Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

Playing Smart Devices and Being Protected – Myth or Reality ?

Moderator

Wolfgang Leister

Panelists

Harald Gjermundrød

Florian Kammueller

Arno Wagner

Dmitry Namiot

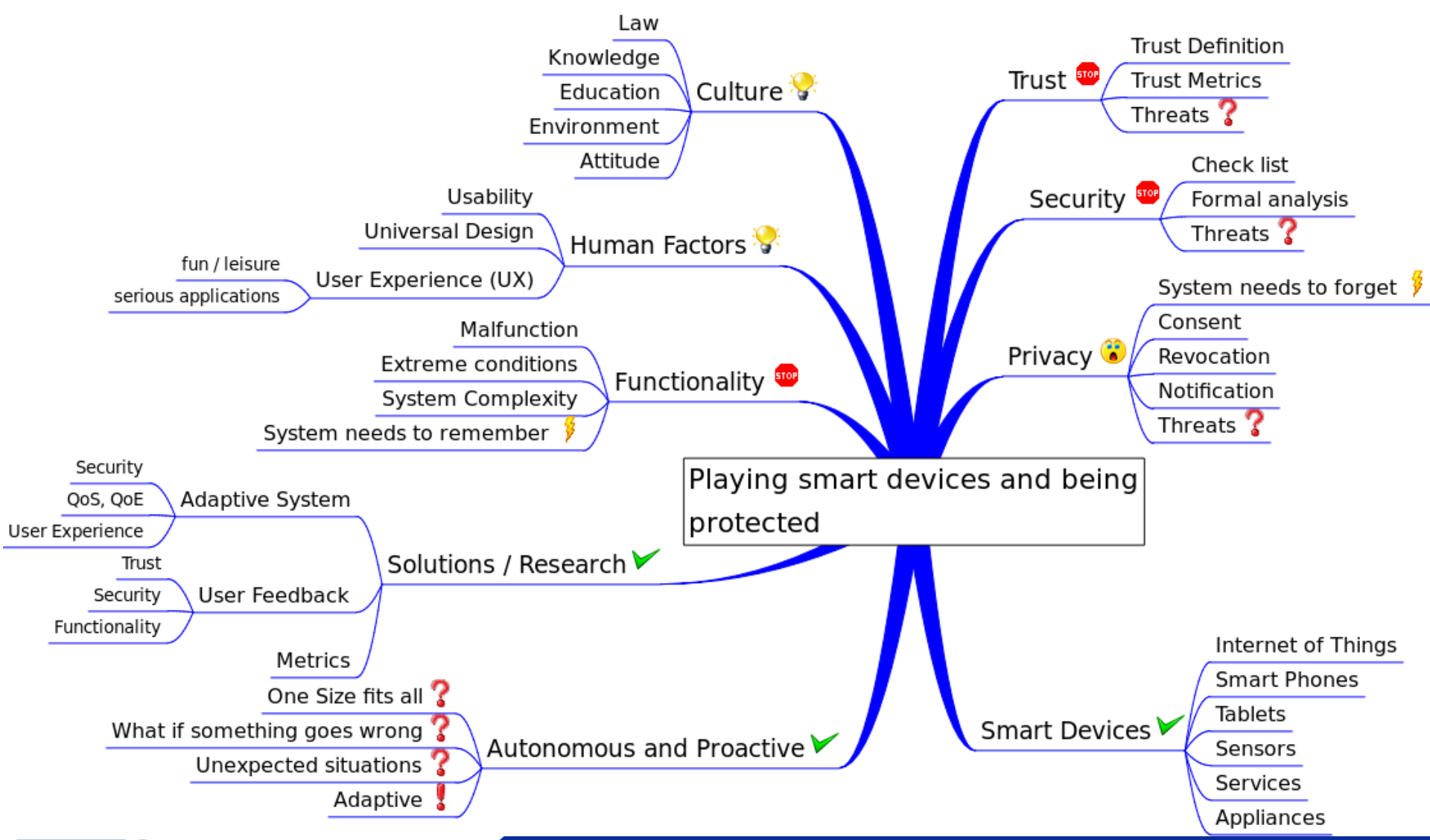
Yuval Beck

De claris mulieribus, Giovanni Boccaccio, 15th century

SMART 2012

May 2012 – Stuttgart, Germany

Playing Smart Devices and Being Protected



Discussion Elements

- Playing vs. Protected ?
- Trust, Security, Privacy
  - What are the Threats ?
- The role of culture and human factors ?
- Functionality vs. Protected ?
- How to evaluate ?

De claris mulieribus, Giovanni Boccaccio, 15th century

Playing Smart Devices and Being Protected: Myth or Reality

F. Kammüller

Middlesex University London

ICIMP12

Stuttgart, 28. May 2012

Protection and Security

Issues with Mobile Device Security

- Physical security of device (SmartCards)
- Independent of Network Technology: Authentication (GSM)

$\Longrightarrow$ Protocols and attacks

- General security problem: organisational security (insider attacks)

Physical Security Issues: Smartcards

- Example SIM cards
- Critical question: *can opponent obtain unsupervised access to the security device*

$\Rightarrow$ *Yes* for smartcards

- Keys are stored on card!

