Stefan Krempl

Chaos und Kontrolle

19. Chaos Communication Congress in Berlin

Das Jahrestreffen des Chaos Computer Club lockte dieses Mal 3000 Besucher an die Spree – mehr als je zuvor. Schwerpunkte bildeten die Auseinandersetzung mit Kontrollplattformen wie TCPA und Palladium, Sicherheitslücken in Funknetzen und Embedded Systems sowie Überwachungsbestrebungen von Regierungen.

Hacker sind ein eigenes Volk: Nichts läuft ihnen mehr zuwider als Überwachung, sei es durch Polizei, Geheimdienste oder Computerfirmen. Die Kontrolle über den eigenen Rechner und andere technische Geräte geht ihnen über alles. Autonomie ist der gemeinsame Nenner der Szene, aus dem sich Werte wie Informationsfreiheit oder Datenschutz und eine gehörige Portion Skepsis gegenüber Zensur und Machtkonzentration ableiten. Kein Wunder daher, dass der Chaos Computer Club (CCC) das von ihm veranstaltete Jahrestreffen der europäischen Hacker ganz unter das Motto des Kampfes gegen neue Kontrollbestrebungen durch Industrie und Politik stellte. Der Leitspruch der dreitägigen Veranstaltung im Haus am Köllnischen Park lautete 'Out of Order'. Laut CCC-Sprecher Andy Müller-Maguhn spielte das Motto auf den 'kaputten' Überwachungswahnsinn, insbesondere der USA, nach den Anschlägen vom 9. September an. Als Logo diente der Grundriss des Pentagons, da das US-Verteidigungsministerium für die Hacker spätestens nach seiner Initiative 'Total Information Awareness' beim kompletten Ausspionieren der Bürger eine weitere Grenze überschritten hat.

Sorgen vor TCPA

Als eine der bedrohlichsten Instanzen zur technischen Kontrolle der Computernutzer erscheint den CCC-Anhängern die Trusted Computing Platform Alliance (TCPA). Dahinter verbergen sich etwa 170 Firmen aus der Hard- und Softwarebranche. Argwohn weckt unter zu Verschwörungstheorien neigenden Hackern bereits, dass auf der Website www.trustedcomputing.org keine Mitgliederliste einzusehen ist – denn diese ist passwortgeschützt. Bekannt ist nur, dass Größen wie HP, IBM, Intel, Infineon und Microsoft an Bord sind. Die Redmonder etwa planen im Zusammenspiel mit der TCPA eine eigene 'Sicherheits-Softwarekomponente' namens Palladium, die schon in der nächsten Windows-Version (Codename: 'Longhorn') implementiert werden soll. Gravierend erscheint den Computerfreaks, dass mit dem Kernstück der Allianz, dem 'Trusted Platform Module' (TPM) in Form eines unscheinbaren und angeblich aus Sicherheitsgründen nötigen Chips, ein 'feindlicher Agent' in die Rechner implantiert wird. Über dieses Kuckucksei können Außenstehende mit der Hardware kommunizieren, ohne dass der Nutzer es merkt, sagte Rüdiger Weis von den Amsterdamer Cryptolabs.

Die TCPA unterläuft so nach Ansicht der Hacker just das von ihr selbst im Namen geführte Vertrauen. Der Nutzer erhält den Plänen der Allianz zufolge nur noch einen 'unprivilegierten' Status auf seinem PC. Er könne also nicht mehr alles mit seinem Gerät machen, was er wolle, erklärte Weis. Auch wenn prinzipiell nichts dagegen spreche, dass ein Rechnermodul anhand von Prüfsummen eingesetzte Hard- und Software automatisch auf Sicherheit teste, stehe und falle ein solches System damit, welche Instanz hinter dem permanenten Computercheck stecke. Bisher sei alles darauf angelegt, dass dies die amerikanischen Industriegrößen und damit möglicherweise auf indirektem Weg auch US-Regierungsstellen sein könnten.

