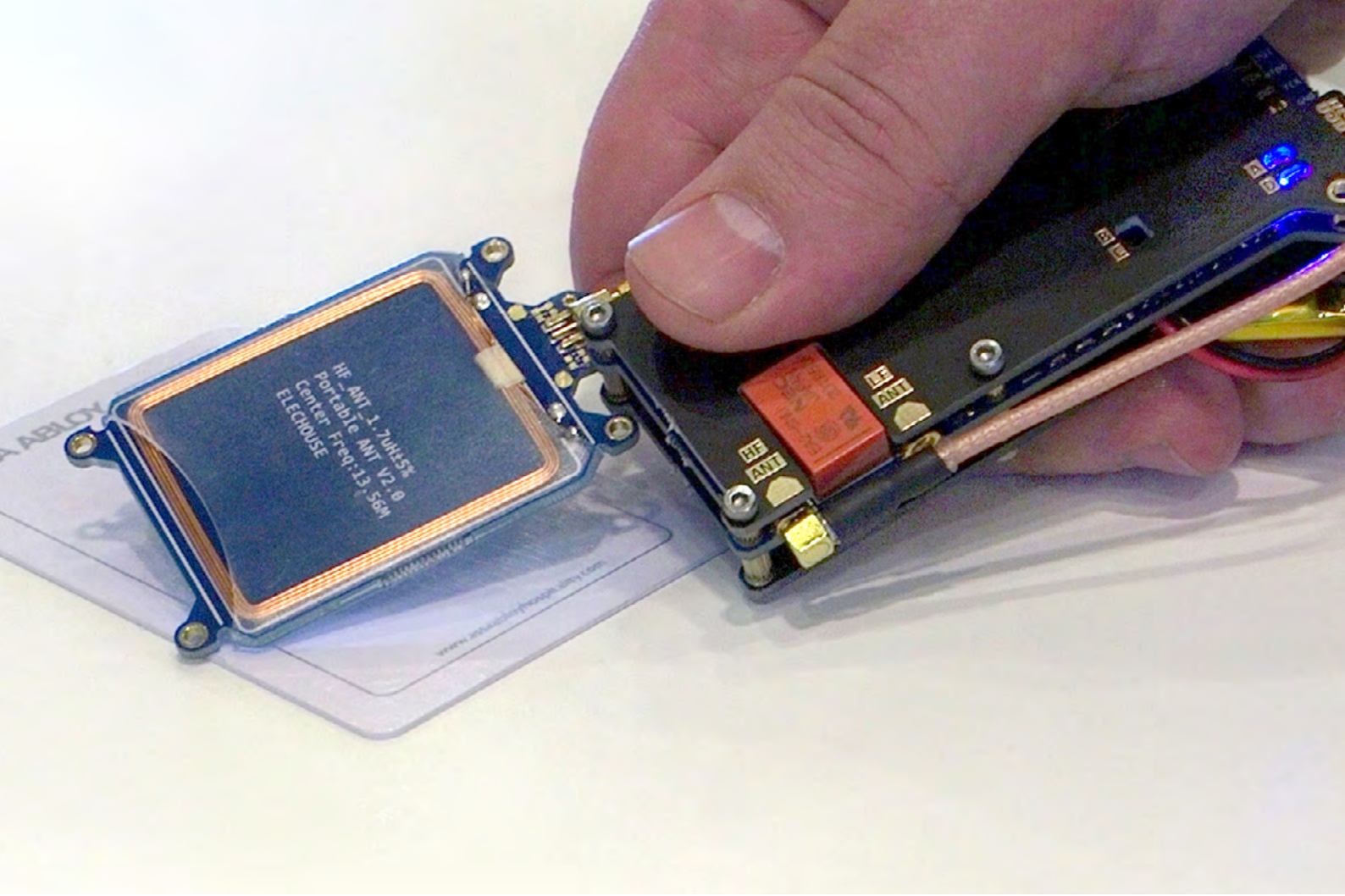

FAQ

GHOST IN THE LOCKS

F-Secure hat eine Sicherheitslücke in den Zugangssystemen weltweit operierender Hotelketten entdeckt, das von Angreifern kompromittiert werden kann, um sich unbemerkten Zugang zu allen Räumen zu verschaffen.

