Hochschule für Technik
und Wirtschaft Berlin

University of Applied Sciences

Ausarbeitung zum Thema Spionage Chips

für das Modul

Datenschutz und Datensicherheit

an der

Hochschule für Technik und Wirtschaft (HTW) Berlin

Gutachter: Dr. Prof. Wojciech Dabrowski, Herr Prof. Zielinski und Herr Helbig

Von: Max Hager

Datum: 11.06.2022

Spionage Chips

1 Einleitung

Diese Arbeit ist eine Ausarbeitung des Themas Spionage Chips im Kurs Datenschutz und Datensicherheit bei Dr. Prof. Wojciech Dabrowski, Herr Prof. Zielinski und Herr Helbig an der HTW Berlin. Die Arbeit ist eine Auseinandersetzung mit dem Thema Spionage Chips und zeigt Beispiele wie Spionage Chips eingesetzt werden oder eingesetzt werden können. Das Ziel ist es den Leser einen ersten Einblick in die Möglichkeiten dieses Bereiches zu geben. Die Arbeit ist so aufgebaut, dass verschiedene Beispiele beschrieben werden. Folgend die Strukturierung für jedes gegebene Beispiel:

Spionage Gerät

Definition

Gerüchte und Funde

Abschließend greift die Arbeit einen Ausblick in die Zukunft auf.

2 Mikrochip

2.2 Definition

Ein Mikrochip oder auch integrierter Schaltkreis genannt ist üblicherweise ein Halbleiterplättchen aus Silizium, das eine Sammlung von elektronischen Schaltkreisen integriert. Zu den Bauelementen dieser elektronischen Schaltkreisen gehören Widerstände, Transistoren, Kondensatoren und Dioden. Die Bauelemente werden so zusammengeschaltet, dass diese zusammen eine bestimmte Funktion ausführen. Jede einzelne Funktion auf einem Computer wird von einem Schaltkreis auf dem Mikrochip gesteuert. Das heißt, für das öffnen von Google Chrome oder Visual Studio Code sind ganz bestimmte Schaltkreise notwendig. Solch ein Microchip wird mit anderen für einen Computer notwendigen Komponenten auf einer Leiterplatte befestigt. Auf solch einer Leiterplatte ist es auch möglich Microchips zu implementieren, die dafür dienen sollen einen Angreifer Zugang zu bestimmten Informationen zu erstatten oder Manipulationen unter den auf dem Computer laufenden Programmen durchzuführen.

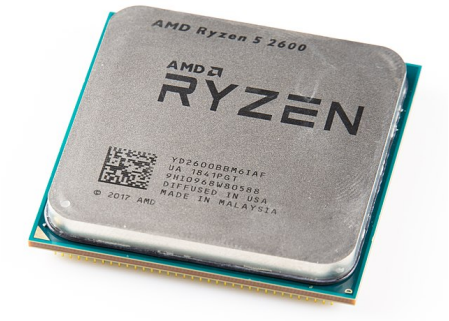

Figure 1: [1] Mikrochip

2.3 Gerüchte und Funde

Am 4ten Oktober 2018 ist ein ausführlicher Artikel mit den Titel “The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies” in Bloomberg erschienen [2]. Darin geht es darum, wie angeblich Mikrochips in Server, die von US amerikanischen Unternehmen benutzt wurden eingeschleust wurden sind. Konkret soll das das Unternehmen Supermicro [3] dabei verantwortlich gewesen sein, dass Spionage Chips auf die server der us amerikanischen Unternehmen landen konnten. Supermicro ist ein us amerikanisches Unternehmen welches eines der weltweit größten Unternehmen für die Erstellung von Server Hauptplatinen ist. Es gab Produktionsstellen des Unternehmens in China. Dort sollen die Mikrochips unter Einfluss chinesischer Mitglieder der Volksbefreiungsarmee auf die in der USA verwendeten Hauptplatinen drauf gelötet wurden sein. Aus dem Bloomberg Artikel ist nicht genau ausfindig zu machen, wie der Chip genau funktioniert, aber es ist davon auszugehen, dass der Chip der winzig klein ist (siehe Bild) auf eine Stelle an der Hauptplatine gelötet wurde, wo es schwierig ist Ihn als Spionagechip zu erkennen. An der Stelle angebracht solle der Chip die Fähigkeit haben durch Fernzugriff Datenströme auszulesen.

