secorvo
security consulting

Secorvo Security News

August 2009

Gefährliche Gewissheiten

In seinem kürzlich erschienenen lesenswerten Thriller „Der Täuscher“ (2009) schildert Jeffery Deaver, wie leicht überzeugende Tatbeweise konstruiert und so Straftaten Unschuldigen „untergeschoben“ werden können.

Nicht ahnen konnte er beim Verfassen seines Romans (Originaltitel: „The Broken Window“), dass es noch schlimmer kommen würde. Inzwischen wissen wir, dass selbst DNA-Spuren ein zweifelhaftes Beweismittel sind. Nicht nur, dass DNA auch bei der Spurensuche am Tatort und durch Verunreinigung hinterlassen werden kann, wie die monatelange peinliche Suche nach dem „Phantom“ eindrucksvoll bewies. Nun wiesen vier israelische Forscher in dem am 17.07.2009 im Fachorgan der International Society for Forensic Genetics erschienenen Beitrag „Authentication of forensic DNA samples“ nach, dass jeder Biologiestudent im 3. Semester DNA-Spuren fälschen kann.

Auch IT-forensische Beweismittel wackeln. Nach einem Bericht des Daily Telegraph vom 25.08.2009 belegt eine interne Studie der britischen Polizei die geringe Wirkung der aufwändigen Videoüberwachung: Auf je 1.000 Kameras käme gerade eine aufgeklärte Straftat – pro Jahr. Eine Erkenntnis, die sich mit den Ergebnissen einer Studie der Berliner Verkehrsbetriebe aus dem Jahr 2006 deckt: Das Bildmaterial erlaubte selten eine Täteridentifikation, und eine Abschreckungswirkung war nicht nachweisbar. Ein ähnliches Schicksal droht der Vorratsdatenspeicherung, sofern sie kommt: Darf man aus der IP-Adresse eines DSL-Anschlusses tatsächlich auf einen Täter schließen? Was, wenn sich dahinter ein schlecht oder gar nicht geschütztes WLAN verbirgt? Dasselbe gilt für forensische Analysen beschlagnahmter PCs. Was beweist die Entdeckung kinderpornographischer Bilder, wenn das Passwort schlecht gewählt oder bekannt ist?

Rechtfertigt mit dem zweifelhaften Argument gesteigerter innerer Sicherheit dulden wir die Entstehung unkontrolliert wachsender Datensammlungen – mit der voraussehbar fatalen Folge einer kontinuierlichen Verkleinerung des privaten Rückzugsraums.

Inhalt

Security News

iSpion

Die kontrollierte Verbreitung mobiler Applikationen, wie von Apple für das iPhone und von Nokia für SymbianOS praktiziert, bietet in der Praxis nur einen unzureichenden Schutz, wie ein Blogeintrag am 31.07.2009 enthüllte: Auf zahlreiche Benutzerdaten, von der ID-Nummer des Geräts über das Geburtsdatum (falls Facebook genutzt wird) bis zum aktuellen Standort als Geokoordinate, greifen beliebige iPhone-Apps zu – um die gesammelten Daten an die Firma Pinchmedia weiter zu leiten, die daraus Statistiken z. B. zur Nutzungshäufigkeit und -dauer erstellt. Um Zustimmung zu dieser Übermittlung werden Nutzer von den wenigsten Apps gebeten – nach Ansicht von Pinchmedia genügt dazu die allgemeine Nutzervereinbarung von Apple.

Um so erfreulicher der Ansatz, den Rich Cannings vom – nicht gerade für Datensparsamkeit bekannten – Konzern Google am 12.08.2009 auf der diesjährigen Usenix in Montreal vorstellte: In das auf Linux und OpenSource basierende Handy-Betriebssystem Android werden Mechanismen integriert, die den Benutzer entscheiden lassen, ob er z. B. einem Spiel den Zugriff auf seinen Adressbestand gestatten möchte. Auch wenn die Gefahr besteht, dass wenig versierte Benutzer einfach „permit all“ wählen, erscheint der Ansatz geeignet, das zu Grunde liegende Privacy-Problem durch Transparenz und Benutzerkontrolle zu lösen.

RainbowCrack 1.4

Am 17.08.2009 gab das Projekt RainbowCrack (siehe SSN 6/2009) eine erneut deutlich verbesserte Version 1.4 ihres Passwort-Crackers frei: Auf einem mit der Grafikkarte NVIDIA GForce 9800 GTX+ ausgestatteten PC prüft sie knapp 104 Milliarden NTLM-Hashwerte pro Sekunde – eine 40-prozentige Steigerung. Alpha-numerische 10-Zeichen-Passwörter sind damit nach spätestens 1,5 Monaten gefunden.

Blitzkekse

Am 10.08.2009 veröffentlichten fünf amerikanische Forscher eine Studie über Sicherheits- und Datenschutzimplikationen von Flash-Cookies („Flash Cookies and Privacy“). Dabei handelt es sich wie bei HTTP-Cookies um Mechanismen zur Speicherung von Statusinformationen zwischen Aufrufen von Webseiten.

