European Commission

Digital Footprint in a Mobile Environment

Proceedings of a workshop at JRC Ispra

Jan Löschner, Pasquale Stirparo, Vincent Mahieu, David Shaw, Stefan Scheer, Ioannis Kounelis

2012

Report EUR 26051 EN

Joint Research Centre

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Stefan Scheer
Address: Joint Research Centre,
E-mail: stefan.scheer@jrc.ec.europa.eu
Tel.: +39 0332 78 5683
Fax: +39 0332 78 9007
https://ec.europa.eu/jrc

JRC71644

EUR 26051 EN

ISBN 978-92-79-32352-2 (PDF)
ISBN 978-92-79-32353-9 (print)

ISSN 1831-9424 (online)
ISSN 1018-5593 (print)

doi:10.2788/59068

Luxembourg: Publications Office of the European Union, 2012

Abstract
On 28th and 29th of November 2011 the Citizen Digital Footprint Action (CIDIPRINT) organised a workshop on "Digital Footprint in a Mobile Environment". The workshop was aiming to turn the current debate on 'privacy vs. security' into a collaborative approach to define privacy with embedded security.
This required:
• To understand what are the problems and approaches related to security;
• To understand the concerns related to privacy, their foundations and the actual concrete risks;
• To identify possible solutions to such problems and risks, as well as directions where research should point to;
• To identify the points of intersection, complementarities and conflicts.

Outline of the workshop: The workshop brought together representatives of privacy and security in order to work on a win – win approach. It was oriented towards facilitating an open and constructive debate between the security and privacy promoters. Experts on both sides were encouraged to reconsider the current technical measures in order to reconcile in an innovative way the various trends.
These proceedings summarize the discussion on outstanding questions such as:
• The role of public debate in the policy making process related to security?
• Can privacy be used as a design criterion for security systems?
• How to combine privacy and security? The workshop helped to develop the groundwork for follow-up discussions and actions to converge vs. a consensual goal.

Table of Content

List of participants

Panoptykon Foundation: Katarzyna SZYMIELEWICZ, lawyer, co-founder and executive director
Privacy International: Alexander HANFF, head of Ethical Networks
Nokia: Janne UUSILEHTO, head of Product Security
TU-Berlin/ T-Labs: Collin MULLINER
Independent security researcher: Vincenzo IOZZO
Italian Data Protection Authority: Elia FLORIO
University of Milan: Giuseppe VACIAGO, attorney, lecturer at Univ. of Milan
Politecnico di Milano: Stefano ZANERO, professor at Politecnico di Milano
uTrustIT Project: Daniel PETRO
Webinos Project: Andrea ATZENI
ENISA: Demosthenes IKONOMOU
JRC: Jan LOESCHNER, Mehmet COLAK, Vincent MAHIEU, Stefan SCHEER, Lothar BREITENBACH, Laurent BESLAY, Pasquale STIRPARO, Ioannis KOUNELIS, Maurizio BAROFFIO, Gianmarco BALDINI

1. Introduction

1.1. Rationale

The increasing need for security in mobile IT environments is apparent in every aspect of our society. The need for tools and instruments to perform related policy assessment is becoming a priority. Security measures related to the profiling and identification of individuals tend to raise privacy concerns in our technological world. A commonly expressed concern is that security might only be enhanced at the expense of privacy, or vice versa. This has clearly led to a controversy on security policies related to the protection of citizens from organized crimes and terrorism as well as cybercrime and lawful interception.

The Digital Footprint of a citizen, in a growing mobile and digital society, forms a common threat in current debates on security vs. privacy. Rapid changes in technology are challenging the concepts of security and reasonable expectations of privacy. The policy makers are expected to reach a balanced solution respecting security, privacy and economy. There is a need for clear understanding of the relevant issues and to aim towards trusted embedded security architecture for the next generation systems.

One of the objectives of the CIDIPRINT Action[1] is to develop and assess scenarios associated with information recorded when a citizen interacts in a digital smart environment, in particular with the internet of the future and with intelligent transport systems[2]. Moreover another deliverable[3] mentions the organization of an expert workshop at the Joint Research Centre (JRC) thus inviting stakeholders with relevant key projects and key clients in order to prioritise the elements of such an inventory.

At the time of the workshop one key document /1/ was about to be published thus describing the state-of-the-art of all types of digital footprints left behind by citizens while interacting in a digital environment.

1.2. Digital Agenda

CIDPRINT's work is mainly driven by key challenges put forward in the communication from the Commission "A Digital Agenda from Europe", in particular the action areas "2.3 Trust and Security" and "2.1 A Vibrant Digital Single Market". Within the Digital Agenda it is explicitly mentioned that if the citizen trust in digital applications and interactions is not or no more guaranteed (e.g. if derived use of his data is felt as an intrusion), then the use and development of the whole digital single market is at risk.

The border-less nature of digital transactions and communications to which the citizens are exposed in our days calls for a multi-disciplinary approach where the JRC can play a role in the definition of international standards and best-practice guidelines.

Hence one of CIDIPRINT's top priorities for 2012 is to look into cyber threats concerning mobile device applications like for example mobile payments or mobile cloud interfaces.

[1] CIDIPRINT stands for Citizen Digital Footprint; it is one of three actions of the Digital Citizen Security (G7) unit of the Joint Research Centre (JRC).
[2] Deliverable 01.1
[3] Deliverable 01.2

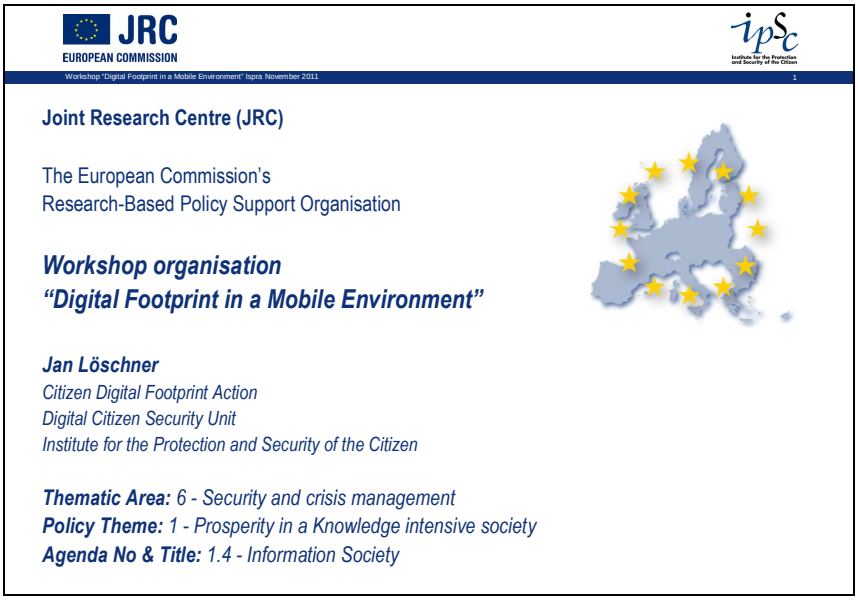
1.3. Workshop format and objectives

The format of the workshop was to let the participants give their presentations, each scheduled within a certain session, and followed by a short Q&A session; after the last session a round-table discussion was scheduled thus involving all presenters and all other participants.

The workshop was divided into four main sessions:

1. *Policy background* with the objective to strengthen trust and security of the European Citizen in a sustainable and inclusive ICT-based European society by scientific research on how emerging Information and Communication Technologies will impact on the security and privacy of citizens' daily life. In the balance between European security needs and fundamental citizen rights, the unit works on risk mitigation, on cyber security, data protection, privacy and other ethical considerations, and on the associated legal and regulatory frameworks.
2. *Technical challenges and security issues* with the objective to improve and develop technologies and methods further with the aim to make them trustworthy, privacy friendly, more security measureable and controllable to the stakeholders.
3. *Data and privacy protection* with the objective to know more about the current data protection legislation. One key challenge is to ensure that the same citizen's data, which are used in business and personal transactions, is also not used by unauthorized parties or "reused" in contexts or applications which can bring harmful consequences to citizen and businesses.
4. *Applications solutions* with the focus on the border between personal computers and mobile devices, which is now "blurred" in the sense that similar applications and services can be provided on both platforms.

1.4 Workshop organisation (J. Löschner, JRC) & final agenda



The final workshop agenda was as follows:

Digital Footprint in a Mobile Environment

28 November, 2011

12:30-14:00 **Lunch**
Offered by the JRC

14:00-15:30 **Session 1: Policy Background**
Jan Loeschner, JRC
"The citizen digital footprint between applications and EU regulations"

Katarzyna Szymielewicz, Panoptykon Foundation

Alexander Hanff, Head of Ethical Networks at Privacy International

15:30-16:00 **Coffee Break**

16:00-17:30 **Session 2 - Technical challenges for mobile security**
Janne Uusilehto, Head of Nokia Product Security
"Challenges in Software Security"

Gianmarco Baldini, JRC / iCore Project

Vincenzo Iozzo - Independent Security Researcher

Collin Mulliner - Researcher at TU-Berlin
"NFC and Mobile Payments Security"

20:30 **Social Dinner**
Offered by the JRC

29 November, 2011

09:00-10:30 **Session 3 – Data and Privacy Protection**
Laurent Beslay, JRC

Elia Florio, Officer at Italian Data Protection Authority

Demosthenes Ikonomou, ENISA

Giuseppe Vaciago, Attorney, Lecturer at University of Milan
"Geo-Location, Privacy and Data Retention in a Mobile Cloudy World"

10:30-11:00 **Coffee Break**

11:00-12:30 **Session 4 – Application Solutions**
Stefano Zanero, Prof. at Politecnico di Milano

Daniel Petro, uTrustIT Project

Andrea Atzeni, Webinos Project

Pasquale Stirparo, JRC

Ioannis Kounelis, JRC

12:30 **Lunch**
Offered by JRC

2. Presentations by participants

2.1 Session 1: "Policy Background"

2.1.1 J. Löschner (JRC)

Jan Löschner has a degree in Electrical Engineering from the Technical University of Ilmenau in Germany. He works as a Scientific Support Officer for Research, testing and evaluation of electronic equipment and he has more than 15 years experience in testing of security components. He has organised a number of instrument test campaigns as well for nuclear detectors as well as for electronic passports. He has contributed in advisory groups for international bodies like in IAEA and ISO. He was the JRC coordinator in a number of EC founded research projects such as PRIME and STABORSEC.

Citizen Digital Footprint - CIDIPRINT

Is one of the tree actions of the Digital Citizen Security Unit

is addressing the impact that new information and communication technologies have on the citizen.

The European citizen as an individual is put to the centre of the considerations that will address issues such as the acceptance of new ICT, data protection and privacy concerns, security ethics, citizen profiling and electronic traces.

Citizen Digital Footprint - CIDIPRINT

develop and assess scenarios associated with information recorded when a citizen interacts in a digital smart environment, in particular with the internet of the future and with intelligent transport systems

CIDIPRINT action and the Digital Agenda

The Digital Agenda for Europe

addressed issues like Trust and Security, a vibrant digital single market through building digital confidence and ICT-enabled benefits for the EU society and Intelligent Transport Systems for safer, more secure and more efficient transport and better mobility in Europe.

The CIDIPRINT action is committed to:

- Increase Awareness and Understanding
- Elaborate Suitable Answers to mitigate the possible drawbacks
- Foster the Digital Confidence

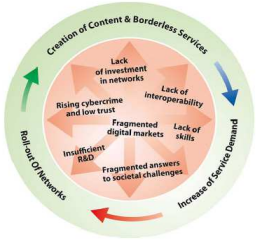
The Digital Agenda for Europe

The Digital Agenda is Europe's strategy for a flourishing digital economy by 2020.

It outlines policies and actions to maximise the benefit of the Digital Revolution for all.

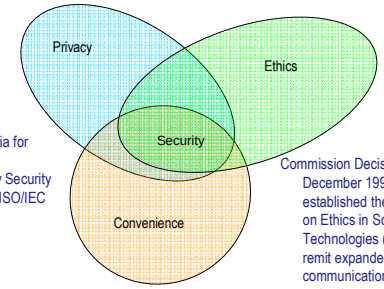
The overall aim of the Digital Agenda is to deliver sustainable economic and social benefits from a digital single market based on fast and ultra fast internet and interoperable applications.

http://ec.europa.eu/digital-agenda



ICT and its regulatory dimensions

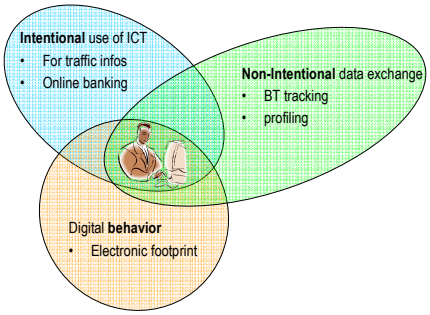
Lisbon Treaty → EU Charter on Fundamental Rights (Article 7: Privacy, Article 8: Data Protection)



Common Criteria for Information Technology Security Evaluation ISO/IEC 15408

Commission Decision dated 16 December 1997 (SEC(97) 2404) established the European Group on Ethics in Science and New Technologies (EGE). The EGE's remit expanded to include communications and information technology.

The Citizens an actor and an object regulated and regulator



The Citizens and the situation he is in…

Regulation will apply to:

- standard a situation
  - What is a standard situation?
  - How to get in and out of it?
  - Which services and data are available?
- An emergency
  - What is an emergency situation?
  - How to get in and out of it?
  - Which services and data are available and wanted by the citizen and a first responder?

A assessment method

To assess the impact of the digital society on the citizen the following approach will be considered: a decomposition of the digital foot print in 3 dimensions.

1: Trust and digital identification between Citizen and Processes

(Who is involved?)

2: Citizen Digital Data

(What information is dealt with?)

