secorvo
security consulting

Secorvo Security News

Oktober 2017

Die Schildkröte

Eine meiner Lieblingsparadoxien ist die von Achilles und der Schildkröte. Überliefert von Aristoteles und zugeschrieben Zenon von Elea lautet sie etwa wie folgt:

Achilles, Sohn des Peleus und der Nymphe Thetis, Held der Griechen beim Kampf gegen Troja und schneller Läufer, tritt im Wettlauf gegen eine Schildkröte an. Um das Rennen fairer zu gestalten, räumt er ihr einen Vorsprung ein – und verliert.

Denn während er die Strecke des der Schildkröte gewährten Vorsprungs durchläuft, ist diese bereits weiter gekrabbelt – und hat sich einen neuen, wenn auch kleineren Vorsprung erarbeitet. Holt er diesen auf, hat die Schildkröte wiederum etwas Strecke gut gemacht, und passiert er auch die, ist sie wieder ein Stück weiter – Achilles wird sie daher, so schnell er auch laufen und so unendlich nah er ihr auch kommen mag, niemals überholen.

Mathematiker werden jetzt einwenden, dass unendliche Reihen auch endliche Summen haben können. Aber das rettet uns nicht aus der Denkfalle – denn als Sicherheitsexperte erkennen wir uns in Achilles wieder: Fühlen wir uns nicht oft wie er, wenn wir durch präventive Maßnahmen, Patches oder Policies Angriffsfläche reduzieren – dabei aber feststellen müssen, dass wir Angreifern nachjagen, die sich derweil wieder mit neuen Angriffsmethoden oder unter Ausnutzung neu entdeckter Sicherheitslücken erneut einen kleinen Vorsprung erarbeitet haben.

Dabei widerspricht Zenons Paradoxon unserer Erfahrung. Und tatsächlich ist es die Perspektive, die uns täuscht: Wenn wir uns selbst als hinter Angreifern her hechelnden Achilles sehen, der ständig die von jenen aufgerissenen Löcher stopft, werden wir die Aufholjagd nicht gewinnen können.

Deshalb sollten wir die Perspektive wechseln und uns klarmachen: Für Resignation gibt es keinen Grund. Denn wenn wir schneller sind als die Schildkröte werden wir sie auch überholen.

Inhalt

secorvo
security consulting

Security News

Deterministischer Zufall

Am 18.10.2017 wurde eine Schwachstelle in Infineons Firmware-Bibliothek für Smartcard- und TPM-Chips veröffentlicht – gleich mit GitHub-Archiv. Sie steckt in einem Beschleunigungsalgorithmus für die RSA-Schlüsselerstellung: Er testet nicht einfach Zufallszahlen, bis zwei Primzahlen gefunden sind, sondern konstruiert stattdessen zufallsabhängig Kandidaten, die nicht durch kleine Primzahlen teilbar und somit wahrscheinlicher prim sind.

Hier zeigt sich wieder die Schwierigkeit, Sicherheit als Qualitätsmerkmal nachzuweisen: Die inkriminierte Firmware-Bibliothek wurde u. a. vom BSI nach Common Criteria zertifiziert. Jahre später griffen nun tschechische Forscher auf eine Angriffsmethode zurück, die bei heutiger Schlüssellänge eigentlich nicht mehr relevant ist. Von Infineon-Chips konstruierte 2048 bit lange RSA-Schlüssel aber kann man damit in der Amazon-Cloud für ca. $ 40.000 binnen Tagen brechen. Ob der eigene RSA-Schlüssel betroffen ist, lässt sich übrigens mit Hilfe verschiedener Testtools prüfen.

Als etwas hilflose Panik-Reaktion muss man wohl die Beschränkung des Zugriffs auf die öffentlichen RSA-Schlüssel 750.000 estnischer Ausweiskarten bewerten: das Nicht-Veröffentlichen öffentlicher Schlüssel ist nicht nur eine Contradictio in Adiecto, sondern zudem wirkungslos, denn schon zwei digitale Signaturen können ausreichen, um daraus den öffentlichen Schlüssel zu ermitteln – zumindest wenn dafür wie üblich das traditionelle RSA-Padding-Verfahren (PKCS#1 v1.5) anstelle des seit gut 15 Jahren empfohlenen PSS-Verfahrens verwendet wird.

WLAN-Ü-Ei

In postfaktischen Zeiten benötigt eine Schwachstelle einen griffigen Namen, ein Logo und eine eigene Webseite. Daneben vereint die am 16.10.2017 veröffentlichte KRACK-Attacke drei Dinge auf einmal: Angriff, Ansatzpunkt und Theorie.

