Management of Privacy in mobile Applications

Prof. Dr. Hannes Federrath
Security in distributed systems
http://svs.informatik.uni-hamburg.de/

Autoritat Catalana de Protecció de Dades,
Barcelona, 25 Feb 2014

Protection Goals

Subject of communication
WHAT?

Circumstances of communication
WHEN?, WHERE?, WHO?

Confidentiality

Contents

Anonymity
Unobservability

Sender

Location

Recipient

Integrity

Contents

Accountability
Legal Enforcement

Sender

Billing

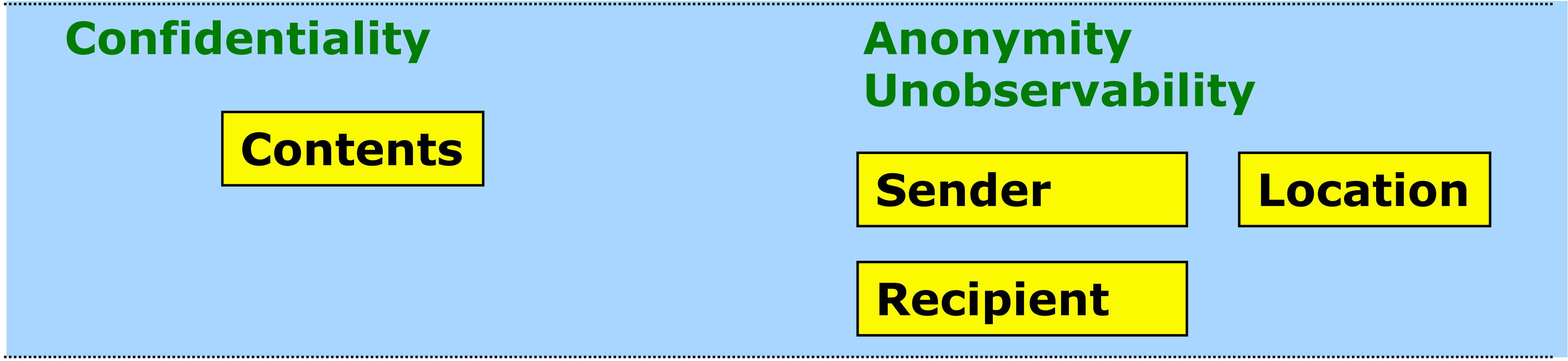
Recipient

Availability

Protection Goals

Subject of communication
WHAT?

Circumstances of communication
WHEN?, WHERE?, WHO?



