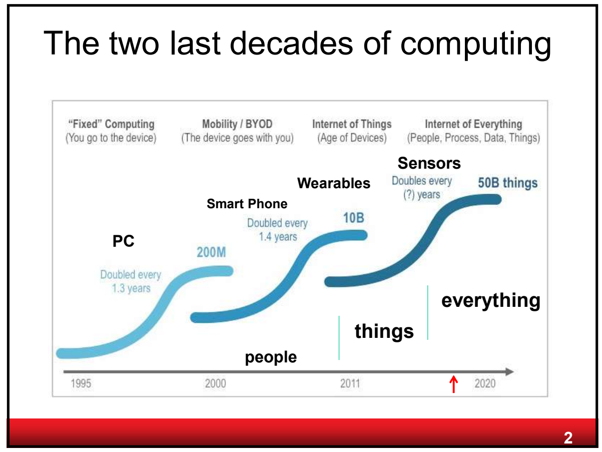
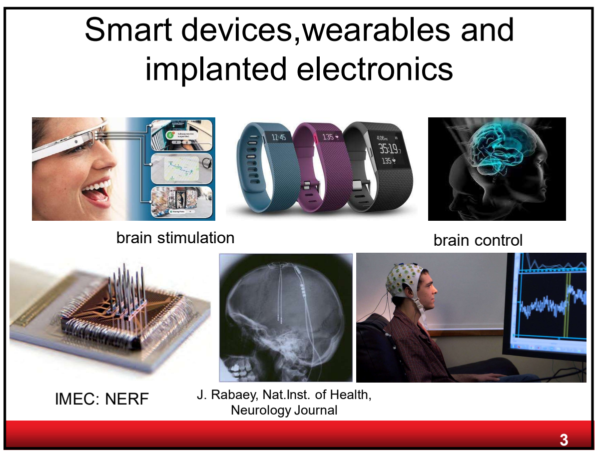
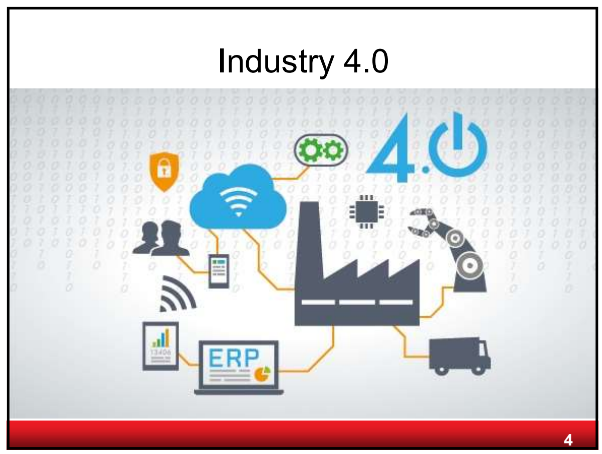
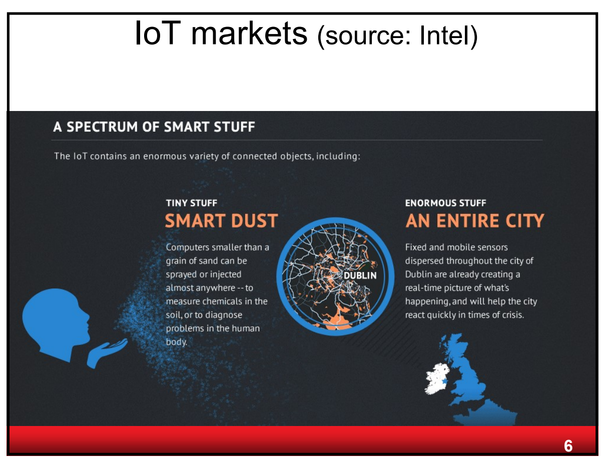

imec
embracing a better life
KU LEUVEN
THE INTERNET OF THINGS
Security and Privacy Challenges for the IoT
Bart Preneel
imec-COSIC KU Leuven, Belgium
Bart.Preneel(at)esat.kuleuven.be
June 2017
www.comsoc.org/blog
© KU Leuven COSIC, Bart Preneel
1


The two last decades of computing
"Fixed" Computing (You go to the device)
Mobility / BYOD (The device goes with you)
Internet of Things (Age of Devices)
Internet of Everything (People, Process, Data, Things)
PC
Doubled every 1.3 years
200M
Smart Phone
Doubled every 1.4 years
Wearables
10B
Sensors
Doubles every (?) years
50B things
people
things
everything
1995
2000
2011
2020
2


