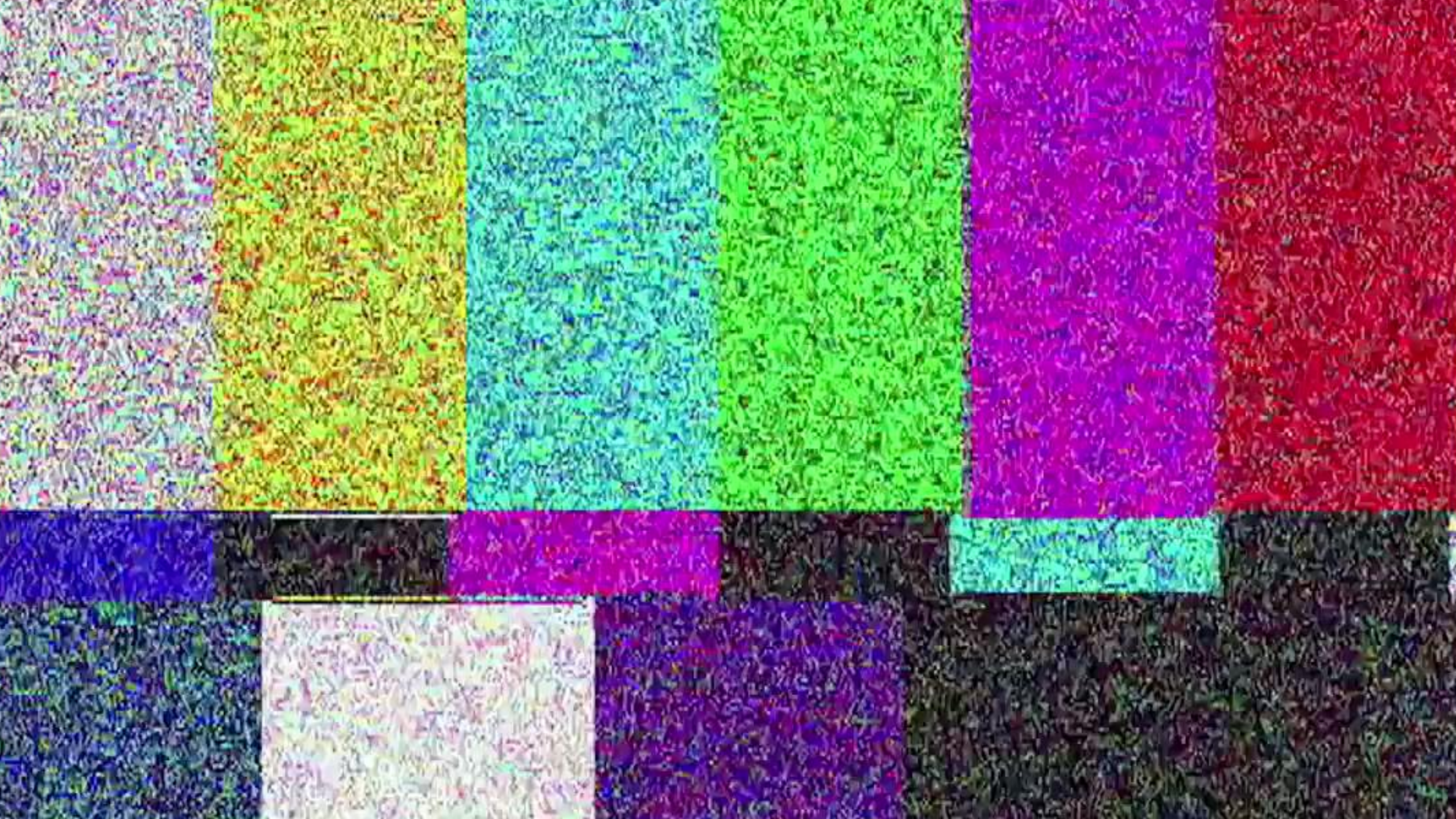
CAN WE TRUST SMART THINGS?