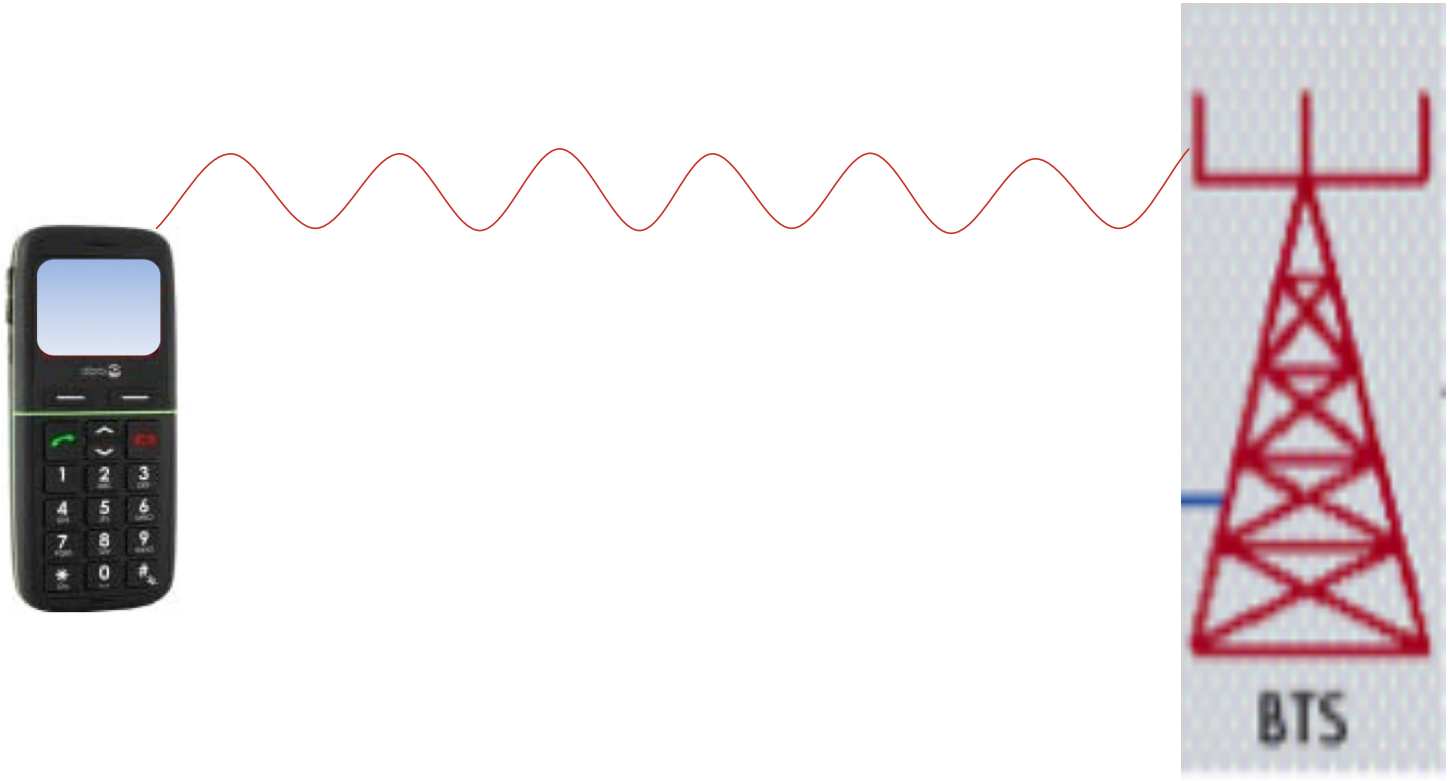
$\Longrightarrow$ Logical attacks (produce glitches to jump security code)

$\Longrightarrow$ Use probing needles and ion beams to manipulate physical layer of chip

Protocol issues: Incomplete Authentication in GSM

Global System for Mobile Communciations (SIM-card/mobile phones)

- Connection uses only one sided authentication: mobile phone is challenged but not vice versa