Smart devices,wearables and implanted electronics
brain stimulation
brain control
IMEC: NERF
J. Rabaey, Nat.Inst. of Health, Neurology Journal
3


Industry 4.0
4.0
ERP
4


THE TOP CONNECTED APPLICATION IN 2020: THE CONNECTED CAR


IoT markets (source: Intel)
A SPECTRUM OF SMART STUFF
The IoT contains an enormous variety of connected objects, including:
TINY STUFF
SMART DUST
Computers smaller than a grain of sand can be sprayed or injected almost anywhere -- to measure chemicals in the soil, or to diagnose problems in the human body.
DUBLIN
ENORMOUS STUFF
AN ENTIRE CITY
Fixed and mobile sensors dispersed throughout the city of Dublin are already creating a real-time picture of what's happening, and will help the city react quickly in times of crisis.
6

What is the Internet of Things (IoT)?

Oxford: "A proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data.

Wikipedia: IoT is the network of physical objects or "things" embedded with electronics, software, sensors and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices

ISO: draft Technical Report on use cases: 80 pages

What is the Internet of Things?

Internet of Things envisions a self-configuring, adaptive, complex network that interconnects 'things' to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely identifiable. The representation contains information including the thing's identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration."

Domenico Rotondi, Roberto Minerva, Abyi Biru. Towards a Definition of the Internet of Things (IoT). http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf, 2015

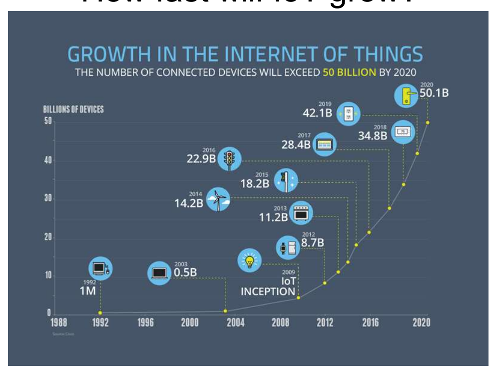
What is the Internet of Everything (IoE)?

Cisco: the networked connection of people, process, data, and things. The benefit of IoE is derived from the compound impact of connecting people, process, data, and things, and the value this increased connectedness creates as "everything" comes online.

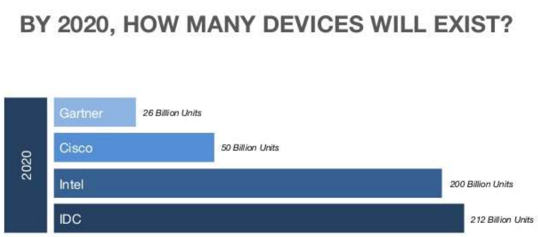
– IoE comprises many technology transitions (including IoT)

[…] a $4.6 trillion opportunity for global public-sector organizations over the next decade, as a result of cost savings, increased productivity, new revenues and enhanced citizen experiences

How fast will IoT grow?



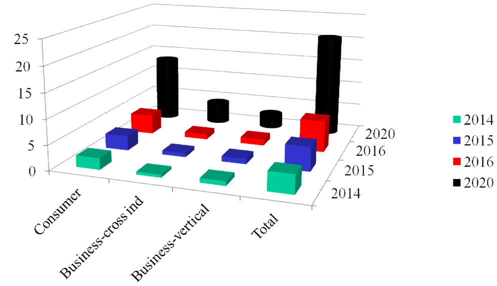
How fast will IoT grow? (2)



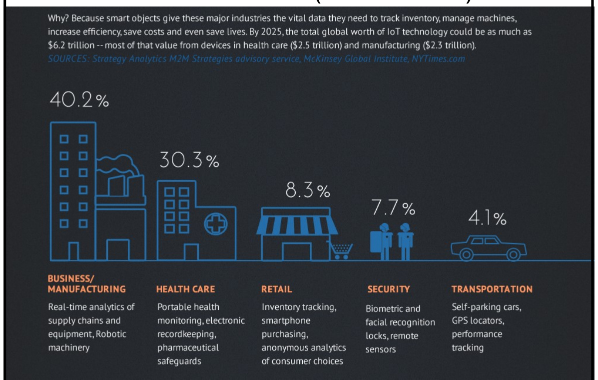
Source:
[1] http://www.gartner.com/newsroom/id/2684616
[2] http://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html
[3] http://share.cisco.com/internet-of-things.html
[4] http://www.zdnet.com/article/internet-of-things-8-9-trillion-market-in-2020-212-billion-connected-things/

