TELECOM PARIS
école nationale supérieure des télécommunications

A Survey of Network Security Research at ENST



Gwendal Le Grand

gwendal.legrand@enst.fr

Ecole Nationale Supérieure des Télécommunications (ENST), Paris France

CNRS (LTCI – UMR 541)

get

Outline

- Presentation of ENST
- Digital security in 2005: crisis, stakes and roadmap
- Network security and projects at ENST (selected activities)
- Conclusion

ENST : Ecole Nationale Supérieure des Télécommunications

- Website : http://www.enst.fr/en
- **computer science and network** (INFRES) department
  - ≈ 50 permanent staff
  - ≈ 50 PhD students
- Research @INFRES:
  - Software & System engineering, Middleware, Reconfigurability, Adaptability, software radio
  - Heterogeneous networks, interconnection, interworking and administration, Traffic modelling, Architecture Design, Metrology, QoS ;
  - Mobile technologies : GSM, GPRS, UMTS, WiFi, Bluetooth,
  - Queues, performance assessment, distribution approximations, stochastic analysis.
  - Discrete structures, graphs, algorithms ; Algebraic coding, cryptology ;
  - Artificial Intelligence, expert systems, natural languages processing ;
  - Databases, Semantic Web.
  - Security : Critical Infrastructure Protection, QuantumNetworks, Grid security, Network security (802.11, Bluetooth), Ad hoc & active network security, Privacy, cryptology, watermarking, cryptographic protocols, PKIs, IPv6 security, Authentication, Honey pots, IDS, protection of services ;
- ENST is part of Euronetlab (www.euronetlab.net).
  - Study of security of QoS routers and mobile routers.

The security crisis

- No real trust in ICT
  - Physical relationship still important in exchanges and commerce (relative failure of e-commerce, …)
    - trust in the exchanges ≠ security of electronic payment.
  - Virtual world
    - Anonymity, geographic virtuality.
- No real spread of existing technologies
  - Digital signature not used
  - PKI (too complicated, non interoperable, hard to assess)
  - Smart card does not really spread out of France
  - How to protect distributed systems?
  - Biometry still not used (except digital identity maybe)
  - Need to define new concepts for security
    - Find alternatives to Alice and Bob, claissical cryptography, SSL …
- Security is hard to sell: No “added value”, noRoI

ICT Security stakes in 2005

- Restore trust in the digital world
  - ⇨ E-commerce, e-business, e-content, e-government, e-vote, e-democracy
- Resilient infrastructures
- Protected Networks and systems
  - ⇨ Multimedia, software, dissemination of knowledge
- Protect infospheres
  - ⇨ Individual : protect privacy
  - ⇨ Company : anticipate problems
  - ⇨ Critical infrastructures : prevent domino effect, limit cybercriminality
- Immune applications and data

… in a mobile world with ambient intelligence

• Avoid drastic security measures
  Crisis management
• ICT vulnerability
  •Interconnected, more complex and fragile
  Interdependencies
  Just-in-time business

• A quality label (certification)
  Software engineering

• Protection against any type of attack
  Physical attacks

Towards a digital order?
Security incompatible with uncontrolled world.
Need of some principles (ethics, responsability, transparency, autonomy, …) in a realistic world.
Applicable for the international community.
Accepted by users and stakeholders

Why are systems vulnerable?

- Complexity
  - ⇨ Ontologies and their structuration
  - ⇨ Heterogeneity
    - Size, number of actors, entities and actions
  - ⇨ Architecture
    - Semantics and types of components and links
    - Each canonic architecture has its intrinsic vulnerabilities
  - ⇨ Virtual (abstraction)
    - Digital imitation (machine, network, OS, company …)
- Distribution
  - ⇨ Scalability
  - ⇨ Protocols and exchanges
- Sensitivity
  - ⇨ Tangible value
  - ⇨ Corporate image (symbolic attack …)
- Movement
  - ⇨ Mobility … but a mobile world has a history
    - footprints of the ontologies (subjects, objects, operations)
    - Witnesses

Mobility and ambient intelligence

- Classical security models are timeless and not fitted to mobility
  - ⇨ Must enrich existing models, policies, protocols to take into account context and spatio temporal properties.
  - ⇨ Tracability to log history
    - Keep the memory of the system
- Morphology of the system is linked to its protection and its security
- Restore trust in ICT systems requires to reform Internet, prevent anonymity, provide proofs.
  - ⇨ Need of alibis to prove that here and now there are witnesses of events.
  - ⇨ Need to identifying spatio-temporal trusted invariants in this environment: location of base stations, trusted clock, etc.
- Mobility may be an asset
  - ⇨ Liberty: intelligence and information may move where needed
  - ⇨ Creates entropy: useful to introduce randomness and secrets (mobile cryptography).

Security R&D roadmap

- Classical security technologies
  - ⇨ Cryptology, cryptographic protocols and formal methods
  - ⇨ Security policies and models
  - ⇨ Certification and assessment methodology
- Security of infrastructures
  - ⇨ Model the big public open domains
    - PKIs, quantum, critical infrastructures …
  - ⇨ Model privacy
    - Personal infospheres …
- Security of non functional properties
  - ⇨ Mobility: ad hoc networks, mesh networks, PANA …
  - ⇨ Configurability: personalized middleware, downloadable software, mobile agents
  - ⇨ Distribution: security of grids, virtual machines, distributed OS
  - ⇨ Architectures
- Security of the content and services (application layer)
  - ⇨ DRM, IPR
  - ⇨ Watermarking
  - ⇨ Cryptographic protocols dedicated to specific uses
- Network security
  - ⇨ Security of multi service networks (GPRS, UMTS …)
  - ⇨ Security of protocols (AAA, DNSSec, Mobile IP, …)
  - ⇨ IDS, honeypots …
- Hardware entities
  - ⇨ Personal trust entity (smart card)
  - ⇨ Secure hardware architecture : configurable crypto-processor high throughput cryptography
- Biometry

Projects at ENST (recent past, **present and near future**)

National (RNRT)

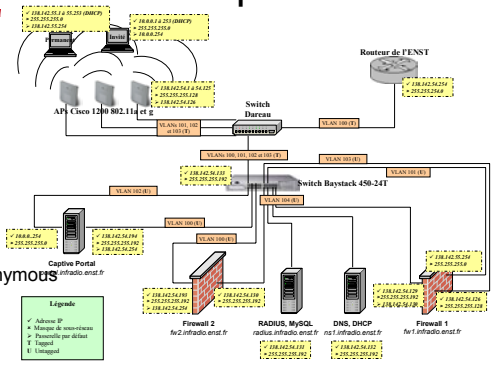
- Icare :trusted infrastructures, PKIs
- Swap : WAP security
- MMQoS : security, mobility and QoS
- Anaïs : security of Professional Mobile Radio
- **Infradio : Security on a campus and of infospheres in meshed networks**
- Epis : smart card security E2E with IPv6
- Resodo : Security of domestic networks
- Aquaflux : mediametry watermarking
- Artus : augmented reality marking