Der Verschlüsselungsexperte warnte ferner vor möglichen Sicherheitslücken in den kryptographischen Implementierungen des TPM. So sei der wichtigste Bestandteil der Lösung ein 'RSA Endorsement Key', der von einem Hersteller mit dessen 'Master Key' unterschrieben und damit als vertrauenswürdig deklariert würde. 'Die ganze Zukunft der TCPA hängt von diesen kleinen Bithaufen ab', führte Weis den Hackern in der überfüllten Aula des Congress-Zentrums vor Augen.

Sich bereits abzeichnende Angriffsflächen entstünden durch unschwer mögliche Messungen des Zeitverbrauchs der Verschlüsselungsabläufe. Auch könnte die Konstruktion so genannter 'hidden channels', die bei der Zufallszahlen-Generierung genutzt werden, die übertragenen Schlüssel kompromittieren. Weis fürchtet gar, dass bewusst Schwachstellen in das System eingebaut werden – woran bei dem augenblicklichen Überwachungswahnsinn kein Paranoiker zweifelt. Denn wäre die Verschlüsselung wirklich sicher, gäbe es auch für Strafverfolger und Geheimdienste keine Möglichkeit zum gesetzlich verbrieften Abhören. Und diese Behörden sind momentan in Europa und den USA dabei, über Standardisierungsgremien die gesamte Kommunikationstechnik mit Abhörschnittstellen auszurüsten. Die Folgen eines erfolgreichen Angriffs auf TCPA will sich Weis lieber nicht ausmalen. Kritische Applikationen bei der Feuerwehr oder beim Militär würden häufig auf Windows-Plattformen laufen. Sie wären damit von Aussetzern der vermeintlichen Sicherheitstechnik direkt betroffen.

Dass die kryptographischen Bedenken keine Hirngespinste sind, zeigte eine Entwicklergruppe auf dem Congress. Das vier-

Congress-Besucher mussten am Freitagmorgen bis zu einer Stunde Wartezeit in Kauf nehmen.

köpfige Kernteam des Xbox-Linux-Projekts (http://xbox-linux.sourceforge.net) führte vor, dass die von Microsoft entwickelte Sicherheitsarchitektur für die Spielkonsole vollständig ausgehebelt werden kann. So hüpfte bei der von den Fachleuten modifizierten Xbox der Pinguin schon beim Starten ins Auswahlmenü – zum Beweis, dass sich dem 'Hochsicherheitstrakt' unsignierter Code unterjubeln lässt. Die Maschine fuhr nach Druck auf den Knopf 'Boot Linux' klaglos eine Mandrake-Distribution komplett mit KDE-Desktop und OpenOffice hoch. Die Verwandlung in einen etwas schicker designten und von Microsoft sogar noch subventionierten PC ist damit geglückt.

Hack the box

Andy Green, der Hardware-Spezialist der Crew, erläuterte aber auch, dass der im Oktober innerhalb weniger Tage geschaffte Folgehack der von Microsoft zusätzlich abgesicherten Version 1.1 der Xbox eine Gefahr für einen Kernbestandteil der zukünftigen Softwarestrategie der Redmonder darstellen könne. Die Versiegelung der überarbeiteten Konsole entspricht laut Green der ersten 'funktionierenden' Umsetzung des Palladium-Konzepts. Während das für den Hack elementare BIOS der Box in der ursprünglichen Variante mit einem RC4-Schlüssel abgeriegelt war, hätten die Entwickler beim zweiten Modell die gesamte Bootloader-Sektion im ROM mit Hilfe einer digitalen Signaturfunktion und darauf beruhenden Prüfsummen festgenagelt. Der verwendete Tiny Encryption Algorithm (TEA) hat allerdings eine Schwäche, wie die Freaks mit Hilfe des Usenet herausfanden: Er wirft in jedem 66-Bit-Block dasselbe Check-Resultat aus, wenn Bit 31 und 63 zusammen verändert werden. So gelang es den Experten, über einen Programmiertrick mit einem JUMP-Befehl der Box wieder das im RAM abgelegte Linux-Startprogramm anzudienen. 'Wir hatten den Multimillionen-Dollar-Aufwand Microsofts damit durch den Austausch von zwei Bits zunichte gemacht', berichtete Green stolz. Zukünftigen Palladium-Anwendungen gesteht der Experte nach diesen Erfahrungen nur geringe Haltbarkeit zu: 'Wir müssen nur einmal Glück haben, Microsoft die ganze Zeit'.