How fast will IoT grow? (3)

[Gartner, Nov 2015]

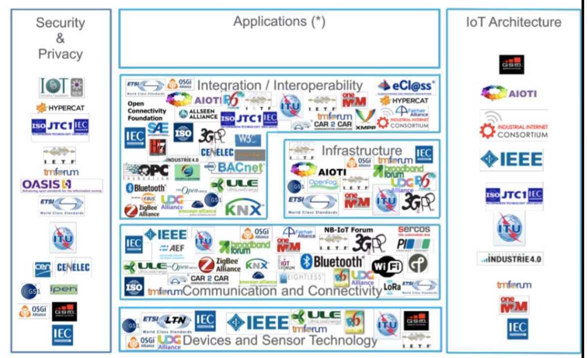


IoT markets (source: Intel)



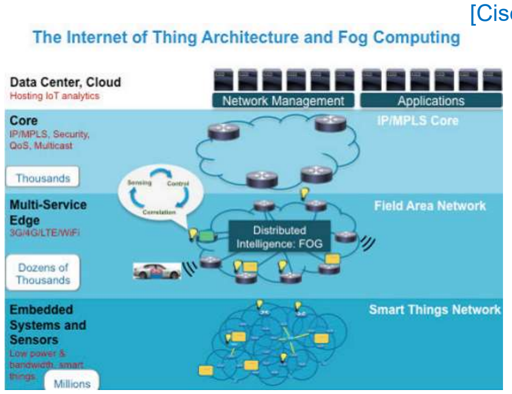
13

IoT standardization (source: AIOITI WG3)

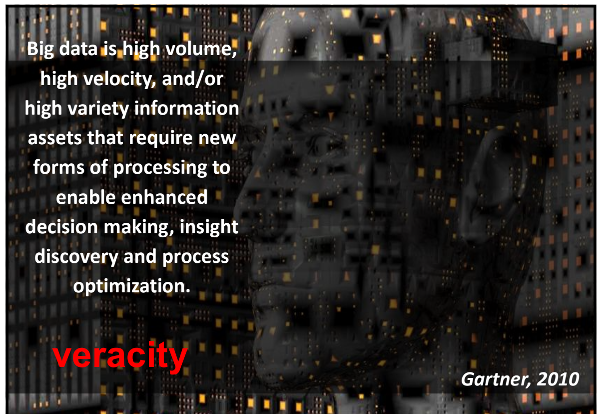


14

[Cisco]

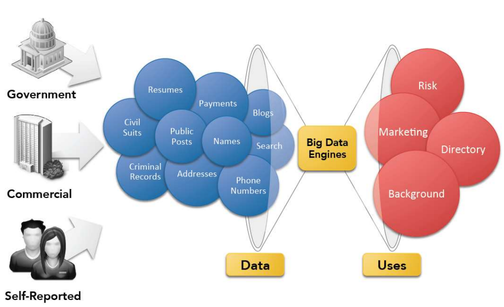


15



16

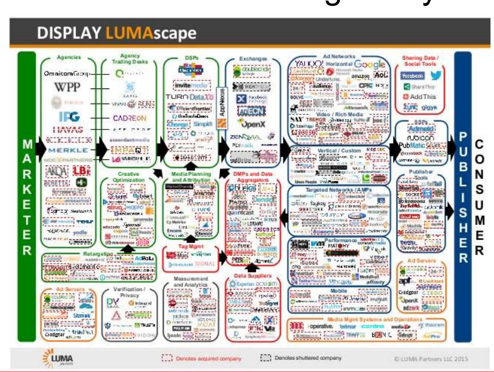
The data supply chain [Jim Adler]



https://www.usenix.org/sites/default/files/conference/protected-files/adler_sec13_slides.pdf