Tom Gaffney
@gaffto

F-Secure

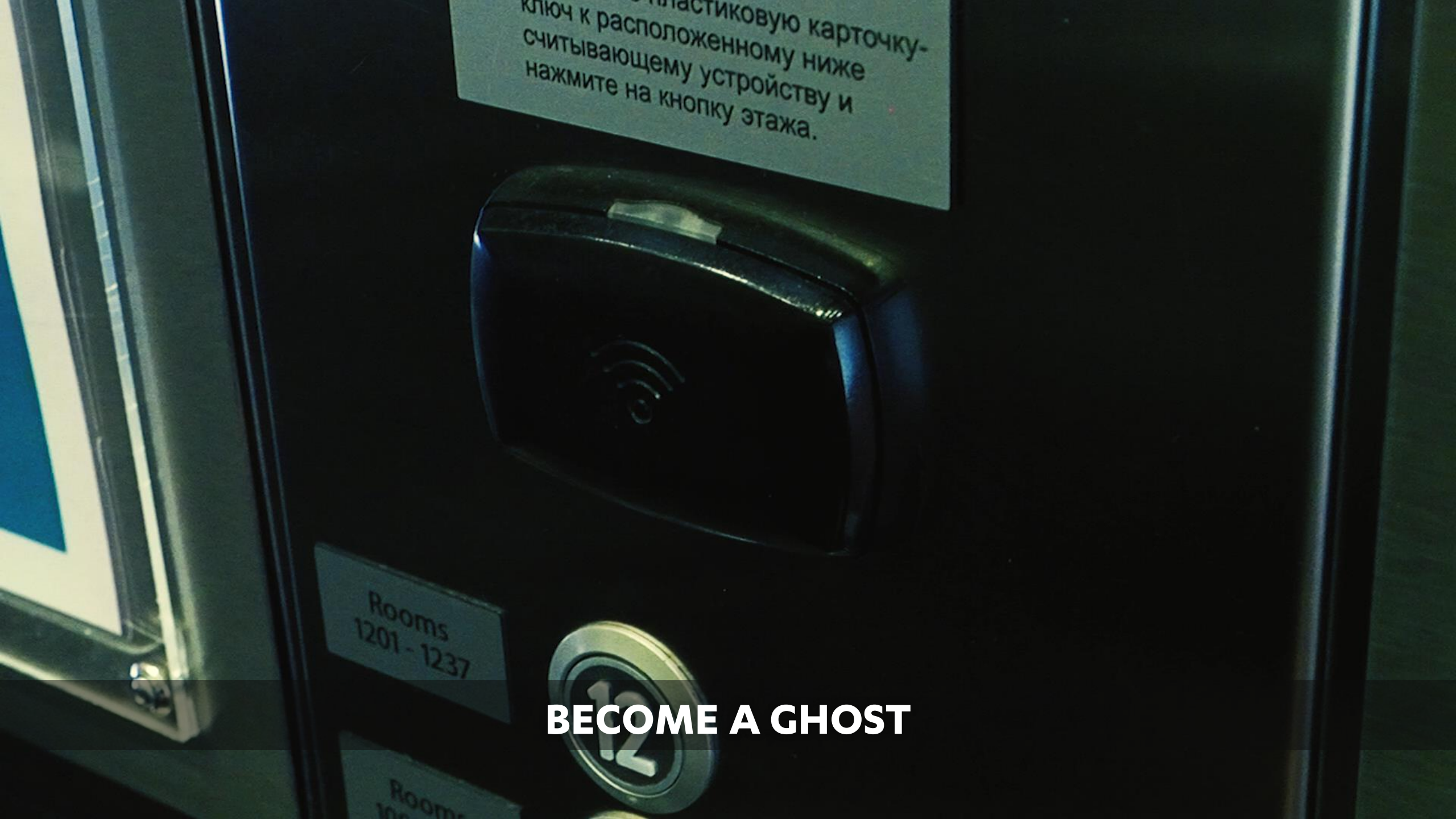

SMART = VULNERABLE
TED
Talks
Mikko Hyppönen's Law
Chief Research Officer, F-Secure




One Card to rule them all
VingCard

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.

InterContinental Toronto Centre

Renaissance Toronto Downtown Hotel

Radisson RED

ULTRA Hotel


Holland America Line


SEA LAUNCH COMMANDER
SEA LAUNCH


COSTA FORTUNA


Carmel
AGREXCO


NCL
NORWEGIAN STAR


StarVirgo

vision
by VingCard®

- Bypass the electronic lock

Assassination of Mahmoud Al-Mabhouh

From Wikipedia, the free encyclopedia

The **assassination of Mahmoud Al-Mabhouh** (Arabic: محمود المبحوح, *Maḥmūd al-Mabḥūḥ*; 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

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.[*citation needed*] 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.[41] The locks in question, VingCard Locklink brand,[42] can be accessed and reprogrammed directly at the hotel room door.

