Secorvo Security News
August 2004

Dirk Fox, Stefan Gora, Stefan Kelm,
Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 8, 3. Jhrg. 2004
Stand 23. August 2004

ISSN 1613-4311

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

Inhalt

Editorial: DES – Ein Nachruf

"NIST determined that the strength of the DES algorithm is no longer sufficient to adequately protect Federal government information."

Jetzt ist es amtlich: Das NIST hat am 26.07.2004 offiziell angekündigt, den DES-Standard FIPS 46-3 zurückzuziehen.

Erinnern wir uns: Seit 1977 prägte der DES – vom National Bureau of Standards als FIPS 46-1 publiziert –, das weltweit erste standardisierte Verschlüsselungsverfahren, sowohl die Kryptoanalyse als auch die Diskussion über die Rolle des amerikanischen Geheimdienstes NSA, zeitweilig in „No Such Agency" umgetauft. Der DES entstand 1975 aus einer Entwicklung des IBM-Kryptologen Feistel, der Lucifer-Cipher. Tatsächlich reduzierte die NSA für den Standard die ursprüngliche Schlüssellänge von 128 auf 64 bit – und machte weitere 8 bit zu Paritätsbits. Schon damals war diese Schlüssellänge von 56 bit Stein des Anstoßes; mit der Geheimhaltung des Entwurfs der S-Boxen aber nährte die NSA zudem den Verdacht, eine Hintertür im Algorithmus verborgen zu haben.

Biham und Shamir gelang 1990 eine Attakke auf den DES; sie war theoretisch bedeutsam, aber nicht praxisrelevant. Erst die Koordination von mehreren 10.000 PCs über das Internet, die in Idle-Zeiten DES-Schlüssel durchprobierten, versetzte dem DES Ende 1997 den „Todesstoß": Die erste DES-Challenge wurde so in 140 Tagen gelöst. Schließlich schockte Mitte 1998 der DES-Cracker der EFF, der ein Cluster von Spezialchips verwendete, die Krypto-Welt: In weniger als drei Tagen war der Key der zweiten DES-Challenge gefunden. Abgelöst wurde der DES mit der Veröffentlichung des Advanced Encryption Standard 2001 (FIPS 197). Der mehrjährige Auswahlprozess fand in der Fachöffentlichkeit statt – und wurde selbst von kritischen Beobachtern wie Bruce Schneier als sachlich und fair bewertet. Mit dem DES hat die Krypto-Gemeinde nun nicht allein einen Algorithmus, sondern auch ein verbindendes, lieb gewonnenes Feindbild verloren.

1 Security News

1.1 WinXP SP 2 verfügbar

Nach einigen Verzögerungen ist am 10.08.2004 das lange angekündigte Servicepack 2 für Windows XP erschienen. Neben zahlreichen Bugfixes enthält es insbesondere im Bereich Sicherheit einige Neuerungen: Unter anderem wurde die Funktionalität der Personal Firewall erweitert, und sicherheitsrelevante Einstellungen können nun übersichtlich im „Security Center“ eingesehen werden.

Die verbesserten Funktionen der Personal Firewall sind allerdings nicht ganz „State-of-the-art“, da beispielsweise ausgehende Verbindungen nicht überwacht werden. Ein gewisser Basisschutz ist durch die Firewall jedoch gegeben; für sensible Bereiche wird dennoch der Einsatz einer dedizierten Personal Firewall empfohlen. Die Virenschutz-Meldungen im Security Center hängen maßgeblich von den integrierten Produkten von Drittherstellern ab – und nicht alle Hersteller liefern diese Meldungen.

Microsoft scheint jedenfalls auf dem richtigen Weg zu sein. Allerdings: Nur wenige Tage, nachdem das SP 2 erschien war, tauchten bereits die ersten Probleme auf: Offenbar gibt es Schwierigkeiten, die knapp 270 Megabyte große Datei fehlerfrei zu installieren. Es wird von Systemabstürzen und Datenverlusten berichtet. Microsoft selbst veröffentlichte jetzt eine (leider nicht sortierte) Liste von über 200 Anwendungsprogrammen, die nach der Installation unter Umständen nicht mehr richtig funktionieren.

Pikanterweise finden sich auf dieser Liste auch Microsoft-Lösungen wie Word und Outlook. Microsoft macht also offenbar gründlich ernst mit dem eigenen Anspruch, nunmehr mehr auf die Sicherheit als auf Abwärtskompatibilität zu setzen. Fazit: Für dieses Servicepack gilt einmal mehr: Vor dem Roll-Out ausgiebig innerhalb einer geschlossenen Testumgebung prüfen.

