secorvo
security consulting

Secorvo Security News

Juli 2012

Als gestern noch Zukunft war

Erinnern Sie sich noch? Bush ist neuer US-Präsident, Scharping tritt als Bundesverteidigungsminister zurück. Der Kanzler heißt Schröder, der Formel-1-Weltmeister wieder Schumacher und der gerade erst eingeführte Euro „Teuro“: wir schreiben das Jahr 2002. Noch immer gibt es kein betriebsbereites UMTS-Mobilfunknetz, obwohl die Lizenzen schon seit zwei Jahren versteigert sind. Gerade erst wurde der AES nach dreijährigem Auswahlverfahren zum Nachfolger des DES gekürt. Online-Banking-Transaktionen werden mit einfachen TAN-Listen autorisiert, Apple hat den ersten iPod vorgestellt. Niemand weiß, was ein ‚Smartphone' sein soll, Compaq wird von HP übernommen und Mannesmann Mobilfunk heißt nun Vodafone D2. Und im Juli erscheint die erste Ausgabe der „Secorvo Security News“.

Zehn Jahre, 480 Seiten und knapp 1.000 Nachrichten liegt dieses Ereignis nun zurück. Die Themen und Herausforderungen, die uns in den vergangenen zehn Jahren beschäftigt haben, werden uns zweifellos auch im kommenden SSN-Jahrzehnt begleiten.

Allerdings wird es nicht leichter für IT-Sicherheit und Datenschutz. Daten werden in wachsendem Umfang Cloud-Diensten anvertraut, die IT wird sich mehr und mehr von einer Infrastruktur- zu einer Service-Dienstleistung entwickeln. Die Endgeräte werden kleiner, leistungsfähiger und unabhängiger – und zukünftig, ob wir das wollen oder nicht, auch direkt mit anderen Endgeräten (POS-Terminals, Ticket-Kontrollgeräten, medizinischen Geräten, Zugangssystemen, SmartMetern etc.) kommunizieren. Immer mehr digitale Spuren werden unser Verhalten detailliert protokollieren; zugleich werden zentrale Konfiguration und Kontrolle der Endgeräte schwieriger – eine Entwicklung, der das geltende Datenschutzrecht und heutige IT-Sicherheitskonzepte nur begrenzt gewachsen sind.

Wir werden diese Entwicklung weiterhin kritisch begleiten. Wenn Sie uns anlässlich des zehnten Geburtstags der SSN dazu ermutigen möchten, freuen wir uns über einen Kommentar von Ihnen.

Inhalt

secorvo
security consulting

Security News (2002-2012)

Neuer SHA-Standard

Am 28.08.2002 gab das US-amerikanische NIST einen neuen Secure Hash Standard (SHS) bekannt, der den SHS (FIPS PUB 180) aus dem Jahr 1993 ab 01.02.2003 ersetzt. FIPS PUB 180-2 umfasst neben SHA-1 drei weitere Algorithmen, die jeweils einen 256 (SHA-256), 384 (SHA-384) und 512 (SHA-512) bit langen Ausgabewert erzeugen. Die neuen Hashfunktionen ermöglichen ein höheres Sicherheitsniveau für digitale Signaturen: Ab einer Schlüssellänge von 1.500 bit (RSA) bzw. 168 bit (DSS) ist bislang der Hashwert das kryptografisch schwächste Glied.

SSN 09/2002 – Selbst zehn Jahre später wird der Standard noch nicht durchgängig unterstützt.

Security Tools: „Top 75"

Als Ergebnis einer Umfrage in der Newsgroup des Nmap Netzwerk-Scanners wurde eine Liste der 75 beliebtesten Sicherheits-Tools publiziert. Darin werden die Tools mit Bezugsquelle vorgestellt und bewertet. Diese Security Tools ermöglichen Administratoren, die Sicherheit ihrer Systeme und Netzwerke zu überprüfen – erleichtern allerdings auch die Durchführung von Angriffen.

SSN 03/2003 – Diese auf heute 125 Tools erweiterte Liste bietet immer noch einen guten Überblick.

SigG-Novelle

Am 19.11.2004 hat der Bundestag in zweiter und dritter Lesung das deutsche Signaturgesetz (SigG) novelliert. Zentrale Änderung: Für die Beantragung eines qualifizierten Signaturschlüssel-Zertifikats genügt nunmehr ein PIN-TAN-basierter Prozess – der eigenhändig unterschriebene Antrag mit Vorlage des Personalausweises ist bei bestehenden Kunden nicht mehr erforderlich. Damit kommt die Novelle den deutschen Banken entgegen, die eine Vereinfachung der Prozesse gefordert hatten, um ihre Bankkarten zu Signaturkarten aufwerten zu können. Die Bundesregierung erhofft sich mit diesem Schritt eine erhebliche Ausweitung der nach wie vor nur marginalen Verbreitung qualifizierter Signaturen; freilich fehlen trotz dieser Verfahrensvereinfachung noch immer die seit vielen Jahren versprochenen Anwendungen für „Otto Normalsignierer", die für ihn einen erkennbaren Zusatznutzen darstellen und einen Technikwechsel rechtfertigen.