Confidentiality

Contents

Anonymity
Unobservability

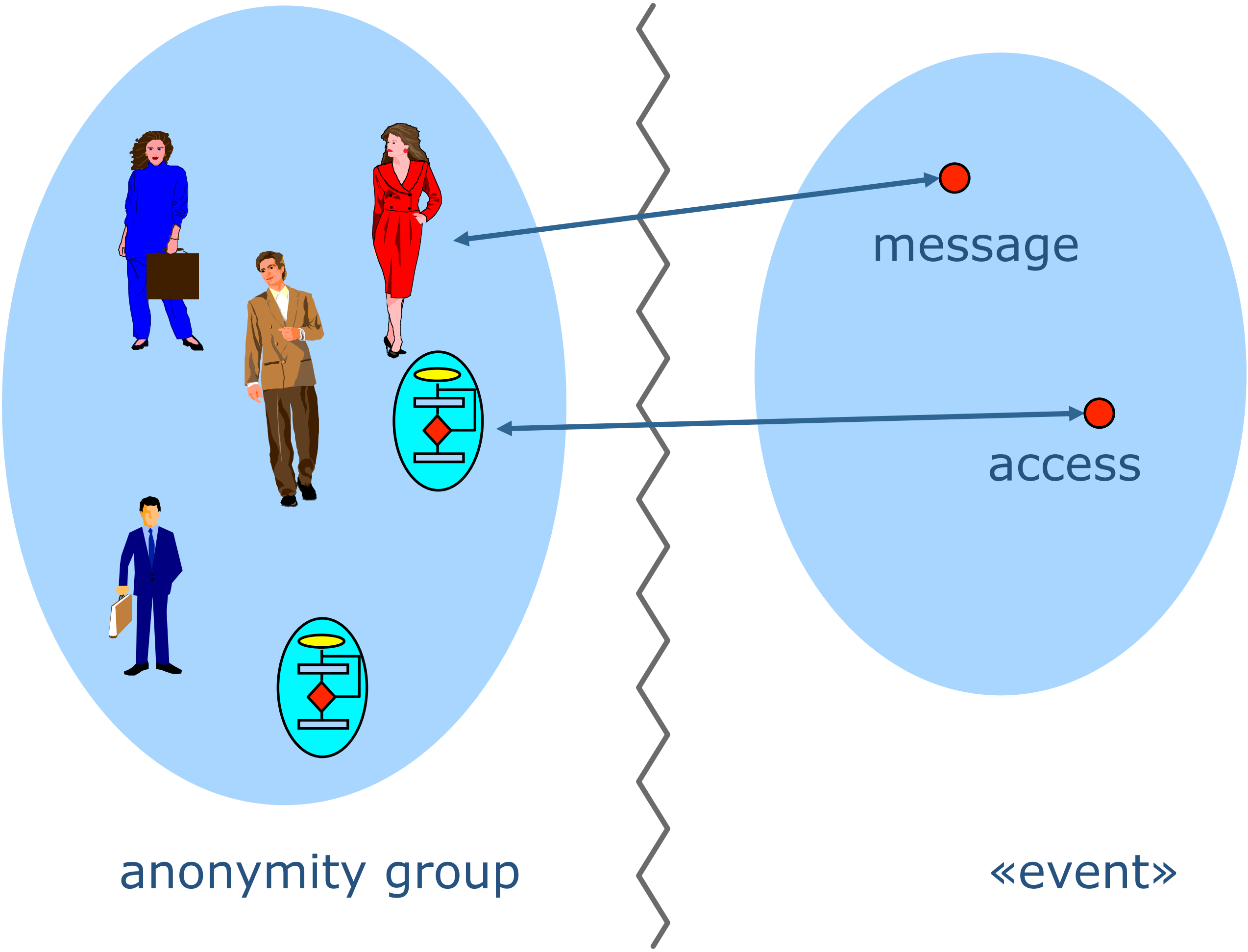
Sender

Location

Recipient

- Privacy mostly seen as confidentiality
  - Protection of the contents of messages
    - Encrypted data storage and data transfer
  - Protection of the identity of a user while using a service
    - Anonymity in counseling services
  - Protection of the communication relations of users
    - Users may know identity of each other

Privacy – protected in a crowd of other users and messages



message

access

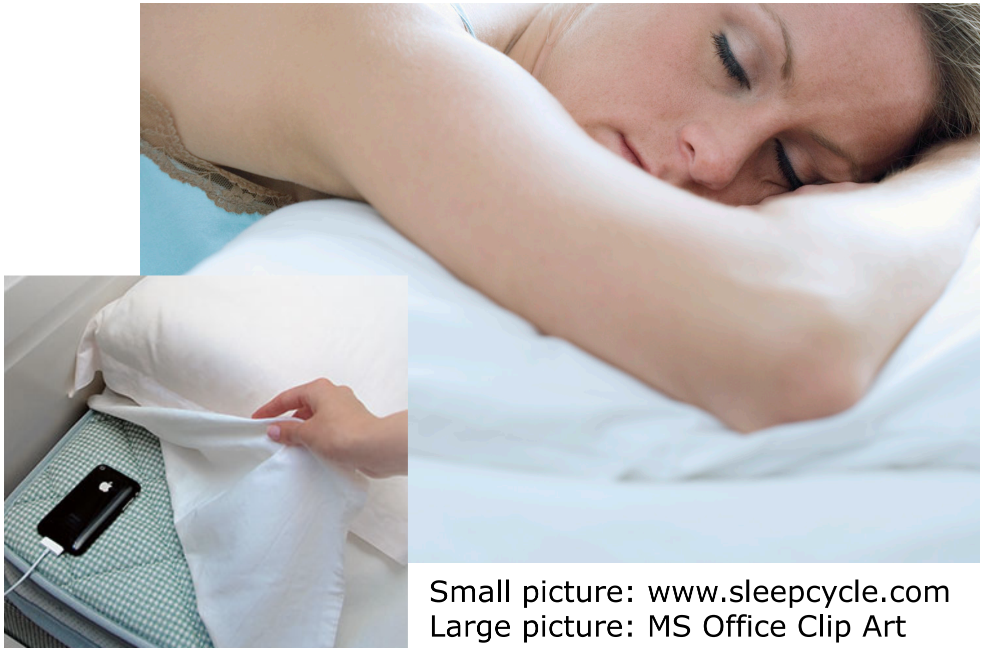
anonymity group

«event»

