# Hardware security in the payment industry

cEDM event

08-12-2017

an atos company

worldline
e-payment services

# Agenda

1 Worldline in a nutshell

2 Payment Card Industry

3 Attacks and how to protect

4 Security in IoT

5 Conclusion

# 1 Worldline in a nutshell

# ATOS

# our parent company

# Our mission: Empowering the cashless society

Processor of *e-Payment services*

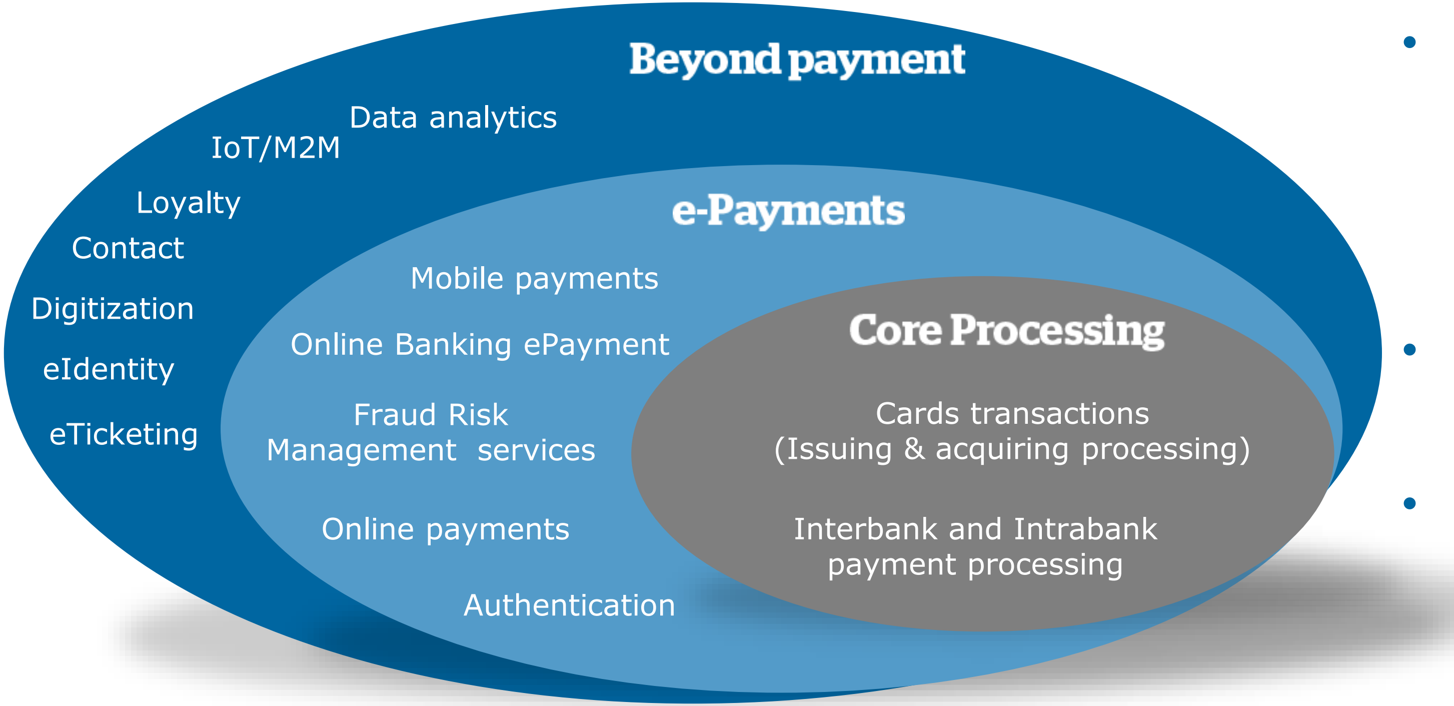
Provider of end-to-end *digital B2C and B2B transactional services*