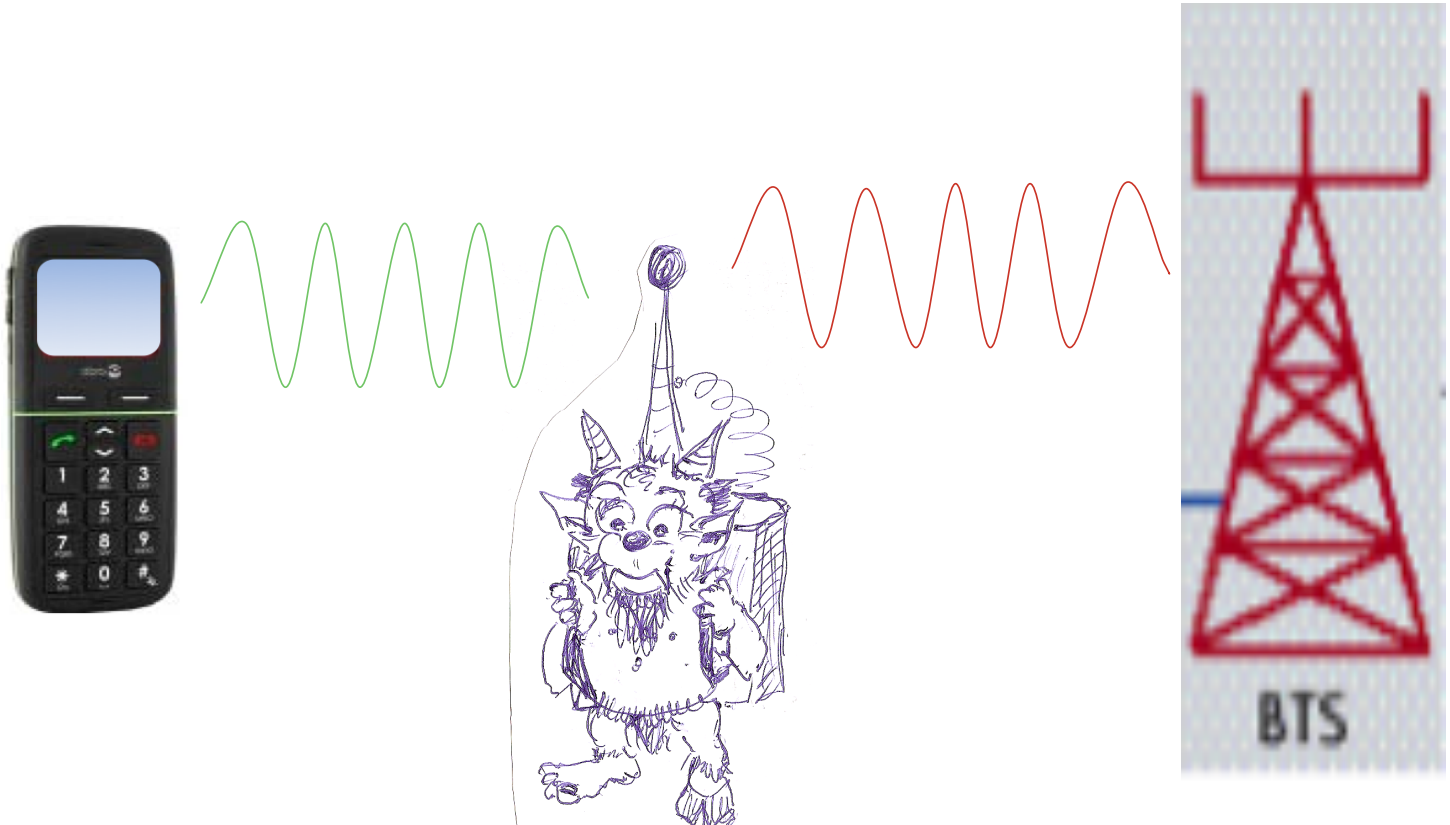


Protocol issues: Incomplete Authentication in GSM

Global System for Mobile Communciations (SIM-card/mobile phones)

- Connection uses only one sided authentication: mobile phone is challenged but not vice versa

$\Longrightarrow$ Malicious portable base station can launch a Man-in-the-Middle attack



Countermeasures?

- Physical attacks on cards:

$\Longrightarrow$ Active cards (battery) can delete data

- Protocol attacks

$\Longrightarrow$ formal specification, logical analysis (e.g. modelchecking)

Problems beyond Physical Attcks and Authentication

- Social engineering attacks (for example, phishing)
  - Use cognitive bias (`www.micosoft.com`)
  - Make user disclose security sensitive

$\Longrightarrow$ Integrate physical, logical and organisational security

★ Improved security models

★ Model various system aspects in one model

Panel For:
The Seventh International Conference on Internet Monitoring and Protection (ICMP 2012)

The First International Conference on Smart Systems, Devices and Technologies (SMART 2012)

May 27 - June 1, 2012 - Stuttgart, Germany

In auto drive to become an online celebrity for 5 minutes

Harald Gjermundrod
Assistant Professor

UNIVERSITY OF NICOSIA

Power of Information

- Teenagers upload a substantial amount of their private life online and it seems that privacy is not an issue.
  - If you are not online and everybody doesn't know exactly what you do at any given time then you are a nobody.
- A person may regret in the future all the information that were posted and can be viewed by a future employee or wife/husband/child.
  - How can information be deleted in our digital world?
- Control of large amount of information is POWER
  - Power should always be shared and regulated
  - How can this be done with the borderless Cyber World?

Some Questions for the Future

- Information that is posted (and replicated) online is hard (if not impossible) to remove.
- With more smart devices, more information with higher fidelity can be made available even in real time.
- When will the autonomous small devices be made available? If so who is responsible for the material that they may share with the rest of the world?
- Are we approaching a 1984 world? But it is not the government that is monitoring all the actions but the large cooperation. And the citizens are providing the information voluntary (at least at the time the information was uploaded).

Solution to Protection of Privacy

- Educate the teenagers and/or citizens
  - We all prefer to learn through our own mistakes, instead of the mistakes of our parents/teachers
  - But luckily for the older generations there are no photos/videos poster everywhere
- Universal Legal Frameworks
  - Will any legal framework be accepted universally and will it be able to keep up with the relentless progress of technology?
- Technical Solution (Sci-Fi)
  - Can we make data disappear automagically?