Everybody can be the originator of an «event» with an equal likelihood

Appification

- One app for one purpose
  - Taxi
  - Weather
  - Wikipedia
  - Shopping list
  - Writing app
  - Notebook
  - Doc scanning
  - Sleep rhythm
  - Running app



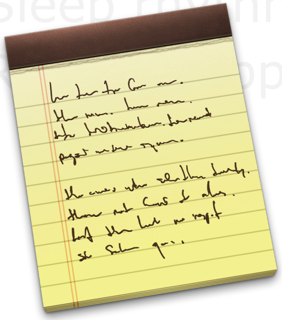
Small picture: www.sleepcycle.com
Large picture: MS Office Clip Art

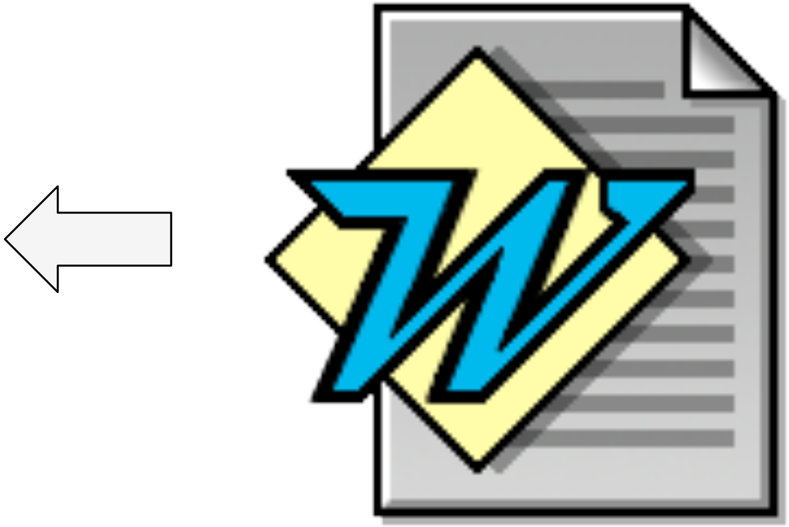
…

  - Video apps (product advertisement)
  - Torch apps

Appification

- One app for one purpose
  - Taxi
  - Weather
  - Wikipedia
  - Shopping list
  - Writing app
  - Notebook
  - Doc scanning
  - Sleep rhythm
  - R[illegible]pp
  - …
  - Video apps (product advertisement)
  - Torch apps



