secorvo
security consulting

Secorvo Security News

Januar 2019

Protokoll

Ein Protokoll ist die Niederschrift einer Ereignisabfolge – oder die Beschreibung eines festgelegten Ablaufs. In der Kommunikationstechnik spielen Protokolle eine zentrale Rolle: Als standardisierte Ablaufbeschreibungen für den Austausch von Daten zwischen Endsystemen.

Eine der größten Herausforderungen der Kryptografie ist die Entwicklung „sicherer" Protokolle – Ablaufbeschreibungen für einen Datenaustausch, der bestimmte Sicherheitseigenschaften (authentisch, vertraulich, verbindlich etc.) besitzt und resistent gegen Angriffe ist. Dabei genügt es nicht, lediglich einzelne kryptografische Mechanismen zu kombinieren: Ohne eine enge Verzahnung der Mechanismen haben Angreifer leichtes Spiel. Ein Beispiel: So reicht eine (gar einseitige) Authentifikation der Endsysteme zu Beginn des Protokolls nicht aus, denn ein Angreifer kann sich später als „Man-in-the-Middle" in die Verbindung einklinken. Die Authentifikation muss gegenseitig erfolgen und mit weiteren Mechanismen über alle Datenpakete aufrechterhalten werden. Wie komplex und fehleranfällig das im Konkreten sein kann, haben viele erfolgreiche Angriffe auf kryptografische Protokolle gezeigt. Dafür verstehen Protokoll-Designer inzwischen einigermaßen, worauf es ankommt.

Ähnliches gilt für Abläufe im echten Leben. Zahlreiche Angriffe wie die Skimming-Attacken an Geldautomaten oder die automatische Überwindung von Captchas, die Angreifer auf Erotik-Seiten weiterleiten, um sie dort von Menschen lösen zu lassen, sind nichts anderes als „analoge" Man-in-the-Middle-Angriffe. Auch das 2018 erstmals aufgetretene „Job Scamming" gehört in diese Kategorie: Mit falschen Stellenangeboten werden Bewerber zur Versendung fotografierter Ausweispapiere oder zu einem Video-Ident-Verfahren verleitet – und diese vom Angreifer für die Eröffnung eines (Geldwäsche-) Kontos verwendet.

Dabei könnte man inzwischen von den Protokoll-Designern lernen.

Inhalt

secorvo
security consulting

Security News

Schwarzer Tag für die Biometrie

Alle Jahre wieder beschert der Chaos Communication Congress zwischen Weihnachten und Neujahr einige interessante Angriffe. So kippten Julian und Starbug am 28.12.2018 auf dem 35c3 mit ihrem Vortrag „Venenerkennung hacken“ (Video) einen der letzten Hoffnungsträger biometrischer Systeme: die Venenerkennung.

Handvenen sind ein in Hochsicherheitsumgebungen (wie beispielsweise der Zentrale des BND in Berlin) beliebtes biometrisches Authentifikationsmerkmal, da ihre Analyse bisher als eines der sichersten Verfahren galt. Da die Systeme berührungslos arbeiten sind sie zudem für öffentliche Anwendungen wie Geldautomaten oder Hygienebereiche wie Krankenhäuser besonders gut geeignet. Die Sicherheitsforscher konnten jedoch zeigen, dass ein Foto einer Hand, aufgenommen mit einer Kamera ohne Infrarotfilter aus mehreren Metern Entfernung, und etwas Nachbearbeitung genügen, um mittels eines Laserdruckers und einfachem Bienenwachs eine Attrappe zu erstellen, die von Handvenenscannern akzeptiert wird. Getäuscht wurden auf diese Weise sowohl die Handflächen- als auch die Fingervenenerkennung. Trotz der (vom Hersteller behaupteten) Lebenderkennung der Zutrittskontrolllösung wurde die Attrappe nicht zurückgewiesen.

Die Forscher skizzierten weitere Angriffsszenarien wie einen in einem berührungslosen Handtrockner eingebauten Raspberry Pi mit Kameramodul, der ausreichend gute Bilder für einen erfolgreichen Angriff liefert. Damit werden sichere Biometrieverfahren langsam knapp.

PKI in Entwicklungsumgebungen

Wer PKI-Anwendungen nicht nur nutzt sondern auch selbst entwickelt oder in einer Testumgebung betreibt, steht gleich vor einem doppelten Dilemma: Einerseits sind Test- und Entwicklungssysteme oft nicht sicher genug – sie werden nicht auf dem gleichen Sicherheitsniveau betrieben wie Produktivsysteme. Schlüssel zu Zertifikaten sind dort weniger geschützt, Sperrprozesse oft nicht sorgfältig umgesetzt, und daher kann das Vertrauensniveau einer produktiven PKI leiden.