**Merchant Services**
c. 186,000 merchants

**Financial Services**
c. 250 banks

**Mobility & e-Transactional Services**
c. 350 customers on various industries

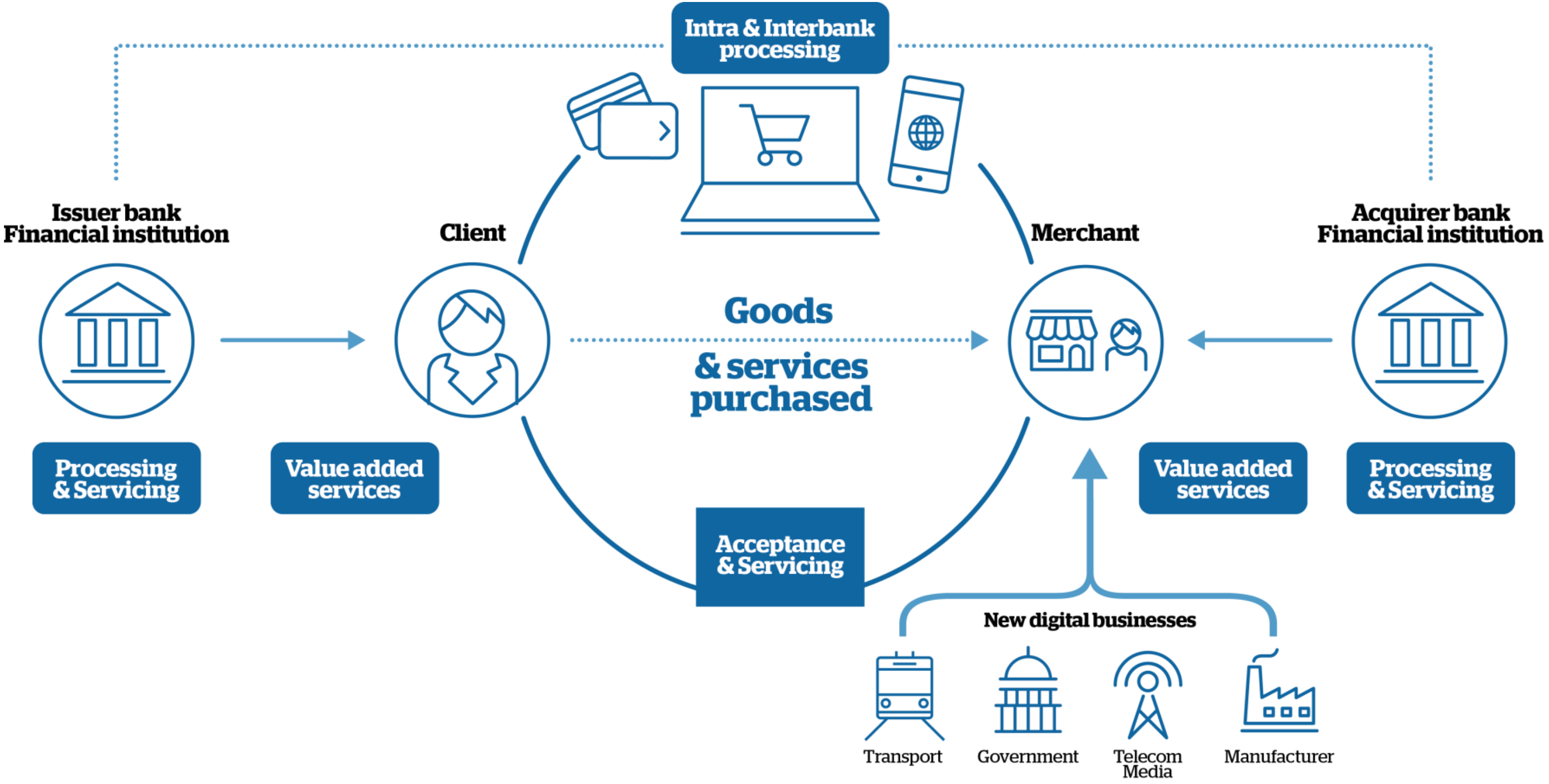
# Technology as a key differentiator



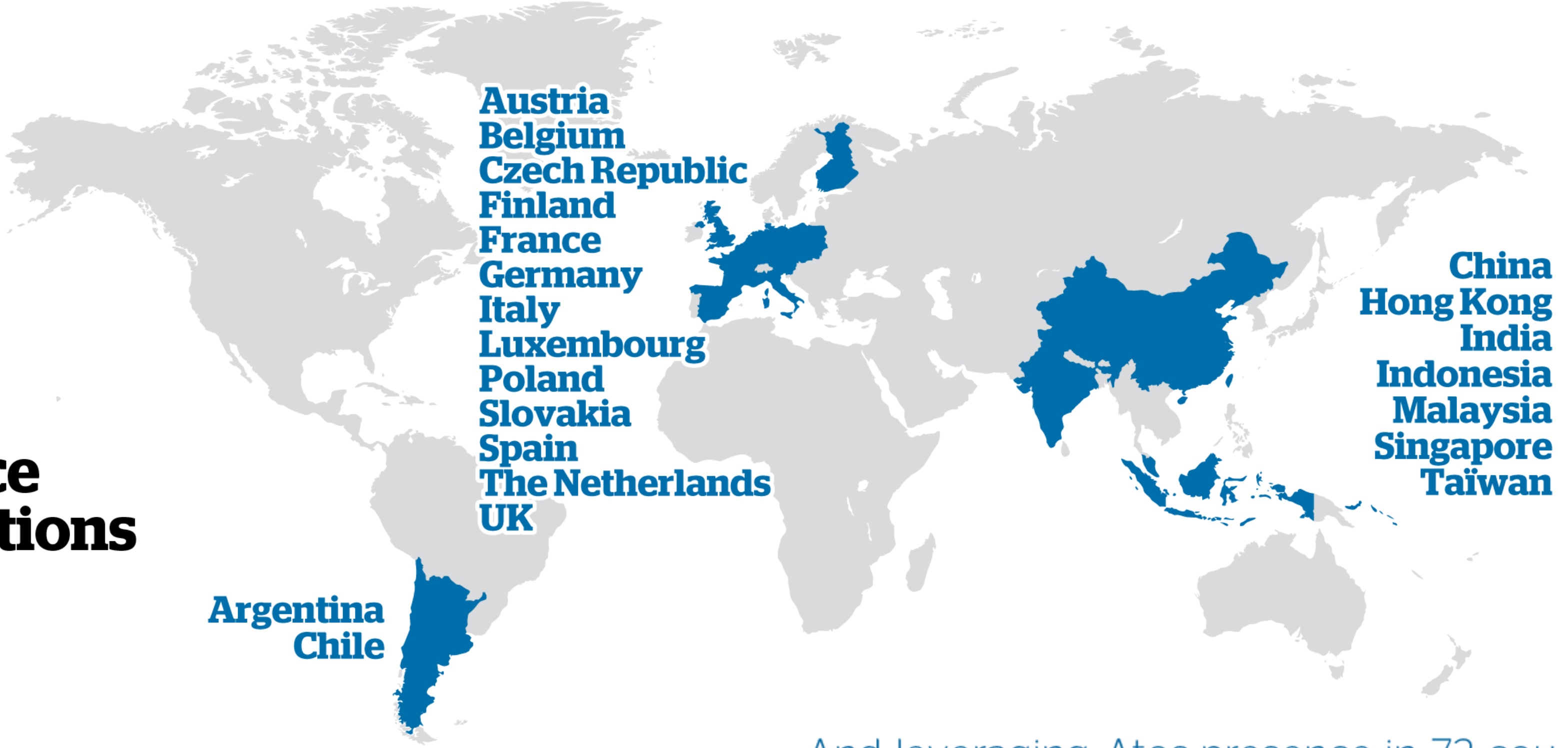
## One global factory

- Supported by **EU hub (with 5 major DC)** interconnected with **Latam hub (1 DC)** and **Asia hub (3 DC)** for synchronization & monitoring
- **c. 16,720 servers** with a capacity of **c.11.3PB of data**
- European hub processes **c.1,000 payment transactions per second**

# We are covering the whole Payment value chain



# Our international footprint



**Office locations**

And leveraging Atos presence in 72 countries

# Terminals Services for Merchants

A Secure Digital "Point Of Interaction" between merchant and consumer

## Next generation Android-based terminals

**VALINA** Unattended '17

**NEW** Countertop '18-19

Customer Survey