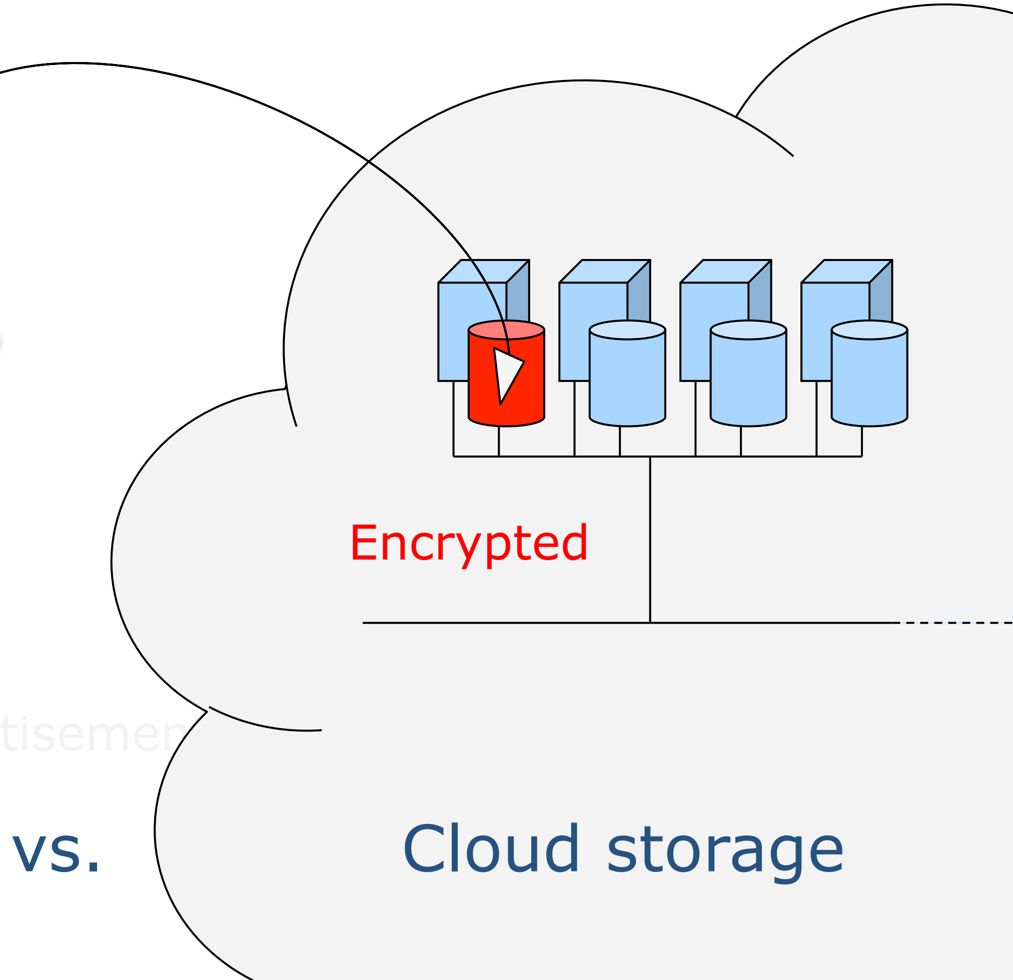


After

Before

Storage in the cloud

- One app for one purpose
  - Taxi
  - Weather
  - Wikipedia
  - Shopping list
  - Writing app
  - Notebook
  - Doc scanning
  - Sleep rhythm
  - R [illegible] pp
  - …
  - Video apps (product advertisemen
  - Torch apps



Encrypted

Local storage vs. Cloud storage

Sensors

- Sensors in mobile devices make new apps possible
  - GPS
  - WiFi
  - Bluetooth
  - Microphones
  - Cameras
  - Motion sensors
  - Adapters for more sensors
    - Personal: heart rate monitors
    - Environmental
      - Cars: CAN bus adapters
      - Houses: smart meter, heater, alarm system

