Can We Trust Smart Things?

Dmitri Vellikok
Senior Principal Consultant

F-Secure
CAN WE TRUST SMART THINGS?

@dmitrivellikok
SMART = VULNERABLE

Mikko Hyppönen’s Law
Chief Research Officer, F-Secure
One Card to rule them all
READ ANY CURRENT OR EXPIRED KEY
ELEVATE TO FACILITY MASTER KEY
BECOME A GHOST
IMPACT

source: https://www.assaabloyhospitality.com/
Case Studies and References from Hospitality Providers

ASSA ABLOY Hospitality has provided solutions to a range of Hotels and Hospitality providers worldwide. Click on any of the Hotel Logos below to see how our solutions and products have changed the way hotels interact with their customers.
• Bypass the electronic lock
Assassination of Mahmoud Al-Mabhouh

The assassination of Mahmoud Al-Mabhouh (Arabic: مصطفى المبحوح, Mahmoud al-Mabhouh; 14 February 1961 – 19 January 2010) was an assassination that took place on 19 January 2010, in a hotel room in Dubai, United Arab Emirates. Al-Mabhouh—a co-founder of the Izz ad-Din al-Qassam Brigades, the military wing of Hamas—was shot dead by two masked men.

A readout of activity that took place on the hotel room's electronic door lock indicated that an attempt was made to reprogram Al-Mabhouh's electronic door lock at this time. The investigators believe that the electronic lock on Al-Mabhouh's door may have been reprogrammed and that the killers gained entry to his room this way. The locks in question, VingCard Locklink brand, can be accessed and reprogrammed directly at the hotel room door.

According to initial reports, Al-Mabhouh was drugged, then electrocuted and suffocated. Lt. Gen. Dhahi Khalfan Tamim of the Dubai Police Force said the suspects tracked Al-Mabhouh to Dubai from Damascus, Syria. They arrived from different European destinations and stayed at different hotels, presumably to avoid being detected and, with the exception of three of his members suspected of "helping to facilitate" who had left on a ferry for Iran several months before the assassination, departed after the assassination to different countries. Dubai's police chief said that he was "99% certain" that the assassination was the work of Israel's Mossad. On 1 March 2010, he stated that he was "sure" that all of the suspects are hiding in Israel. He said that Dubai would ask for an arrest warrant to be issued for Meir Dagan, the head of Mossad, if it is confirmed that the Mossad is involved and responsible for the assassination. The Hamas leadership also holds Israel responsible, and has vowed revenge.
- Clone an access token
- Produce an access token with more privileges
- Produce an access token with all privileges
1. General description

NXP Semiconductors developed the contactless smart ticket, smart card in combination with a Proximity Coupling Device (PCD). The MF0ULx1 is designed for use in public transportation networks, serving as a replacement for conventional ticketing solutions such as paper tickets, magnetic stripe tickets or coins.

The MIFARE Ultralight EV1 is suitable for functional backwards compatible, efficient implementations and offers the mechanical and electrical specifications that meet the requirements of inlay and card vendors.

1.1 Contactless energy and data transfer

In a contactless system, the MF0ULx1 fits the TFC.0 (Edmondson Ref. 8).

The MF0ULx1 chip, which is available supports both TFC.1 and TFC.0 ticket formats.

1.2 Anticollision

An intelligent anticollision function is provided to prevent the execution of a transaction with interference from another card in the same vicinity.

As the usage of contactless proximity smart cards becomes more and more common, transport and event operators are switching to completely contactless solutions. The introduction of the MIFARE Ultralight for limited use tickets may lead to a reduction of system installation and maintenance costs. Terminals may be less vulnerable to damage and mechanical failures caused by ticket jams. MF0ICU1 can easily be integrated into existing schemes and even standard paper ticket vending equipment can be upgraded.

This solution for low cost tickets can help operators to reduce the circulation of cash within the system.

The mechanical and electronic specifications of MIFARE Ultralight are tailored to meet the requirements of paper ticket manufacturers.

1.1 Contactless energy and data transfer

In the MIFARE system, the MF0ICU1 is connected to a coil with a few turns. The MF0ICU11 chip supports the TFC.0 (Edmondson) and TFC.1 (ISO) ticket formats as defined in ISO 14443 A.
Sometimes, hacking is just someone spending more time on something than anyone else might reasonably expect.
DNS REBIND ATTACK

<table>
<thead>
<tr>
<th>Vulnerable device manufacturers¹</th>
<th>Representative manufacturers</th>
<th>Estimated number of vulnerable devices, worldwide²</th>
</tr>
</thead>
<tbody>
<tr>
<td>87% of switches, routers, and access points</td>
<td>Aruba, Avaya, Cisco, Dell, Extreme, Netgear</td>
<td>14 million</td>
</tr>
<tr>
<td>78% of streaming media players/speakers</td>
<td>Apple, Google, Roku, Sonos</td>
<td>5.1 million</td>
</tr>
<tr>
<td>77% of IP phones</td>
<td>Avaya, Cisco, NEC, Polycom</td>
<td>124 million</td>
</tr>
<tr>
<td>75% of IP cameras</td>
<td>Axis Communications, GoPro, Sony, VivoteK</td>
<td>160 million</td>
</tr>
<tr>
<td>66% of printers</td>
<td>Hewlett Packard, Epson, Konica, Lexmark, Xerox</td>
<td>165 million</td>
</tr>
<tr>
<td>57% of smart TVs</td>
<td>Roku-integrated, Samsung, Vizio</td>
<td>28.1 million</td>
</tr>
</tbody>
</table>

¹ Based on data from Armis, Inc., 2018.
² Based on estimated market share and device vendor data.
GARTNER: THE THREE MAIN SECURITY ISSUES WITH CONNECTED HOME DEVICES

LACK OF SECURITY STANDARDS

SECURITY IMPLEMENTATION IS OFTEN JUST AN AFTERTHOUGHT

SLOW REPLACEMENT

THREAT ACTORS

**CYBER CRIMINALS**
They want to steal money. Doesn’t matter from whom.

**HACKTIVISTS**
They have a political or ideological agenda, and want publicity.

**STATE ACTORS**
They create Malware. Mass collection of user data.
“No one shall be subjected to arbitrary interference with their privacy, family, home, or correspondence.”

The Universal Declaration of Human Rights
1948
THE RISE OF SURVEILLANCE CAPITALISM
CONSUMERS FEELING HELPLESS

68% CONCERNED about security & privacy

48% POSTPONING purchasing of IoT devices

43% of respondents aged 18 to 34 are fearful that smart devices know too much about them

Source: F-Secure consumer survey 2018, n= 5000

Putting the Human First in The Future Home, Accenture / The Dock, 2019
OK, SO WHAT NOW?
THE 5 RULES

1. No updates = no Internet
2. Force default password change
3. Patch
4. Bug bounty
5. Only collect and process RELEVANT data
AI DRIVEN 3-LAYER CYBER SECURITY

- Network Security
- Router Security
- Endpoint Protection

Man and Machine
OPERATORS SIMPLIFYING
WHOLE HOME EXPERIENCE
PROTECTION EVERYWHERE. SIMPLIFIED.

F-Secure
Can We Trust Smart Things?

Dmitri Vellikok
Senior Principal Consultant

F-Secure.

broadband forum
June 2-4, 2020
Den Haag, The Netherlands

The date has been set!

An event by tech innovators for tech leaders!

Powered by:

BASe
broadband forum
TNO
Thank you

Learn more about the Broadband Forum at:
http://www.broadband-forum.org/

Interested in joining? Contact membership development leader Rhonda Heier at:
rheier@broadband-forum.org