SSN 11/2004 – Auch 2012 sind SigG-Signaturen per Bankkarte und Anwendungen dafür Mangelware.

iTAN

Auf Phishing-Angriffe reagieren jetzt auch die deutschen Banken mit zusätzlichen Sicherheitsmerkmalen. Die Postbank meldete am 07.08.2005, dass sie ihr PIN-TAN-Verfahren um ein iTAN genanntes Merkmal ergänzt: Zukünftig sind die TAN auf der Liste indexiert. Bei jeder Transaktion schickt der Bankserver den Index, und nur die passende TAN ist gültig. Dieser einfache Challenge-Response-Mechanismus entwertet abge-"phishte" TAN. Die iTAN schützt nicht vor allen Angriffen, erhöht aber die Sicherheit des Online-Bankings deutlich.

SSN 08/2005 – Der Anfang vom Ende des PIN-TAN-Verfahrens. Die Jagd hat begonnen.

WAF-Auswahlhilfe

Das Web Application Security Consortium (WASC) hat die Version 1.0 der „Web Application Firewall Evaluation Criteria" vorgelegt. Dabei handelt es sich um eines der ersten Dokumente, in welchem Entscheidern und Firewall-Architekten ein ausführlicher Katalog wichtiger Anforderungen an eine Web Application Firewall (WAF) zur Verfügung gestellt wird. Diese Anforderungsliste erleichtert den Vergleich, die Bewertung und die Auswahl geeigneter WAF-Lösungsansätze und verfügbarer Produkte

SSN 01/2006 – Noch immer sind WAFs kein Standard-Schutzmechanismus von Web-Applikationen.

Der König ist tot ...

... es lebe der König: Am 01.07.2007 wurde der ISMS-Standard ISO/IEC 17799:2005 vom Technical Committee JTC 1/SC 27 in ISO/IEC 27002:2005 „Information technology – Security techniques – Code of practice for information security management" umbenannt. Inhaltlich blieb er unverändert. Mit der Umbenennung hat die ISO einen wichtigen Beitrag zur Bereinigung der babylonischen Namensverwirrung im Bereich der sicherheitsrelevanten Standards geleistet – nach ISO/IEC 27001:2005 und ISO/IEC 27006:2007 existiert jetzt der dritte Standard im Nummernkreis 270xx. Die Nummerierung verdeutlicht die „Verwandtschaft" zu ISO 9001 (Qualitäts-) und ISO 14001 (Umweltmanagement).

SSN 08/2007 – Mittlerweile ist die ISO-Reihe 270xx sechsteilig und nicht mehr weg zu denken.

Mifare-Cloning

Auf dem Jahreskongress des Chaos Computer Clubs stellten Karsten Nohl und Henryk Plötz am 28.12.2007 einen Angriff auf das Authentifikationsverfahren kontaktloser Mifare-Chipkarten vor. Dem vom Hersteller geheimgehaltenen, etwa 15 Jahre alten „CRYPTO1"-Algorithmus waren sie mit einer

Mikroskop-Analyse des Chip auf die Spur gekommen, um dann nach kryptographischen Schwächen (zu kleiner Zufallswert, lineares Schieberegister) darin zu suchen. Zu dieser Krypto-Schwachstelle gibt es nun den passenden „Mifare-Cloner“: Am 12.03. 2008 haben Forscher der Radboud Universiteit Nijmegen ein Video in YouTube veröffentlicht, auf dem sie zeigen, wie sie mit minimalem Aufwand Mifare-basierte Zugangskarten duplizieren. Von der Attacke betroffen sind Tausende von Anwendungen mit einer Milliarde ausgegebenen Karten, vom Betriebsausweis über die Kantinenkarte bis zum bargeldlosen Bezahlsystem im öffentlichen Nahverkehr, sofern sie Mifare-Chips des Typs MF1 IC S50 oder S70 verwenden. Fein raus ist, wer seine Anwendung bereits auf den neueren Mifare DESFire (MF3 IC D40) migriert hat – statt einer etwas ältlichen Stromchiffre verwendet er bei der Authentifikation wahlweise DES oder TripleDES.

SSN 03/2008 – Eingesetzt werden sie noch immer. Ende 2009 hat es auch Mitbewerber Legic erwischt.

SSL-Authentifikation für alle

SSL – seit zehn Jahren unter dem Namen Transport Layer Security (TLS) genormt – ist ein bekanntes, bewährtes und deshalb von seinem ursprünglichen Zweck, der Absicherung von Webzugriffen, auch auf andere Bereiche wie z. B. VPN oder WLAN übertragenes Sicherheitsprotokoll. Sollte man meinen. Auch sollte sich im Jahr 20 nach der Erstveröffentlichung des X.509 Standards herumgesprochen haben, dass Zertifikate naturgemäß öffentliche Daten sind und für sicherheitsrelevante Operationen das private Gegenstück des per Zertifikat bestätigten öffentlichen Schlüssels benötigt wird.