WAS IST DAS GENAUE PROBLEM?

Die F-Secure Experten Tomi Tuominen and Timo Hirvonen, haben kritische Konstruktionsfehler in den von Assa Abloy weit verbreitetem Hotelschloss-Softwaresystem Vision by Vingcard gefunden.

WIE KANN EIN ANGREIFER DIE SCHWACHSTELLEN AUSNUTZEN?

Zunächst muss sich ein Angreifer einen elektronischen Schlüsselkarte zur Zielanlage besorgen. Tatsächlich reicht jede Art von Schlüsselkarte, sei es für ein Hotelzimmer, eine Abstellkammer oder eine Garage. Zudem muss die Karte zur Zeit des Angriffs nicht einmal aktiviert sein: Selbst eine abgelaufene Karte eines Aufenthaltes von vor fünf Jahren reicht aus.

Der Angreifer liest die Karte aus und verwendet dazu eine Hardware mit der er weitere Karten für das Gebäude errechnen lassen kann. Diese Karten können mit jedem Schloss in den Räumlichkeiten getestet werden. Innerhalb weniger Minuten ist das Lesegerät dann in der Lage, einen Generalschlüssel für das Gebäude zu generieren. Das Gerät selbst kann anschließend anstelle einer Schlüsselkarte verwendet werden, um jedes beliebige Schloss im Gebäude zu öffnen oder alternativ eine vorhandene Schlüsselkarte zu überschreiben, der dann den neu erstellten Generalschlüssel enthält.

WAS HABEN DIE F-SECURE EXPERTEN NOCH HERAUSGEFUNDEN?

Darüber hinaus haben Tomi Tuominen und Timo Hirvonen bei ihren Untersuchungen festgestellt, dass die Vision-Software im gleichen Netzwerk genutzt werden kann, um Zugang zu sensiblen Kundendaten zu erhalten.

WER IST ASSA ABLOY?

Das Unternehmen Assa Abloy mit Hauptsitz in Schweden ist weltweit der größte Schlosshersteller. Assa Abloy Hospitality ist der Geschäftsbereich des Unternehmens, der Schließsysteme für Hotels, Kreuzfahrtschiffe und andere Branchen produziert. Die vom Angriff betroffene Software Vision kommt jedoch nur in Hotels und auf Kreuzfahrtschiffen zum Einsatz.
https://www.assaabloyhospitality.com/en/aah/com/solutions/

WURDE DAS PROBLEM BEHOBEN?

Assa Abloy hat die Fehler in der Vision-Software behoben und dazu im Februar 2018 entsprechende Softwareupdates veröffentlicht. Die vom Angriff betroffenen Hotels sollten diese Sicherheitsupdates so schnell wie möglich einspielen, wobei wir nicht genau wissen, wie viele dies bereits getan haben. Die Hotels, die die Updates in ihre Systeme eingespielt haben, sind nicht mehr für den Angriff anfällig.

Weitere Informationen zum Bugfix finden Sie hier:
https://assaabloyhospitality.service-now.com/user_registration_request.do?sys_id=-1&sysparm_view=ess

WELCHE HOTELS SIND BETROFFEN?

Alle Hotels, die Assa Abloys weit verbreitetes Vision-Softwaresystem verwenden, sind von dem Angriff betroffen. Die Vision-Software wird von unabhängigen Hotels und örtlichen Hotelketten sowie einigen bekannten, internationalen Unternehmen verwendet.

Die Referenzen von Assa Abloys Hospitality finden Sie hier:
https://www.assaabloyhospitality.com/en/aah/com/case-studies/case-studies-and-references/

Assa Abloy hat auch andere Softwaresysteme in der Hotelbranche, die jedoch nicht betroffen sind.