Assassination of Mahmoud Al-Mabhouh

Target	Mahmoud al-Mabhouh
Attack type	Assassination
Weapons	Pillow, muscle relaxant
Deaths	1
Perpetrators	33 people, using forged and fraudulently obtained passports
Suspected perpetrator	Mossad

According to initial reports, Al-Mabhouh was drugged,[9] then electrocuted and suffocated.[5] 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 its 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.[2][5] 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.[10][11] 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.[12] The Hamas leadership also holds Israel responsible, and has vowed revenge.[13] Hamas, which is itself on the US and EU lists of terrorist organizations (and also considered a terrorist organization by the governments of Israel,[14] and Japan,[15] as is its military arm by the United Kingdom[16] and Australia[17]), requested that Israel be added by the EU to its list because of suspicions that Israel was involved in the assassination.[18] However, later in March, Dubai police chief said, "I am now completely sure that it was Mossad", and went on to say "I have presented

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export

- Clone an access token
- Produce an access token with more privileges
- Produce an access token with all privileges

INTERNATIONAL STANDARD **ISO/IEC 14443-2**

Identification integrated cir cards —

Part 2:
Radio freque

Cartes d'identification Cartes de proximité —

Partie 2: Puissance d

INTERNATIONAL STANDARD **ISO/IEC 14443-3**

Identification integrated circ cards —

Part 3:
Initialization a

Cartes d'identification – Cartes de proximité —

Partie 3: Initialisation et

MF0ULx1

MIFARE Ultralight EV1 - Contactless ticket IC

Rev. 3.1 — 30 June 2014
234531

Product data sheet
COMPANY PUBLIC

1. General description

NXP Semiconductors developed t
contactless smart ticket, smart can
Device (PCD). The MF0ULx1 is de
environment (see Ref. 1). The targ
in public transportation networks, l
serves as a replacement for conve
magnetic stripe tickets or coins. It i
card families such as MIFARE DE

The MIFARE Ultralight EV1 is succ
functional backwards compatible. I
efficient implementations and offer

The mechanical and electrical spe
meet the requirements of inlay and

1.1 Contactless energy and da

In a contactless system, the MF0U
MF0ULx1 fits the TFC.0 (Edmond
Ref. 8.

The MF0ULx1 chip, which is availa
supports both TFC.1 and TFC.0 tic

1.2 Anticollision

An intelligent anticollision function
simultaneously. The anticollision al
the execution of a transaction with
interference from another card in t

MF0ICU1

MIFARE Ultralight contactless single-ticket IC

Rev. 3.9 — 23 July 2014
028639

Product data sheet
COMPANY PUBLIC

1. General description

The MIFARE MF0ICU1 has been developed by NXP Semiconductors to be used in a contactless smart ticket or smart card in combination with a Proximity Coupling Devices (PCD) in accordance with ISO/IEC 14443 A (see Ref. 1). It is intended for use as single trip or limited use tickets in public transportation networks, loyalty cards or day passes for events as a replacement for conventional ticketing solutions such as paper tickets, magnetic stripe tickets or coins.

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 electronical 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 MF0ICU1 fits the TFC.0 (Edmondson) and TFC.1 (ISO) ticket formats as defined in BS