Sci-fi Vision

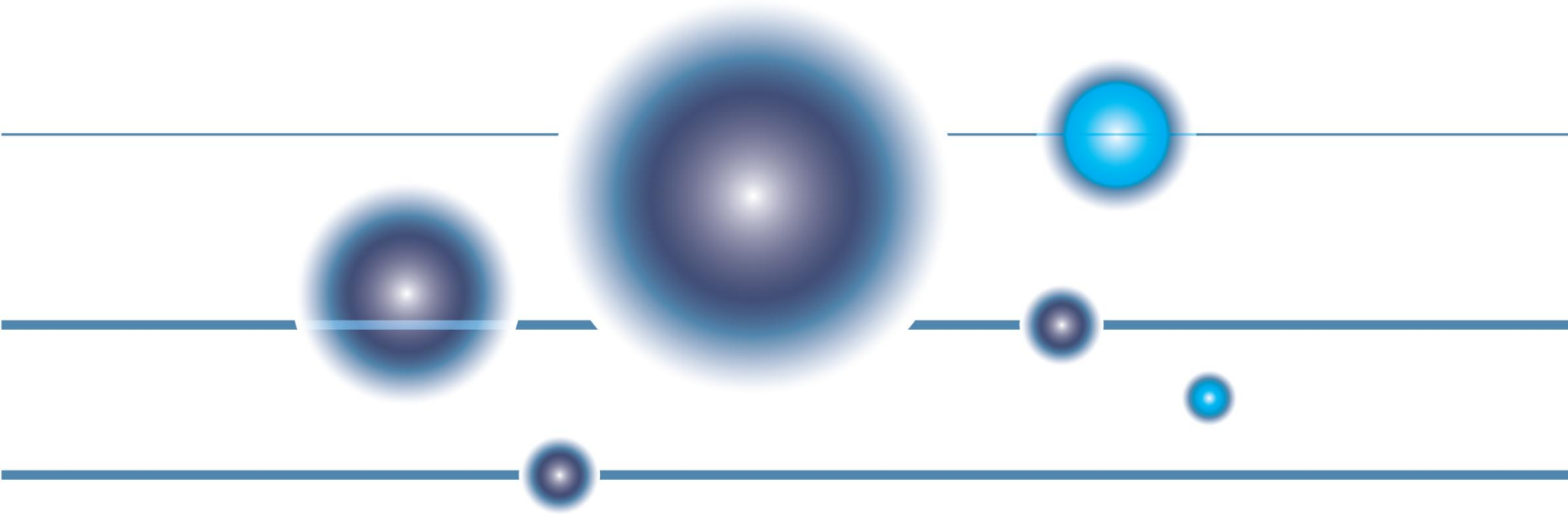
- By Definition: Data is passive

The BIG question
Can we make Data Active ??

Thank you for your attention!

Discussion, Comments, Viewpoints?

More info contact me:
harald@unic.ac.cy
www.cs.unic.ac.cy/harald



Consecom AG – ICT Security Consulting

Panel Contribution ICIMP 2012:

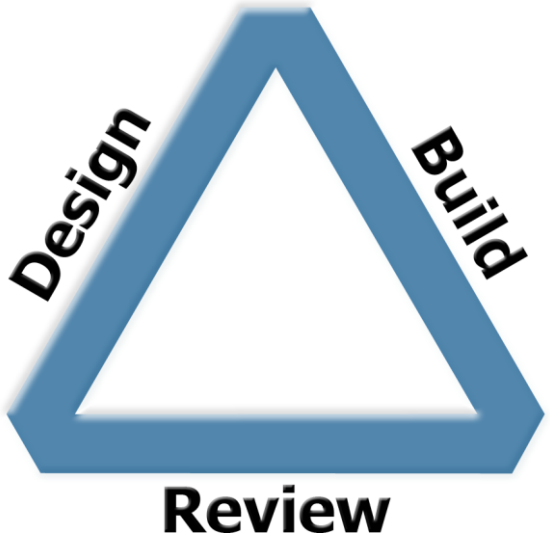
Security of Smart Devices

Consecom AG
Bleicherweg 64a
CH-8002 Zürich
http://www.consecom.com

Dr. Arno Wagner
Arno.Wagner@consecom.com

Consecom AG – Your Partner for Strategic ICT Security Consulting

- **Design**
  - Creation of strategies, organizational structures , processes, solutions, policies, security concepts
- **Build**
  - Implementation and integration of custom solutions
  - Project management
- **Review**
  - Audit, review, penetration testing, assessment of governance-structures, processes, technologies, algorithms, plattforms and infrastructures
  - 2nd Opinion, research projects



Security of Mobile (Smart) Devices

- Current Status: Not good
- Outlook: Will get worse

Reasons:

- Mobile OS security is not very good
- Malware creators are still learning
- Opportunities to monetize attacks are growing
- Mobile devices are becoming more widespread => more targets
- OS „rot“ is not (yet) in full bloom
- ...

The situation should stabilize in a few years (on lower level than today).
It will improve eventually, but *when* is everybodys guess.

Current Special Topics

➢BYOD (Bring Your Own Device):

This is a real catastrophe!

- Makes professional system administration impossible
- Most devices will not even have amateur-level administration
- Heterogenity can be extreme
- Rich field for malware, targetted attacks, etc.

Although in the very long run, this may be the standard model and it may even work!

➢„Walled Gardens“:

Harm more than they help

- Only delays platform compromise
- Users do not like them (JailBreak detection gets negative votes in the AppStore)
- When the inevitable happens, nobody is prepared
- Users will be even less aware of the risks

So, what can be done?

- IT Security in general is an awareness and education problem (And still a research problem as well!)
  - May take decades to fix
  - Efforts so far are not very impressive
  - Needs a changed mindset
  - Need long-term thinking (not possible today for mobile devices)
- Mobile security is in its infancy. The technologies are not mature

- Consumer IT still moves to fast for solid, long-term engineering
  - Not even hardware has a reasonable lifetime
  - New services get established fast
  - A lot of emergent properties (i.e. surprising behaviour) can be observed
  - Development is often done by people that do not have the expertise to handle the dynamics. (Developers often do not even see that they may have a problem...)
  - Business/management strategies often (typically?) ignore technological realities

Consecom AG – Global Vision – Swiss Values

Thank You!

