SSL Downgrade von IOT-Geräten

Seminar "Das Internet der Dinge – Ein Hackerparadies?"

Alexander Korff, Sergej Maul, Yannik Stöcklin
Sebastian Philipp, Daniel Seidinger, Fabian Neumeier
Lukas Stöckli, Manuel Rickli, Désirée Nusch
Samuel Hugger, Clement Francois, Joel Grossenbacher

17. Dezember 2017

1 Lorem ipsum

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus.

Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

2 Lokale Kommunikation mit der Philips Hue

Nach einigen Beobachtungen stellten wir fest, dass in der Zeit zwischen dem Befehl an das Amazon Echo, das Licht anzuschalten, und dem tatsächlichen Aufleuchten der Lampe kein Traffic zwischen der Philips Hue Bridge und dem Internet zu beobachten war. Daher nahmen wir an, dass der Befehl zum Anschalten im lokalen Netzwerk gesendet wird. Lokaler Traffic würde auch nicht in den mitgeschnittenen Paketen enthalten sein, da wir ARP Spoofing nur zwischen der FRITZ!Box und der Hue Bridge betrieben hatten.

Entsprechend änderten wir unser Vorgehen, um den Traffic zwischen dem Echo und der Hue Bridge mitzuschneiden. Dies war sofort erfolgreich; wir konnten feststellen, dass das Echo eine HTTP Request im Klartext an die Hue Bridge sendet. Eine auf das Wesentliche

```
PUT /api/-UaDNHD5j44y07zYdAOEg0JuIakQpu72ivJXXHVS/lights/2/
   state HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 13

{"on": false}
```

Listing 1: Ein HTTP Request zum Ausschalten von Lampe Nr. 2.

gekürzte Version eines solchen Requests zum Ausschalten einer Lampe ist in Listing 1 dargestellt.

Abgesehen davon, dass der falsche Wert für `Content-Type` angegeben wird (anstatt dem tatsächlichen `application/json`), fielen folgende Punkte auf:

- Die Request enthält eine nicht weiter bekannte Art von Zugriffsberechtigung oder ID in der URL. Dies stellte jedoch kein Hindernis dar; die ID liess sich beliebig oft wiederverwenden.
- Die Lampe, die angesprochen wird, wird ebenfalls numerisch in der URL übergeben, in diesem Fall Lampe Nr. 2.
- All dies geschieht komplett unverschlüsselt; ein SSL Downgrade war daher gar nicht notwendig.

Analog konnten wir die Befehle zum Ausschalten, zum Setzen der Helligkeit sowie der Farbe mitschneiden und auch problemlos selbst versenden. Da sich die Farbe mit dem Amazon Echo nur verändern lässt, wenn man einen Philips Hue Account verwendet, schnitten wir hierzu den Datenverkehr zwischen der Hue Bridge und einem Smartphone mit, auf welchem die zugehörige Software verwendet wurde, welche das Setzen der Farbe auch ohne Login erlaubt. Auch hier war wieder keine Verschlüsselung im Spiel.Mit dem HTTP Request in Listing 2 wird die Lampe angeschalten und auf eine gegebene Helligkeit und Farbe gesetzt. Die Helligkeit ist eine einzelne Zahl im Bereich zwischen 0 und 255. Die Farbe wird durch zwei Werte “x” und “y” zwischen 0 und 1 beschrieben; die Bedeutung dieser Werte erschloss sich uns jedoch nicht. Wir stellten hierzu zwei Hypothesen auf:

- Die Werte ensprechen den (normalisierten) Koordinaten der Farbe im Farbauswahldialog der Smartphone-App.
- Die Werte entsprechen dem Farbton und der Sättigung im HSV-Farbmodell; die Helligkeitskomponente wird separat übergeben.

Beide Hypothesen liessen sich durch Versuche falsifizieren. Die API ist zwar vom Hersteller dokumentiert, aber erfordern wiederum einen Login, um darauf zuzugreifen. [1] Aus Zeitgründen wurde diese API nicht weiter untersucht.

```
PUT /api/-UaDNHD5j44y07zYdAOEg0JuIakQpu72ivJXXHVS/lights/2/
   state HTTP/1.1
Content-Type: application/json
Content-Length: 42

{"on": true, "bri": 255, "xy": [1.0, 1.0]}
```

Listing 2: Ein HTTP Request für bunte Lampen.

3 LED Matrix

Die in einem früheren Projekt der Vorlesung *Computer Architecture and Operating Systems* gebaute LED Matrix wurde im Verlauf des Seminars bereits um einige Funktionalitäten im Bereich des Internets der Dinge erweitert. Unter anderem ist es möglich mittels Sprachbefehlen (Amazon Alexa) das aktuelle Wetter, eine Notiz oder auch verschiedene Farben anzuzeigen zu lassen. Die Matrix wird mit einem Arduino Mega angesteuert, welcher seine Informationen von einem eigenen Webserver abruft. Bisher fand diese Kommunikation mit dem Internet über eine unverschlüsselte Verbindung mittels einer sogenannten Ethercard, einer Ethernet Erweiterung für den Arduino, statt.

Zum Testen der zahlreichen Angriffsmethoden auf SSL musste also zuerst eine verschlüsselte Verbindung hergestellt werden, um im Anschluss versuchen zu können diese zu knacken. Da der Arduino selbst nicht genug Rechenleistung zum herstellen einer SSL Verbindung besitzt musste das Setup entsprechend verändert werden. Dazu wurde die Ethercard durch einen WiFi-Chip des Typs ATWINC1500 ersetzt, welcher die benötigte SSL Funktionalität mit sich bringt.

Nach Umrüstung der Hardware musste die Software entsprechend angepasst werden, um vom neuen Netzwerkinterface Gebrauch zu machen. Mit der Arduino WiFi101-Bibliothek [2] wird eine SSL Verbindung zum Webserver aufgebaut. Der Webserver selbst war bereits für SSL eingerichtet, womit nur Änderungen beim Arduino-Client nötig waren. Die SSL Zertifikate werden manuell mittels eines Firmware-Updaters auf das WiFi-Modul geladen werden.

```
if (client.connect(server, 443)) {
...
}
```

Listing 3: Port 443 ohne Fallback auf Port 80

Nach Implementierung aller Änderungen wurden diverse Angriffsversuche unternommen. Das blockieren von Port 443, um eine SSL Verbindung zu unterbinden und einen Fallback auf Port 80 zu erzwingen, erwies sich wie vorhergesehen als erfolglos, da schlicht kein Fallback im Code 3 vorgesehen ist und der Arduino ausschliesslich auf Port 443 einen Verbindungsaufbau versucht. Auch die nächste Methode SSL-Strip blieb erfolglos aufgrund der expliziten Nutzung von SSL ohne Fallback. Zuletzt wurde mittels SSL-Sniffing

probiert ob gefälschte Zertifikate vom WiFi-Chip akzeptiert werden um die Verschlüsselung zu umgehen, jedoch erwies sich auch diese Methode als nutzlos, da nur die korrekt eingespielten SSL Zertifikate akzeptiert werden.

Die Matrix ist somit gegen allen getesteten Angriffsmethoden immun, aufgrund von korrekter Konfiguration und strikter Verwendung von SSL.

4 Quellenverzeichnis

[1] Koninklijke Philips Electronics N.V. *Philips hue API*. 2016. URL: `https://developers.meethue.com/philips-hue-api` (besucht am 11. 12. 2017).

[2] Arduino AG. *WiFi101 library*. 2016. URL: `https://www.arduino.cc/en/Reference/WiFi101` (besucht am 17. 12. 2017).