Situational security, controlled privacy

Session: Advanced technologies for a hyper-connected society including security aspects

6th Japan-EU Symposium on ICT Research and Innovation

7th October 2016

Klaus Moessner

k.moessner@surrey.ac.uk

It's always about people, citizens, users!!!

Complexities and forecasts

The drive towards automatism and need for knowledge

Domains

- Transport
- Logistics
- Assisted living
- Energy
- Entertainment
- Work/workflows
- Finances
- …

Information Sources

- Personal profiles (1 each? or rather n?)
- Personal sensors
- Environment sensors
- Our history with…
- Public information
- …

Knowledge producers (current)

- Data analysts
- Banks and account hosts (energy, water, etc)
- Google, Amazon, and alike
- Fitness service providers, health care providers
- Insurances
- ..

Complexities and forecasts

We want something that is simple and handles all of this

Complexities and ownership

Who owns my data and how can I control it?

Traditionally through accounts and passwords…

- Increasing number of online representations (number of passwords registered to ONE email account
- What if we forget them?

- And what about the handling of data from our sensors?
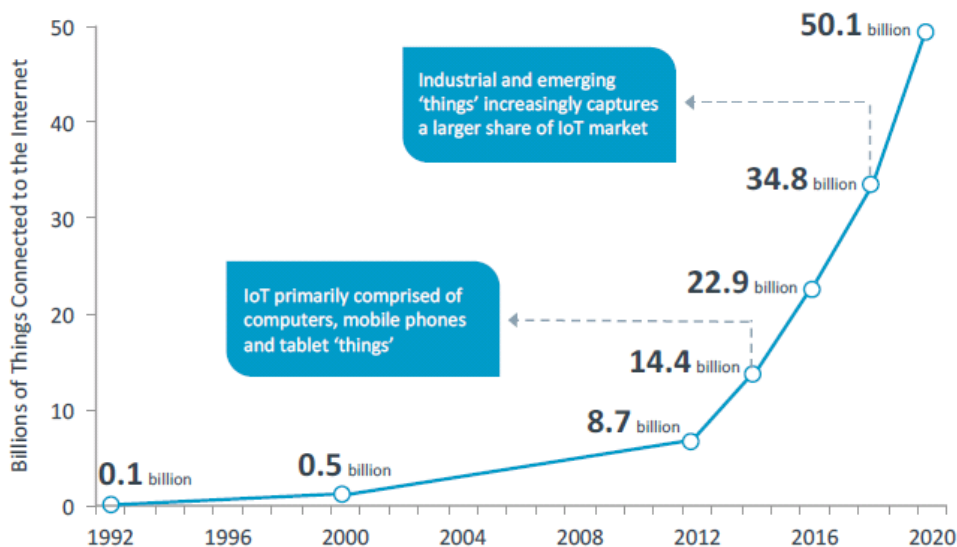- What about the handling of knowledge generated on information from and about us?

We have an overwhelming password problem

COMPANIES

Amount that sent passwords in **PLAIN TEXT** when customers requested to reset their passwords:

10%

GOOD NEWS: THAT IS LESS THAN BEFORE!

INDIVIDUALS

Number of times the average person reused their favorite password:

4

US	ROW	UK	FR
4	4	6	9

11   22   46

Infographics from: https://blog.dashlane.com/

Complexities, ownership and threats

And what about sensing and Io generated/harvested information?

Projecting the 'Things' Behind the Internet of Things

From 2014-2020, IoT grows at an annual compound rate of 23.1% CAGR

Industrial and emerging 'things' increasingly captures a larger share of IoT market

IoT primarily comprised of computers, mobile phones and tablet 'things'

Billions of Things Connected to the Internet

- 50.1 billion (2020)
- 34.8 billion
- 22.9 billion
- 14.4 billion
- 8.7 billion
- 0.1 billion (1992)
- 0.5 billion (2000)

CompTIA

Sources: Group SJR | Cisco | CompTIA

- • 7 connected sensors/things per person in 2020

- • How many in 2025, 2050?

