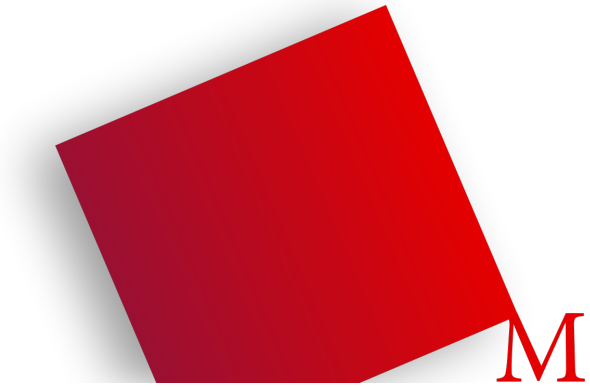
Fachbereich 07 Informatik/Mathematik



Praktikum Datenschutz und Datensicherheit
Sommersemester 2016

Prof. Dr. Rainer W. Gerling
Heidi Schuster

Man-in-the-Middle

Fabian Uhlmann
IF6

Diana Irmscher
IF7

18. Juli 2016

Zusammenfassung

Im Rahmen des Studiums Bachelor Informatik absolvieren wir (Fabian Uhlmann und Diana Irmscher) die zusätzliche Ausbildung zum betrieblichen Datenschutz an der Hochschule München.
Das Thema Datenschutz und IT-Sicherheit ist in den letzten Jahren immer mehr in den Vordergrund getreten. Medien berichten fast täglich über diverse Angriffe wie z. B. auf den Bundestag im Mai 2015 oder aktuell über den Krypto-Trojaner Locky.
Wir haben das Thema "Man-in-the-Middle" gewählt, weil es sich dabei um Angriffsszenarien handelt, die jeden (vernetzten) Nutzer jederzeit treffen können.
Das Thema ist in zwei Unterthemen aufgeteilt. Herr Uhlmann wird darauf eingehen, wie man die Sicherheit eines Systems mit einem MITM-Angriff sehr effizient aushebeln kann. Frau Irmscher beschäftigt sich mit dem gezielten Angriff in TLS/SSL und in gesnifften Netzwerken.

München, 18. Juli 2016

Inhaltsverzeichnis

Aufgabenstellung

Dell und Lenovo haben demonstriert, dass man mit Man-in-the-Middle Angriffen die Sicherheit eines Systems sehr effizient aushebeln kann. Wie funktioniert ein derartiger Angriff und was kann man tun, um sich zu schützen.

1 Bedeutung einer Man-in-the-Middle Attacke

Man in the Middle (MITM) ist ein Angriffsszenario, bei der ein unberechtigter Dritter versucht, in eine zwischen zwei Kommunikationspartnern geführte, sichere (verschlüsselte) oder auch unsichere (unverschlüsselte) Kommunikation einzudringen. Ziel des Angreifers ist es, die zu übertragenden, vertraulichen Informationen unbemerkt mitzulesen und/oder zu manipulieren. Um unerkannt im Hintergrund an die Daten beziehungsweise Informationen zu gelangen, täuscht der Angreifer vor, der jeweilige andere Kommunikationspartner zu sein. Ein MITM-Angriff kann auf den verschiedenen Ebenen des ISO/OSI Schichten-Modells [1, vgl.], z. B. auf Anwendungsebene (HTTP/HTTPs) oder Netzwerkebene (IP) stattfinden. Quelle: [2, vgl.]

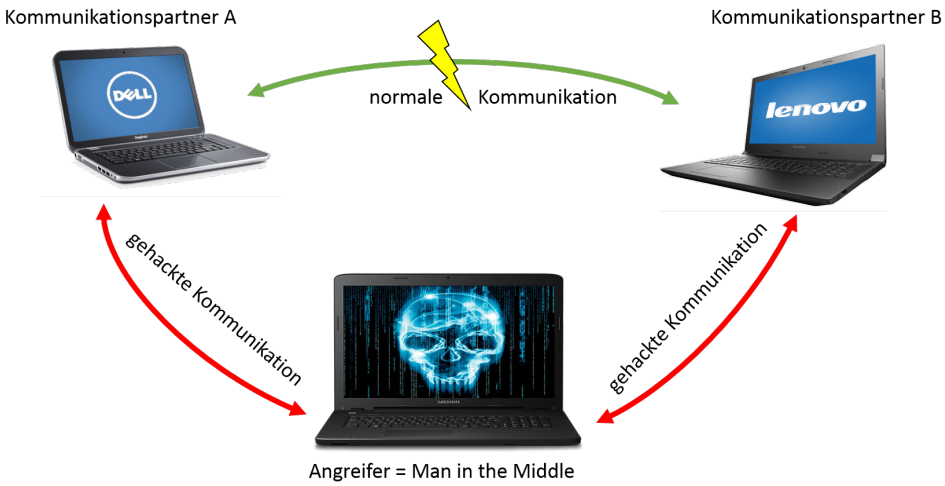


Abbildung 1: Man in the Middle Angriff [3]