Advertising
Coupons
Loyalty
Customer
Business apps

**Business benefits**

- *New services* for merchants
- *More* customer *intimacy*
- *New interactions*

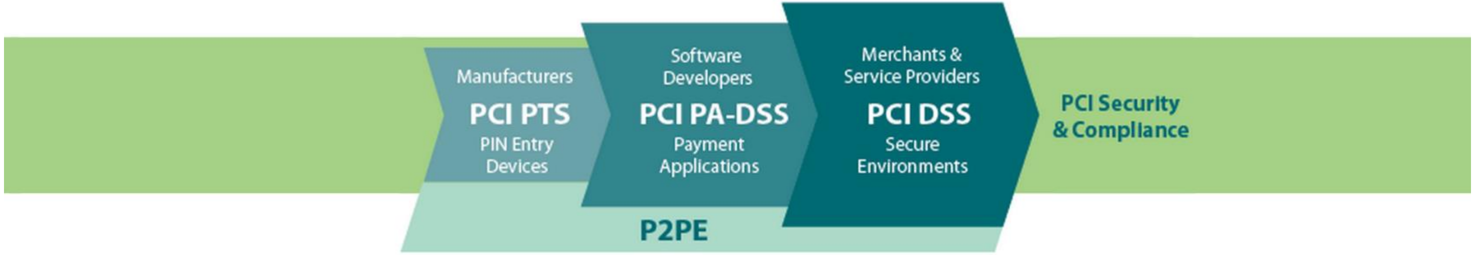
| Increase value for Merchant | Verticalisation of offering | Increase Merchant engagement | Value client data | Drive additional service revenues |
|---|---|---|---|---|

# 2 Payment Card Industry

# PCI SSC
## Payment Card Industry Security Standards Council

PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data



Manufacturers
**PCI PTS**
PIN Entry Devices

Software Developers
**PCI PA-DSS**
Payment Applications

Merchants & Service Providers
**PCI DSS**
Secure Environments

**P2PE**

PCI Security & Compliance

Ecosystem of payment devices, applications, infrastructure and users

**PARTICIPATING ORGANIZATIONS**

Merchants, Banks, Processors, Hardware and Software Developers and Point-of-Sale Vendors

