SWISS ENGINEERING
FAEL, Langackerweg 10, 5303 Würenlingen
Tel. (+41 44) 268 37 11, info@fael.ch, www.fael.ch

Internet-Security – Wo lauern die Gefahren?

Institut für Kommunikationssysteme ICOM der HSR Hochschule für Technik Rapperswil

Am 5. November 2008 fand das Seminar «Internet-Security - Wo lauern die Gefahren?» statt. Fünf Vertreter von Hochschulen und dem Bund referierten über verschiedenste Gefahren und Bedrohungsszenarien im Zusammenhang mit dem Internet. Rund 90 Zuhörerinnen und Zuhörer zeigten, dass das Thema aktuell ist und interessiert.

Bilder: Daniel Megnet

Internet-Security geht heute jeden an.

Organisiert wurde der Anlass durch die Fachgruppe Elektronik und Informatik (FAEL) des Swiss Engineering STV unter Mithilfe der Informationstechnischen Gesellschaft ITG und des Instituts für Kommunikationssysteme ICOM der HSR Hochschule für Technik Rapperswil.

Der erste Vortrag des Abends mit dem Titel „Alice, Bob and the man in the middle" schuf die Grundlagen für die nachfolgenden Präsentationen und Diskussionen und wurde durch Carlo Nicola, Professor an der Fachhochschule Nordwestschweiz, bestritten. Es ging um sogenannte Dreiecksbeziehungen, welche auch in diesem Zusammenhang höchst unerwünscht sind, und um die mathematischen Modelle, welche sie beschreiben. Schutz gegen solche „man-in-the-middle"-Angriffe schaffen Authentifikationsprotokolle wie Diffie-Hellmann oder RSA. Beide Protokolle beruhen darauf, dass eine bestimmte Funktion (z.B. das Produkt zweier Primzahlen oder die Exponentialfunktion in einem finiten Feld) relativ einfach, deren Umkehrfunktion aber nicht in vernünftiger Zeit zu berechnen ist. Die dadurch erlangte Sicherheit nützt allerdings nichts gegen Phishing-Attacken und ähnliche Bedrohungen, die darauf abzielen, geheime Daten direkt von der Benutzerin oder dem Benutzer zu erhalten.

Die meisten Angriffe im Internet richten sich heute gegen Web-Applikationen. Weil fast jede Firma Web-Applikationen in irgendeiner Form einsetzt, kann kein Unternehmen die damit verbundenen Sicherheitsprobleme ignorieren. Marc Rennhard, Professor der Zürcher Hochschule für Angewandte Wissenschaften, illustrierte im zweiten Referat zum Thema „Angriffe auf Web-Applikationen" solche Sicherheitsprobleme. Angriffsszenarien wie SQL-Injection und Cross-Site-Scripting wurden nicht nur erklärt, sondern anhand kurzer Demos eindrücklich gezeigt. Viele zurzeit aktive Web-Applikationen sind anfällig auf solche Angriffe. Man kann so relativ leicht an sensible Kundeninformationen und Passwörter gelangen.

Stefan Frei, Doktorand und Dozent an der ETH Zürich, präsentierte aktuelle Forschungsresultate im Zusammenhang mit dem Verhalten, welches grosse Firmen wie Microsoft und Apple an den Tag legen, wenn es um die schnelle Behebung von entdeckten Sicherheitslücken geht. Das sogenannte Sicherheitsökosystem wurde anhand dieser Resultate charakterisiert. Die gesammelten Daten

FAEL, Langackerweg 10, 5303 Würenlingen
Tel. (+41 44) 268 37 11, info@fael.ch, www.fael.ch

1) Carlo Nicola: „Phishing-Attacken lassen sich vor allem mit gesundem Menschenverstand und Skepsis vermeiden."

2) Marc Rennhard: „Einfache Javascripts lassen sich oft in Web-Formularen ausführen und können Passwortinformationen aufdecken."

3) Stefan Frei: „Die Vendors haben realisiert, dass sie die Hacker-Community auf ihre Seite bringen müssen."

4) Marc Henauer: „Der Cybercrime-Markt ist etabliert und hochrentabel."

5) Eric Dubuis: „Es gibt Länder, welche die Einführung von E-Voting-Technologien wieder rückgängig gemacht haben."

widersprachen dem allgemeinen Gefühl, dass Apple-Produkte sicherer seien als jene von Microsoft. Korrelationen mit den Release-Zeiten verschiedener Softwareversionen zeigen, dass schnelle Behebungszeiten vor allem in ruhigen Zeiten zwischen den Releases möglich sind (denn da haben die Software-Entwickler Zeit).

Die aktuellen Bedrohungen für die Informations- und Kommunikationstechnologien wurden von Marc Henauer, Chef der Sektion MELANI/Cybercrime beim Dienst für Analyse und Prävention des Bundesamtes für Polizei, illustrativ aufgelistet. Die entsprechenden Akteure und ihre Mittel sowie der Untergrundmarkt wurden beleuchtet und die damit verbundenen möglichen Abwehr- und Sicherheitsmassnahmen diskutiert. Zunehmend wichtig ist eine integrale und umfassende Lösung im Bereich der Informationssicherung, welche nicht mehr nur auf IT-Sicherheit basiert, sondern auch ein entsprechendes Handling des Benutzers mit vertraulichen Daten voraussetzt.

Die Tagespresse berichtete im vergangenen Jahr regelmässig über neue Pilotprojekte im Bereich E-Voting. Eric Dubuis, Professor an der Berner Fachhochschule, gab im abschliessenden Vortrag einen Überblick über den aktuellen Stand und die gemachten Erfahrungen. Er erklärte die sich zum Teil widersprechenden Anforderungen an elektronische Wahlsysteme und zeigte, wie mittels E-Voting-Protokollen in elektronischen Wahlsystemen versucht wird, diese Anforderungen zu erfüllen. Im Gegensatz zu E-Banking, wo erfolgreiche Angriffe aufgedeckt werden (im Nachhinein auf Grund des Kontoauszugs), sind Angriffe auf E-Voting Systeme nicht als solche erkennbar. Ausserdem sind die Folgen schwerwiegend und von bleibender Natur. Häufig müssen komplexe kryptographische Mechanismen wie blinde Signatur und anonyme Kanäle verwendet werden, um die Sicherheit zu garantieren. Trotz dieser Mittel bleiben bestimmte Risiken bestehen. Das Hauptrisiko ist auf der Plattform der Benutzerin oder des Benutzers zu orten, z.B. durch Computer-Viren oder Trojaner. (*Heinz Mathis)* ■

Die Unterlagen zu den einzelnen Vorträgen sind online verfügbar unter: http://www.fael.ch (Downloads in Menubar wählen).

infoDIREKT www.elektronikjournal.de textcode

Wiederum wurde die Gelegenheit zur Diskussion beim anschliessenden Apéro rege genutzt.

Veranstaltungskalender

Wissensmanagement in der Industrie
Dienstag, 20. Januar 2009, 9:00 - 17:00, Hotel Arte,
Riggenbachstrasse 10, 4600 Olten,
Info und Anmeldung: www.fael.ch ➔ Anlässe ➔ Focus 539

Feierabend-Event: Konvergenz in Triple-Play Applikationen,
Mittwoch, 18. März 2009, 17:30 - 19:30, Flurstrasse 50, Zürich,
Info und Anmeldung: www.fael.ch ➔ Anlässe ➔ Focus 543