3: Digital Processing

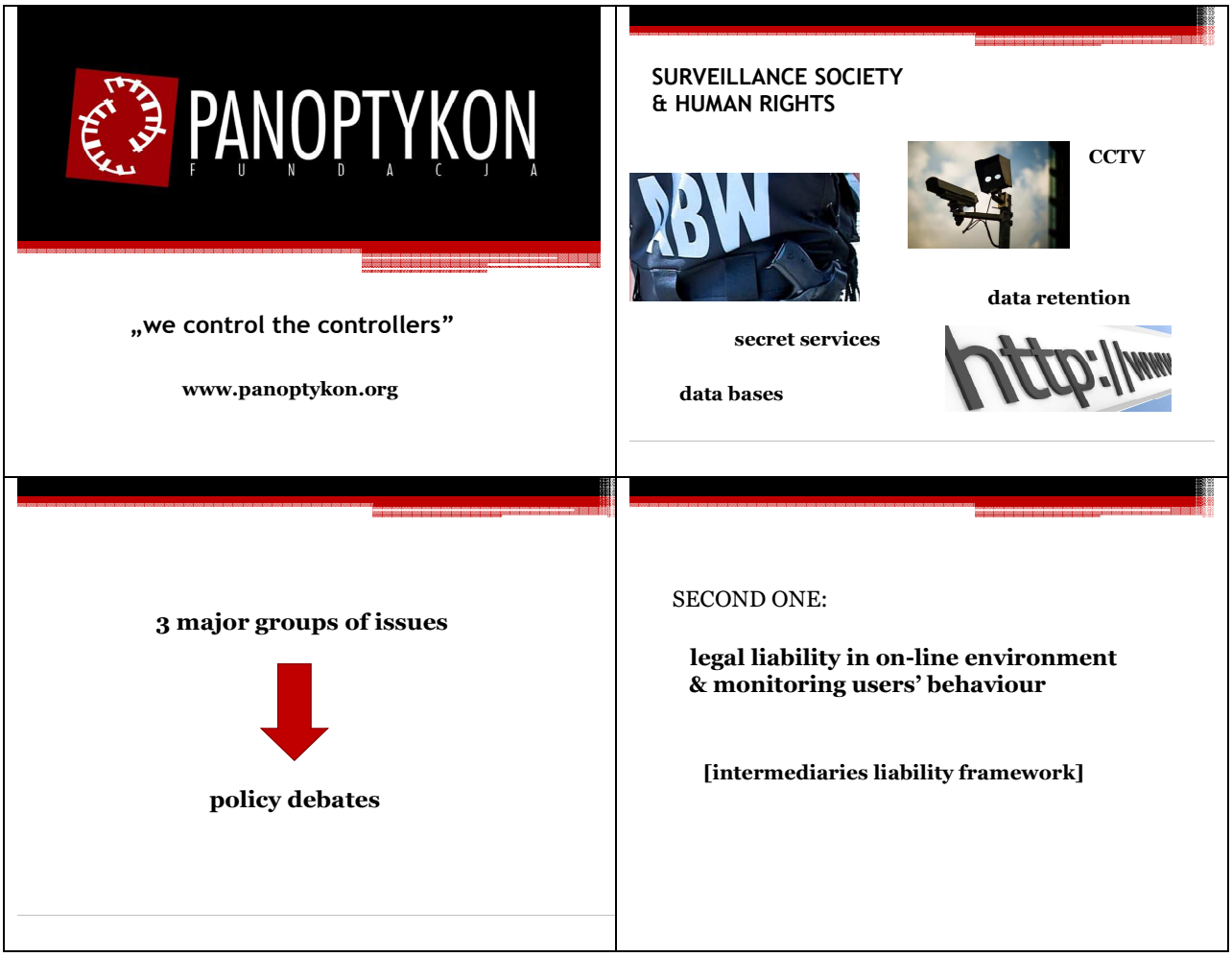
(How are the information processed?)

Mobile situations the citizen is in…

- Mobile interface to the internet, the cloud or a infrastructure
- The using of smart cards in mobile devices
- Possessing / moving with identifiable objects
- Moving as human (face / body recognition)

2.1.2 Katarzyna Szymielewicz (Panoptykon Foundation)

Katarzyna Szymielewicz is a human rights lawyer and activist. She is co-founder and executive director of the Panoptykon Foundation - the only Polish NGO working on surveillance society issues, a member of European Digital Rights Initiative. Panoptykon runs watchdog, think-tank and awareness rising activities. Currently her work is devoted mainly to digital rights - both monitoring abuses and advocating for a systemic change. She is particularly interested in data retention, Internet filtering and blocking, ACTA, Project Indect and similar projects.



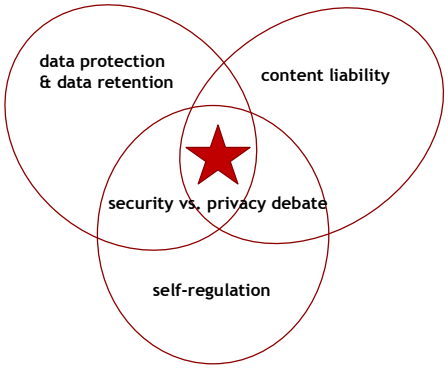
THIRD ONE:

how to regulate these areas of business activity ...

& whether self-regulation is an option

privatisation of law enforcement?

- **main areas: child protection and intellectual property enforcement**
- **European Commission encouraging ISPs to become a sort of "internet police"**
- **B2B agreements (UK, Poland)**
- **Vodafone and Orange campaigning *against* intermediary liability protections**
- **USA legislation (Protect IP Act, SOPA)**



challenges:

- **globalisation of web based services**
- **USA (Patriot Act, FISA)**
- **mandatory data retention regime (EU)**
- **lack of evidence of its „neccessity" for law enforcement**
- **EU-wide standards for data protection in vertical relationships**
- **more services to come – Internet of Things, smart grid, ubiquitous geolocation**

more problems...

- **tools of surveillance: what is legal, what is acceptable**
- **further use of „retained" data: crime detection, crime prevention or mass profiling?**

conclusions

➡ **need to reconcile more effective law enforcement on-line and respect for the rule of law**

➡ **the conflict between security and privacy is not a fact of life / it is an approach**

2.1.3. Alexander Hanff (Privacy International)

Alexander is a Privacy Advocate and Academic with a strong interest in politics, law, privacy and technology. In March 2005 Alexander made history when he answered a knock on the door - still in his dressing gown and not yet full of coffee, opened the door, only to be served with a lawsuit by Paramount, Twentieth Century Fox, Universal City Studios and Warner Bros. His supposed transgression: The movie studios suspect him of running a BitTorrent hub and helping people download copyrighted films via P2P technology. The MPAA (Motion Picture Association of American) has gone after numerous BitTorrent hubs on similar charges and managed to shut many of them down. The plot here is a familiar one. There are, however, a couple of factors that make Hanff's story unique. For one, the US studios served Hanff papers at his home - in England. Secondly, Hanff, 31, owns the DVDR-Core domain name and pays for its server, but he has never actually administered the site. That's done by a group of online friends that Hanff has never met in person. Lastly, Hanff plans to fight the movie studios, making him a rarity among BitTorrent hub owners.

Alexander Hanff gave an oral presentation; hence no slides can be presented herewith.

2.2 Session 2: "Technical Challenges for mobile security"

2.2.1 J. Uusilehto (Nokia)

Mr. Janne Uusilehto has a long experience in ICT industry. He began working with security related tasks as an IT Support and Electronic Banking Specialist; this took place in several Finnish banks. Latest position in a bank he held in Nordea (then Merita-Nordbanken) as a global Cash Management Specialist and product responsible for telecommunication areas of cash management software. Among other duties, Mr. Uusilehto was a member Nordbanken Cash Management Services team who initiated Internet sales portals in Finland in mid 1990's. Nokia recruited Mr.Uusilehto at 1998. His current position is the Head of Nokia Product Security, globally responsible for Nokia product security development. His team is the overall owner of Product Security and product security related education, awareness and process improvement tasks. Janne Uusilehto is also a member of several Nokia internal security related management boards, Nokia's main representative to Trusted Computing Group, Chairman of TCG Mobile WG, Strategic Director of Global Platform and Nokia's main representative and board member to SAFECode forum.

Nokia Research Center Demo

HW security is matter of choice an example

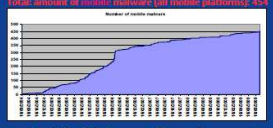
On-board Credentials (ObCs): Virtual credentials protected by on-board trusted HW

- Secure due to the use of hardware security unlike in software credentials.
- Inexpensive to deploy because of already deployed generic secure hardware.
- Open in spirit to multi-application smartcards, but without issuer control.
- Done by TPM.

Nokia Research Center

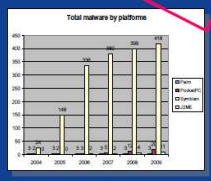
Mobile malware status – Year 2009

Getting mobile malware statistics is currently not feasible as increase is so small. ATTN: Web applications breakthrough may change this situation rapidly !!



Mobile Malware Development

Source: F-Secure Thu 26.11.2009



Note: According F-Secure they get about 200.000 malware samples every day. About 5000-6000 of them are real malware and few thousand of those completely new ones.

TOTAL CUMULATIVE AMOUNT over last 10 years of mobile malware for all mobile platforms is around 500.

http://www.tietokone.fi/uutiset/hypponen_rikolliset_alkavat_iskea_windows_7_aan

What is needed next?

1. We have gained an understanding of many secure development practices and are having success with broader adoption.
2. Are there any areas of the SEP/SDLC where more work is urgently needed?
3. There are plenty of standards existing in security area as well.
4. What are the challenges with implementing a secure development lifecycle?
5. How do business objectives fit into the picture?

Challenges ..

In following slides there are some examples of challenges in different areas of security and privacy of consumer systems (in random order).

Technical challenges

- Basically there are not much technical challenges, but ...
- Heat, energy consumption and bandwidth.
- How to verify security from binaries as well (App testing, malicious SW)
- How to utilize platform HW security for security critical apps
- How to secure Internet against cyber criminals, etc. (Redesign Internet?)
- ...

"Almost anything can be done technically, but ..."

Challenges with engineering

- Continuous systems security engineering education
- How to ensure suppliers skills for SW security engineering
- How to ensure 3rd party SW security engineering skills
- How to ensure good SW security verification/testing
- ...

"Difference between IT security and product security..."

Challenges with awareness

- How to ensure reasonable expectations towards to SW security
- Proper curriculum available for universities (engineering, design..)
- Safe use of Internet, education in schools (How to behave)
- User involvement: Usability, security (what to ask, what to trust)
- Visibility of reactive security and proactive security for general public
- ...

Challenges in policy & regulation

- How to ensure reasonable expectations towards to SW security
- Fair and reasonable liability sharing between players
- Reasonable global harmonization of SW security (US,China,EU,..)
- Lawful interception related issues harmonization globally
- Freedom of speech vs. controls & protection of information assets
- How to limit the risk of "over regulation" and keep the global markets functioning
- ...

Principles based regulation!!

"Secrity creates controls, controls create politics ..."

Challenges in process

- There is no absolute measure for SW security (product security)
- How to keep reactive SW security in right limits (90/10 -rule)
- What is the right role for certification (the true value of it)
- Business management involvement to requirements settings
- ...

Challenges in standards

- There are quite many already existing in security, privacy etc.
- Many are still "regional". Not many globally accepted (If any)
- How to ensure standard will enable progress not to block it
- Standardization is slow, but making new technologies is not
- ...

Many forums are already solving these challenges. Is it enough?

- 3GPP (Telecomm & network security)
- BSIMM (Security engineering management maturity)
- DIGITALEUROPE (Industry level issues in security & privacy)
- FIRST (Incident response)
- Global Platform (TEE ecosystem security)
- ICASI (Protect the Internet)
- Mobey (Mobile banking security)
- NFC (Wireless Payments Security)
- OMA (Content protection related security)
- OWASP (Internet application security)
- SAFECode (SW engineering Security)
- Trusted Computing Group (Systems security & HW security)
- ...

In a nutshell

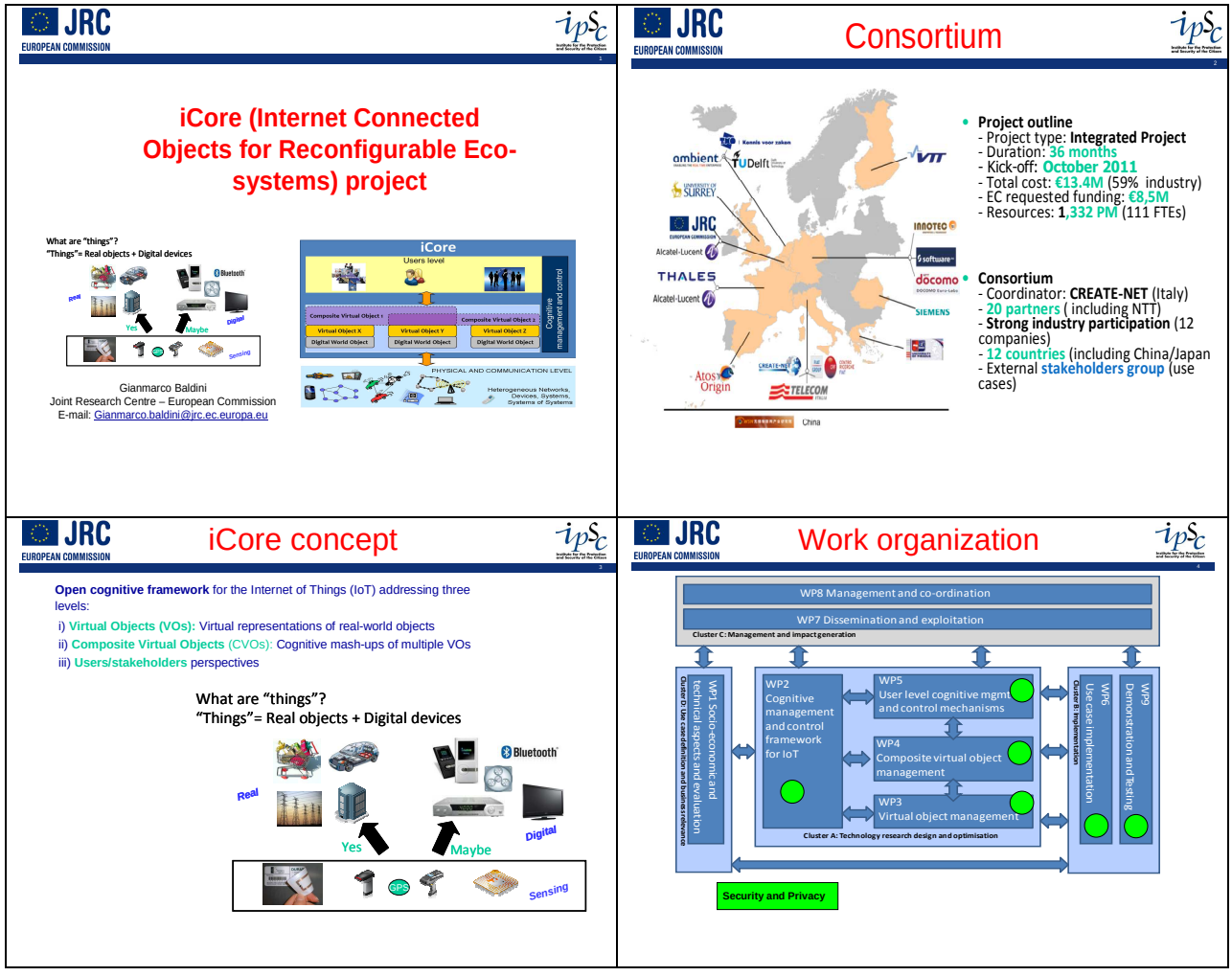
- There is a lot of industry collaboration already.
- Standards & interoperability are must.
- Mobile malware is a real threat.
- Security is enabler for privacy and trust.
- Most of the challenges are political and/or commercial.
- Technically it is possible to make secure systems.