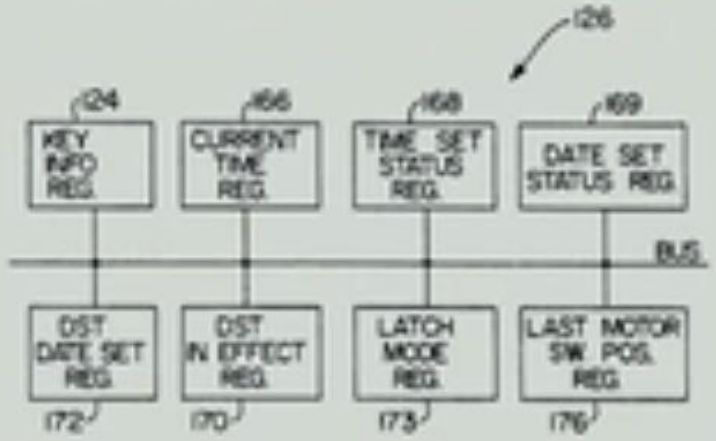


FIG. 5

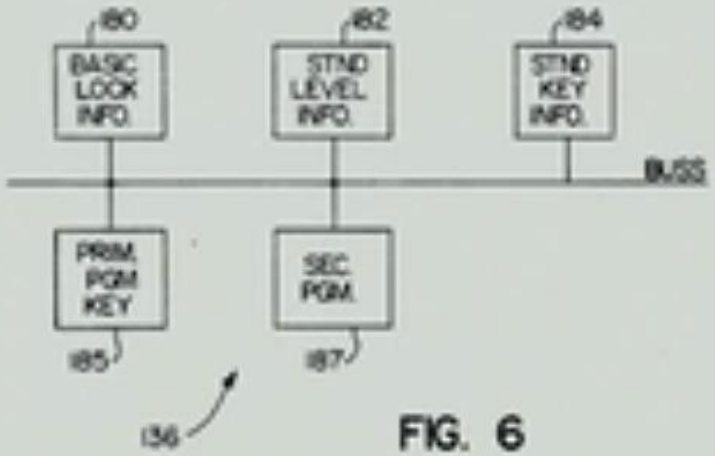


FIG. 6

FIG. 7

- LEVEL CODE
- KEY TYPE
- PROP. NUMBER
- KEY REC. #
- NEW KEY D/T
- EXP DATE OFFS.
- EXP TIME
- DUPL. KEY I.D.
- SEQ # /COMBIN.
- INVALID DAYS
- PASS AUTHOR #
- OPEN/NON-OP
- OVERRIDE DEADBLT

138

United States Patent [19]
Mims et al.

[11] Patent Number: 5,198,643
[45] Date of Patent: Mar. 30, 1993

[54] ADAPTABLE ELECTRONIC KEY AND LOCK SYSTEM

[75] Inventors: Nancy C. Mims, Royal Oak; Vance E. Neff, Birmingham, both of Mich.
[73] Assignee: Computerized Security Systems, Inc., Troy, Mich.

[21] Appl. No.: 661,302
[22] Filed: Feb. 26, 1991
[51] Int. Cl.[5] E05B 47/00
[52] U.S. Cl. 235/382; 235/382.5
[58] Field of Search 235/382, 382.5, 380

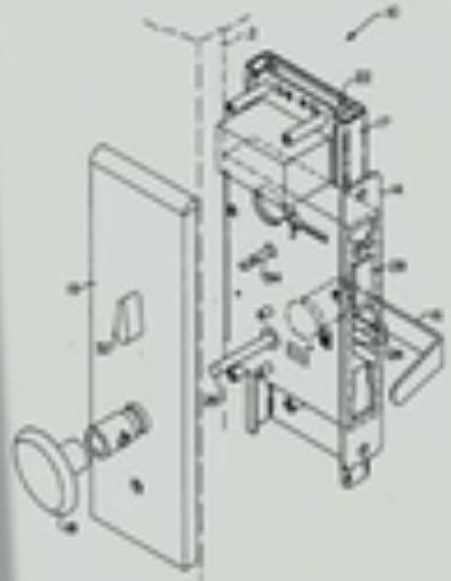
[56] References Cited
U.S. PATENT DOCUMENTS
1. Dowell et al. 235/382.5
2. Gasser et al. 235/382.5
3. Germanowski 235/382
4. Roland et al. 235/382
5. Gasser 235/382
6. Steckinger et al. 235/382
7. Raymond et al. 235/492
8. Couch et al. 235/382
9. Clarkson et al. 235/382
10. Rollins 235/382.5
11. Downs et al. 235/382

