Security of Wireless/Mobile Networks

Claude Castelluccia – INRIA – 2013
Claude.castelluccia@inria.fr

Course Outline (lectures)

1. Introduction to Wireless/Mobile Network Security
   - Why is it different?

2. Security of WiFi networks
   - 802.11 architecture and protocols
   - (un)authorized access: MAC filtering, WEP, WPA, 802.1X, 802.11i

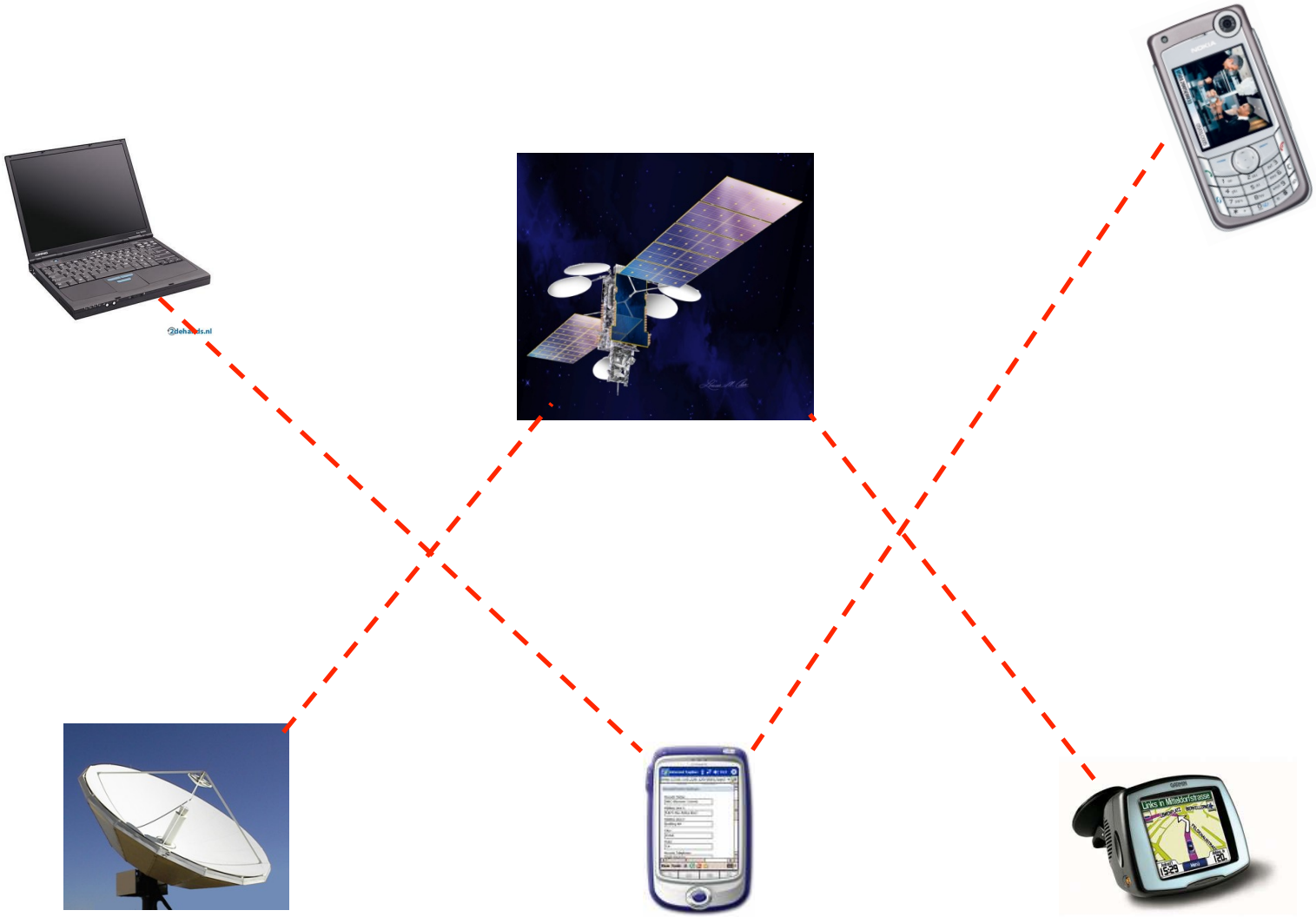
3. Smart Phone Security and Privacy

4. Mobile Privacy

5. WSN and RFID Security

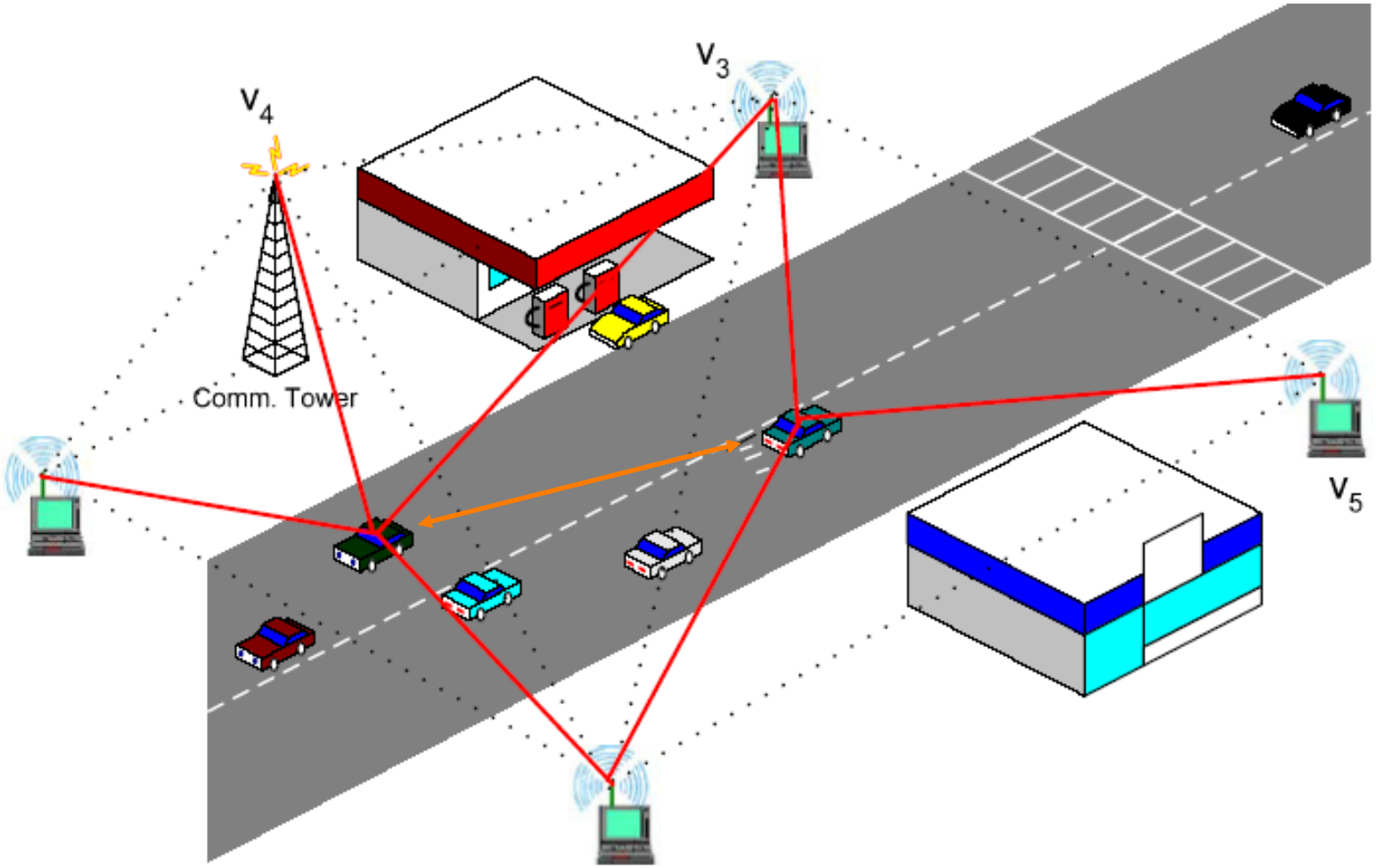
Wireless Networks

Mobile services/devices...

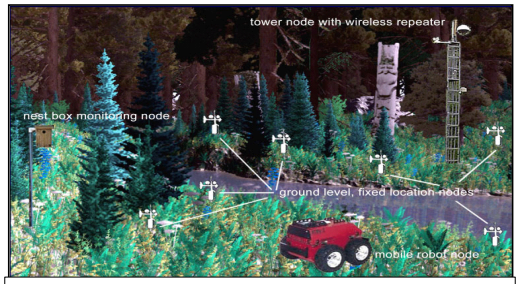


Smart Phones

Vehicular Networks



Wireless Sensors



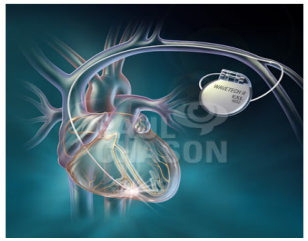
Environmental Monitoring

Interactive VR Game

Wearable Computing

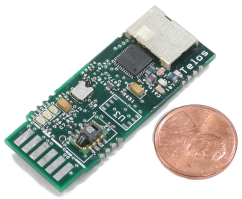
Disaster Recovery

Earth Science & Exploration



Immerse Environments

Wireless Sensor Networks

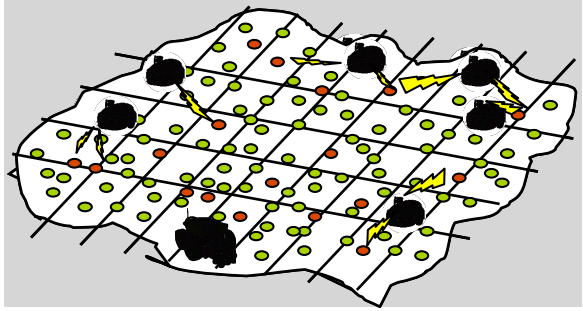


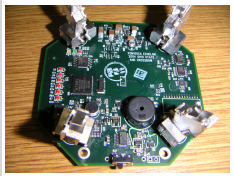
Hazard Detection

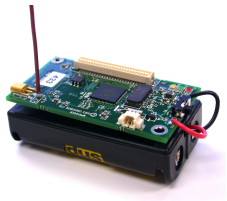
Smart Evironment

Linear Structure Protection

Military Surveillance







Road Safety

RFID devices

Applications of Wireless Networks

- **Infrastructure-based**
  - Cellular - ANY DATA
  - WiFi access – ANY DATA
  - GPS – LOCATION, TIME
  - Local Area (Indoor) Navigation – LOCATION, TIME
- **Infrastructure-less** (multi-hop)
  - Sensor networks – ENVIRONMENTAL (SENSED) VALUES
  - Ad hoc (e.g. vehicular network) – ANY DATA
  - Mesh networks (e.g., home networks) – ANY DATA
- RFID tags – IDENTITY

Different networks/topologies/services (data, location, time…)

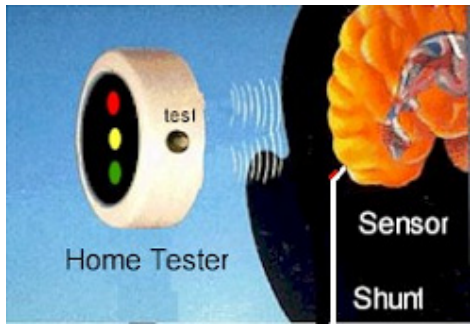
The Software is Eating the World

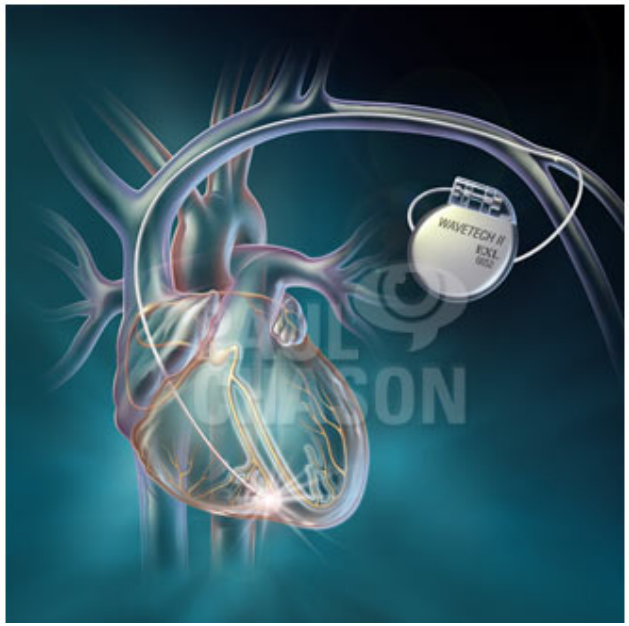
- Software is now everywhere!
- Medical devices
- Powerplant
- Cars
- Houses
- … and many more in the future

- We have to make sure that these systems are secure…
  - Otherwise we will leave a nightmare!
  - Pacemakers will be attacked!
  - Powerplants will be attacked (stuxnet)
  - ….