**PCI SSC FOUNDERS**

AMERICAN EXPRESS

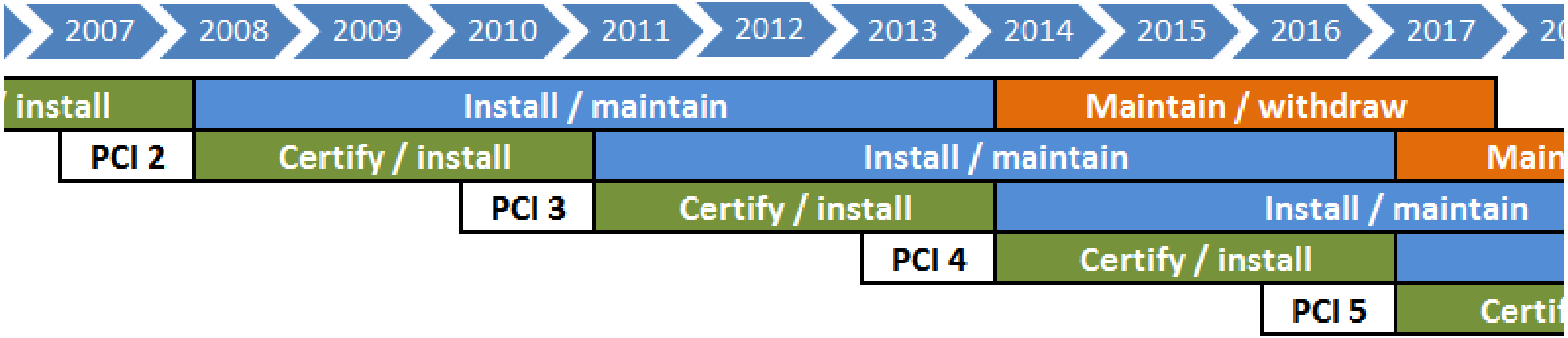
DISCOVER

JCB

MasterCard Worldwide

VISA

# PCI PTS program management
## Standard Release and Terminal Validation



2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 20

/ install | Install / maintain | Maintain / withdraw

PCI 2 | Certify / install | Install / maintain | Main

PCI 3 | Certify / install | Install / maintain

PCI 4 | Certify / install

PCI 5 | Certif

See https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices for list of approved terminals

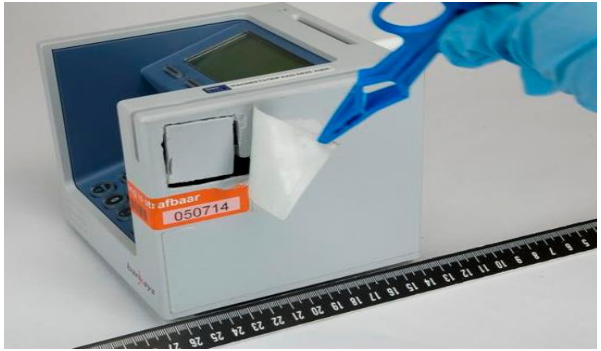
# What to protect

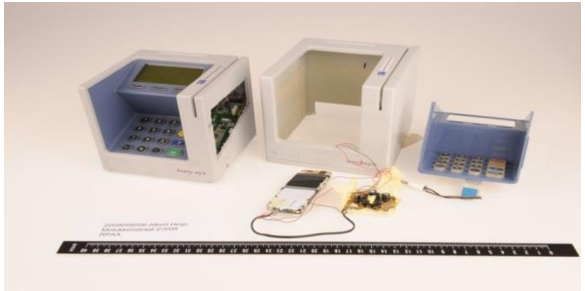
- Cryptographic keys
- Card data
- PIN code
- Communication