Umso größer die Verwunderung, als Microsoft am 10.03.2009 im Security Bulletin MS09-007 einräumte, dass die SSL-Komponente in Windows – vom Veteranen Windows 2000 bis zum neuesten 64-Bit-System – bei der Client-Authentifikation jahrelang patzte: Zwar wurde die Gültigkeit des vorgelegten Zertifikats geprüft; der im Standard vorgeschriebene Schritt, per Signatur der ausgetauschten Protokollnachrichten zu verifizieren, dass der Client auch den passenden privaten Schlüssel verwendet, wurde jedoch eingespart. Tatsächlich akzeptierte der Server also jeden Client mit irgend einem gültigen Zertifikat - ob nun dem eigenen oder einem fremden.

Durch das weite Einsatzspektrum von SSL/TLS sind wahrscheinlich nicht nur IIS-basierte Webanwendungen von diesem Bug betroffen, sondern jede zertifikatsbasierte VPN-, WLAN- und NAC-Anmeldung, sofern dabei der Microsoft-eigene RADIUS-Dienst IAS zum Einsatz kommt. Vielleicht haben sich die Microsoft-Entwickler bei der Implementierung auf das SSL-Diagramm in Wikipedia verlassen – das den wichtigen Verifikationsschritt ebenfalls fehlerhaft darstellt. Manchmal geht Studieren doch über Probieren.

SSN 03/2009 – Blindes Vertrauen in die Implementierung von Sicherheitsprotokollen ist gefährlich.

iPhone Security

In nicht wenigen Unternehmen hält derzeit Apples iPhone Einzug. Trotz seiner nach wie vor deutlichen Nachteile bei Business-Anwendungen gegenüber RIMs BlackBerry wiegen „Sex-Appeal“ und Nimbus des Geräts auch bei Führungskräften oft schwerer. Wie sicher aber sind Unternehmensdaten auf einem iPhone? Was ist von der Hardware-Verschlüsselung und anderen Schutzmechanismen zu halten? Lassen sich iPhones ohne Inkaufnahme zusätzlicher Risiken in die IT-Infrastruktur integrieren? Diesen Fragen ist Jörg Völker auf den Grund gegangen – und hat die Ergebnisse seiner Untersuchungen nun in der Fachzeitschrift „Datenschutz und Datensicherheit“ (DuD) veröffentlicht.

SSN 06/2010 – Die ungebrochene Popularität von Smartphones hält das Thema im Brennpunkt.

c = m

Kryptografie kann so einfach sein. Das dachen wohl auch die Programmierer der Entwicklerversion von Ruby bei der Implementierung des RSA-Verfahrens: Wenn $c = m^e \bmod n$ zu berechnen ist – dann geht das mit $e := 1$ am schnellsten. Damit folgt: $c = m \bmod n$, $m < n \Rightarrow c = m$. Falls Sie mit dieser Ruby-Version zwischen dem 01.09. und dem 04.11.2011 RSA-Schlüssel erzeugt haben, sollten Sie diese schnellstmöglich ersetzen.

SSN 11/2011 – Hoffentlich haben Rivest, Shamir und Adleman das nicht lesen müssen...

Secorvo News

Freie Plätze sichern

Die Schulung zum T.I.S.P.-Zertifikat mit den Autoren des T.I.S.P.-Buchs am **17.–21.09.2012** ist fast ausgebucht. Das nächste T.I.S.P.-Seminar (und letzte in 2012) findet vom **12.–16.11.2012** statt – frühzeitige Anmeldung wird empfohlen.

Security Awareness Symposium

Am **11.–12.09.2012** sind wir mit dem 8. Security Awareness Symposium wieder zu Gast in der Buhlschen Mühle in Ettlingen. Das Programm ist noch in Abstimmung – wer das Event auf keinen Fall verpassen möchte, kann sich aber bereits heute online anmelden. Wir freuen uns auf Ihr Kommen!

Veranstaltungshinweise

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

August 2012	
06.-08.08.	DFRWS 2012 (DFRWS, Washington/US)
08.-10.08.	21th USENIX Security Symposium (Usenix, Bellevue/US)
19.-23.08.	Crypto 2012 (IACR, Santa Barbara/US)
20.-24.08.	SecSE 2012 (SINTEF, Prag/CZ)
27.08.	Sommerakademie 2012 (ULD Schleswig-Holstein, Kiel)
September 2012	
11.-12.09.	8. Security Awareness Symposium (Secorvo, KA-Ettlingen)
17.-21.09.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
18.09.	Anwendertag IT-Forensik 2012 (Fraunhofer SIT, Darmstadt)
24.-27.09.	CPSSE-Schulung (Secorvo College, Karlsruhe)
25.-26.09.	D·A·CH Security (GI/OCG/BITKOM/SI/TeleTrusT, Konstanz)
Oktober 2012	
09.-11.10.	Sicherheitsmanagement heute (Secorvo College, Karlsruhe)
12.10.	1. Freiburger Datenschutztag (vivaSoft/Datenschutz individuell, Freiburg)
23.-26.10.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College, Karlsruhe)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Jochen Schlichting

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