Attorney, Agent, or Firm—Rohm, Ellington, Bernard, Perry & Milton

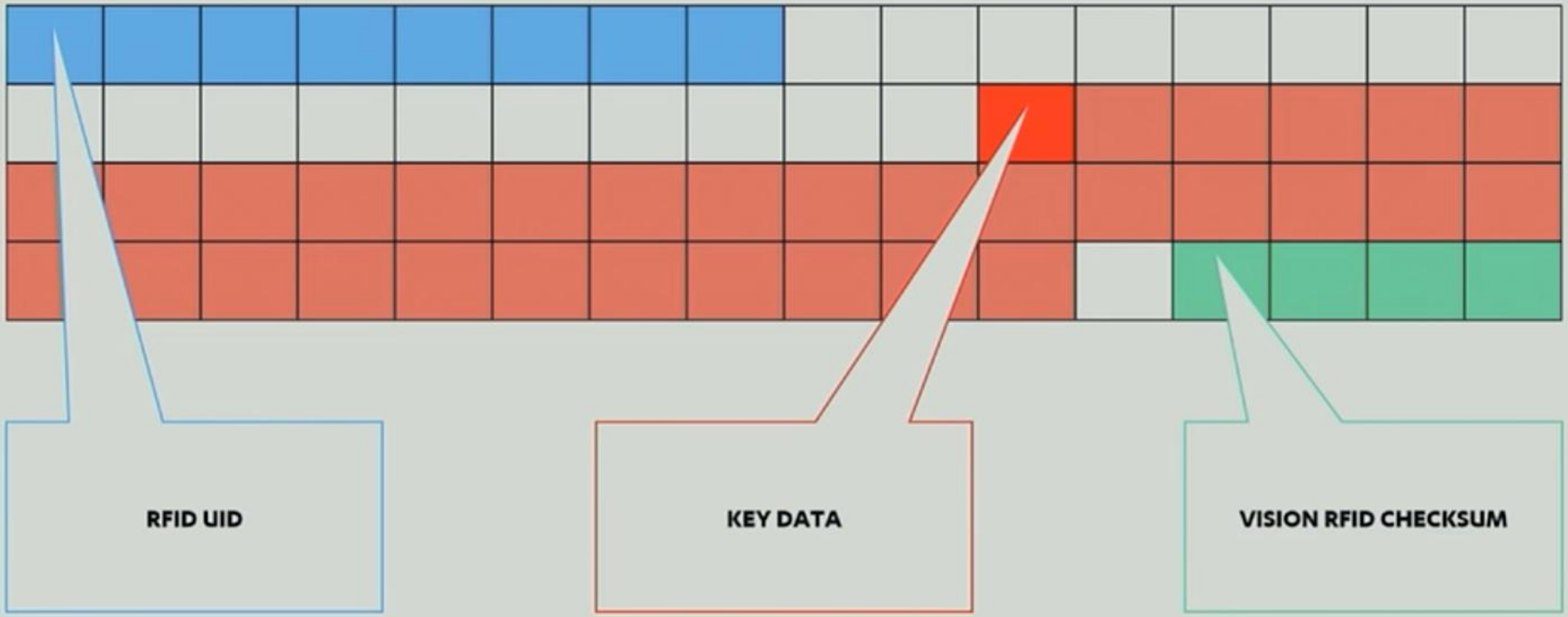
[57] ABSTRACT

A locking system is utilized to control the locking and unlocking of a lock, such as on a door. The lock includes a magnetic card reader for reading a coded key card into a lock computer which in turn determines functions of and access to the lock. The key card includes a key code, key level code, and key record number stored thereon. The lock includes a memory accessed by the computer which is partitioned and includes a level storage area with level records identified by a lock level code and operational information for the level, and a key storage area for storing lock key records identified by a lock record number and associated with at least one lock level for storing key information associated with the record number. The computer validates a key card by reading and comparing the key level code to the lock level code to determine the level and the key record number to one of the lock record numbers identified with the level in the key storage area. The key code is representative of a real time based on time of issuance, and validation occurs by comparing a lock time to the key code. Additional functions include group pass codes, batch processing, and automatic unlatching times.

20 Claims, 10 Drawing Sheets



KEY DATA ILLUSTRATED V2



BRUTEFORCING 1/SECOND

4 bits	8 bits	12 bits	16 bits
16 seconds	**4 minutes**	**1 hour**	**18 hours**

BRUTEFORCING 1/SECOND

20 bits	24 bits	28 bits	32 bits
12 days	**6 months**	**8 years**	**138 years**

Jerry Gamblin

@JGamblin

Seuraa

Sometimes, hacking is just someone spending more time on something than anyone else might reasonably expect.