http://blog.digifit.com/wp-content/uploads/2011/02/

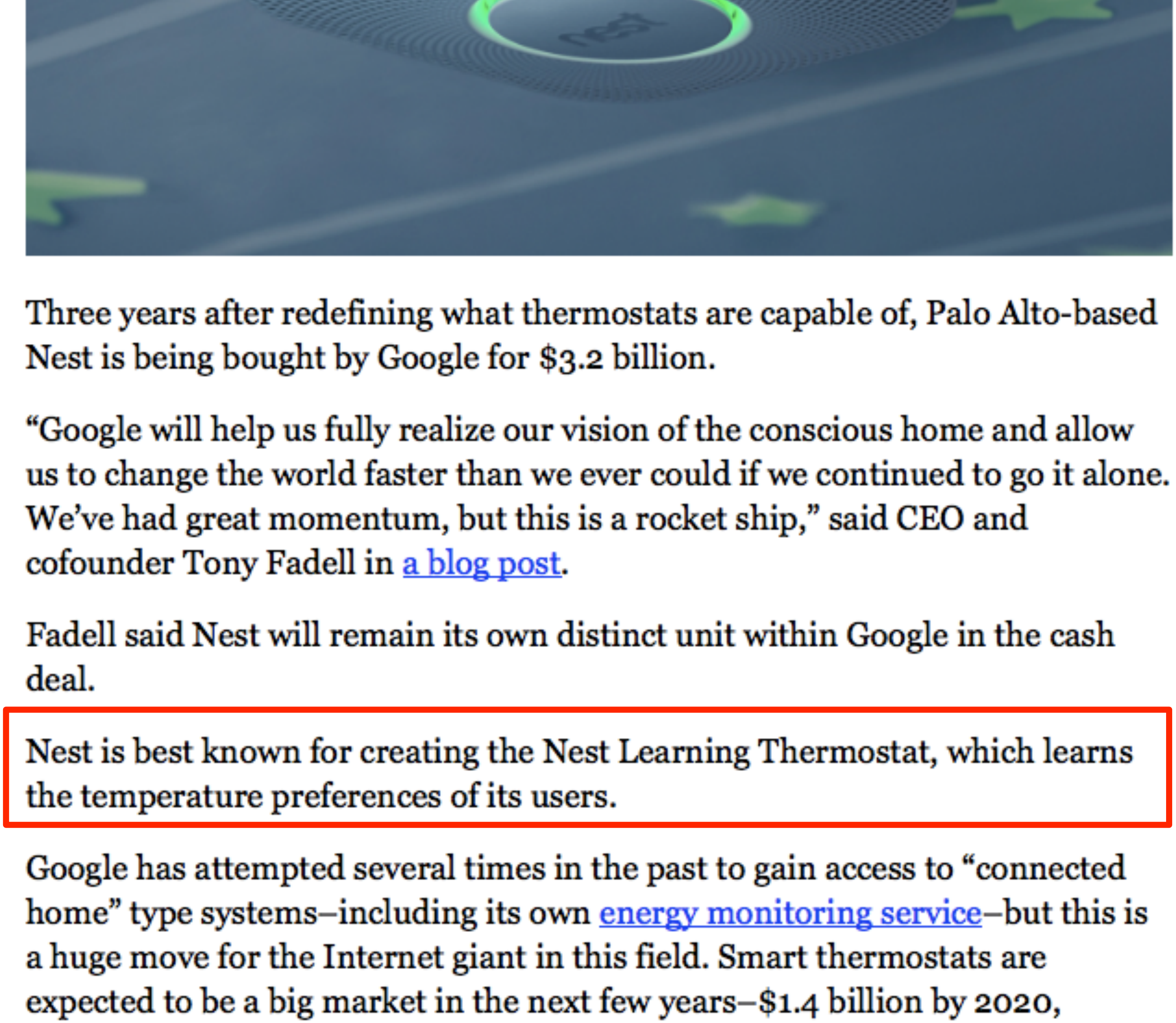
… and new tracking possibilities reality

Example: Sensors in Houses: smart meter, heater, safety

Forbes

Google Acquires Smart Thermostat Maker Nest For $3.2 Billion

http://www.forbes.com/sites/aarontilley/2014/01/13/google-acquires-nest-for-3-2-billion/print/



Three years after redefining what thermostats are capable of, Palo Alto-based Nest is being bought by Google for $3.2 billion.

“Google will help us fully realize our vision of the conscious home and allow us to change the world faster than we ever could if we continued to go it alone. We’ve had great momentum, but this is a rocket ship,” said CEO and cofounder Tony Fadell in a blog post.

Fadell said Nest will remain its own distinct unit within Google in the cash deal.

Nest is best known for creating the Nest Learning Thermostat, which learns the temperature preferences of its users.

Google has attempted several times in the past to gain access to “connected home” type systems–including its own energy monitoring service–but this is a huge move for the Internet giant in this field. Smart thermostats are expected to be a big market in the next few years–$1.4 billion by 2020,

http://www.forbes.com/sites/aarontilley/2014/01/13/google-acquires-nest-for-3-2-billion/print/

Useful stand alone apps

- Access to sensors is needed
  - APIs (Application Programming Interfaces) usually have no access to special hardware features
  - Some platform independent APIs for camera, mic available (e.g. flash)
- Local storage of data
  - Always if access in Offline situations is needed
  - Always if privacy aspects speak for local storage
- Special interface design (needed)
  - Mostly hardware dependent features

- Alternative for simple server-based apps without these ⇧ needs
  - type URL in browser
  - look & feel is rebuilt

Appification …

- leads to a technology shift in tracking techniques
  - Server based tracking was and is always possible
    - Get IP address
    - Store an access log
  - Client based tracking needs tracking functionality on user devices – provide an app
    - Tracking at the source
    - No control of data leakage by end user
    - Full access by app provider

- Most apps are based on a browser engine
  - Online component of app could be realised as web service, useable in browser
  - Example: News magazines
    - App and mobile web pages: same info and look & feel
    - No need for an app (technically spoken)

Which data an app is usually sending

- Controlled by the app
  - Date/Time of start and stop of app and/or
  - Date/Time of start and stop of particular app functions
  - possible: any data within app