Zunächst deckt sie einen in Linux und Android weit verbreiteten Bug auf, der es Angreifern ermöglicht, Nutzer betroffener Geräte unbemerkt und ohne Social Engineering in ein Evil-Twin-Netz umzuleiten. Dahinter steckt eine im WLAN-Standard begründete Schwäche, über die die unterste Ebene der Schlüsselableitung angegriffen werden kann: der pseudozufällige Schlüsselstrom einzelner Datenpakete. In Kombination mit geratenen oder bekannten Inhalten lassen sich so einzelne Pakete in einem per AES-CCMP gesicherten WPA2-Netz entschlüsseln oder wiedereinspielen. Dies ist meist noch nicht schwerwiegend, jedoch ein potenter Ansatzpunkt für weitere Angriffsschritte. Und schließlich erhellt KRACK unser Verständnis vom Wert theoretischer Sicherheitsbeweise: Der Angriff auf das Kryptoprotokoll widerlegt nicht die formalen Beweise, sondern bewegt sich haarscharf außerhalb deren Gültigkeitsbereichs.

Eilige Warnungen, deswegen auf Online-Banking per WLAN zu verzichten, sind jedoch unangemessen: Dass anstelle von leicht aus der Ferne zu dirigierender Man-in-the-Browser-Malware jetzt Flotten von Kleintransportern mit WLAN-Man-in-the-Middle-Ausrüstung in deutsche Wohnviertel ausschwärmen, ist wohl eher unwahrscheinlich. Handlungsbedarf ergibt sich dagegen aus dem Schlaglicht, das KRACK auf das zu erwartende Schwachstellenmanagement im Internet-of-Things wirft: Man beachte, welche Hersteller und Geräte *nicht* in den Listen verfügbarer Patches auftauchen.

Versteckte Minenarbeiter

Seit Mitte September erfreuen sich JavaScript-Miner immer größerer Beliebtheit. Ursprünglicher Zweck solcher Bitcoin-Miner war es, Webseitenbetreibern eine – im Vergleich zu Werbung – beständigere und effizientere Möglichkeit der Finanzierung zur Verfügung zu stellen. Dabei sollte der Nutzer den eingebetteten Miner selbst starten und während des Webseitenbesuchs laufen lassen. Seiten wie „The Pirate Bay“ erweiterten dieses Konzept jedoch und lieferten einen Miner aus, der sofort mit seiner Arbeit beginnt – auch ohne Einverständnis des Nutzers und meist sogar ohne dessen Wissen. Nun haben die Entwickler des JavaScript-Miner reagiert und erzwingen ein Opt-In.

Wer sicher gehen will, dass sein Endgerät nicht für Fremde Bitcoins schürft, sollte JavaScript im Browser blockieren – z. B. mittels Erweiterungen wie NoScript. Alternativ kann man einzelne Seiten auch über den Dienst „Who runs Coinhive?“ prüfen.

Nutzungsanalyse

Das am 13.10.2017 von Harlan Carvey veröffentlichte PlugIn recentapps für das forensische RegRipper Toolset erlaubt die Gewinnung zusätzlicher Informationen über Benutzeraktivitäten unter Windows 10 (und ergänzt damit den UserAssist-Registry-Key). Dazu zählen zum Beispiel die ‚Last-Write Time‘ des Application GUID Subkeys, die unabhängig von der ‚LastAccess Time‘ im NTFS-Dateisystem gespeichert wird. Diese Zeitinformation stellt eine wertvolle Möglichkeit zur Validierung von Programmaufrufen eines Benutzers dar, sogar wenn die Zeitangaben im Dateisystem selbst und in der Master-Dateitabelle manuell verändert wurde.

Praktischerweise liefert das Plugin seine Ergebnisse im Timeliner-Format *.TLN, womit es die forensische Timeline eines Benutzerkontos ergänzt und z. B. Informationen darüber liefert, welche Programme eine Schadsoftware in diesem Benutzerkontext aufgerufen hat.

Zielgruppenansprache à la Facebook

Das Bayerische Landesamt für Datenschutzaufsicht führt in einem Bericht vom 04.10.2017 aus, ob und unter welchen Voraussetzungen der Facebook-Dienst „Custom Audience" den Datenschutzanforderungen des BDSG und der DS-GVO entspricht.

Gemeinsam ist den nach Anwendungsfällen unterschiedenen Varianten des Werbedienstes die zielgenaue Ansprache von Facebook-Nutzern. Dazu erhält Facebook von seinem Auftraggeber entweder eine Adressatenliste oder es wird ein Facebook-Pixel auf der Auftraggeber-Website eingebunden.

Beim Pixel-Verfahren seien die Auftraggeber verpflichtet, Betroffene über die Datenerhebung zu informieren und ein Opt-Out-Verfahren anzubieten. Die Verantwortung für den rechtmäßigen Einsatz der „Facebook Custom Audience" obliege dabei dem jeweiligen Unternehmen. Die Übermittlung der Listendaten erfordere eine gesonderte Rechtsgrundlage, in der Regel die Einwilligung der betroffenen Personen.

