Technical Aspects of Privacy

Ciarán Bryce and Frédéric Le Mouël

ciaran.bryce@inria.fr , frederic.le-mouel@insa-lyon.fr

20 June 2007

INSTITUT NATIONAL
DE RECHERCHE
EN INFORMATIQUE
ET EN AUTOMATIQUE

INRIA

Agenda

Introduction to Ambient Computing Systems

Hardware

- RFID

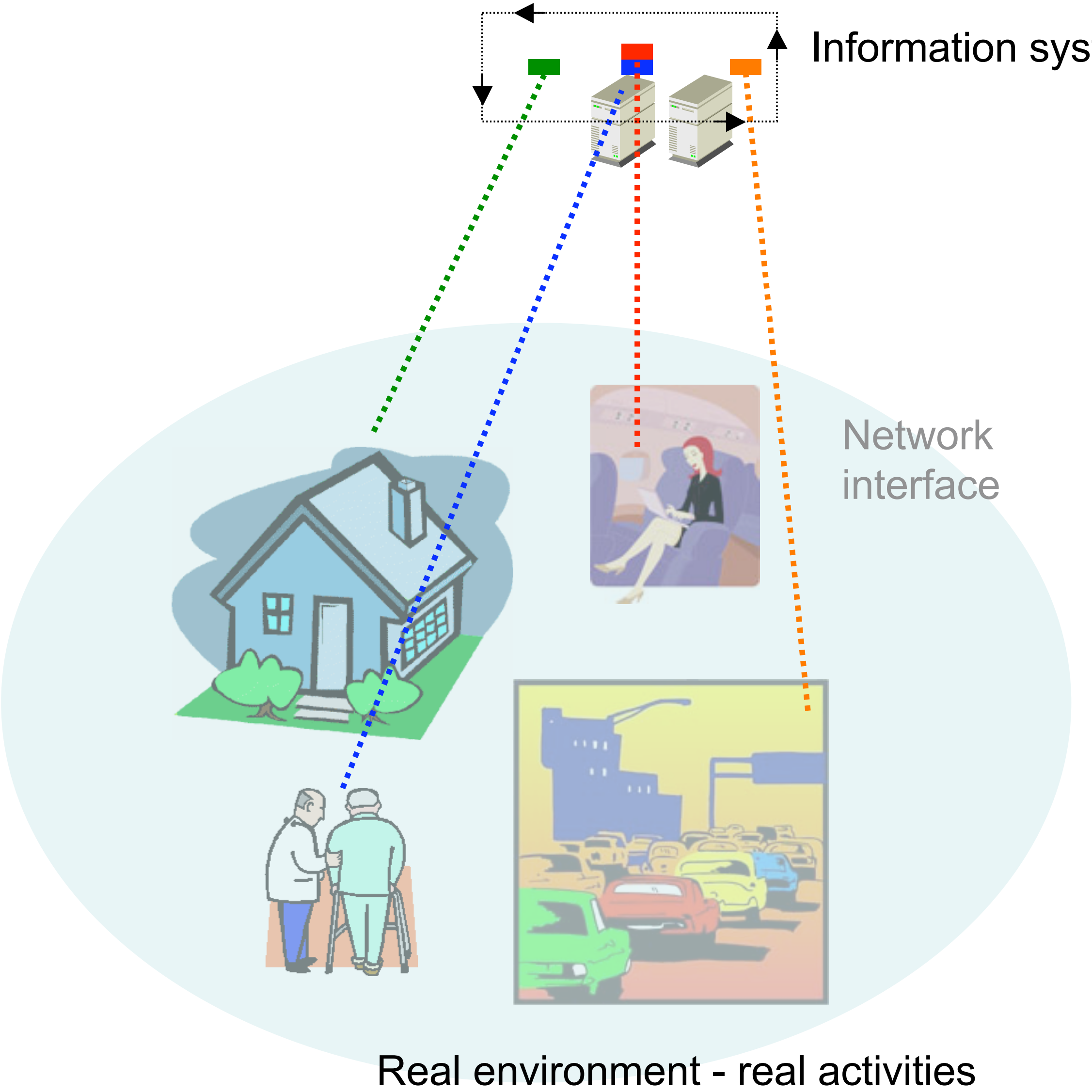
Protocols

- Trust protocols

Infrastructure

- Trusted Platform Module

Ambient Computing Systems



Information system servers
Network interface
Real environment - real activities

Ambient Information System

Virtual and real-world worlds are merged;
Real-world objects compute

Origin

Xerox Parc, Mark Weiser

- Merging physical and digital world
  - Intelligence in everyday objects (*Ubiquitous computing*)
  - Simplify interactions between people and objects (*Disappearing computer*)

Project ParcTab

- Infrastructure based on infrared
- Information server centralizing information about people
- Terminals (« tab »), similar to PDAs
- Contextual Services
  - Service offered to a user depends on his location, preferences, activities, etc.
  - Reminders and electronic post-it

Recent Developments

Mobile phones are massively popular

- And more and more functionality included: PDA = mobile phone
  - Networking: WiFi and Bluetooth
  - Near Field Computing computing technology, e.g., RFID.
  - Smart sensors

Embedded processors

- 98% of today’s processors are embedded in real-world objects

Increasing industrial awareness of ambient computing potential

Applications

Intelligent environments (smart spaces)

- Enriched perception
- Handicap removal

Automated control

- E.g., smart fridges

Stock management, inventory systems, tracing substances and products

Games (augmented reality)

Etc.

Wireless technologies

Global networks: coverage greater than one Km

- GSM : 2G, 9.6 Kbps
- GPRS : 2,5G, 144 Kbps
- UMTS : 3G, 2 Mbps
- …

Local networks : 10 to 100 meters

- Wi-fi : 2,4 GHz, 54 Mbps
- Bluetooth : 2,4 GHz, 1-2 Mbps
- …

Others: several centimeters to several meters

- RFID : LF 134,2 KHz; HF 13.56 MHz; UHF 868 MHz-928 MHz

WIFI: characteristics

Frequencies : 2,4 GHz

Range: up to 50 meters inside a building to 300 meters outside

Rates:

- 802.11b 11Mbps,
- 802.11g 54 Mbps

Power consumption: 100mW

Modes :

