secorvo
security consulting

Secorvo Security News

Februar 2008

Editorial: Captcha

Informatiker kennen den nach seinem Erfinder Alan Turing (1912-1954) benannten Turing-Test, in dessen Verlauf ein Mensch in fünf Minuten entscheiden soll, welcher von zwei mit ihm über einen Computer verbundenen Gesprächspartnern eine Maschine und welcher ein Mensch ist. Bis heute hat es kein Computerprogramm geschafft, einen menschlichen Tester zu täuschen.

Diese Frage nach der Unterscheidbarkeit von „künstlicher" und „menschlicher" Intelligenz, die in den 80er Jahren die Informatik aufwühlte, ist heute hinter eine andere zurückgetreten: Kann ein *Computer* entscheiden, ob ein Computer mit ihm spricht? Dieser gewissermaßen „umgekehrte Turing-Test" entwickelt sich zur Schlüsselfrage zahlreicher Web-Angebote. Denn vielfach sind automatische „Gesprächspartner" unerwünscht, wie z. B. Antwort-Automaten bei Wissenstests, Trojaner beim Online-Banking oder Spam-Bots, die Suchmaschinen für die Recherche von E-Mail-Adressen einspannen und News-Weiterleitungen für Postings missbrauchen.

Als Fachbegriff für solche Tests hat sich das Akronym „CAPTCHA" durchgesetzt: *Completely Automated Public Turing test to tell Computers and Humans Apart*. Dabei wird dem Nutzer des Angebots eine Aufgabe gestellt, die möglichst nur ein Mensch lösen kann – meist das Herauslesen verfremdeter Ziffern und Buchstaben aus einer Grafik. In zahlreichen Anwendungen werden solche Bild-CAPTCHAs inzwischen als Sicherheitsmechanismus eingesetzt. Ein Problem dieser CAPTCHA-Mechanismen ist, dass für viele nach und nach automatische Lösungen entwickelt werden, und daher deren Komplexität ständig zunimmt. Je komplizierter aber das CAPTCHA, desto schwerer ist es auch für einen Menschen zu lösen.

Austricksen lassen sich CAPTCHAs aber noch viel einfacher: Präsentiert ein Online-Banking-Trojaner ein abgefangenes CAPTCHA auf einer vielbesuchten Erotik-Seite, erhält er die Lösung in Sekunden „frei Haus" – beantwortet von einem unwissentlichen Mittäter. Sicherheit ist eben mehr als die Summe guter Mechanismen.

Inhalt

secorvo
security consulting

Security News

TrueCrypt 5

Die freie Software TrueCrypt zur Verschlüsselung von Daten auf Festplatten ist am 05.02.2008 in der Version 5 erschienen. Highlight der Neuerungen ist die Möglichkeit, nun auch die komplette Festplatte inklusive Betriebssystem zu verschlüsseln. Weiter wurde erstmals eine Version für Mac OS X veröffentlicht, und Linux-Benutzer können sich endlich über eine grafische Oberfläche freuen. Zusätzlich gab es einige Detailänderungen bei den genutzten kryptografischen Verfahren.

Erste Tests bestätigen den guten Eindruck früherer Versionen der Software. Sowohl die Vollverschlüsselung als auch die Kompatibilität mit alten Versionen funktionierten problemlos. TrueCrypt ist eine gut gemachte, kostenlose Verschlüsselungssoftware. Neben vielen guten Eigenschaften lässt sie allerdings einige für den Einsatz in Enterprise-Umgebungen wichtige Funktionalitäten wie z. B. Mehrbenutzerfähigkeit und PKI-Anbindung vermissen.

Leitfaden Kritis

Am 24.01.2008 stellte Staatssekretär Dr. August Hanning vom Bundesministerium des Inneren den neuen Leitfaden „Schutz Kritischer Infrastrukturen - Risiko- und Krisenmanagement" vor. Das 87-seitige Dokument wendet sich primär an Behörden und Unternehmen mit Verantwortung im Bereich KRITIS. Der Leitfaden beschreibt die Phasen Vorplanung, Risikoanalyse, Vorbeugende Maßnahmen und Krisenmanagement und stellt einen umfangreichen Anhang mit Literatur, Gefahrenlisten, Checklisten und einer beispielhaften Risikoanalyse zur Verfügung. Auch für Unternehmen und Behörden, die nicht zu den primären Adressaten des Leitfadens zählen, enthält das Dokument interessante Ansätze für Risiko- und Krisenmanagement. Weitere gute Dokumente zum Thema bietet die Risk Management Series der amerikanischen Federal Emergency Management Agency (FEMA).

ITGK-Ergänzung 9

Seit dem 15.02.2008 ist die 9. Ergänzungslieferung der IT-Grundschutzkataloge online und zum Download auf den Seiten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) verfügbar. Eine angepasste Version des Grundschutztools GSTOOL ist angekündigt.