- Controlled by operating system (after granting access)
  - Global Identifiers: WiFi name (SSID), Serial Number of Device, …
  - Location (based on different techniques: GPS, CI, TOA, …)
  - Address book entries (r/w)
  - Possible: any data stored on device

- Different models: User
  1. is not informed about any access or transmission of data
  2. is informed about requested privileges before installation
  3. has to confirm access to data and sensors at first run
  4. confirms access whenever app wants access to data or sensors

Access control models – differences between systems

- iOS (earlier versions):
  - No access control (trust)
- Android:
  - During installation or updating an app:
    - User can read which sensors or data the app is requesting for
    - Very fine-grained information but: all or nothing
  - While running the app:
    - Trust (based on the privileges granted during installation)
- iOS (newer versions):
  - During installation or updating
    - Trust
  - while running:
    - First time the app is requesting for rights, user has to confirm or reject access
    - Can be changed afterwards in device settings
    - Limited to location, network access and address book

Example 1

- Torch app
  - Free of charge
- Before installation:
  - User reads feature list (they promise everything)
- During installation:
  - App asks for privileges
    - App will read address book entries
    - App will connect to the Internet
- After installation:
  - App is allowed to do everything within its privileges
  - Can ask for more rights

Example 2

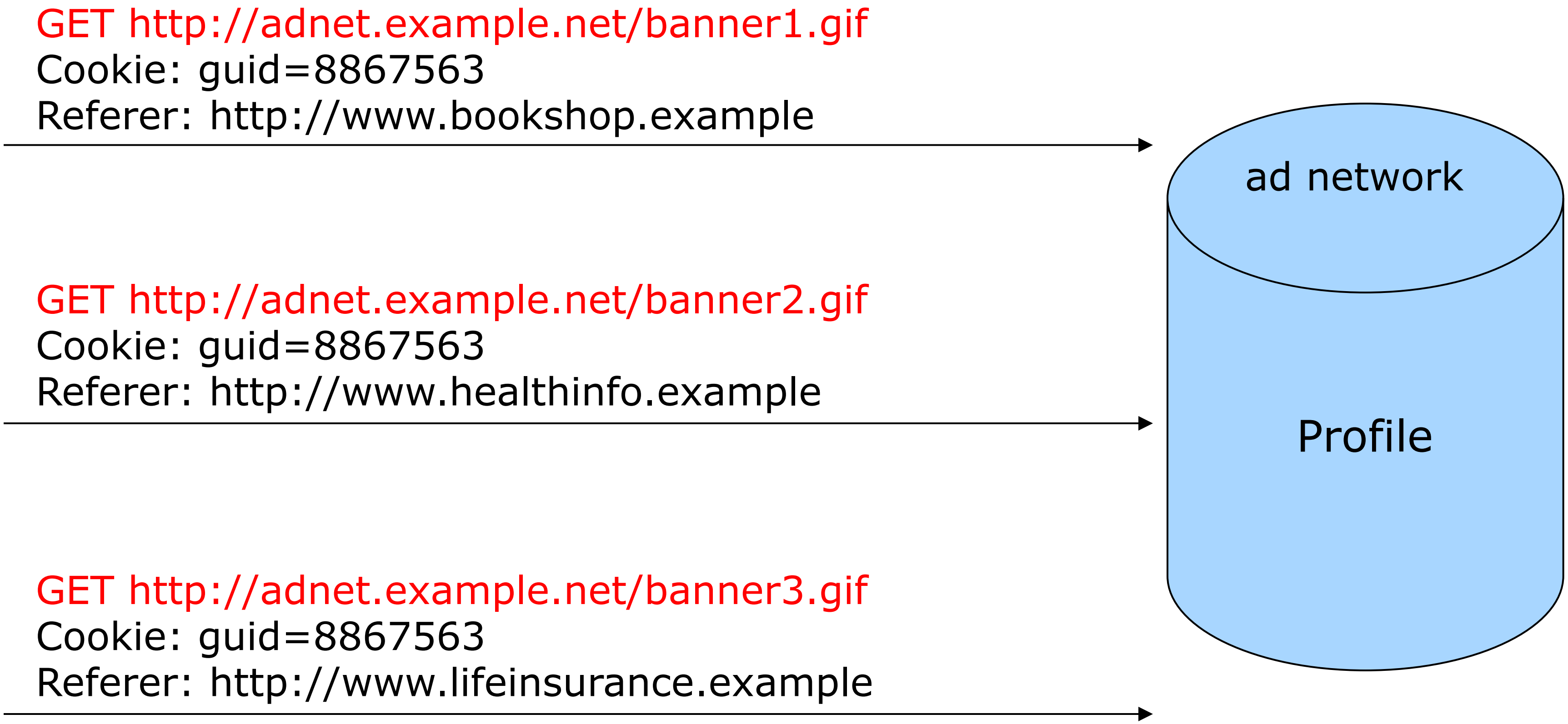
- Railway app
  - Find travelling connections