- Infrastructure with access points,
- Ad-Hoc for peer-to-peer operation

Users

- Local networking, hotspots, information gathering, …

Bluetooth : characteristics

Frequency : 2.4 GHz

Range:		10 - 15 meters

Data rate: 2 Mbps

Weak consumption : 2,5mW

7 devices can simultaneously participate in a piconet

Connection time from 10 to 30 seconds,

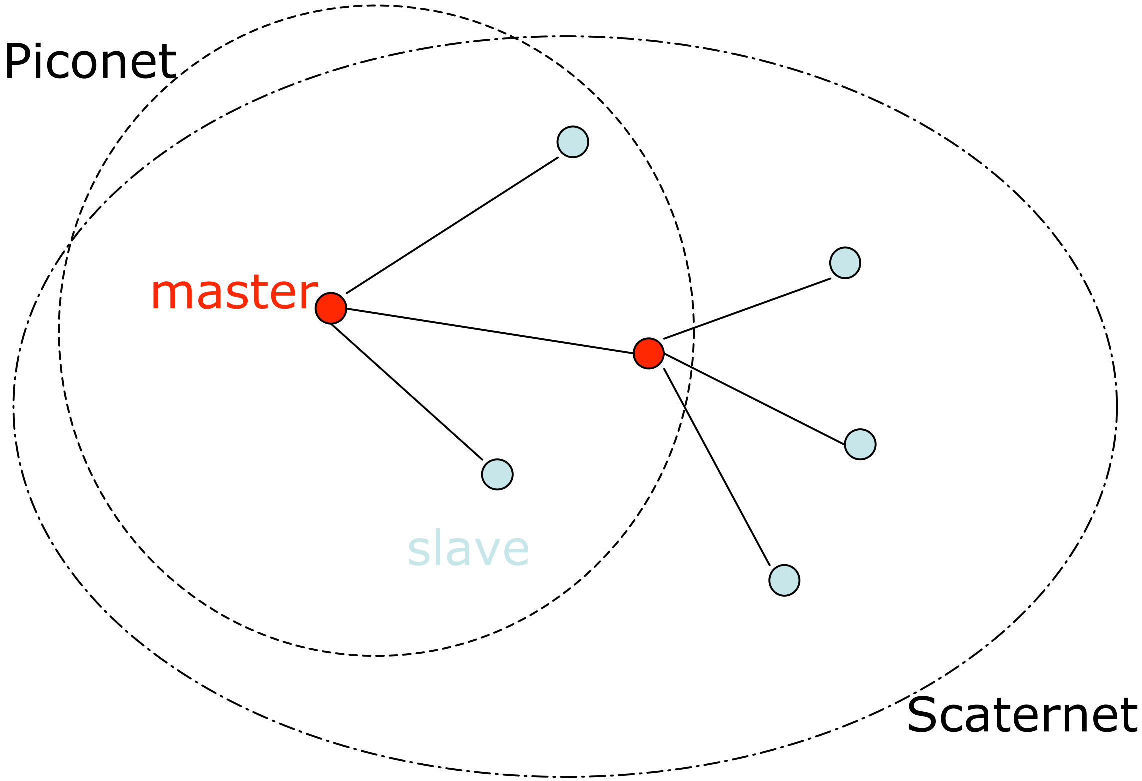
- Which is not very useful for highly mobile applications

Frequency hopping occurs to avoid interference

Uses

- Earplugs, removing wires from the body, mice, data synchronization, ..

Bluetooth : Structure



More information on ambient systems

collection informatique dirigée par Jean-Charles Pomerol

Informatique diffuse

des concepts à la réalité

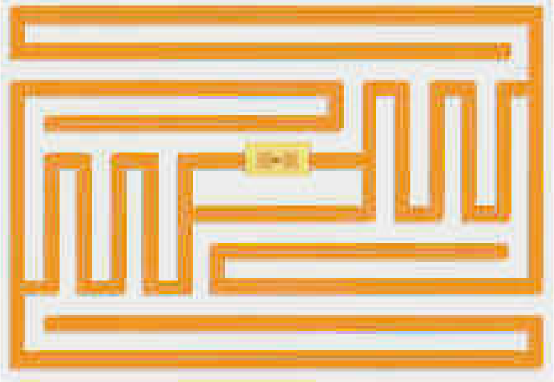
Michel Banâtre
Ciarán Bryce
Paul Couderc
Frédéric Weis

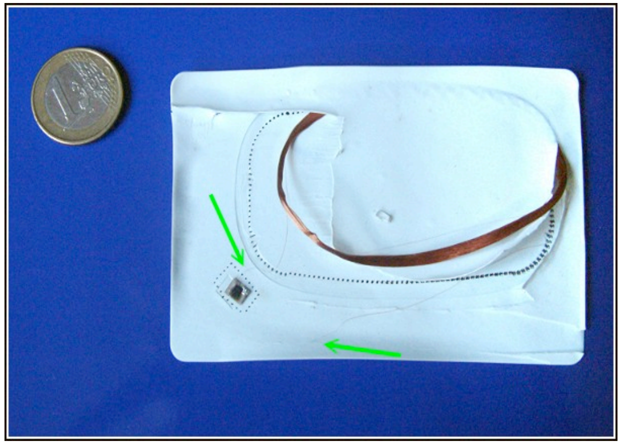
hermes

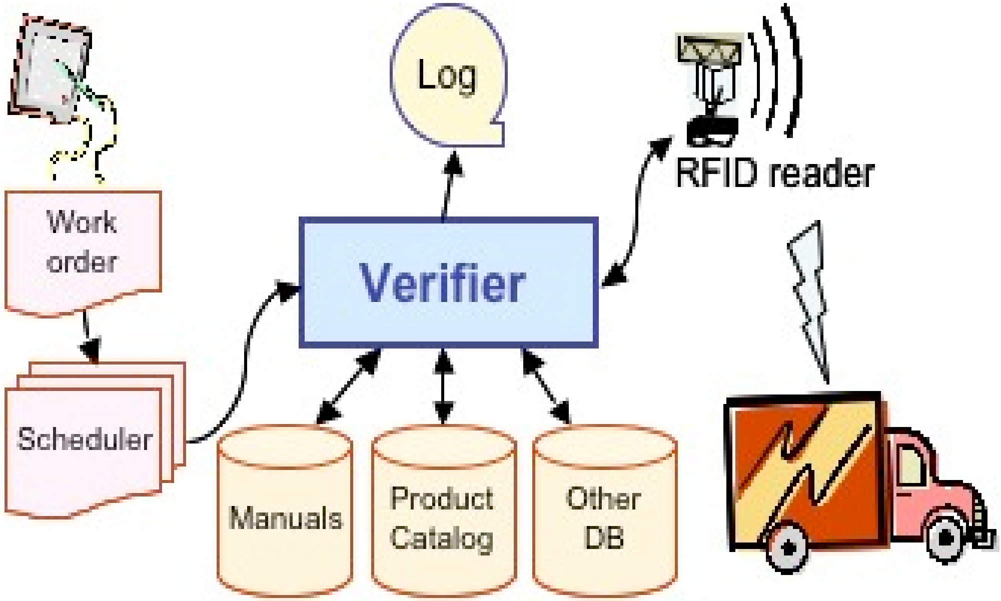
Lavoisier

Radio Frequency Identification (RFID)

RFID






Log
RFID reader
Work order
Verifier
Scheduler
Manuals
Product Catalog
Other DB

Radio Frequency Identification

Device that holds a small amount of unique data

- Serial number or other unique attribute of the item

Data can be read from a distance – no contact or even line of sight necessary

Enables individual items – down to the proverbial “can of beans” - to be individually tracked from manufacture to consumption!