Consecom AG
Bleicherweg 64a
CH-8002 Zürich
http://www.consecom.com

Dr. Arno Wagner
Arno.Wagner@consecom.com

Playing Smart Devices and Being Protected: Myth or Reality

Dmitry Namiot
dnamiot@gmail.com

Lomonosov Moscow
State University

SMART 2012

What is a myth?

- “Playing smart-phones is privacy-dangerous” is a myth
- Devices alone cannot hurt the privacy.
- The usage model – what is actually hurt

Where I am?

- Within 3 hours: Moscow and Far East
- Cross posting does not correspond
- Is it privacy problem?

Girls Around Me

Dmitry Namiot
http://servletsuite.blogspot.com

Navizon ITS: Google Analytics Indoor

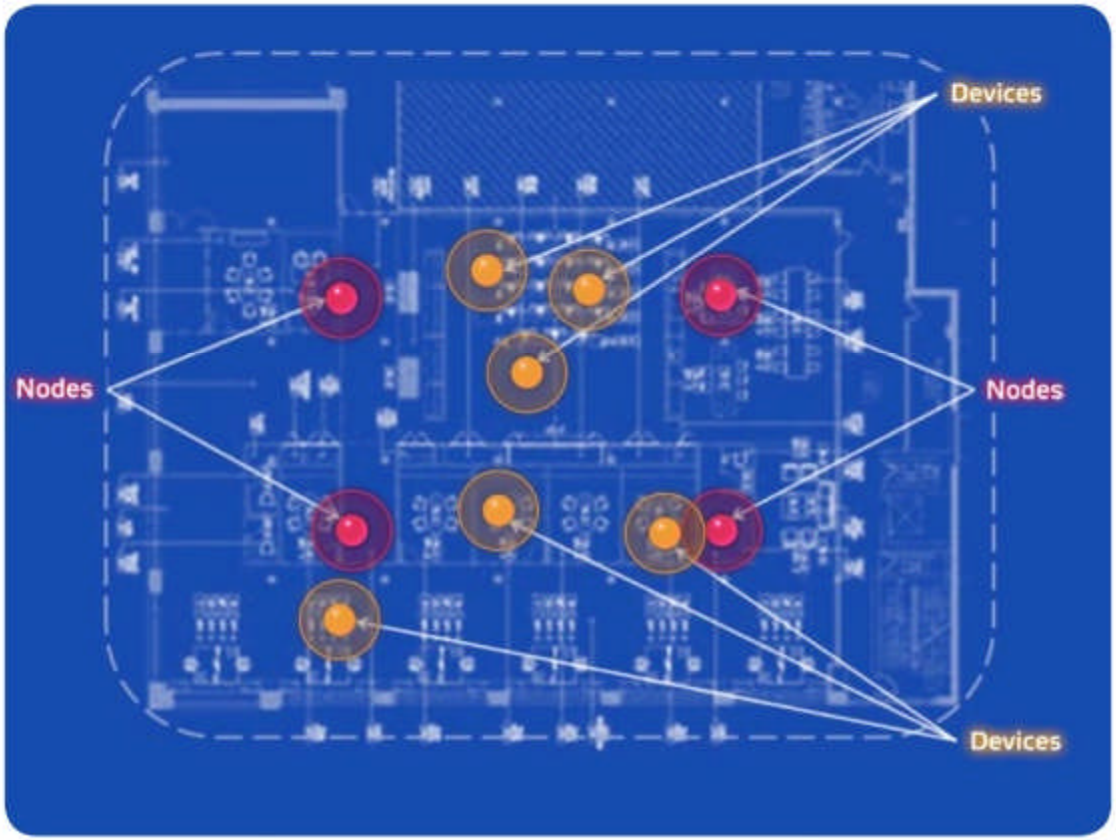
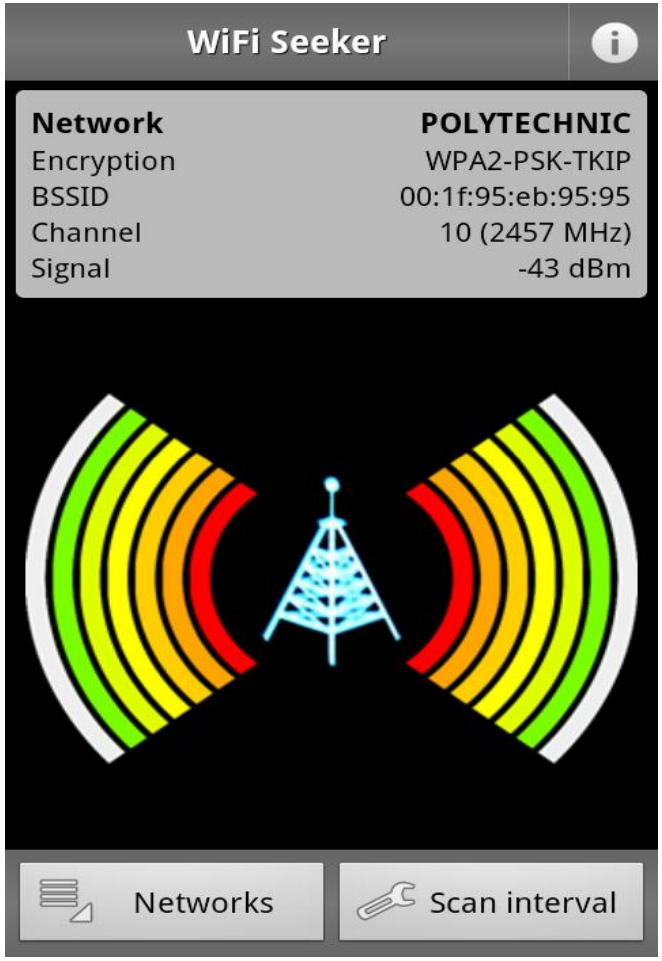
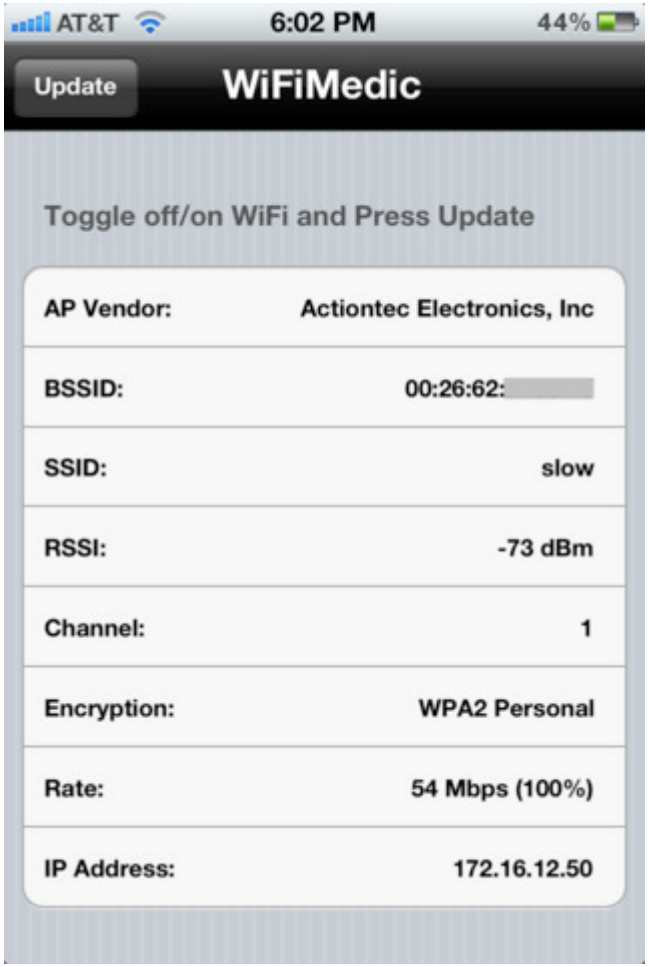