Andererseits sind produktive PKIs oft zu sicher – Zertifikate für Test und Entwicklung werden „auf Zuruf“ benötigt; sorgfältige manuelle Validierungsschritte bremsen die Entwicklungsarbeit aus. Hinzu kommt, dass fehlerträchtige Ereignisse wie die Sperrung oder der Ablauf eines Zertifikats in einem verglichen mit dem späteren Produktivbetrieb kurzen Entwicklungszeitplan meist nicht auftreten – Test-Zertifikate sollten daher eine deutlich kürzere Gültigkeit haben als in einer Produktivumgebung.

Eine schlechte Lösung für dieses Dilemma ist, bei Test- und Entwicklung mit selbstsignierten Zertifikaten und den üblichen, „wegzuklickenden“ Meldungen zu arbeiten. Eine aufwändige ist es, eine separate zweite PKI zu betreiben, deren Root-CA nur in der Entwicklung und für Tests vertraut wird.

Einen Mittelweg geht das von einem Google-Entwickler am 07.01.2019 veröffentlichte Paket mkcert. Es bietet einen einfachen Zugang zu einer ad-hoc erstellten OpenSSL-CA und platziert deren Zertifikat in alle gängigen lokalen Root-Stores. Eine künftige Version soll auch eine Zertifikatsbeantragung per ACMEv2 unterstützen. Für viele Test- und Entwicklungsumgebungen könnte dies die gesuchte Lösung sein.

Drum prüfe, wer sich ewig bindet

Aller europäischen Vereinheitlichung zum Trotz gibt es – nach wie vor – auch außerhalb der DSGVO und des neuen BDSG Datenschutzbestimmungen. Am 18.12.2018 hat das Bundessozialgericht (BSG) auf Grundlage des § 284 SGB V eine datenschutzrechtliche Entscheidung zu elektronischen Gesundheitskarten getroffen.

Die Versicherten (ausgenommen Kinder und Personen, die dazu außerstande sind) müssen den Krankenkassen Passbilder zur Ausstellung der elektronischen Gesundheitskarte zur Verfügung stellen. Wie dies zu geschehen hat ist gesetzlich nicht geregelt. Nach dem Urteil des BSG steht nun fest, dass die Krankenkassen die Bilder nach der Ausstellung der Karte unverzüglich zu löschen haben.

Dies entspricht dem Grundsatz der Zweckbindung und der Datensparsamkeit. Es ist zu begrüßen, dass die Bilder nicht dauerhaft, etwa zur Ausstellung von Ersatzkarten o. ä. gespeichert werden dürfen, auch wenn ganz offensichtlich ist, dass dies sowohl für die Kassen als auch für die Versicherten einen Mehraufwand bedeutet, wenn eine Karte abgelaufen, verloren gegangen oder auf andere Weise abhandengekommen ist.

Anderes gilt bei Ausweispapieren wie dem Reisepass, Personalausweis oder der Fahrerlaubnis. Hier liegen der Speicherung andere gesetzliche Ermächtigungen (PassG, PAuswG, StVG) zugrunde, die es den Behörden erlauben, die Bilder auch nach Erstellung der Ausweisdokumente weiter zu speichern.

Dabei dürfen die Daten im Fahrerlaubnisregister nach § 61 Absatz 4 StVG nur bis zur Vollendung des 110. Lebensjahres gespeichert werden dürfen. Was auch immer mit dieser Begrenzung bezweckt wurde – sie könnte sich eines Tages noch rächen...

secorvo
security consulting

Patchen ist gut...

...zum Schutz vor (bekannten) Sicherheitsschwachstellen. Das haben wir alle seit Jahren immer wieder gehört (und weitergesagt). Aber Patchen aus einer verlässlichen, integren Quelle ist besser. Das mussten all jene schmerzlich lernen, die im Zeitraum zwischen (vermutlich) Juli 2018 und Januar 2019 Software vom „PHP Extension and Application Repository“ (PEAR) auf ihrem Webserver installiert haben. Denn wie die Betreiber des Repositories am 19.01.2019 mitteilten, war mindestens eines der Installationspakete in diesem Zeitraum mit Schadsoftware bestückt.

Während immer mehr kommerzielle Softwarehersteller ein ISO 27001-Zertifikat für ihr Security Management vorweisen, scheinen manche Open-Source-Softwarequellen zwar mit viel Enthusiasmus zu arbeiten, aber dem sicheren Betrieb noch immer wenig Aufmerksamkeit zu widmen.

Angesichts geradezu inflationärer Security-Labels und -Zertifizierungen wäre ein Label für professionell sicher betriebene und regelmäßig auditierte Open Source Repositories ein deutlicher Fortschritt. So wie einige große OpenSSL-Anwender das am 21.01.2019 veröffentlichte Security Audit der TLS-1.3-Implementierung von OpenSSL mitfinanziert haben fänden sich bestimmt Sponsoren, denen die Integrität der von ihnen genutzten Softwarepakete am Herzen liegt.