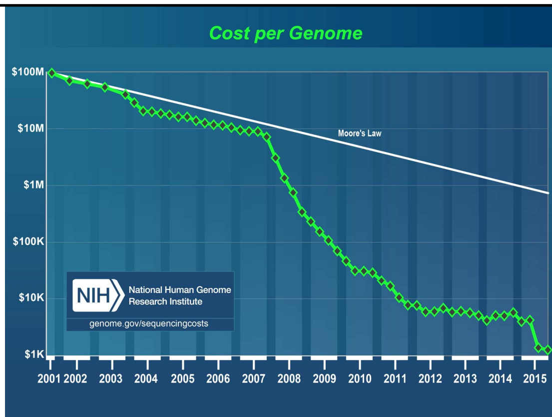
17

The Internet advertising ecosystem



http://www.lumapartners.com/lumascapes/display-ad-tech-lumascape/

18



https://www.genome.gov/images/content/costpergenome2015_4.jpg

IoT security risks

IoT security risks

More pervasive and intrusive: building, car, body

- low cost
- larger attack surface
- harder to update

Security

- bringing down the internet (e.g. Mirai)
- bringing down the grid
- hacking cars and drones
- burglary
- hacking medical devices

Cybersecurity and security for IoT

Governments are undermining ICT systems rather than improving cybersecurity

- part of industry is helping them

Problems at system level:

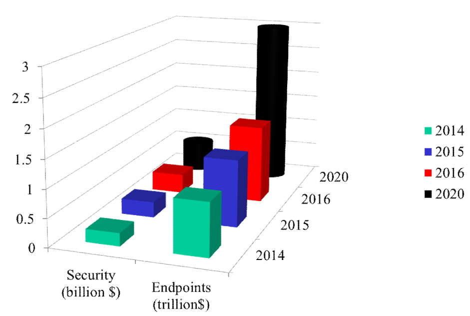
- secure execution
- secure update
- supply chain security
- 0-day market

Problems at network level

- end-to-end deployment of encryption
- meta data: IP address, location, …
- network protocols such as BGP, DNS

IoT: security vs. endpoint spending

[Gartner, Apr 2016]



OWASP IoT top 10 2014

https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

1 Insecure Web Interface
2 Insufficient Authentication/Authorization
3 Insecure Network Services
4 Lack of Transport Encryption
5 Privacy Concerns
6 Insecure Cloud Interface
7 Insecure Mobile Interface
8 Insufficient Security Configurability
9 Insecure Software/Firmware
10 Poor Physical Security

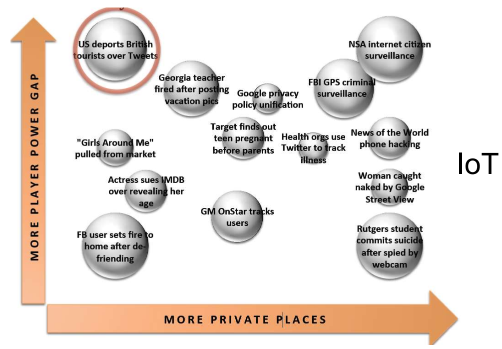
IoT privacy nightmare?

What is privacy?
What are the limitations of the current approach?
What are the future problems?

HP IoT study: 90% of devices collected at least one piece of personal information via the device, the cloud or its mobile application

Privacy problems: Places/Players/Perils

[Jim Adler]



What is privacy?

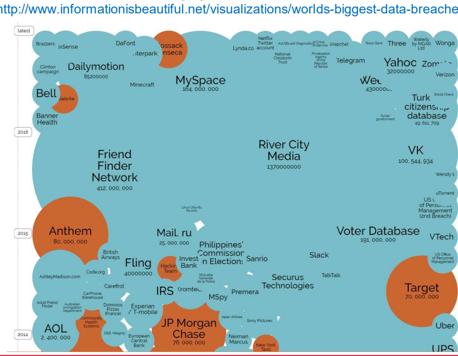
Abstract and subjective concept, hard to define
Depends on cultural aspects, scientific discipline, stakeholder, context
Conflicts are inherent

Privacy problems

- Data breaches
- Profiling
- Discrimination
- Manipulation
- Prediction
- Mass surveillance

World's Biggest Data Breaches

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks



Legal approach

Data controller: trusted
Limited purpose: can be hard to define
Proportional: which forms of data mining are?
Consent: how will this work in IoT/IoE?
Right to verify and correct: after a long legal battle?

Irish privacy commissioner here

Challenges

Technology
complexity
fast evolution
security & privacy as afterthought

Psychology
Difficult to deal with risks

Who is in charge?