Example: Implantable Medical Devices

- More and more IMD use wireless com.
  - Ease configuration
  - Allow to store and download data remotely(measures)
  - Remote monitoring of patients

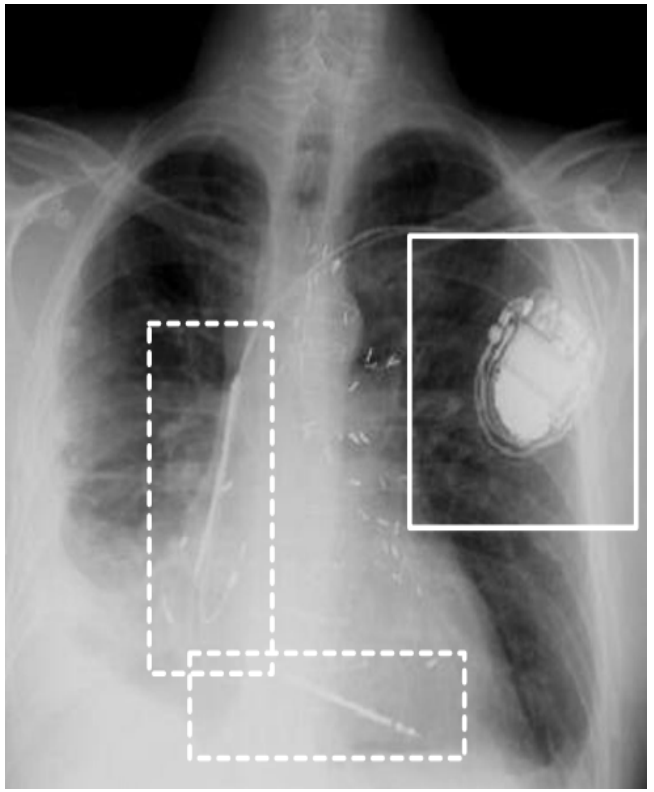




Pacemakers and Defibrilators

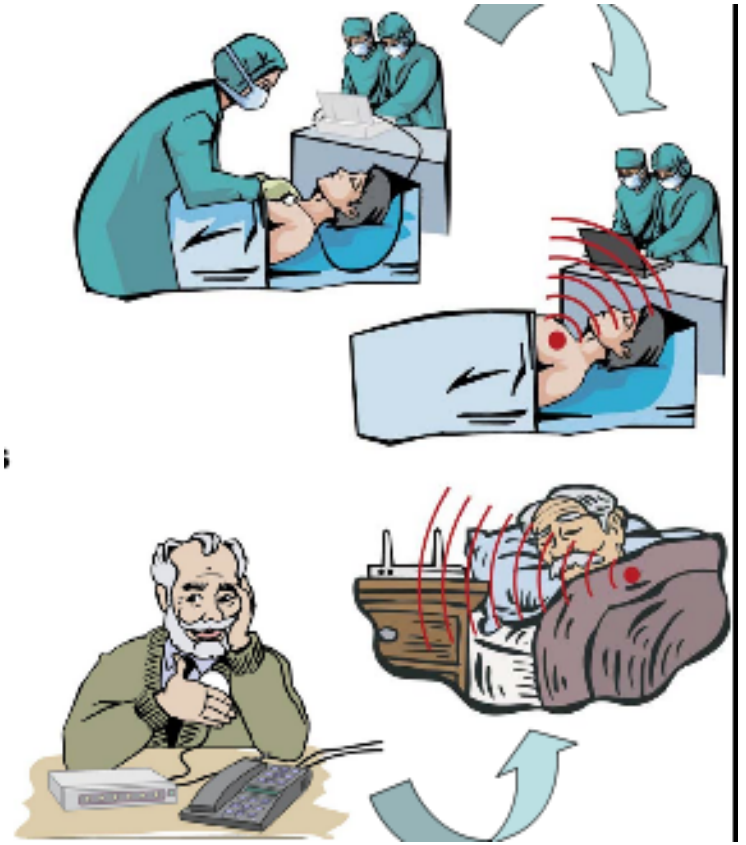
- Stimulateur Cardiaque (Pacemaker): émet périodiquement des petits stimulis électriques au cœur

- Défibrillateur: émet des stimulis plus puissants pour restaurer un rythme “normal”

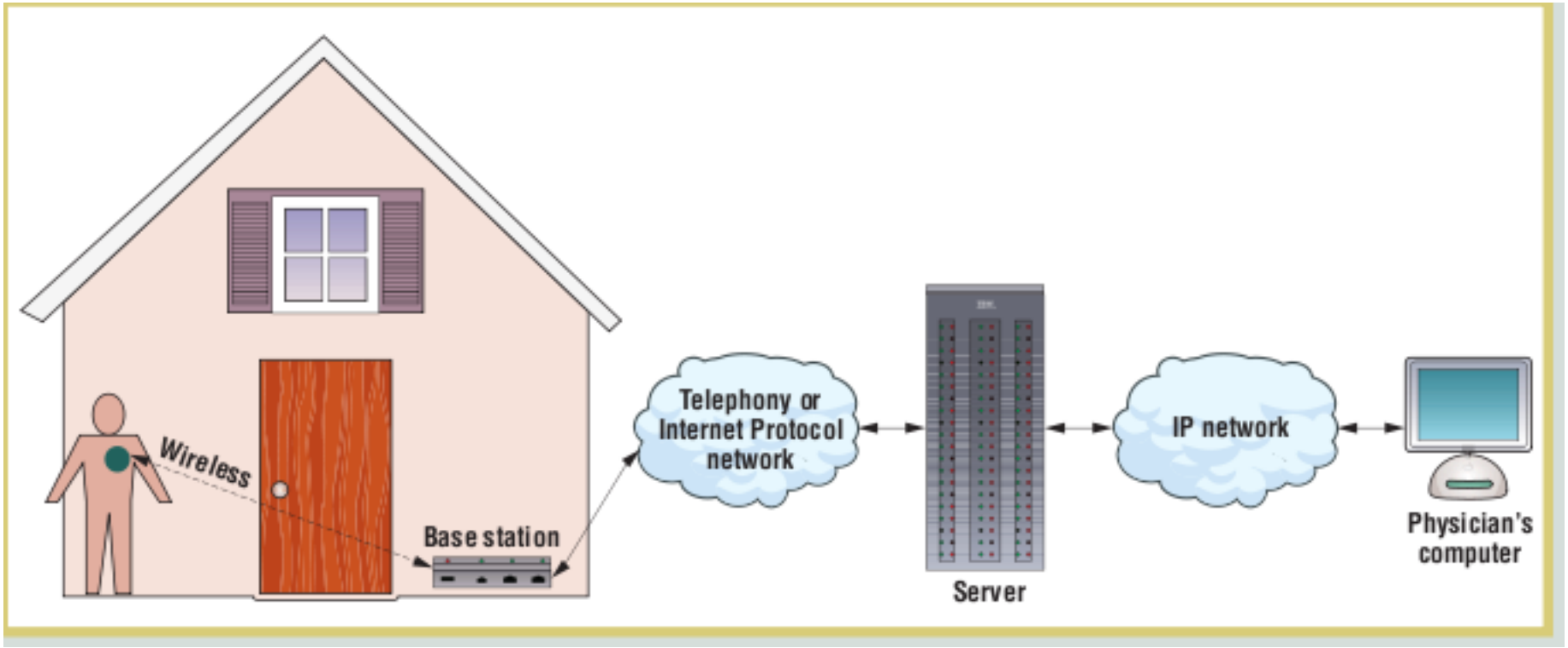


Les implants médicaux: Pacemakers/défibrillateurs

- Current systems
  - Ultra-low-power CPU + 128 ko. RAM (donnée patient, log,…)
  - Communication by induction
  - Short range
    - Contact with patient
  - Limited Bandwidth
- New systems
  - Longer range (~2m)
    - Remote monitoring of patients
    - Ease configuration and installation
  - More Bw (~400 kbits/s)
    - Enable new applications
    - Reduction consultation time

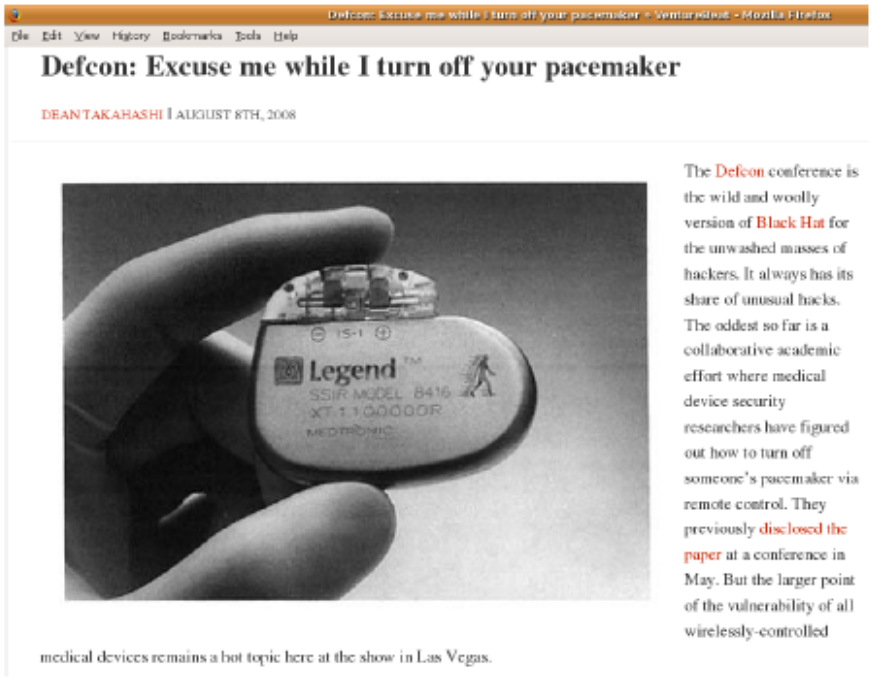


IMD: New Applications



- problèmes de confidentialité, intégrité
- le médecin peut lire les données a distance…
- …mais bientôt il pourra les modifier par l'Internet!!

Existing Attacks



Defcon: Excuse me while I turn off your pacemaker - VentureBeat - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Defcon: Excuse me while I turn off your pacemaker

DEAN TAKAHASHI | AUGUST 8TH, 2008

The Defcon conference is the wild and woolly version of Black Hat for the unwashed masses of hackers. It always has its share of unusual hacks. The oddest so far is a collaborative academic effort where medical device security researchers have figured out how to turn off someone's pacemaker via remote control. They previously disclosed the paper at a conference in May. But the larger point of the vulnerability of all wirelessly-controlled medical devices remains a hot topic here at the show in Las Vegas.

`http://venturebeat.com/2008/08/08/defcon-excuse-me-while-i-turn-off-your-pacemaker/`

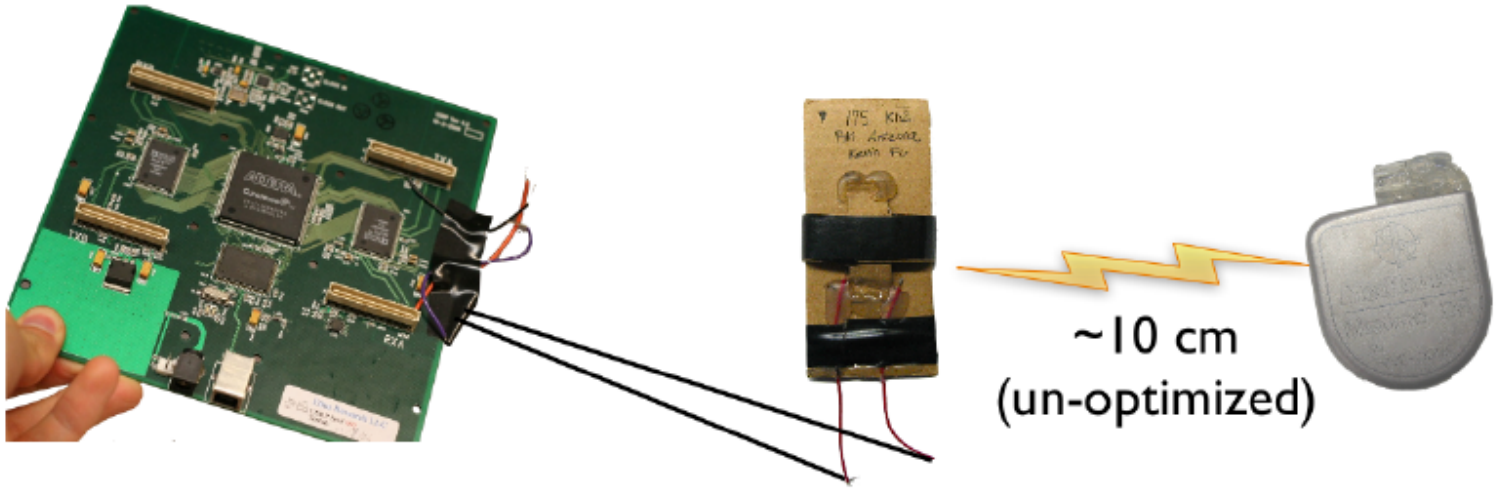
`http://www.secure-medicine.org/icd-study/icd-study.pdf`

- Replay attacks. Attacker needs little knowledge
- Trigger information disclosure
- Change patient name
- Change ICD clock
- Change therapies (disable functions)
- Induce fibrillation

[1] Halperin and al., Pacemakers and implantable cardiac defibrillators: Software radio attacks amd zero-power defenses, IEEE Security and Privacy, Oakland, 2008.

Attack – Build Device Programmer

- Software radio
- GNU Radio software, $0
- USRP board, $700
- Daughter boards, antennas: $100



Attack – Eavesdrop On Private Data

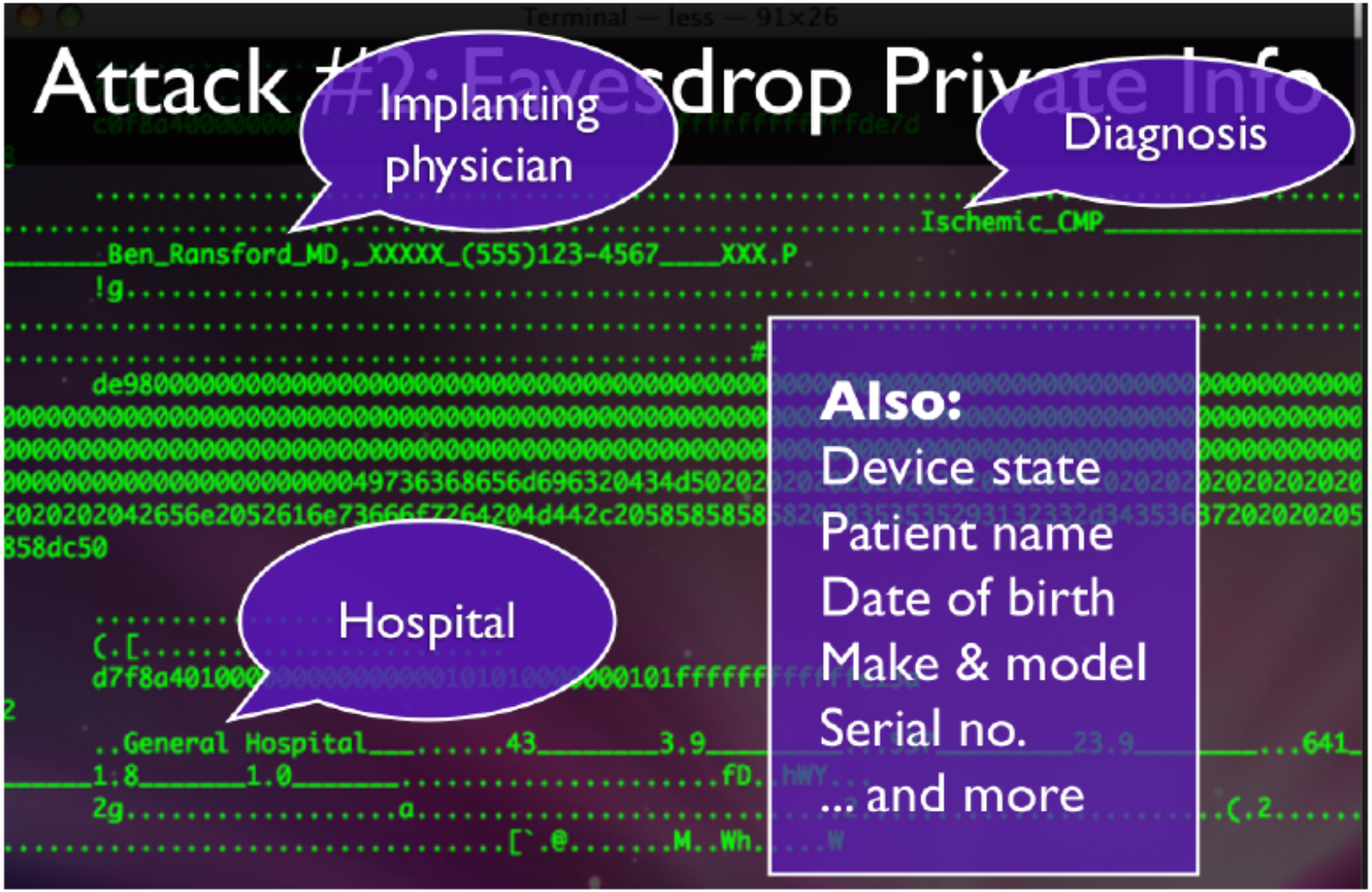


Figure is "borrowed" from *Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power*

4 Years Later….

Home / Security News / Hackers

Hacked terminals capable of causing pacemaker deaths

By Darren Pauli on Oct 17, 2012 12:33 PM
Filed under Hackers

Security holes enable attackers to switch off pacemakers, rewrite firmware from 30 feet away.