Eine für alle

Die französischen Datenschutz-Aufsichtsbehörde CNIL hat am 21.01.2019 ein 50 Millionen Euro schweres Bußgeld gegen Google verhängt. Nach dem mit der DSGVO eingeführten „One-Stop-Shop“-Prinzip soll es bei grenzüberschreitenden Verarbeitungen für betroffene Unternehmen nur einen einzigen Ansprechpartner in Europa geben, die sogenannte „federführende Aufsichtsbehörde“, falls eigentlich mehrere verschiedene Aufsichtsbehörden zuständig wären. Dann müssen Unternehmen nur mit einer Behörde kommunizieren, es gibt nur ein Bußgeld – und damit zugleich mehr Rechtssicherheit. Die federführende Behörde muss sich mit den anderen zuständigen Datenschutzbehörden abstimmen.

Vor diesem Hintergrund stellt sich die Frage, was in Deutschland passiert, wenn es zwar keinen grenzüberschreitenden, wohl aber einen Verstoß gibt, der mehrere Bundesländer betrifft. Denn dann sind bis zu 18 Datenschutzbehörden zuständig. Zwar bezieht sich die Regelung in der DSGVO auf grenzüberschreitende Verstöße, aber die EU-weit geltenden Maßstäbe müssten auch innerhalb des Bundesgebietes angewendet werden, so dass sich die Landesdatenschutzbehörden untereinander und mit der federführenden Behörde abstimmen müssten, also derjenigen, in deren Bundesland das gegen die DSGVO verstoßende Unternehmen seinen Sitz hat.

Secorvo News

Secorvo Seminare

Im März 2019 starten wir mit einem PKI- (**18.–21.03.2019**), T.I.S.P.- (**25.–29.03.2019**) und „IT-Sicherheit heute“-Seminar (**02.–04.04.2019**) in die Weiterbildungs-Saison 2019. Die vollständigen Programme und eine Möglichkeit zur Online-Anmeldung finden Sie unter www.secorvo.de/seminare. Wir freuen uns auf Ihre Teilnahme!

Teamzuwachs

Ab dem 01.02.2019 verstärkt Jannis Pinter das Secorvo-Team. Als Informatiker mit mehreren Jahren Erfahrung in der IT-Sicherheit bringt er insbesondere vertiefte technische Kenntnisse über Public Key-Infrastrukturen mit.

Gut gehört und schon gehackt.

Oder: Wie Sennheiser das TLS-Protokoll aushebelte. Leser der Security News kennen die Hintergründe (SSN 10/2018): Ein klitzekleiner „Workaround“ der Entwickler wuchs sich im vergangenen Herbst zu einem Sicherheits-Desaster für alle betroffenen Systeme aus. Eine Design-Schwachstelle im Zertifikatsmanagement der Software Sennheiser Head-Setup unterhöhlte ohne Wissen der Nutzer die Sicherheit aller TLS-Verbindungen – für die Beseitigung der Schwachstelle war die Mitwirkung von Microsoft erforderlich. Dass ein solches Desaster überhaupt möglich war, hatte allerdings mehrere Ursachen, für die nicht ausschließlich Sennheiser verantwortlich gemacht werden sollte.

Beim Jahresauftakt-Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am 21.02.2019 zeigen die Secorvo-Experten André Domnick und Hans-Joachim Knobloch, wie durch die Schwachstelle ein Man-in-the-Middle-Angriff auf TLS gelingt, stellen dar, gegen welche lang bekannten Design-Prinzipien für sichere Software verstoßen wurde und wie eine sichere Lösung hätte aussehen können.

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

Veranstaltungshinweise

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

Februar 2019	
06.-07.02.	26. DFN-Konferenz "Sicherheit in vernetzten Systemen" (DFN-CERT Services GmbH, Hamburg)
20.-21.02.	29. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
21.02.	Gut gehört und schon gehackt. (KA-IT-Si, Karlsruhe)
März 2019	
13.-14.03.	secIT 2019 (Heise Medien GmbH&Co.KG, Hannover)
14.-15.03.	Future Security 2019 (Fraunhofer VVS, Nürnberg)
18.-21.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
25.-29.03.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
29.03.	SECMGT-Workshop: IoT – ein Thema für den CISO? (GI-Fachgruppe SECMGT, Frankfurt/Main)
April 2019	
02.-04.04.	IT-Sicherheit heute – praxisnah, aktuell, kompakt (Secorvo, Karlsruhe)
09.-10.04.	Datenschutztage 2019 (FFD Forum für Datenschutz, Wiesbaden)
11.-12.04.	Security Forum 2019 (Hagenberger Kreis zur Förderung der digitalen Sicherheit, Hagenberg/AT)
24.-26.04.	DFRWS EU Conference (DFRWS, Oslo/NOR)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Hans-Joachim Knobloch, Friederike Schellhas-Mende

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