2 Zusammenhang HTTP(s) und Zertifikate

Typischerweise fragt ein Nutzer eine Internetseite über das unsichere Hypertext Transfer Protocol (HTTP) an. Dabei werden alle benötigten Informationen wie zum Beispiel Benutzername und Passwort im Klartext übermittelt. Ebenfalls wird die Rückantwort unverschlüsselt übertragen. Für einen sicheren Datenaustausch sollte ein Anwender, falls dies angeboten wird, die Internetseite per Hypertext Transfer Protocol Secure (HTTPs) aufrufen. [4, vgl.] Seriöse Online-Banking-Webseiten unterstützen beispielsweise nur noch HTTPs-Aufrufe. Dabei wird dem Aufrufer durch das Kürzel HTTPs in der Adressleiste signalisiert, dass es sich hierbei um eine verschlüsselte Verbindung handelt. Genauer gesagt bedeutet es, dass eine HTTP-Kommunikation über SSL (Secure Sockets Layer) / TLS (Transport Layer Security)

verschlüsselt abläuft. Bei jeder HTTPs-Kommunikation muss sich der Webserver, auf dem die Internetseite gehostet wird, gegenüber des Webseitenaufrufers, meist ein Client, authentifizieren. Für den Client besteht hierbei kein Muss, im Normalfall wird in der Praxis auf die clientseitige Authentifizierung verzichtet. Die Authentifizierung des Webservers gegenüber des Clients erfolgt durch ein für den Webserver ausgestelltes Zertifikat[1]. [6, vgl.] Dieses enthält unter anderem den öffentlichen Schlüssel (Public Key), einen eindeutigen Fingerabdruck und Angaben über den Zertifikatsinhaber. [7, vgl.] Ein Zertifikat verbindet somit eindeutig einen Inhaber mit einem öffentlichen Schlüssel. Mit dem Public Key kann der Client verschiedene Daten, z. B. einen Pre-Shared Key, verschlüsselt zum Webserver schicken. Anhand des Fingerabdrucks, welcher auch als digitale Signatur des Zertifikats bezeichnet wird, überprüft der Client vor der Datenübermittlung, ob er mit dem richtigen Webserver kommuniziert. Der Fingerabdruck wird durch einen Hash-Algorithmus wie z. B. SHA-2 erzeugt. Bei der Erzeugung gehen diverse Informationen wie z. B. Zertifikatsaussteller, öffentlicher Schlüssel und Identifizierungsdaten über den Webserver mit ein. Wenn das Zertifikat von einer Zertifizierungsstelle (Certification Authority = CA) ausgestellt wurde, deren eigenes Zertifikat (= Root-Zertifikat oder Wurzelzertifikat) bereits im Browser installiert ist, dann wird dem ausgestellten Zertifikat automatisch vertraut. In den bekanntesten Webbrowsern wie z. B. Firefox, Chrome oder dem Internet Explorer sind bereits viele Root-Zertifikate von weltweit verschiedenen Zertifizierungsstellen vorinstalliert.

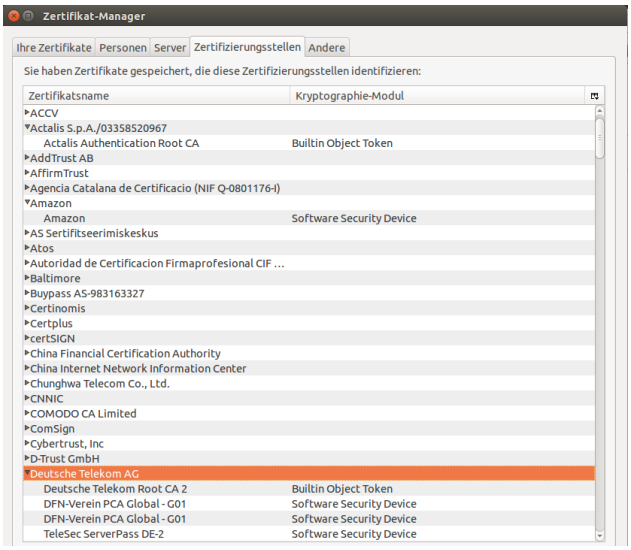


Abbildung 2: Ausschnitt vorinstallierter Zertifizierungsstellen und deren ausgestellten Zertifikate im Firefox Browser

Nutzt der Webservers ein selbst ausgestelltes (selbst signiertes) Zertifikat zur Authentifizierung, dann wird beim Verbindungsaufbau dem Nutzer eine Warnung angezeigt. Der Nutzer kann anschließend selbst entscheiden ob er dem Zertifikat vertraut oder nicht. Außerdem entscheidet er über Dauerhaftigkeit des Vertrauens, entweder nur ein einziges Mal, d. h. nur für diese Verbindungssession, oder für immer.
Ist letzteres der Fall, dann wird das Zertifikat fest im Browser installiert. Es wird dann bei den schon vorinstallierten Zertifikaten mit abgelegt. Diese dauerhafte Ausnahme hat zu Folge,

[1]Es handelt sich hierbei in der Regel um digitale Zertifikate nach dem ITU-T X.509 Standard [5, vgl.]

