im Schulterschluss mit mehreren Großunternehmen initiierte Bündnis soll dem Markt für elektronische Signaturen zum lang ersehnten Durchbruch verhelfen: Deutschland sei „Vorreiter im Recht. Aber leider nicht in der Praxis.“, so Staatssekretär Wewer auf der Gründungsveranstaltung. Zu den Konvergenzzielen des Bündnisses zählen insbesondere die Standardkonformität technischer Komponenten sowie die Förderung multifunktionaler Chipkarten.

Bemerkenswert ist, dass Innen-, Wirtschafts- und Finanzministerium an der Gründung gemeinsam mitwirkten. Das ist ein wichtiges Signal, denn diese Ministerien waren in der Vergangenheit nicht immer einer Meinung, wenn es um die Förderung elektronischer Signaturen ging.

1.3 Bundestag verabschiedet neues Urheberrecht

Nach dem Signaturgesetz und einigen damit verbundenen Gesetzesänderungen befindet sich Deutschland nun auch im Bereich des Urheberrechts auf dem Weg in die Informationsgesellschaft: Der Bundestag hat am 11.04.2003 den „Gesetzesentwurf zur Regelung des Urheberrechts in der Informationsgesellschaft“ verabschiedet.

Ähnlich wie der in den USA bereits in Kraft getretene Digital Millenium Copyright Act (DMCA) soll auch das neue deutsche Recht das Eigentum an digitalen Daten besser schützen – so soll insbesondere das Umgehen von Kopierschutzsystemen zukünftig verboten sein. Lediglich für bestimmte private Zwecke sowie für die Forschung sollen Ausnahmen erlaubt werden, die jedoch recht ungenau gefasst wurden.

Damit ist die Diskussion um die Neugestaltung des Urheberrechts keineswegs beendet: Etliche Industrieverbände sowie private Initiativen haben bereits massive Kritik an der Neuregelung geäußert; die Bundesregierung selbst kündigte inzwischen eine weitere Urheberrechtsnovelle an.

1.4 CERT Summary 1/2003

Bei der Vielzahl an Sicherheitslücken und Hacker-Angriffen, die täglich in diversen

Medien veröffentlicht werden, ist es auch dem versierten Systemadministrator nahezu unmöglich, den Überblick zu behalten und die richtigen Entscheidungen effizient zu treffen.

Diesem Umstand trägt das CERT/CC mit dem CERT Summary Rechnung: Diese einmal pro Quartal herausgegebene Zusammenfassung listet stichwortartig diejenigen Sicherheitsvorfälle des vergangenen Quartals auf, denen das CERT/CC eine besondere Bedeutung zumisst. Damit stellt es eine echte Bereicherung im „Informationsdschungel“ dar.

Das Ende März veröffentlichte CERT Summary für das 1. Quartal 2003 beschreibt zehn Schwachstellen in verbreiteten Softwarepaketen und gibt Verweise auf weiter führende Informationen. Es finden sich Informationen zu Lücken in sendmail, Microsoft Windows, Samba, SSH, usw.; siehe dazu auch die Ausgaben 1-3/2003 der Secorvo Security News.

1.5 CERT-Sicherheitswarnung „entwichen“

Bereits seit 1988 gibt das US-amerikanische CERT Coordination Center (CERT/CC) in Pittsburgh aktuelle Sicherheitswarnungen zu Angriffen und Sicherheitslücken heraus – die sog. CERT Advisories.

Diese Advisories beschreiben – ohne eine „Anleitung zum Hacken“ darzustellen – Sicherheitslücken in Programmen und Betriebssystemen sowie Lösungsmöglichkeiten zu deren Beseitigung. Die Veröffentlichung dieser Advisories geschieht dabei in der Regel nach einer fest vorgegebenen Informationspolitik: Wird eine Schwachstelle entdeckt, wird der Hersteller informiert, um diesem die Behebung der Schwachstelle (z. B. durch entsprechende Patches) zu ermöglichen. Erst danach wird die Öffentlichkeit durch Herausgabe eines Advisories über die gefundene (und behobene) Sicherheitslücke informiert.

Diese Informationspolitik wird seit vielen Jahren kontrovers diskutiert. Gegner führen als Argumentation regelmäßig an, dass neue Sicherheitslücken unmittelbar und mit allen Details (full disclosure) veröffentlicht werden müssten, um die Hersteller zur Behebung der Lücken zu „zwingen“.