Sowohl das Einwilligungserfordernis als auch die Informationspflicht über die Verarbeitung durch Facebook machen eine rechtskonforme Umsetzung faktisch unmöglich. Mit Blick auf die empfindlichen Ordnungsgelder der DS-GVO sollte daher von einer Nutzung der Dienste Abstand genommen werden.

Kopieren oder nicht kopieren...

Mit einer Änderung von § 20 Personalausweisgesetz (PAuswG) vom 07.07.2017 wurde das Kopieren von Personalausweisen unter bestimmten Voraussetzungen ermöglicht. So muss die Kopie als solche dauerhaft erkennbar sein (z. B. schwarz-weiß) und die Einwilligung des Inhabers vorliegen. Dient die Ablichtung zur weiteren Verwendung der Personalausweisdaten, so bedarf dies einer gesonderten Einwilligung; selbstverständlich sind zudem alle einschlägigen Datenschutzvorschriften einzuhalten.

Bislang war die vielfach auch in Privatunternehmen bestehende Praxis, zur Dokumentation des Identitätsnachweises den Ausweis zu scannen oder zu kopieren, durch § 14 PAuswG untersagt. Das Verbot hat sich in der Praxis nie wirklich durchgesetzt, die der neue § 20 nun legitimiert. Ein wenig wirkt dieser Interessensausgleich daher wie eine Kapitulation.

Secorvo News

Verstärkung

Im Sommer ist es uns gelungen, unser Beratungsteam zu erweitern: Seit dem 01.10.2017 verstärkt Sarah Niederer den Bereich Datenschutz. Sie bringt vieljährige Berufserfahrung aus den Bereichen Compliance, Business-Impact-Analysen, Risikomanagement und insbesondere vertieftes Datenschutz-Know-How mit.

Secorvo-Seminare

Für Schnellentscheider bieten wir in diesem Jahr noch drei Seminare an: PKI (06.-09.11.2017), IT-Sicherheit heute (21.-23.11.2017) und das T.I.S.P.-Seminar (27.11.-01.12.2017) mit anschließender Zertifizierung.

Programme, die Möglichkeit zur Anmeldung und die Seminartermine 2018 finden Sie unter www.secorvo.de/seminare.

Sicherheit auf Wolke sieben

Die Verarbeitung von Daten in der ‚Cloud' stößt immer wieder (und oft berechtigt) auf Sicherheitsbedenken. Dabei ginge es auch anders: Mit ‚Privacy & Security by Design' lassen sich Cloud-Lösungen mit hohem Sicherheits- und Datenschutzniveau realisieren. Wie das geht, zeigen wir bei unserem kommenden KA-IT-Si-Event am **23.11.2017** an Beispielen aus anwendungsnahen Forschungs- und Entwicklungsprojekten. Gastgeber ist das Karlsruher „House of Living Labs" des Forschungszentrums Informatik (FZI). Für Interessierte bieten wir vorab eine Führung durch dieses Innovationslabor an.

Im Anschluss haben Sie wie gewohnt Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (zur Anmeldung).

Krypto im Advent – 24 Tage, 24 Rätsel

Verschlüsseln und entschlüsseln, grübeln und Spaß haben, lösen und gewinnen: Das ist Krypto im Advent. Mehr als 2.400 begeisterte Rätselknacker begaben sich im vergangenen Advent täglich in die Welt der Kryptologie. Am 01.12.2017 geht es nun wieder los. An diesem Adventsrätsel, das in Zusammenarbeit mit der Pädagogischen Hochschule Karlsruhe entwickelt wurde, können alle Schülerinnen und Schüler der **Klassen 3 bis 9** teilnehmen. Dank unseren Sponsoren gibt es wieder zahlreiche Preise zu gewinnen. Auch ältere, an Ver- und Entschlüsselungsverfahren Interessierte sind herzlich eingeladen mitzumachen – allerdings außer Konkurrenz.

Veranstaltungshinweise

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

Oktober 2017	
30.10.-03.11.	ACM CCS 2017 (ACM/SIGSAC, Dallas/US)
November 2017	
06.-09.11.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
14.-15.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
14.-15.11.	ISSE 2017 (EEMA, Brüssel/BEL)
14.-17.11.	DeepSec In-Depth Security Conference Europe (DeepSec GmbH, Wien/AT)
15.-17.11.	41. DAFTA (GDD Gesellschaft für Datenschutz und Datensicherheit, Köln)
21.-23.11.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
27.-28.11.	7. Handelsblatt Jahrestagung - Cybersecurity (Handelsblatt/EUROFORUM, Berlin)
27.11.-01.12.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
Dezember 2017	
04.-07.12.	Black Hat Europe 2017 (Blackhat, London/UK)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Fabian Ebner, Hans-Joachim Knobloch, Michael Knopp, Sarah Niederer, 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