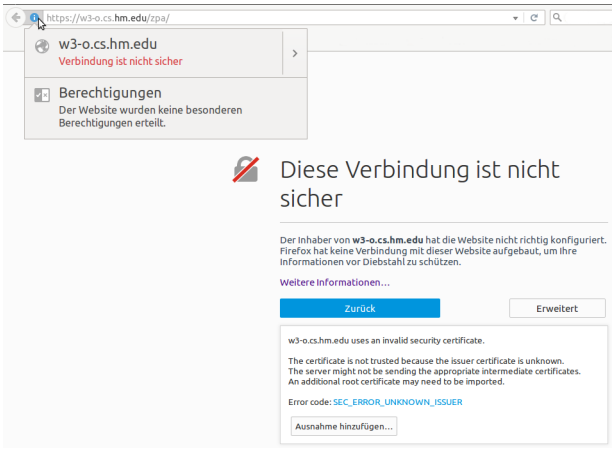


Abbildung 3: Warnung bei unbekanntem / nicht vertrauenswürdigem Zertifikat

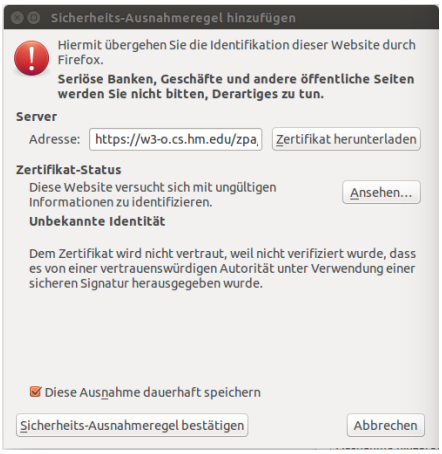


Abbildung 4: Ausnahmeregel für ein unbekanntes / bislang nicht vertrauenswürdiges Zertifikat

dass der Benutzer beim Verbindungsaufbau zu der zugehörigen Webseite vom Webbrowser nicht mehr gewarnt wird.

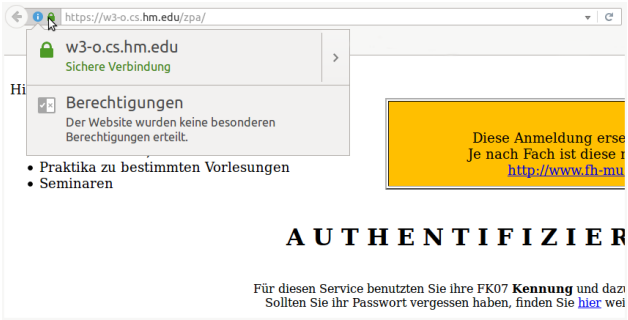


Abbildung 5: Keine Warnung nach dauerhafter Ausnahme / fester Installation des Zertifikats im Browser

3 Sicherheitslücken bei bekannten Computer Herstellern

Man sollte davon ausgehen können, dass die großen PC-Hersteller selbst am besten wissen müssten, wie hart der Markt in der Computerbranche umkämpft ist. Neben einer hohen Hardware-Qualität ist Kundenvertrauen immens wichtig. Zwei der weltweit bekanntesten und erfolgreichsten Computerhersteller [8, vgl.] haben den Faktor "Vertrauen"nicht hinreichend erfüllt. Denn sowohl Lenovo als auch DELL haben das Vertrauen ihrer Kunden stark missbraucht.

3.1 Lenovo

3.1.1 Allgemeiner Ablauf

Durch eine bereits vorinstallierte Software der Firma Superfish hat Lenovo versehentlich eine gravierende Sicherheitslücke auf einigen ihrer vertriebenen Notebookmodelle eingebaut. Dadurch wurde der Kunde einer zusätzlichen Gefahr eines erleichterten Hackerangriffes ausgesetzt. Mit der Superfish-Software beabsichtigte Lenovo, dem Nutzer gezielt personalisierte Werbung während des Surfens im Internet anzuzeigen. Um dies auch bei verschlüsselten Internetverbindungen (HTTPs) zu ermöglichen, wurde bei der Softwareinstallation auf den neuen Notebooks ein von Superfish selbst erstelltes Root-Zertifikat mit installiert. Der Kunde kaufte somit unwissentlich ein neues Notebook, auf dem ein bereits vor der Auslieferung manipuliertes Windows-Betriebssystem läuft. Mit dem selbst signierten Root-Zertifikat wurden sichere (verschlüsselte) HTTPs-Verbindungen in Form einer Man-in-the-Middle Attacke aufgebrochen. Dadurch konnte sämtlicher Datenverkehr mitgelesen und manipuliert werden. Im Fall von Lenovo geschah dies durch Einblendung von Werbung.

3.1.2 Der Angriff und die benötigten Mittel

Die Internetseite `www.golem.de` beschreibt die Idee und den Ablauf von den benutzerspezifischen Werbeeinblendungungen auf den Lenovo-Rechnern wie folgt:

> Grundsätzlich ist die Idee von Superfish, dass das Programm Bilder auf Webseiten durchsucht und anhand von Algorithmen versucht zu erkennen, was sich darauf befindet. Auf Basis dessen werden dem Nutzer passende Shopping-Angebote als Werbebanner angezeigt. Geradezu zynisch wirkt die Beschreibung des Lenovo-Angestellten im Forum: Die Funktion diene dazu, Nutzern zu helfen, visuell Angebote für Produkte zu finden, bei denen sie Schwierigkeiten haben, sie mittels einer textbasierten Suchmaschine zu finden.[9]

Für die Umsetzung der Idee reichte es nicht, dass nur ein Programm von Superfish auf den Lenovo-Rechnern installiert wird. Zusätzlich benötigte Superfish unbedingt ein eigenes signiertes Root-Zertifikat auf dem System. Ohne dieses Zertifikat wäre es nicht möglich gewesen, auch in verschlüsselten Internetverbindungen den Suchalgorithmus anzuwenden, um anschließend personalisierte Werbung einzublenden. Mit dem eigenem Root-Zertifikat war Superfish in der Lage, für jede Verbindung, die zu einer HTTPs-Webseite aufgebaut wurde, ein eigenes, gefälschtes Zertifikat dynamisch zur Laufzeit zu erzeugen. Diesem Zertifikat wurde automatisch vertraut, da bereits dem zugehörigen Wurzelzertifikat vertraut wurde. Dem Superfish Root-Zertifikat wurde wiederum vertraut, da dieses von Superfish direkt im Windows-Zertifikatsspeicher abgelegt wurde. Der Anwender bekam dadurch nicht mit, dass keine direkte verschlüsselte Kommunikation zu dem eigentlichen Server, der die Webseite hostet, aufgebaut wurde.