Economics
externalities
misaligned incentives

Societal/Legal
undermining social fabric and power relations
stakeholders play catch-up game

31

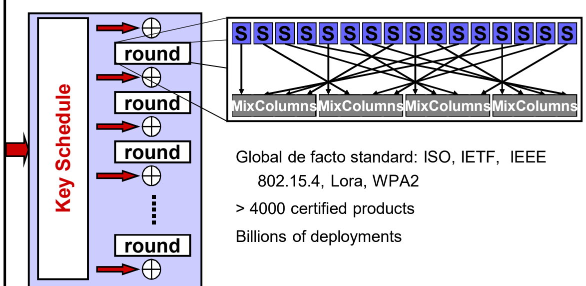
Crypto challenges

PRNGs
secure messaging
location-based services
- secure localization
- location privacy

cliptography
….
low-cost crypto
secure implementation
post-quantum cryptography

32

AES: Rijndael (FIPS 197)



Global de facto standard: ISO, IETF, IEEE 802.15.4, Lora, WPA2
> 4000 certified products
Billions of deployments

33

AES Implementations

Fast software
7.6 cycles/byte on Intel
< 1 cycle/byte on Intel with AES instruction

Tiny software
49 bytes of RAM on 8051

Fast hardware
(.15 mm²) (45 nm)
53 Gbit/s
125 mW
434 Gbps/W

Tiny hardware
(2400 GE) (0.18 μm)
56 Kbit/sec
3.7 μW
15 Gbps/W
65 pJ/bit

34

Medical implants

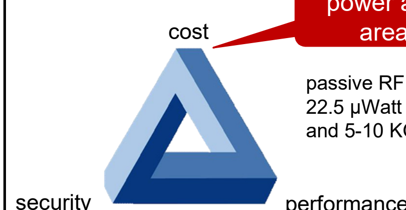
Power is limited: < 0.5 μWatt
- implanted devices only temperature Δ < 1 °C
- cooling problem

Battery is limited
- pace maker battery is not rechargeable

Slide credit: Ingrid Verbauwhede

35

Lightweight crypto: Can we improve over AES?

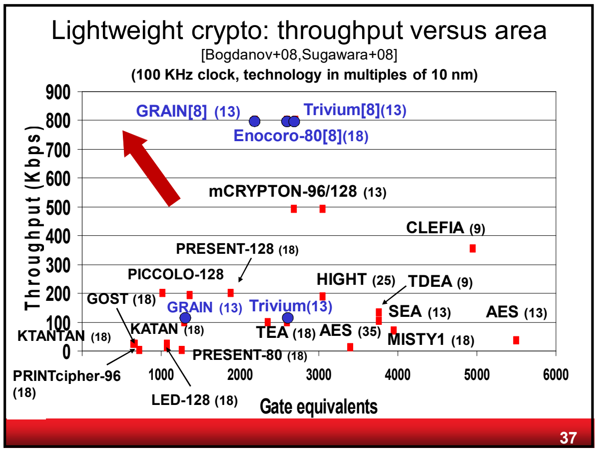


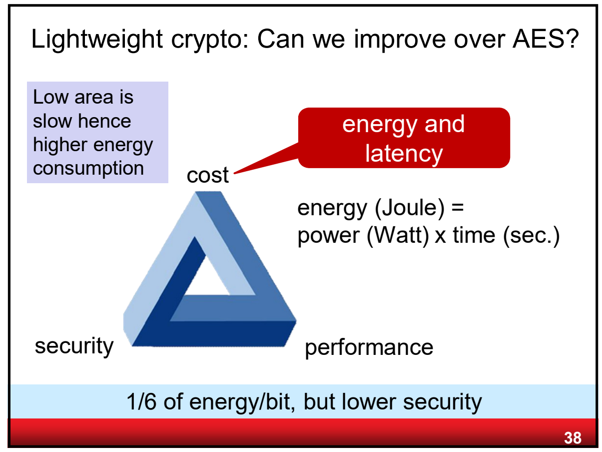
power and area

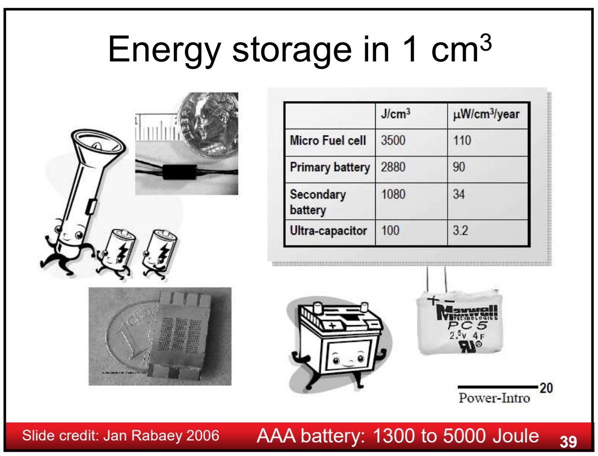
passive RFID example:
22.5 μWatt @1.5V
and 5-10 KGE