Im März nun ist es offenbar einem Hacker gelungen, drei im Entwurfsstadium befindliche Advisories zu „stehlen“ und die zwischen dem CERT/CC und den Herstellern diskutierten vertraulichen Informationen an die Öffentlichkeit zu bringen, bevor ein Advisory veröffentlicht werden konnte. Ob hieraus Schaden entstand, ist nicht bekannt; der Vorfall zeigt jedoch, wie kontrovers die Informationspolitik der CERTs zur Zeit diskutiert wird.

1.6 „Evil Flag“ für IP-Pakete

Von der Fachwelt lange erwartet erschien pünktlich am 1. April 2003 RFC 3514, in dem Steven Bellovin, Co-Director der IETF Security Area das „Security Flag in the IPv4 Header“ spezifiziert. Es nutzt ein seit 1981 unbelegtes Bit im Kopf von IP Paketen, um anzuzeigen, ob das Paket harmlos ist oder bösartigen Intentionen dient.

Sobald die namhaften Hersteller die Nutzung dieses sogenannten „Evil Flag“ in den IP-Stacks ihrer Betriebssysteme implementiert haben, ist es nur noch ein kurzer Weg zur perfekten Firewall.

2 Secorvo News

2.1 Secorvo College aktuell

Das neue Seminarprogramm 2003/2 von Secorvo College ist erschienen. Es wurde um einen einwöchigen Intensivkurs zum Thema „Information Security Management“ erweitert, dessen erste drei Tage getrennt gebucht werden können:

- Information Security Management von A(udit) bis Z(ertifizierung), **12.-16.05.2003**.

2.2 IT Risk Management

Vom **19.-20.05.2003** findet die Konferenz IT Risk Management 2003 unseres Partners Computas in Karlsruhe statt. Topthema: Awareness.

2.3 Let's do the time warp again

Die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) startet am **15.05.2003** (18 Uhr) zu einer Zeitreise zu den Höhepunkten der Geschichte der IT-Sicherheit – und lädt anschließend zum „Schlemmer-Networking". Referent ist Dirk Fox, Geschäftsführer von Secorvo und Herausgeber der Zeitschrift „Datenschutz und Datensicherheit" (DuD).

2.4 Security Awareness Symposium 2003

Ein wirkungsvoller Informationsschutz steht und fällt mit der aktiven Unterstützung durch alle Mitarbeiter des Unternehmens. Häufig jedoch werden Sicherheitsmaßnahmen als Arbeitsbehinderung gesehen, wird die eigene Verantwortung nicht wahrgenommen oder werden vernünftige Risikoannahmen als realitätsfern abgetan – und damit Bedrohungen der Informationssicherheit durch Mitarbeiter mitverursacht.

Durch geeignete Security Awareness-Maßnahmen können sowohl das erforderliche Grundwissen vermittelt, die Sensibilität der Mitarbeiter für Informationssicherheit erhöht als auch Einstellungen und Verhaltensweisen nachhaltig verändert werden.

Ziel des Security Awareness Symposiums 2003, das Secorvo gemeinsam mit zwei Partnern, dem E-Learning-Spezialisten digital spirit ag und der Agentur Dauth, Kaun & Partner am **24.-25.06.2003** im Technologiepark Karlsruhe durchführt, ist ein intensiver Erfahrungsaustausch mit und zwischen Unternehmen, die Security Awareness-Kampagnen planen oder bereits umsetzen. Dafür konnten Referenten mehrerer Großunternehmen gewonnen werden.

3 Veranstaltungshinweise

Mai 2003	
05.-06.05.	DuD 2003 (Computas, Berlin)
06.-07.05.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
08.05.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
12.-16.05.	Information Security Management von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
13.-15.05.	BSI-Kongress 2003 (BSI, Bonn)
15.05.	Let's do the time warp again (KA-IT-Si, Karlsruhe)
19.-20.05.	IT Risk Management (ITRM 2003) (Computas, Karlsruhe)
20.-21.05.	Lotus Notes Security (Secorvo College, Karlsruhe)
Juni 2003	
24.-25.06.	Security Awareness Symposium 2003 (Secorvo, Karlsruhe)
24.-26.06.	IT-Sicherheit heute (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Der Bezug der Secorvo Security News ist kostenlos. Eine Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail (Subject: „Subscribe Security News") an security-news@secorvo.de anfordern.

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