Breakpoint 2012 was a hit.

Breakpoint swag.

The Ruxcon 2012 logo.

Pourquoi ce manque de Sécurité ?

- Juger inutile (par les fabriquants) car nécessite d'être proche du patient
  - Mais attaquant peut utiliser un équipement non standard (amplificateur, antenne puissante,…)
- Coûteux en terme de ressource
  - CPU, bande passante, mais surtout énergie!
  - Réduit la durée de vie!
- Compromis Sécurité/Sureté!
  - La sécurité ne doit pas mettre la vie du patient en danger en cas d'urgence!
    - Les attaquants ne doivent pas avoir accès aux données…mais les données doivent être disponibles en cas d'urgence…!
    - Un attaquant ne doit pas pouvoir desactiver l'appareil mais un medecin doit absolument le faire en cas d'urgence.

Sécurité des pacemakers/ Un problème très difficile…

- Authentification des lecteurs
  - Gestion des clefs est difficile?
    - Capteur configuré avec une clef et la clef est donnée au médecin traitant…
      - Mais comment faire si le patient voyage ou admit d'urgence?
      - Carte a puce?
    - Pas de solution idéale!!…
  - Comment révoquer des lecteurs?
    - PKI?

Sécuriser les Pacemakers (2)

- Comment éviter les attaques de type déni de service??
  - Cryptographie/Sécurité Coûte cher en terme d'énergie
  - Un attaquant pourrait émettre des fausses requêtes d'authentification/autorisation
  - Le capteur consommerait sa pile pour rien ☹

Why is Wireless/Mobile Security Different?

Why is mobile security different?

- **Specificities:**
  - 1. Wireless links
    - Difficult to identify perimeters
    - DoS attacks: jamming,…
  - 2. Mobility
    - Connect to malicious access points
    - Location privacy

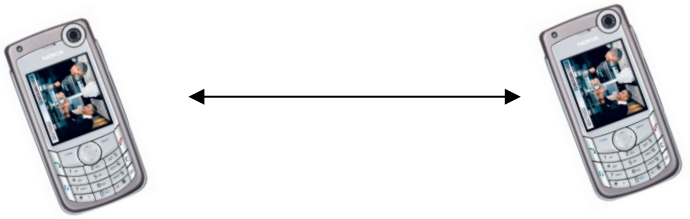
Why is wireless security different? (2)

- 3. Constrainted Devices
  - Small display
    - Not easy to enter long passwords…
  - Small CPU
    - Public key crypto. is hard
- 4. Battery Operated
  - Protocols/operations should optimize battery

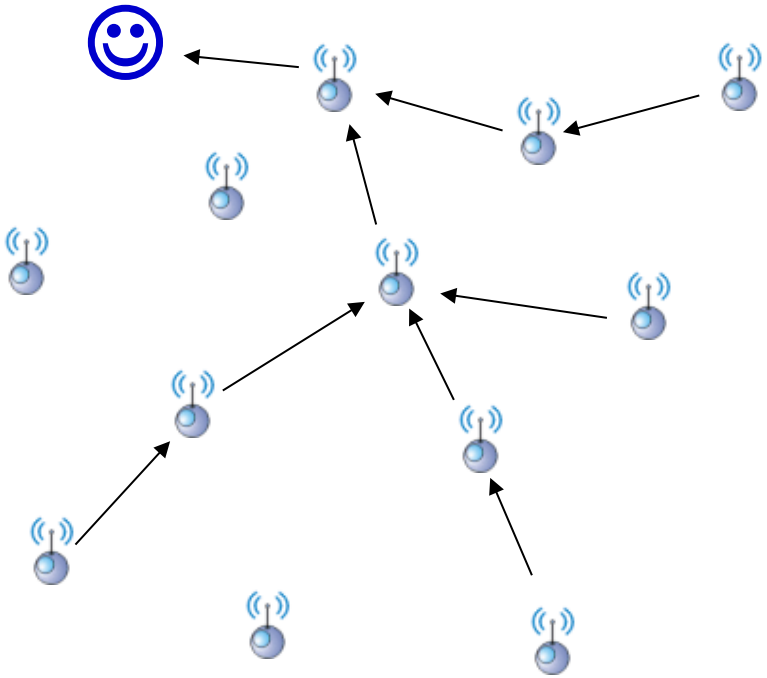
- Different devices with different security requirements
  - Voice security ≠ Sensor security

Application-specific constraints and security goals

Cellular networks
- infrastructure based
- single-hop (to the BS)



Informally: to **communicate privately!!!**
confidentiality is the prime security goal



Sensor Networks
- infrastructureless
- multihop
- node compromise
- node sabotage
- displacement
- ...

Informally: to accurately **measure and deliver sensed data**
confidentiality not an issue – data authentication is important

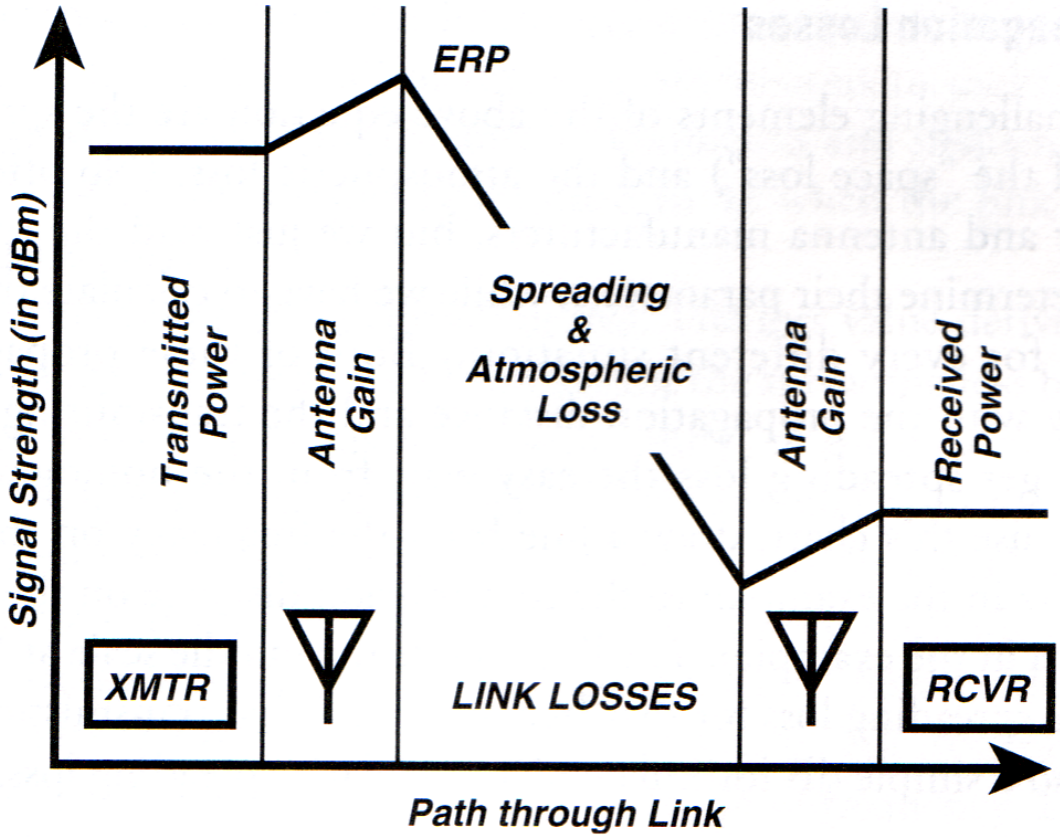
Wireless Communication Channel

Why security is more of a concern in wireless?

- no inherent physical protection
  - physical connections between devices are replaced by logical associations
  - sending and receiving messages do not need physical access to the network infrastructure (cables, hubs, routers, etc.)
  - Attacker can be far away from network!

- broadcast communications
  - wireless usually means radio, which (generally) has a broadcast nature
  - transmissions can be overheard by anyone in range
  - anyone can generate transmissions,
    - which will be received by other devices in range
    - which will interfere with other nearby transmissions and may prevent their correct reception (jamming)

Wireless channel



To calculate the received signal level (in dBm), add the transmitting antenna gain (in dB), subtract the link losses (in dB), and add the receiving antenna gain (in dB) to the transmitter power (in dBm).

Different Types of Attacks

- Passive attacks
  - The attacker is just listening and is not actively taking part of the communication
    - E.g. eavesdropping or snooping…

  Hard to detect in wireless com.….
- Active attacks
  - The attacker is able to alter the channel and/or modify/ inject messages to reach its goal
    - Message Forgery
    - Message modification/Man in the Middle
    - Denial of Service (flooding, jamming)

  Easier to perform in wireless com. (since no physical access control)…

Different Types of Attacks

Most existing attacks combine passive and active technique.

….

- Let's consider each of these attacks …

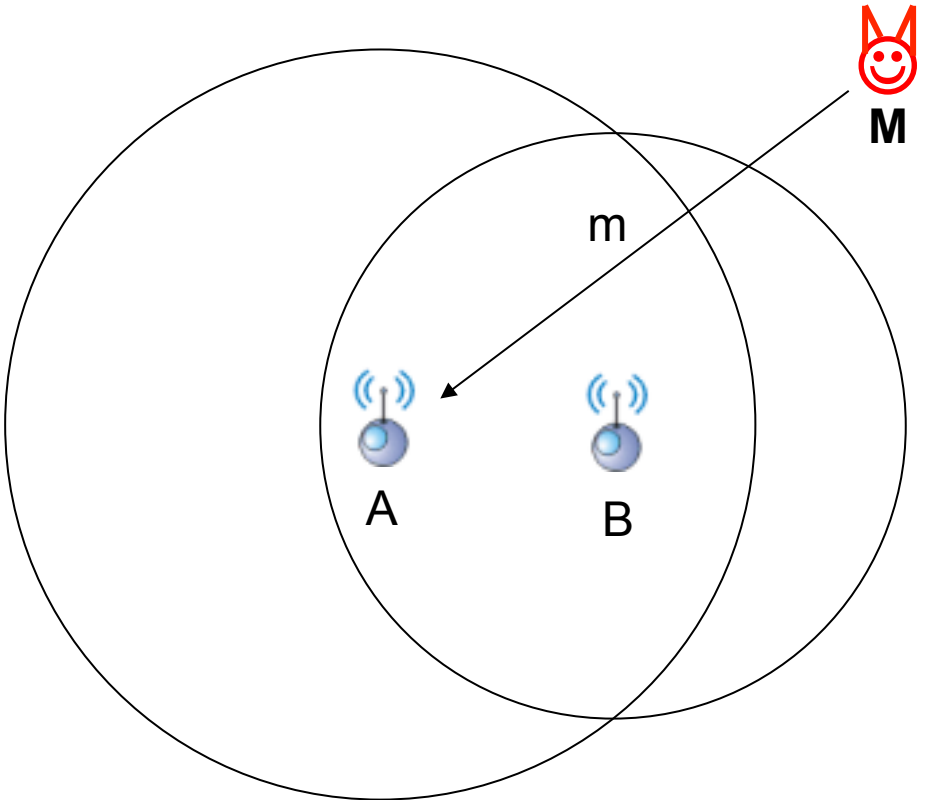
1. Snooping/eavesdropping attacks (passive attacks):

2. Modification Attacks (active attacks)

3. Denial of Service Attacks (active attacks)

1. Eavesdropping/snooping Attack

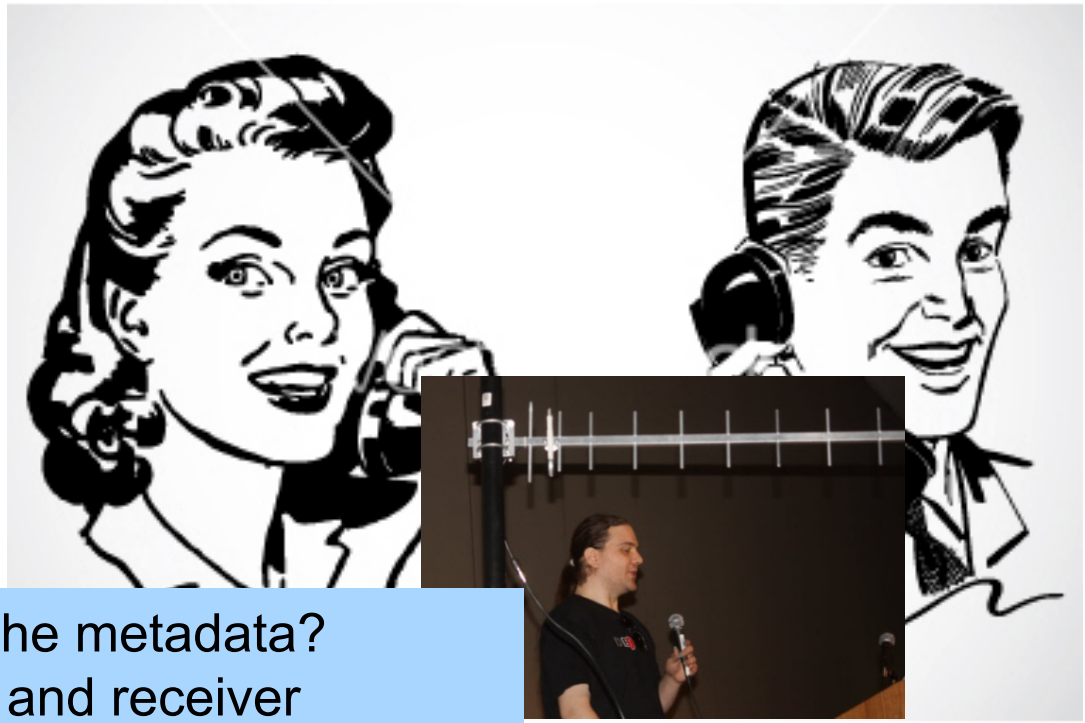
- the attacker is listening to the communication in order to access private information (emails, secrets,…)
- Precondition:
  - The attacker knows the frequency/modulation/coding on/by which the communicating parties exchange their information.



Snooping attack (passive attack)

- The proposed solution is ***encryption (WEP, 802.11i)***!
- But is encryption enough?

METADATA…



What are the metadata?