1.2 Déjà-vu bei Check Point

Am 28.07.2004 wurde von ISS auf eine Sicherheitsschwäche beim VPN-Verbindungsaufbau von Check Points Produktlinie VPN-1 hingewiesen – ein Déjà-vu-Erlebnis in doppelter Hinsicht: Nicht nur, dass die Schwachstelle einmal mehr in den ASN.1-Bibliotheken liegt, auf die schon häufig, in den SSN zuletzt im Januar hingewiesen wurde. Auch das aktuelle Advisory von Check Point hat auffällige Ähnlichkeit einem früheren vom Mai 2004.

1.3 Acrobat ohne Netz

Seit dem 12.08.2004 wurden in kurzer Folge mehrere Sicherheitslücken in Adobes Acrobat veröffentlicht, die auch den Reader und sowohl Windows- als auch Unix-Versionen betreffen. Da der Acrobat Reader auf Arbeitsplätzen praktisch aller Betriebssysteme inzwischen zur Standardausstattung gehört, wird ein Wechsel auf die aktuelle Version angeraten, obwohl die Funktionenvielfalt der neueren Versionen die Wahrscheinlichkeit einer Sicherheitslücke zweifellos grundsätzlich erhöht.

1.4 Biometrische Realität

Am 06.08.2004 wurde von BSI, BKA und Fraunhofer-IGD der öffentliche Abschlussbericht der Studie „BioFinger“ zu Fingerabdruck-Systemen in überarbeiteter Form (Erstfassung: 20.05.2004) veröffentlicht. Die Studie attestiert dem besten System eine Falschakzeptanzrate von 0,1% – bei einer Falschzurückweisungsrate von 2%. Übersetzt heißt das: Damit nur jeder tausendste Attentäter in ein Flugzeug kommt, müssen bei jedem voll besetzten Jumbo sechs bis acht Passagiere unfreiwillig am Boden bleiben.

Möglich, dass Studienergebnisse dieser Art dazu beigetragen haben, dass die Forderung der USA, ab Oktober nur noch Pässe mit digitalen Fingerprint-Daten zuzulassen, am 10.08.2004 vom US-Kongress für ein Jahr zurückgestellt wurde.

1.5 Sicherheitsloch in PuTTY

Am 03.08.2004 wurde ein kritischer Fehler in dem bei Administratoren sehr beliebten Telnet/SSH-Client PuTTY entdeckt. Er erlaubt es einem Angreifer, via Spoofing oder über einen gehackten Server beliebigen Code auf dem Client-System auszuführen. Der Autor Simon Tatham empfiehlt dringend ein Upgrade auf Version 0.55.

1.6 Musterrichtlinien des BSI

Das BSI stellte am 07.06.2004 Musterrichtlinien zur IT-Sicherheit als Teil des BSI-Grundschutzhandbuchs elektronisch bereit. Sie umfassen ein Übersichtsdokument und neun Beispielkonzepte und –Richtlinien, die sich an unterschiedliche Adressatenkreise richten und eine Hilfestellung bei der Entwicklung eigener Security Policies bieten sollen. Die einzelnen Regelungsvorschläge wurden um zahlreiche Referenzen auf die entsprechenden Maßnahmen des Grundschutzhandbuchs (GSHB) ergänzt. Leider sind diese Querbezüge weder in der Word- noch der pdf-Version des Dokuments mit den Maßnahmenbeschreibungen des GSHB verlinkt, was die Nutzung aufwändig gestaltet.

1.7 MD5: Keine Panik

Auf der diesjährigen Kryptographen-Konferenz Crypto 2004 (15.-19.08.2004) kündigten chinesische Wissenschaftler an, sie hätten Kollisionen in den Hash-Algorithmen MD4, MD5 und SHA-0 entdeckt. Diese Ankündigung sorgte unter Krypto-Experten für einige Aufregung; es gab sogar Gerüchte, die Angriffe ließen sich auf heutige Algorithmen wie den SHA-1 übertragen.

Tatsächlich scheinen die Wissenschaftler Kollisionen gefunden zu haben, die denselben Hashwert zu unterschiedlichen Eingangswerten liefern. Der Weg zu einem praktikablen Angriff ist dennoch weit. So hatte Hans Dobbertin bereits 1996 Kollisionen für den MD5 beschrieben. Der Algorithmus gilt seitdem als unsicher – gebrochen wurde er indes bis heute nicht.