Angesichts der allgemein zur Schau gestellten Ablehnung von Palladium und TCPA, die durch Sorgen um die Zukunft des freien Informationsaustauschs verstärkt wurde, hatte der einzige die Chip-Plattform verteidigende Industrievertreter einen schweren Stand. Dirk Kuhlmann, Forscher an den HP Labs in Bristol, warb für eine Koalition von TCPA und freier Softwarebewegung. Er verteidigte die entwickelten Ansätze mit der Begründung, dass Chips in immer mehr Alltagsgeräte eindrängen und ein Check der Bestandteile der Kommunikationsmaschinen unerlässlich sei. Keineswegs stünden Methoden zur Verbesserung des Digital Rights Managements im Vordergrund. Um das undurchsichtige Kernmodul der Allianz vertrauenswürdiger zu machen, schlug der langjährige Congress-Besucher vor, das Projekt unter der GNU General Public License (GPL), dem strategischen Mittelpunkt zahlreicher Free-Software-Projekte, zu publizieren.

Spaß mit Technik

Am Rande der Vorträge, die sich auch mit Fortschritten in der Quantenkryptographie, der Halbwertzeit kryptographischer Lösungen, einem Open-Source-Projekt zur Verschlüsselung der Kommunikation in WLANs, manipulierbaren Druckern und Routern oder den Praktiken der Manipulation von Geheimdiensten und Marketingspezialisten auseinander setzten, warteten zahlreiche 'sportliche' Aktivitäten auf die Besucher. Im spirituellen Zentrum des Congresses, dem wie immer schlecht belüfteten Hackcenter, widmeten sich die Freunde des kreativ-kritischen Umgangs mit der Technik hauptsächlich dem File-Sharing, vergnügten sich mit nicht auf Checksummen achtenden Online-Gewinnspielen und probierten neue Netz-Sniffer aus. 'Offene' Rechner fanden die Freaks auch außerhalb der Anlagen ihrer Kollegen reichlich. Diebische Freude bereitete es den selbst ernannten Servertestern vor allem, die Club-Flagge mit dem 'Pesthörnchen' auf der Webseite einer konservativen Partei zu hissen. 'Es wurde wahrgenommen, dass die hessische CDU Congress-Werbung geschaltet hat', kommentierte Müller-Maguhn den Vorgang. Aber auch die Landeskollegen der SPD blieben nicht verschont: Ihre MySQL-Datenbank erwies sich als leicht einsehbar.

Daneben boomte die praktische Arbeit mit Bohrer oder Lötkolben an Schlössern, Leuchtdioden, Lego oder Pappe. Gebastelt wurden 'Kampf-Roboter' aus bunten Bauklötzen, WLAN-Antennen aus Klorollen oder Chips-Büchsen sowie BlinkenMinis aus Leuchtdioden, Holzbrettern und Schieberegistern.

Noch bevor der Congress nach dreitägigem Dauerhacken und einem Terabyte Datenverkehr in einem moderaten Chaos aus Mate-Flaschen und einem Hauch von Coffeeshop endete, zogen die Veranstalter eine positive Bilanz. Mit dem nach Angaben des Leitungsteams 'gut 50-prozentigen Teilnehmerzuwachs' hatte in Zeiten der IT-Krise niemand gerechnet. Dass ernsthafte Diskussionen mit Vertretern aus Politik und Wirtschaft, die nicht dem Dunstkreis des CCC angehören, dieses Mal fehlten, schien nur wenige Freaks zu stören. Wer auf den 'kollektiven Spaß am Gerät' nicht bis zum Ende 2003 warten will, kann sich bereits den Easter(H)egg am Osterwochenende in Hamburg oder das zweite Chaos Communication Camp im August bei Berlin vormerken. (pab)