- Caller and receiver
- Caller and receiver current location
- Length of call
- …

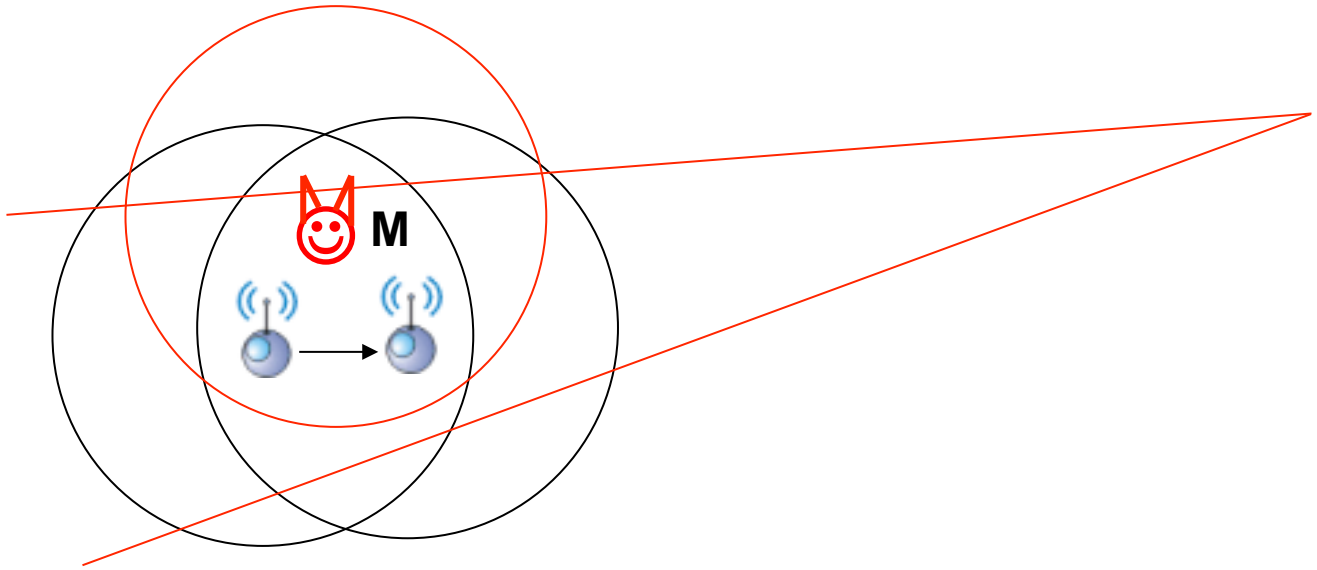
Snooping attack (passive attack)

- The proposed solution is ***encryption (WEP, 802.11i)***!
- But is encryption enough?
  - No, an attacker can still perform ***traffic analysis*** on encrypted data!
  - It can, for exemple, identify the number of access point and wireless devices …and eventually the network topology!
  - It can identify the traffic type (email, web browsing, VoIP, …) by looking at packet size and time information…
    - Even the VoIP language can be identified!
  - It can identify if someone is currently using the network (useful for robbery!)…this creates some privacy issue!

- Snooping is a major problem in wireless networks
  - An attacker can eavesdrop from very far with a directional antenna

Implications of antenna directionality on security

- Attackers can eavesdrop communication from much longer distances than anticipated
  - Attacks on Bluetooth (designed for 10m range) Reported eavesdropping from 3 km (LOS) !!!



2. Modification Attacks (active attacks)

- The attacker modifies:
  - The information contents (email, web,…)
  - The IP destination address to *redirect* traffic somewhere….
  - The IP destination address to *masquerade/ impersonate* another host/user!!
- There are at least 2 ways to modify a message:
  - The message is modified on the fly…
    - Difficult…
  - The message is intercepted, modified and then replayed: Man in the Middle (MiTM) attack!

Modification Attacks (active attacks)

- MiTM attacks is simple enough in wired networks
  - An attacker cuts the wire, receives all the data, modifies them and re-injects them
  - An attacker can corrupt a router…
- MiTM is more difficult in wireless networks! Why?
  - No wire to cut! The attacker must stop the receiver from getting the message on the initial transmission…
  - Difficult but not impossible!

- So how to protect against Modification attacks??

Modification Attacks (active attacks)

- Mutual authentication!
  - Alice authenticates Bob's messages
  - Bob authenticates Alice's messages

Modification Attacks (active attacks)

- For example:
  - Bob gets and verifies certificates/credentials from Alice
  - Alice gets and verifies certificates/credentials from Bob

  - Alice and Bob establish a secret key using Diffie-Hellman key exchange protocol..
  - Messages are authenticated using a MAC (message authentication code)

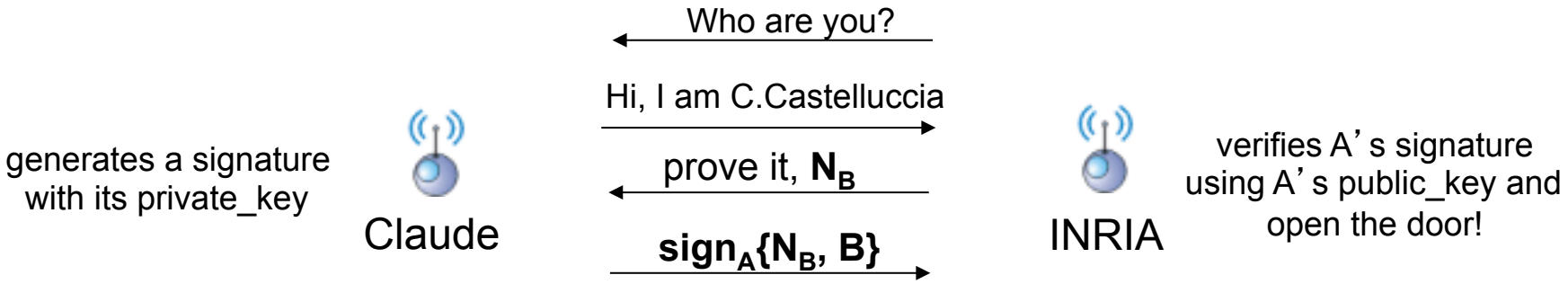
    Or
  - Messages are signed….

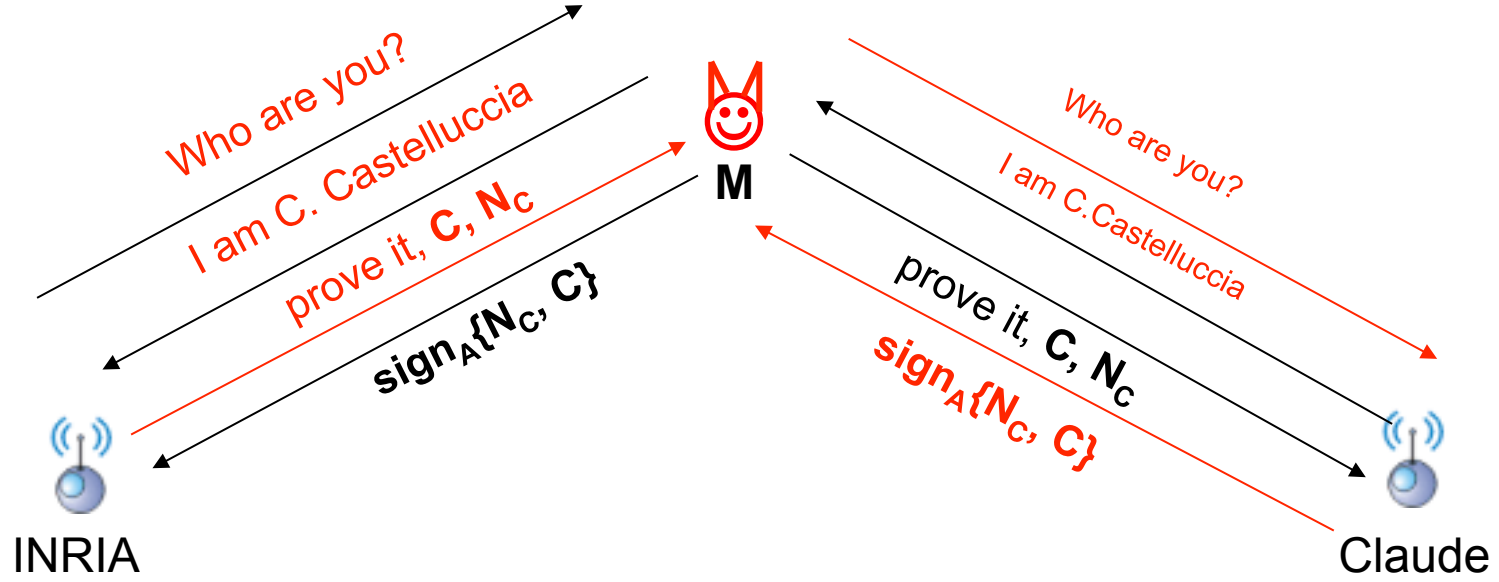
Modification Attacks (active attacks)

- Mutual authentication is efficient in most of the cases …but not always ☹!!!

Message relay

- Door access control- Does authentication help?





verifies A's signature using A's public_key and open the door!

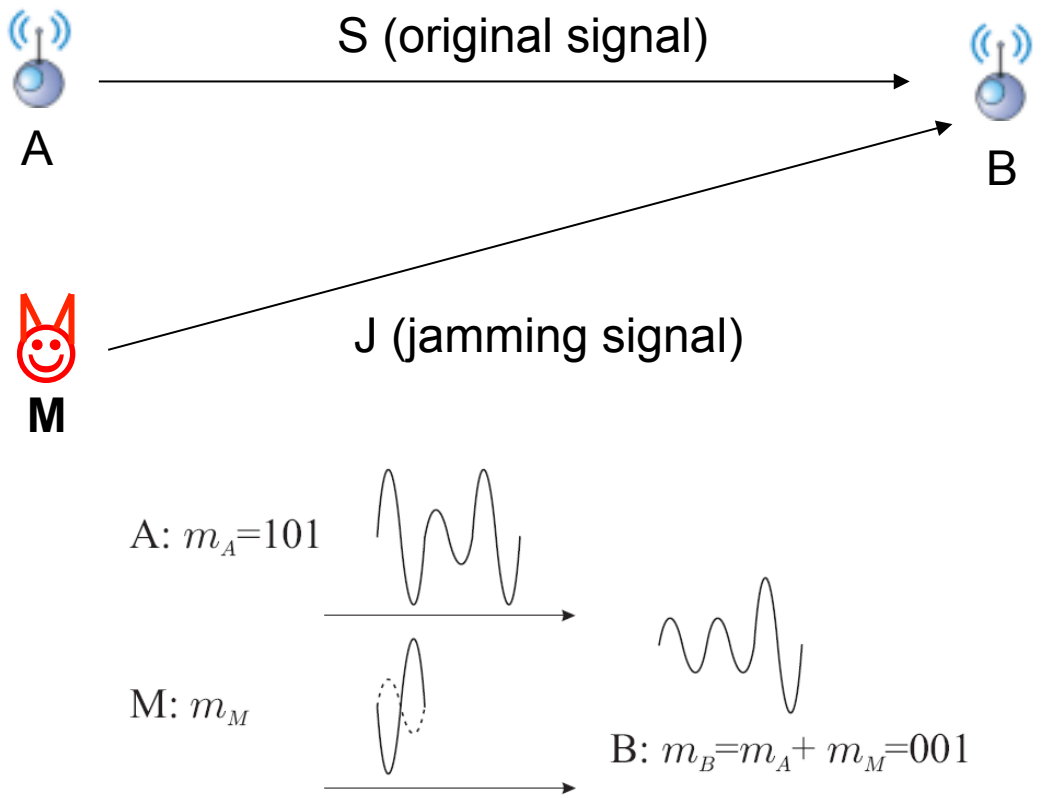
Authentication does not help!

3. Denial of Service Attacks (active attacks)

3. Denial of Service Attacks.
   - The goal of the attacker is to cause damage by preventing operation of the networks
   - DDoS: flooding a host with a huge number of packets…
   - In wireless networks, the most important DoS attack is jamming…
     - Add physical noise on the channel to corrupt messages…
   - These attacks are simple and very difficult (if not impossible) to prevent…

Adversarial interference: jamming

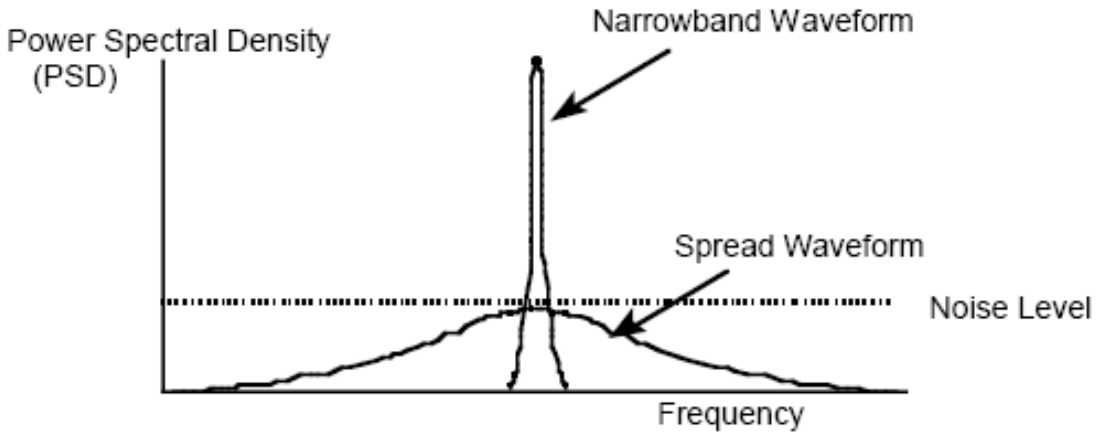
- Transmitting a signals on the same frequency on which the honest parties communicate
- Blocks the reception of the message at the receiver B



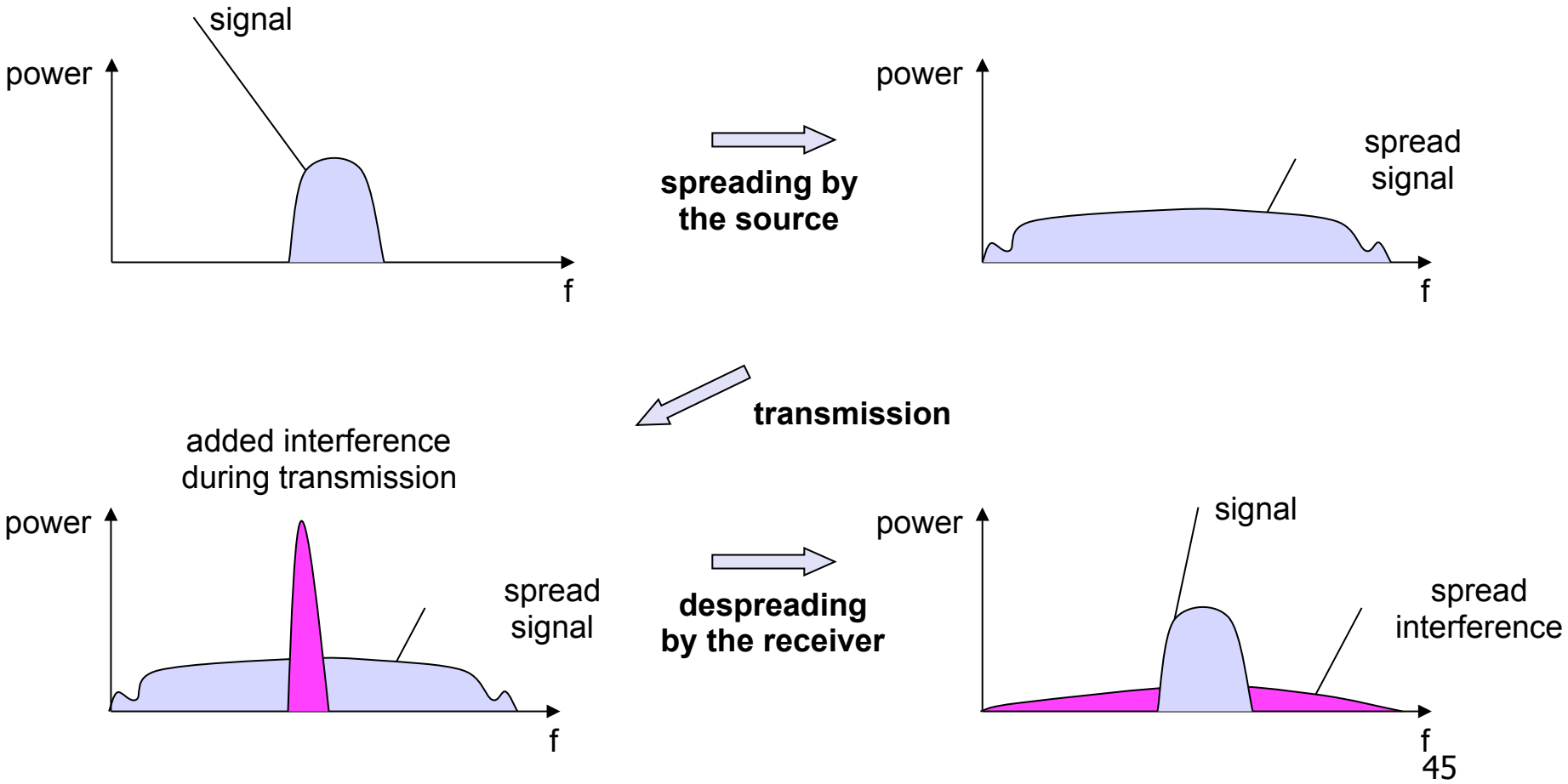
Simple amplitude modulation example

DSSS : Direct Sequence Spread Spectrum

- Secret spreading code – DSSS **HIDES** THE SIGNAL
- Signal detection is now more difficult
  - signal “hidden” in the noise
- Signal interception/modification difficult
- Jamming
  - narrowband jamming now requires much higher power
  - broadband jamming still effective