Complexities, ownership and threats

The "Domains" and "knowledge producers have also problems…

- User interaction changes and reveals much more about us

- Meaning the choice of devices/platforms becomes a matter of trust

...Do People Care About Privacy...
Or Do They Care About *Who* Has Their Data?

Amazon Echo
The Echo's Alexa Voice Service listens to all speech in default mode

Google Gboard
Integrated keyboard for iOS devices that had an estimated 500K+ downloads within the first week of launch
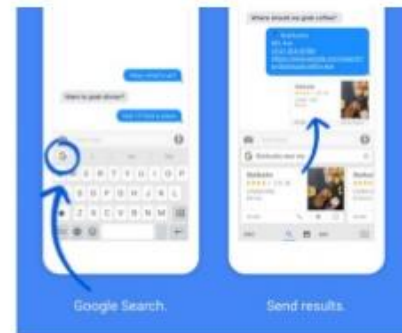
Google Search.   Send results.

@KPCB

KPCB INTERNET TRENDS 2016 | PAGE 211

Complexities, ownership and threats

Trust is easily lost, and takes a long time to be established

Consumer Data Privacy Concerns Rising Rapidly

How Concerned are You About Data Privacy & How Companies Use Customer Data?

4%
46%
50%

45%
Are more worried about their
Online privacy than one year ago

74%
Have limited their online activity
in the last year due to privacy
concerns
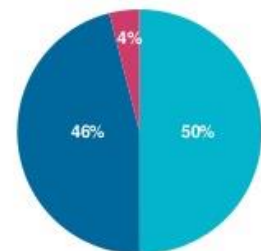
- Very Concerned
- Somewhat Concerned
- Not Concerned

@KPCB

KPCB INTERNET TRENDS 2016 | PAGE 309

Recent high level cases:

- TalkTalk in UK (customer data and account information hacked)

- Yahoo (huge number of accounts hacked)

… and many more...

Complexities, ownership and threats

..and these issues do not even think about IoT… remember we do all this to make user's life easier, to keep their trust they need to have (at least) some engagement
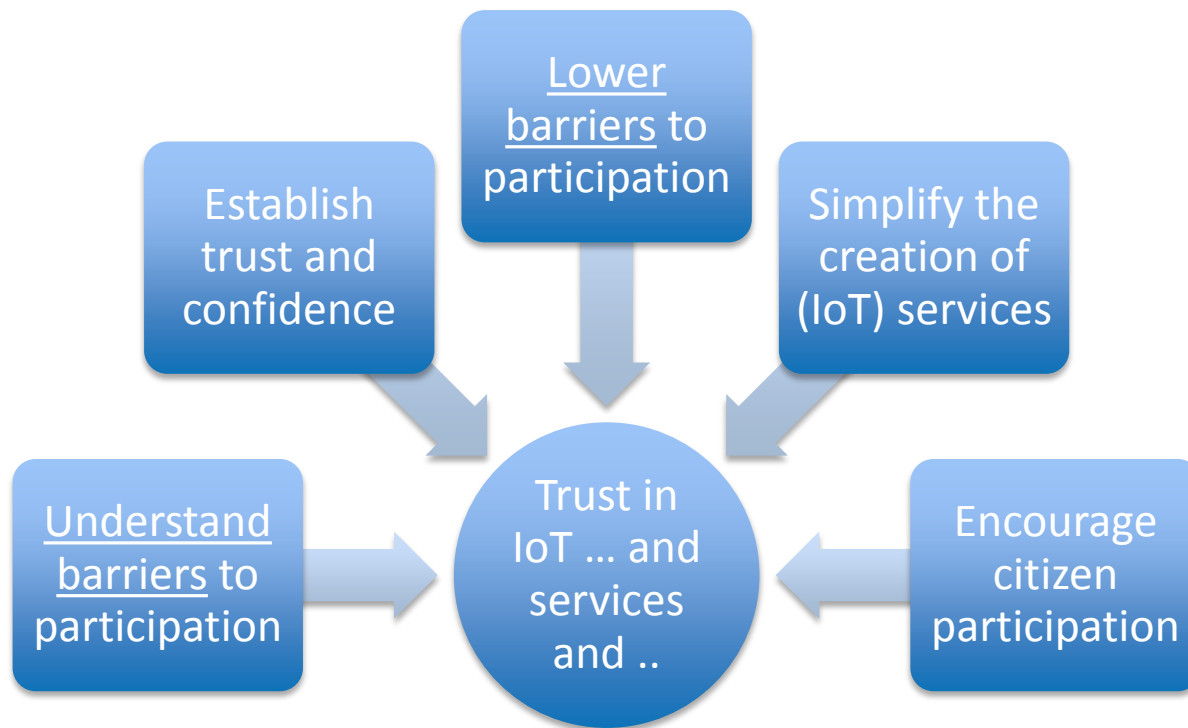
This means