Die Studie gibt einen guten Überblick über die Technik der immer populäreren Flash-Cookies. So kann ein Flash-Cookie 100 KB an Informationen speichern – gegenüber maximal 4 KB bei traditionellen HTTP-Cookies. Flash-Cookies können browserübergreifend ausgelesen werden, und werden von den Privacy-Mechanismen in aktuellen Browsern nicht erfasst.

Komfortable Werkzeuge zur Benutzerkontrolle von Flash-Cookies sind Mangelware. Adobe bietet zur Steuerung der lokalen Einstellungen den „Settings Manager“ als Flash-Applikation an, der – wenn auch unkomfortabel – eine gewisse Kontrolle von Flash-Cookies ermöglicht. Seit Version 2.19.889 (Mai 2009) unterstützt das freie Tool CCleaner die Löschung von Flash-Cookies. Nutzern von Firefox immerhin bietet das Add-on BetterPrivacy eine Flash-Cookie-Kontrolle.

Fortschritte bei AES-Analyse

So sicher wie der Tag der Nacht folgt verbessern sich auch Analysen kryptographischer Verfahren. So hat ein Team um Biryukov und Khovratovich zum zweiten Mal in diesem Jahr einen Angriff auf AES vorgestellt. Dessen Grundlage ist eine Schwäche im Key-Scheduling, das die Rundenschlüssel aus dem eigentlichen Schlüssel ableitet.

Der gegen AES-192 und AES-256 mit reduzierter Rundenzahl gerichtete Angriff ist eine Related-Key-Attacke, d. h. der Angreifer benötigt nicht beliebige Klartext-Schlüsseltext-Paare, sondern solche, die *verschiedene* Schlüssel in einer *dem Angreifer bekannten* Beziehung verwenden. Der Angriff ist wirkungslos, wenn für jede Verschlüsselung ein zufällig gewählter Schlüssel verwendet wird, und betrifft keine AES-Variante mit voller Rundenzahl.

Dennoch ist der Angriff etwas befremdlich: Obgleich man eine stetige Verbesserung der Angriffe erwarten kann, ist der sprunghafte Fortschritt überraschend. AES-256 hat 14 Runden, davon sind bereits 10 mit einem praktikablen Angriff überwunden. Und ausgerechnet AES-256, das mutmaßlich stärkste Mitglied der AES-Familie, weist hier die größten Schwächen auf, während AES-128 praktisch unbehelligt bleibt. Man hüte sich jedoch vor falschen Schlüssen: AES-256 ist nach wie vor erheblich schwerer zu brechen als AES-128, denn für beide Verfahren ist bei voller Rundenzahl weiterhin Brute-Force der beste bekannte Angriff.

Wird den AES nun dasselbe Schicksal ereilen wie den SHA-1, dessen Sicherheit schneller als erwartet erodiert ist (siehe SSN 6/2009)? Die Autoren halten den Angriff für bedenklich, gleichwohl sind sie weit davon entfernt, AES als unsicher zu deklarieren. Auch David Wagner, Koautor von Twofish, meldet sich in Bruce Schneier's Blog in diesem Sinne zu Wort: Der AES ist, spezifikationsgemäß eingesetzt, sicher. Kein Grund zur Panik also.

Exploits kein Kinderspiel

Alexander Sotirov präsentierte am 12.08.2009 auf der Usenix einen historischen Abriss der letzten 10 Jahre Exploit-Entwicklung. Danach schien 2004 die Welt aus Entwicklersicht noch in Ordnung: War eine Schwachstelle entdeckt, ließ sich ein Exploit innerhalb kurzer Zeit entwickeln. Während Schwachstellen seitdem immer leichter zu finden sind, wird die Entwicklung von Exploits hingegen durch neue Sicherheitsmechanismen in Betriebssystemen erschwert. Zwar ist ein Denial-of-Service-Angriff über einen Buffer Overflow immer noch eine vergleichsweise einfache Sache – die Ausführung von eigenem Code wird hingegen schwieriger. Nach Sotirov kann die Entwicklung eines zuverlässigen Exploits heute mehrere Monate erfordern.

Damit verschiebt sich im Wettrennen zwischen Exploits und Patches das Gleichgewicht zu Ungunsten der Angreifer, sofern die Schwachstelle bekannt ist – vorausgesetzt, die Sicherheitsfunktionen des Betriebssystems werden ausreichend genutzt.

Fast alles über Chipkarten

Die fünfte Auflage des „Handbuchs der Chipkarten“ von Wolfgang Rankl und Wolfgang Effing erschien nach zweijähriger Überarbeitung im August 2008. Angesichts von über 1100 Seiten braucht man eine kräftige Hand, um das Buch zu halten. Da ist es einfacher zu sagen, was nicht darin enthalten ist: Kryptologische Grundlagen werden nur so weit behandelt, wie dies für Anwendungen in Chipkarten relevant ist, und auch zur Einbindung in PC-Betriebssysteme finden sich eher überblicksartige Informationen – Details zu Themen wie Windows Smart Card Logon, .NET-Karten oder Kartenmanagement-Systeme sucht man vergeblich.