Figure 1: Sample Navizon ITS floor plan

Dmitry Namiot
http://servletsuite.blogspot.com

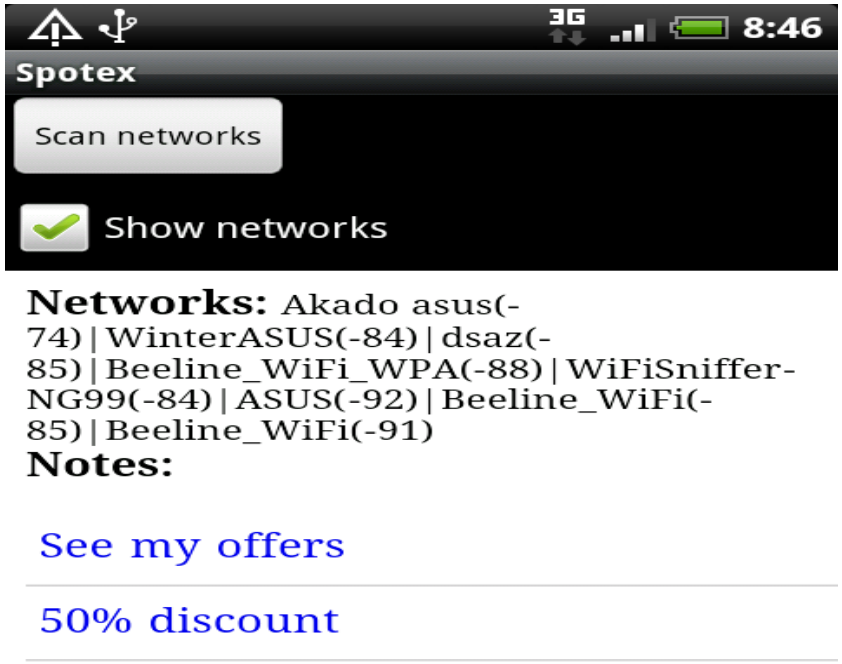
Wi-Fi related applications





Dmitry Namiot
http://servletsuite.blogspot.com

Client’s application

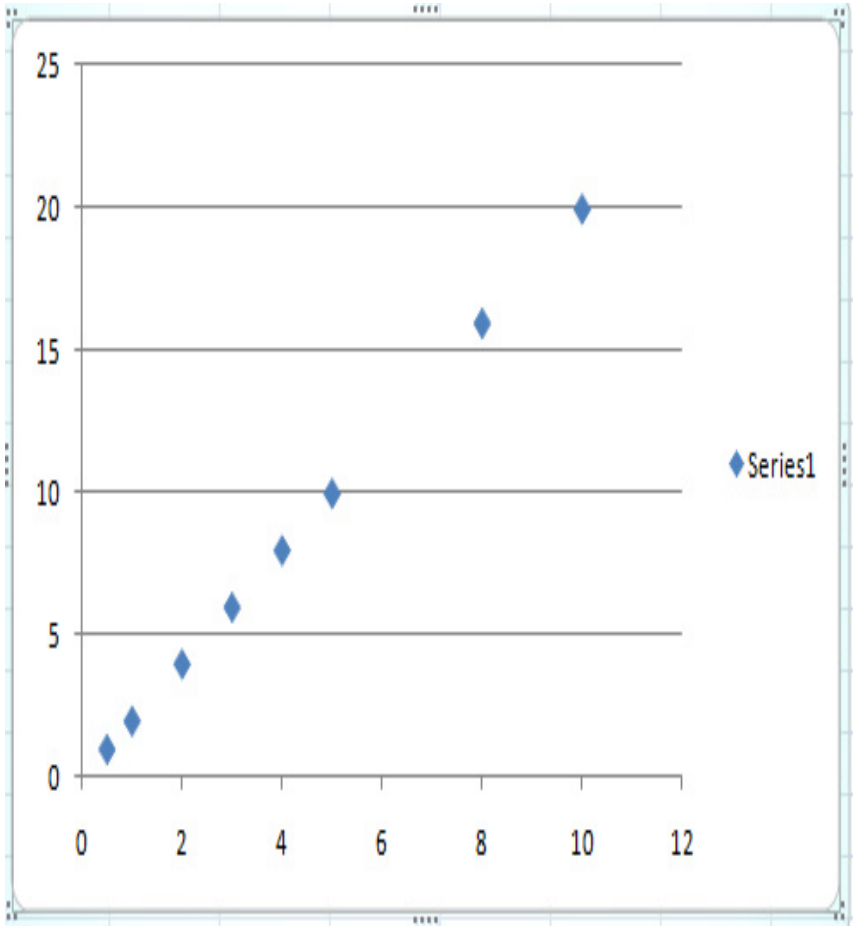


- Client-side application
- Shows visible networks
- Shows working rules (conclusions)

Wi-Fi chat

- Hyper-local communication tool based on SpotEx