The old approaches don't work anymore and new ones emerge

Data Security & Management as a Platform = Ionic Security

THEN Securing Infrastructure to Keep Data Safe

NOW Ionic Security

Distributed data protection & management platform that has processed tens of billions of API requests to enable customers to secure & control their data

@KPCB

Advanced approaches
for the advanced challenges of a hyper-connected society

Ionic security is but a start!

But this will not be enough, looking at the user:

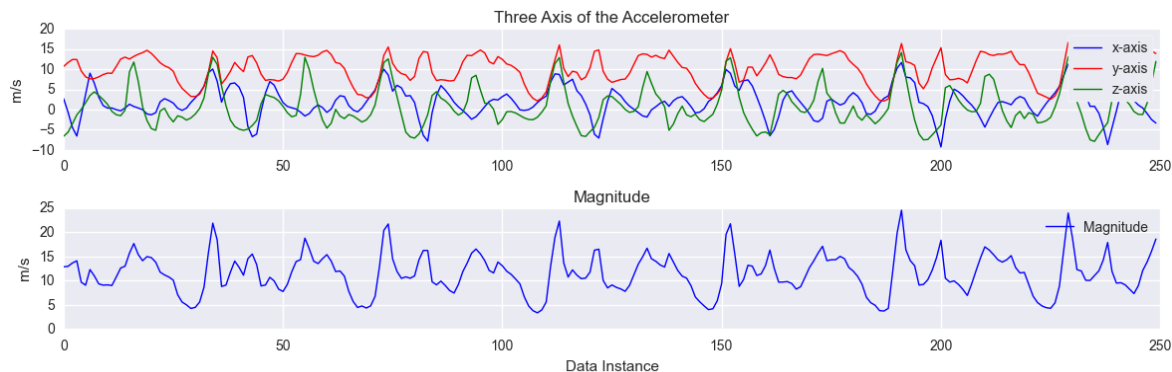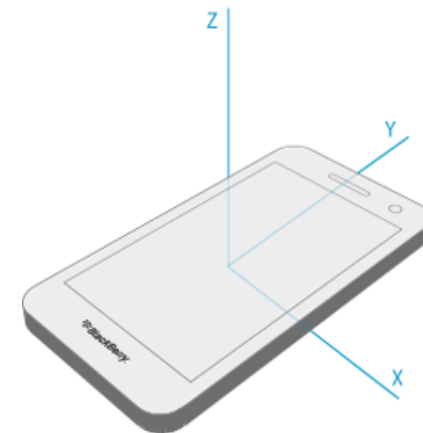Technology solutions for identification – authentication