- Comfort functions available
  - App asks for address book access (faster input of destination)
  - App asks for location information (faster input of current location)
- Although if not granted
  - App works fine

- Optimizations: confirmation while running
  - Location on/off
  - Access to single address book entries

- Confirmation every time while running
  - Needs to be implemented in OS

Third-Party Cookies



GET http://adnet.example.net/banner1.gif
Cookie: guid=8867563
Referer: http://www.bookshop.example

GET http://adnet.example.net/banner2.gif
Cookie: guid=8867563
Referer: http://www.healthinfo.example

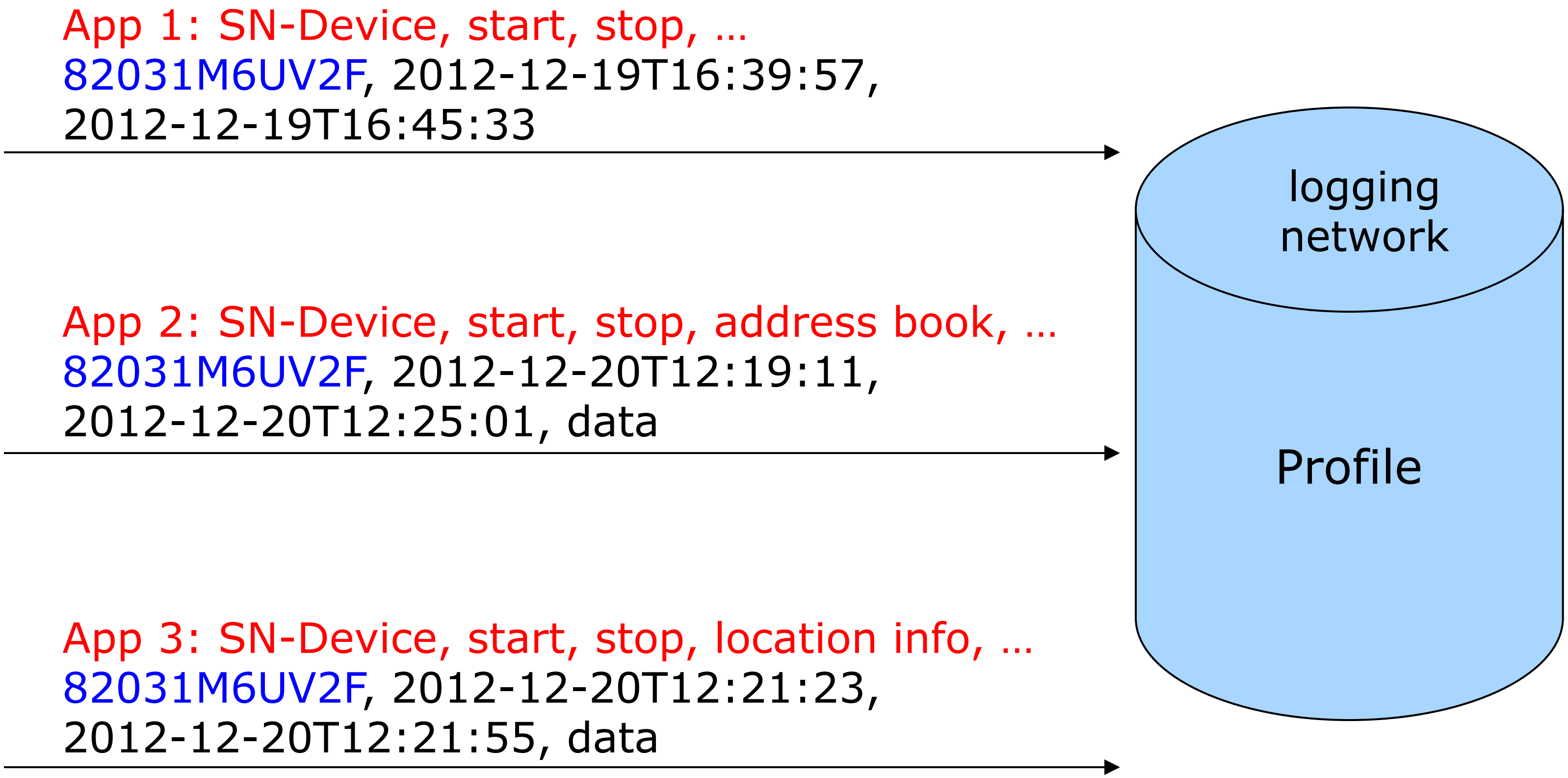
GET http://adnet.example.net/banner3.gif
Cookie: guid=8867563
Referer: http://www.lifeinsurance.example