Identification using radio waves

- Chip-based tags contain silicon chips and antennas
- 5 frequency bands (100-135kHz, 13,56MHz, 868/915MHz, 2.56GHz, 5.8GHz).

What’s It All About?

Performa Long Range Reader

Authentication

- The customer simply passes line with the shopping cart.

Identification

- The storage capacity is much higher than bar codes so can store more than the product name

Integration

- The wireless aspect helps to seamlessly integrate the technology into clothes etc. (Protection from dirt, etc.)

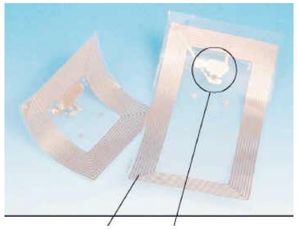
Authentication

- Can store cryptographic information - the car immobilizer is a good example.

Passive and Active Tags

Passive RFID tags have no internal power supply.

- Minute electrical current induced in antenna by incoming radio frequency signal provides power for CMOS IC in tag to transmit response.
- The tag chip can contain non-volatile EEPROM for storing data.
  - In February 2007 Hitachi unveiled an even smaller RFID measuring 0.05x0.05mm, and thin enough to be embedded in a sheet of paper.



Active RFID tags have their own internal power source which is used to power any integrated circuits that generate the outgoing signal.

- Conducts a "session" with a reader.
- Many active tags have practical ranges of hundreds of meters, and a battery life of up to 10 years.

RFID Tag Attributes

	Active RFID	Passive RFID
Tag Power Source	Internal to tag	Energy transferred using RF from reader
Tag Battery	Yes	No
Availability of power	Continuous	Only in field of reader
Required signal strength to Tag	Very Low	Very High
Range	Up to 100m	Up to 3-5m, usually less
Multi-tag reading	1000’s of tags recognized – up to 100mph	Few hundred within 3m of reader
Data Storage	Up to 128Kb or read/write with sophisticated search and access	128 bytes of read/write

Current uses

Passports

- First RFID passports ("e-passports") issued by Malaysia in 1998.
  - e-passports record the travel history (time, date, and place) of entries and exits from the country.
  - RFID tags are included in new UK and some new US passports
  - Passports incorporate thin metal lining to make it difficult for unauthorized readers to "skim" information when the passport is closed.

Transport payments and toll collection

Product Tracking

- Replacement for barcode tags
- American Express Blue credit card now includes a high-frequency RFID tag.

Current uses

Automotive

- RFID tags have been used in car keys for 10 years.
  - Michelin began testing RFID transponders embedded into tires.
    - Tire tracking in compliance with US Transportation, Recall, Enhancement, Accountability and Documentation Act (TREAD Act).

Animal identification

Human implants.

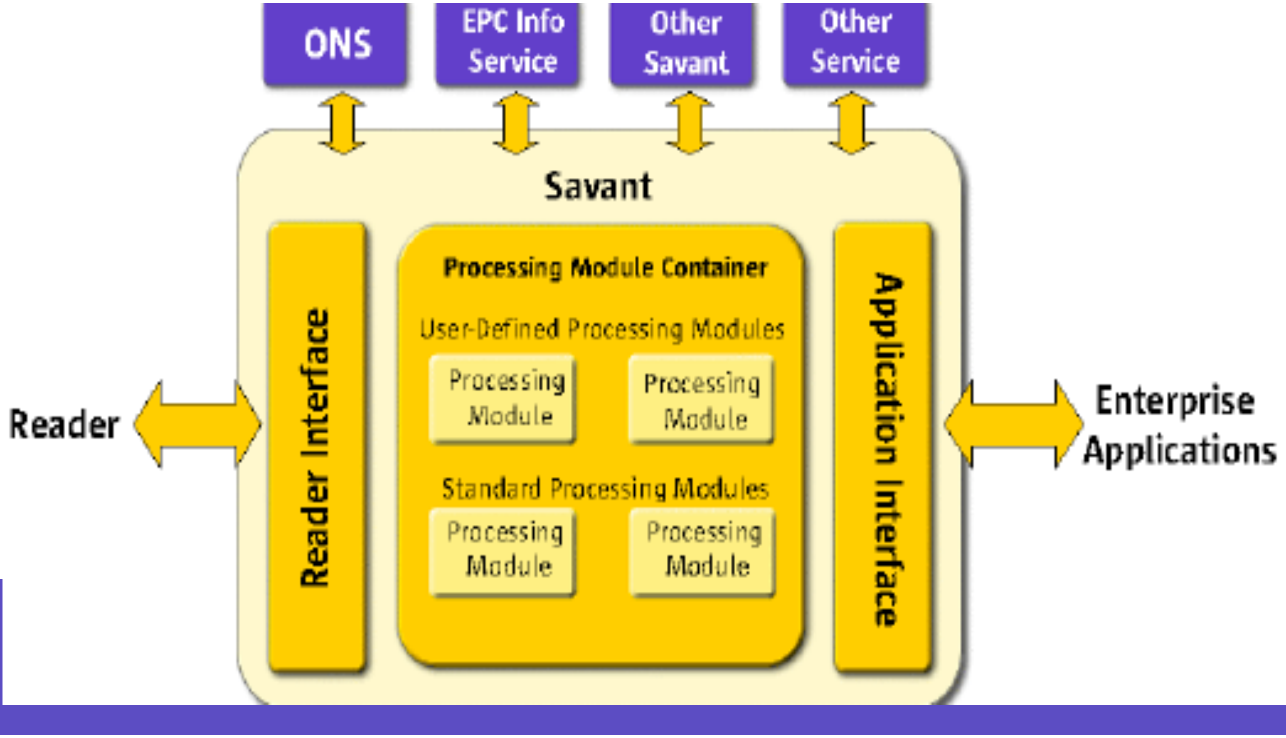
- Night clubs use an implantable chip to identify their VIP customers
- In 2004, the Mexican Attorney General's office implanted 18 of its staff members with the Verichip to control access to a secure data room.

Electronic cash, e.g. SmarTrip in Washington, DC, USA, EasyCard in Taiwan, Suica in Japan, T-Money in South Korea, etc.