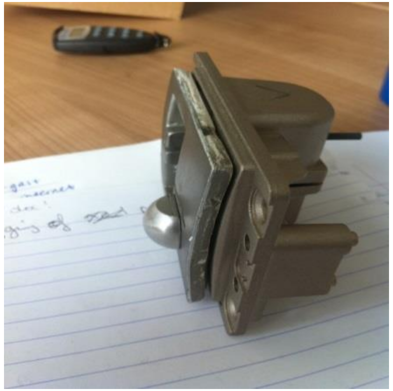
# 3 Attacks and how to protect

# Fraud & Skimming

## Skimming: capture PIN and card data

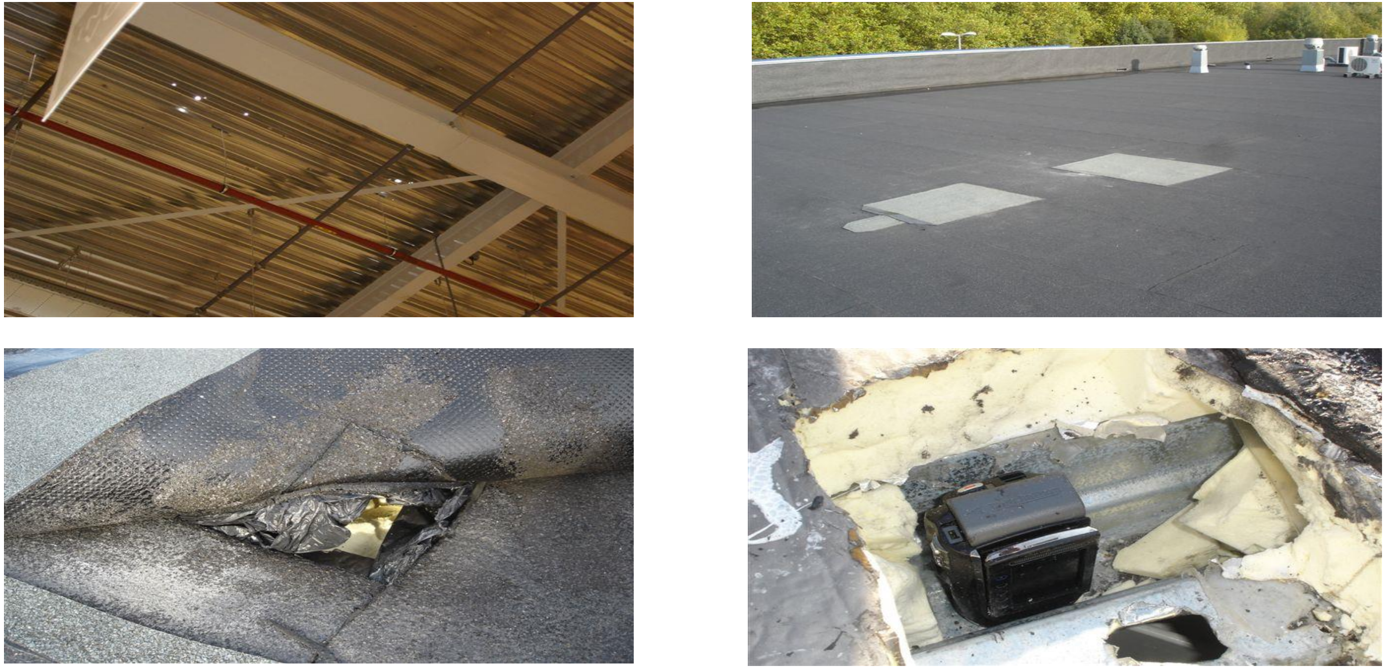






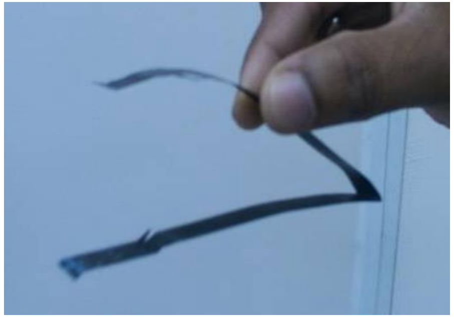
# Fraud & Skimming

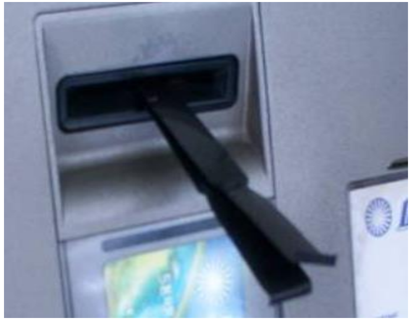
## Skimming: capture PIN and card data



# Fraud & Skimming

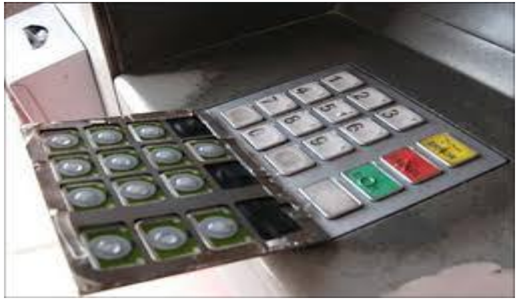
## Lebanse Loop

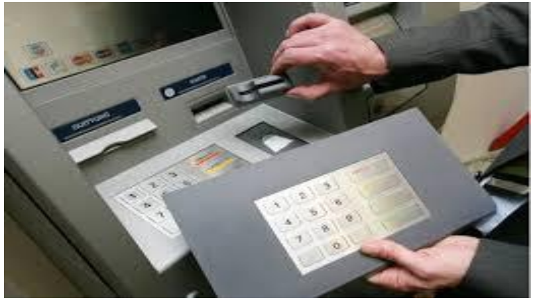




# Fraud & Skimming

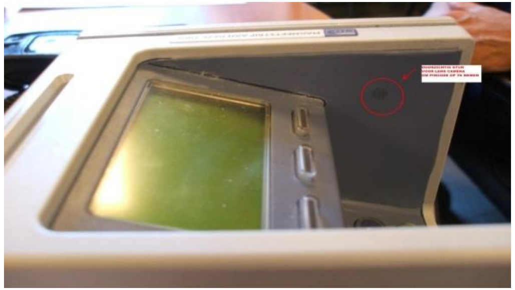
Keyboard overlay

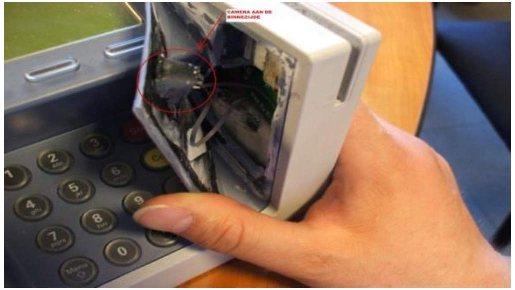




# Fraud & Skimming

## Mini camera





# Hacking

## Buffer Overflow vulnerability found in German Credit card terminals

by Sabari Selvan on Tuesday, July 17, 2012 |

Like 15 G+1 0 Tweet 0 Share 0 StumbleUpon 0 Reddit 0

Security Researchers from Security Research Labs (SRLabs), have discovered Buffer Overflow vulnerability in the Germany's Hypercom Artema Hybrid

take control of the device.

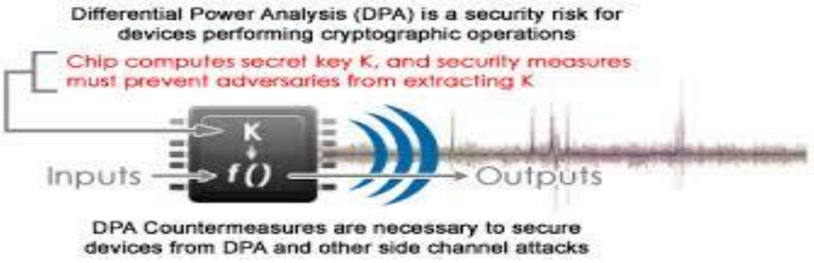
The vulnerability is critical because it doesn't require an

easily exploit the vulnerability via TCP/IP connection .

# Side channel attacks

General classes of side channel attack include:

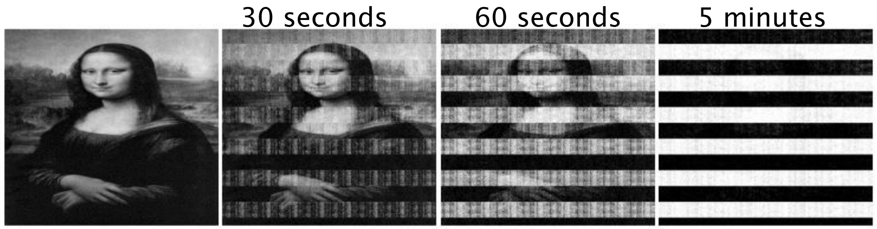
- Timing
- Power-monitoring attack
- Electromagnetic
- Acoustic cryptanalysis
- Differential fault
- Data remanence

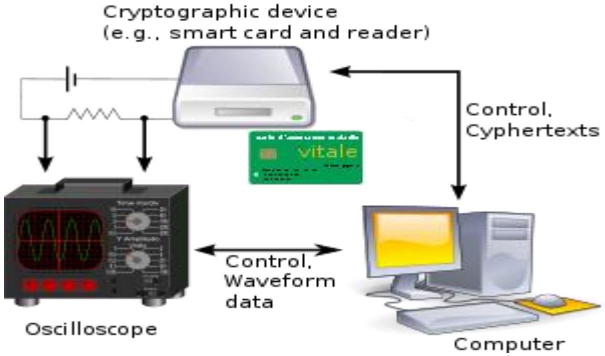


Differential Power Analysis (DPA) is a security risk for devices performing cryptographic operations

Chip computes secret key K, and security measures must prevent adversaries from extracting K

DPA Countermeasures are necessary to secure devices from DPA and other side channel attacks





# How to protect secure assets

## Secure electronics

Secure boot
Tamper circuit
TrustZone and firewall
Hardware crypto
On-the-fly encryption

## Secure software

Trusted software
Authenticated software distribution
Secure software update
Code audit

## Secure life-cycle

Manufacturing
Secure room
Personalisation system (using HSM)
Certified repair centre

## Secure housing

Wiring shields: flex and PCB
Blind keys, tamper switches
Avoid open cavities
Avoid flat surfaces

# Tampering

**Tamper-resistance:** make intrusion difficult, usually by employing hardened casing

**Tamper-evident:** make intrusion attempts evident to subsequent viewers, often by employing seals which must be broken during intrusion

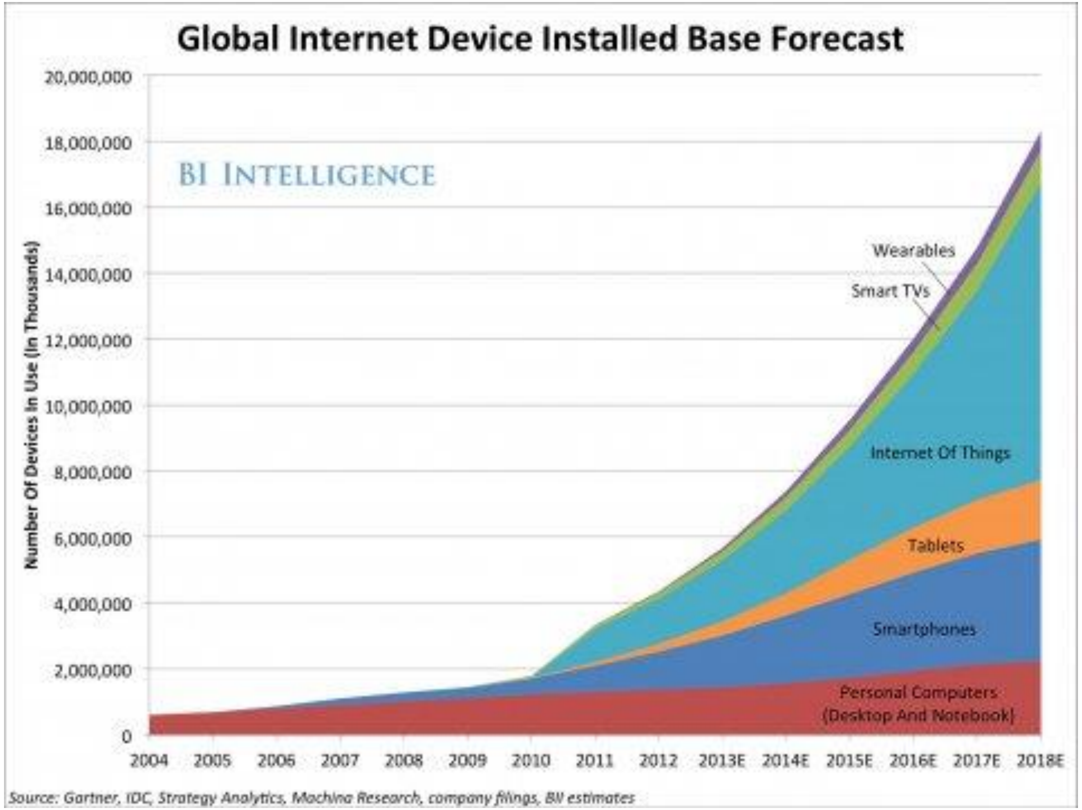
**Tamper-responsive:** detect the intrusion attempt and destroy the contents in the process

# Tamper circuit

- Sensors
  - Wire mesh
  - Voltage monitoring
  - Temperature monitoring
  - Frequency monitoring
  - Die shield
  - Crystal monitoring
- Actuator
  - Erase secure battery protected memory
  - Erasure of any sensitive data in memory if device is powered

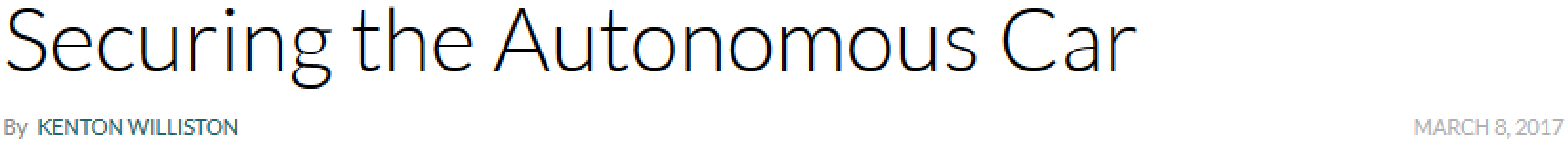
# 4 Security in IoT

# The rise of IoT



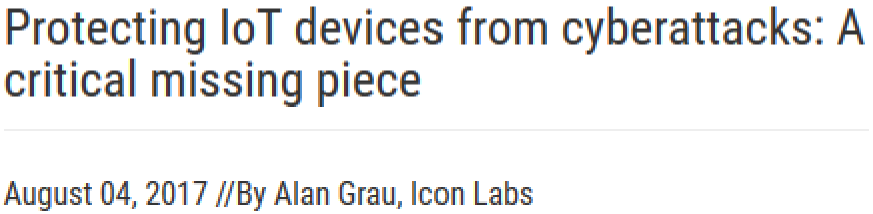
Source: Gartner, IDC, Strategy Analytics, Machina Research, company filings, BII estimates

# IoT Security in the press



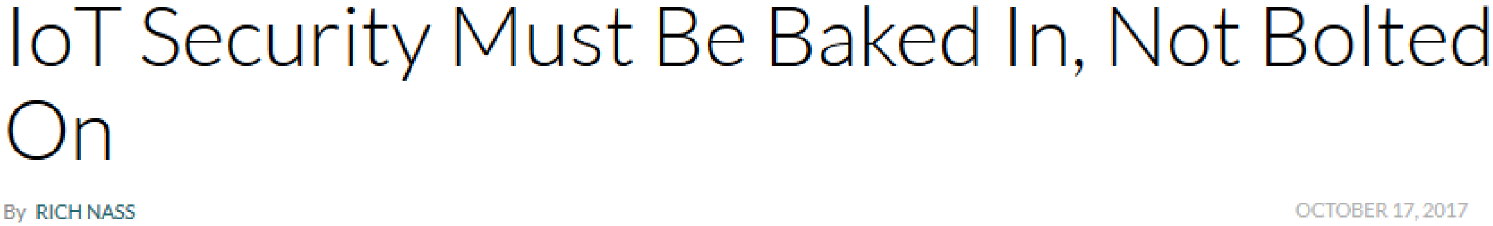
Securing the Autonomous Car

By KENTON WILLISTON MARCH 8, 2017



Protecting IoT devices from cyberattacks: A critical missing piece

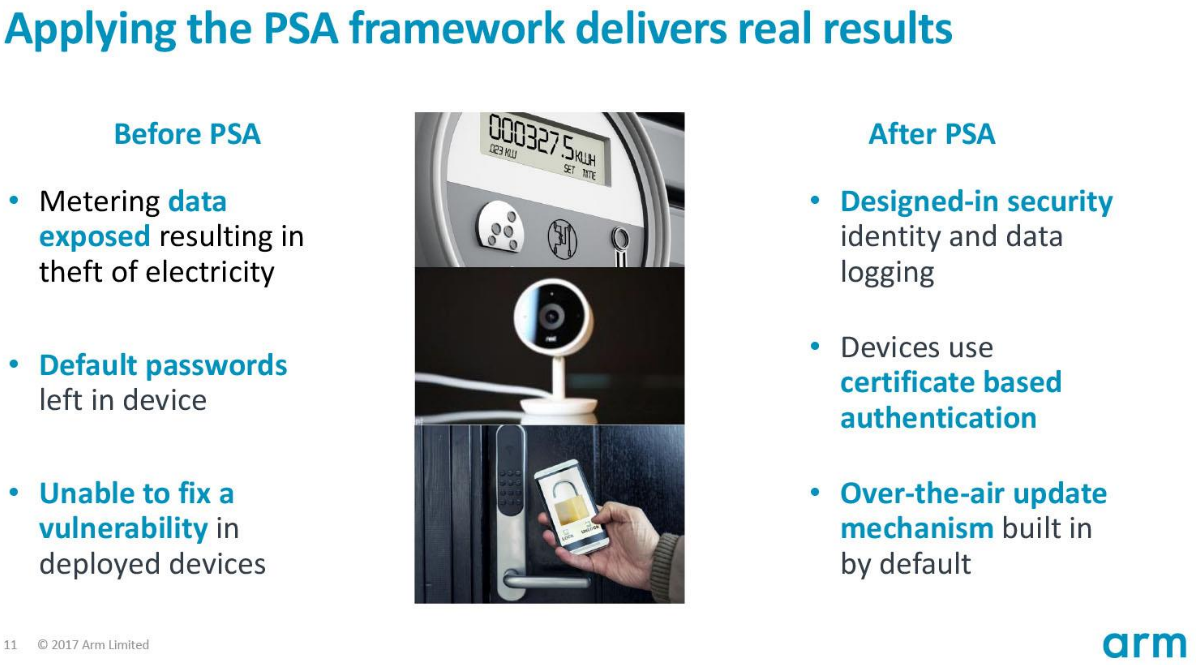
August 04, 2017 //By Alan Grau, Icon Labs



IoT Security Must Be Baked In, Not Bolted On

By RICH NASS OCTOBER 17, 2017

# Arm announces PSA security architecture for IoT devices



## Applying the PSA framework delivers real results

### Before PSA

- Metering **data exposed** resulting in theft of electricity
- **Default passwords** left in device
- **Unable to fix a vulnerability** in deployed devices

### After PSA

- **Designed-in security** identity and data logging
- Devices use **certificate based authentication**
- **Over-the-air update mechanism** built in by default

11 © 2017 Arm Limited

arm

# 5 Summary

# Summary

- Security for payment terminals exists for decades
- Strict regulation and certification exists today
- Hacking success rate is very low
- Similar type of challenges appear in emerging technologies
- Practises and principles can now be used in other industries

Thanks for your attention!

# Thanks

For more information please contact:

T+ 32 2 7276350
M+ 32 495 596862
peter.timmermans@worldline.com

an atos company

worldline
e-payment services