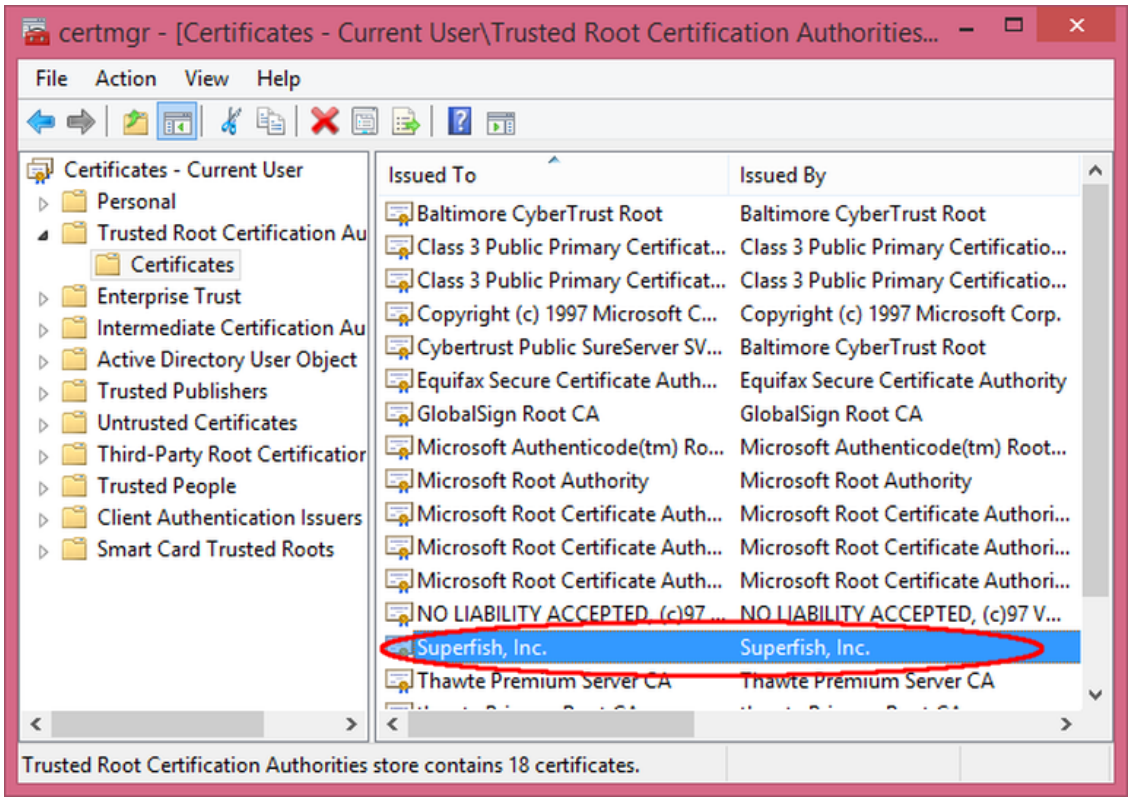


Abbildung 6: Superfish Root-Zertifikat im Windowszertifikatsspeicher, Quelle: [10]

Weiterhin kam erschwerend hinzu, dass das Programm von Superfish für die Man-in-the-Middle Attacken ein schwaches Zertifikat nutzte. Das Root-Zertifikat verwendet für die digitale Signatur einen SHA-1 Hash-Alsgorithmus und für die asymmetrische Verschlüsselung ein 1024 Bit RSA-Verschlüsselungsverfahren. [11, vgl.] Sowohl der SHA-1 Hash-Algorithmus als auch das RSA-Verschlüsselungsverfahren mit einer Schlüssellänge von 1024 Bit sind bereits erfolgreich geknackt worden und daher als unsicher einzustufen. [12, 13, vgl.] Doch noch fataler als der Einsatz des unsicheren Hash-Algorithmus und des zu schwachen Verschlüsselungsfahrens, ist die Leichtigkeit der Entschlüsselung des privaten, geheimen Schlüssels. Robert Graham beschreibt in seinem Blog auf Errata Security eindrucksvoll, wie mit simplen Mitteln der Private Key exportiert und anschließend mit einer einfachen Wörterbuch-Attacke entschlüsselt werden konnte. [14, vgl.] Durch den privaten Schlüssel, welcher für alle betroffenen Geräte identisch ist, ist jeder Angreifer in der Lage, genau wie das Superfish-Programm, eigene „vertrauenswürdige“ Zertifikate für bösartige Verwendungen zu erstellen. Dadurch, dass den Angreifer-Zertifikaten ebenfalls automatisch vertraut wird, bekommen Anwender nicht mit, dass sie z. B. auf einer gefälschten Webseite surfen und ihre Daten ausspioniert werden. Da das Superfish Root-Zeritifikat im Windows-Zertifikatsspeicher abgelegt wurde, können Angreifer mit Zertifikaten, die durch dieses Root-Zertifikat signiert wurden, nicht nur bösartige Webseiten, sondern auch kriminelle Software (z. B. Malware) dem Nutzer problemlos als gutartig erscheinen lassen.