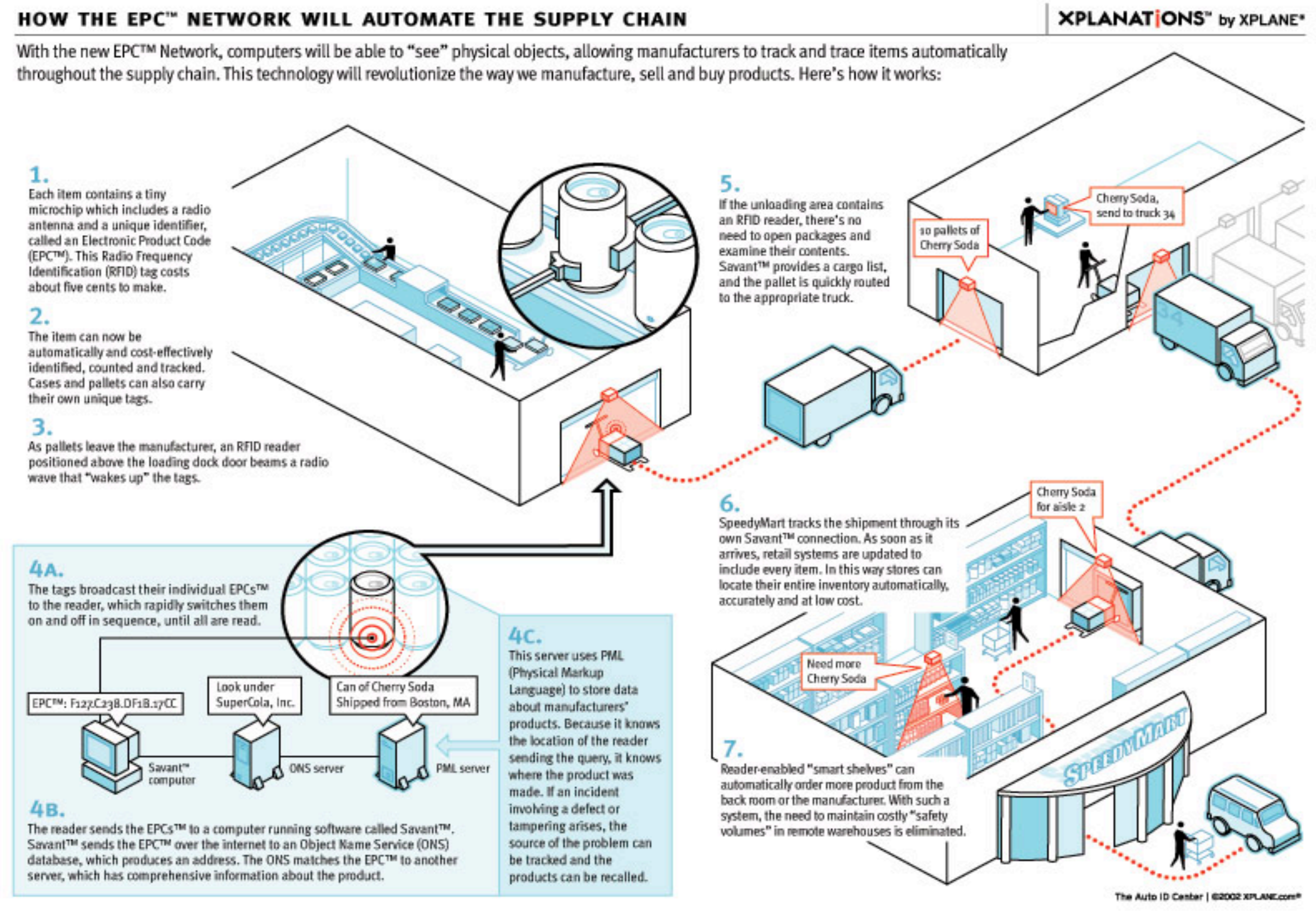
EPCglobal

A standards management and development body with the aim of automating the supply chain

Each object is uniquely identified with an Electronic Product Code (EPC), and linked by RFID to an EPC Network



Supply Chain – Global Vision



HOW THE EPC™ NETWORK WILL AUTOMATE THE SUPPLY CHAIN

XPLANATIONS™ by XPLANE®

With the new EPC™ Network, computers will be able to "see" physical objects, allowing manufacturers to track and trace items automatically throughout the supply chain. This technology will revolutionize the way we manufacture, sell and buy products. Here's how it works:

1. Each item contains a tiny microchip which includes a radio antenna and a unique identifier, called an Electronic Product Code (EPC™). This Radio Frequency Identification (RFID) tag costs about five cents to make.

2. The item can now be automatically and cost-effectively identified, counted and tracked. Cases and pallets can also carry their own unique tags.

3. As pallets leave the manufacturer, an RFID reader positioned above the loading dock door beams a radio wave that "wakes up" the tags.

4A. The tags broadcast their individual EPCs™ to the reader, which rapidly switches them on and off in sequence, until all are read.

4B. The reader sends the EPCs™ to a computer running software called Savant™. Savant™ sends the EPC™ over the internet to an Object Name Service (ONS) database, which produces an address. The ONS matches the EPC™ to another server, which has comprehensive information about the product.

4C. This server uses PML (Physical Markup Language) to store data about manufacturers' products. Because it knows the location of the reader sending the query, it knows where the product was made. If an incident involving a defect or tampering arises, the source of the problem can be tracked and the products can be recalled.

5. If the unloading area contains an RFID reader, there's no need to open packages and examine their contents. Savant™ provides a cargo list, and the pallet is quickly routed to the appropriate truck.

6. SpeedyMart tracks the shipment through its own Savant™ connection. As soon as it arrives, retail systems are updated to include every item. In this way stores can locate their entire inventory automatically, accurately and at low cost.

7. Reader-enabled "smart shelves" can automatically order more product from the back room or the manufacturer. With such a system, the need to maintain costly "safety volumes" in remote warehouses is eliminated.

EPC™: F127.C238.DF1B.17CC
Look under SuperCola, Inc.
Can of Cherry Soda Shipped from Boston, MA
Savant™ computer
ONS server
PML server
10 pallets of Cherry Soda
Cherry Soda, send to truck 34
34
Cherry Soda for aisle 2
Need more Cherry Soda
SPEEDYMART

The Auto ID Center | ©2002 XPLANE.com®

RFID Limitations

Lack of Reading Precision

- i.e., read your groceries and not those of the person behind you in the line.

Rogue readers with high read ranges

- (higher than the nominal read range).

Read ranges defined under laboratory conditions … in practice, read ranges are dependent on environmental conditions

Security and Privacy?

Security and Privacy

http://www.boycottbenetton.com

Security and Privacy Concerns

Illicit tracking of RFID tags

- Tags which are world-readable pose a risk to both personal location privacy and corporate/military security.

Most people have still not heard of RFID.

- The bar code (invented in the 1950s) and deployed in July 1974 caused a similar debate.

Clandestine scanning

- E.g., Thieves passing before a house and learning the content

Eavesdropping

Data leakage

- (letting more information than necessary being released).

Protection

Cryptography to prevent tag cloning

- Reader issues a challenge to the tag, which responds with a result computed using a cryptographic circuit keyed with some secret value
  - Protocols may be based on symmetric or public key cryptography.
- Secret tag information is never sent over the insecure communication channel between tag and reader

Some tags use rolling code scheme

- Tag identifier information changes after each scan

  thus reducing the usefulness of observed responses.

Other tags include a deactivate command

Protection

Clipped Tag

- Suggested by IBM researchers Paul Moskowitz and Guenter Karjoth.
- Principle:
  - After the point of sale, a consumer may tear off a portion of the tag. This allows the transformation of a long-range tag into a proximity tag that still may be read, but only at short range – less than a few inches or centimeters.
  - The modification of the tag may be confirmed visually. The tag may still be used later for returns, recalls, or recycling.