Spread spectrum : main idea



Spread Spectrum Techniques

There are two basic spread spectrum techniques:

- Direct Sequence Spread Spectrum (DSSS):
  - the signal is multiplied by a spreading code in the time domain
  - the spreading code is a pseudo random sequence that looks like noise
- Frequency Hopping Spread Spectrum (FHSS)
  - the signal changes of carrier frequency
  - sequence of frequency changes is determined via a pseudo random sequence

DSSS Technology

- The initial application of spread-spectrum (SS) techniques was for military applications
- SS investigation was motivated primarily by the desire to achieve highly jam-resistant communication systems
- It is now used in civil applications
  - Multiple Access (ex: CDMA) / Modulation
  - coordinated systems coexistence (ex: SS UMTS)
  - uncoordinated systems coexistence (ISM bands)

- *A system is defined to be a SS system if the signal occupies a bandwidth much in excess of the minimum bandwidth necessary to send the information*

Conclusion

- Wireless Security is hard because the attackers do not have to physically compromise the network!
- It is even harder for small wireless devices, such as RFID or sensor, that can't perform expensive crypto. Operations and can be physically compromised!
- Getting it right requires a lot of work!
  - Never design your own algorithm… use an existing (secure) one instead…
- In the following class, we give 2 examples:
  - What not to do! The WEP example!
  - How to do it…: 802.11i!

Finally: What about Privacy?

- The promises of new technologies
  - Implantable Medical Devices
  - Location-Based Services
  - Internet
  - Smart meters, sensors
- Privacy threats of new technologies
  - Leave traces (cookies, …)
  - Reveal a lot of information about users (e.g. smart meters)
  - Leak information
    - Directly: e.g. mobile aps
    - Indirectly: e.g.Inference attacks on OSN (Gaydar, ndss2012)

DATAVEILLANCE = DATA + SURVEILLANCE

- Systematic monitoring of people's actions or communications through the application of information technology.

- We leak data, leave traces when we are browsing the web or using our smart phone…
  - On the visible web
  - On the invisible web

- For economical or security reasons

Dataveillance on the « Visible » Web

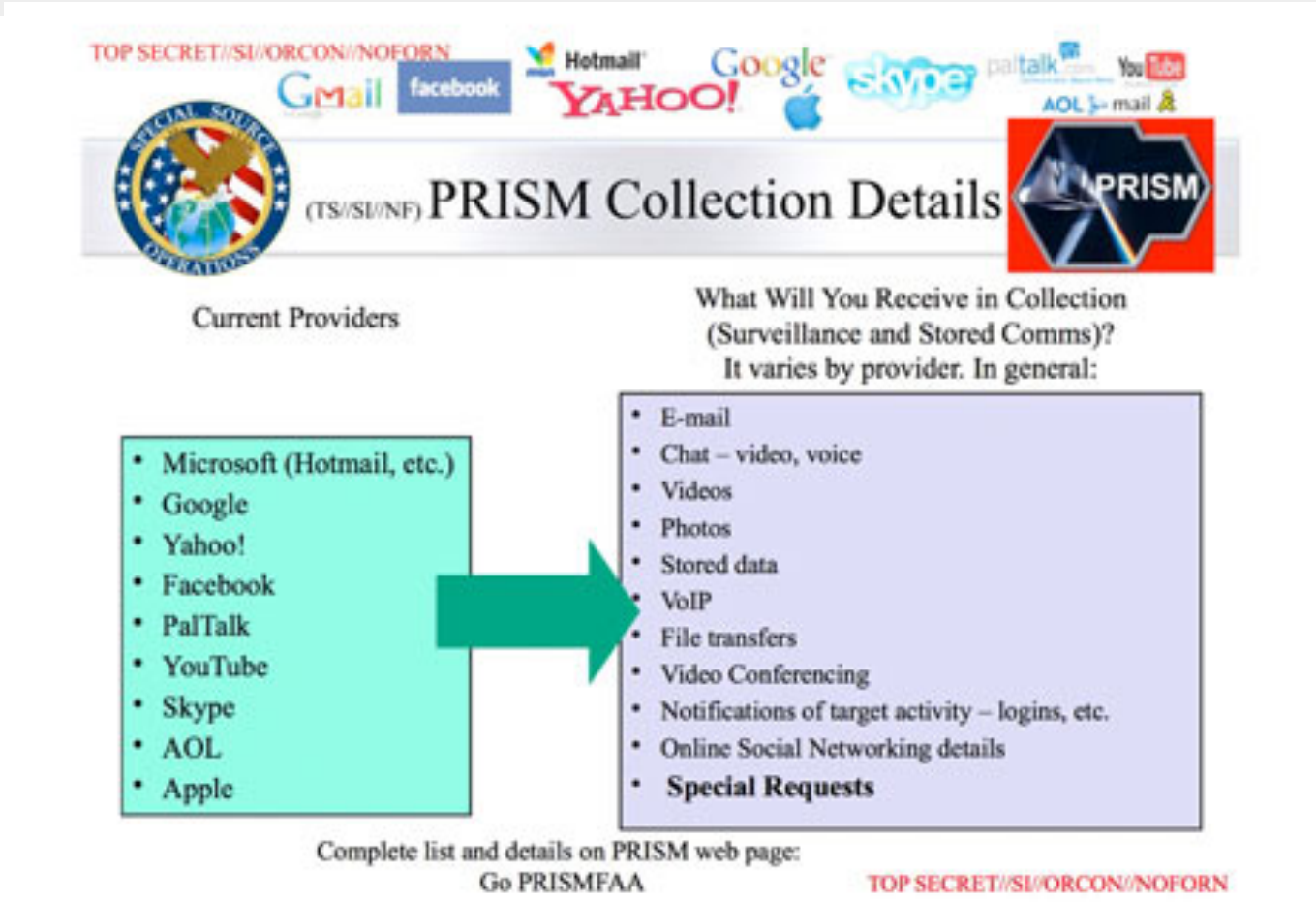
- Foursquare knows where you are
- Flickr knows what you see
- Facebook knows what you do
- Linkedin knows what you've done
- Twitter knows what you say
- Amazon knows what you buy
- Google knows what you think

Dataveillance on the "Invisible" Web

- "Meta-data"
- Tags, Web bugs, pixels and beacons that appear on Websites to track and profile users
- Allows trackers to build profiles of users

Dataveillance on the “Invisible” Web

A Example of Abuse: NSA PRISM



OBAMA's ANSWER

- « Now, with respect to the Internet and emails [of PRISM], **this does not apply to U.S. citizens**, …., **it only applies to foreigners**! ». (Obama, Wall Street Jounal, June 7, 2013)

- « We only collect metadata of U.S. citizens… »

Metadata = Surveillance

- Imagine you hired a detective to ***eavesdrop*** on someone. He might plant a bug in their office. He might tap their phone. He might open their mail. The result would be the details of that person's communications. That's the "**data**. »
- Now imagine you hired that same detective to **surveil** that person. The result would be details of what he did: where he went, who he talked to, what he looked at, what he purchased -- how he spent his day. That's **all metadata**.
- When the government (or a company) collects metadata on people, the government puts them under surveillance!

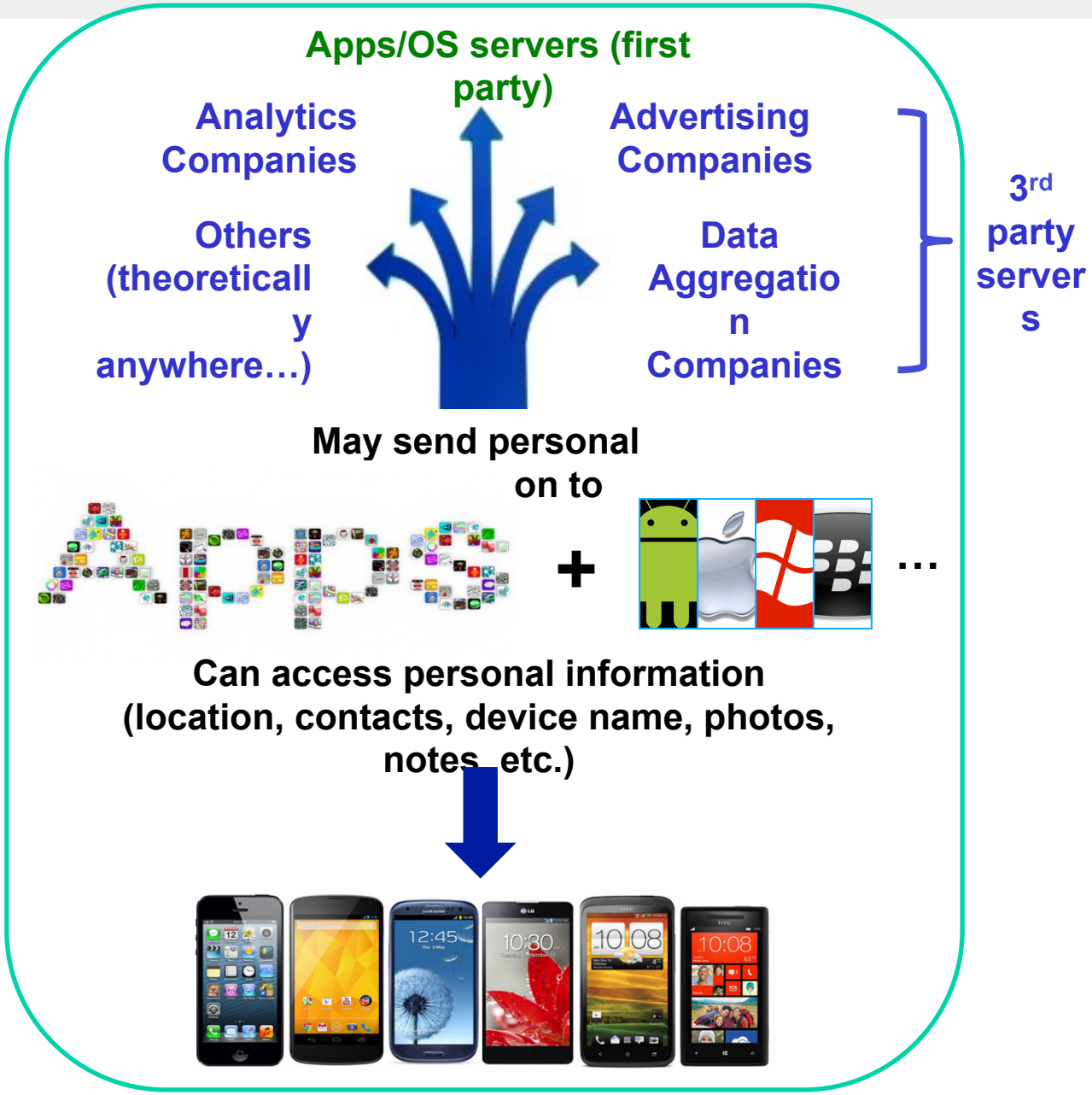
https://www.schneier.com/blog/archives/2013/09/metadata_equals.html

Our “personal spy assistant”

- smartphones have become our companions
  - useful and user-friendly, always connected
  - easy to customize to match everybody expectations
  - ~20% of mobile phones are smartphones

- but smartphones know a lot of our cyber-activities
  - they **gather** private information
    - while we’re using them
  - they **generate** private information
    - GPS, NFC, WiFi, camera

Our "personal spy assistant"…



Privacy leakage

- Spy, spy, spy…

  http://www.stealthgenie.com
  http://global.ikeymonitor.com

stealthGenie

World's Most Powerful Cell Phone Spy Software

- Protect Child
- Monitor Employees
- Geo-Location & Tracking
- Spy on any Phone

What can you do with iKeyMonitor?

For Parents

Read and report SMS and website logs to email box. Figure out the recent situation of children.

For Employers

Watch the key presses and take screen shots. Detect improper behaviors of employees.

For Spouses

Run in stealth mode and capture everything. Catch cheating spouses or clear suspicions.

For All iOS users

Monitor the activities on the iPhone/iPad you own. Track lost or stolen iPhone and iPad.

Privacy leakage

- data aggregation at Flurry
  - http://www.flurry.com/flurry-analytics.html

The enormous amount of data Flurry handles directly translates into unique, powerful insights for you. The service takes in over 1.4 billion app session reports per day totaling more than 1.5 terabytes, and our storage is in the petabytes. Here are some examples of how we use big data to create advantages for you:

FLURRY ESTIMATES THE AGE, GENDER & INTERESTS OF YOUR APP AUDIENCE

Smart Phone Mobility Privacy Issues

- Why are we tracked?
  - Personalized services to user and location.
  - Mobile-ADV (mobile advertisement)
    - Personalized ads to user's interests AND location.
    - Smart phones are great targets for advertisers
      - The number of mobile phones will soon surpass # of PCs
      - Phones contain/leak a lot of information!
      - A phone is owned and used by a single person, always on and always carried by its owner.

Online Advertising: Simplified Model

- 3 main entities:
  - **Advertiser (**annonceur**)**: entity that wants to advertise a service/products (i.e. hotels, car manufacturers,…)
  - **Publisher (**editeur**)**: entity that hosts the advertisements (i.e. online news, lemonde.fr,…)
  - **Ad-Network**: entity that places advertisements on Publisher sites (i.e. google,…)

Online Advertising: Illustration

ADVERTISER (maier.com)

PUBLISHER (lemonde.fr)

AD-NETWORK (doubleclick.com)

Online Advertising: Money Flow

ADVERTISER (maier.com)

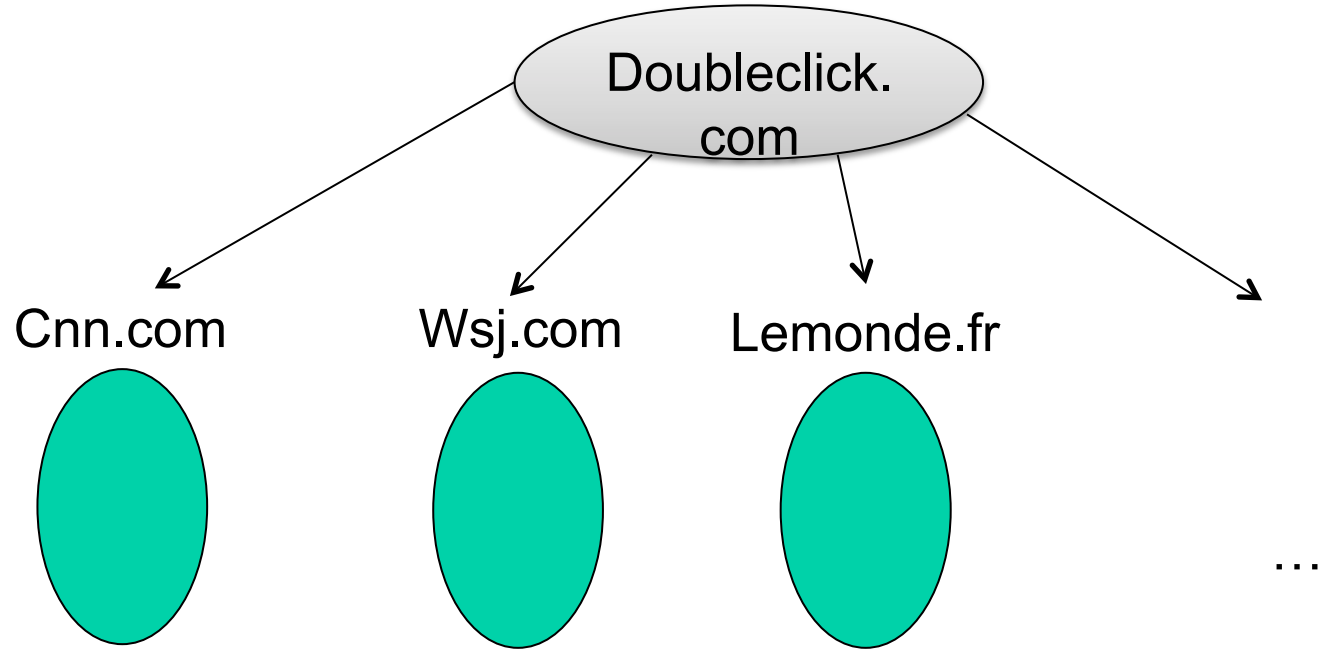
PUBLISHER (lemonde.fr)

$$$

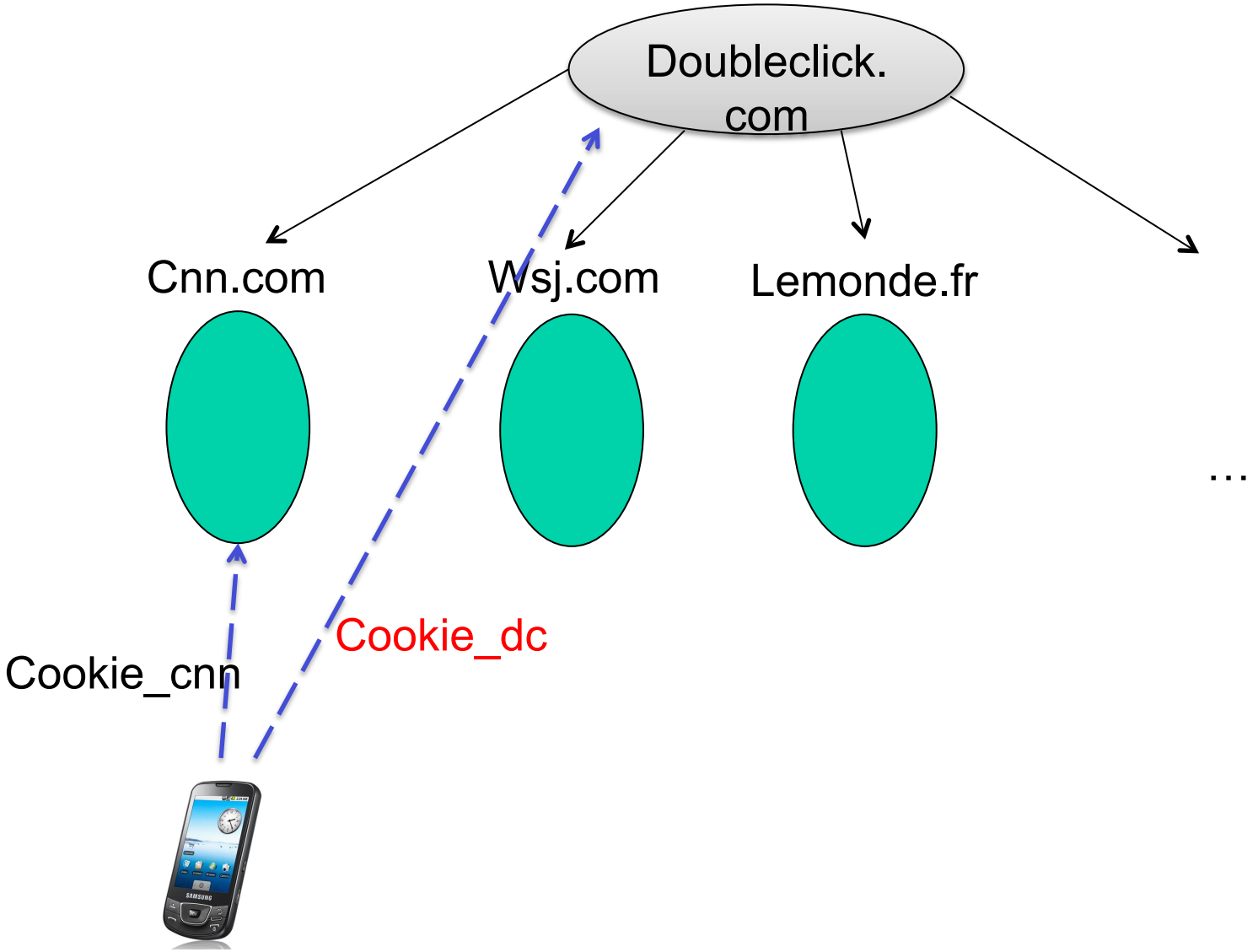
AD-NETWORK (doubleclick.com)

$

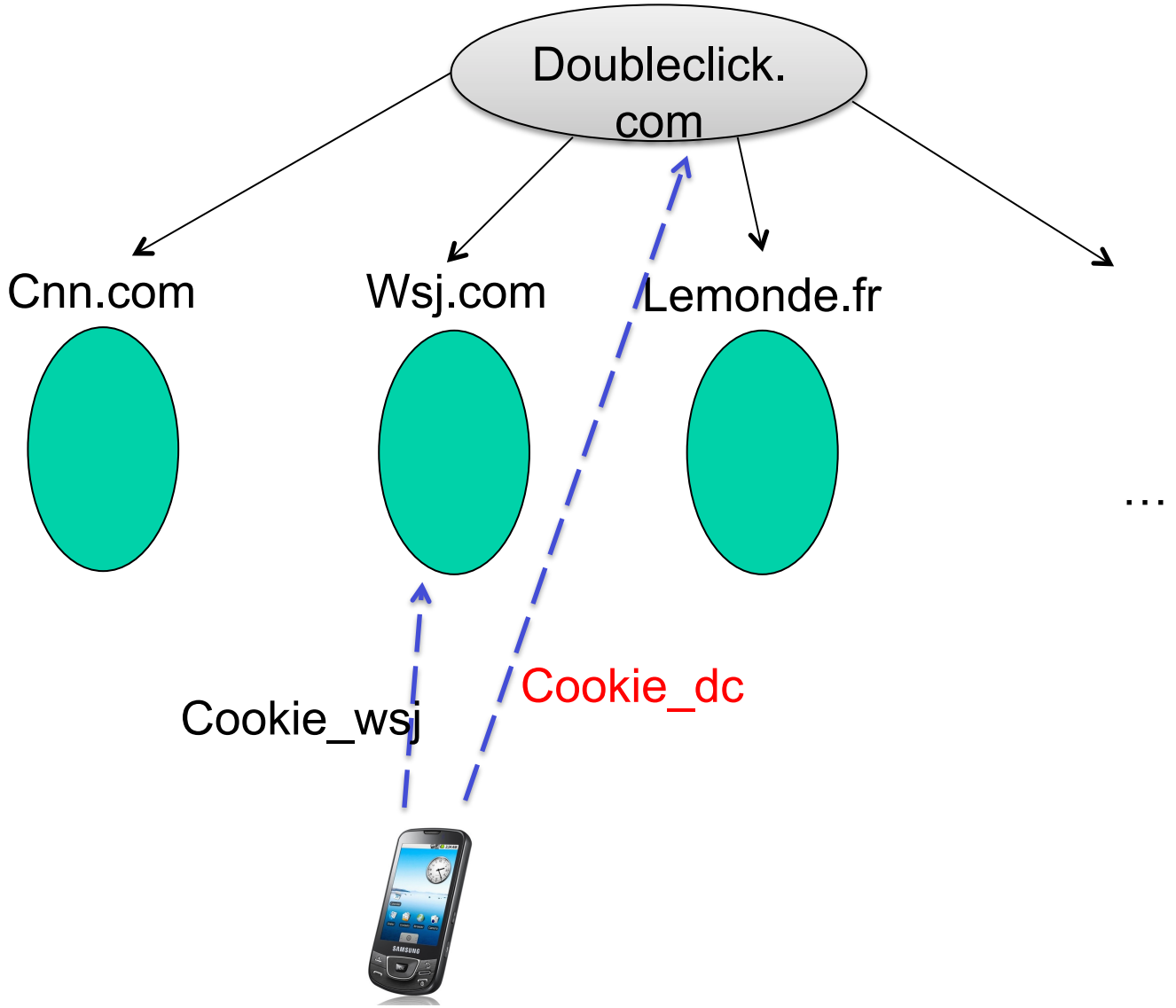
Browsing Profiling: How?



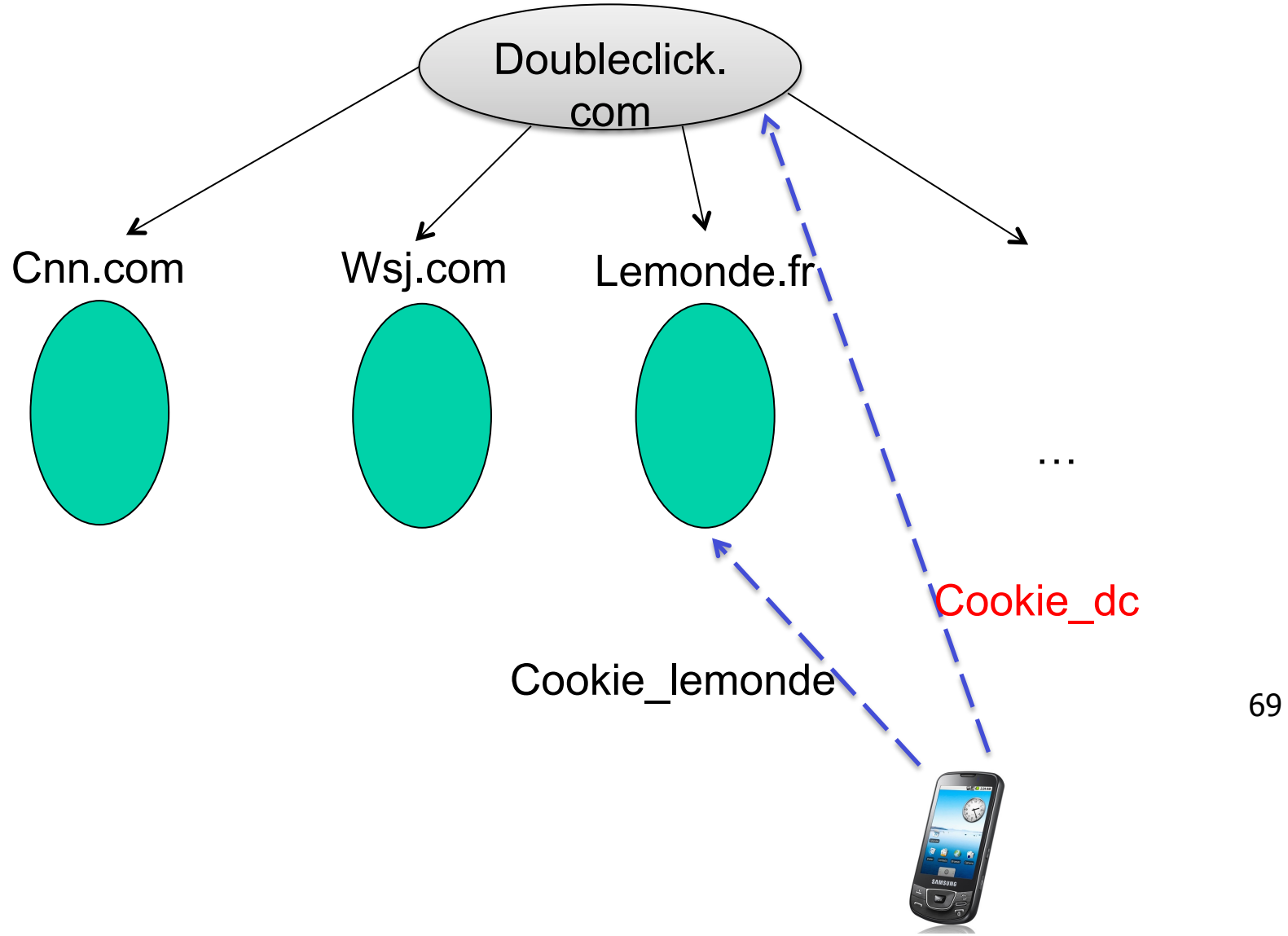
Browsing Profiling (2)