Die Weiterentwicklung umfasst neue Bausteine, die sich u. a. mit Themen wie elektrotechnischer und IT-Verkabelung, Netzdruckern, Datenträgeraustausch und dem unscheinbaren, aber immer wichtigeren Thema „mobile Datenträger" beschäftigen. Zusätzlich sind neue Maßnahmen und Gefährdungen in die Kataloge eingearbeitet worden.

Auch sprachlich passt das BSI die Kataloge dem wachsenden Bedürfnis nach umfassender Informationssicherheit an. Sukzessive wird der etablierte Begriff „IT-Sicherheit" durch „Informationssicherheit" ersetzt – das ist ein sehr sinnvoller Schritt, geht es doch um den Schutz von Informationen unabhängig von der Form, in der sie vorliegen.

Metasploit 3.1

Am 28.01.2008 wurde Version 3.1 des Metasploit Project vorgestellt, dessen Ziel es ist, Penetrationstestern, Forschern und Exploit-Entwicklern aktuelle Informationen und Hilfsmittel zu Exploit-Techniken verfügbar zu machen. Die neue Version enthält Werkzeuge beispielsweise zur Sicherheitsüberprüfung von WLANs und des neuen Apple iPhone, wurde um weitere Funktionen ergänzt und bietet nun auch unter Windows eine vollständige grafische Oberfläche.

Ergonomie und Leistungsfähigkeit des Werkzeugs sind beachtlich. Wie so viele „dual use"-Produkte wird es in den falschen Händen allerdings zu einem mächtigen Angriffswerkzeug, mit dem sich erheblicher Schaden anrichten lässt.

Shmoocon 2008

Auf der diesjährigen Shmoocon (15.-17.02.2008) wurden eine ganze Reihe neuer Angriffstechniken vorgestellt. Besonders interessant waren das Entschlüsseln von GSM-Verbindungen mit vertretbaren Investitionskosten, potentielle Schwachstellen auf Citrix-Servern und das Einbringen von echten Exploits in virtuelle Welten wie „second live". Daneben wurden auch gesellschaftspolitische Themen wie die soziale Verantwortung der Hacker-Community diskutiert und Hilfsprojekte wie Hackers for Charity vorgestellt.

In seiner Keynote am 15.02.2008 stellte Alex Halderman unglaubliche Sicherheitsmängel amerikanischer Wahlcomputer vor. Stimmt der Dateiname, wird ein infiziertes Systemimage anstandslos geladen und kann sich über eine PCMCIA-Speicherkarte auf weitere Wahlcomputer verbreiten. Prüfsummen und kryptografische Schutzmechanismen sucht man vergeblich; der PCMCIA-Schacht kann nur mit einem Schloss physikalisch gesperrt werden – das bau- und „schlüsselidentisch" mit einem bei Jukeboxen und Geldspielgeräten eingesetzten ist. Nach dem holländisch-deutschen Wahlmaschinen-Debakel (siehe SSN 10/2006) ist nun vielleicht auf politische Einsicht zu hoffen – auch bei der Entwicklung und Prüfung von Wahlmaschinen

sollte man jemanden fragen, der etwas davon versteht. Die Vortragsunterlagen und Videos der gelungenen Veranstaltung können in Kürze von der Website geladen werden.

Protokollierung

Das Thema Protokollierung ist so etwas wie die Achillesferse der IT-Sicherheit: fast jedes System bietet Protokolldaten, die Auswertungstools sind meist primitiv, die Formate uneinheitlich – und nicht jede Protokollierung ist zulässig. Mit der am 17.01.2008 veröffentlichten „Studie über die Nutzung von Log- und Monitoringdaten im Rahmen der IT-Frühwarnung und für einen sicheren IT-Betrieb“ will das BSI Licht in den Logdatendschungel bringen – und hat dem Thema möglicherweise einen Bärendienst erwiesen.

Die 294 Seiten umfassende Fleißarbeit listet die Merkmale von Logdateien wichtiger Systeme und Anwendungen auf, ignoriert aber die rechtlichen Anforderungen praktisch vollständig. Die wenigen Andeutungen zu Anforderungen des Datenschutzrechts sind irreführend bis falsch und lassen diesbezügliche Unkenntnis der Autoren vermuten; Hinweise auf Mitbestimmungspflicht und die Unzulässigkeit der Speicherung von Verbindungsdaten nach Telekommunikationsgesetz fehlen ganz. Von einer Umsetzung der Empfehlungen der Studie ohne vorausgehende Betrachtung der rechtlichen Anforderungen wird daher dringend abgeraten.