16.04 - 25. maalisk. 2017

773 uudelleentwiittausta **1 556** tykkäystä

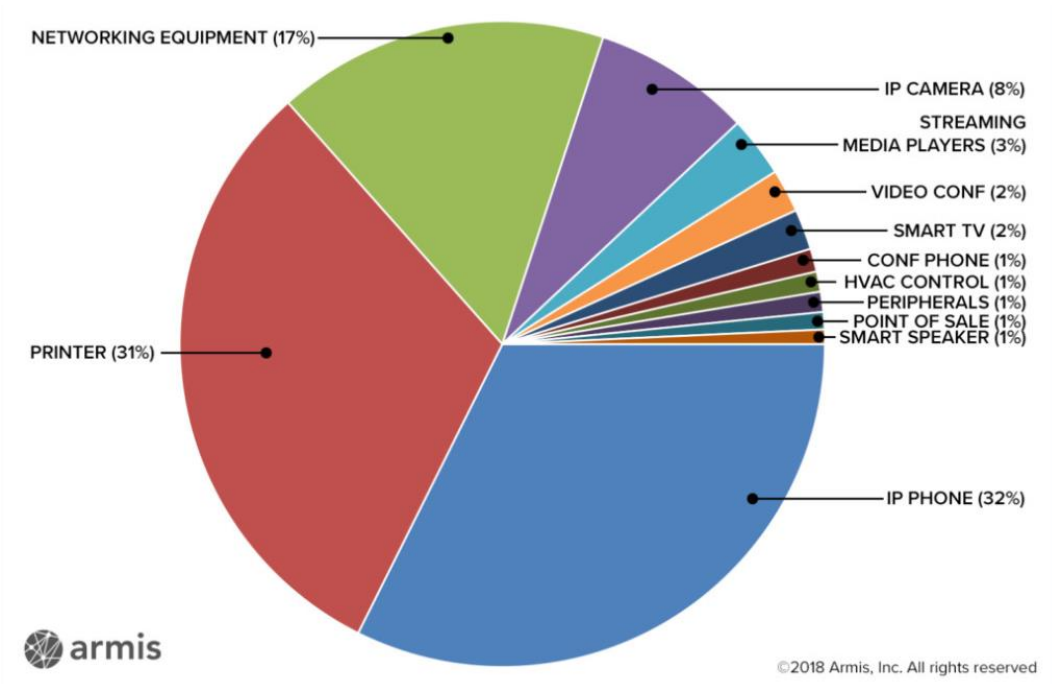
25 773 1,6 t.


Prykarpattyaoblenergo
22
21

F-Secure.