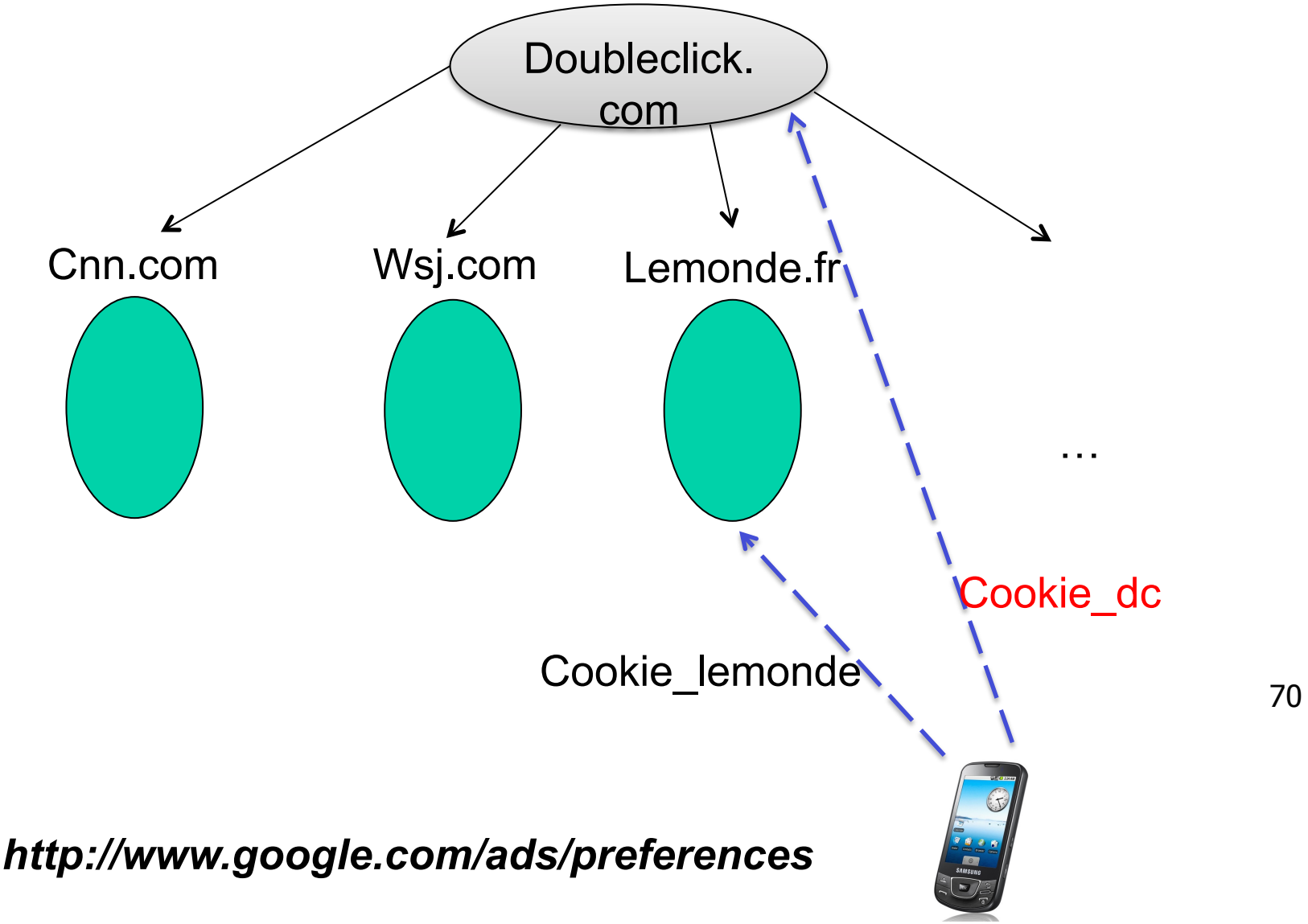
Browsing Profiling (2)



Browsing Profiling



Browsing Profiling



http://www.google.com/ads/preferences

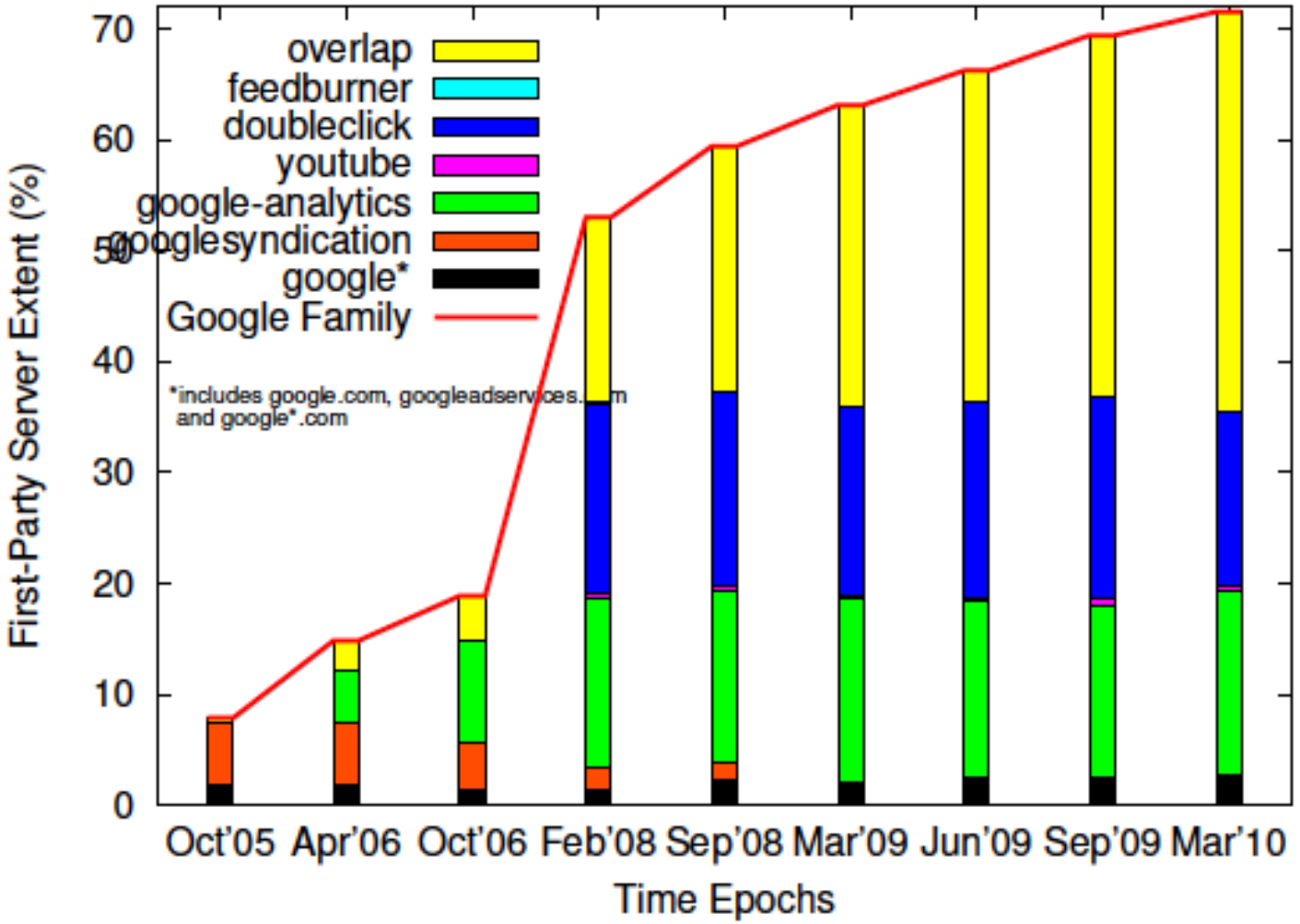
http://www.google.com/ads/preferences

Your categories Below you can edit the interests and inferred demographics that Google has associated with your cookie:

Category	
Business & Industrial - Energy & Utilities - Electricity	Remove
Business & Industrial - ... - Renewable & Alternative Energy	Remove
Computers & Electronics	Remove
Computers & Electronics - Electronics & Electrical	Remove
Finance - Credit & Lending - Home Financing	Remove
Home & Garden - Home Appliances	Remove
News - Weather	Remove
Real Estate	Remove
Real Estate - Apartments & Residential Rentals	Remove
Real Estate - Real Estate Listings	Remove
Travel - Tourist Destinations - Mountain & Ski Resorts	Remove
Demographics - Gender - Male	Remove

Add categories Google does not associate sensitive interest categories with your ads preferences.

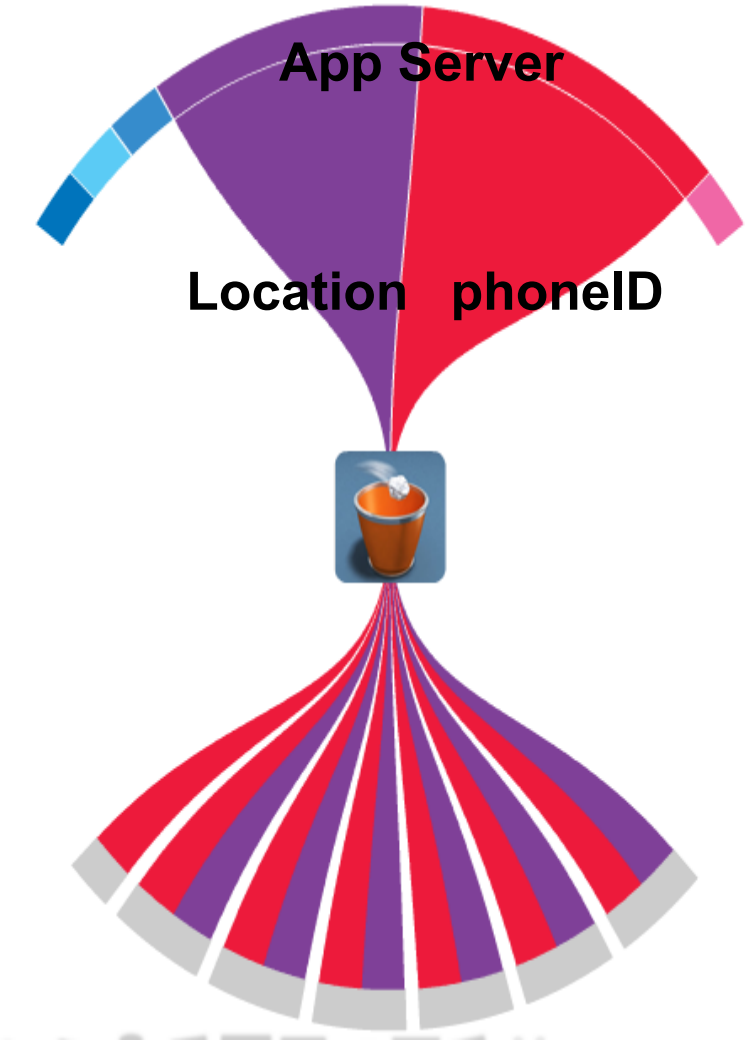
Online Tracking:
Tracking on the Internet…



Online Tracking: Smart Phone

- Marketers are tracking smartphone users through “apps” — games and other software on their phones.
- Some apps collect information including location, unique serial-number-like identifiers for the phone, and personal details such as age and sex.
- Apps routinely send the information to marketing companies that use it to compile dossiers on phone users

Paper Toss App (iPhone)

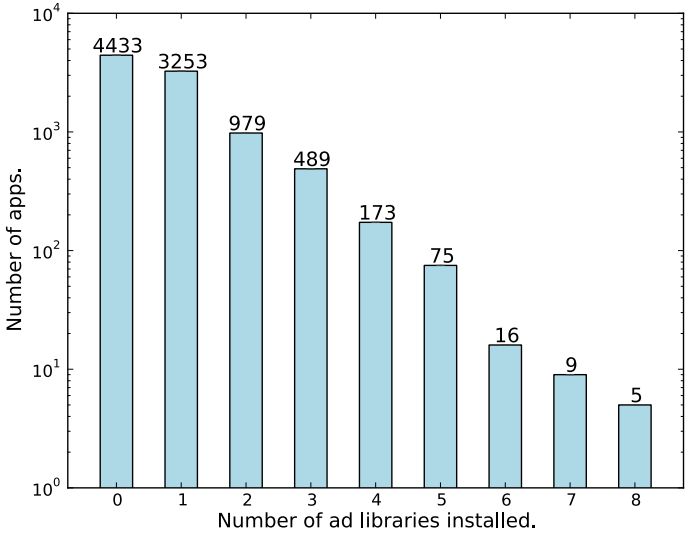


Third-party (google, flurry,…)

About Mobile Ads…

- some facts
  - **"77% of top 50 Android free Apps were Ad supported"** on July 2011 [1]
  - 35% of Android free Apps that use Ads **use 2 or more Ad libraries** [2]
    - a way to increase revenues
    - a trend is to use "Ad aggregators"

    who promise to select the Ad lib that maximizes profit



- ref:
  - [1] "Don't kill my ads! Balancing Privacy in an Ad-Supported Mobile Application Market", HotMobile 2012.
  - [2] "AdSplit: Separating smartphone advertising from applications", Usenix Security 2012.

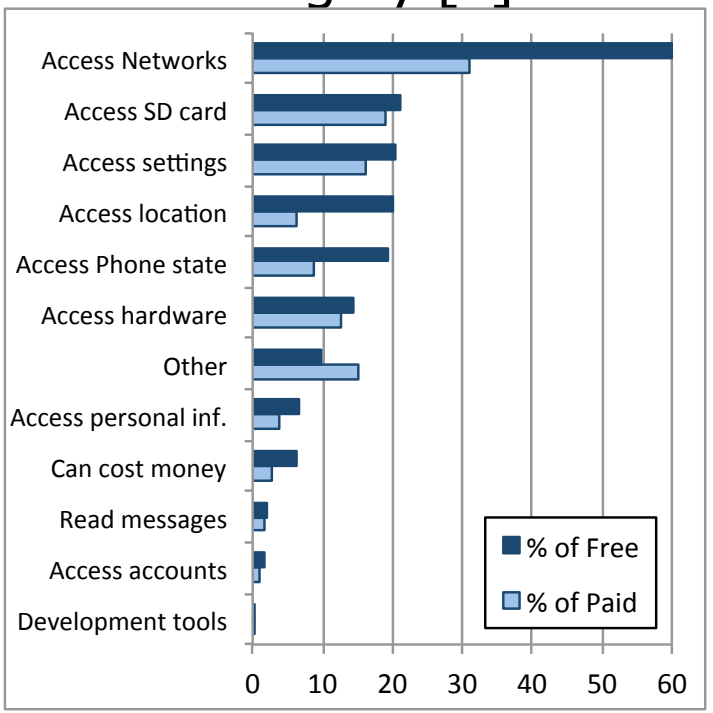
About Mobile Ads…

- it does impact the App behavior
  - Ad libs ask for potentially dangerous Android permissions
    - free Apps usually request 2-3 additional permissions compared to paid Apps of the same category [1]

Ad Library	Internet	NetworkState	ReadPhoneState	WriteExternalStorage	CoarseLocation	CallPhone
AdMob [22]	✓	✓			○	
Greystripe [25]	✓	✓	✓			
Millennial Media [36]	✓	✓	✓	✓		
InMobi [29]	✓	○			○	○
MobClix [38]	✓	○	✓			
TapJoy [53]	✓	✓	✓	✓		
JumpTap [32]	✓	✓	✓		○	

✓(required), ○ (optional)

permissions per Ad lib [2]



dangerous permissions asked for by free/non-free Aps [1]

