Cirosec IT-Defense 2016, Mainz

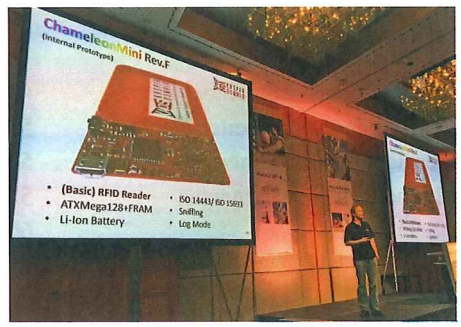
Das Internet der angreifbaren Dinge

Zum 14. Mal lud Veranstalter Cirosec zu seiner Sicherheitskonferenz IT-Defense, dieses Jahr nach Mainz, und über 200 Teilnehmer kamen. Das Vortragsspektrum reichte vom Hacken mit Steganografie bis zu Angriffen auf vernetzte Fahrzeuge und andere Bausteine im Internet der Dinge (Internet of Things, IoT).

Saumil Shah eröffnete die Veranstaltung mit seinem Vortrag über Angriffe mit per Stegosploit kompromittierten Bilddateien. „Ein guter Exploit ist einer, der mit Stil ausgebracht wird", so Shah. Stegosploit versteckt Exploit-Code in den Pixeln. Das Verfahren, so Shah, nutze Polyglotte, also das Vermischen von Mustern, die gegenseitig ihre Syntax brechen. Für ein Browser-Exploit, erläuterte Shah, bringe Stegosploit Steganografie-Tools, Polyglott-Tools und Exploits mit. Der binäre Code des Exploits werde dazu in einem niedrigen Bit-Layer der Acht-Bit-Grauskala bestimmter Pixel (jedes dritte, jedes vierte …) versteckt. Er demonstrierte das Verfahren: Bei Code-Einbringung in Bit-Layer 7 wäre die Manipulation noch sichtbar, auf Bit-Layer 2 aber ist sie für das menschliche Auge nicht mehr erkenntlich.

Ein Problem, so Shah, stellen JPGs dar, da diese beim Speichern per Kompromierung verändert werden. Durch einen mehrfach iterativen Ansatz konnte Shah diese Hürde aber überwinden: Nach zirka neun Iterationen erhalte man trotz der JPG-Komprimierung verlustfreien Code. Jeder Browser, der HTML5 unterstützt, sei heute dank der Canvas-Integration in HTML 5 in der Lage, ein derart manipuliertes Bild zu decodieren. Bildbasierte Angriffe, so Shah, seien derzeit dabei, „in freier Wildbahn" Verbreitung zu finden. Als schnellen Workaround zur Abwehr könne man Bilder neu codieren. Das grundlegende Problem seien die Parser in den gängigen Web-Browsern: Nötig wären wirklich strenge Parsing-Regeln für diese.

Allianz-CISO Stephan Gerhager diskutierte Angriffe auf vernetze Fahrzeuge. Er zeichnete ein recht bedrohliches Bild – selbst für deutsche Hersteller. Ein heutiger PKW beinhaltet laut Gerhager über 100 ECUs (Electronic Control Units), in neuesten Fahrzeugen finde man noch deutlich mehr. Funktionen wie Parkassistenten



White-Hat-Hacker Timo Kasper erläuterte auf der IT-Defense in Mainz Angriffe auf elektronische Schließsysteme. Bild: Dr. Wilhelm Greiner

erforderten dabei die Echtzeitkommunikation zwischen ECUs über Bus-Systeme wie CANbus. Der Wunsch nach Remote-Funktionalität wie etwa das Betätigen der Hupe per App zum leichteren Finden des Fahrzeugs setzten zudem eine Anbindung ans Internet voraus. Die Folge, wie 2015 der Jeep-Cherokee-Hack von Charlie Miller und Chris Valasek (LANline berichtete: lanl.in/1N2gqC2) erkennen ließ: Die komplette Übernahme eines modernen Autos durch einen Angreifer ist nicht nur per Diagnose-Port, sondern auch via Internet möglich. Gerhager zeigte dazu ein kurzes Video, in dem Dan Kaufman von der US-Behörde DARPA (Defense Advanced Research Projects Agency) einen solchen Angriff demonstrierte (www.youtube.com/watch?v=7E1WsdODxu0).