OWASP Publikationen

Veröffentlichungen der OWASP-Initiative sind seit Kurzem über den digitalen Verlagsmarktplatz LULU in gedruckter Form oder als formatiertes PDF verfügbar. Die Prints sind preislich sehr attraktiv, die PDFs kostenlos und tragen hoffentlich dazu bei, die qualitativ sehr hochwertigen Informationen der OWASP weiter zu verbreiten.

Der neue Gola/Wronka

Peter Gola und Georg Wronka haben Ihr Standardwerk „Handbuch zum Arbeitnehmerdatenschutz“ erneut überarbeitet und am 28.11.2007 in einer aktualisierten 4. Auflage herausgebracht.

Leider konnten sich die Autoren nicht von ihrem Konzept trennen, das sich an Verarbeitungsphasen orientiert, wodurch die Erörterung praktisch zusammenhängender Themen häufig in unterschiedlichen Kapiteln erfolgt. Auch wenn der Praktiker einige brandaktuelle Themen vermisst (z. B. Forensische Untersuchungen) und andere sehr allgemein abgehandelt werden (z. B. Whistleblowing), so bietet das Werk doch nach wie vor einen guten Überblick und stellt insbesondere die Verschränkung mit Mitbestimmungsfragen umfassend dar.

Secorvo News

Secorvo College aktuell

Die CeBIT wird es wieder zeigen: PKIs leben – wenn auch oft versteckt als „Treibsatz“ z. B. hinter E-Mail-Verschlüsselungslösungen. Wer verstehen will, wie PKIs funktionieren, wie sie aufgebaut und in Anwendungen und Verzeichnisdienste integriert werden, dem sei das Seminar PKI – Grundlagen, Vertiefung, Realisierung vom **11.–14.03.2008** ans Herz gelegt. Das Seminar umfasst praktische Übungen.

Der „Klassiker“ IT-Sicherheit heute wird wegen der hohen Nachfrage als Zusatztermin vom **27.–30.05.2008** stattfinden. Nach einer grundlegenden Überarbeitung und Aktualisierung deckt die Agenda jetzt in vier Tagen die wichtigsten aktuellen Themen der IT-Sicherheit ab. Eine Einführung in das Information Security Management von A(udit) bis Z(ertifizierung) mit Umsetzungsworkshop bietet Secorvo College vom **15.–18.04.2008**.

Detaillierte Programme, vollständige Jahresübersicht und Online-Anmeldung unter http://www.secorvo.de/college

Identity Management Symposium

In vielen Unternehmen existieren historisch bedingt zwei „Identitäts-Management“-Systeme unverbunden nebeneinander: Der Betriebsausweis, meist im Verantwortungsbereich der Corporate Security, und die Benutzerauthentifikation mit Rechnerzugang, in der Regel in der Zuständigkeit der IT-Security. Dabei kommt es zu Doppelarbeit, denn für beide Bereiche ist das Management eines „Berechtigungs-Lebenszyklus“ erforderlich.

Mit der Verbreitung elektronischer Zugangssysteme und Authentifikationslösungen, die Passworte durch Token ersetzen, rücken beide Systeme zusammen: Idealerweise sollten alle an die Identität eines Mitarbeiters gekoppelten Dienste über eine Karte möglich sein. Erste Unternehmen haben inzwischen ihre Identity Management-Systeme zusammengeführt. Die Komplexität dieser Projekte lag dabei sowohl in der Technik als auch in zahlreichen zu bewältigenden praktischen „Fallstricken“.

Gemeinsam mit der vps GmbH will Secorvo mit dem „Identity Management Symposium“ am **22.–23.04.2008** einen intensiven Erfahrungsaustausch mit und zwischen Unternehmen und Behörden initiieren, die ein solches integriertes „Identity Management“ vorbereiten oder bereits eingeführt haben (Programm, Online-Anmeldung).

Veranstaltungshinweise

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

März 2008	
09.-12.03.	11. International Workshop on Practice and Theory in Public Key Cryptography (IACR, Barcelona/ES)
11.-14.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College, Karlsruhe)
19.-21.03.	5. Theory of Cryptography Conference (TCC 2008) (IACR, New York/US)
April 2008	
02.-04.04.	Sicherheit 2008 (GI, Saarbrücken)
14.-17.04.	Eurocrypt 2008 (IACR, Istanbul/TR)
15.-18.04.	Information Security Management - von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
15.04.	First USENIX Workshop on Large-scale Exploits and Emergent Threats (Usenix, San Francisco/US)
22.-23.04.	Identity Management Symposium 2008 (Secorvo, Karlsruhe-Ettlingen)
Mai 2008	
06.-07.05.	9. Datenschutzkongress 2008 (Euroforum, Berlin)
06.-08.05.	IT-Sicherheitsaudits in der Praxis (Secorvo College, Karlsruhe)
26.-29.05.	IT Sicherheitsforum 2008 (GAI Netconsult, Frankfurt)
27.-30.05.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
Juni 2008	
02.-06.06.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Karin Schuler

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