1/2-1/3 area or x10 throughput/area (but lower security)

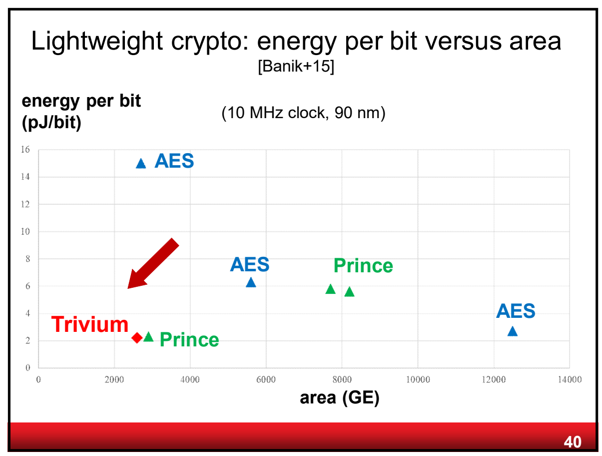
36

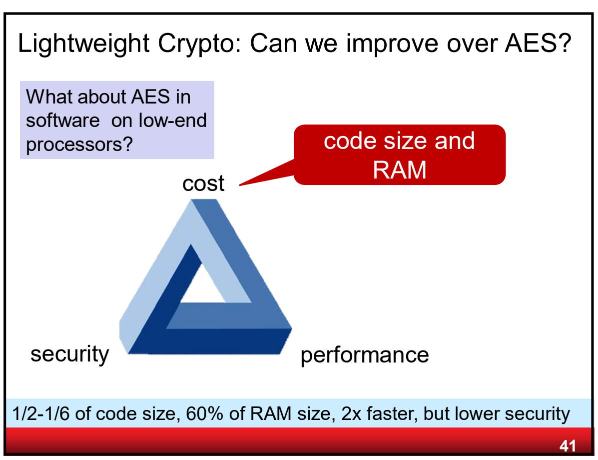


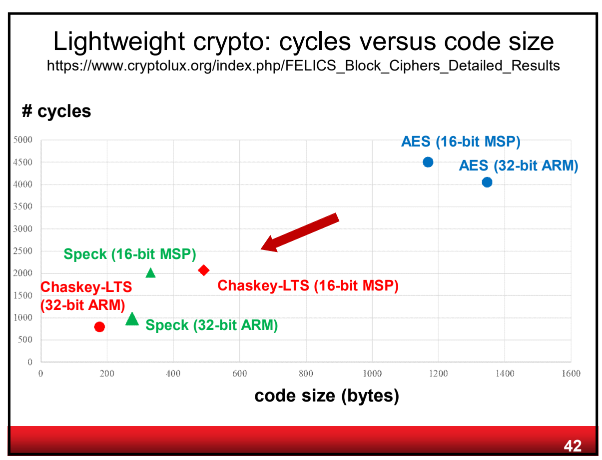




	J/cm³	µW/cm³/year
Micro Fuel cell	3500	110
Primary battery	2880	90
Secondary battery	1080	34
Ultra-capacitor	100	3.2



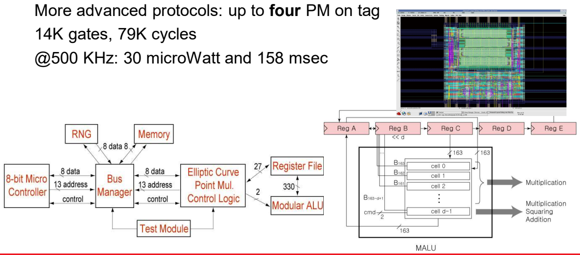




Result: 4.8 μJoule per point multiplication

ECC co-processor:
- ECC point multiplications (163 by 4)
- scalar modular operations (8-bit processor with redundancy)

Schnorr (secure ID transfer, but no tracking protection): **one** PM
More advanced protocols: up to **four** PM on tag
14K gates, 79K cycles
@500 KHz: 30 microWatt and 158 msec