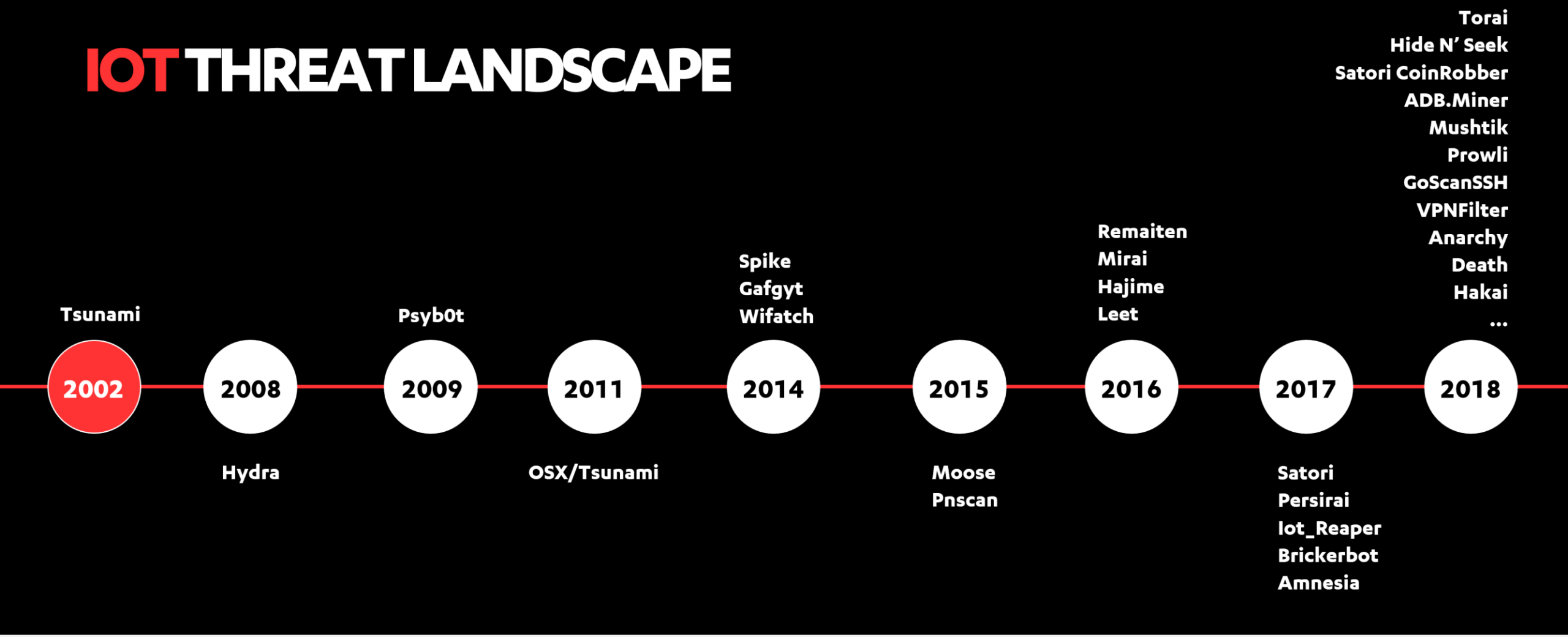
DNS REBIND ATTACK

Vulnerable device manufacturers[1]	Representative manufacturers	Estimated number of vulnerable devices, worldwide[2]
87% of switches, routers, and access points	Aruba Avaya Cisco Dell Extreme Netgear	14 million
78% of streaming media players/speakers	Apple Google Roku Sonos	5.1 million
77% of IP phones	Avaya Cisco NEC Polycom	124 million
75% of IP cameras	Axis Communications GoPro Sony Vivotek	160 million
66% of printers	Hewlett Packard Epson Konica Lexmark Xerox	165 million
57% of smart TVs	Roku-integrated Samsung Vizio	28.1 million



F-Secure

IOT THREAT LANDSCAPE



F-Secure.

GARTNER: THE THREE MAIN SECURITY ISSUES WITH CONNECTED HOME DEVICES

LACK OF SECURITY **STANDARDS**

SECURITY IMPLE-MENTATION IS OFTEN JUST AN **AFTERTHOUGHT**

SLOW **REPLACEMENT**

Source: Gartner Inc., Market Insight: Address 3 Critical Security Issues to Differentiate Yourself in the Connected Home Market, Annette Zimmermann, Saniye Alaybeyi, 26 April 2018. Charts/graphics created by F-Secure based on Gartner research.

F-Secure

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

F-Secure.

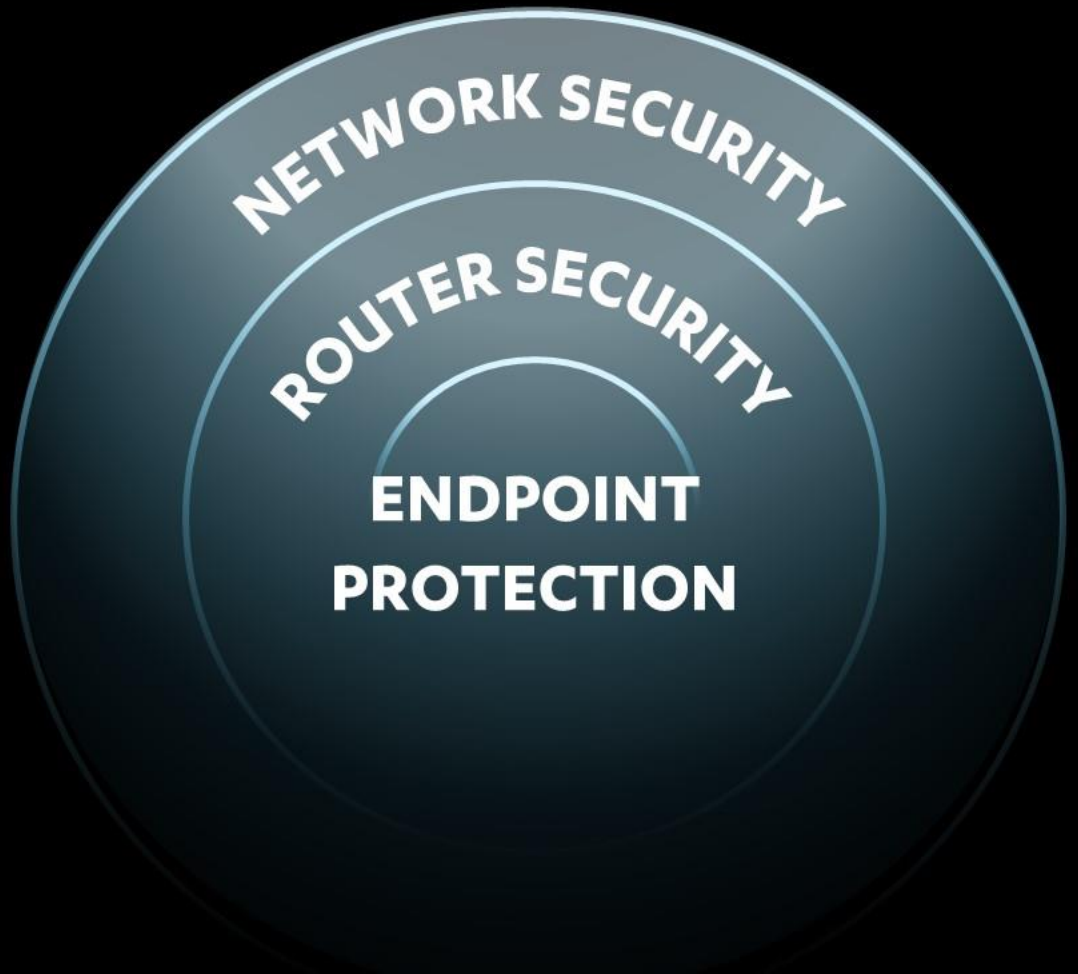
OK, SO WHAT NOW?

