

---

# Security and Privacy Challenges in the Real World Internet

**Claudia Diaz**

---

Katholieke Universiteit Leuven  
Dept. Electrical Engineering – ESAT/COSIC

FIA - Future Internet Assembly  
Madrid, December 9, 2008

# COSIC: COmputer Security and Industrial Cryptography (KULeuven)

- > 50 people
- Headed by: B. Preneel, I. Verbauwhede, V. Rijmen
- Research areas
  - Symmetric Key Crypto
  - Public Key Crypto
  - Secure Hardware Implementations
  - Identity Management
  - Privacy
  - Secure Mobile Networks
  - Software Security

- FP6 and FP7 Projects:

- Coordinator of:

- FP6 NoE **E-CRYPT**
- FP7 NoE **E-CRYPT II**
- FP7 IP **TAS3**

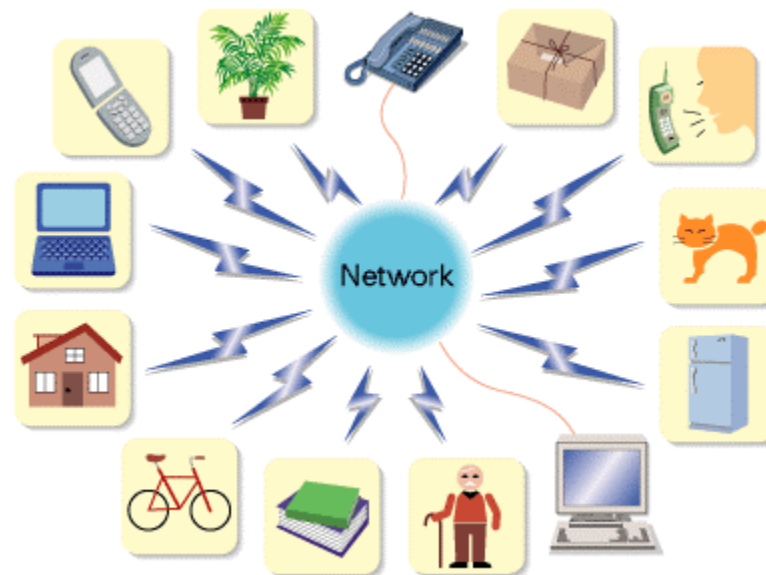
- Participating in:

- FP6 IP **PRIME**
- FP6 MIBG **SEVEN**
- FP6 STREP **SCARD**
- FP6 STREP **TEAHA**
- FP6 IP **OpenTC**
- FP6 NoE **FIDIS**
- FP6 FET **SPEED**
- FP6 STREP **RE-TRUST**
- FP6 STREP **SEVECOM**
- FP7 IP **PRIME Life**
- FP7 IP **TURBINE**

**I will not present the fact sheets of these projects!**

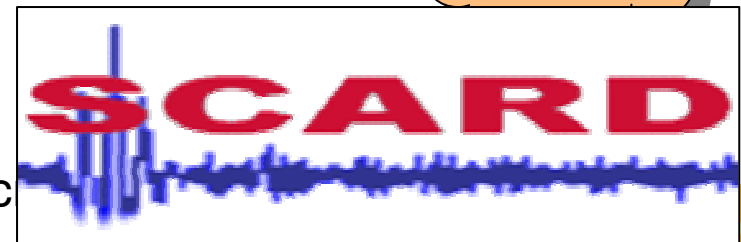
# The Real World Internet

- Zillions of devices with computing and communication capabilities (everyware)
- Everything is networked
- Physical spaces with sensors
- Backend systems
  - Information is collected, stored, linked, processed and interpreted



# Basic security challenges

- Scenario: heart device that:
  - Monitors heart activity, sends data to the doctor, and adjusts pacemaker according to instructions from the doctor
- Security threats:
  - Data is modified:
    - Doctor gets incorrect data
    - Pacemaker gets incorrect instructions
  - Data is falsified:
    - Adversary impersonates doctor / patient device
  - Communication is jammed (availability)
  - Confidentiality breach
- Challenges:
  - Limited resources: need for lightweight c
    - Fast, cheap (resources) and secure
  - Secure implementations
  - Tamper resistant hardware
  - Secure backend systems and architectures



---

# What about privacy?

- The RWI relies on huge amounts of information being available, and many of these pieces of information relate to individuals:
  - Identity
  - Location
  - Interests / preferences
  - Behavior
  - Health data
  - Social network
  - ...
- If these data are **linkable** to the individual (or each other), the RWI will be a **mass surveillance system**
  - To avoid that, we will need to build in privacy properties such as **anonymity** and **unlinkability**
- Popular arguments against privacy / anonymity:
  - “If you care so much about your privacy it’s because you have *something to hide*”
  - “Surveillance is good and privacy is bad for national security”
  - “If people are anonymous they won’t be accountable in case of misbehavior. We need a tradeoff between privacy and security”
  - “People don’t *care* about privacy”

# “I have nothing to hide”

- “I don’t care about surveillance because I have nothing to hide”
- “If you are so concerned about people/the police/the government knowing what you do, it’s because you know you’re doing something wrong”
- Solove:
  - “The problem with the ‘nothing to hide’ argument is its underlying assumption that **privacy is about hiding bad things.**”
  - “Part of what makes a society a good place in which to live **is the extent to which it allows people freedom from the intrusiveness of others. A society without privacy protection would be suffocation.**”



The Economist:  
“Learning to live with  
Big Brother” (09/2007)

---

# Surveillance = Security?

- Law enforcement keywords to justify more surveillance:
  - Terrorism, child pornography, money laundering, crime
- The problems with using surveillance to achieve security:
  - Strategic adversaries (e.g., terrorists) will adapt to stay under the radar and evade surveillance, while law-abiding citizens will not
    - Indiscriminate instead of targeted (old times)
  - Lack of transparency and safeguards may easily lead to abuses
  - We run the risk that the surveillance facilities will be subverted or actually used for crime/terrorism
  - Example: Greek Vodafone scandal: “someone” used the **legal interception** functionalities (backdoors) to monitor: Greek PM, ministers, senior military, diplomats, journalists... (106 people)
- The RWI enables surveillance capabilities for private entities
  - Function creep
- Information asymmetries → power asymmetries

---

# Are authentication/accountability incompatible with anonymity?

- Unique identifiers
  - Reconciling anonymity and authentication
  - Anonymous credentials, private credentials, minimal disclosure tokens
    - Privacy-enhanced PKI functionality:
    - Authenticated attributes from trusted issuer (CA)
    - Data minimization (data protection principle)
    - Pseudonymity
      - Unlinkability of pseudonyms (different entities)
    - Anonymity (one-time pseudonyms)
      - Unlinkability of pseudonyms (same entity)
-

# Scenario: Alice wants to enter a disco

## PKI

- Protocol:
  - Disco reads Alice's id
  - If Alice's age > 18, she can enter
- Disco learns:
  - Alice's id number, name, birthdate, address, picture, ...
- Next time Alice enters, the disco can link the two visits
- Disco A and disco B can check whether Alice is a common client (and aggregate yet more data about her)

## Anonymous credentials

- Protocol:
  - Alice proves that her id encodes an age greater than 18
- Disco learns:
  - The person entering is older than 18
- Next time Alice enters, the disco **cannot** link the two visits
- Disco A and disco B **cannot** check whether Alice is a



PrimeLife



---

# Transparency and awareness

- Sometimes anonymization is not possible / not enough
  - Identification required
  - Long-term pseudonyms
  - We are associated with profiles
- Need for transparency mechanisms
  - What information is being collected? By whom? For what purpose?
  - How is it processed / aggregated into profiles?
  - What inferences can be made from it?
  - How are these profiles applied back to me?
- Awareness
  - Tools for knowing what others know about us
  - Empowerment: ability to predict and to react
  - Accountability for data holders and processors



# Traffic data

- Even if communication is encrypted, traffic data can reveal a lot of information: source, destination, volume, etc.
- Some examples where sensitive data can be inferred from traffic data
  - Scenario 1: Home monitoring system that sends information to oncology department
    - Source-destination enough to determine that the person living in the house has cancer
  - Scenario 2: Fridge that orders food from the Kosher shop
    - Source-destination enough to determine religious beliefs
  - Scenario 3: Device to hear streaming radio from a highly conservative news station
    - Source-destination enough to determine political beliefs
  - Other: companies searching for patents/info on a subject; localization of police cars; etc.
- Who can listen to these traffic data?
  - Anyone who can eavesdrop on the communication channel
  - Any communication intermediary
  - Much easier than breaking crypto protocols
- Techniques for anonymizing the communication
  - Huge challenge, mostly overlooked



---

## Some more privacy challenges I didn't talk about

- Privacy requirements
  - Location privacy
  - Database privacy
  - Privacy policies
  - Private information retrieval
  - Privacy-enhanced biometric authentication
  - Privacy models and metrics
  - Privacy-preserving data mining
  - Legal, economic and usability aspects
-

---

# Conclusions

- It is *important* that security and privacy protections are built into the RWI
- Security challenges are tough, but at least reasonably well understood
- Privacy challenges are formidable, and not yet fully understood
- Some research problems are receiving some attention (e.g., basic security or identity management)
- Some are receiving no attention (e.g., anonymous communication infrastructures)
- In general, research on privacy invasive technologies is better funded than research on privacy enhancing technologies

# Thank you!



<http://www.myconfinedspace.com/>

- For more information:
  - ❑ <http://www.esat.kuleuven.be/cosic/>
  - ❑ [claudia.diaz@esat.kuleuven.be](mailto:claudia.diaz@esat.kuleuven.be)