Das Problem laut Gerhager: Die Mitarbeiter eines Automobilkonzerns, die von IT-Sicherheit Ahnung haben, sitzen in der IT des Herstellers, nicht in deren Entwicklungsabteilung. „Jetzt machen die [die Entwickler, d. Red.] dieselben Fehler, die wir in der IT vor zehn, 15 Jahren gemacht haben", warnt der Allianz-CISO.

Jede Fahrzeugserie hat laut Gerhager heutzutage seine eigene IT-Architektur, die es zuerst per Sniffing zu ermitteln gelte. Dies sei dank aktueller Linux-Tools wie CANtact kein Problem mehr. Nach einem Tag Arbeit habe ein (allerdings in Autotechnik sehr versierter) Praktikant in Gerhagers Haus einen erfolgreichen Angriff von innerhalb eines (nicht genannten) Fahrzeugs durchführen können.

Nach internen Angriffen die nächste Stufe: ein Angriff an der Außenhaut des Fahrzeugs. Ein Angreifer könne sich zum Beispiel bei einem Remote Key per Man-in-the-Middle-Angriff zwischenschalten und so das Verschließen des Fahrzeugs verhindern. Der anspruchsvollste Angriff – wie jener von Miller und Valasek – ist ein Remote-Zugriff auf die Steuerungselektronik des Automobils. Per Reverse Engineering können Angreifer dann die Fahrzeugsoftware manipulieren. Für den Fernzugriff benötigt man laut Gerhager ein fest vorgegebenes Challenge (Seed). Dies könnte zum Beispiel der Herstellungszeitpunkt sein – der allerdings mitunter, je nach Hersteller, der Fahrgestellnummer zu entnehmen sei. In der Firmware der Fahrzeuge finde man zudem zahlreiche Angaben, die Angreifern wichtige Hinweise für ihr weiteres Vorgehen geben können, warnt der Allianz-Mann.

Laut Gerhager waren die zwölf Angriffe von Miller und Valasek bei deutschen Herstellern dank Maßnahmen wie Netzwerk-

segmentierung überwiegend erfolglos. Dennoch lautete Gerhagers Fazit: Die Autohersteller – auch die deutschen – hätten wichtige Entwicklungen der IT-Sicherheit „verschlafen“, ihre Lernkurve beim Thema IoT-Sicherheit gehe jetzt erst los. Die Autobauer setzten auf den unsicheren CAN-bus, und durch das Öffnen der Fahrzeuge zum Internet seien die PKWs nun kompromittierbar. Für Spezialisten, wie es sie zum Beispiel im Umfeld des Chip-Tunings gebe, stehe damit das Tor für Kompromittierungen offen. Neben Autodiebstahl seien gezielte Angriffe oder auch Erpressungen der Fahrzeughersteller denkbar.
Michael Ossman von Great Scott Gadgets wiederum präsentierte das „NSA Playset“,

Saumil Shah demonstrierte, wie man Exploits in Bilddateien versteckt. Bild: Dr. Wilhelm Greiner

also eine Sammlung selbstgefertigter Hardware, die die Spionagemöglichkeiten des „ANT-Katalogs“ der NSA aufgreift und (durch ähnlich alberne Namensgebung) parodiert. Der manipulierte USB-Stecker „Turnipschool“ zum Beispiel erweitert ein USB-Kabel um ein Funkmodul, das einem Angreifer Fernzugang verschafft.