ad network

Profile

Delete cookies when closing the browser

Logging networks



App 1: SN-Device, start, stop, …
82031M6UV2F, 2012-12-19T16:39:57,
2012-12-19T16:45:33

App 2: SN-Device, start, stop, address book, …
82031M6UV2F, 2012-12-20T12:19:11,
2012-12-20T12:25:01, data

App 3: SN-Device, start, stop, location info, …
82031M6UV2F, 2012-12-20T12:21:23,
2012-12-20T12:21:55, data

Question: How to delete this data?

Security model

- Technical background
  - Every app has a (registered) digital certificate
  - Necessary to identify the app provider
  - Used to identity the app during and after installation

- Privileges are bound
  - to a particular app
  - to a app provider (any app of this provider/developer)

- Concepts are not limited to mobile devices and can be used on every computer
  - Windows 8 implements some of these features (TPM Spec. 2.0)
  - Digital rights management is the driver

The concept of trusted computing

- Privilege management in the Appification context
  - Technically based on trusted computing
  - Trusted computing is a hardware-based approach
    - Trusted Platform Module (TPM)
- Good news: malware protection is easy
  - App provider of malware can be identified afterwards
  - Certificate of app (and/or app provider) will be revoked
    - Remark: This conforms to the security model of classical integrity mechanisms.
    - Idea: We cannot protect from damage, but defend attacks: violations will be prosecuted.
    - Similar approach: virus detection as a consequence of a first few infections
- Bad news: end users lose control over their hardware devices
  - Censorship of apps
  - Deactivation of apps

What is needed

- At least: Informed consent by user
- Activism: App testing and classification regarding privacy
- Standards: Privacy profiles for classes of applications
- Law: App providers really must respect laws
- Best: External privacy certification (app privacy seal)

- Worst: current situation

- Regulations needed
  - Inform the users what and why data is used (transparency)
  - Restrict to the necessary (principle of data minimization)
  - International regulations or national laws applicable to app providers

  - Remark: Self commitments of app providers are useless

What is needed

- Before installation: Detailed information of end user about
  - privileges requested by an app and why requested
  - identity of developer and/or app provider (incl. certificate)
- While installation
  - Confirmation on all requested privieges
  - Usability aspect: automatic confirmation for some (harmless) classes of privileges (i.e. Internet access) might be acceptable, however, this will probably be app-dependent
- After installation
  - Fine-grained, understandable and clear access control mechanisms
- Within app
  - No logging functions without user consent

Closing remarks

- Before shift to Mobile Applications
  - Multi-purpose apps, browser-based services
  - Many general problems lead to regulation
    - Cookie example: Directive 2002/58 on Privacy and Electronic Communications
- Appification
  - many single-purpose apps
  - developers lost the scope
    - user has no control about tracking techniques used in apps
    - everything is possible
    - “What are the general principles of privacy?”
- Next steps
  - Privacy classification of apps
  - Find generalised approach for regulation
  - Privacy seal for app

Prof. Dr. Hannes Federrath
Computer Science Department
University of Hamburg
Vogt-Kölln-Straße 30
D-22527 Hamburg

E-Mail federrath@informatik.uni-hamburg.de

Phone +49 40 42883 2358

http://svs.informatik.uni-hamburg.de

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG