FROM RESEARCH TO INDUSTRY

cea tech

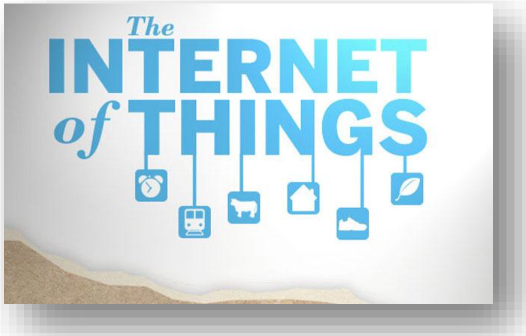
leti

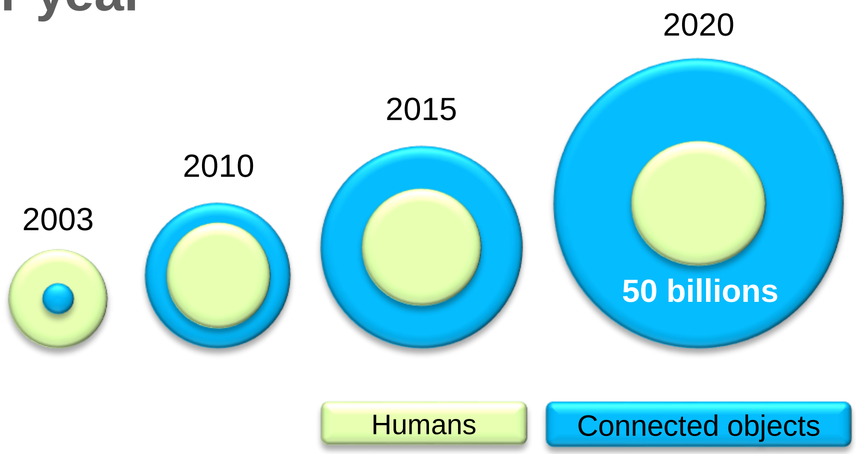
SECURITY FOR CONNECTED OBJECTS

Alain MERLE
CEA-LETI
Alain.merle@cea.fr

IOT: SOME FIGURES

- **Cisco predicts 50B of connected object by 2020**
- **X-as-a-service**
  - a breakthrough for carrier's business according to Ericsson
- **Estimated market value $2 trillion by 2020**
- **Up-to 1 trillion sensors deployed**
- **Traffic grows by 25% per year**





Source: CISCO, AT&T

- **What about security?**

SECURED COMMUNICATING EMBEDDED SYSTEM

- ✓ Real physical object
- ✓ Embedded hardware and software

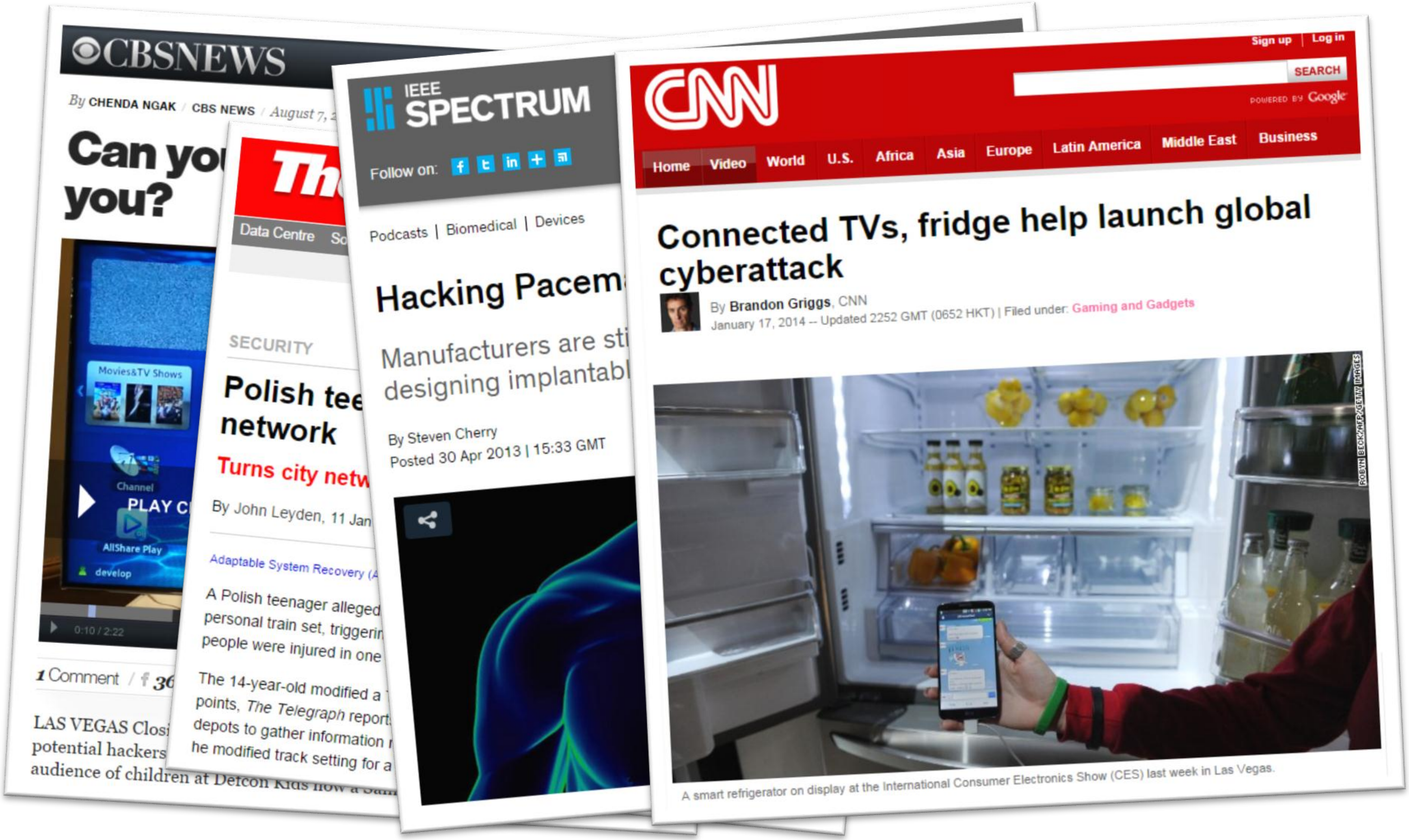
- ✓ There is physical access to the object
- ✓ « Telecom » link
- ✓ Often internet connection

- ✓ Use of cryptography
- ✓ Embedded cryptography

SECURITY WEAKNESSES ? ATTACKS ?

IOT: THE INTERNET OF THREATS

- Today security / privacy issues make the newspaper headlines



CBSNEWS

By CHENDA NGAK / CBS NEWS / August 7, 2

Can yo
you?

1 Comment / 36

LAS VEGAS Clos
potential hackers
audience of children at Defcon Kids how a sam

Th

Data Centre So

SECURITY

Polish tee
network

Turns city netw

By John Leyden, 11 Jan

Adaptable System Recovery (A

A Polish teenager alleged
personal train set, triggerin
people were injured in one

The 14-year-old modified a
points, *The Telegraph* report
depots to gather information
he modified track setting for a

IEEE SPECTRUM

Follow on:

Podcasts | Biomedical | Devices

Hacking Pacem

Manufacturers are sti
designing implantabl

By Steven Cherry
Posted 30 Apr 2013 | 15:33 GMT

CNN

Sign up | Log in

SEARCH

POWERED BY Google

Home Video World U.S. Africa Asia Europe Latin America Middle East Business

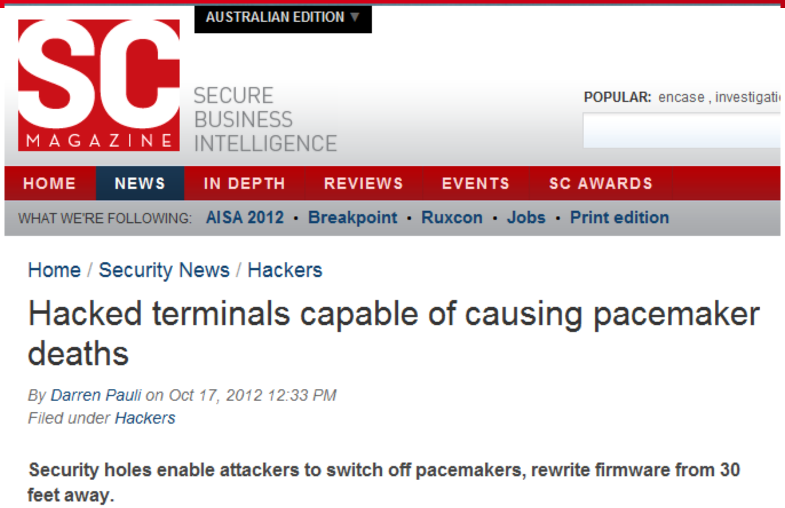
Connected TVs, fridge help launch global cyberattack

By **Brandon Griggs**, CNN
January 17, 2014 -- Updated 2252 GMT (0652 HKT) | Filed under: Gaming and Gadgets

ROBYN BECK/AFP/GETTY IMAGES

A smart refrigerator on display at the International Consumer Electronics Show (CES) last week in Las Vegas.

FOR E-HEALTH



AUSTRALIAN EDITION ▾

SC MAGAZINE

SECURE BUSINESS INTELLIGENCE

POPULAR: encase , investigati

HOME NEWS IN DEPTH REVIEWS EVENTS SC AWARDS

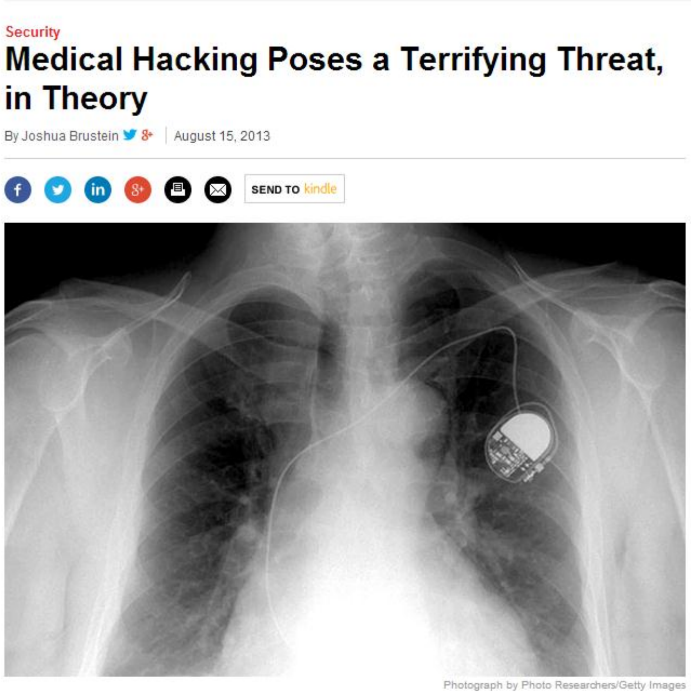
WHAT WE'RE FOLLOWING: AISA 2012 • Breakpoint • Ruxcon • Jobs • Print edition

Home / Security News / Hackers

Hacked terminals capable of causing pacemaker deaths

By Darren Pauli on Oct 17, 2012 12:33 PM
Filed under Hackers

Security holes enable attackers to switch off pacemakers, rewrite firmware from 30 feet away.



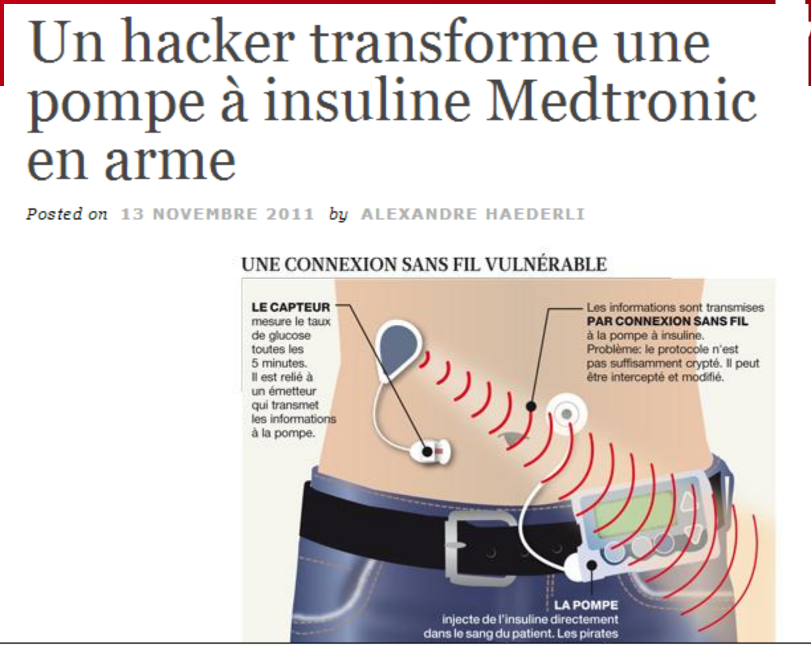
Security

Medical Hacking Poses a Terrifying Threat, in Theory

By Joshua Brustein | August 15, 2013

SEND TO kindle

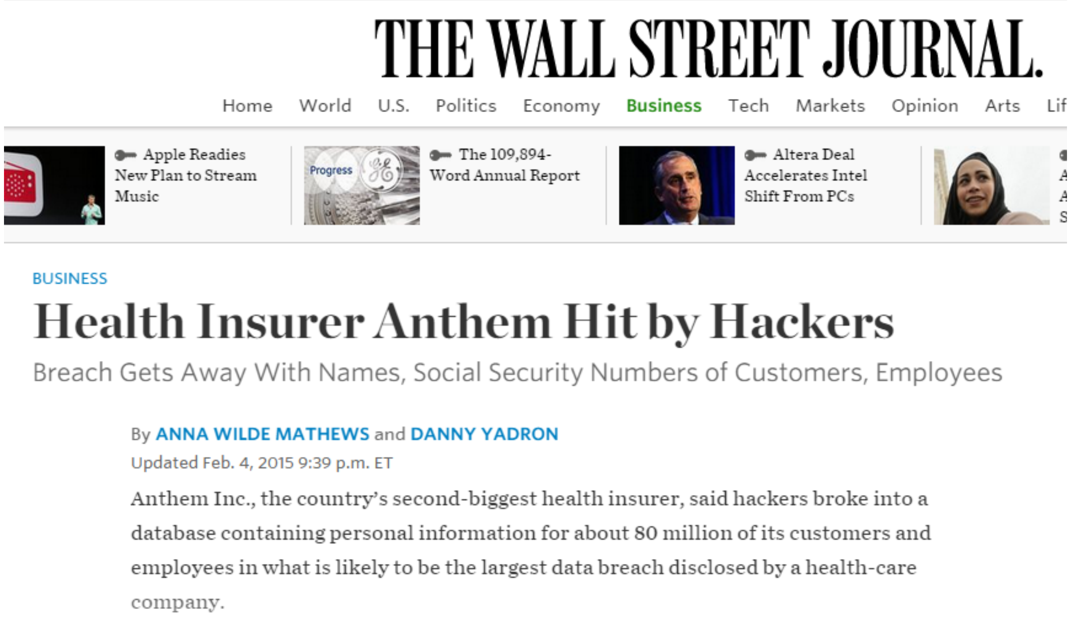
Photograph by Photo Researchers/Getty Images



Un hacker transforme une pompe à insuline Medtronic en arme

Posted on 13 NOVEMBRE 2011 *by* ALEXANDRE HAEDERLI

UNE CONNEXION SANS FIL VULNÉRABLE
LE CAPTEUR mesure le taux de glucose toutes les 5 minutes. Il est relié à un émetteur qui transmet les informations à la pompe.
Les informations sont transmises PAR CONNEXION SANS FIL à la pompe à insuline. Problème: le protocole n'est pas suffisamment crypté. Il peut être intercepté et modifié.
LA POMPE injecte de l'insuline directement dans le sang du patient. Les pirates



THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Lif

Apple Readies New Plan to Stream Music

The 109,894-Word Annual Report

Altera Deal Accelerates Intel Shift From PCs

BUSINESS

Health Insurer Anthem Hit by Hackers

Breach Gets Away With Names, Social Security Numbers of Customers, Employees

By ANNA WILDE MATHEWS and DANNY YADRON
Updated Feb. 4, 2015 9:39 p.m. ET

Anthem Inc., the country's second-biggest health insurer, said hackers broke into a database containing personal information for about 80 million of its customers and employees in what is likely to be the largest data breach disclosed by a health-care company.

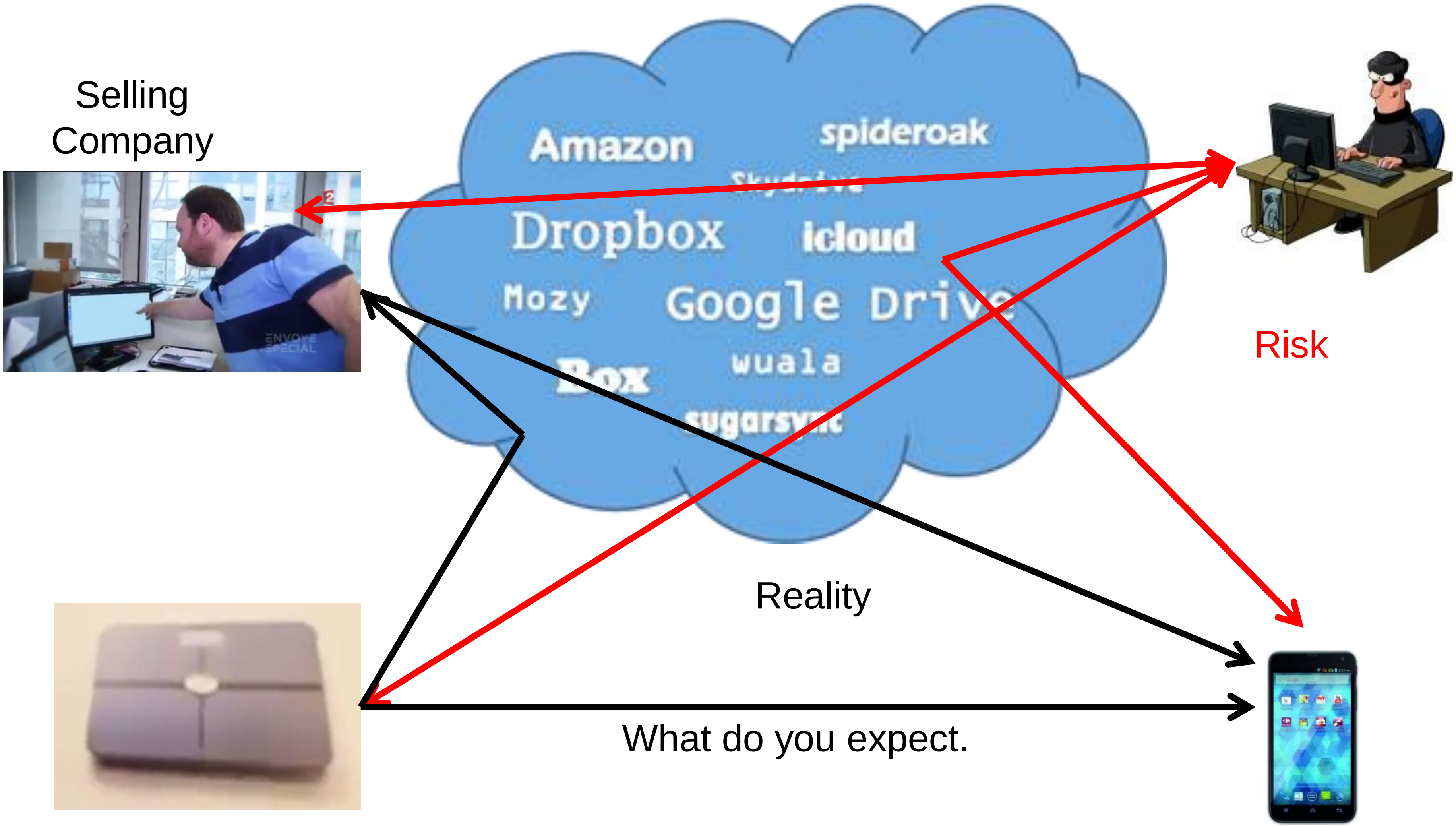
NULL CTRL

- Source:
  - http://www.dagbladet.no/2013/12/16/nyheter/nullctrl/shodan/english/english_versions/30861347/
  - Journalism in Dagbladet (Norway), European Press Prize 2013
  - Search engine: SHODAN
- **2048 Cameras, 1781 Printers, 2500 Control systems**
  - Unprotected, « Open » access

PRIVACY ?

- **TV magazine on June 5th, 2014**
  - Antenne2, « Envoyé spécial »

Selling Company

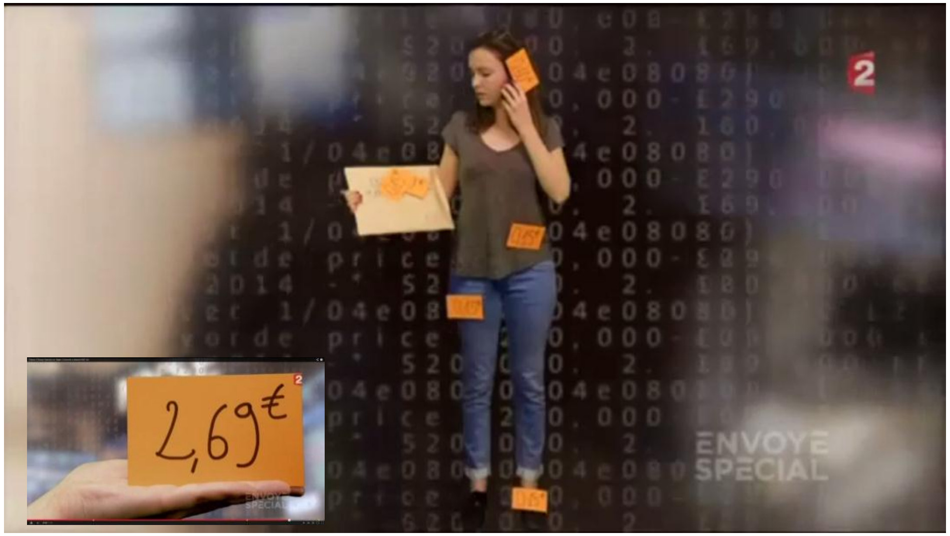


Risk

Reality

What do you expect.

PRIVACY



There is also an interest (societal, economy, health) in statistics on datasets

France 2 Envoye Special Les Objets Connectes à Internet WiFi 4G
2
CEDRIC HUTCHINGS
PDG DE WITHINGS
ENVOYE SPECIAL

"*We do not exclude to sell the personal data … anonymized*"

Already sold in USA, non anonymized (bonus for insurance if loosing weight)

COUNTERFEITING

Buying a fake branded handbag for your loved one?

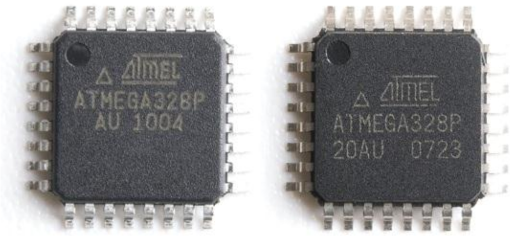
Finding horse meet in your beef lasagna?

Fake portable hard drive?

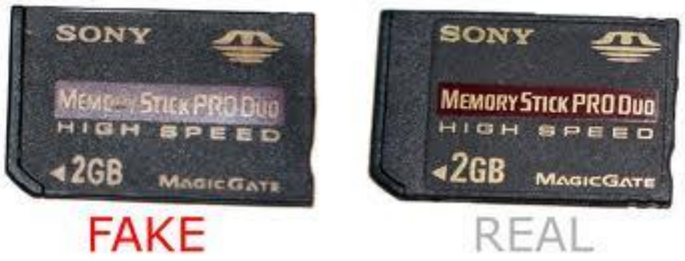
Having easy access to counterfeit medicines?

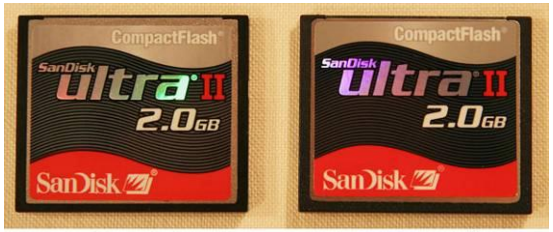
Counterfeiting accounts for 2% of the world trade!
Expected to exceed $1.7 trillion by 2015!

ALSO IN HARDWARE



Fake & genuine Atmel chips

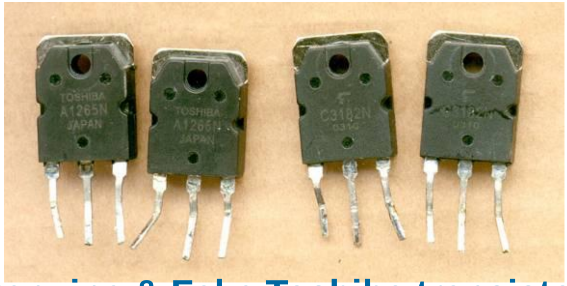




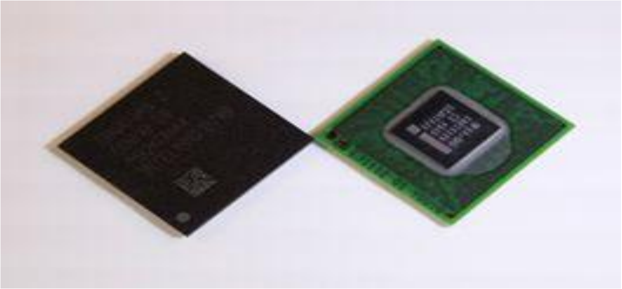
fake card

genuine card

http://martybugs.net



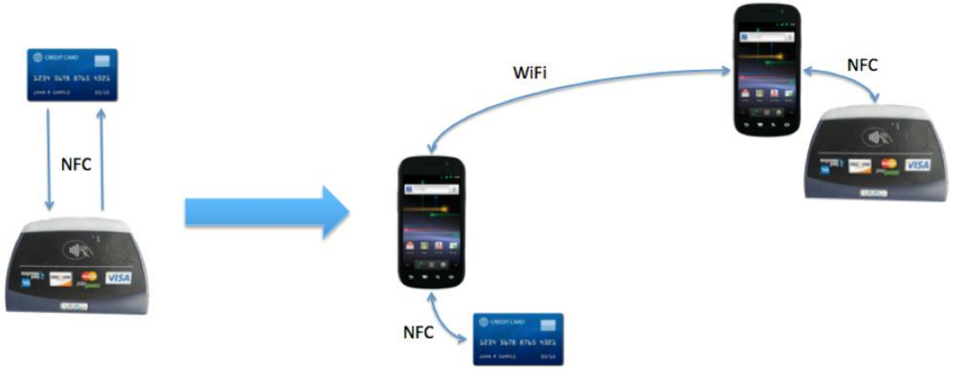
Genuine & Fake Toshiba transistors

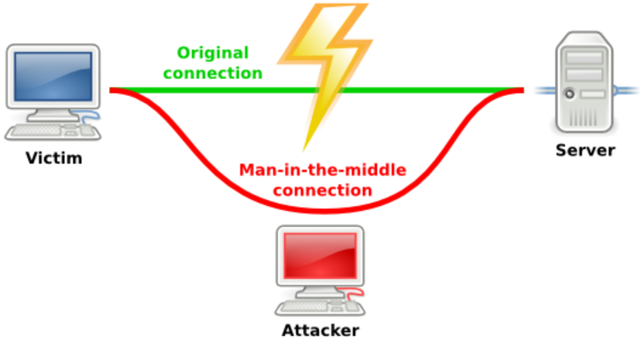


Fake chips sold to US military in 2010 (VisionTech scandal)

ATTACKS TOWARDS THE WIRELESS LINK

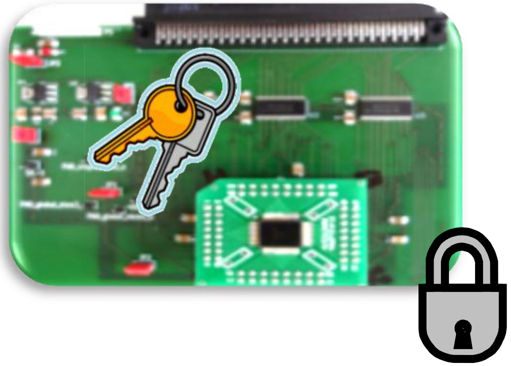
- Relay
  - Independent of the crypto
- Man on the middle
- Denial of service
- Eavesdropping/Skimming





- ➢ **NFC characterization**
  - ➢ **Eavesdropping: > 20m**
  - ➢ **Skimming: > 1m**

ATTACKS ON SECURE DEVICES



Cryptanalysis

RC5,

MIFARE,

Brute force attacks,

Etc.

Software attacks

Buffer overflows,

Brute force attacks,

Attacks on protocols

Etc.

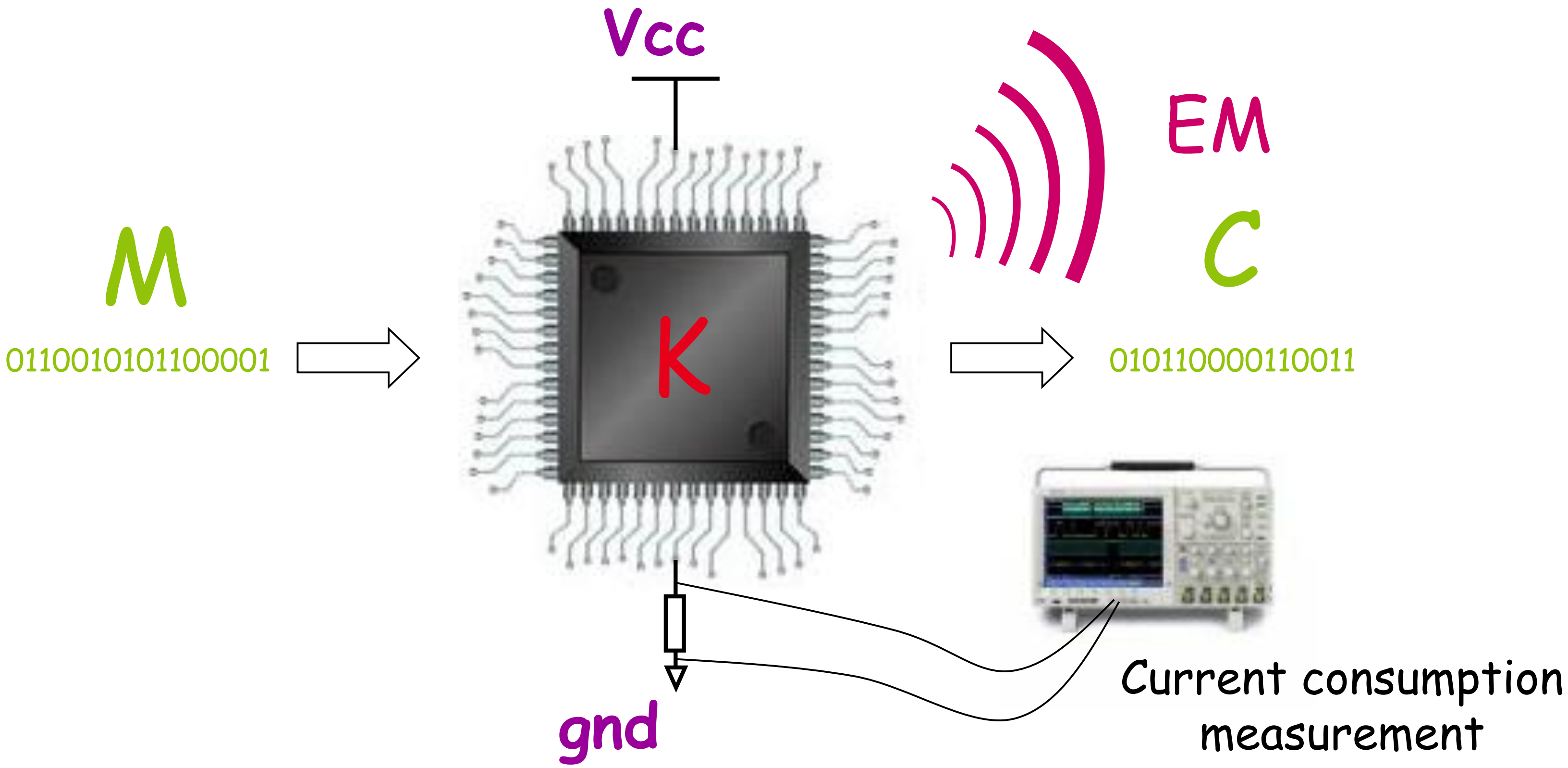
Hardware attacks

Extremely powerfull thanks to the direct access to the component:

Example:

AES-128 key cracking in minutes on a 32-bit unsecure microcontroller

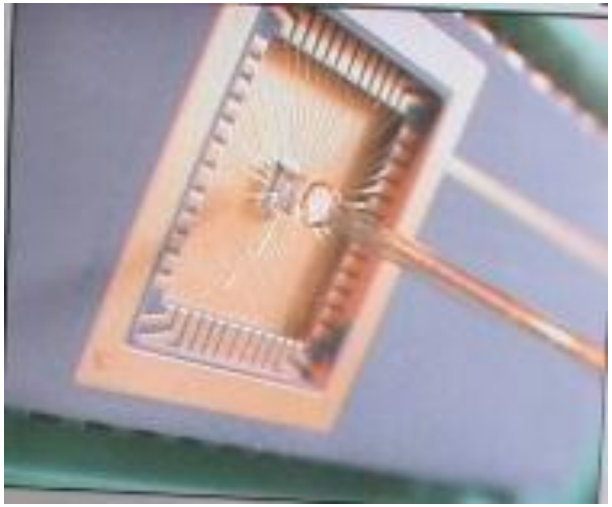
SIDE CHANNEL ANALYSIS (SCA, DPA)

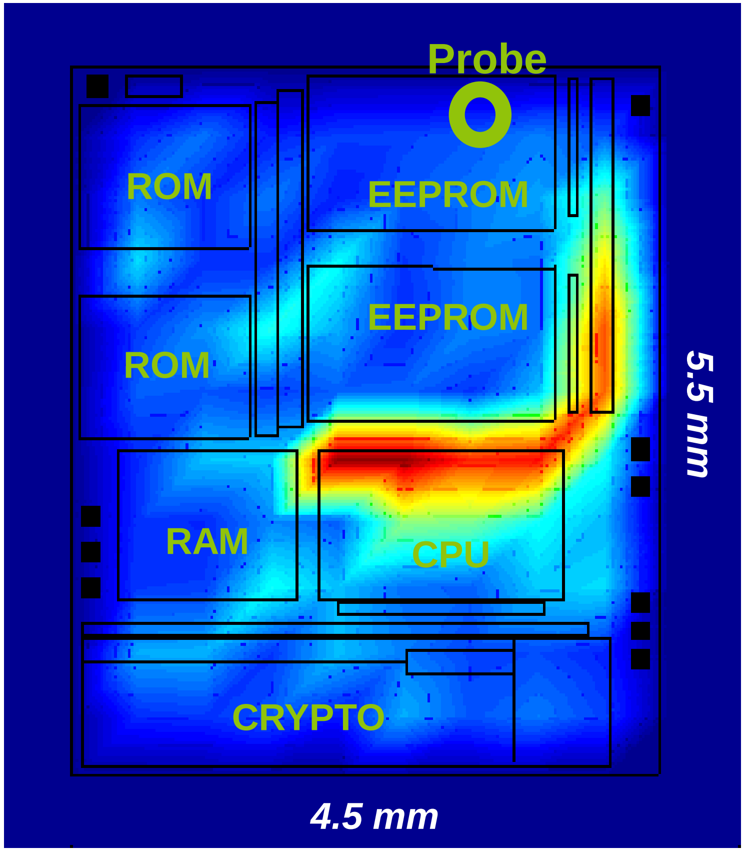


The power consumption of a chip depends on

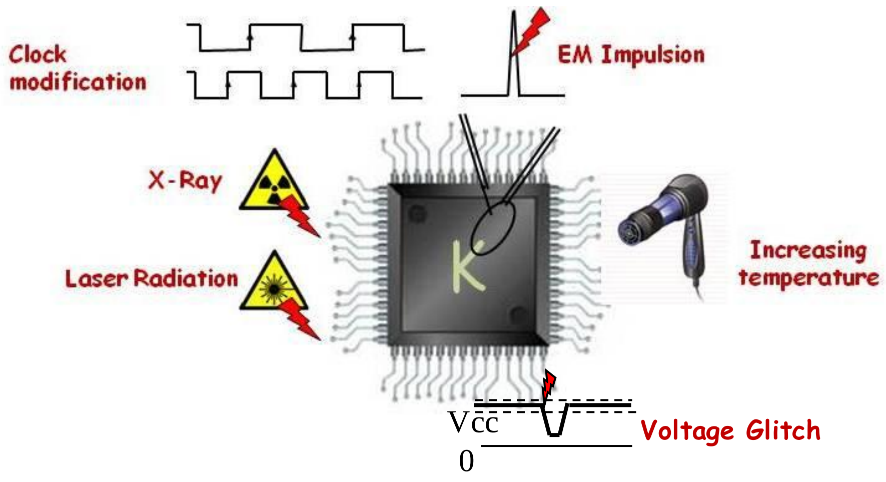
- the manipulated data
- the executed instruction

ELECTROMAGNETIC LEAKAGE





FAULT ATTACKS

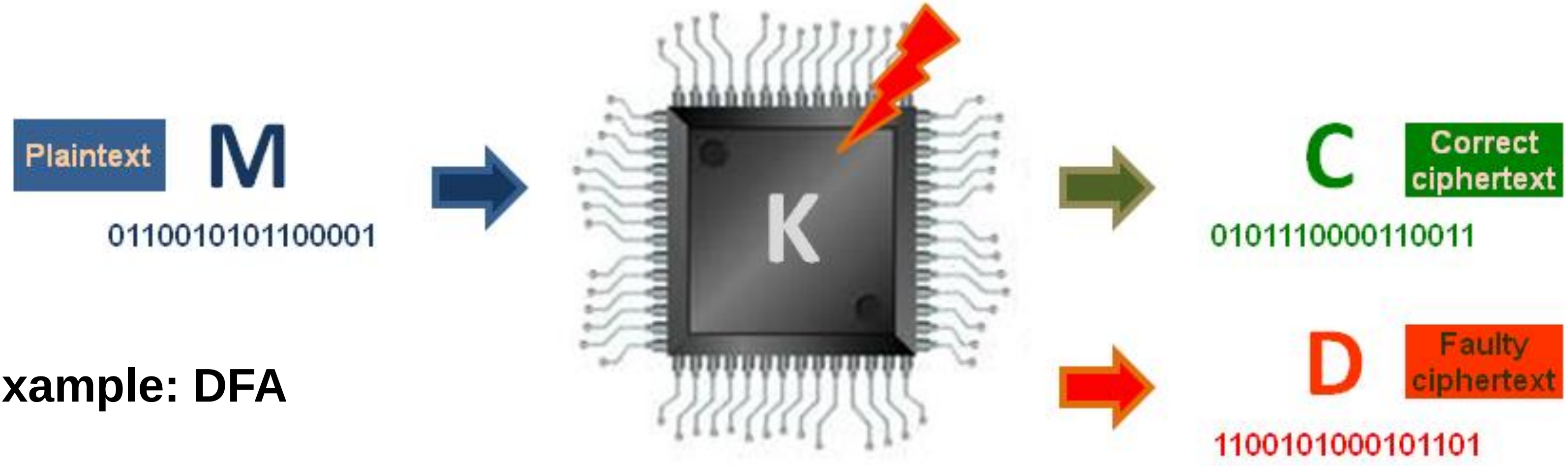


Voluntary modification of a chip's environment

Altering the chip's functioning

Security Weakness

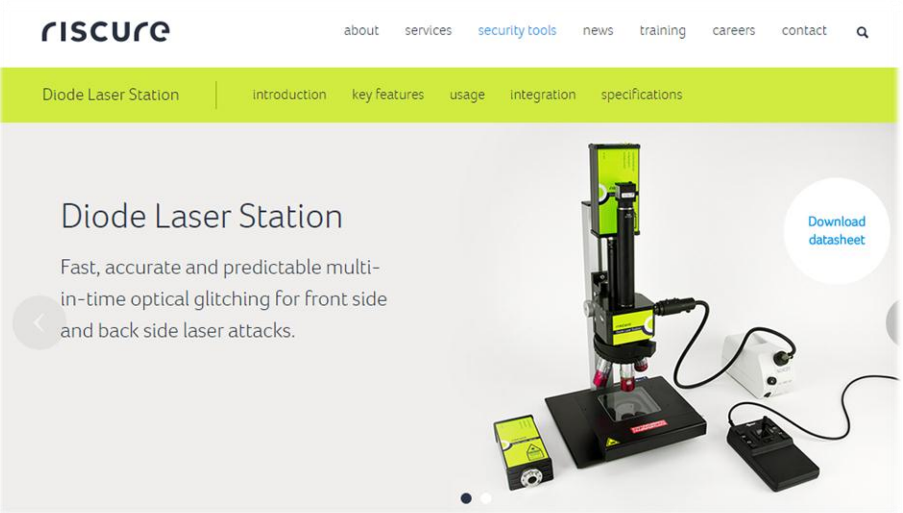
Example: DFA



FROM RESEARCH TO INDUSTRY
cea tech

PRACTICAL FAULT INJECTION

leti


riscure

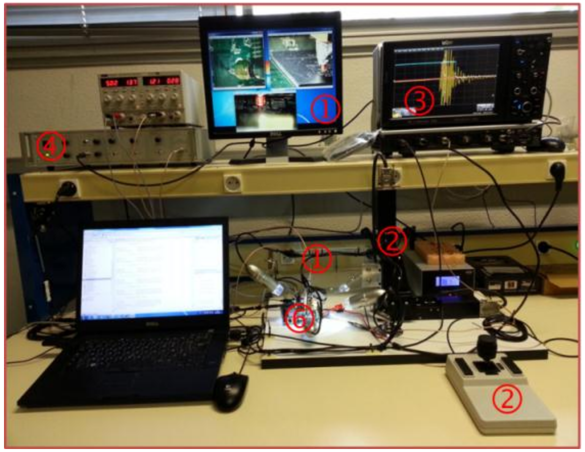
about services security tools news training careers contact

Diode Laser Station | introduction key features usage integration specifications

Diode Laser Station

Fast, accurate and predictable multi-in-time optical glitching for front side and back side laser attacks.

Download datasheet



① 3-axes vision system

② 3-axes positioning system

③ Oscilloscope

④ Pulse generator

⑥ Hand made injection probes

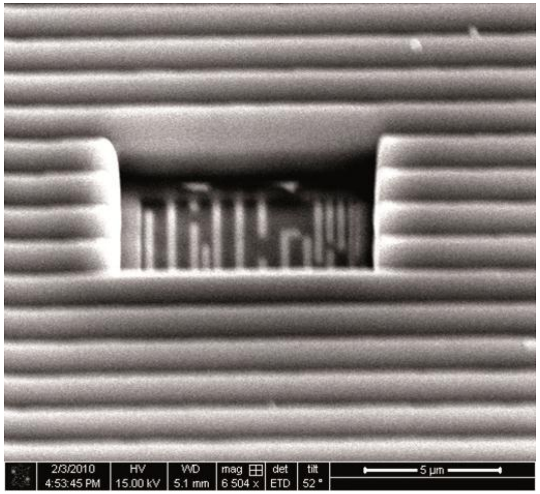
⑦ a laptop

arcsis
Micro-PackS

www.arcsis.org

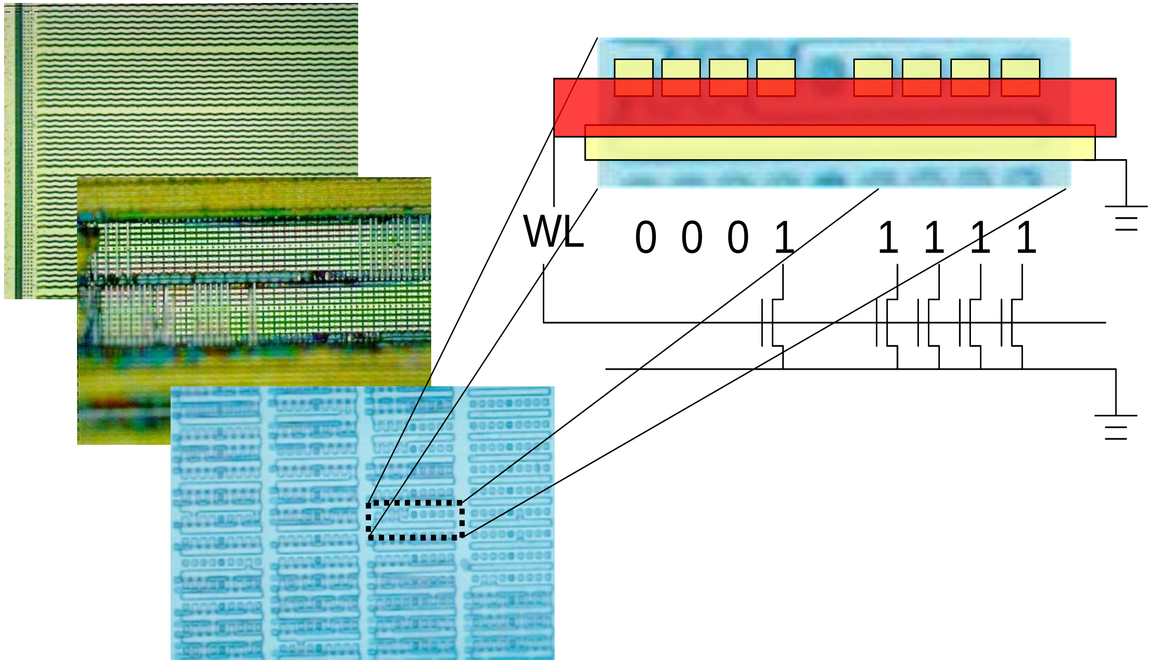
INVASIVE ATTACKS

- Delayering
- Deposit probe pads on a bus or through conductive grid
- Connect tracks
- Cut tracks

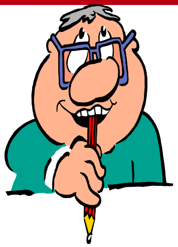


❑Remove the top layers

❑Read the content of the array



SECURITY PARADIGM



New counter-measure designed

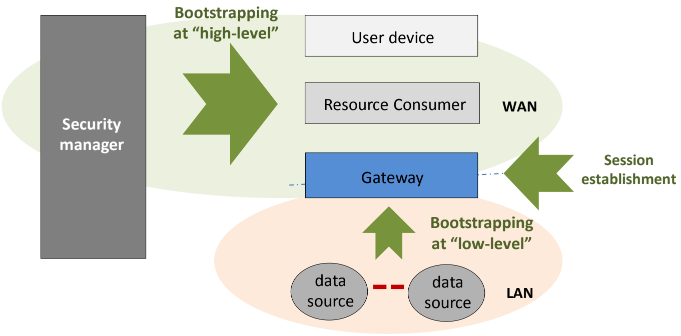
The security of a system is determined by the security of its weakest link

Very fast evolving area: Take care of the life time

New attacks /
New tools /
Better computing power…

BOOTSTRAPPING, DEPLOYMENT, UPDATE, RECOVERY

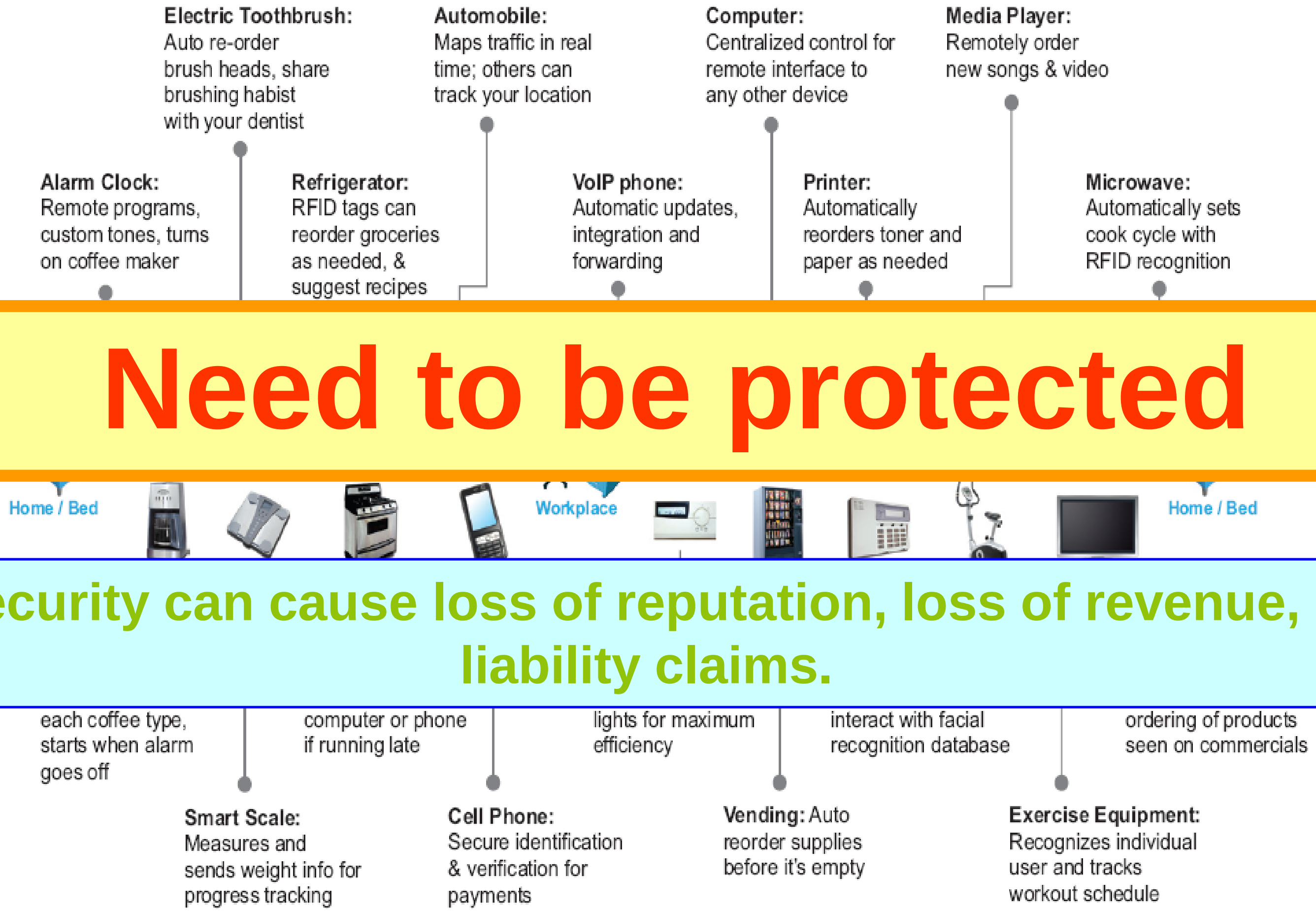
- **How an user to personalize a virgin node into his network?**
  - Lowlevel bootstrapping: local credentials (eg. network access)
  - Highlevel bootstrapping: access to the resources (eg. Service)
  - Directions
    - In-band pairing
    - Out-band pairing
    - Secure storage
    - Preshared certificates



- **How to have a Secure Update of the SW ?**
- **How to recover from a compromised situation ?**

Source: CATRENE workshop on smartcities

EMBEDDED SYSTEMS



Electric Toothbrush: Auto re-order brush heads, share brushing habit with your dentist

Automobile: Maps traffic in real time; others can track your location

Computer: Centralized control for remote interface to any other device

Media Player: Remotely order new songs & video

Alarm Clock: Remote programs, custom tones, turns on coffee maker

Refrigerator: RFID tags can reorder groceries as needed, & suggest recipes

VoIP phone: Automatic updates, integration and forwarding

Printer: Automatically reorders toner and paper as needed

Microwave: Automatically sets cook cycle with RFID recognition

Need to be protected

Lack of security can cause loss of reputation, loss of revenue, and even liability claims.

each coffee type, starts when alarm goes off

computer or phone if running late

lights for maximum efficiency

interact with facial recognition database

ordering of products seen on commercials

Smart Scale: Measures and sends weight info for progress tracking

Cell Phone: Secure identification & verification for payments

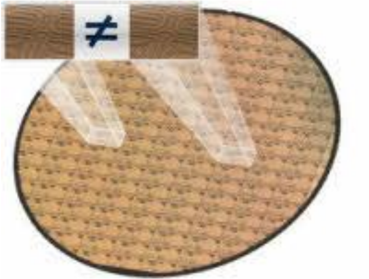
Vending: Auto reorder supplies before it's empty

Exercise Equipment: Recognizes individual user and tracks workout schedule

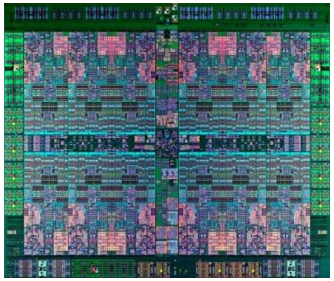
Source: Attacks on Mobile and Embedded Systems – Five important trends, June 20, 2011, Mocana Corporation https://www.mocana.com/

SOLUTIONS ?

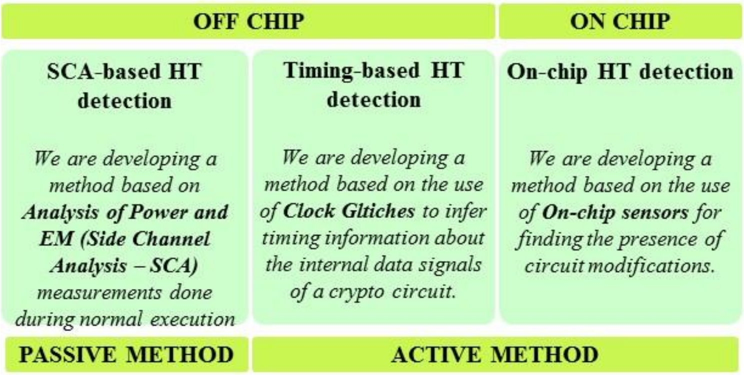
- **Unique identifier (key) for each object**
  - PUF, Secure element, PKI
- **Secured implementation of adapted cryptography**
  - Lightweight, Homomorphic, functional, etc
- **Generalized integrity checking (HW, SW)**
- **Adapted protocols**
- **And some others ….**



Source: VERAYO



Tamper resistant chip design



OFF CHIP		ON CHIP
SCA-based HT detection *We are developing a method based on **Analysis of Power and EM (Side Channel Analysis – SCA)** measurements done during normal execution*	**Timing-based HT detection** *We are developing a method based on the use of **Clock Gltiches** to infer timing information about the internal data signals of a crypto circuit.*	**On-chip HT detection** *We are developing a method based on the use of **On-chip sensors** for finding the presence of circuit modifications.*
PASSIVE METHOD	ACTIVE METHOD	

TO CONCLUDE: SECURITY IS COMPLEX !

- **Cryptography (AES 128) is not all the solution**
  - Security of the implementation
  - Protocols (bootstrapping, Update, Recovery)
- **There are no quick fixes : « Nobody is perfect »**
  - Vulnerabilities discovered every day
  - The secure hardware is the best solution but it is not perfect
  - Be careful to the life cycle of products
- **Any errors are attack paths**
- **Evaluation/Certification is good tool**
  - Competent third party
  - National security (ANSSI)

CONCLUSION 2

- **Difficulties to have a common global security model**
  - What to protect ?
  - Attackers typology

- **Security in the early phases of design.**
  - Limit cost/complexity
  - Improve efficiency

Merci de votre attention