3.2 DELL

Der Computerhersteller DELL leistete sich einen ähnlich gravierenden Sicherheitsfehler wie sein Konkurrent Lenovo zuvor. Genau wie Lenovo hat DELL auch selbst signierte Root-Zertifikate auf einigen seiner Laptops installiert. Bei dem US-amerikanischen Hersteller sind es sogar zwei Root-Zertifikate. Sowohl das eDellRoot, als auch das DSDTestProvider Zertifikat wurden, genau wie das Superfish-Zertifikat, im Windows-Zertifikatsspeicher abgelegt. Beim Aufruf der allgemeinen Eigenschaften des eDellRoot-Zertifikats wird sogar ein Hinweis angezeigt, dass ein passender Private Key vorhanden ist. Joe Nord wendet in seinem Online-Blog die gleichen Vorgehensweisen zum Export und zur Entschlüsselung des DELL Private Keys an, wie Robert Graham beim Superfish Private Key. [15, vgl.]

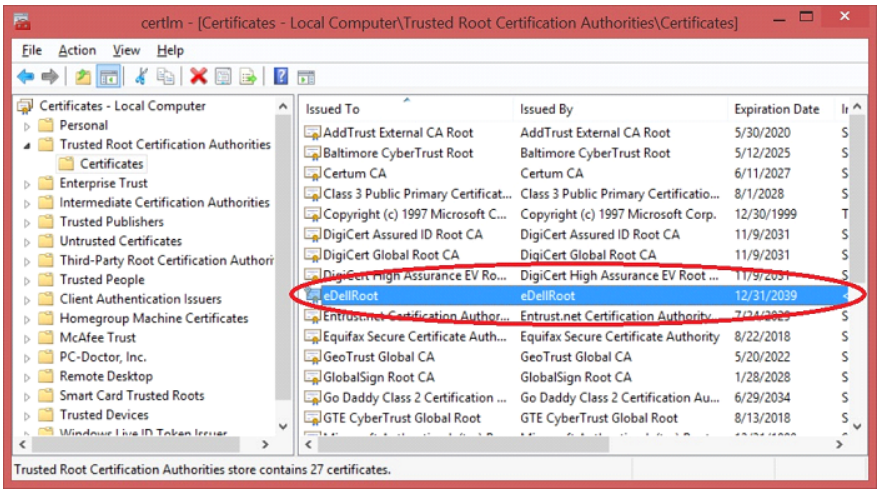


Abbildung 7: Ausschnitt aus Windowszertifikatsspeicher mit installiertem eDELLRoot Zertifikat, Quelle: [16]

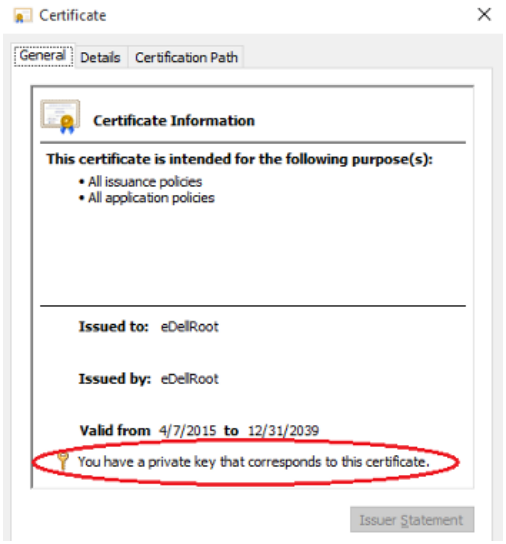


Abbildung 8: Eigenschaftsansicht von eDELLRoot Zertifikat mit Hinweis auf Private Key, Quelle: [15]

Angreifer mit dem privaten DELL Schlüssel haben die gleichen Angriffsmöglichkeiten auf infizierte DELL Geräte, wie Angreifer mit dem Superfish Private Key auf infizierte Lenovo Geräte. Beide DELL Zertifikate wurden durch Software installiert, das eDellRoot Zertifikat mit dem Dell Foundation Services Programm und das DSDTestProvider Zertifikat mit der Dell System Detect Software. Sie sollen, laut DELL, für einfacheren Support dienen. DELL hat auf seiner Webseite folgende Stellungnahme publiziert:

> [...] Das Zertifikat eDellRoot wurde zusammen mit unserer Anwendung Dell Foundation Services installiert und wird zur Unterstützung einer besseren, schnelleren und einfacheren Support-Erfahrung für unsere Kunden verwendet. Das Zertifikat ist keine Schadsoftware oder Adware. Es war ursprünglich dazu gedacht, die Service-Tag-Nummer des Systems an den Onlinesupport von Dell zu übermitteln, damit wir schnell das Computermodell identifizieren und unseren Kunden so einen unkomplizierteren und schnelleren Service bieten können. Das Zertifikat wird nicht zum Sammeln persönlicher Kundendaten verwendet. Bitte beachten Sie, dass sich das Zertifikat nicht von selbst neu installiert, nachdem es mit dem empfohlenen Dell Prozess ordnungsgemäß entfernt wurde.
> Wenn wir eDellRoot kennen, können wir uns auf alle unsere Anwendungen konzentrieren, die auf Dell PCs geladen werden. Wir können bestätigen, dass keine weiteren Root-Zertifikate auf dem werkseitig installierten Image installiert wurden. Wir haben jedoch herausgefunden, dass die Anwendung Dell System Detect und das dazugehörige Root-Zertifikat DSDTestProvider ähnliche Eigenschaften hat wie eDellRoot. Im Fall von Dell System Detect lädt der Kunde die Software proaktiv herunter, um mit der Webseite vom Dell Support zu interagieren. Dadurch können wir eine bessere und individuell abgestimmte Support-Erfahrung anbieten. Wie eDellRoot auch wurde das fragliche Support-Zertifikat entwickelt, um unseren Kunden einen schnelleren und einfacheren Support zu bieten. Die Vorteile sind jedoch auf die Kunden beschränkt, die die Funktion zur Produkterkennung auf unserer Support-Webseite zwischen dem 20. Oktober und dem 24. November 2015 genutzt haben. Die Anwendung wurde von der Dell Support-Webseite sofort entfernt und es steht ab sofort eine neue Anwendung ohne das Zertifikat zur Verfügung. Wir unterstützen proaktiv ein Software-Update, um das Problem anzugehen und haben im Folgenden Anweisungen zum Entfernen des Zertifikats bereitgestellt.[16]