Shielding

- Simply wrapping an RFID card in aluminum foil, essentially creating a Faraday cage, is claimed to make transmission more difficult
  - yet not be completely effective at preventing it.

Other Concerns

Ars Technica Reported in March 2006 an RFID buffer overflow bug that could infect airport terminal RFID Databases for baggage

- and also Passport databases to obtain confidential information on the passport holder !

Protocols for Privacy

Protocols

Goals

- Users Identification
- Information exchanges

Two points of view:

Security Protocols

- Authentication protocols: strong
- Information exchange protocols: secure channels, cryptography

Trust Protocols

- Authentication protocols: light, no a priori, learning, even anonymization
- Information exchange protocols: secure and unsecured channels

Anonymization protocols

Packet masking

- I. Aad, C. Castelluccia, and J.P. Hubaux
- Multicast ad-hoc networks and onion encryption
- Packet routing headers and packet payloads are treated separately resulting in a constantly changing packet

Location-tracking

- Reynold Cheng, Yu Zhang, Elisa Bertino, and Sunil Prabhakar
- Mobile ad hoc network without losing the quality of services
- Lower the spatial and temporal resolution of location data sent to the server
- Control uncertainty to provide high quality and privacy-preserving service
- Preserve against trajectory-tracing

Trust Protocols

Communities

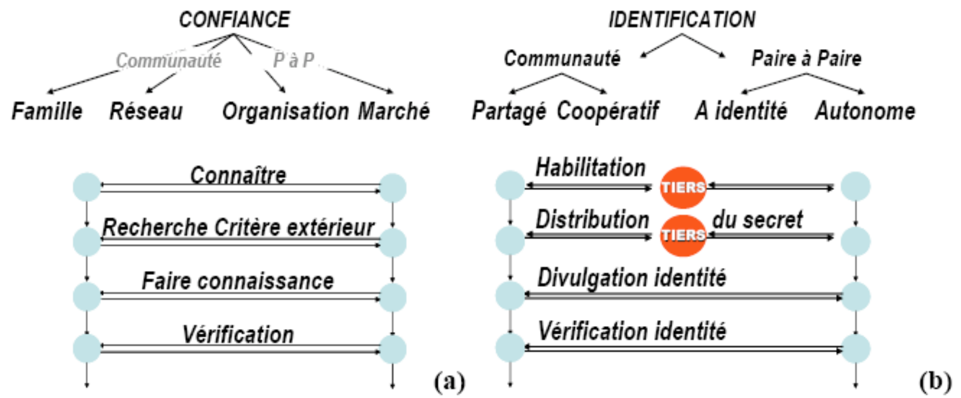
- Open-source communities
- Enterprise communities
- Peer-to-peer networks communities
- Etc.

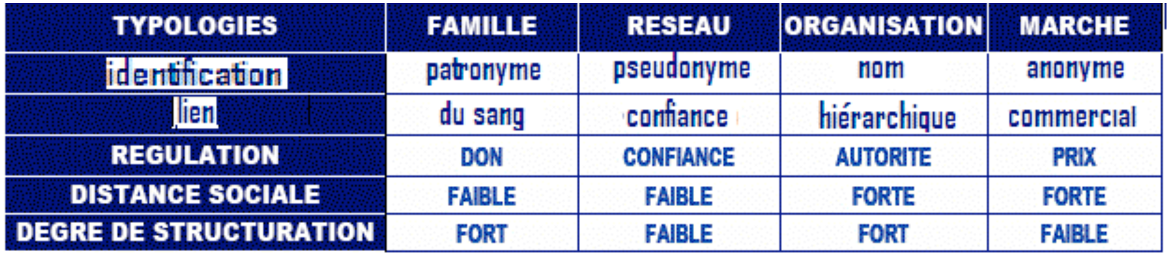
Devices communities

- KAA http://kaa.citi.insa-lyon.fr
- Gradual need of trust
- Ad hoc hybrid networks, spontaneous, self-organized

Trust Protocols – Devices Communities

- **Modèle social**
- **Modèle électronique**





TYPOLOGIES	FAMILLE	RESEAU	ORGANISATION	MARCHE
identification	patronyme	pseudonyme	nom	anonyme
lien	du sang	confiance	hiérarchique	commercial
REGULATION	DON	CONFIANCE	AUTORITE	PRIX
DISTANCE SOCIALE	FAIBLE	FAIBLE	FORTE	FORTE
DEGRE DE STRUCTURATION	FORT	FAIBLE	FORT	FAIBLE

Trust Protocols – KAA

Devices communities

- KAA http://kaa.citi.insa-lyon.fr
- Impregnation stations
  - Community: cryptographic germ
- Each device is autonomous
  - Historic: public and private
  - Calculation of trust : “Friends of my friends are my friends”
- Cryptographic tools
  - Elliptic curves to guarantee the history

Trust Protocols

Services communities

- C. Levy-Bencheton, F. Le Mouël
- Each service is autonomous
  - Semantics' of service
  - Properties : author, vendor, characteristics (QoS, etc.), history
  - Calculation of trust :
    - Reputation: “Friends of my friends are my friends”, dissemination, (repudiation)
- Negotiation
  - Risk: divulgation of more and more properties
  - Contracts

Trusted Platform Module

An initiative of the Trusted Computing Group

http://www.trustedcomputinggroup.org

Risks in Today’s Information Systems

Compromised Systems

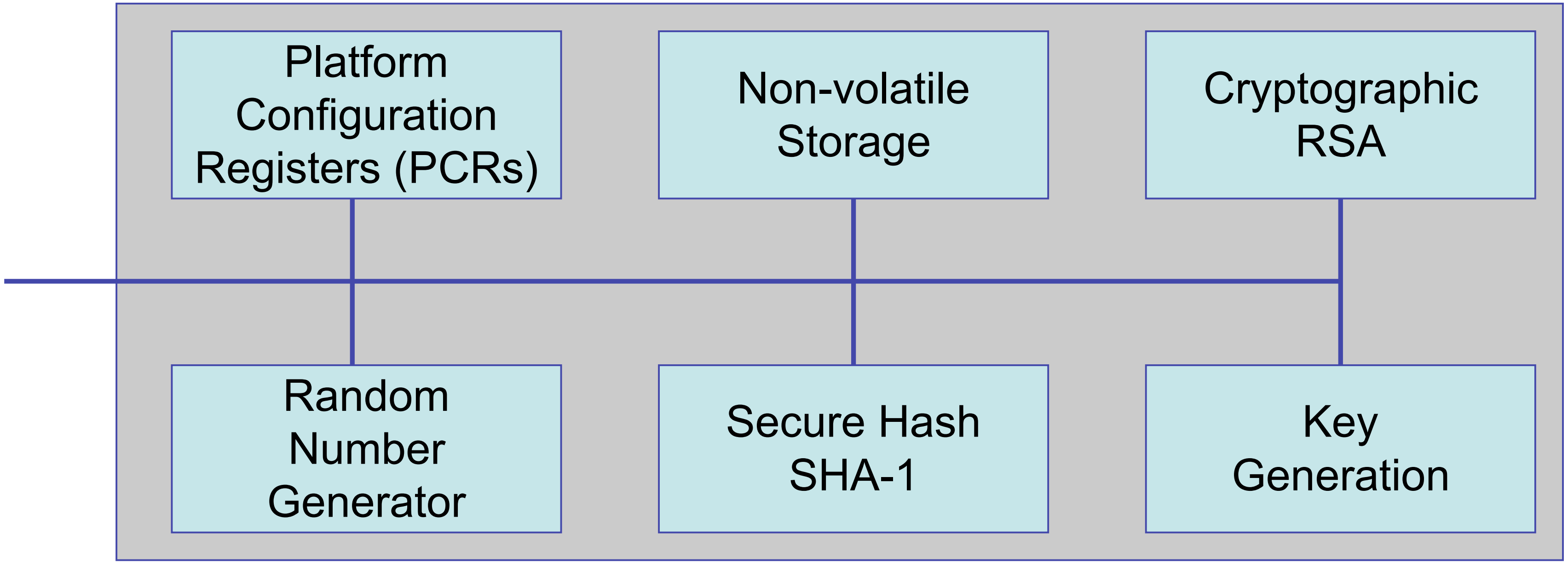
- Verify passengers for weapons before they board the plane!