Thank you!

NOKIA

2.2.2 G. Baldini (JRC, iCore project)

Gianmarco Baldini completed his Laurea degree in 1993 in Electronical Engineering from the University of Rome "La Sapienza" with specialization in Wireless Communications. He has worked for more than 16 years in the design, development and testing of wireless communication systems in the R&D departments of multinational companies like Ericsson, Lucent Technologies, Hughes Network Systems and Selex Communications before joining the Joint Research Centre in 2007. He participated to large-scale projects in Italy, Sweden, UK and USA on GSM/UMTS, TETRA and Satellite Communications, as Senior Technical Architect and System Engineering Manager. He is the current chairman of Working Group 4 in ETSI TC Reconfigurable Radio Systems (RRS), which is focused in Public Safety and Security aspects. He has authored or coauthored more than 15 publications in wireless communications, security and cognitive radio systems.



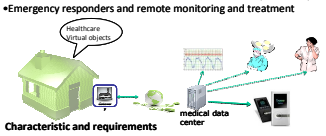
Use Cases

To show the applicability of the concept four use cases have been selected for demonstration:

- Smart city/transport-**Personalization of car**
- Smart home-**Living assistant**
- Smart office- **Easy meeting**
- Smart business-**Supply chain**

Smart home Living assistant

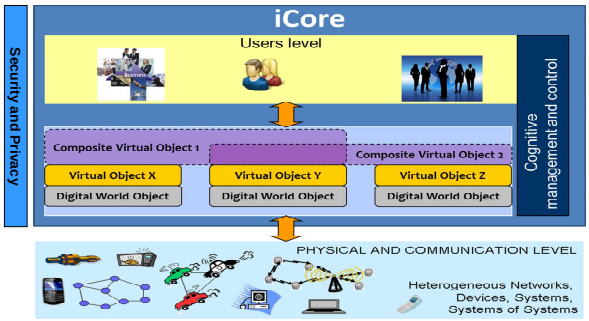
- Patient condition and medical data collection and analysis in Hospital
- Emergency responders and remote monitoring and treatment



Characteristic and requirements
- Equipped with various medical sensors
- Merging real and digital health equipments

Involved stakeholders: Health-care service provider, network providers and device providers

Overall framework

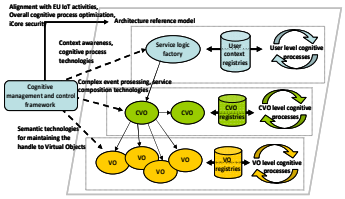


iCore technical challenges

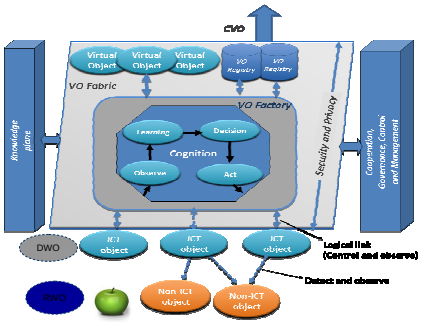
- Addressing **interoperability** issues through VO/CVOs
- Increase the **reusability of objects** outside the scope in which they were originally deployed
- Increase **reliability and availability of services**
- Increase **energy efficiency**
- Allow **Business integration** on the view of multiple stakeholders in the composition of services
- Validate **security and privacy** requirements, without compromising the shared access to resources.

Technical approach

VO and CVO:
- **Cognitive mechanisms** (self-management and learning capabilities)
- Sensing and **context/resources** extractions (computing, storage, profile, etc.)
- Offering access to **information and knowledge** on the RWO/DWO context from service point of view
- **Semantic descriptions** of the virtual and composite virtual objects
- The possibility of **sharing** data and resources in the IoT, which through iCore becomes **application domain and initial context agnostic**



Technical approach



Security and Privacy

The objective for Security & Privacy in iCore should be to:

•To integrate novel privacy & security techniques right from the start such that security & privacy won't become an afterthought or add-on feature.

•Address the specific security & privacy challenges that need to be solved to enable "dynamic creation of virtual objects and to support re-use of real and virtual objects for providing reconfigurable services". (iCore vision).

• Ensure that security and privacy do not impact significantly performance metrics, scalability, price,… of the overall system.

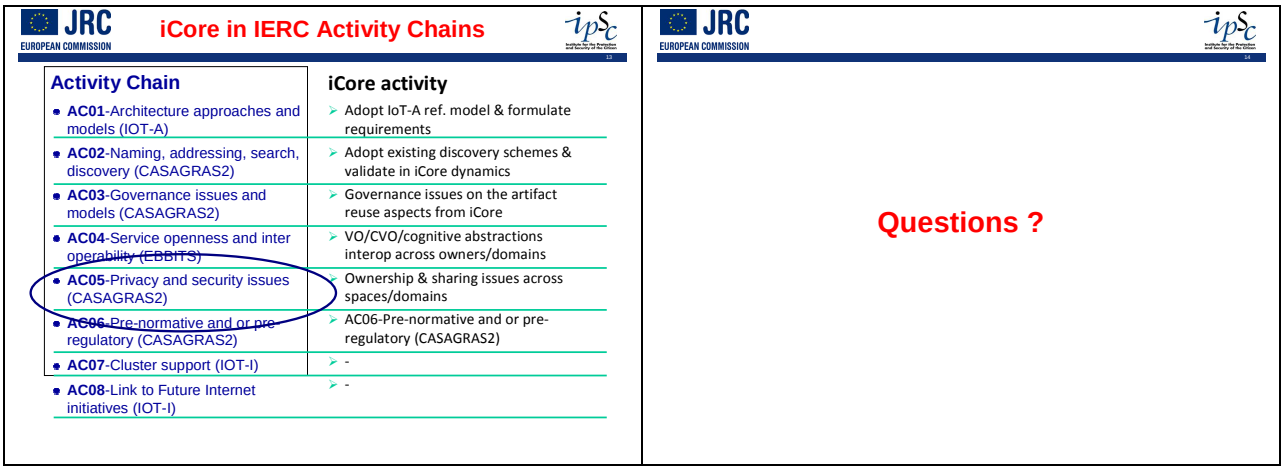
• Address the current regulations for security and privacy (especially the latter). These regulations can be quite different across the world.

Security and Privacy 1/2

- Secure & Privacy preserving data sharing
  - Data from Real/Virtual World Sensors may only be shared when certain conditions are fulfilled.
  - Approach based on Policies and access control, where resources, objects (virtual or real), data and services are all accessed in the same way using policies.
  - Revocable privacy
- Access Control to Real/Virtual World Objects (both sensors and actuators)
  - context-aware access control
    - Location based access control (e.g. only allowed to switch of light in the room where the user is standing)
  - federated identity & access management
- Claim based access control
  - Claim could be "proof that you are guest in the hotel"
- Reuse of what is already done in the Semantic Web security group and tailor it to virtual/real object model: WS-*, SAML, OWL languages for security (Rei)

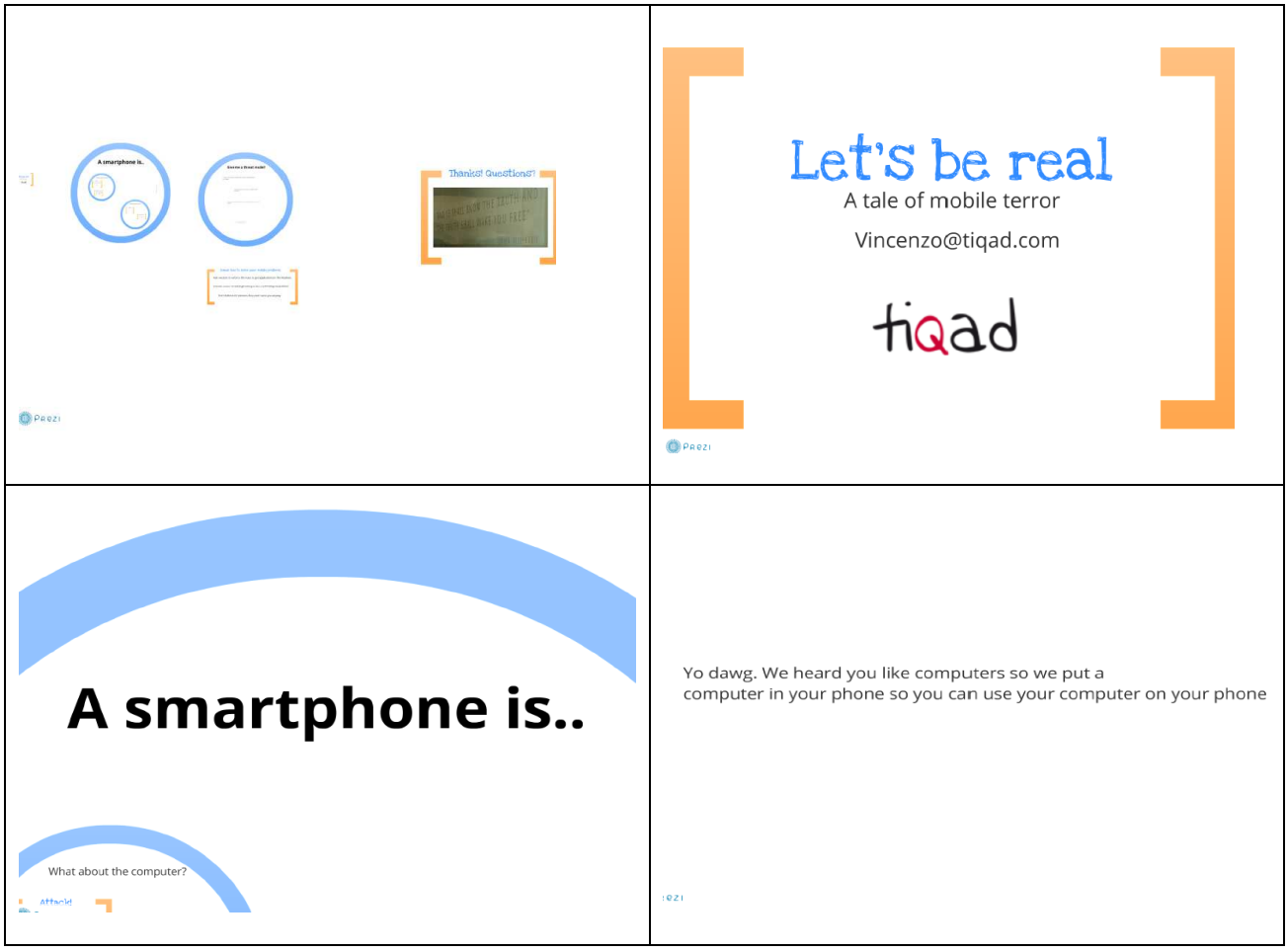
Security and Privacy 2/2

- Trustworthiness of Real/Virtual World Objects
- Multi-level security model
  - Requires to integrate autonomous/adaptive security functions
    - supported in security policy, reasoning on required level of security capability, security functions
  - Security capability negotiation
  - Protection against down grade attacks
- Identity Management.
- Address the integration of real-objects, which have specific security frameworks or they are not internet based. For example, the UMTS authentication profiles must be matched with the security framework based on policies described above.
- Audit and accountability must be present to verify that the access rights and policies are executed correctly.



2.2.3 V. Iozzo (director Vulnerability Intelligence at Trail of Bits)

Vincenzo Iozzo is Director of Vulnerability Intelligence at Trail of Bits, an independent information security company focused on security research, red teaming and incident response. He is a regular speaker at various information security conferences including Black Hat, CanSecWest and DeepSec. He is perhaps best known in the information security industry for co-writing the exploits for BlackBerryOS and iPhoneOS to win Pwn2own 2010 and Pwn2own 2011. He is also a member of the Review Board committee of Black Hat.



What about the computer?

Attack!

browser, file reader, email, random apps

Maybe I'm not!

Attack!

browser, file reader, email, random apps

What about Canvas, Metasploit and so forth?
Staggering figures! 3 android exploits, 3 iphone exploits (taken from the JB community)

so you have widespread malware that doesn't use some form of SE.. not really, no

so you can buy an exploit-kit full of mobile exploits.. not really, no

What about Canvas, Metasploit and so forth?
Staggering figures! 3 android exploits, 3 iphone exploits (taken from the JB community)

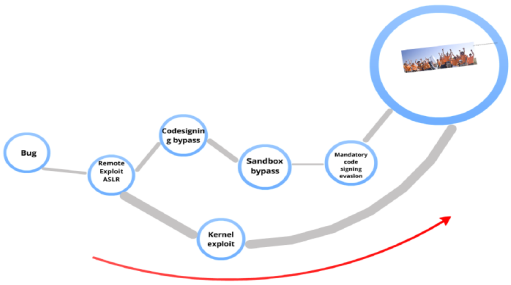
Maybe I'm not!