DELL hat mit seiner Aussage offiziell bestätigt, eigene Zertifikate auf Nutzer-Endsystemen installiert zu haben. Das eDellRoot wurde augenscheinlich bereits vor Auslieferung auf den Geräten installiert und das DSDTestProvider erst nachträglich durch Installation und Verwendung des DELL Support-Programms. Durch das DELL-Statement fällt auf, dass das eDellRoot Zertifikat sich eventuell erneut installieren kann, wenn es nicht mit spezieller DELL Software bzw. geeignetem DELL Prozess richtig deinstalliert wurde.

> [...] Bitte beachten Sie, dass sich das Zertifikat nicht von selbst neu installiert, nachdem es mit dem empfohlenen Dell Prozess ordnungsgemäß entfernt wurde.“[16]

Die Ursachen für eine eventuelle Neuinstallation des DELL Zertifikats sind im Kapitel 4 Schutzmöglichkeiten beschrieben.

4 Schutzmöglichkeiten

Bedauerlicherweise haben Betroffene nicht allzu viele Möglichkeiten, sich gegen eben beschriebene Sicherheitslücken zu schützen. Eine Option wäre der Kauf von neuen Systemen ohne vorinstalliertem Betriebssystem. Wenn der Anwender selbst ein Betriebssystem nach dem Kauf installiert, kann er mit großer Sicherheit davon ausgehen, dass sich keine ungewollte, vorinstallierte Software und/oder kein selbst signiertes Zertifikat auf dem neu angeschafften Gerät befindet. Jedoch schützt diese Option nicht vor solchen Zertifikaten, die sich erst nachträglich installieren. Ein Beispiel ist das DSDTestProvider Zertifikat, das durch das DELL Support-Programm "Dell System Detectäuf das Endsystem kommt. [16, vgl.] Eine andere Variante des Schutzes ist die regelmäßige Kontrolle der auf dem System installierten Zertifikate. Durch diese Maßnahme können auch nachträglich installierte Zertifikate entdeckt werden. Zugegeben, bei der heutigen Masse an vorhandenen, vertrauenswürdigen Zertifizierungsstellen sowie zugehörigen Zertifikaten ist es nicht leicht, den Überblick zu behalten. Erschwerend kommt hinzu, dass viele Programme, z. B. Webbrowser wie Chrome oder Firefox, eigene Zertifikatsspeicher besitzen. Dabei kann nicht immer davon ausgegangen werden, dass diese Speicher sich auf den Zertifikatsspeicher des Betriebssystems beziehen und die identischen Zertifikate beinhalten.
Um sicherzustellen, dass mit dem richtigen Server kommuniziert wird und folglich keine Verbindung zu einer gefälschten Webseite besteht, sollte man das Zertifikat prüfen, welches für die aktuelle Kommunikation verwendet wird. Jeder Browser zeigt neben der HTTPs-Adresse ein Schlosssymbol. Über dieses Symbol werden die Eigenschaften des aktuell für diese verschlüsselte Verbindung verwendeten Zertifikats erreicht.

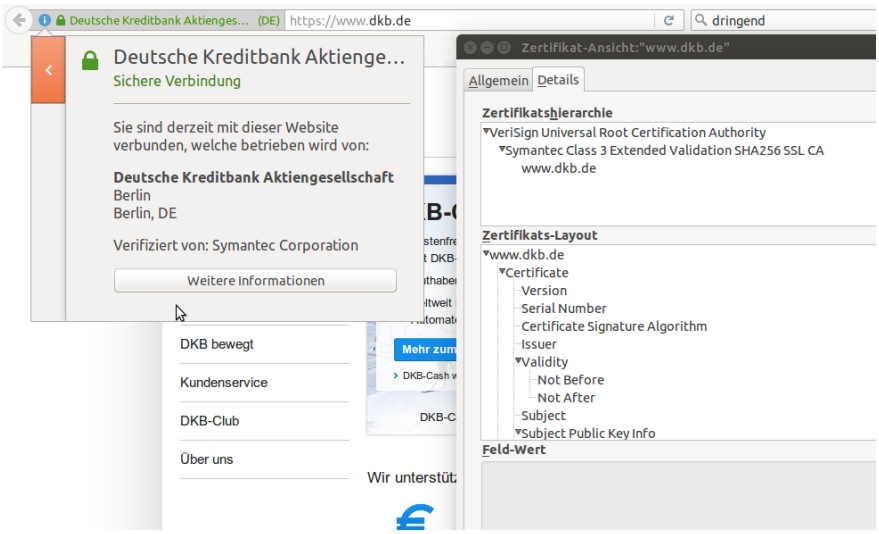


Abbildung 9: Aufruf der DKB Webseite. Details des Zertifikats, welches für die Verbindung verwendet wird

