secorvo
security consulting

Secorvo Security News

Oktober 2008

Editorial: One man – no vote?

Wählen mit Computerhilfe – der Traum aller Wahlhelfer, die unter Zeitdruck tausende Stimmzettel auszählen müssen. Einfach bestechend: Per Mausklick lassen sich Auszählung und Wahlvorgang beschleunigen und Zählfehler ausschließen.

Elektronische Wahlen sind nichts Neues in Deutschland. Die Gesellschaft für Informatik wählt ihr Präsidium seit 2004 über das Internet, an Universitäten wird die Selbstverwaltung mit Computerhilfe bestimmt und in mehreren Bundesländern werden Wahlcomputer bei Kommunal-, Landtags- und Bundestagswahlen eingesetzt. Am 24.10.2008 erhielt Bingo Voting, ein an der Universität Karlsruhe entwickeltes Verfahren mit der Möglichkeit zur Prüfung der korrekten Zählung der eigenen Stimme, den Deutschen Sicherheitspreis 2008.

Tatsächlich ist E-Voting nicht so einfach, wie es scheint. Denn aus der Perspektive des Wählers ist ein Wahlcomputer eine Black Box, der er bei Stimmabgabe blind vertrauen muss. Nicht immer ist dieses Vertrauen berechtigt. So wird in Deutschland der Nedap-Wahlcomputer eingesetzt, ein Gerät, dessen Version ES3B der Chaos Computer Club (CCC) 2006 analysiert hat – mit bitteren Ergebnissen: Der Manipulationsschutz beruht auf simplen, leicht fälschbaren Papiersiegeln, das Master-Passwort war mit „GEHEIM" vorbelegt, und durch einen Firmwaretausch ließ sich der Wahlcomputer in einen Schachcomputer verwandeln (siehe SSN 10/2006). In Brandenburg stellten Wahlbeobachter des CCC am 28.09.2008 – wie zuvor in Hessen – erhebliche Mängel beim Umgang mit den Wahlcomputern fest: Fehlende Siegel, unbeaufsichtigte Lagerung, Fehlbedienung und unerklärliche Zähldifferenzen.

Manipulierbare Wahlcomputer wären eine gefährliche Waffe in den Händen einer Partei oder Regierung. Stimmzettel lassen sich durch Unabhängige nachzählen – Computerdaten nicht. Das wurde auch in der öffentlichen Anhörung vor dem Bundesverfassungsgericht am 28.10.2008 deutlich. Bleibt zu hoffen, dass Papier und Bleistift noch eine Chance haben – wenigstens dann, wenn der Souverän wählt.

Inhalt

secorvo
security consulting

Security News

Clickjacking

Auf der diesjährigen amerikanischen OWASP-Konferenz sorgte das Zurückziehen eines Vortrags zum Thema „Clickjacking“ durch die Autoren Robert „RSnake“ Hansen und Jeremiah Grossman für einiges Aufsehen. Inzwischen sind durch einen Blog-Eintrag Robert Hansens vom 07.10.2008 sowie die Veröffentlichung eines Proof of Concept und eines Videos erste Details zu der architektonisch bedingten Schwachstelle bekannt. Darin werden verschiedene Ausprägungen vorgestellt.

Clickjacking wird das Platzieren eines „unsichtbaren“ Click-Buttons auf einer Webseite genannt, auf den der Nutzer klickt, während er vermeintlich einen darunter liegenden Link auswählt. Bis zur Beseitigung dieser Browserschwachstelle bietet das – auch in anderem Kontext sehr nützliche – Firefox Add-On „NoScript“ mit „ClearClick“ einen gewissen Schutz.

Forensische Spirale 2.0

Seit vielen Jahren schon gehört die Live-CD Helix in den virtuellen Werkzeugkasten jeder Forensikerin. Helix ist eine der wenigen umfangreichen Tool-Sammlungen, die sowohl unter Windows als auch unter Linux zu verwenden sind – sie war allerdings schon etwas in die Jahre gekommen.

Am 15.09.2008 wurde endlich die von vielen herbei gesehnte Helix Version 2.0 veröffentlicht. Wir haben die neue Version in unserem forensischen Labor ausgiebig getestet. Ergebnis: Das Warten hat sich gelohnt. Zunächst wurden die einzelnen Tools auf den neuesten Stand gebracht bzw. um neue Software ergänzt. Die größte Änderung ist jedoch der Umstieg der Boot-Partition auf Ubuntu, was u. a. die Unterstützung neuer Hardware spürbar verbessert. Helix 2.0 ist und bleibt damit eine interessante Ergänzung oder sogar Alternative zu kommerziellen forensischen Tools. Wir werden Helix 2.0 bereits im kommenden Forensik-Seminar berücksichtigen.