* see also Dino Dai Zovi, Attackers Math

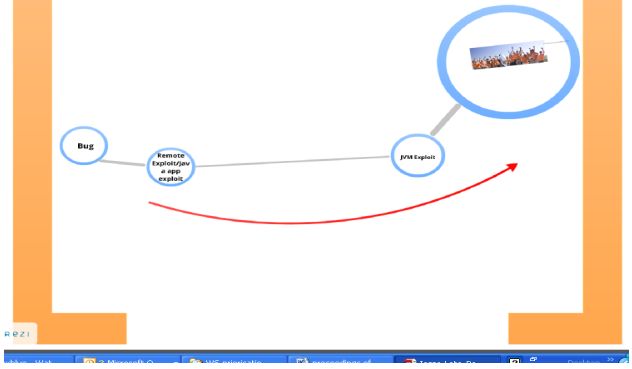
A criminal will take the shortest/easiest path to profit

An "APT" will take the easiest path to achieve its goal

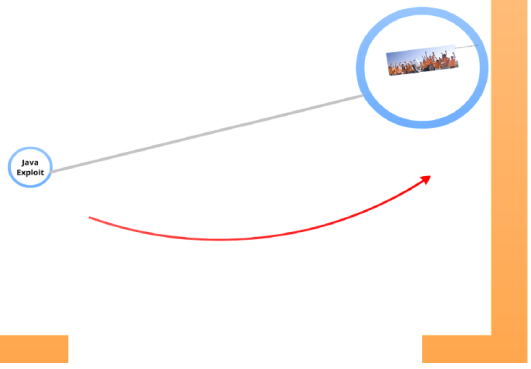
iPhone



Blackberry



On a Desktop



Attackers are lazy

DEP Bypasses (5)	
Developed by APT	3
Developed by Whitehats	2
Developed by Malware Authors	0

Logic Flaws (8)	
Discovered by APT	0
Discovered by Whitehats	8 (!)
Discovered by Malware Authors	0

Dan guido, EIP-2.0

What about the phone?

ttack

Attack

Fundamental problem: Baseband code was written with the idea that an attacker could not get there

Protocols themselves are not that secure either

so am I going to get hacked through the baseband? Not quite

Am I going to see malware spread through the baseband? Most likely you won't

Why?

An attacker most likely needs proximity

It's in general hard to go from the baseband to the "computer"

remember lazyness: it takes a lot of work

Give me a threat model!

Do you often discuss sensitive info? Expect baseband/voice recording

Give me a threat m

Do you often discuss sensitive info? Expect baseband/voice recording

Can your phone be a point of access for a sensitive network?

Can your phone be a point of access for a sensitive network? Expect an APT

Can your phone be a point of access for a sensitive network? Expect an APT

You country is ruled by a dictator and he controls the telcos... You're tosted anyway

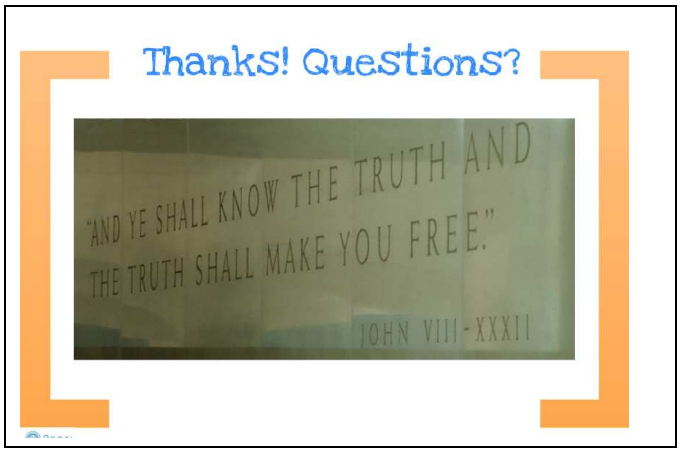
You're just a random guy, got news for you! none of those will hit you any time soon

Bonus: how to Solve your mobile problems

Ask vendors to enforce the rules to get applications in the markets

Educate users: Social Engineering is not a technological problem

Don't believe AV vendors, they won't save you anyway



2.2.4 C. Mulliner (TU Berlin)

Mr. Mulliner is one of the most known researchers on mobile security, mainly protocol related. Previously he worked also as researcher at Fraunhofer SIT. He is probably best known for: first practical (successful) attacks to NFC mobile phones; several attacks and bug discovered on bluetooth protocol with the Trifinite research group; taking control (owning/pwning) an iPhone via malformed SMS.

NFC Tech

- Frequency: 13.56 Mhz
- Communication range: ~4cm
- Data transfer rate: 106, 216, 412 kbit/s
- Supported tags (by the standard):
  - ISO 14443 A/B
  - NXP Mifare Ultralight, Classic/Standard 1k/4k, DESFire
  - Sony FeliCa
  - Innovision Topaz, Jewel tag

NFC "general" Security

- No link level security (wireless not encrypted)
  - Eavesdropping (sniffing)
  - Man-in-the-middle
  - Data: Modification, Corruption, Insertion [9]
- Tamper with NFC/RFID tags
  - Modify original tag
  - Replace with malicious tag

NFC Mobile Phones

- Phones you can buy:
  - Nexus S (smartphone, Android)
  - Nokia 6212 classic (feature phone, S40)
  - Nokia 6131 NFC (feature phone, S40)

Inside an NFC Phone

- RFID/NFC interface is active if phone is "active"
  - active = screen unlocked
- If NFC aware application is running
  - App handles interaction with NFC hardware
    - Especially true for NFCIP (P2P)
- If non-NFC app is running the phone SW takes care and ...
  - reads tag if in range
  - tag data (NDEF data) is parsed
  - if "known" data is found it is pushed to "registered" app
    - HTTP URIs pushed to browser

The NFC Concept so far...

- Touch "tag" with your mobile phone
  - Phone reads tag ⇨ performs action

NFC Usage

- The NFC P2P mode (NFCIP)
  - Right now only used for games and/or file transfer :-(
- NFC card emulation
  - Should be **the big thing** for NFC after all NFC is build for payment
  - Haven't seen real services using this
- Custom applications
  - The "VISA" iPhone NFC adapter

NFC Data Exchange Format (NDEF)

- Container format to store NFC-data in RFID tags
  - Independent from tag type (mostly)
- Defines a number of NFC specific types
  - URI, TextRecord, SmartPoster, ...
- Standardized by the NFC Forum [2]
  - Specs are public
  - Available for free
- NFC services based on passive tags storing NDEF data
  - Field deployed services!

The NFC SmartPoster

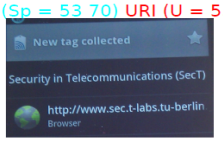
- URI with a title!
  - Title is a "descriptive" text
  - And an optional icon (not implemented anywhere!)
- Defines additional subtypes
  - Recommended action 'act' (what to do with the URI)
    - Execute, save, edit
    - Not implemented anywhere
  - Size and type of object the URI points to
- **This is one of the proclaimed key use cases of NFC!**

SmartPoster: example

Title: Security in Telecommunications (SecT)
URI : http://www.sec.t-labs.tu-berlin.de

```
03 58 D1 02 53 53 70 91 01 23 55 00 68 74 74 70
3A 2F 2F 77 77 77 2E 73 65 63 2E 74 2D 6C 61 62
73 2E 74 75 2D 62 65 72 6C 69 6E 2E 64 65 51 01
28 54 02 65 6E 53 65 63 75 72 69 74 79 20 69 6E
20 54 65 6C 65 63 6F 6D 6D 75 6E 69 63 61 74 69
6F 6E 73 20 28 53 65 63 54 29 FE
```

NDEF SmartPoster (Sp = 53 70) URI (U = 55) Text (T = 54)



NFC Security : Attack Targets

- The mobile phone / smartphone
  - Crash system and/or application
  - Hijack phone (install malicious application)
  - Application bugs and design issues (fraud!)
- The services / applications
  - Attack the service tags and back-end infrastructure
  - Mostly designed to protect service provider not customer

NFC Phone Security

- NDEF SmartPoster analysis (this stuff is used heavily)
  - URI spoofing possible?
- NDEF fuzzing
  - How good are the implementations?
- Nexus S NFC security
  - What is implemented and what is broken?

(My) NFC Security Toolkit

- Tag reader/writer
  - Stationary and mobile (for field analysis)
- NDEF parsing and construction library
  - Analyze tag data collected in the field
  - Test NFC mobile phones (fuzzing)
- RFID (Mifare) tag security tester
  - Check read/write mode of tags in the field
- All available at: http://www.mulliner.org/nfc/

SmartPoster Spoofing 1/2 : The Web Browser

Nokia 6131 NFC

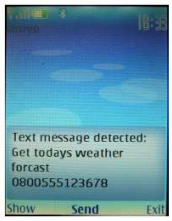
URI is "http://mulliner.org/blog/"
Title: "http://www.nokia.com\r\r\rAddress:\rhttp://www.nokia.com\r...\r."

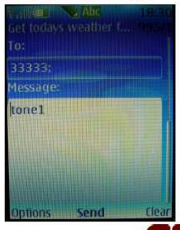
Survives brief inspection by user.

SmartPoster Spoofing 2/2 = SMS

Nokia 6131 NFC

URI: "sms:33333?body=tone1" ← buys a 3 Euro ring tone
Title: "Get todays weather forecast\r0800555123678"





Proof-of-Concept NDEF Worm (Nokia S40)

- Idea we had while playing with the push registry
  - Push registry allows registration for URI Record
- Basic idea: writable tags as transport for worm
  - Use URI spoofing to hide the worm-install-URL
  - Silent MIDlet installation
    - No security warning when downloading a JAR file!
    - Auto install – user will only be asked before execution!
  - Spreads by writing URL pointing to itself to tag
  - Worm is activated by phone reading plain URI tag
- For full details see slides at: http://mulliner.org/nfc/

NFC / NDEF Fuzzing

- NDEF just cries to be fuzzed
  - Fuzzer = Pyhton NDEF lib + RFID writer + Mifare cards
- NDEF Record Payload length field (0xFFFFFFFF) crashes...
  - Nokia NFC phones and Nexus S ← same bug!
- NDEF URI 'U' (well known type = 0x01)
  - "SMS,TEL":<exactly 124 numbers> crashes Nokia 6131
    - Shorter no. is accepted, longer no. produces an error
    - Best guess: off-by-one
- NDEF Record length > Record payload
  - Crashes Android tag reader application

Fuzzing…

- Fuzzing using tags is hard work
  - Tag: on writer, to phone and back (no automation)
- Phone switches off after 4 crashes in a row
  - This is the S40 watchdog, nice thing that helps switching off phones
- Symbian Series 40 not very interesting
  - No known code injection technique
- This will be interesting for smartphones
  - Code injection via RFID/NFC? (work in progress)

Attacking Nokia's NFCIP-based file transfer

- Target: the Nokia 6212 classic's file transfer feature
- Based on NFCIP (P2P mode) in combination with Bluetooth
- Allows to install J2ME application without user's knowledge
- Paper: "Practical attacks on NFC enabled cell phones"
  Roel Verdult and Fancois Kooman
  published Feb. 2011 [17]

Present Time NFC Phone Security (Nexus S)

- Not too many NFC apps / services yet
  - Google Wallet test installations only
- This is what I did so far…

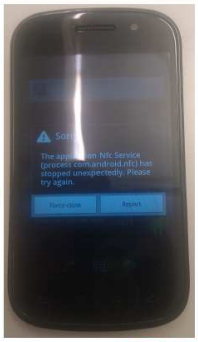
  1) NDEF fuzzing

  2) Poking auto launch URIs

  3) Investigated SmartPosters
  - Only basics are implemented
  - URL spoofing?

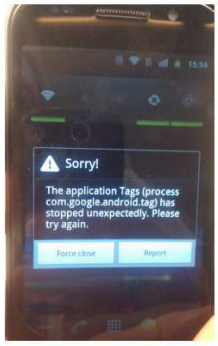
Nexus S

- I only took a brief look…
- NFC Tag TLV bug (from Nokia S40)
  - 0xFFFFFFFF as tag data length
  - Also crashes the Nexus S
    - Crashes the **com.android.nfc** service, low level NFC daemon
  - First thing I tried on the Nexus :)
  - Nothing serious
    - Bad user experience



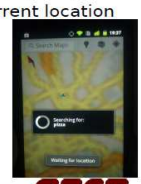
Nexus S cont.

- Playing with NDEF …
- Simple bug in NDEF parsing code…
  - Crashes the tag reader app **com.google.tag**
  - Record
    - length 0x0F
    - content "none"
  - Nothing serious
    - Bad user experience



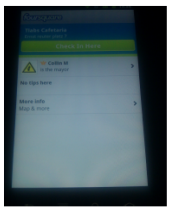
Potential "fun" with Android NFC/NDEF

- **Automatic action on tag content (auto launch)**
- All URLs that contain **http://maps.google.TLD** are opened automatically in maps
- My pizza tag: http://maps.google.de/maps/place?q=pizza
  - Opens maps and searches for **pizza** at current location
- Also works with driving directions…
  - Copy & Past your maps URL to an NDEF tag



Foursquare …

- has automatic URL handler… (taken from AndroidManifest.xml)
- http://m.foursquare.com/[user/venue/shout/checkin/checkins]
- Foursquare tag for your "venue"
  - http://m.foursquare.com/venue/*VenuID*
  - My favorite:
    http://m.foursquare.com/3610408
    - The "T-Labs Cafeteria" :-)
- Stuff like this could be the source for a lot of "fun"



SmartPoster Spoofing and the Nexus S

- Nokia style SmartPoster spoofing?
  - TEL and SMS do not work
  - HTTP works, kind of…

Security of early NFC Services

- Small survey to find vulnerable services (2007/2008)
  - Places: **Vienna, Austria** and Frankfurt/M., Germany
- Most services use default phone features
  - User doesn't need to install an extra application
- All services use Mifare Classic 1k for their tags
- Conducted survey with just the NFC phone
  - Data analysis in the home lab
- So far no real service uses card emulation (SE) or NFCIP

Wiener Linien

- NFC Ticketing for inner city Vienna Austria
  - SMS-based (request and receive ticket via SMS)

Collin Mulliner - "NFC Phone and Service Security" 28/29.11.2011

Wiener Linien cont.

- Tags are read-only
  - Including unused sectors
- Tag attack (sticky tag, discussed later)
  - Use Nokia 6131 spoofing attack to replace actual phone number with "bad" (premium rate) number
- User will trust tag because it **worked** before
  - Maybe spoofing is not even required

Collin Mulliner - "NFC Phone and Service Security" 28/29.11.2011

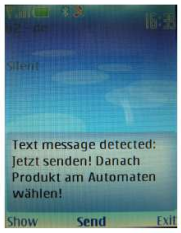
Wiener Linien cont.