Figure 2: [4] Demonstration Größe Mikrochip “The Big Hack”

3 RFID

3.1 Definition

Radio-frequency identification (RFID) benutzt elektronische Felder für das automatische identifizieren und tracken von Sendern welche zu einem Empfänger zugehörig sind. Ein Sender oder Transponder ist ein Mikrochip auf dem Informationen abgespeichert werden können. Der Empfänger liest die Daten, die sich auf einem Sender empfinden. Zum Beispiel könnte die HTW Studierenden Karte so funktionieren, dass ein Mikrochip welcher der Sender ist einer Identifikationsnummer im Speicher zugewiesen ist. Im Fall der Bezahlung mit der Studierenden Karte an der Kasse für das essen, gibt es einen Empfänger, der die Identifikationsnummer ausliest, welche mit einem bestimmten Studenten in einer Datenbank gelinkt ist. Dadurch Sender und Empfänger mit elektronischen Wellen funktioniert, gibt es einen Zeitpunkt in dem sich die elektronischen wellen frei in einem Raum bewegen und daher durch Angreifer abgefangen werden.

3.2 Gerüchte und Funde

Nicht ganz RFID aber der Vorreiter der RFID Technik kam nach dem zweiten Weltkrieg zum Einsatz. “The Thing” oder auch bekannt als “The great Seal bug” war ein Geschenk der Sowjetunion an den US amerikanischen Botschafter W. Averall Harriman.

Figure 3: [5] “The Thing”

Das Geschenk wurde in der US amerikanischen Botschaft aufgehangen. In “The Thing” wurde eine Art Antenne eingebaut welche durch von außerhalb gesendeten Signalen abgehört werden konnte. RFID kann zu einem vielfältigen tracking zum Einsatz kommen. Eine Idee wäre es Produkte in einem Supermarkt mit einem RIFD Chip auszustatten, um Kassen überflüssig zu machen. Der Käufer geht nur durch eine Schranke mit Empfänger Geräten, welche alle Item Nummern der jeweilig ausgewählten Produkte ausließt und daraufhin eine Bezahlung auslöst. Wenn die gekauften Produkte dann zuhause im Mülleimer landen könnte jemand mit einem Empfängergerät und dem Wissen darüber welche Identifikationsnummer welches Produkt ausmacht genau auslesen welche Lebensmittel die Person gekauft hat. Das Beispiel lässt sich auf Prozesse mit sensibleren Daten wie Zahlungskarten oder Autoschlüssel wiederholen.

4 Mini GPS tracker

4.1 Definition

Ein mini GPS Gerät ist ein Gerät welches GPS (global positioning system) verwendet um mithilfe der WGS84 UTM geografischen Position die Position zu bestimmen [6]. WGS84 UTM ist ein einheitliches System für die Messung von Punkten auf der Erde, indem man durch das System Koordinaten auf der Oberfläche der Erde zugehörig macht. Das mini GPS Gerät empfängt Signale von mindestens vier Satelliten. Von jedem Satellit gehen Kreise aus und an dem Punkt, wo sich das Gerät befindet, was die Signale empfangen soll lässt sich durch das schneiden der Kreise die genaue Lokalisierung des Gerätes möglich machen. Die Satelliten für GPS sind im Besitz der USA. Es gibt auch

andere Lokalisierungssysteme, das sind Satelliten die zu anderen Länder oder Vereinigungen zugehörig sind. GPS ist allerdings die am weitesten verbreitetste Methode. Die Daten zur genauen Lokalisierung von Objekten oder Menschen sind stark sensibel. Durch das wissen der Position eines Autos von einem Opfer lässt sich für den Angreifer leicht nachvollziehen, wann eine gute Zeit wäre in das Haus des Opfers einzubrechen.

4.2 Gerüchte und Funde

4.3 Shenzhen i365 Tech

Shenzhen i365 Tech ist ein chinesischer GPS tracker Hersteller. Das Unternehmen hat GPS tracker hergestellt, bei dem jedem Gerät als ID Nummer ihre International Mobile Equipment Identity zugewiesen wurde (IMEI) [7]. Die IMEI ist eine einzigartige Nummer, mit der man ein Gerät in einem Mobilfunknetz identifizieren kann. Ein Mobilfunknetz ist ein drahtloses Kommunikationsnetzwerk zwischen verschiedenen Geräten die in so einem Netz miteinander kommunizieren können. Allen Geräten wurde das gleiche Passwort "123456" vergeben. Durch diese Sicherheitslücken ist es möglich, wenn man sich im gleichen Netzwerk wie die chinesischer GPS tracker befindet, den Datenaustausch abzuleiten oder zu modifizieren. Das heißt einem Angreifer wäre es möglich die Positionsdaten des Gerätes ausführlich zu machen oder Daten, die das Gerät sendet zu manipulieren.