Neue Hash-Funktionen

SHA, der Secure Hash Standard, war die erste standardisierte Hashfunktion, 1994 vom US-amerikanischen NIST veröffentlicht. Am 01.08.2002 legte das NIST mit einer erweiterten Spezifikation nach, die vier Varianten der nun SHA-2 genannten Algorithmenfamilie mit unterschiedlich langen Hashwerten umfasste (FIPS PUB 180-2). 2004 wurde die Spezifikation um die Variante SHA-224 ergänzt; eine Endfassung des Standards erschien am 17.10.2008 (FIPS PUB 180-3).

Doch die Tage des in die Jahre gekommenen SHA-2 sind gezählt. Da für einen Nachfolger keine geeigneten alternativen Verfahren in Sicht waren, schrieb das NIST am 02.11.2007 – wie beim AES – einen Wettbewerb für SHA-3 aus. Wenige Tag vor der Einreichungsfrist (31.10.2008) waren schon über 30 Verfahren beim NIST eingegangen. Ein sehr aussichtsreicher Kandidat ist der Skein getaufte Algorithmus einer Kryptographengruppe um Bruce Schneier. Auch ein „Veteran“ ist dabei: Ron Rivest, einer der Väter des RSA-Verfahrens, hat MD6 ins Rennen geschickt.

Virenschutz für VMs

Vom Virenschutz-Anbieter McAfee wurden am 17.09.2008 Lösungen zum Scannen von virtuellen Maschinen vom Virtualisierungs-Host aus (VMware ESX) vorgestellt. Auf den ersten Blick ein vorteilhafter Ansatz: Virtuelle Maschinen werden, auch wenn sie nicht verwendet werden, zentral überprüft, und bei Bedarf wird sogar der auf den Gastsystemen installierte Virenschutz aktualisiert.

Aber Vorsicht: Jedes Gastsystem sollte – wie bei „echten“ physikalischen Servern – über einen installierten und regelmäßig aktualisierten Virenschutz verfügen. Einen Mehrwert bietet die neue Produktserie nur dann, wenn die Systeme gerade ausgeschaltet sind. Auch besteht die Gefahr, sich durch die zusätzliche Software auf dem Hostsystem Angriffsmöglichkeiten und Sicherheitsprobleme einzuhandeln. Denn in den Listen von Produkten mit sicherheitskritischen Fehlern fanden sich in den vergangenen Jahren zahlreiche Hersteller und Produkte von Sicherheitssoftware.

Unsere Empfehlung lautet daher: Keep it simple. ESX-Systeme sollten ohne Verwässerung der Sicherheitsfunktionen wie guter schottischer Whisky genossen werden: pur – und ohne Eis.

Surf-CD vom BSI

Am 08.08.2008 wurde vom BSI eine auf Knoppix basierende „Surf-CD“ vorgestellt. Die Idee dahinter ist, durch Booten von CD ein sauberes System zu erhalten und damit bspw. sicheres Online-Banking zu ermöglichen. Dazu wurde das von CD zu startende System durch mehrere Maßnahmen gehärtet und der verwendete Browser „Iceweasel“, die Debian-Variante von Firefox, durch Sicherheits-Plugins aufgepeppt. Im Vergleich zu anderen Boot-CDs überzeugt unter anderem, dass ein schreibender Zugriff auf weitere Datenträger, beispielsweise auf interne oder externe Festplatten des Systems, kernelseitig unterbunden wird.

Eine gute Lösung für Anwender, die ihr System beim Surfen vor eingefangener Schadsoftware

schützen möchten – oder dem vom Filius zum Spielen genutzten System nicht mehr ihre PINs und TANs anvertrauen mögen.

OWASP Appsec 2008

Am 24.-25.09.2008 fand die OWASP NYC Appsec 2008 Conference im Big Apple statt. Das wachsende Interesse an Applikationssicherheit wurde durch die ansehnliche Zahl von über 850 Teilnehmern eindrucksvoll verdeutlicht. Die an der einen oder anderen Stelle dadurch verursachten Reibungsverluste wurden durch die engagierte Konferenzorganisation überkompensiert.

Fachlich hatte die Tagung einige Highlights zu bieten. Hervorzuheben sind die Vorträge von Gunter Ollmann zum Thema „Multidisciplinary Bank Attacks", Ausflüge in die Praxis von Angriffen wie „Get Rich or Die Trying – Making Money on The Web, The Black Hat Way" von Tom Brennan, Jeremiah Grossman und Trey Ford. Für Interessierte, die nicht an der Konferenz teilnehmen konnten oder verpasste Parallelvorträge ansehen möchten, stehen die Videos der Vorträge online bereit.

Die vorgestellten theoretischen und praktischen Arbeiten sind für die Beschäftigung mit verschiedenen Aspekten der Applikationssicherheit wertvoll. Daher sollte man den Termin der OWASP Germany 2008 Conference am 25.11.2008 in Frankfurt vormerken.