- Tags are read-only
  - Including unused sectors
- Tag attack (sticky tag, discussed later)
  - Use Nokia 6131 spoofing attack to replace actual phone number with "bad" (premium rate) number
  - **Got a 3 Euro ring tone instead of your metro ticket?**
- User will trust tag because it **worked** before
  - Maybe spoofing is not even required

Collin Mulliner - "NFC Phone and Service Security" 28/29.11.2011

Selecta Vending Machine

- Mobile phone payment via SMS (Vienna)
  - Payment via phone bill (SMS ties customer to machine and transaction)



Collin Mulliner - "NFC Phone and Service Security" 28/29.11.2011

Selecta Vending Machine cont.

- Tags are read-only (including unused sectors)
- Malicious tag attack, but...
- Can be abused to cash out anonymously
  - Make tags pointing to vending machine A and stick them on machine B, C, D, ...
  - Wait at machine A and pull out your free snack
  - (I haven't actually tried this, I swear!)

Collin Mulliner - "NFC Phone and Service Security" 28/29.11.2011

Tag Attacks

- Stick a "bad" tag on top of "good" tag
  - Use tinfoil for shielding off original tag
  - Use RFID-Zapper [8] to fry original tag
  - Sticky paper tag is ~1,20€ (in low quantities) [7]
- Replace original "good" tag with "bad" tag

- Hijack tag of service provider
  - Break write key and overwrite with malicious data
  - Ultimate user trust!

Collin Mulliner - "NFC Phone and Service Security" 28/29.11.2011

NFC Phone / Service DoS

- Possible Goals
  - Discredit NFC-based service
  - User awareness (this stuff is still kinda insecure)
- Action
  - Write "problematic" content to sticky tags
  - Place sticky tags on top of service tags
- Result
  - Phone / app will crash
    - Users will stop using the service

Collin Mulliner - "NFC Phone and Service Security" 28/29.11.2011

Future Attacks

- NFC will be big in smartphones
- Smartphones already heavily targeted by Trojans
- Trojans will be tailored to NFC
  - Remember NFC is payment
  - NFC-phone has build in smartcard (secure element, SE)
  - Trojans will try to interact with SE
  - Man-in-the-middle between SE and user
- Relay-attacks using the phones build in IP connectivity
- Smartphone botnets with access to the NFC creditcard

Conclusions

- NFC is build for payment → heavy attacks will follow
- NFC + smartphone could be deadly
- Malware targeting NFC applications
- Bugs in NFC phones can be used to discredit services

Berlin Institute of Technology
FG Security in Telecommunications

Questions?

Thank you!

SECT

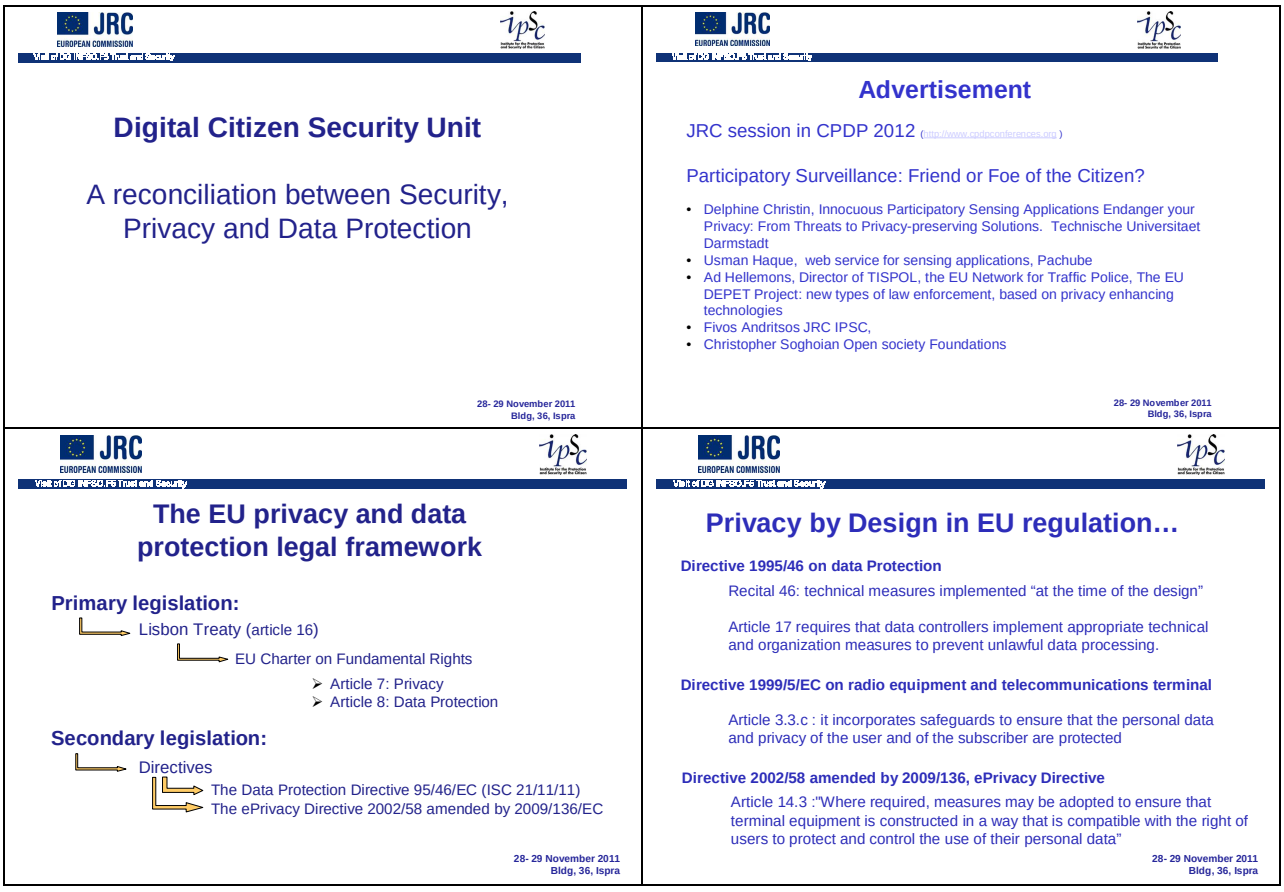
References

[1] http://www.mulliner.org/nfc/ (NFC Security Tools)
[2] http://www.nfc-forum.org (NFC-Forum)
[3] http://europe.nokia.com/A4307094 (Nokia 6131 NFC)
[4] http://www.rmv.de/coremedia/generator/RMV/Tarife/RMVHandyTicket
[5] http://www.forum.nokia.com/main/resources/technologies/nfc/ (Nokia NFC SDK)
[6] http://www.openpcd.org/openpicc.0.html (Sniffing RFID)
[7] http://www.quio.de/Karten/papieretiketten_13.56/papieretiketten_13.56.html (RFID Tag Shop)
[8] http://events.ccc.de/congress/2005/static7r/f/i/RFID-Zapper(EN)_77f3.html (RFID-Zapper)
[9] http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf
[10] http://prisms.cs.umass.edu/~kevinfu/papers/RFID-CC-manuscript.pdf
[11] http://doi.ieeecomputersociety.org/10.1109/ARES.2008.105
[12] http://rfidiot.org/ (Copying RFID Credit Cards – ChAP.py)
[13] http://www.cs.virginia.edu/~evans/pubs/usenix08/usenix08.pdf (Mifare CRYPTO1 broken)
[14] http://www.nfc.at/ (NFC in Austria)
[15] http://europe.nokia.com/A4991361 (Nokia 6212 Classic)
[16] http://developer.android.com/reference/android/nfc/package-summary.html
[17] http://www.computer.org/portal/web/csdl/doi/10.1109/NFC.2011.16
[18] http://intrepidusgroup.com/insight/category/nfc/
[19] http://www.madlmayr.at/blog/?p=139

2.3 Session 3: "Data and privacy protection"

2.2.5 L. Beslay (JRC)

Laurent Beslay, MA in International Relations, post-master in Global Management of Technological Risks and Crisis from the Sorbonne University of Paris. He works as a Scientific Project Manager at JRC since September 2011. From 2004 until September 2011, he worked as Coordinator on Security and Technology for the European Data Protection Supervisor. In addition to his scientific advisory role toward the Supervisor, his responsibilities included 1500 prior-check opinions, policy opinions, complaints, security inspections and audits of EU large scale IT systems. Prior to that he worked, for 6 years, for the JRC Institute for Prospective Technological Studies in Spain where he contributed to the successful set-up of EU projects like FIDIS, SWAMI.



Privacy by design

Privacy by design aims at building privacy and data protection up front, into the design specifications and architecture of information and communication systems and technologies, in order to facilitate compliance with privacy and data protection principles.

Best Available Techniques

Best Available Techniques refer to the most effective and advanced stage in the development of activities and their methods of operation, which indicate the practical suitability of particular techniques for providing in principle the basis for complying with the EU data protection framework. They are designed to prevent or mitigate risks on privacy and security.

Basic technological trends fuelling innovation in the Information Society

Unlimited bandwidth

Unlimited storage capacity

Ubiquitous network access points

Where the smart ingredients will go ?

Without privacy by design…

With privacy by design…

Tire-Pressure Monitoring System and Wireless Sensors

Numerous accidents (Firestone- Ford Explorer)

US Transportation Recall Enhancement, Accountability and Documentation (TREAD) Act November 2000.

Obligation to equip cars with direct measurement TPMS (2008)

Results:
Eavesdropping is possible at a distance of 40m
Tracking the car is possible as a fixed identifier is used
Spoofing of sensor messages is possible as no authentication protocol is implemented

http://www.winlab.rutgers.edu/~Gruteser/papers/xu_tpms10.pdf

European Commission Access control badge

PACS or PSG

- A contactless proximity chip, ISO/IEC 14443 Type A
- A biometric verification based on fingerprint minutiae, stored exclusively on the chip internal memory

⇨ Risk of tracking underlined by the EDPS

⇨ For this application anti-collision protocol should use random UID

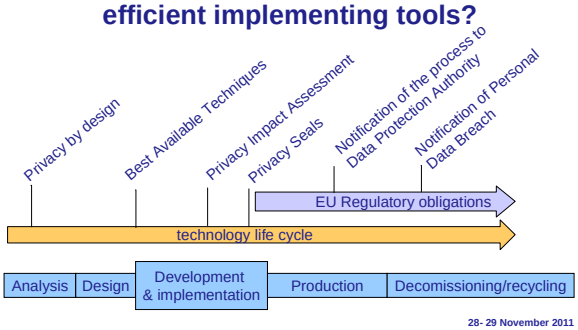
Internet of Things and the Resurrecting Duckling security policy model

(Frank Stajano and Ross Anderson)

Four principles:

- ***Two states: imprinted or imprintable***
- ***Imprinting***
- ***Death***
- ***Assassination***

How to equip the EU privacy toolbox with efficient implementing tools?



JRC
EUROPEAN COMMISSION

ipsc

28- 29 November 2011
Bldg, 36, Ispra

2.3.2. D. Ikonomou (ENISA)

Data and Privacy Protection

Demosthenes.Ikonomou@enisa.europa.eu
29 November 2011, JRC

About ENISA
(European Network and Information Security Agency)

- Created in 2004
- Located in Heraklion / Greece
- Around 30 Experts (total number of staff ~55)
  - Centre of expertise
- Supports
  - EU institutions and
  - Member States
- Facilitator of information exchange
  - EU institutions,
  - public sector and
  - private sector
- Has an advisory role
  - the focus is
    - on prevention and preparedness
  - for NIS topics

Activities

- The Agency's principal activities are as follows:
  - Advising and assisting the Commission and the Member States on information security.
  - Collecting and analysing data on security practices in Europe and emerging risks.
  - Promoting risk assessment and risk management methods.
  - Awareness-raising and co-operation between different actors in the information security field.
- Areas of interest:
  - CERT;
  - CIIP;
  - Risk management, risk assessment;
  - Privacy, Accountability and Trust;

Privacy and Trust

- Privacy is about handling of data about or of persons according to accepted social norms,
  - valid in a particular context;
- Privacy & Trust need joint consideration of technology with
  - social science;
  - economics, ethics;
  - law and other disciplines;
- Needs to be addressed from a pan-European perspective;

What is happening…

The problem(??

- Internet is open and distributed without authoritative control;
- In many cases, service providers need to collect **some** data in order to better dimension their services;
- In terms of privacy a number of challenges are posed:
  1. Data 'pollution'
     - Data are disseminated without control and
     - **Replicated** on multiple servers and Peers;
  2. Contrary to humans, data lives forever
     - emails (not only web mail), social networking sites, online collaborative spaces (e.g. Google docs);
- In 2010 ENISA introduced a new area of work on Privacy, Accountability and Trust;

The Joy of Tech™ by Nitrozac & Snaggy

Areas of (possible) intervention

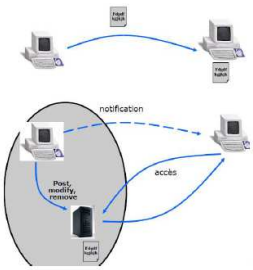
- Information/Education
  - People have to be aware and educated!
  - However, remember the example of the car industry (100+ years)
    - Safety as a competitive advantage;
    - Liability;
- Policy maker
  - Order to remove contents;
  - Promote availability of subscription based services in addition to free;
  - Avoid online service providers lock-in by fostering user profile portability;
  - Implement Data Breach Notification;
- Technology
  - Limit data pollution (e.g. minimal disclosure);
  - Limit content's lifetime (e.g. ephemeral communication);
  - Limit data leakage by design (privacy by design) by introducing more traceability;
- Some examples follow…

On ephemeral communications

- In such a scenario data owner can easily retrieve its data, and modify them if necessary;
- Some existing services partially implement this paradigm:
  - With Youtube, you watch video without downloading them (video streaming)
  - With Skype Chat service, a user can modify its past conversations.
- Researchers are working towards generalizing this paradigm to all Internet services (email, forum, web, social networks,..).
- Not a complete solution to Internet Privacy Issues
  - it does not prevent Google from collecting data from users;
  - Other solutions are also required (anonymizing network, e.g.TOR, encryption, minimal disclosure, etc.).

[ref] Owner-Centric Networking: A New Architecture for a Pollution-Free Internet
[source] INRIA

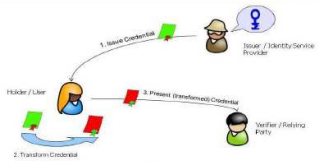
An example: emai



- When an email is sent
  - It is stored on a local server;
  - Recipient gets receive an email with a link to the server;
  - To read the email content, recipient has to connect to the server;
- Email sender can, at any time:
  - Modify/remove the content of his email;
  - Control on who accesses the content;
- Source keeps full control over its data;
- Email can also « self-destruct » after a given time;

[ref] «Vanish» [Usenix Security 2009]
[source] INRIA

Minimal disclosure - Attribute-based Credentials (ABCs)



- Build Attribute-based Credentials (ABCs) systems in a way that they can be trusted, like normal cryptographic certificates, while at the same time protecting the privacy of their holder (e.g., hiding the real holder's identity).
- ABCs are issued just like ordinary cryptographic credentials (e.g., X.509 credentials) using a digital (secret) signature key.
- New credentials containing only a subset of the attributes contained in the original credential.
- ABC can still be verified just like ordinary cryptographic credentials (using the public verification key of the issuer);

FI applications introduce new challenges

- Smart grids / metering;
- Sensor Networks;
- How can we trust a sensor reading?

The world map of social networking for 2010 (in millions of users)

On Privacy by Design

- Widely used definition/term in recent years;
- Received support by data protection policy makers (FTC, EC Communication on 'A comprehensive strategy on data protection in the European Union');
- Privacy needs to be taken into account from the systems development stage, however
  - it is not clear how this can be translated into network design;
- We also need to accept the existence of a plethora legacy networks (3G, 4G, WiFi, GPRS, etc.);

Concluding Remarks

- Private data are considered a competitive advantage;
- Difference of privacy perception across EU MSs;
- Lack of co-ordination at EU level;
- Regulations re-active than pro-active;
- Regulators are not yet prepared (e.g. EU MSs DPAs size);
- Perception of privacy risks depends on the users age group;
- Privacy economics play an important role;
  - As a function of time and context;

Contact

European Network and Information Security Agency

Science and Technology Park of Crete (ITE)
P.O. Box 1309
71001 Heraklion - Crete – Greece

http://www.enisa.europa.eu

2.3.3 G. Vaciago (University of Milan)

Giuseppe Vaciago has been a lawyer and a member of the Milan Bar since 2002 and for the last 10 years his primary focus has been IT Law with a focus on cyber crime. He has assisted many national and international IT companies. Academically, he received his PHD on Digital Forensics from Università di Milano and he is a lecturer at Insubria University (Varese and Como) where he holds a course on IT law. He recently attended Fordham Law School and Stanford Law School as a 'Visiting Scholar' to expand his studies in his own particular research area. Giuseppe Vaciago is the author of many publications on cybercrime, including both scientific journals and textbooks, which have been adopted by the University where he teaches. He has also delivered many lectures and presentations in both Italy and abroad.

Geo-Location, Privacy and Data Retention in a Mobile Cloudy World"

Giuseppe Vaciago

DIGITAL FOOTPRINT IN A MOBILE ENVIRONMENT
WORKSHOP
European Commission
Joint Research Centre (JRC)

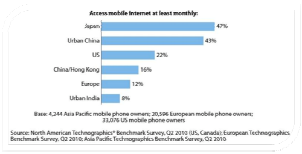
November 29th, 2011

Agenda

- Introduction
  - *Digital Mobile Stats*
- Geo-location
  - *Not only Wi-Fi and Tethering…but Cell Tower and GPS*
  - *Why do we worry?*
  - *Why do we accept to be located?*
- Privacy concerns
  - *Italian Data Protection Authority*
  - *Working Party Article 29 – Opinion 185/2011*
  - *Privacy vs. Security: Data Retention and Facial Recognition*
- Digital Mobile Forensics in a Cloudy World
  - *Jurisdiction*
  - *4 possible solutions for jurisdiction issue*
- Conclusion

Introduction – Digital Mobile Stats

- The estimated world population today is **6,960,028,416**
  (http://www.census.gov/main/www/popclock.html)
- The estimated number of Mobile subscribers on **2010** was **5,300,000,000**
  (http://www.itu.int/ITU-D/ict/statistics/)



- At the end of **2009** almost **530 million users** browsed the mobile Web on their handset. This is forecast to rise to over **1 billion** by **2015**
  http://www.strategyanalytics.com/default.aspx?mod=ReportAbstractViewer&a0=5367)
- The percentage of people regularly accessing the mobile Web in Japan and urban **China is more than double the US**
  (http://blogs.forrester.com)

Geo-location: not only Wi-Fi and Tethering…but Cell Tower and GPS

It is also possible to geo-locate using:

1.Cell phone tower: A phone connects to a single tower at a time – the one with the strongest signal. Each tower has a unique ID. Not only does your tower know your phone is connected to it, your phone knows which tower it is connected to

1.Global Positioning System (GPS) uses signals from 24 satellites (about 10 at a time) and calculates position by knowing the position of the satellites and the delay in time from each satellite.

Geo-location: why do we worry?

The real reason why we are worry is not the technology, but because new players process these data

Google · YAHOO! · facebook · Microsoft · SKYHOOK WIRELESS

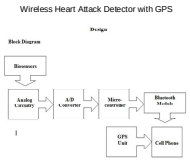
Do we need to start worrying about these players as well?

Geo-location: why do we accept to be located?

There are two main reasons:

1.We have no choice if we want to use the service and we are apps-addicted

1.Seldom if ever an app could be really useful



Privacy: Italian Data Protection Authority

Article 37 – Italian Data Protection Code

The geographical localisation of people or objects gives rise to an obligation to notify the Data Protection Authority (article 37, paragraph 1, sub paragraph a). However, the law refers to the localisation of people or objects when the device permits the continuous identification – including when there are intervals – of the user's position in the territory in given geographical areas

(Clarification of processing to be notified to the Data Protection Authority - 23 April 2004).

Google Street View ≠

Privacy: Working Party Article 29 – Opinion 185/2011

"Providers of geolocation applications or services should implement retention policies which ensure that geolocation data or profiles derived from such data are deleted after a justified period of time"

"The balance of interests between the rights of the data controller and the rights of the user requires an opportunity for the user to easily and permanently opt out from the database, without providing additional personal data"

BUT THERE ARE DIFFERENT BALANCES OF INTEREST….

Privacy vs. Security: Data Retention

Does geolocation data fall within the scope of the 06/24/CE Directive?

If so, what is the retention period?

What will the future of the 06/24/CE Directive be in view of the decisions handed down by the German, Romanian, Irish and Hungarian Constitutional Courts?

Facial Recognition: Privacy vs Security

Faces of Facebook: Privacy in the Age of Augmented Reality
(Alessandro Acquisti, Ralph Gross, Fred Stutzman - Heinz College, Carnegie Mellon University)

They investigated whether the combination of publicly available Web 2.0 data and off-the-shelf face recognition software may allow large-scale, automated, end-user individual re-identification.

Most of the volunteer (75%) were identified within three seconds.

Digital Mobile Forensics in a Cloudy World

There is a growing understanding of how to conduct digital forensic analysis on mobile devices. However, there is little understanding of how to apply digital forensic methodologies in Cloud computing, and even less understanding of how to apply forensic methodologies in mobile Cloud investigation. (Zhu Meng, Mobile Cloud Computing: implications to smartphone forensic procedures and methodologies, http://aut.researchgateway.ac.nz/handle/10292/2660?show=full).

This also applies to legal aspects and specifically to jurisdiction

Digital Mobile Forensics in a Cloudy World

We have 4 different possible principle to solve the "loss of location" in a cloudy world:

- **Territorial principle** by virtue of which the Court in the place where the data is located has jurisdiction (Art. 32, Convention on Cybercrime).
- **Nationality principle** by virtue of which the nationality of the perpetrator is the factor used to establish criminal jurisdiction.
- **"Flag principle"**, which basically states that crimes committed on ships, aircraft and spacecraft are subject to the jurisdiction of the flag state.
- **"Power of Disposal Approach"**. From a practical point of view, a regulation based on the power of disposal approach would make it feasible for law enforcement to access a suspect's data within the cloud.

Houston We Have a Problem !

Thanks for your attention

Giuseppe Vaciago

Mail: giuseppe.vaciago@htlaw.it
Blog: http://infogiuridica.blogspot.it
Linkedin: http://it.linkedin.com/in/vaciago

2.4 Session 4: "Application solutions"

2.4.1. S. Zanero (Politecnico di Milano)

Stefano Zanero received a PhD in Computer Engineering from Politecnico di Milano, where he is currently an assistant professor with the Dipartimento di Elettronica e Informazione. His research focuses on intrusion detection, malware analysis, and systems security. Besides teaching "Computer Security" at Politecnico, he has extensive speaking and training experience in Italy and abroad. He has co-authored over 30 scientific papers and books. He is an associate editor for the "Journal in computer virology". He's a Senior Member of the IEEE (covering volunteer positions at national and regional level), and of the IEEE Computer Society (for which he is the current chair of the Italy chapter). He is also a member of the ACM. Stefano co-founded the Italian chapter of ISSA (Information System Security Association), and sits in the International Board of Directors of the same association.

A Fast Eavesdropping Attack Against Touchscreens

Federico Maggi, Alberto Volpatto,
Simone Gasparini, Giacomo Boracchi, **Stefano Zanero**

Politecnico di Milano

How sensitive data is compromised

- Direct attacks
  - Well-known in both literature and industry
  - Very active research community
- **Other types of attacks**
  - Social engineering attacks
  - Side-channel attacks
  - Difficult to mitigate (if not through awareness)

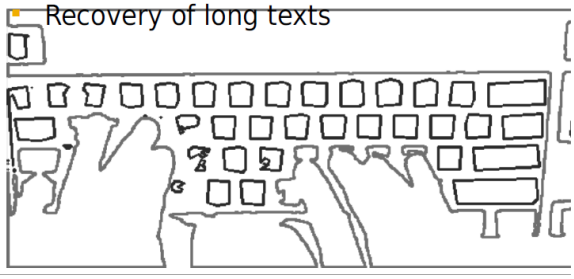
Side-channel Attacks

- Less known yet very effective
- Digital side-channels
  - Example: decrypting SSL through wifi LAN sniffing
- **Physical-world observation**
  - Direct observation
    - Shoulder surfing
  - Indirect observation
    - Sound emanations
    - Reflections
    - Magnetic radiations
    - Desk surface vibrations

Physical-world Observation

Automated Shoulder Surfing

- First attempt of **automatic** shoulder surfing
- Recovery of long texts

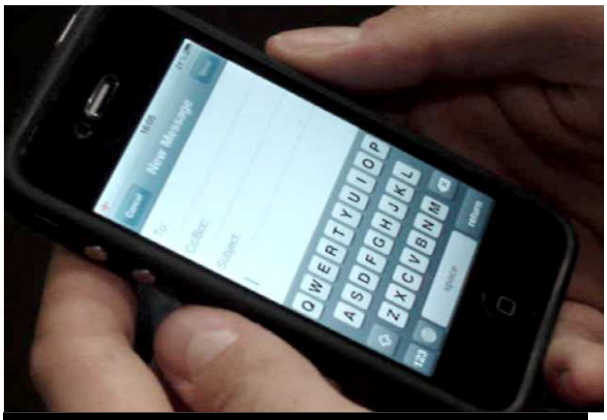


Ubiquitous Touchscreen Mobiles

- **2010** survey on 2,252 US citizens
  - 72% use a mobile phone for **texting**
  - 30% use a mobile phone for **instant messaging**
  - 38% use a mobile phone for Web **browsing**
- (1970) **touchscreen** technology was invented
  - 2010: **5 billion** US dollars market
  - 159% market **grow** rate
  - Q3 2010: 417 million of touchscreen devices sold

Automated Shoulder Surfing

- Non-automated
  - not interesting
  - time consuming
- Automated
  - Is it feasible?
  - Mobile context poses several constraints



Mobile Settings Constraints

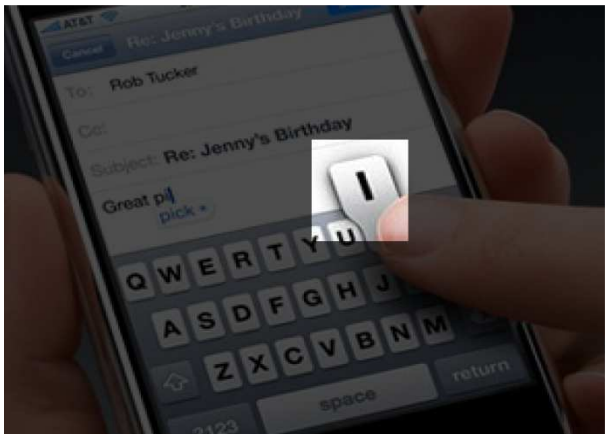
- Moving target
- Fixed observation point not always feasible
- Very small keyboards
- No visibility of pressed keys
- No visible key occlusions

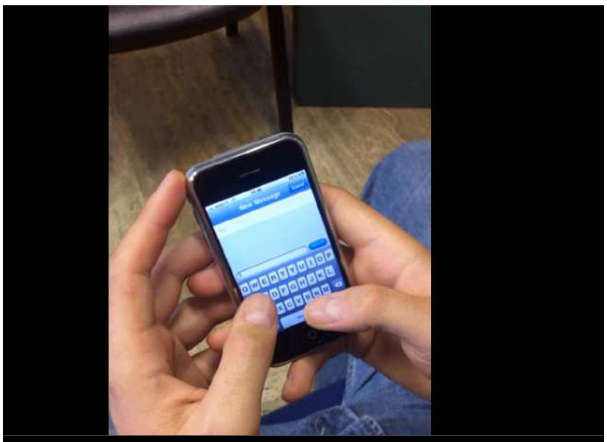
Touchscreen to the rescue

- Lack of tactile feedback
- Early soft keyboards were hard to use
- UI engineers came up with **usable keyboards**

Usability vs Security

- Old dilemma
- More secure, less easy to use
- Example: Google's 2-step authentication
  - Very secure
  - Very unusable
    - Wait for the verification code every time you do email
- Apply also in this context
  - Feedback-less touchscreen keyboards
    - hard to type on
  - Feedback-rich keyboard keyboards
    - easy to type on
    - eyes follow the feedback naturally during typing





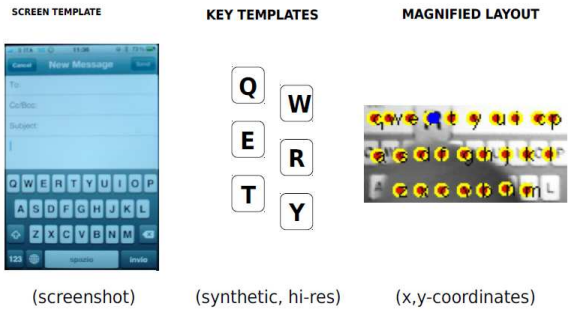
Simple Threat Model

Our approach

- **Requirement 1**
  - iPhone-like visual feedback mechanism
- **Requirement 2**
  - Template of the target screen known in advance

Requirement 1 is often satisfied

Requirement 2 is very easy to satisfy



(screenshot) (synthetic, hi-res) (x,y-coordinates)

Outline of the Approach

- **Phase 1**
  - Screen detection and rectification
- **Phase 2**
  - Magnified key detection
- **Phase 3**
  - Keystroke sequence reconstruction

Phase 1

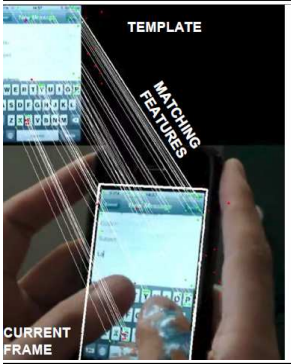
- **Input**
  - Image depicting the current scene (current frame)
- **Output**
  - Synthetic image of the rectified, cropped screen
- **Procedure**
  - Screen detection
  - Screen rectification

Screen Detection

- The current frame is searched for the screen template (Requirement 1)

SCREEN TEMPLATE | CURRENT FRAME | MATCHING PATCH

Screen Detection via Template Matching

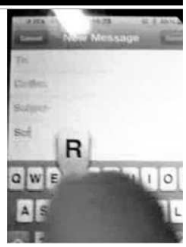


- **SURF** features
  - Edges
  - Corners
- Invariant to:
  - Rotation
  - Scale
  - Skew
  - Occlusions
- **Homography** estimation

Screen Rectification via Homography

CURRENT FRAME

- Estimate during screen detection
- Successfull matches improve matches in subsequent frames



RECTIFIED FRAME

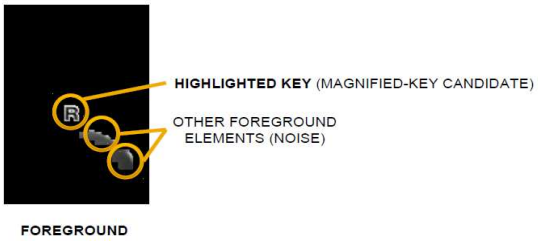
Phase 2

- **Input**
  - Image of the rectified screen
- **Output**
  - Areas where magnified keys appeared
- **Procedure**
  - Background subtraction

Phase 2

- **Input**
  - Image of the rectified screen
- **Output**
  - Areas where magnified keys appeared
- **Procedure**
  - Background subtraction

Spurious output



FOREGROUND

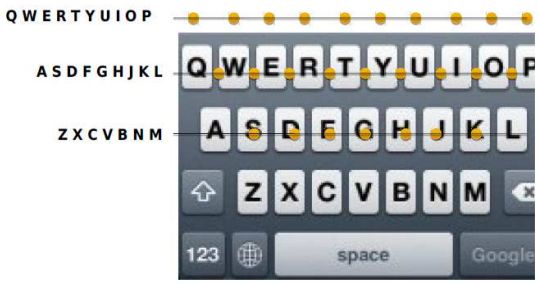
Phase 3

- **Input**
  - Magnified-key candidates
- **Output**
  - Sequence of typed symbols
- **Procedure**
  - Approximate neighbors lookup
  - Best matching key identification
  - Fast pruning
  - Key sequence analysis

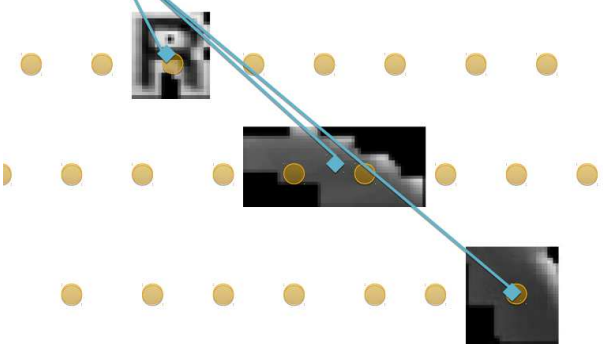
Approximate Neighbor Lookup

- Known keyboard layout (Requirement 2)
- Centroid identification
- Match centroids with keyboard layout

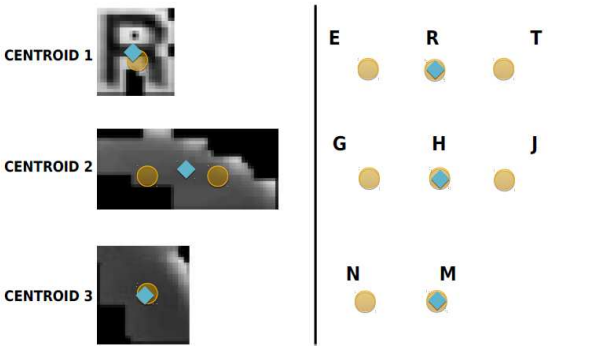
Known keyboard layout



Centroid identification

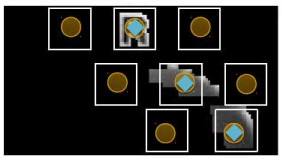


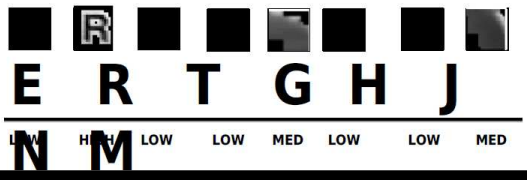
Match centroids with layout



Key similarity

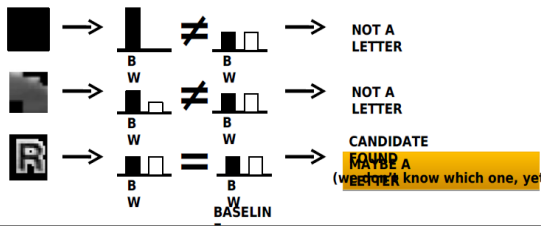
- Region of interest
- Key template (Req. 2)





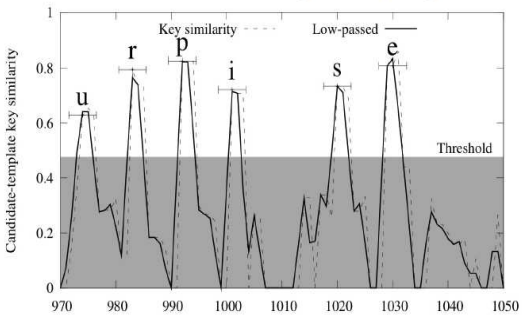
Fast Pruning

- Computing the key similarity is **expensive**
- Black-white distribution of the ROI
- %B/W-**heuristic** is way faster



Key Sequence Analysis

- Find maxima of the key similarity



Implementation Details

- **Phase 1**
  - C++
  - OpenCV
- **Phase 2-3**
  - Matlab
  - Compiled into C
- **Threshold estimation**
  - Confidence interval (mean, variance)
  - Video samples collected in "no typing" conditions

DEMO

http://www.youtube.com/watch?v=aPuS8kNI30U

http://www.youtube.com/watch?v=t9BxB3dO0KQ

Experimental Evaluation

- Types of text
  - Context-free
  - Context-sensitive
- 3 attackers, 3 victims
- Goals
  - Precision and speed
  - Resilience to disturbances

Overall evaluation procedure

- **Typing**
  - 3 victims are given the input text
  - Victims type text on their iPhones
- **Recording**
  - A recording camera was used for repeatability
- **Attack**
  - 3 attackers are provided with the videos
  - Attackers have “infinite” time to analyze videos
- **Comparison**
  - Automatic attack vs. human attackers

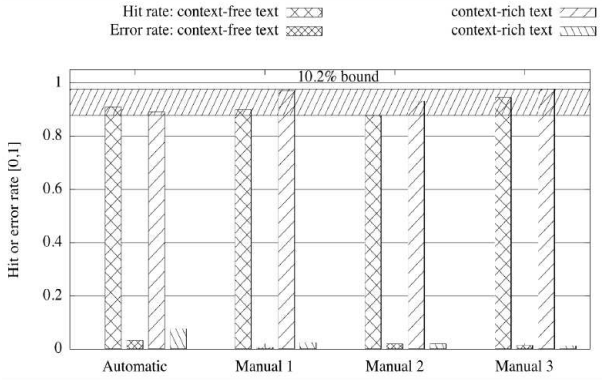
Context-free text

spent chapter foundation identified because first which material notation summarized time spent volume much technical little system reference figured number measurement lorem referring abstract text introductory shown in the we observing request second objective books relationship astute formidable quantile convenient remainder between utilizable tool law resident minutes exemplified the product then temporarily number will per systematic average accumulated south specialty terminal numerous introduce

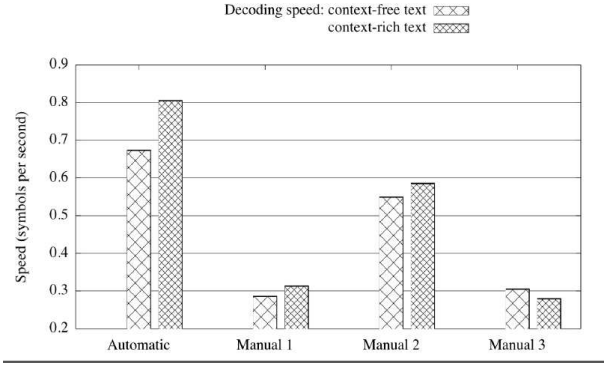
Context-sensitive text

close your eyes and begin to relax take a deep breath and let it out slowly concentrate on your breathing with each breath you become more relaxed imagine a brilliant white light above you focusing on this light as it flows through your body allow yourself to drift off as you fall deeper and deeper into a more relaxed state of mind now as i

Almost as precise as a human



Way faster than a human



Extreme conditions

Aberration	Phase 1	Phase 2-3	
		h%	ε%
1) Permanent occlusion	difficult	44.44	33.33
2) Shake device	feasible	67.74	8.70
3) Shake camera	feasible	96.00	4.00
4) Shake device + camera	unfeasible	0.00	-

Limitations

- **Non-magnifying keys**
  - Space (on iPhone only)
  - Layout-switching keys
  - **Mitigation**
    - Device-specific heuristics
    - E.g., on iPhone, exploit color-changing spacebar
- **Alternative layouts** (minor limitation)
  - **Mitigation**
    - Detect switch
    - Loop through different templates during detection

Alternative layouts

iSpy: A Happy Coincidence

- [Raguram, CCS 2011]
- Appeared at the same conference
- Completely different approach
  - Classification-based
  - They require training
- Really, the very same accuracy 97~98%

Conclusions

- Touchscreen mobile devices are widespread
- Shoulder surfing is automatable
- Automatic shoulder surfing is precise too
- Counteract these attacks with privacy screens
- But…

Finger tracking

- **Challenge**
  - How to detect tapping?

THANKS!

Stefano Zanero
stefano.zanero@polimi.it

@vp_lab
Dipartimento di Elettronica e Informazione
Politecnico di Milano

2.4.2. D. Petró (uTRUSTit project)

uTRUSTit
Usable Trust in the Internet of Things

Project Reference: 258360
FP7-ICT (Area: ICT-2009-1.4 Trustworthy ICT)
Project Duration: 1 Sep 2010 – 31 August 2013

UTRUSTIT

11/29/2011

2

Dániel Attila Petró
project manager

mobile: +36-20-373-6573
e-mail: daniel.petro@search-lab.hu
www.search-lab.hu

SEARCH-LAB
SECURITY EVALUATION ANALYSIS AND RESEARCH LABORATORY

3

Our Definitions and Goals

- Internet of Things = ?
- Trust = ?
- Usability = ?

4

INTERNET OF THINGS

- The IoT connects devices that surround us, enabling communication and programmed cooperation (e.g. home or office automation).

5

TRUST

Trust

Security

6

TRUST

- We use the notion of *trust* as a positive belief that a system will work as expected, combined with a feeling of control over it.
- Our goal is to make and maintain a balance between the user's perception of trust and their actual security status when using the system. This is undertaken via customized conversations with the user.

7

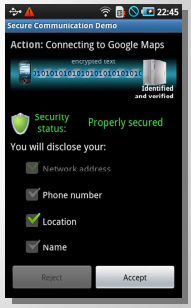
USABILITY

- Most users do not understand such messages as:

8

USABILITY

- We need feedbacks customized to different user needs, with only the necessary security information displayed. An example is shown on the right.



9

Workflow

- User requirements assessment
- Use case scenario definitions
- Assesment of legal issues
- Designing the feedback system
- Creating IoT prototype to test trust on real users
- Virtual Reality environment for VR-based trust tests
- Performing user evaluations

10

User Requirements

- Mental models and Personas are used to create profiles covering different user needs, tastes and capabilities.

11

Use Case Scenarios

- We perform the evaluation of the feedback system in 3 environments:

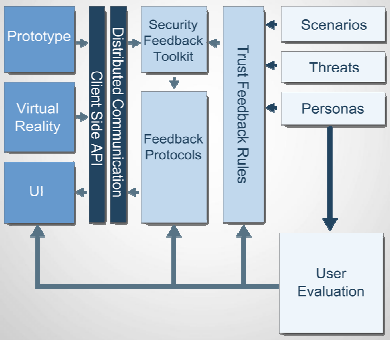

Smart Home


Smart Office


E-voting

12

The uTRUSTit system architecture



13

Prototyping the IoT

- Preparation for real-world testing of the uTRUSTit feedback system

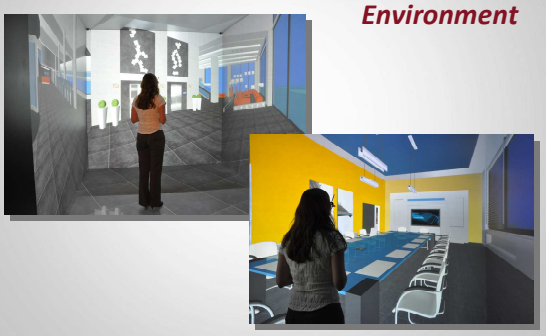
14

Virtual Reality Environment

- Testing in Virtual Reality provides more freedom in future IoT simulation.

15

Interaction with the Virtual Reality Environment



16

Consortium Partners

CHEMNITZ UNIVERSITY OF TECHNOLOGY

NR

SEARCH-LAB
SECURITY EVALUATION ANALYSIS AND RESEARCH LABORATORY

SWEDEN CONNECTIVITY

KATHOLIEKE UNIVERSITEIT LEUVEN

cure
center for usability research & engineering

17

Thank you for your attention

2.4.3. A. Atzeni (Webinos Project)

webinos

Secure Web Operating System
Application Delivery Environment.
www.webinos.org

Nov 2011 (v2)

Who is driving webinos

webinos

- Today
  - 22 founding partners from 9 countries who committed resources for 3 years to deliver webinos
  - Academic + industrial
  - Non-polarised
  - Cross-domain
  - Affiliate Members
- Tomorrow
  - Open (source) community of academia, industrial and developers driving and using the developments

About

webinos

- A cross web platform that enables applications to run across connected devices (TV, Automobile, Mobile, PC).
  - Same application can run on multiple devices
  - Applications can use resources across devices
  - Applications allow to control devices remotely and safely
- Developed through an industry driven, technology research and development project with very clear and fast deliverables

What webinos will deliver

webinos

- A web platform designed to allow apps to run across mobile, home media, PC and automotive comprising
  - Terminal specifications
  - Open source platform developments
  - Proof of concept applications and demos
- Plus eco-system building in form of
  - workshops and seminars,
  - research publications and
  - liaisons with industry standards

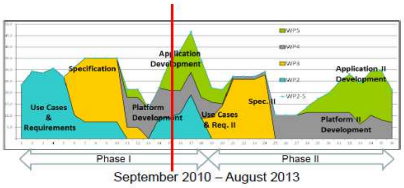
webinos Approach

webinos

- The webinos project will progress its deliveries in a phased approach.
- The first platform release and apps are planned 1.5yrs after launch, i.e. Spring 2012

Key Deliverables

- Use case definition / requirements
- Landscape analysis
- Concepts, architecture and key enablers
- Open Source Platform specification & development
- Application development
- Eco-system development
- Standardisation
- Industry alignment



webinos

Webinos Security and Privacy Framework (T3.5) and User Expectations of Security and Privacy (T2.7, T2.8)

The scenario

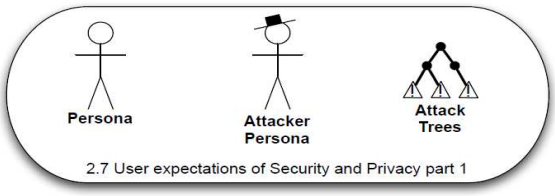
webinos

- Augmented connectivity increases the impact of malware and any security or privacy violation.
- Balancing of security, privacy, performance, ecosystem requirements, standards compliance, platform independence, …
- Evolutionary approach of security controls development (with variations depending on the platform and scenario)

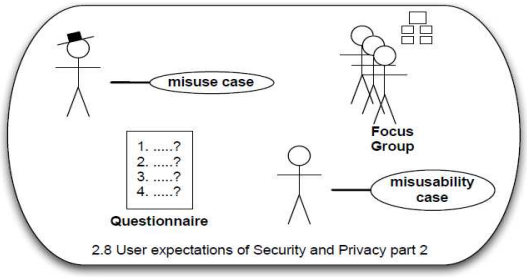
webinos personas

webinos

from T2.7



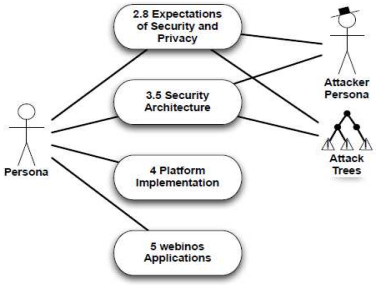
from T2.8



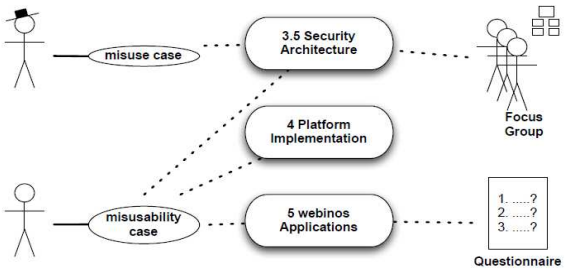
Example threats

- Peter loses his webinos-enabled mobile
  - Ethan finds it and extracts the stored credentials. He sends phishing messages to Peter's friends via his social network profile.
- Anna installs a new media player application.
  - It installs a keylogger on *all* her webinos-enabled devices to extract her passwords and credit card information.
- Justin is using webinos via public wifi
  - Frankie intercepts all network traffic and gains access to Justin's social network accounts.

Relationships

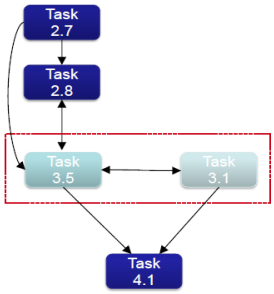


Relationships (cont.)



Architecture

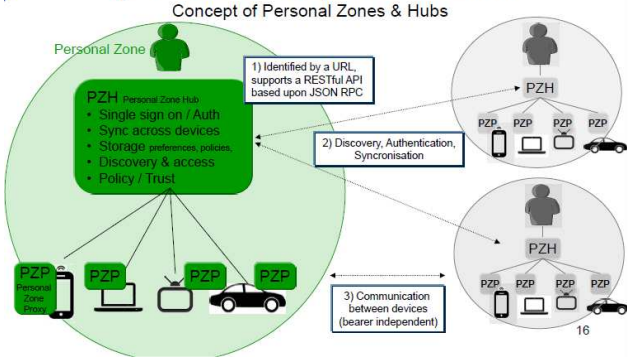
- Security policies
- Privacy policies
- Authentication
- Runtime authorisation and user interfaces
- Privileged applications
- Secure storage
- Security for extensions
- Personal zone security
- Platform integrity
- Application certification, installation and trust
- Device permissions
- Session security



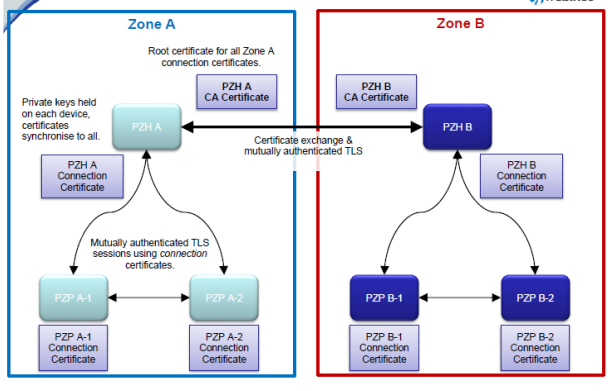
4) webinos Implementation

In progress <Feb 2012

Concept of Personal Zones & Hubs

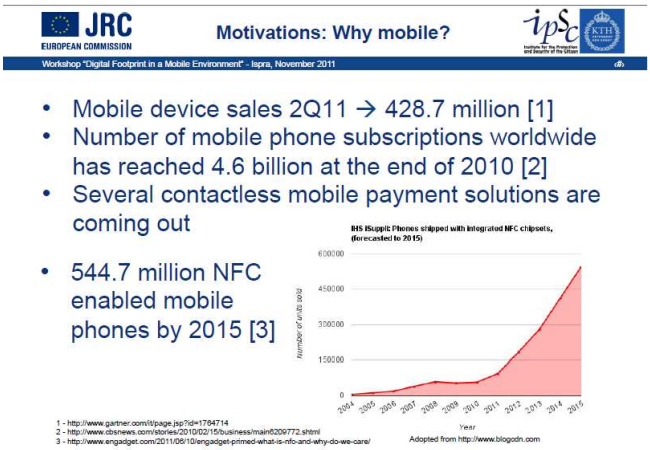


16



2.4.4. P. Stirparo (JRC, KTH Stockholm)

Pasquale Stirparo is Digital Forensics and Mobile Security Researcher at the Joint Research Centre of European Commission. His research interests include security and privacy issues related to mobile devices communication protocols, mobile malware, mobile forensics and cybercrime. Prior to join JRC, Pasquale was working as Security Consultant and Digital Forensics Analyst for an Italian based private company. He has also been invited as speaker to several Italian conferences and seminars on Digital Forensics and lecturer on the same subject for Politecnico di Milano and United Nations (UNICRI). Pasquale is currently enrolled as Ph.D. student at the Royal Institute of Technology (KTH) of Stockholm, holds a MSc in Computer Engineering from Politecnico di Torino (2008) and he is certified GCFA, OPST, OWSE, ECCE.



Mobile Security

Workshop "Digital Footprint in a Mobile Environment" - Ispra, November 2011

- Communication Protocols
  - Mobile communication == Wireless
  - Bluetooth, NFC/RFID, GSM, etc.
  - Threats: Surveillance, Traceability, Sniffing, Eavesdropping, etc.

- Applications
  - Mobile payments
  - High Value goods traceability
  - Mobile Gaming

Adopted from www.nfc-research.at

Adopted from www.nokioteca.net

- Mobile Malware
  - Unsecure OS/protocols can lead to proliferation of malware
  - Malware RevEng → understand proliferation mechanisms and OS weaknesses

Thank you for your attention

Workshop "Digital Footprint in a Mobile Environment" - Ispra, November 2011

Joint Research Centre (JRC)

Web: www.jrc.ec.europa.eu

Contact:
pasquale.stirparo@jrc.ec.europa.eu

Mobile Forensics

Workshop "Digital Footprint in a Mobile Environment" - Ispra, November 2011

- Shift of Trends
  - As more critical services are moved to mobile (i.e. financial transactions, mobile payments), criminals will focus more on these devices as well
- No more "National Borders"
  - Cybercrimes involve several different jurisdictions
  - Classical concept of National Borders doesn't apply anymore

- Standardized Methodology and Best Practice
  - Need of harmonized laws, policies and procedures
  - Mobile forensics evidence collection, acquisition and preservation require particular care
  - ISO/IEC 27037

3. Business opportunities / conclusions

The business opportunities and conclusions are the result of a round table collection during the workshop; they are so far a collection which needs to be prioritised.

Issues around geo-localisation in respect to devices used directly or indirectly by citizens are an important element to consider; hence CIDIPRINT's work should be re-focussed accordingly. This counts as well as for questions around data retention.

Specific attention has to be given to preinstalled SW (services, applications) on mobile devices such as Carrier IQ.

Privacy can still be assured when identity is separated from device ID.

Privacy agreement can be accepted of refused by users, there is no such think like partially accept or accept only for the next event. If the user rejects the privacy agreement he will typically not be able to get the product or use the service.

It has to be considered that users are typically the weakest point in the mobile system in respect to security and privacy. User awareness and training level should be raised in the future. An example is that typically viruses are launched with user consent, thus awareness needs to be improved a lot. The perception of privacy is related to the age, which is well reflected in a EDPS report about this topic. The user trusts typically the developer, the provider etc. and expects that everything is done well. In the dialogue with the users it is important to be more careful with using certain terminology such as: citizen, individual, consumer, data subject, etc. Young people are typically fully aware of what they are doing but they accept it anyhow. The dishonest are lazy, so they will execute the best value for money attack.

It has to be stated that from the technological prospective it can be anticipated that:

- NFC will be heavily deployed for mobile payment.
- In respect to NFC attacks, the distance is a specific element, so the reintroduction of the local element is interesting.
- Application, OS and protocol are important elements for security and privacy protection.
- Mutual authentication will be a key element.

New technologies raise new questions such as: How about data retention in case of cloud implementation?

Privatisation of law enforcement is questionable as they should not look what happens inside the communication. If states are aiming to analyse data there is hardly anything the user can do against.

Data retention principles can be found in the new regulation, the fight about opt in and opt out, has 2 dimensions:

i. The one regarding the EC regulation (number 9546)

ii. The one for all the rest (like the discussion how long Google will keep client data), the 2006 communication regulation.

The dimension of consent and the EU culture is to be defended by states or authorities; the difficulty is to find the right balance between the consent which can be given and the needs coming from law enforcement, for example, geo-localisation and maybe also contextual information.

It was commonly understood that we still have a couple of years in front of us until the first heavy attacks will prevail in the mobile world. More cross links between the project designing future Internet will be needed.

Attackers use very sharp techniques to explore vulnerabilities and to do very specific attacks but there are only very fuzzy ideas how to prevent them.

References

S. Scheer, I. Kounelis, J. Löschner, V. Mahieu, D. Shaw, P. Stirparo: *Citizen Digital Footprint, state-of-the-art*. JRC Scientific and Technical Report, JRC 65960. Publications Office of the European Union, Luxembourg, 2011.

URL's:

http://www.mulliner.org/nfc (NFC security tools)

www.nfc-forum.org (NFC forum)

www.openpcd.org/openpicc.0.html (Sniffing NFC)

www.nfc.at (NFC in Austria)

europe.nokia.com/A4307094 (Nokia 6131 NFC)

www.forum.nokia.com/main/resources/technologies/nfc/ (Nokia NFC SDK)

www.quio.de/Karten/papieretiketten_13.56/papieretiketten_13.56.html (RFID Tag Shop)

events.ccc.de/congress/2005/static/r/f/i/RFIDZapper(EN)_77f3.html (RFIDZapper)

rfidiot.org/ (Copying RFID Credit Cards – ChAP.py)

www.cs.virginia.edu/~evans/pubs/usenix08/usenix08.pdf (Mifare CRYPTO1 broken)

europe.nokia.com/A4991361 (Nokia 6212 Classic)

European Commission
EUR 26051 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen

Title: **Digital Footprint in a Mobile Environment**

Authors: Jan Löschner, Pasquale Stirparo, Vincent Mahieu, David Shaw, Stefan Scheer, Ioannis Kounelis

Luxembourg: Publications Office of the European Union

2012 – 52 pp. – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1831-9424 (online), ISSN 1018-5593 (print)

ISBN 978-92-79-32352-2 (PDF)
ISBN 978-92-79-32353-9 (print)

doi:10.2788/59068

XX-NA-26051-EN-N

JRC Mission

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Serving society
Stimulating innovation
Supporting legislation

doi:10.2788/59068

ISBN 978-92-79-32352-2

Publications Office