Rogue devices and services (war driving).

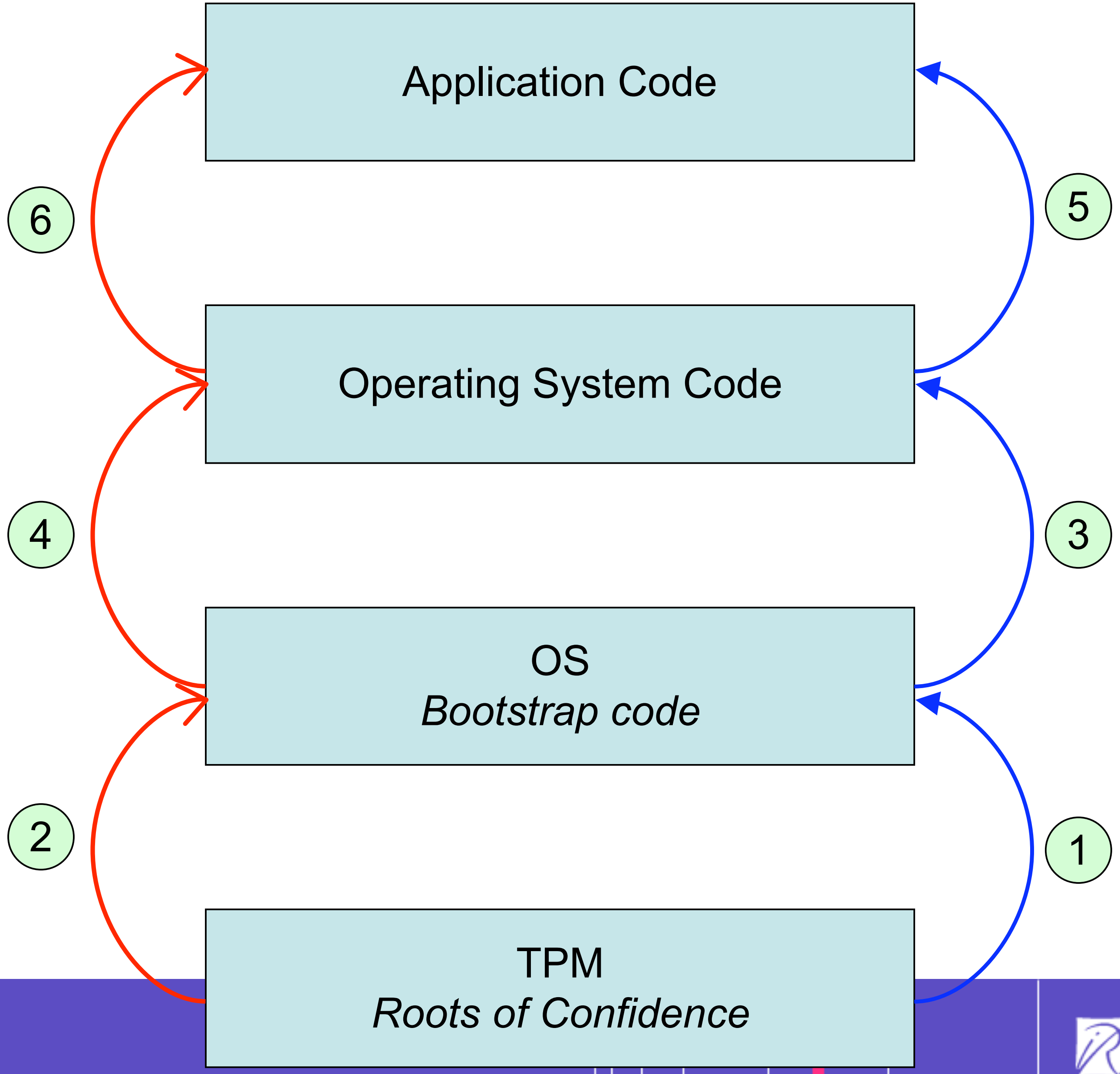
Lost or stolen data

- Citibank and Bank of America lost back-up tapes;
- Boeing – stolen laptop.

Structure of a TPM

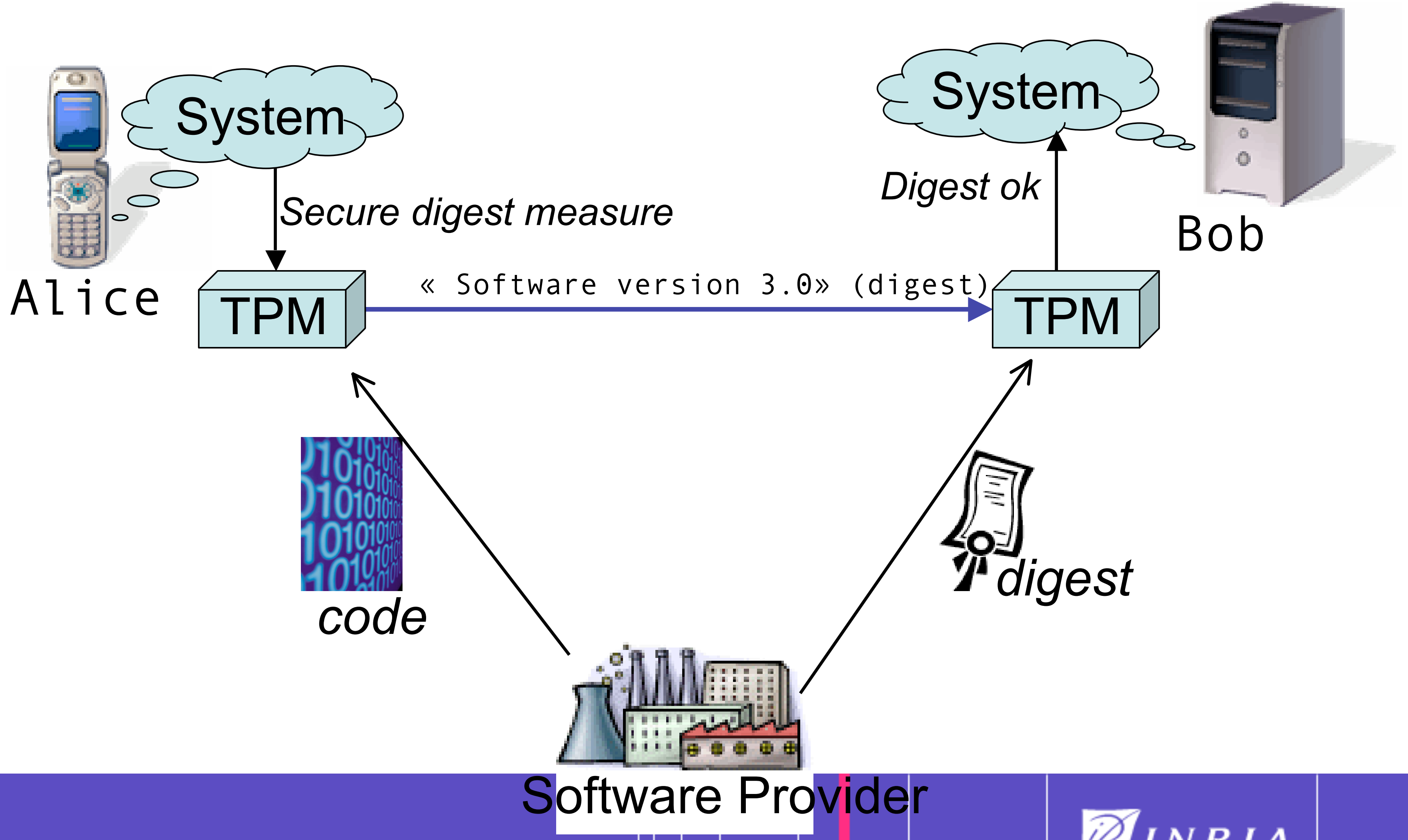


Roots
Of
Trust



On effectue des mesures d'intégrité de tout composant qui tourne.

Software Attestation



Technical Notes

Security can be built incrementally

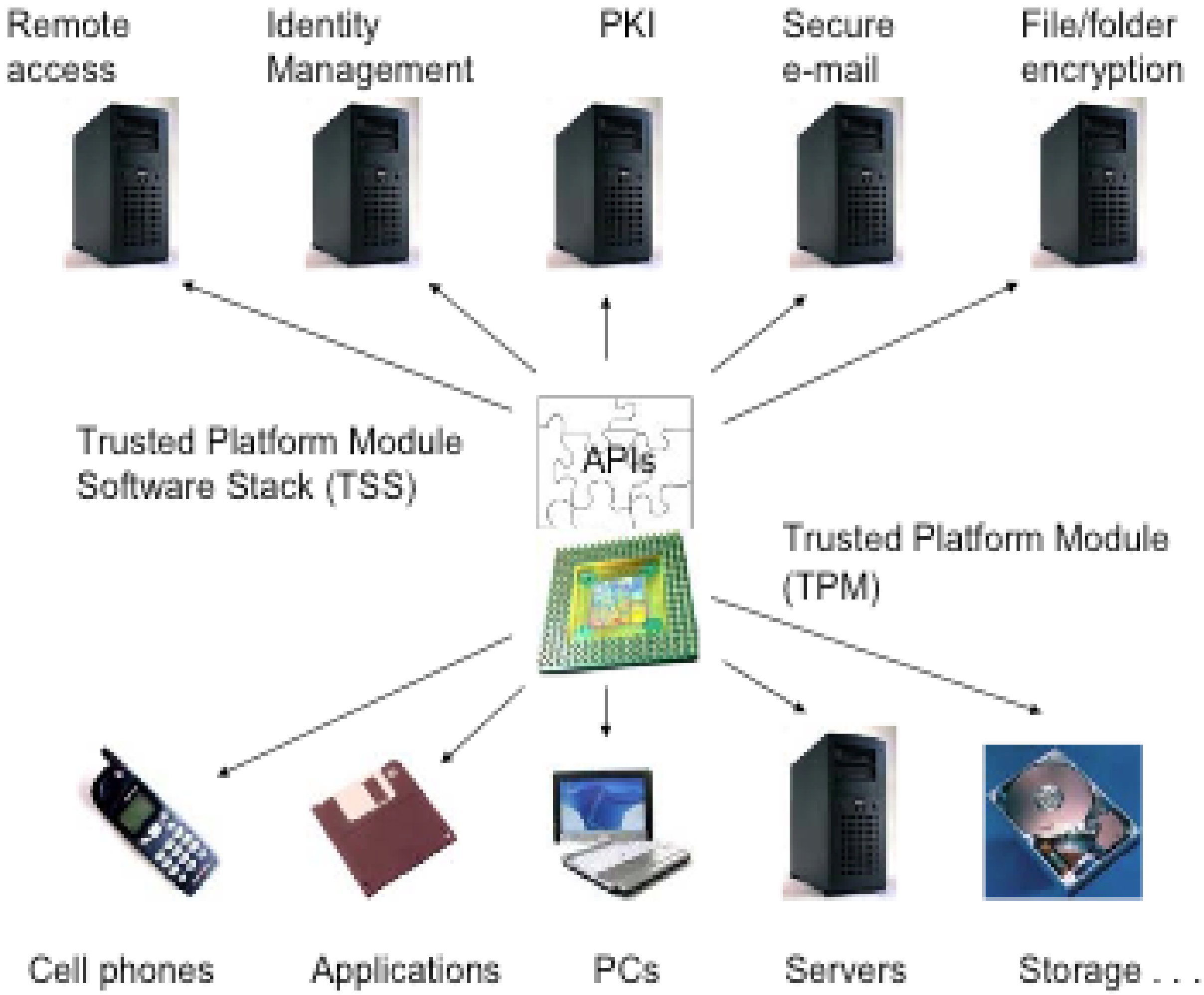
- Specification accompanied by a suite of protocols for Trusted Network Connection, Secure Storage, etc.

TCG is an optional model: pre-BIOS set-up.

To avoid lost key problem, private keys can be securely backed-up on another TPM.

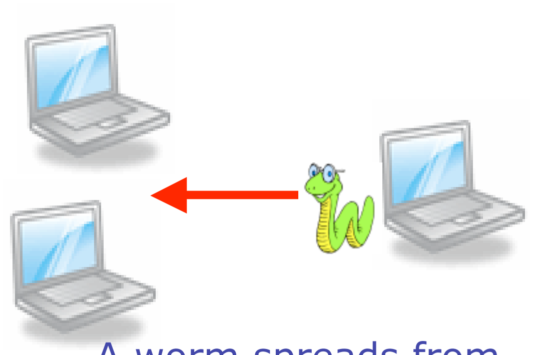
Trusted Computing Stack (TCS) is software layer interface to TPM

TCS / TPM


Remote access
Identity Management
PKI
Secure e-mail
File/folder encryption
Trusted Platform Module Software Stack (TSS)
APIs
Trusted Platform Module (TPM)
Cell phones
Applications
PCs
Servers
Storage . . .

Trusted Enterprise Model

Existing model



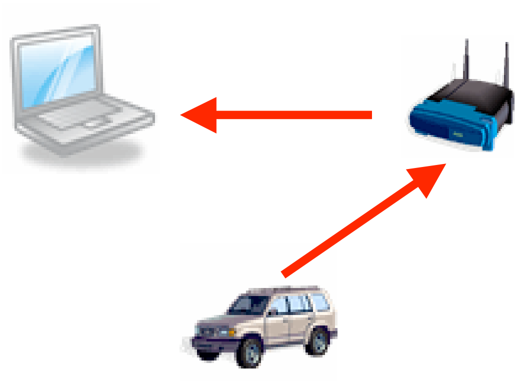
A worm spreads from
A single PC across network

Trusted enterprise model

TCC/TPM allows machines to
detect and isolate worm

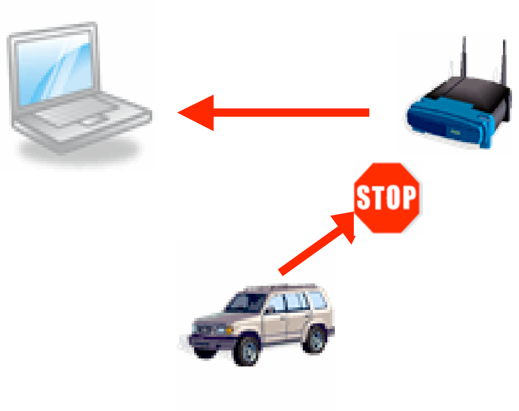
Trusted Enterprise Model

Existing model



Rogue access yıelds avenue
for war driving

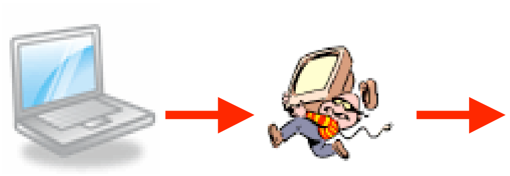
Trusted enterprise model



Rogue immediately recognized
as untrusted, and refused access

Trusted Enterprise Model

Existing model

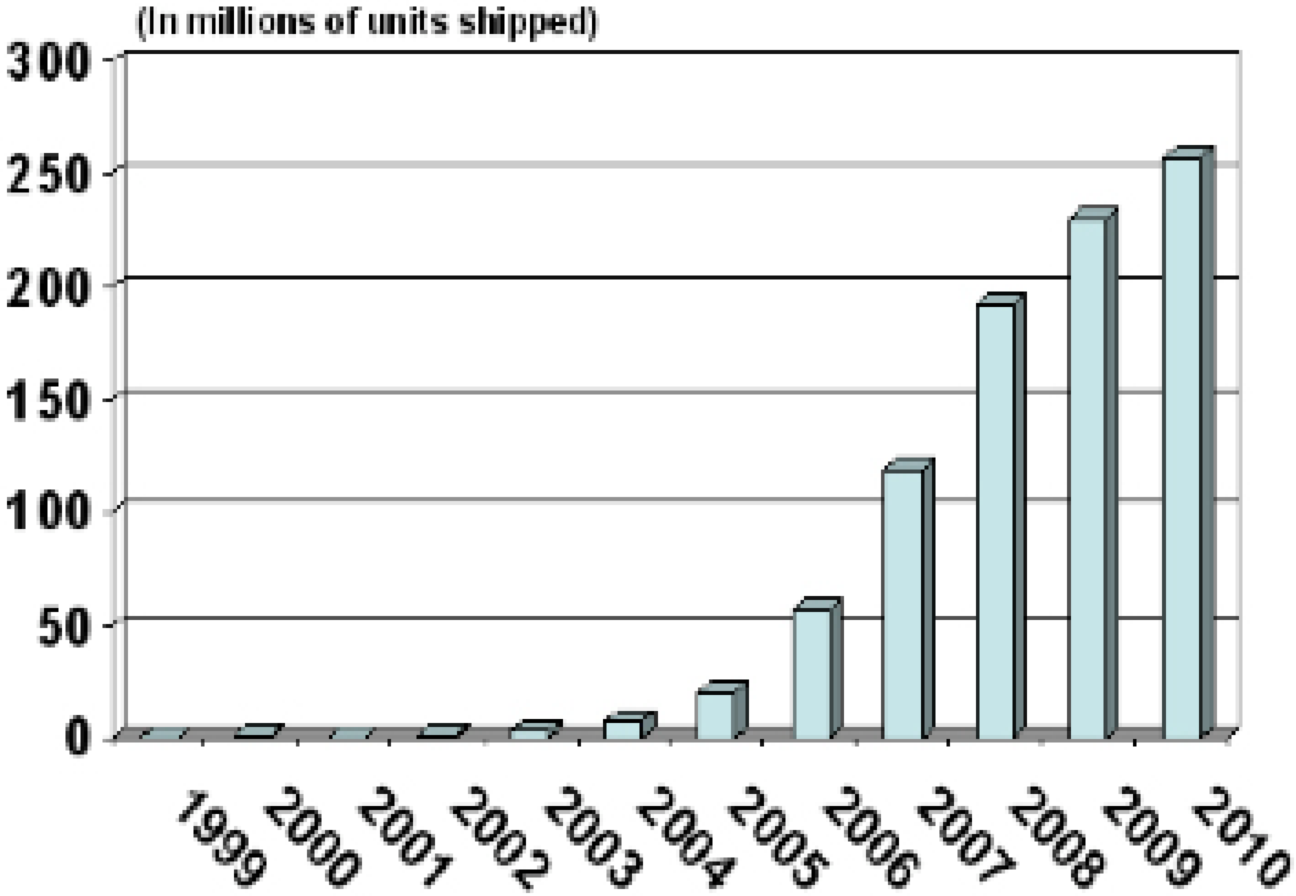


Device theft leads to information leakage

Trusted enterprise model

Theft only leads to encrypted
Documents being lost

TPM Availability Forecast



Current Work Around TPM

Trusted Servers

- Specification about how servers are created, managed and maintained
- Issues of asset management, configuration management, backups and data migration, distributed servers

Trusted Storage

- Drive security for standard hard disks
- Issues include full-disk encryption, disk-erase enhancement, drive locking, forensic logging
- Integrates into SCSI and ATA commands

Mobile Phones

- Issues include subscription management, mobile payment and ticketing, secure software download, etc.