WARUM HAT F-SECURE DIESE UNTERSUCHUNG DURCHGEFÜHRT?

Das Interesse unserer Forscher an Hotelschlössern wurde vor rund 15 Jahren geweckt, als der Laptop eines unserer Sicherheitsexperten aus einem verschlossenen Hotelzimmer gestohlen wurde. Es gab keinen Hinweis auf unbefugten Zutritt ins Hotelzimmer oder in den Zugangsprotokollen für die Räume, so dass die Hotelmitarbeiter die Beschwerde zum Diebstahl des Laptops ablehnten. Unsere Experten stellten sich dann die Frage, ob es eventuell möglich ist, durch Manipulation des Schließsystems in ein Hotelzimmer einzubrechen, ohne Spuren zu hinterlassen - auch keine digitalen.

WARUM MACHEN SIE DIESE EXPLOITS ÖFFENTLICH? WERDEN DIESE FÜR JEDERMANN ZUGÄNGLICH GEMACHT?

Die Analyse von Exploits ist unerlässlich, um Produkte zu verbessern und somit die Sicherheit für alle zu verbessern - der Ansatz “Security through Obscurity” funktioniert in diesem Zusammenhang nicht. Wir haben es uns zur Aufgabe gemacht, Sicherheitsprobleme mit einen koordinierten und konstruktiven Ansatz anzugehen und öffentlich zu machen. Dabei wollen wir das Bedürfnis der Öffentlichkeit, über Sicherheitsfragen informiert zu werden, mit dem Bedürfnis von Produktanbietern in Einklang bringen, genug Zeit für die Behebung dieser Probleme zu haben.

WARUM HAT DIE FORSCHUNG MEHR ALS EIN JAHRZEHNT LANG GEDAUERT?

Die Komplexität der Funktionsweise der Schließanlagen, der Software und der Schlüssel ist sehr hoch. Ein elektronisches Zutrittskontrollsystem zu bauen und zu hacken ist sehr schwierig, weil es dabei viele Facetten zu beachten gibt. Assa Abloy ist ein renommierter Hersteller von Schlössern und abgesehen von den anfangs scheinbar harmlosen Sicherheitslücken in der Software, sind die Produkte insgesamt sehr gut konzipiert.

Die entdeckten Sicherheitslücken waren dabei keineswegs offensichtlich. Es bedurfte eines gründlichen Verständnisses des gesamten Systemdesigns, um selbst kleine Fehler ausfindig zu machen. Unsere Experten haben diese Fehler dann kreativ kombiniert, um den Angriff auf das System zu simulieren.

WURDEN DIESE KONSTRUKTIONSFEHLER JEMALS IN DER “FREIEN WILDBAHN” AUSGENUTZT?

Derzeit liegen uns keine Berichte über Vorfälle vor, bei denen Vingcard-Schlösser von Assa Abloy gehackt wurden und uns ist nicht bekannt, ob die von uns gefundenen Schwachstellen in der Realität ausgenutzt worden sind. Aber natürlich können wir nicht mit hundertprozentiger Sicherheit sagen, dass ein solcher Fall nicht eingetreten ist.

SIND HOTELGÄSTE NUN GEFÄHRDET?

Ehrlich gesagt, gibt es einfachere Wege in ein Hotelzimmer einzudringen. Darüber hinaus werden die Details der Angriffsmethode nicht bekannt gegeben und die Software-Tools werden nicht von uns zur Verfügung gestellt. Hinzu kommt, dass Kriminelle, die in Hotelzimmer einbrechen wollen, indem sie sich auf diese Art und Weise in das Schließsystem hacken, tiefgreifendes technisches Wissen und erheblichen Zeitaufwand mitbringen müssen, wie unsere eigene Arbeit gezeigt hat. Man sollte jedoch nicht davon ausgehen, dass niemand außer uns die gleichen Schwachstellen gefunden hat wie wir, weshalb wir das Einspielen des Softwareupdates dringend empfehlen.