- Web chat and communication forum for the mobile users nearby the same Wi-Fi access point

Proximity & Big Data



- Global UUID for anonymous clients: MAC-address
- We can collect stats associated with context (Wi-Fi access ponts)
- Example: clicks vs. visits

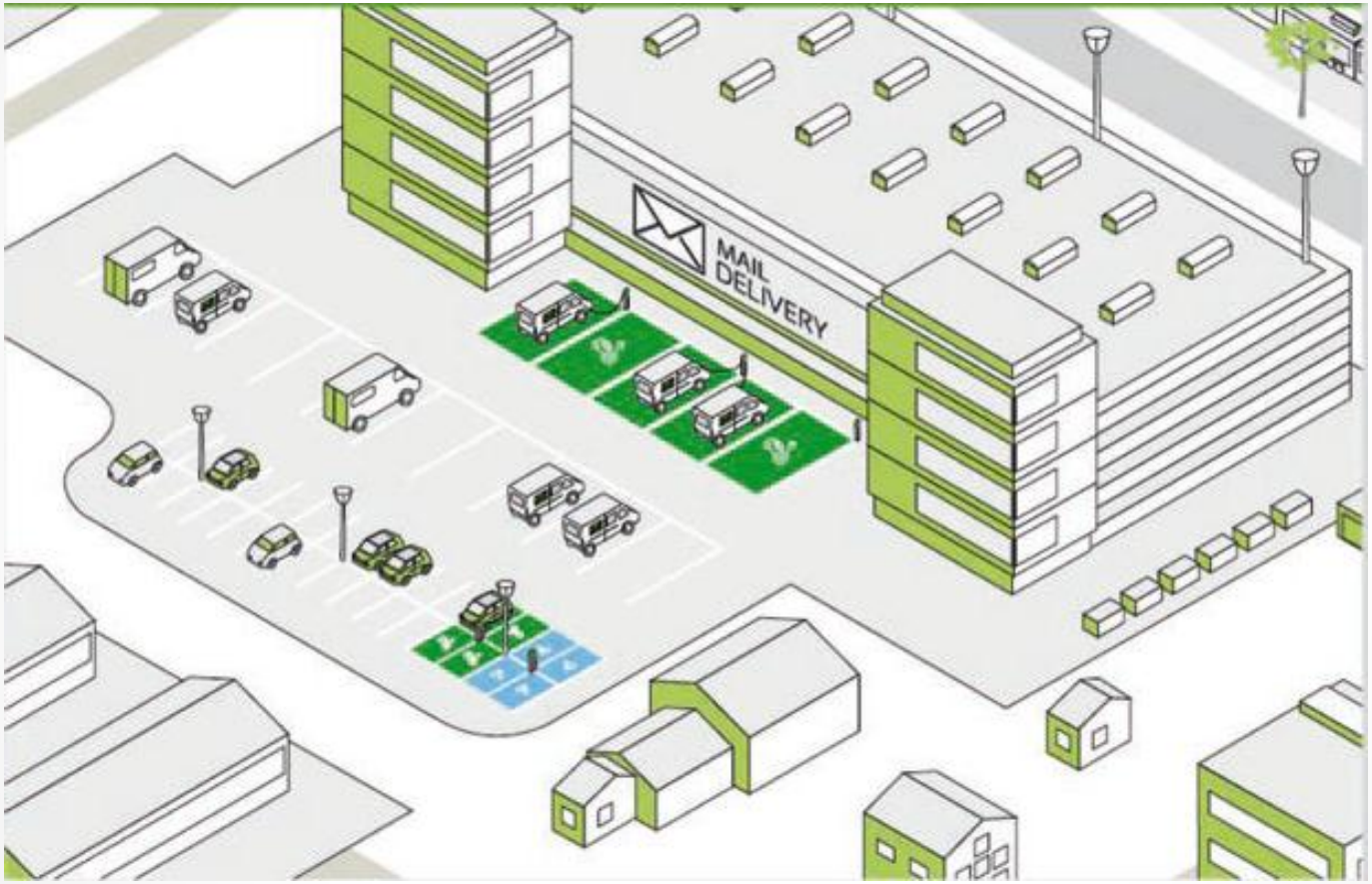
Geo Messages

- Share location as a signature to message (email, SMS)
- Peer to peer sharing
- No 3-rd party server with location info