So…

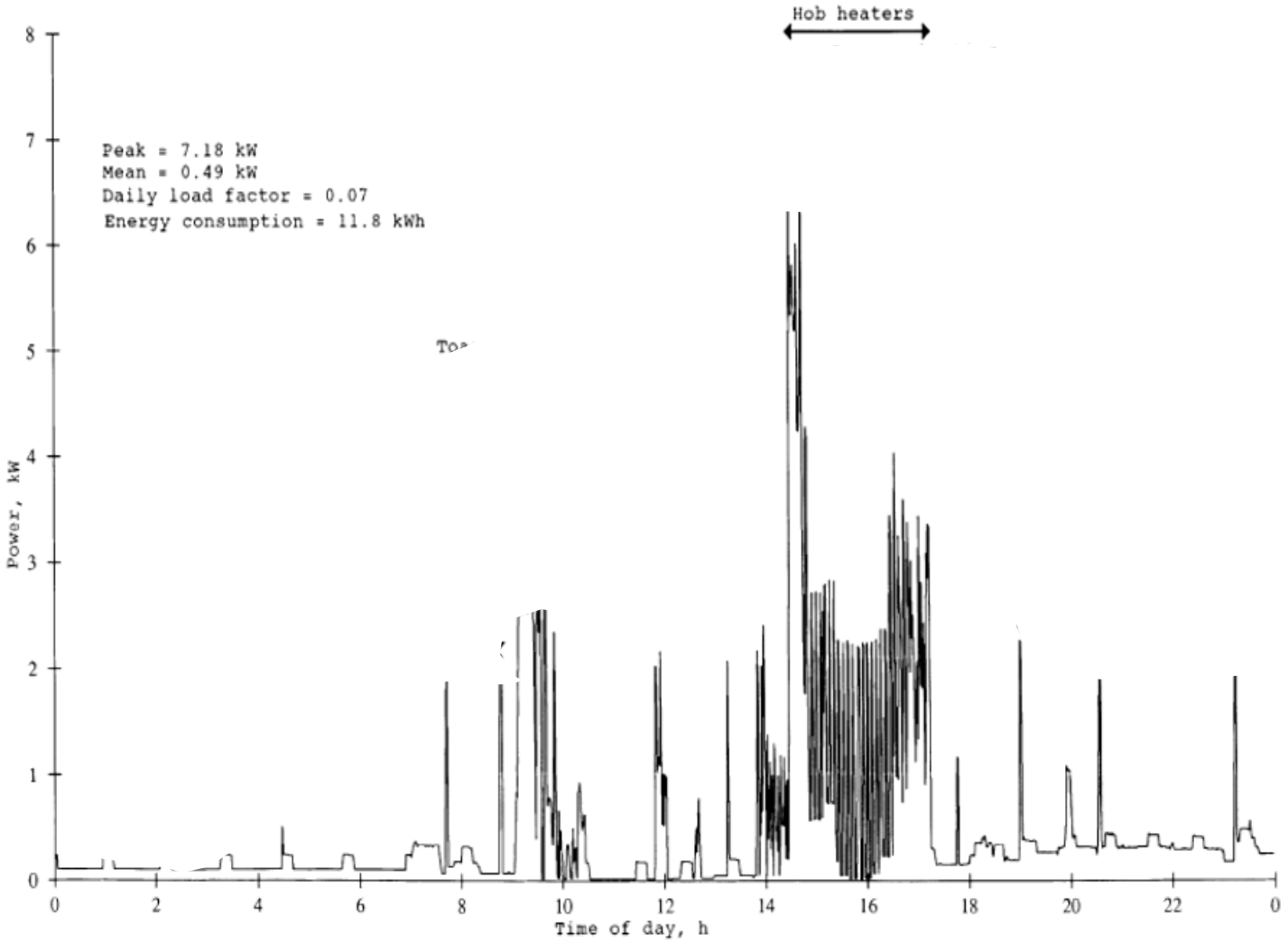
- **"tracking the trackers"** has become a necessity
  - "teach" companies to behave in a privacy-friendly way
- users must **know** the risks…
  - "teach" the end-user
- users must be able to **control** the risks

Our Mobilitics project

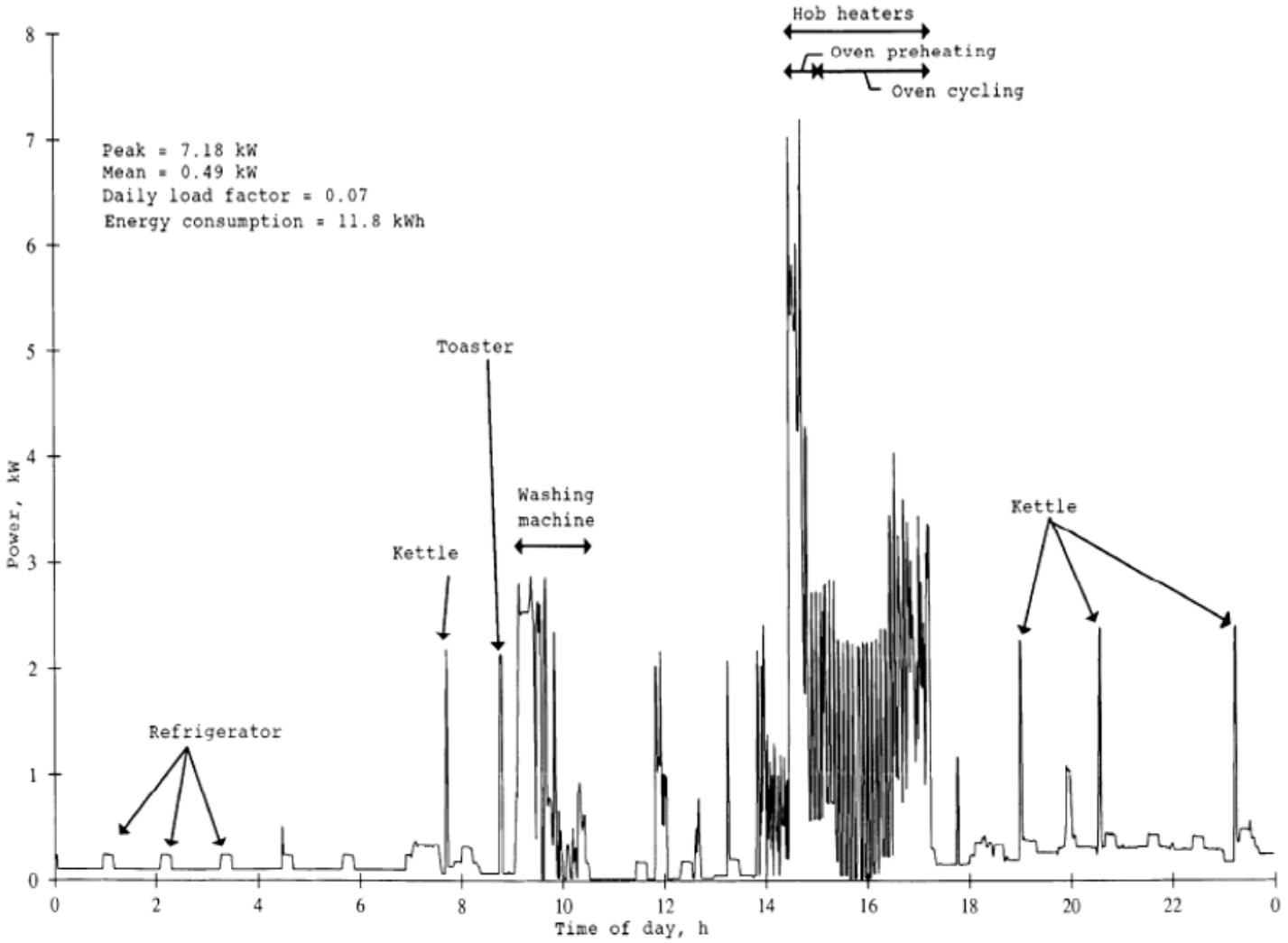
- started in January 2012

- focuses on Android and iOS
  - they are the leading mobile OS
  - they follow different approaches
- goal is to analyze privacy leakage from **Apps** (free or not) and **OS services**
  - compare Android/iOS. Identify best practices and trends
  - gather facts that CNIL can use to discuss with companies
- don't be naïve
  - targeted ads can be "the price to pay" for free Apps

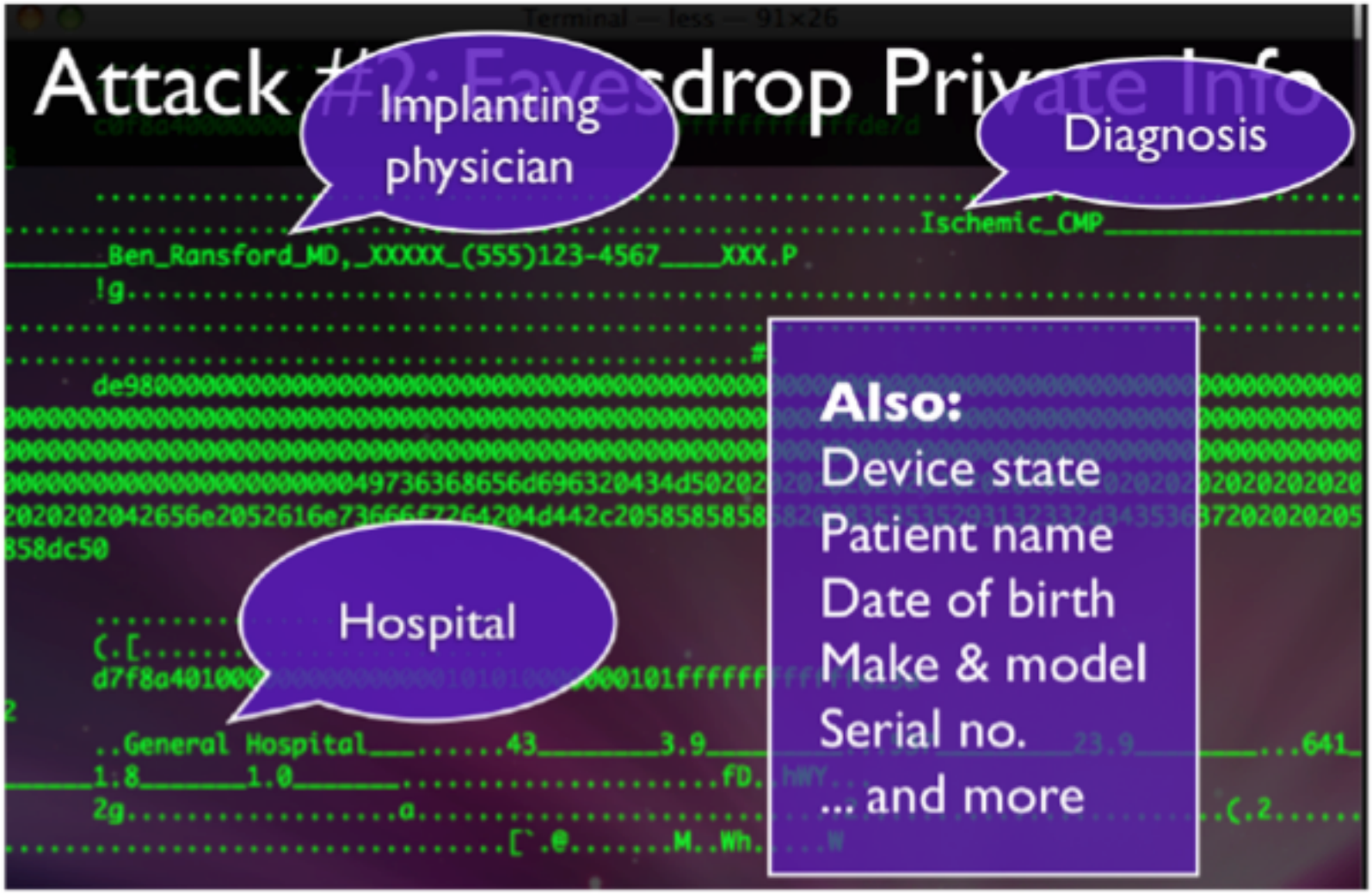
Physical Tracking: Smart metering



Smart Meters



Physical Tracking:
Medical devices & Self-logging



Privacy? The « no-hide » argument!!

Really?


Hey! What about my privacy??
They say that people who worry about their privacy have something to hide ...
sangrea.net

The dangers


SEATTLE POST-INTELLIGENCER '99 GREENBERG
CURRENT MEDICAL RECORDS PRIVACY IN U.S.
INSURANCE COMPANIES
EMPLOYERS
FINANCIAL INSTITUTIONS
MARKETERS

The dangers

Signs of the social networking times.

Monitoring…


THE INDEPENDENT
IVERPOOL'S EUROPEAN
DREAM CRUSHED BY MILAN
Google
IS WATCHING
YOU
'Big Brother' row over plans for personal database

The danger

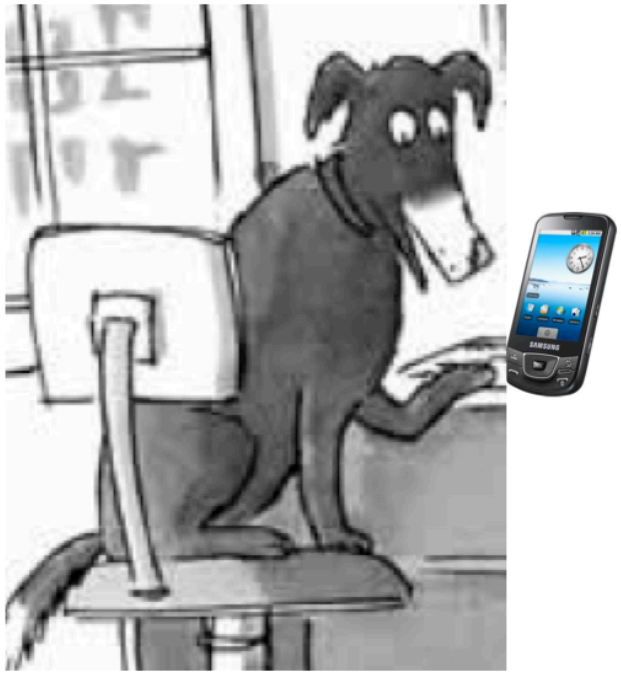
- Surveillance: We move into a surveillance society companies/gov. gather a huge amount of information about users
- Discrimination:
  - Profiling may reveal that a user is suffering from a certain disease.
  - Insurance might then deny insurance
- Personalization:
  - Filter bubble
  - Information leakage

- We need privacy-preserving systems…

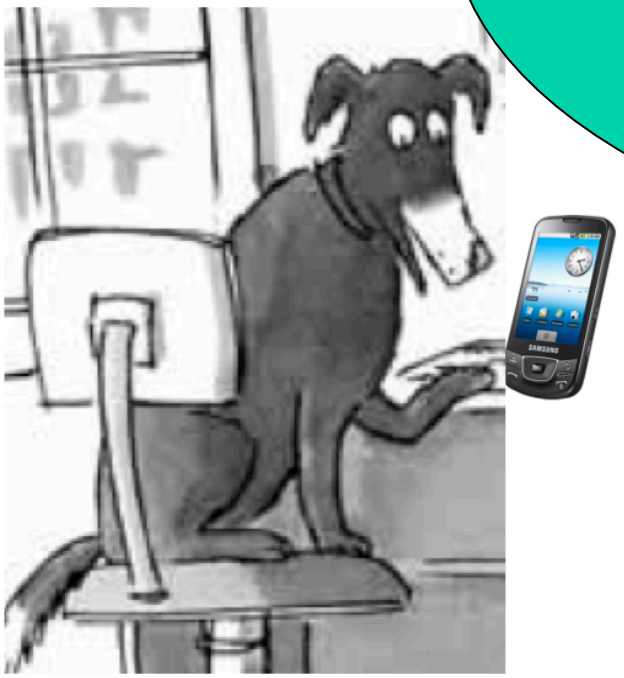
Yesterday (1993)

"On the Internet, nobody knows you're a dog."

Today



Today



Name: Tutu
Race: black dog
Favorite food: meat
Interests: hunting, swimming, skiing
Location: Grenoble, but currently visiting Paris

On the Internet, they now know that you are a black dog!

THANKS!

Claude.castelluccia@inria.fr

http://planete.inrialpes.fr/~ccastel/