Angriffe auf das IoT

Der zweite Tag von Cirosecs Sicherheitskonferenz IT-Defense widmete sich vorrangig dem Internet der Dinge, so auch die Keynote von Eugene Kaspersky. Angriffe, so referierte der Kaspersky-Lab-Chef, zielen heute auf Industrieanlagen, Frachthäfen oder auch Tankstellenketten. Zu den Zielen zählt er das Schädigen von physischen Systemen, digitalen Datenbeständen und Telekommunikationskanälen. Bei der Abwehr führend seien Singapur und Israel, beide Nationen hätten bereits Abwehrstrategien. Der Schutz von Scada- und Industriekontrollsysteme (ICS) erfordere Air Gaps, Traffic-Monitoring und ein gesichertes OS auf neuem Equipment. „Das ist teuer“, so Kaspersky. „Dafür müssen wir die gesamte Scada-Software neu designen.“ Und dies werde Jahre dauern.
Deutlich stärker ins Detail ging der Vortrag von John Matherly, der die IoT-Suchmaschine Shodan betreibt. Die ICS-Branche krisierte Matherly heftig: Viel zu lange habe sie sich auf ihre Existenz in einer Nische („Security by Obscurity“) verlassen. Er zitierte eine Passage aus einer PLC-Dokumentation (Programmable Logic Controller): Da der PLC kein Windows-OS verwende, sei er „mit Standard-Hacking-Methoden nicht angreifbar“. Doch mit der Obskurität sei es nun vorbei. So seien zum Beispiel auf Github die Fragen bezüglich MODbus dramatisch gestiegen. Das Problem, so Matherly: Wenn man MODbus direkt über das Internet erreiche, könne man nach Belieben lesen und schreiben. Denn MODbus kenne weder Benutzernamen noch Passwörter. Zwar gebe es Verschlüsselung, aber ohne Authentifizierung helfe dies wenig.
Mit dem Internet verbundene Dinge, berichtete Matherly, hätten sich letztes Jahr in den USA enorm verbreitet: So gebe es per Internet kontrollierbare Eierbehälter, Kühlschränke mit Internet-Anschluss für das Twitter-Display an der Tür sowie Toiletten mit Online-Bewertungssystem. Samsung habe gemeldet, dass IoT Hubs künftig Teil der hauseigenen Smart-TV-Geräte sein werden. „Man wird künftig keine Wahl mehr haben“, warnt der Shodan-Betreiber. Über ein Drittel der IoT-Anbieter (34 Prozent) haben laut seinen Angaben bei ihren IoT-Produkten grundlegende Sicherheitslücken, auch wenn diese oft einfach zu beheben wären. Ein großes Problem, so Matherly: Einen gefährdeten PC könne man patchen, aber wie patcht man einen Kühlschrank, wenn er anfängt, als Spam-Bot zu agieren?
Der stets unterhaltsame Hacker Timo Kasper von Kaos Kasper & Oswald widmete sich in seinem Vortrag „Tag der offenen Tür(en)“ der Sicherheit elektronischer Schließsysteme. Moderne Transponder, so Kasper, verwendeten ein bidirektionales Challenge/Response-Verfahren mit gegenseitiger Authentifizierung zwischen Schlüssel und Schloss. Ähnlich arbeiteten kontaktlose Smartcards wie neuere Kreditkarten, Nahverkehrsausweise oder auch moderne Skipässe. Zur Kompromittierung hat er den Smartcard-Emulator Chameleon entwickelt. Mit dem Chameleonmini – in der aktuellen Revision F, einem derzeit

„Bei Advanced Malware hat die Sandbox-Analyse versagt, das ist inzwischen Konsens. Man muss zur Abwehr aufs Endgerät – Stichwort Mikrovirtualisierung“, so Stefan Strobel, Geschäftsführer von Cirosec und Veranstalter der IT-Defense. Bild: Dr. Wilhelm Greiner

laufenden Kickstarter-Projekt – könne man in Sekundenschnelle derlei Kartensysteme clonen. Live demonstrierte er das Kopieren einer Moskauer Metro-Karte. Elektronische Türöffner (Transponder) mit bidirektionaler Authentifizierung eines deutschen Anbieters knackte er durch den Ausbau des Microcontrollers. Dank einer Schwäche im proprietären Zufallsgenerator zur Schlüsselerzeugung konnte er, wie er berichtete, die Schlüssel mittels fünf Türöffnungsversuchen innerhalb von Sekunden ableiten. Man habe dem Hersteller die Schwäche gemeldet, sie sei nun behoben.
Der Gesamteindruck aber bleibt: Das Internet der Dinge bietet Angreifern eine Fülle neuer Einfallstore – keine überraschende Erkenntnis, aber eine beunruhigende Lage.

Dr. Wilhelm Greiner

Auf LANline.de: **wgreiner**