Mifare-Exploit online

Jetzt ist es passiert: Am 27.10.2008 hat ein Hacker unter dem Pseudonym 'Bla' eine C-Implementierung des von der Radboud Universiteit Nijmegen auf der europäischen Sicherheitskonferenz Esorics am 06.-08.10.2008 publizierten Angriffs auf Mifare Classic mit dem Titel „crapto1" auf der Open Source Platform Google Code veröffentlicht. Zwar fehlt zu einer „Plug-and-Play"-Attacke noch die Software für Proxmark oder den OpenRFID Sniffer. Für deren Implementierung sind jedoch keine kryptologischen Kenntnisse erforderlich; die öffentliche Bereitstellung ist daher nur eine Frage der Zeit.

Jetzt hilft kein Abwiegeln mehr: Das Clonen und Manipulieren von Mifare-basierten Chipkarten wird in Kürze ein Kinderspiel sein. Wer Mifare Classic einsetzt, sollte sich daher baldigst geeignete Migrationsstrategien einfallen lassen, um nicht gegen Sorgfaltspflichten zu verstoßen.

BSI meets ISACA

Der bereits am 01.09.2008 veröffentlichte „Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" bildet die Grundlage für die Durchführung von IS-Revisionen in Bundesbehörden gemäß des UP Bund. Das konzeptionell klar strukturierte, 37-seitige Dokument enthält neben den konkreten Durchführungsschritten auch eine Aufwandsschätzung über 30 bis 100 Personentage für die so genannte Querschnittsprüfung. Daraus wird ersichtlich, dass Initial- und Betriebsaufwand für das Thema Informationssicherheit deutlich höher sind als das, was viele Behörden operativ investieren. Als Fachqualifikation für die Befähigung zur IS-Revision wird allgemein auf einen „Nachweis der Qualifikation durch Zertifikate" verwiesen. Eine Chance für den IT-Grundschutz?

Im Oktober 2008 hat das ISACA Germany Chapter den – nur in Papierform erhältlichen – „Leitfaden zur Durchführung eines Quality Assurance Reviews der Internen IT-Revision (QAR-IT)" veröffentlicht. Der zehnseitige Prüfungskatalog ist eindeutig und sehr aussagefähig und wird durch eine vollständige Liste aller Prüfungsstandards abgerundet. Er ist zudem so universal einsetzbar, dass damit auch eine QAR für eine IS-Revision durchgeführt werden kann. In Kombination mit dem Leitfaden des BSI lässt sich damit auch die Frage nach der „Kontrolle des Kontrolleurs" beantworten.

Secorvo News

Secorvo College aktuell

Für Schnellentschlossene bietet Secorvo College 2008 noch zwei Weiterbildungschancen:

- Information Security Management von A(udit) bis Z(erzifizierung) am **18.–21.11.2008** sowie eine
- T.I.S.P.-Schulung am **24.–28.11.2008** mit anschließender Prüfung.

Die Termine der Seminare 2009 stehen inzwischen ebenfalls fest – eine praktische Übersicht bietet der ganzjährige College-Kalender.

Detaillierte Seminarprogramme und die Möglichkeit zur Online-Anmeldung (auch schon für 2009) finden Sie unter http://www.secorvo.de/college.

Original oder Fälschung?

Seit fast 20 Jahren prägt ein Karlsruher Unternehmen, die WIBU-Systems AG, die weltweite Entwicklung des „Digital Rights Managements" zum Schutz digitaler Produkte – Software, Dokumente, Medien. Auf dem letzten diesjährigen Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am 04.12.2008 wird Rüdiger Kügler spannende Einblicke in die rasante Entwicklung der DRM-Technologie geben – und zeigen, was uns hinsichtlich des Schutzes digitaler Güter in den kommenden Jahren erwartet.

Veranstaltungshinweise

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

November 2008	
04.-05.11.	Praxistage Datenschutz (BvD, Stuttgart)
11.-13.11.	Forensik (Secorvo College)
18.-21.11.	Information Security Management (Secorvo College)
24.-28.11.	T.I.S.P - Schulung (Secorvo College)
25.11.	OWASP Germany 2008 Conference (www.owasp.org, Frankfurt)
29.-30.11.	ruxcon 2008 (ruxcon.org, Sydney/AU)
Dezember 2008	
04.12.	„Das Original ist die beste Kopie“ (KA-IT-Si, Karlsruhe)
27.-30.12.	25th Chaos Communication Congress (CCC, Berlin)
Januar 2009	
20.-22.01.	Omnicard 2009 (inTIME, Berlin)

Fundsache

Am 29.09.2008 hat das US-amerikanische NIST in der Reihe Special Publication einen 80seitigen „Technical Guide to Information Security Testing and Assessment“ (NIST Special Publication 800-115) veröffentlicht, das eine sehr hilfreiche und praktisch-konkrete Handreichung zur Durchführung von Information Security Audits darstellt. Alle wesentlichen Risiken einer Netzwerkinfrastruktur werden betrachtet und eine systematische Vorgehensweise für deren Analyse vorgeschlagen. Abgerundet wird das instruktive Dokument durch eine aktuelle Liste frei verfügbarer Tools und Informationsquellen über bekannte Schwächen.

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Alexander Göbel, Stefan Gora, Kai Jendrian, Stefan Kelm, 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