Aber alles, was an Chipkarten-Basistechnik dazwischen liegt, ist ausführlich beschreiben. Die Liste der Angriffe auf Chipkarten reicht vom Abgreifen der Kommunikation an den Kontakten bis zu den Mifare-Attacken vom vergangenen Jahr. Eine der wichtigsten Überarbeitungen ist die Darstellung kontaktloser Karten. Speziell die ISO 14443 „Proximity“-Kommunikation wird dank Near Field Communication in Handys und dem elektronischen Personalausweis immer wichtiger.

Auch mit dieser Auflage ist die Geschichte der Chipkarten sicher noch nicht zu Ende: Die Kapitel zu elektronischen Gesundheitskarten und Chipkarten als Ausweisdokumenten warten darauf, fortgeschrieben zu werden. Dennoch gehört das aktualisierte Standardwerk in den Bücherschrank.

Sommerrätsel

Amateur- und Profi-Kryptologen, die ein wenig Denksport an heißen Tagen mögen, mögen sich an dem folgenden Kryptogramm versuchen:

```
signaturif+kaoti+aun+lzqimiuaia+sig
eebu+signaturiz+m0+g9
```

Unter allen richtigen Lösungen, die die Redaktion unter redaktion-security-news@secorvo.de bis zum 30.09.2009 erreichen, verlosen wir unter Ausschluss des Rechtswegs drei Exemplare des „Handbuchs der Chipkarten“.

Secorvo News

Secorvo College aktuell

Unsere Herbstseminare erfreuen sich erheblicher Nachfrage – daher sichern Sie sich bei Interesse möglichst bald einen der wenigen noch freien Plätze des Seminars „IT-Sicherheitsaudits in der Praxis“ (21.-23.09.2009) bzw. „PKI“ (03.-06.11.2009).

Vom 29.09. bis 02.10.2009 gibt es den „Schwarzen Gürtel“ in sicherer Softwareentwicklung – in Gestalt des CPSSE-Zertifikats. Eine Auffrischung Ihrer IT-Security Grundlagenkenntnisse bietet das Seminar „IT-Sicherheit heute“ (13.-16.10.2009).

Programme und Online-Anmeldung unter http://www.secorvo.de/college

Erstes Security News Symposium

Die Themengebiete IT-Sicherheit und Datenschutz unterliegen ständiger Weiterentwicklung – das merken wir nicht zuletzt Monat für Monat bei der Zusammenstellung unserer Security News. Aber nicht alle wichtigen Entwicklungen lassen sich in einem kurzen Textbeitrag angemessen beleuchten.

Daher bieten wir Ihnen in diesem Jahr erstmalig mit dem „Security News Symposium 2009“ am 06.-07.10.2009 in Ettlingen die Gelegenheit, ausgewählte Themen – darunter der Umgang mit USB-Sticks, Aktuelles zur Passwortsicherheit und zur Zukunft des Mifare-Chips – in Vorträgen, Demonstrationen und Diskussionen mit uns und weiteren Fachexperten zu vertiefen.

Die Vorträge und Referenten, das können wir versprechen, werden vom Feinsten sein – ein fachliches „Best of“ in einem inspirierenden Ambiente. Wir freuen uns auf Ihr Kommen und den Austausch mit Ihnen (Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

September 2009	
06.-09.09.	CHES: Workshop on Cryptographic Hardware and Embedded Systems (IACR, Lausanne/CH)
15.-17.09.	IMF 2009: 5th International Conference on IT Security Incident Management & IT Forensics (GI, Stuttgart)
17.09.	RZ-Compliance (Lampertz, Friedrichshafen)
21.-23.09.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
24.09.	Pacta sunt servanda (KA-IT-Si, Karlsruhe)
29.09.-02.10.	ISSECO Certified Professional for Secure Software Engineering – CPSSE (Secorvo College)
Oktober 2009	
06.-07.10.	Security News Symposium 2009 (Secorvo, Ettlingen)
13.-16.10.	IT-Sicherheit heute (Secorvo College)
November 2009	
03.-06.11.	PKI (Secorvo College)
23.-27.11.	TISP-Schulung (Secorvo College)

Fundsache

Am 16.08.2009 veröffentlichte John Gerber in seinem Blog eine hilfreiche Zusammenstellung von 30 „Cheat Sheets“ zu diversen Security Themen, darunter auch ausgefallenere wie „Reverse-Engineering Malware Cheat Sheet“ und „Troubleshooting Human Communications“. Ergänzend verweist er auf weitere „Cheat Sheets“ zu Tools, Netzwerktechniken und weiteren Sammlungen.

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

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

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