secorvo
security consulting

Secorvo Security News

Februar 2010

Editorial: Gotcha

Mit jedem Klick im Browser geben wir viele Informationen preis, die wir für sich genommen harmlos finden. Bei genauer Betrachtung zeigt sich aber, dass 33 bit Information ausreichen, um einen Menschen weltweit eindeutig zu identifizieren. Jeder Browser übermittelt in der Grundeinstellung zahlreiche Daten, die geeignet sind, einen digitalen Fingerabdruck des Surfers zu erstellen. Durch clevere Ergänzungen verraten Browser weitere Informationen wie die eingesetzten Add-Ons oder das Zeitverhalten bei der Passwort-Eingabe.

Damit nicht genug: Wie seit fast acht Jahren in der Mozilla-Community diskutiert, lassen sich den Browsern durch History-Stealing Informationen über vormals besuchte Seiten entlocken. Diese Technik wird von Internetseiten wie didyouwatchporn.com oder whattheinternetknowsaboutyou.com eindrucksvoll demonstriert. Mag man diese Seiten noch amüsant finden, vergeht einem das Lachen spätestens bei der Lektüre der Studie „A Practical Attack to de-Anonymize Social Network Users“, in der erläutert wird, wie durch History-Stealing die tatsächliche Identität eines Surfers über das Nutzerverhalten in Sozialen Netzwerken ermittelt werden kann – dies lässt sich im Selbstversuch leicht überprüfen.

Diese Techniken sind leider nicht nur von theoretischer Bedeutung, sondern werden teilweise schon zum Tracking von Surfern eingesetzt. Mit etwas Fantasie lässt sich ausmalen, was möglich wäre, wenn Dienste wie Google-Analytics oder etracker damit arbeiten würden. Die Tendenz, die Privatsphäre von Internet-Nutzern einzuschränken, ist – aus unterschiedlichen Motiven – weit verbreitet, das zeigen Initiativen wie die Vorratsdatenspeicherung, der Bundestrojaner oder die zahlreichen Datenschutzskandale in der Wirtschaft.

Kundige Nutzer können durch Selbstschutzmaßnahmen ihre Situation verbessern. Für den Schutz der Privatsphäre aller Internet-Nutzer ist es jedoch erforderlich, dass Browser diesen in der Grundkonfiguration respektieren.

Inhalt

secorvo
security consulting

Security News

Bitte einbrechen!

Einsichtsfähigkeit zählt im Allgemeinen nicht zu den menschlichen Stärken. Noch seltener gelingt es den meisten Menschen, die Kluft zwischen Einsicht und Umsetzung zu schließen. Ein Paradebeispiel dafür ist die wachsende Begeisterung, mit der Privates auf Portalen wie StudiVZ, Wer-kennt-wen, Facebook oder Xing preisgeben wird – und Hunderttausende ihren Tagesablauf via Twitter herauszwitschern.

Am 17.02.2010 ging die Webseite „Please rob me!“ online – eine Art „Awareness-Service“ für Uneinsichtige, betrieben von forthehack (Rijswijk). Eine automatische Twitter-Suche liefert alle aktuellen Nachrichten, aus denen die Abwesenheit von zu Hause erkennbar ist, und zeigt Namen, Foto und den aktuellen Aufenthaltsort an (via foursquare). Zugegebenermaßen eine drastische Methode – aber vielleicht wirksamer als Predigten. Wie wäre denn eine Webseite „Don't hire me!“ mit den heftigsten StudiVZ-Fotos vom vergangenen Wochenende?

25 MDPE

Am 17.02.2010 wurden die von Mitre und SANS zusammengestellten „2010 CWE/SANS Top 25 Most Dangerous Programming Errors“ als grundlegende Überarbeitung der vorjährigen Liste veröffentlicht. Wenig überraschend finden sich unter den schwerwiegendsten Schwachstellen Cross Site Scripting, SQL-Injection und Cross Site Request Forgery wieder auf den Plätzen eins, zwei und vier.

Bahnbrechend neue Erkenntnisse liefert die Liste nicht – Dokumente wie die OWASP Top Ten oder WASC Threat Classification (SSN 01/2010) weisen auf die gleichen Gefahren hin. Im Gegensatz zu diesen beiden Dokumenten adressiert die CWE/SANS-Liste die Probleme aus Entwicklersicht und bietet, auch durch Verweis auf die deutlich umfangreichere „Common Weakness Enumeration“-Datenbank, konkrete Hilfestellung zur Vermeidung oder Behebung der identifizierten Probleme. Softwareentwicklern sind alle drei Dokumente zur regelmäßigen Lektüre zu empfehlen.