Verschiedene Webseiten, z. B. `https://globalsign.ssllabs.com`, bieten eine Überprüfung der gewünschten Webseite an. Als Ergebnis zeigen sie unter anderem an, welches originale Zertifikat diese Webseite wirklich verwendet. Mittels dieser Information und der Zertifikats-Eigenschaften durch den Browser ist jeder Internetnutzer in der Lage zu vergleichen, ob die verschlüsselte Verbindung das richtige Zertifikat nutzt. Handelt es sich nicht um das korrekte,

originale Zertifikat und gab es zusätzlich keine Fehlermeldung/Warnung, so muss davon ausgegangen werden, dass keine direkte Verbindung zu der gewünschten Webseite besteht. Solche Fälle deuten stark darauf hin, dass die verschlüsselte Verbindung durch eine MITM-Attacke aufgebrochen wurde und die Daten eventuell mitgelesen oder sogar manipuliert werden. Nach Aufdeckung einer solchen Attacke muss das gefälschte Zertifikat im System (Zertifikatsspeichern) gesucht und anschließend gelöscht werden. Dabei ist zu beachten, dass es nicht immer ausreicht nur das entdeckte Zertifikat selbst zu löschen. Da Zertifikate auf der Basis einer Public Key Infrastruktur [7, vgl.] erstellt sind, können noch weitere Zertifikate für solch eine Attacke verantwortlich sein. Es sollten, neben dem aufgespürten, gefälschten Zertifikat, zusätzlich alle anderen Zertifikate, die sich in der hierarchischen Kette befinden, überprüft und ggf. entfernt werden. Im Lenovo-Beispiel konnten mittels des gehackten, selbst signierten Root-Zertifikats weitere Zertifikate erstellt werden. Mit jedem dieser Zertifikate war anschließend je eine separate MITM-Attacke möglich. Das Sicherheitsproblem war mit der Eliminierung des für die MITM Attacke verwendeten Zertifikats noch nicht gelöst. Erst nach erfolgreichem Entfernen des selbst signierten Root-Zertifikats konnten keine weiteren gefälschten Zertifikate erzeugt werden.
Beim DELL-Vorfall schrieb Liam Tung auf der ZDNET-Webseite:

> [...] das einfache Entfernen des eDELLRoot-Zertifikats aus dem Administrator und persönlichen Zertifikatsspeicher ist nicht genug, um den Nutzer zu schützen. Einige Nutzer haben in der Tat berichtet, dass das Zertifikat nach einem Neustart wieder aufgetaucht ist.[17]

Ursache für die Neuinstallation ist das DELL-Programm „Dell Foundation Services“, welches dieses Zertifikat verwendet. Erst mit der Deinstallation des Programms bzw. eines Plug-ins des Programms und der manuellen Löschung des DELL Zertifikats ist das selbst signierte Zertifikat dauerhaft vom System erfolgreich entfernt und die Sicherheitslücke geschlossen worden. Liam Tung schrieb zur korrekten Entfernung:

> Um es dauerhaft zu entfernen und um zu verhindern, dass es sich erneut installiert, müssen Nutzer das eDELL Plugin entfernen. [17]

Für die detaillierte Information um welches Plug-in es sich genau handelt und worauf besonders zu achten ist, nutzt er die Ergebnisse von den Duo Security Forschern Darren Kemp, Michail Davidov und Kyle Lady.

> ‘Dies kann vollbracht werden mit Hilfe der Löschung des Dell.Foundation.Agent.Plugins.eDell.dll Moduls vom System. Geschieht dies nicht, so kann es weiterhin zur Aussetzung dieser Sicherheitslücke kommen.‘, sagte Duo Security.
> ‘Beachte, immer wenn sie ein Werksreset auf ihrem DELL System durchführen, wird dieses Zertifikat und das eDell Plugin auf dem System wieder hergestellt und sie müssen es erneut manuell entfernen‘ [...] [17]

Die beiden Beispiele zeigen, dass es nicht ausreicht nur die Zertifikatsspeicher auf ungewöhnliche Eintragungen zu durchsuchen, sondern ebenfalls die Programmliste des Systems auf unerwartete oder ggf. unnötig installierte Programme zu kontrollieren.

5 Zwischenfazit

Beide Systemhersteller nutzten ihre Position in der Marktwirtschaft und das Vertrauen, welches ihnen die Kunden entgegenbringen, schamlos aus. Sie ließen dem Käufer im Glauben, dass er ein solides Gerät mit sicherer Software gekauft hätte. Doch ohne selbständige Gegenmaßnahmen des Kunden war dieser, mittels der von Lenovo und DELL selbst signierten Zertifikate, potentiellen Angreifern hilflos ausgesetzt. Die Käufer müssen auf der einen Seite für die Zukunft hoffen, dass die Gerätehersteller aus ihren Fehlern gelernt haben und wieder sichere Systeme herstellen bzw. verkaufen. Auf der anderen Seite kann und sollte jeder selbständig Kontrollen und Überprüfungen durchführen. Außerdem ist es ratsam, sich ein wenig mit den Systemen zu befassen mit denen man täglichen Umgang hat und wichtige Tätigkeiten, wie z. B. Online Banking, durchführt. Darunter zählt auch das regelmäßige Abrufen von Informationen über Sicherheitsneuigkeiten in bekannten Sicherheitsforen, z. B. `https://www.heise.de/security`

Gemäß dem Sprichwort „Vertrauen ist gut, Kontrolle ist besser.“, sollte jeder Benutzer, mit den verfügbaren Möglichkeiten, die verwendeten Systeme und Dienste immer wieder überprüfen.