Autonomous authentication

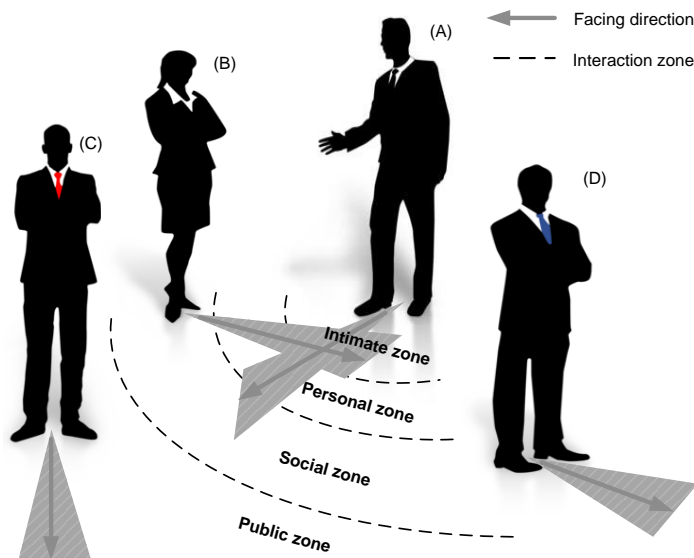- Biometrics (iris, voice, … gait)

smart phones have a variety of sensors.

– Accelerometer

– Gyroscope

The accelerometer is often used to perform gait recognition.

Technology solutions: identification - authentication

Interpreting social interactions to drive privacy settings

Utilising facing direction and relative orientation for detecting social interaction.

- Detect face-to-face interactions:
  - Based on off-the-shelf smartphones
  - No external hardware
  - Opportunistic sensing
  - Privacy preserving

- Key Concepts:
  - Interpersonal distance estimation
  - Relative orientation computation
  - Collaborative sensing

Still not enough, look at the knowledge producer:

The billions of connected things need also to be considered!
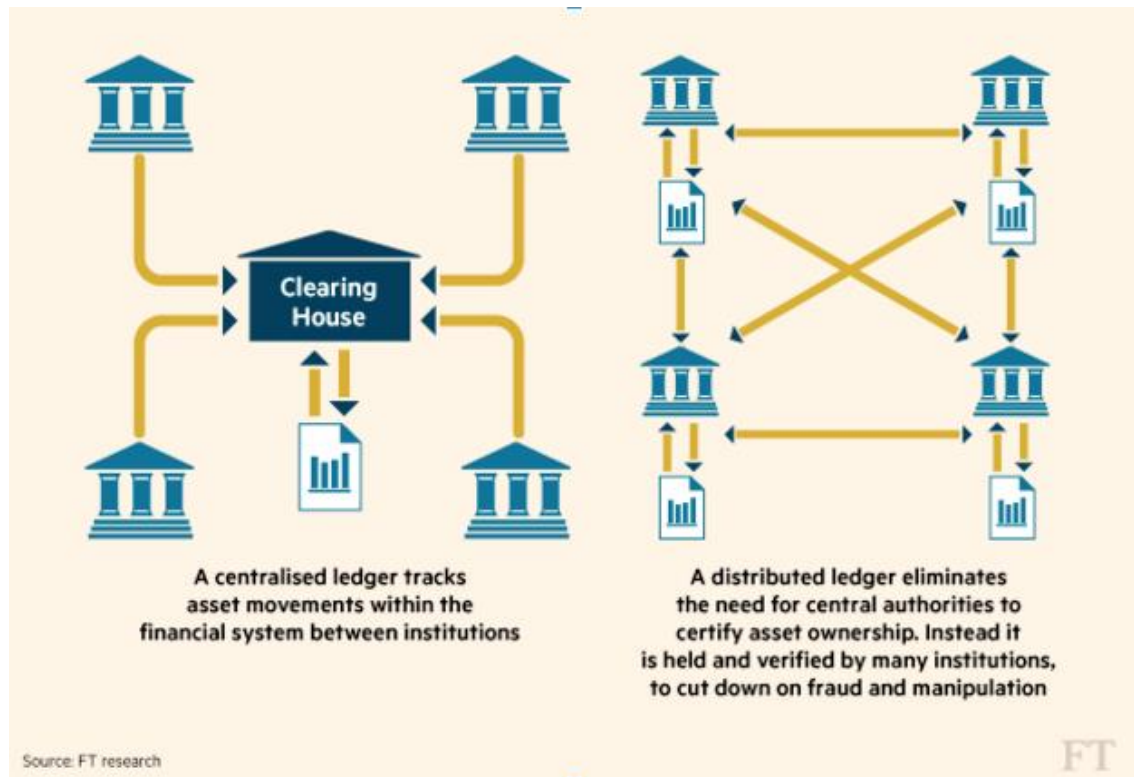
Observations:

- Centralised solutions will not work
- Cloud deployments will be rather challenged as well if the number of devices increases to the extend ("1000 sensors per person…") foreseen
- Different tiers of information/knowledge need different treatment
- Meta knowledge handling will be extremely important

Promising approaches

Solutions that may help solving the dilemma

- Distributed Ledger Technology ("Blockchain")

- Not a panacea, but a pretty good start

A centralised ledger tracks asset movements within the financial system between institutions

A distributed ledger eliminates the need for central authorities to certify asset ownership. Instead it is held and verified by many institutions, to cut down on fraud and manipulation

Source: FT research

FT

Promising approaches

Solutions that may help solving the dilemma

- Distributed Processing ("Cloud Edge Processing")

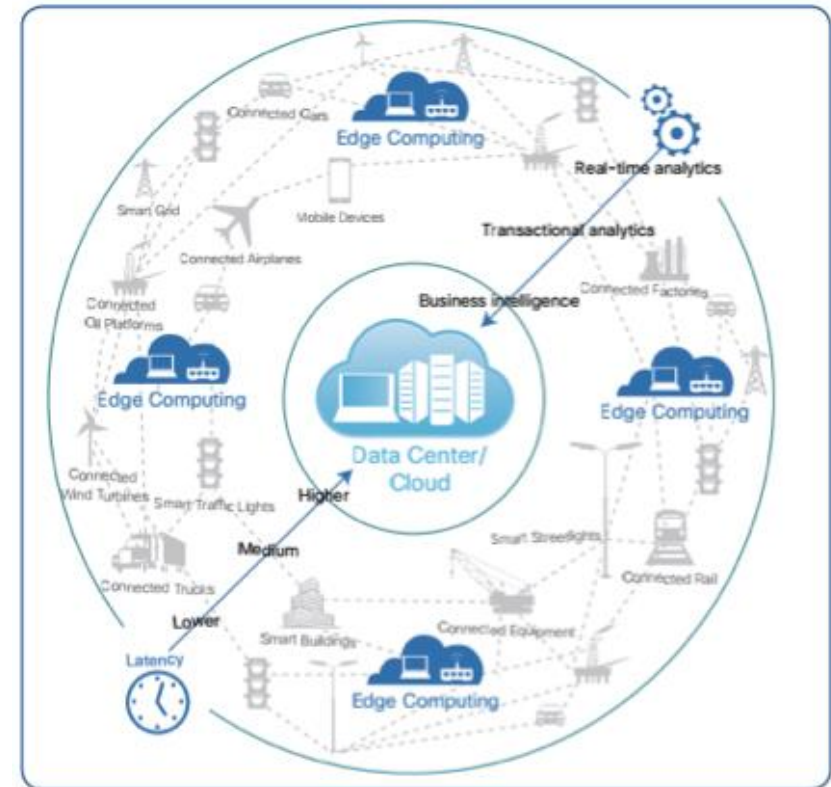For users:

- multi dimensional authentication at the edge

For devices:

- knowledge generation at the edge (otherwise we will never meet real time requirements)
- source identification (raw data, meta data and knowledge)

For data:

- Facilitate history tracking of data, meta data and knowledge

Source: Cisco, 2014

Klaus Moessner, k.moessner@surrey.ac.uk

http://www.surrey.ac.uk/feps/people/klaus_moessner/

@klamoe

Some of our IoT Projects