IT Defense 2010: Angriffe auf SSL-Verbindungen

Allzu menschlich

Jörg Riether

Dass unverschlüsselt ausgelieferte Webseiten nicht vertrauenswürdig sind, liegt auf der Hand. Wie angreifbar aber selbst SSL-/TLS-Verbindungen – nicht selten durch menschliches Fehlverhalten – sein können, zeigte der Sicherheitsexperte Moxie Marlinspike bei der diesjährigen IT Defense.

Wer den CCC-Kongress im Dezember 2009 besucht oder verfolgt hat, ist sicherlich früher oder später über Karsten Nohls Initiative zur Schwachstelle des A5/1-Verschlüsselungsalgorithmus im GSM-Standard gestolpert. Eben damit beschäftigte sich Nohl auch in seinem aktuellen Vortrag in Brühl. Er erläuterte, dass entsprechende Rainbow Tables bereits 2008 durch eine andere Initiative berechnet, aber nie veröffentlicht worden seien – was Nohl änderte, als er mit seinem A5/1-Projekt an die Öffentlichkeit ging (reflextor.com/trac/a51). Innerhalb von drei Monaten errechnete er mittels 40 CUDA-Knoten sowie freundlicher externer Hilfe komplette Rainbow Tables, die Ende des letzten Jahres via BitTorrent verfügbar waren. Damit sei A5/1 praktisch ab sofort für jedermann zu brechen.

Die GSMA versuche jedoch, die Gefahr der Entschlüsselung auf dem Luftweg und in Echtzeit herunterzuspielen, mit dem Argument, der Angriff sei sehr komplex und die benötigte Ausrüstung teuer. Das stimmt laut Nohl keineswegs. Jeder könne sich ein Radio-Empfangssystem, beispielsweise den Ettus Research USRP2 (circa 1400 US-$) und freie Software, etwa OpenBTS besorgen.

Auf diverse Verwundbarkeiten in SSL/TLS-Implementationen wies der unabhängige IT-Sicherheitsexperte Moxie Marlinspike hin. Er erläuterte außerdem Methoden, die sich diese aus Sicht des Hackers zunutze machen – etwa, indem er mit einem Trick einen „null character" in eine Subdomain einschleust. Eine Domain hieße dann zum Beispiel www.example.com[nullcharacter].thoughtcrime.org. Viele Certification Authorities (CAs) schauen nur den Common Name (CN) an, kontaktieren den (vermeintlichen) Besitzer, also thoughtcrime.org, und stellen unter Umständen ein gültiges Zertifikat aus – in diesem Fall für www.example.com\0.thoughtcrime.org.

Wenn nun ein Browser beispielsweise Mozillas Network Security Services (NSS) nutzt, um das Zertifikat zu überprüfen, konnte er bis vor Kurzem am Null-Byte hängenbleiben und erkannte www.example.com als gültige Seite an. Inzwischen haben die Browserhersteller die Schwachstelle behoben.

Mit zwei von Marlinspike entwickelten Tools lassen sich ebenfalls SSL-Verbindungen angreifen. *sslstrip* agiert als Proxy und sucht in von Servern ausgelieferten Seiten nach eingebetteten HTTPS-Links. Es ersetzt sie durch gleichlautende HTTP-Anfragen und merkt sich die Ziel-URL, zu der es seinerseits eine Verbindung aufbaut. Benutzern, die HTTP statt HTTPS aufrufen, kann der Proxy somit zurückliefern, was er beziehungsweise ein Angreifer möchte. *sslsniff* ist ein Man-in-the-Middle-Werkzeug für SSL-Verbindungen, das in der Lage ist, Zertifikate für besuchte Seiten dynamisch zu fälschen und in beliebig signierte Zertifikatsketten einzubinden.

Dilettare humanum est

Johnny Long, weltweit bekannter Social-Engineering-Experte aus Uganda, lieferte eine unterhaltsame Reise durch sein Spezialgebiet. Tenor des Vortrags war, dass die sichersten Systeme keinerlei Sicherheit brächten, wenn sie von Dilettanten bedient würden. Johnny Long demonstrierte das anhand einiger Fotos, die er vor allem auf Flughäfen aufgenommen hatte. Sie zeigten unter anderem Regierungsangestellte, die in mehr als fahrlässiger Weise den Bildschirminhalt ihres Notebooks der Allgemeinheit preisgaben.

Für den Oracle-Sicherheitsexperten Pete Finigan, der in Manchester an einem verschneiten Flughafen festsaß, sprang spontan der bekannte Kryptologie- und Reverse-Engineering-Experte Thomas Dullien ein. Er beschäftigte sich in seinem Vortrag mit aktuellen Beispielen des Reverse Engineering aus der Praxis und erklärte darüber hinaus dessen Wandel hinsichtlich der Komplexität. Was heute teilweise Monate in Anspruch nehme, hätte noch vor einigen Jahren jeder unerfahrene Hobby-Bastler in Minuten schaffen können. Grund seien die modernen Sicherheitsmechanismen, so Dullien.

Martin Roesch, seines Zeichens der Vater des bekannten IDS-Systems Snort, stellte ausgewählte Features von Snort 3.0 vor, das sich gerade in der Entwicklung befinde. Neben nativer IPv6-Unterstützung, Multiprotocol Label Switching (MPLS) und Generic Routing Encapsulation (GRE) sind neue Plug-in-Typen, etwa Analysierer und Decoder, geplant. Fans des Werkzeugs können sich auf ein Multithread Execution Model freuen, es ermöglicht die gleichzeitige Analyse desselben Traffic durch mehrere Analyse-Engines.

Die nächste IT-Defense 2011 wird vom 9. bis 11. Februar 2011 im Lufthansa Training and Conference Center in Seeheim-Jugenheim stattfinden. (ur)