Film-Tipps für Chipkartenfans

Im Januar machte ein RBB-Video Furore, das die Umsetzung des Angriffs auf Legic Prime (siehe SSN 01/2010) am Hamburger Flughafen zeigt. Im Februar sind gleich zwei spannende Videos zu empfehlen: Bei der Konferenz Blackhat DC präsentierte Chris Tarnovsky am 02.02.2010 das Ergebnis monatelanger Analysen: Mit einer Laborausstattung zum geschätzten Anschaffungspreis von US$ 200.000 und unter Verschleiß etlicher Testmuster gelang es ihm, geheime Daten aus dem Trusted Platform Module (TPM) einer XBox Spielekonsole auszulesen – einem TPM-Chip der Infineon SLE66 Smartcard-Chipfamilie. In einem Wired-Video vom 23.08.2008 hatte Tarnovsky bereits demonstriert, wie er einen Smartcard-Chip und seine Datenleitungen frei legt. Nun gibt es eine belegte Abschätzung des nötigen Aufwands an Geld und Zeit.

Den Sicherheitsforschern der Universität Cambridge um Ross Anderson gelang es derweil, mit einem am 11.02.2010 als Vorabdruck veröffentlichten Man-in-the-Middle Angriff das EMV-basierte „Chip & PIN“ Verfahren zu brechen, das in Großbritannien für Kartenzahlungen am Point of Sale (POS) eingesetzt wird. Dabei gaukelten sie der Karte vor, dass das Terminal eine Transaktion mit Unterschrift (statt PIN) angefordert hat, während sie dem Terminal signalisierten, dass eine (beliebige) Ziffernkombination von der Karte als gültige PIN akzeptiert wurde. Die zwischen der (gestohlenen) echten Karte und dem ins Terminal eingesteckten Kartenadapter eingeschobene Gerätschaft passt, wie in einem BBC-Video zum Bericht vom 11.02.2010 demonstriert, bequem in einen Rucksack.

Spektakulär an dem Angriff ist, dass er auch im Online-Modus des POS-Terminals funktioniert und der Kundenbeleg „PIN verified“ ausweist. Chip&PIN verstößt offenbar gegen die wichtige Design-Maxime für kryptografische Protokolle, dass in die errechneten Authentisierungs- oder Signaturdaten alle relevanten Statusinformationen eingehen müssen – in diesem Fall auch die Tatsache, ob eine PIN angefordert bzw. verwendet wurde.

Wert von Sicherheitsbeweisen

Quantenkryptografie wurde bisher von seinen Protagonisten als absolut sichere Verschlüsselungsmethode verkauft, da die Grundlagen des Quanten-Schlüsselaustauschs auf den ehernen Gesetzen der Quantenphysik basieren. Der Traum vom praktisch verwendbaren One-Time-Pad war in so greifbare Nähe gerückt, dass es schon erste kommerzielle Produkte dafür gibt. So bestechend der Sicherheitsbeweis für Quantenkryptografie ist – man muss auch auf die äußeren Umstände einer Implementierung achten, denn der Beweis setzt voraus, dass ein Angreifer den Austausch nicht beobachten kann, ohne bemerkt zu werden.

In einem Beitrag auf dem CCC-Kongress führte ein Team aus Singapur am 27.12.2009 vor, wie gängige Implementierungen ausgehebelt werden können, indem sie geblendet werden. Die Quantenphysik beschreibt Phänomene im mikroskopischen Bereich, was jedoch nicht bedeutet, dass es keine Wechsel-

wirkung mit der makroskopischen Welt gibt. Dies zeigt, dass die Quantenkryptografie noch am Anfang steht, und dass noch Jahre bis zur Entwicklung praxistauglicher Verfahren vergehen werden.

Es zeigt darüber hinaus, dass man die Annahmen, die einem Sicherheitsbeweis zugrunde liegen, sehr genau verstehen muss. Nicht umsonst hat die Forschung etwa zwanzig Jahre gebraucht, um ein brauchbares und allgemein anerkanntes Modell für die Sicherheit von Verschlüsselung zu finden. Dabei wurden viele Beweise und Modelle verworfen, weil die Annahmen zu stark oder implizite Annahmen unrealistisch waren. Es bedeutet jedoch nicht, dass man auf Sicherheitsbeweise verzichten kann, denn ad-hoc-Konstruktionen und intuitive Entwürfe taugen erst recht nicht – das immerhin ist gut belegt.

Learning Websecurity by Doing

Ausprobieren ist eine der besten Methoden, um komplexe Sachverhalte zu verstehen. Diesen Ansatz verfolgt das OWASP WebGoat Projekt. Bisher waren allerdings zu Beginn einige Hürden zu nehmen, wie die manuelle Installation der Anwendung. Seit dem 27.01.2010 ist das nicht mehr erforderlich: Das OWASP Broken Web Applications Projectwaspbwa (owaspbwa) bietet eine VMware-kompatible virtuelle Maschine zum Download an, die eine Vielzahl fertig installierter schwachstellenbehafteter Web-Anwendungen enthält. Dem Lernbegierigen stehen neben WebGoat Konzeptanwendungen wie Vicum, Multidae, Damn Vulnerable Web App und andere, auch ältere Versionen mit echten Bugs von phpBB, WordPress und Yazd zur Verfügung. Wir wünschen viel Erfolg beim „Hands on"-Training.