Slide credit: Ingrid Verbauwhede
43

Public-key cryptography

- No global secrets
- Key management easier
- Energy cost several hundred times larger

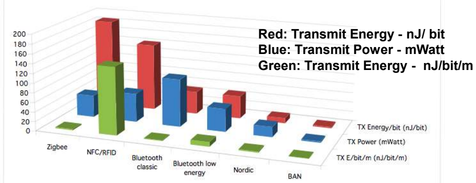
	AES-128 – symmetric-key (128-bit security)	ECC-163 – public-key (80-bit security)
Latency (# cycles)	226	86,200
Power (μW)	3.7	7.3
Energy per bit (pJ/bit)	65	38,600
Technology (μm)	0.18	0.13

2

44

Power/Energy for communication

[G. Dolmans, Imec NL][Singelee+15]



1 μJoule transmit budget
- 300 bits in BAN
- 11 bits Bluetooth
- 3 bits Zigbee

1 μJoule crypto
- 11,000 bits AES
- 500 bits SHA-3
- 0.2 point multiplication

Slide credit: Ingrid Verbauwhede
45

Mutual authentication protocols

[Singelee+15]

Radio for BAN networks in healthcare (2.4GHz ULP OOK)
[Vidojkovic+11]

	ISO 9798-2 (AES-128) (128-bit security)	Randomized Schnorr (ECC-163) (80-bit security)
Communication (nJ)	473 (94%)	1396 (10%)
Crypto (nJ)	31 (6%)	12,655 (90%)
Total (nJ)	504	14051

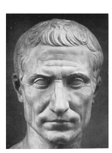
But different tradeoffs for local storage protection

46

Many applications need authenticated encryption

https://competitions.cr.yp.to/caesar-submissions.html

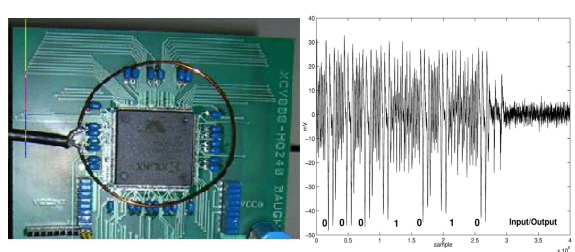
ACORN
AEGIS
AES-OTR
AEZ
Ascon
CLOC and SILC
COLM
Deoxys
JAMBU
Ketje
Keyak
MORUS
NORX
OCB
Tiaoxin



Results of CAESAR competition: late 2017

47

Physical attacks: costly countermeasures change the implementation tradeoffs



48

If a large quantum computer can be built...

- all schemes based on factoring (RSA) and DLOG (also ECC) are insecure [Shor'94]
- symmetric key sizes: x2 [Grover'96]

49

The Crypto Stack

- Implementations
- Specifications
- Standards
- Protocols
- Modes
- Primitives
- Assumptions

reduction proofs are very valuable
more automation needed
question models
be careful with assumptions

It is possible to build a cabin with no foundations, but not a lasting building.
Eng. Isidor Goldreich (1906-1995)

50

The Crypto Stack

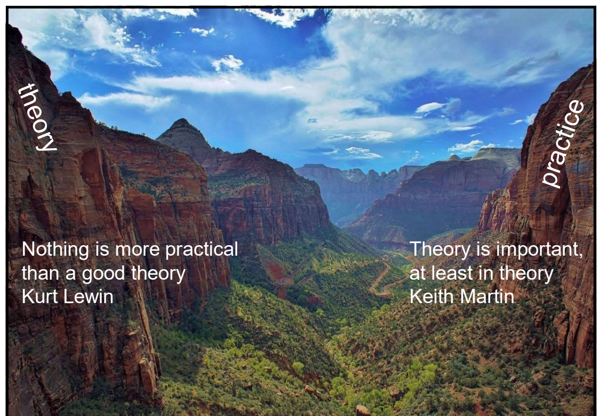
- Implementations
- Specifications
- Standards
- Protocols
- Modes
- Primitives
- Assumptions

much more work needed here:
automation
e.g. miTLS

which problems are hard?