4.4 WLTP

Das Worldwide harmonized Light vehicles Test Procedure ist ein, Messverfahren zur Bestimmung der Abgasemissionen (Schadstoff- und CO2-Emissionen) und des Kraftstoff-/Stromverbrauchs von Kraftfahrzeugen. [8]. Dabei handelt es sich um eine im Auto angebrachte Box die die beschriebenen Informationen ermittelt. Dem Video hier [9] zu entnehmen, soll es dazu gekommen sein, dass Behörden die GPS Daten die über WLTP übermittelt werden genutzt haben, um zu identifizieren, ob Bürger, die durch COVID festgelegte Ausgangsbeschränkung einhalten. Es soll so gewesen sein, dass Personen, derer Fahrzeug zur bestimmten Zeit nicht am Wohnort gewesen sei eine Geldstrafe zugesendet wurde.

5 Ausblick

Mit Fortschritt von Technologie könnten neue Möglichkeiten entstehen, wie Spähattacken mit Mikrochips ausgeführt werden können. Es gibt verschiedene Forschungsinstitute die an der Entwicklung von Schaltkreisen im Nanometer Bereich arbeiten. Ein Nanometer ist gleich zu 10^{-9} Meter oder eine Reihe von 10 Wasserstoff Atomen [10]. RFID Chips die jetzt zum Einsatz kommen könnten dadurch kleiner und unauffälliger gemacht werden. Das könnte ein Risiko darstellen, weil Angreifer ihre Angriffsmittel leichter anonymisieren könnten, was die Entdeckung solcher schwieriger ausfallen lässt. Es ist nicht immer einfach genau festzustellen, welche Daten bei einer Späh Affäre abgekommen sind. Bevor irgendwelche Daten an die Oberfläche gelangen werden die Fälle intern in einem

Unternehmen behandelt. Es kann sogar sein, dass Informationen über einen Angriff erst gar nicht an die Öffentlichkeit gelangen. Das schützt das Unternehmen vor einem schlechten Ruf, welcher Verkaufszahlen des Unternehmens schwinden lassen könnte. Um Fälle wie die Produktion von leicht eindringbaren RFID chips wie bei Shenzhen i365 Tech zu vermeiden könnten Unternehmen mehr Ressourcen in die Sicherheitsabteilung des Unternehmens investieren.

6 Quellen

[1, 4] Wirtschaftswoche. (2021, Januar 19). Mikrochip-Mangel: Autoindustrie fehlt Elektronik-Nachschub. Wirtschaftswoche, von https://www.wiwo.de/unternehmen/auto/lieferengpaesse-der-grosse-mikrochip-mangel-autoindustrie-fehlt-nachschub/26831212.html

[2] O. J. Bloomberg. (04.10.2018). The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. Bloomberg, von https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

[3] Supermicro. https://www.supermicro.com/en/products/x12?utm_term=supermicro&utm_campaign=Searc
12928390&hsa_kw=supermicro&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gclid=Cj0KCQjw-pCVBhCFARIsAGMxhAdc0z_hdUoGLvfA8VxFBD6TE7iYkhCqKGrD3wt3nK-XnULai7cO6WAaAmz-EALw_wcB

[5] Wikipedia contributors. (2022, April 30). The Thing (listening device). Wikipedia, The Free Encyclopedia, von https://en.wikipedia.org/w/index.php?title=The_Thing_(listening_dev

[6] Wikipedia contributors. (2022b, Mai 15). GPS tracking unit. Wikipedia, The Free Encyclopedia, von https://en.wikipedia.org/w/index.php?title=GPS_tracking_unit&oldid=1087972466

[7] Goodin, D. (2019, September 5). 600,000 GPS trackers for people and pets are using 123456 as a password. Ars Technica, von https://arstechnica.com/information-technology/2019/09/600000-gps-trackers-for-people-and-pets-are-using-123456-as-a-password/

[8] Wikipedia contributors. (o. J.). Worldwide harmonized Light vehicles Test Procedure. Wikipedia, The Free Encyclopedia, von https://de.wikipedia.org/w/index.php?title=Worldwide_harmonized_Light_vehicles_Test_Procedure&oldid=

[9] Reifen-KFZ Werkstatt Mietwerkstatt [ReifenKFZWerkstattMietwerkstatt]. (2021, April 21). Ihr PKW wird von Behörden und Staat Überwacht ohne das Sie das Wissen. Wir können das ändern. Youtube, von https://www.youtube.com/watch?v=DQHLRX6HHs4

[10] Wikipedia contributors. (2022b, Mai 7). Nanocircuitry. Wikipedia, The Free Encyclopedia, von https://en.wikipedia.org/w/index.php?title=Nanocircuitry&oldid=1086598403