6 Man-in-the-Middle-Angriffe im geswitchten Netz

Es gibt Man-in-the-Middle-Angriffe nicht nur gegen SSL/TLS Verbindungen sondern auch gegen "normale"Netzwerkverbindungen. Sie werden von Angreifern eingesetzt, um in einem geswitchten Netz zu sniffen.

Literatur

[1] TELECOMMUNICATION STANDARDIZATION SECTOR OF INTERNATIONAL TELECOMMUNICATION UNION (ITU-T).
X.200 : Information technology - Open Systems Interconnection - Basic Reference Model: The basic model,
01. Juli 1994.
http://www.itu.int/rec/T-REC-X.200-199407-I
(Abrufdatum: 15.07.2016).

[2] Serge Malenkovich.
Was ist eine Man-in-the-Middle-Attacke?,
10. April 2013.
https://blog.kaspersky.de/was-ist-eine-man-in-the-middle-attacke/905/
(Abrufdatum: 15.07.2016).

[3] Bild durch Fabian Uhlmann aus Bildern von nachfolgend aufgeführten URLs zusammengestellt.
http://ecx.images-amazon.com/images/I/81LcrgMpIcL._SL1500_.jpg,
http://i5.walmartimages.com/dfw/dce07b8c-6381/k2-_
aa74fc49-072f-4d83-afdc-4164105621f2.v1.jpg,
https://gigaom.com/wp-content/uploads/sites/1/2013/07/
hacker-cyber-attack-640x522.jpg
(Abrufdatum: 15.07.2016).

[4] R. Fielding and J. Reschke.
Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing. RFC 7230, RFC Editor,
Juni 2014.
http://www.rfc-editor.org/rfc/rfc7230.txt (Abrufdatum: 15.07.2016).

[5] A. Freier, P. Karlton, and P. Kocher.
The Secure Sockets Layer (SSL) Protocol Version 3.0. RFC 6101, RFC Editor,
August 2011.
http://www.rfc-editor.org/rfc/rfc6101.txt (Abrufdatum: 15.07.2016).

[6] E. Rescorla.
HTTP Over TLS. RFC 2818, RFC Editor,
Mai 2000.
http://www.rfc-editor.org/rfc/rfc2818.txt (Abrufdatum: 15.07.2016).

[7] TELECOMMUNICATION STANDARDIZATION SECTOR OF INTERNATIONAL TELECOMMUNICATION UNION (ITU-T).
X.509 : Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks,
14. Oktober 2012.
https://www.itu.int/rec/T-REC-X.509-201210-I/en
(Abrufdatum: 15.07.2016).

[8] STAMFORD, Conn.
Gartner Says Worldwide PC Shipments Declined 9.6 Percent in First Quarter of 2016,
11. April 2016.
http://www.gartner.com/newsroom/id/3280626 (Abrufdatum: 15.07.2016).

[9] Hanno Böck.
Lenovo-Laptops durch Superfish-Adware angreifbar,
19. Februar 2015.
http://www.golem.de/news/adware-lenovo-laptops-durch-superfish-adware-angreifbar-
html (Abrufdatum: 15.07.2016).

[10] Screenshot by Robert Graham.
http://www.cnet.com/how-to/lenovo-superfish-adware-uninstall-fix/
(Abrufdatum: 15.07.2016).

[11] Marc Rogers.
Lenovo installs adware on customer laptops and compromises ALL SSL,
19. Februar 2015.
http://marcrogers.org/2015/02/19/lenovo-installs-adware-on-customer-laptops-and-c
(Abrufdatum: 15.07.2016).

[12] Jürgen Schmidt. Kryptoverfahren SHA-1 geknackt, 16. Februar 2005.
http://www.heise.de/newsticker/meldung/Kryptoverfahren-SHA-1-geknackt-135372.
html (Abrufdatum: 15.07.2016).

[13] Andrea Pellegrini, Valeria Bertacco, and Todd Austin. Fault-Based Attack of RSA
Authentication, 2010.
http://web.eecs.umich.edu/~valeria/research/publications/DATE10RSA.pdf
(Abrufdatum: 15.07.2016).

[14] Robert Graham.
Extracting the SuperFish certificate,
19. Februar 2015.
http://blog.erratasec.com/2015/02/extracting-superfish-certificate.
html#.V4uWdu22Hfa (Abrufdatum: 15.07.2016).

[15] Joe Nord.
New Dell computer comes with a eDellRoot trusted root certificate,
22. November 2015.
http://joenord.blogspot.de/2015/11/new-dell-computer-comes-with-edellroot.
html (Abrufdatum: 15.07.2016).

[16] DELL.
Informationen zu den Zertifikaten eDellRoot und DSDTestProvider und Anweisungen
zum Entfernen dieser Zertifikate von Ihrem Dell PC,
letzte Modifizierung 20 Juni 2016.
http://www.dell.com/support/article/us/en/19/SLN300321/DE
(Abrufdatum: 15.07.2016).

[17] Liam Tung.
How to remove Dell's 'Superfish 2.0' root certificate - permanently,
24. November 2015.
http://www.zdnet.com/article/how-to-remove-dells-superfish-2-0-root-certificate-p
(Abrufdatum: 15.07.2016).