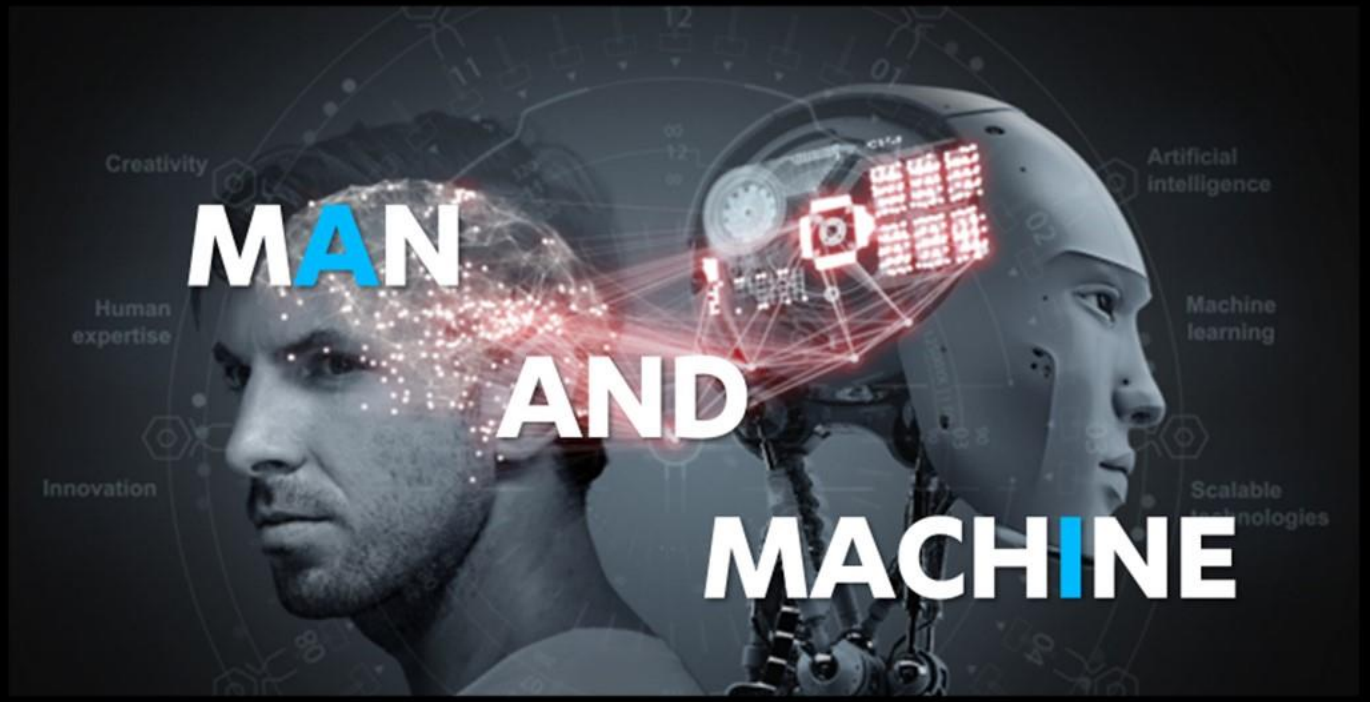
F-Secure.

THE 5 RULES

1. No updates = no Internet
2. Force default password change
3. Patch
4. Bug bounty
5. Map your attack surface

AI DRIVEN 3-LAYER CYBER SECURITY





F-Secure.

PROTECTION EVERYWHERE. SIMPLIFIED.