A hard problem is a problem no one works on
James L. Massey

51

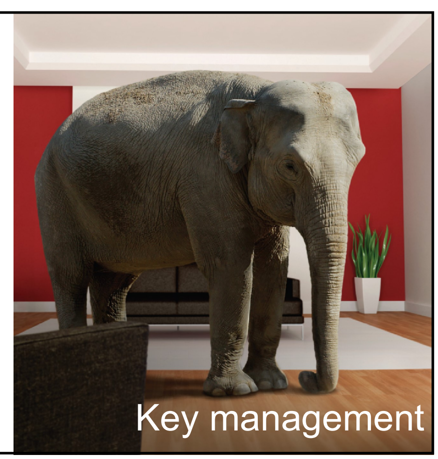


52

Crypto Life Cycle

Crypto design	Kleptography
Hardware/software design	Hardware backdoors
Hardware production	
Firmware/sw impl.	Software backdoors
Device assembly	Adding/modifying hardware backdoors
Device shipping	
Device configuration	Configuration errors
Device update	Backdoor insertion

53



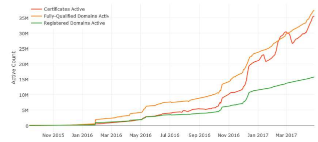
Who will hold the keys? Who will update the keys? And who will revoke them?

- Symmetric key: GSM
  - bad key management: 1 key for every user
  - government access
  - large scale breach waiting to happen
- Secure Element provisioning

PKI and key management: web ecosystem

- 12M + 35 M SSL/TLS servers
- 3-4 billion clients
  - 650 CA certs trustable by common systems
  - Comodo, Diginotar, Turktrust, ANSSI, China Internet Network Information Center (CNNIC), Symantec
  - fake SSL certificates or SSL person-in-the-middle as commercial product or government attack
  - Flame: rogue certificate by cryptanalysis

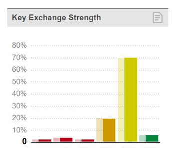
Let's Encrypt
live since November 2015
https://letsencrypt.org/isrg/



[Holz+] TLS in the Wild, NDSS 2016 [Stevens] Counter-cryptanalysis, Crypto'13

PKI and key management: web ecosystem

- Slow upgrade from SSL 3.0/TLS 1.0
  - SSL 2.0: 1995
  - SSL 3.0: 1996
  - TLS 1.0: 1999
  - TLS 1.1: 2005
  - TLS 1.2: 2008
  - TLS 1.3: 2017?



- Snowden (2013) for Perfect Forward Secrecy
- Poodle (2014) was needed to kill some of SSL 3.0
- Secure update and negotiation?
- Certificate transparency?
- DANE
- CA Authorization?

Architecture is politics [Mitch Kaipor'93]

Control:

avoid single point of trust that becomes single point of failure

Stop massive data collection

big data yields big breaches (think pollution)

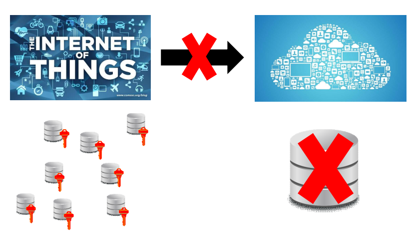
this is both a privacy and a security problem (think OPM)

Governance and Architectures

Back to principles: minimum disclosure
- stop collecting massive amounts of data
  - local secure computation
- if we do collect data: encrypt with key outside control of host
  - with crypto still useful operations

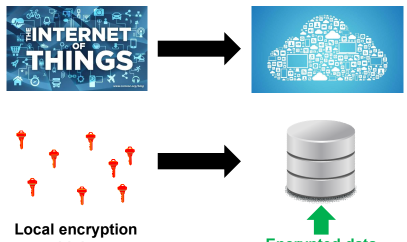
Bring "cryptomagic" to use without overselling
- zero-knowledge, oblivious transfer, functional encryption
- road pricing, smart metering, health care

From Big Data to Small Local Data



Data stays with users

From Big Data to Encrypted Data



Local encryption with low multiplication depth

Encrypted data
Can still compute on the data with somewhat Fully Homomorphic Encryption

61

Open (Source) Solutions

Effective governance

Transparency for service providers

62

Conclusions

- IoT technologies bring major privacy and security risks
  - we cannot afford to continue the “deploy now and fix later” model
- Need to rethink everything
  - architectures: where is the data and who controls it?
  - design of building blocks
  - deployment (including supply chain)
  - secure update mechanisms
- Need open solutions with open audit
- Support: legislation (economic incentives) and non-proliferation treaties
- Essential to protect human rights

63