1.8 Bluetooth-Distanzangriff

Einer Gruppe von WLAN- und Bluetooth-Experten gelang am 03.08.2004 ein sogenannter Snarf-Angriff mit einem modifizierten Bluetooth-Adapter und einer Hochleistungsantenne über eine Distanz von 1,8 km. Die Annahme, dass Bluetooth nur im Abstand von maximal 100-150 m für Angriffe genutzt werden kann, ist damit widerlegt. Bluetooth sollte in Handys daher im Hidden-Modus betrieben oder besser gänzlich deaktiviert werden.

1.9 WPA im Verdacht

Der WLAN-Sicherheitsstandard WPA(2), über den in den letzten SSN berichtet wurde, kam am 26.07.2004 ins Gerede. Bei näherem Hinsehen entpuppte sich der beschriebene Angriff jedoch als „ganz normale“ Wörterbuch-Attacke auf das hinter WPA liegende RADIUS-Protokoll, die durch ein starkes EAP-Authentifikationsprotokoll und gut gewählte Shared-Secrets zwischen RADIUS-Server und WLAN-Access-Point verhindert werden kann.

1.10 SANS XP Survival Guide

Die „Lebenserwartung“ eines ungeschützten und mit dem Internet verbundenen PCs ist innerhalb eines Jahres von durchschnittlich 40 auf unter 20 Minuten gesunken. Das SANS Internet Storm Center ermittelt diesen Erwartungswert aus monatlich mehr als 1 Mio. Einzelmessungen. Im Mai wurde mit acht Minuten ein historischer Tiefststand erreicht. Als Anleitung für eine sichere Anfangskonfiguration und einen einigermaßen sicheren Betrieb empfiehlt sich der von SANS herausgegebene XP Survival Guide („Surviving the first day“).

1.11 BSI-Kongress 2005

Der 9. IT-Sicherheitskongress des BSI am 10.-12.05.2005 wird wie gewohnt in Bonn (Bad Godesberg) stattfinden. Anfang August hat das Programmkomitee den „Call for Papers“ veröffentlicht: Interessierte sind

aufgerufen, bis zum 08.10.2004 eine Kurzzusammenfassung (vier Seiten) mit Gliederung ihres Beitrags einzureichen.

2 Secorvo News

2.1 Secorvo College aktuell

Auf vielfachen Teilnehmerwunsch ergänzen wir – erstmalig am 23.09.2004 – unser Seminar Lotus Notes Security um einen Workshop, dessen Inhalte in Abstimmung mit den Teilnehmern aus folgendem Themenpool ausgewählt werden:

- Gruppen und Gruppenkonzepte
- ID-Administrationswerkzeuge
- Log Files
- Passwort Synchronisation
- Roaming User
- Antispam und Antivirus
- ECL
- Security Best Practices
- Betriebssystem-Sicherheit
- Notes Security Architecture Exposed

Dieser Workshop kann zusammen mit dem Seminar Lotus Notes Security oder separat gebucht werden; Frühbucher zahlen bis zum 31.08.2004 nur 580 € (zzgl. MwSt.). Weitere Auskünfte erteilt Frau Bradatsch (bradatsch@secorvo.de, 0721/6105-500).

http://www.secorvo.de/college

2.2 25. SSN-Jubiläum

Die vorliegende Ausgabe der Secorvo Security News ist die 25. – und unser Anspruch an Inhalt und Qualität entspricht nach wie vor dem, den wir im Editorial der Erstausgabe im Juli 2002 formulierten.

Seitdem hat uns viel Lob erreicht, und zahlreiche Unternehmen verbreiten die News inzwischen über ihr Intranet. Das freut und ehrt uns. Einer unveränderten Publikation der News als vollständiges .pdf stimmen wir grundsätzlich zu – und freuen uns über eine kurze Benachrichtigung: als Balsam für unsere Motivation.

3 Veranstaltungshinweise

September 2004	
20.-21.09.	Elektronische Geschäftsprozesse – EGP 2004 (Klagenfurt)
21.-22.09.	Lotus Notes Security (Secorvo College, Karlsruhe)
23.09.	Lotus Notes Security – Advanced (Secorvo College, Karlsruhe)
28.-30.09.	ISSE 2004 (EEMA/TeleTrusT, Berlin)
28.-29.09.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
30.09.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
Oktober 2004	
12.-13.10.	Live Hacking Lab (Secorvo College, Karlsruhe)
26.-27.10.	Inside Windows Security (Secorvo College, Karlsruhe)
November 2004	
02.-04.11.	Sichere E-Mail-Kommunikation (Secorvo College, Karlsruhe)
09.-11.11.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
22.-26.11.	Information Security Management (Secorvo College, Karlsruhe)

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

Impressum

ISSN 1613-4311

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

Die Zusendung des Inhaltsverzeichnisses können Sie per E-Mail anfordern:
security-news@secorvo.de
(Subject: „subscribe security news“)

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