Brothers are Listening

Aufgrund des am 20.02.2010 auf CryptoMe.org veröffentlichten „Microsoft® Online Services Global Criminal Compliance Handbook" ließ Microsoft die Domäne am 25.02.2010 wegen Verstoßes gegen den Digital Millennium Copyright Act (DMCA) kurzzeitig sperren. Das Dokument vom 29.05.2008 zählt auf Seite 22 die im Rahmen von Auskunftsersuchen der US-Behörden zu liefernden Daten auf. Betroffen sind der Freemail-Dienst Hotmail, die Authentifizierung Windows Live ID, das Instant Messaging mit Windows Live Messenger und das Unterhaltungsportal Xbox. Bei anderen amerikanischen Online-Diensten wie Facebook, Skype, Paypal, MySpace oder Yahoo sieht es hinsichtlich der Kooperationsfreude mit Behörden ähnlich aus, wie die ca. 30 „Lawful Spy Guides" auf CryptoMe belegen.

Zwar haben Benutzer dieser Dienste im Rahmen der Registrierung einer solchen Weitergabe ihrer Daten zugestimmt. Vermutlich werden diese Nutzungsbedingungen aber ebenso genau und häufig gelesen wie kleingedruckte AGB – unterliegen nur nicht denselben Verbraucherschutzbestimmungen. Die Gestaltung der Dienste genügt zudem meist nicht den Anforderungen des Telemediengesetzes (TMG) vom 26.02.2007, das in § 13 wichtige datenschutzrechtliche Anforderungen stellt, darunter die Widerrufbarkeit von Einwilligungen, die Erstellung ausschließlich pseudonymer Nutzungsprofile und die Möglichkeit zur anonymen Nutzung.

Durchsetzbar sind diese Anforderungen bei amerikanischen Anbietern nicht. Zu denken gibt allerdings, dass inzwischen deutsche Anbieter den Amerikanern nacheifern. Angesichts der bekannt gewordenen Datenschutz-Skandale lässt diese Entwicklung für die Zukunft Böses befürchten.

Secorvo News

Secorvo College aktuell

Noch immer wartet das Ausführungsgesetz zum Datenschutzaudit auf seine Verabschiedung. Des ungeachtet sind Datenschutzaudits bereits gängige Praxis in vielen Unternehmen. Das Seminar „Datenschutzaudit: Best Practice" am **20.–21.05.2010** stellt vor, welche Vorgehensweisen sich in der Praxis bewährt haben.

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

Security News Symposium

Am **20.–21.04.2010** ist es so weit – wir laden Sie herzlich ein zum ersten „Security News Symposium". Zahlreiche aktuelle Themen, die uns immer wieder in den Security News beschäftigen, werden im Zentrum intensiver Diskussionen stehen: Von neuen Bedrohungen durch und Empfehlungen zum Umgang mit USB-Sticks über Erfahrungen mit Krisenmanagement-Übungen, die Herausforderung iPhone, die Zukunft von Mifare und digitalen Signaturen bis zu verwurzelten Passwort-Mythen. Wir freuen uns auf Ihre Teilnahme.

Tag der IT-Sicherheit

Den 15.07.2010 sollten Sie sich vormerken: Dann findet der zweite Karlsruher „Tag der IT-Sicherheit", eine Kooperationsveranstaltung der KA-IT-Si mit der IHK Karlsruhe und dem Cyberforum e.V., im Saal Baden der IHK Karlsruhe statt. Es erwarten Sie Praxisberichte u. a. zu den Themen Wirtschaftsspionage, PDA-Sicherheit und Awareness.

Veranstaltungshinweise

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

März 2010	
08.-11.03.	Audit Challenge 2010 (Frankfurt School of Finance & Management, Frankfurt/Main)
23.-25.03.	Sicherheitsmanagement heute (Secorvo College)
April 2010	
13.-16.04.	PKI (Secorvo College)
20.-21.04.	Security News Symposium 2010 (Secorvo, Ettlingen)
20.-22.04.	Datenschutztage 2010 (FFD Forum für Datenschutz, Frankfurt)
27.-28.04.	a-i3/BSI-Symposium 2010 (Arbeitsgruppe Identitätsschutz im Internet/BSI, Bochum)
27.-29.04.	Forensik – Verfahren, Tools, Praxis (Secorvo College)
Mai 2010	
04.-05.05.	11. Datenschutzkongress 2010 (EUROFORUM, Berlin)
17.-19.05.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
20.-21.05.	Datenschutzaudit – Best Practice (Secorvo College)
25.-28.05.	3rd Int. Workshop on Post Quantum Cryptography PQCrypto 2010 (Cased, Darmstadt)

Fundsache

Der bewährte Mustervertrag des Bitkom zur Auftragsdatenverarbeitung liegt seit dem 04.12.2009 in einer neuen, an die Änderungen des BDSG angepassten Fassung 3.0 (inkl. Erläuterungen in Englisch) vor.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, 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