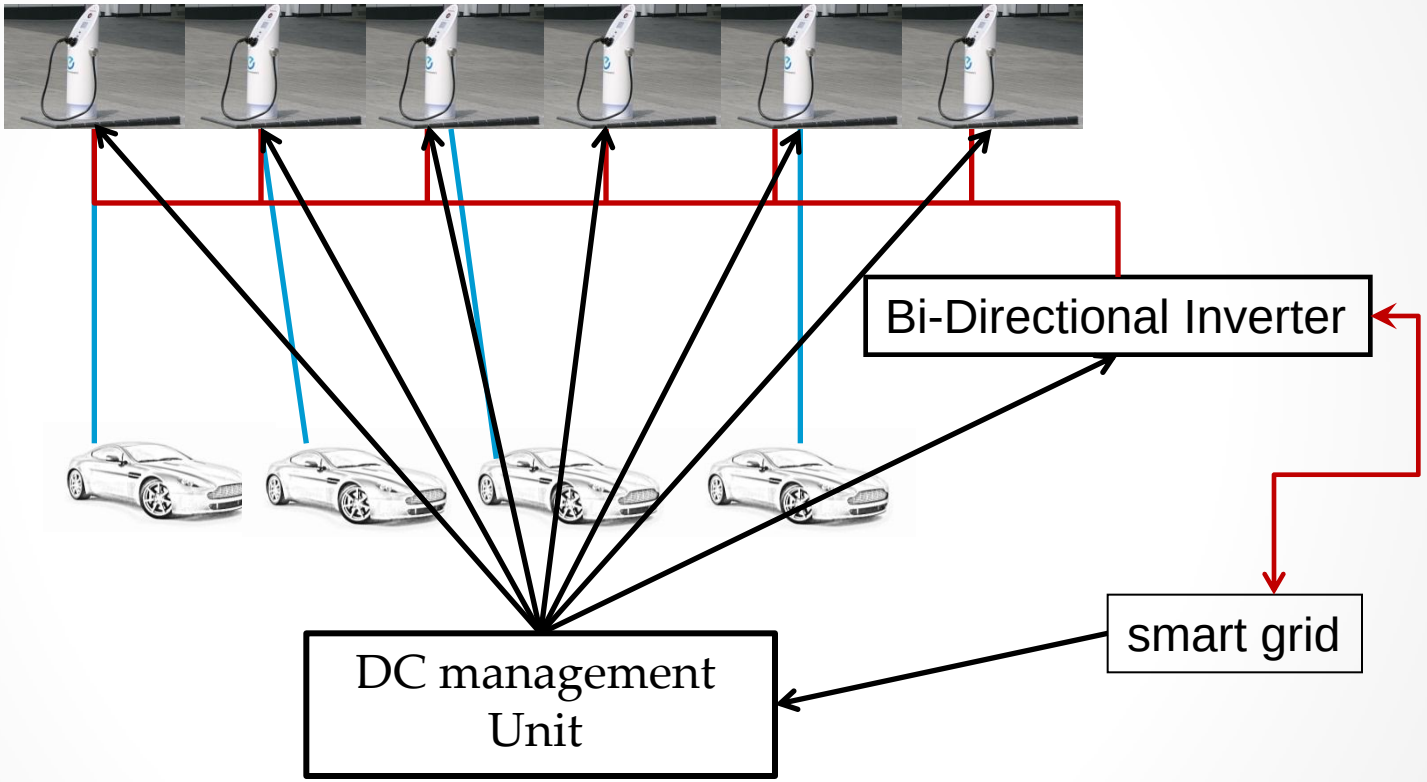
Non Instructive Algorithms for managing EV's

Dr. Yuval Beck
HIT 2012
Smart 2012 May 27- June 1

Commercial area



Commercial area Charging stations



Non intrusive algorithms

- guarantee electric vehicle availability (charged enough for next station).
- **Recognize the owner.**
- **Build owners profile**
- **Estimate the time of stay**
  - Owner feeds the data.
  - **Data mining.**
- Priority decision.

Non intrusive algorithms

- Compatible to smart grid data.
- **Commercial offer to the driver by data from owner recognition and smart grid data.**
- Informs driver of charging urgency and directs to the nearest charging spot with optimizing time management.
- Since it is a crucial system security protocols in all levels of communication.


TJY007
Ken Hayakawa
THANK YOU
FOR LISTENING
聞いてくれて有り難う。
9 120006 459228
www.tjumy.com
www.myspace.com/kenhayakawa
booking: office@tjumy.com
that side
A Little House In The Deep Blue Sea
深く青い海の中にある小さな家。
this side
Thank You For Listening
聞いてくれて有り難う。
For The Moment
今この瞬間だけ
austro mechana
℗2010 the copyright in this sound recording is owned by tjumy records
tjumy records - tjumy records - tjumy records - jum jum
tjumy records - tjumy records - tjumy records - jum jum - www.tjumy.com - office@tjumy.com - LC11288 - made in eu - all rights reserved - © 2010 tjumy records