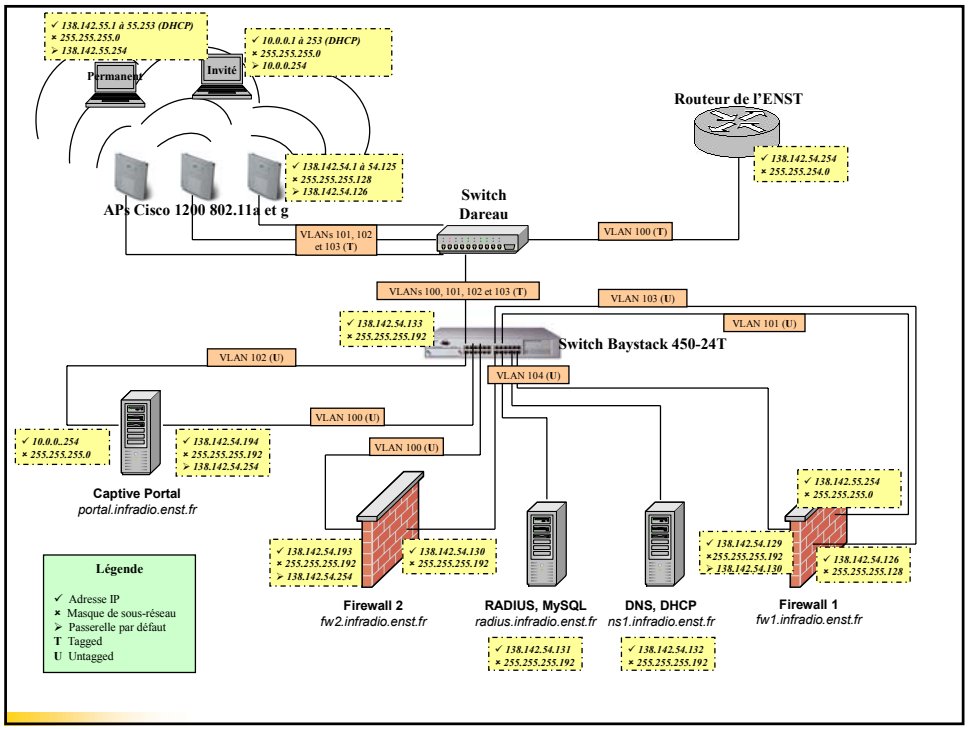
European projects

- ITEA Ambience : security in a mobile world, ambient intelligence
- ITEA BRIC : audiovisual watermarking
- **CELTIC BUGYO: Telecom infrastrucure protection**
- IST Acip : Critical infrastructure protection
- **IST CI2RCO: CIIP**
- **IST IRRIIS (IP): CIIP– starts end 2005**
- **IST DESEREC (IP): CIIP– starts end 2005**
- **IST SECOQC (IP): Quantum network**
- **IST EuroNGI (NoE): Trust …**
- Vipbob : cryptographic protocol with biometric data

INFRADIO (RNRT)– Radio infosphere

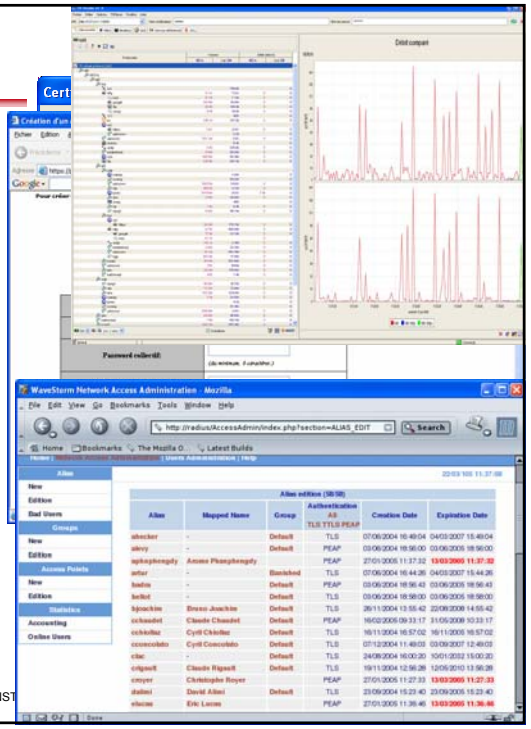
- What radio infrastructure?
  - Communication sphere
  - Variable size, spontaneous, robust
  - Secure, administrated
  - Applications
- Security policies in a semi open world
  - Semi open
    - Permanent staff, usual users, anonymous
    - Variable infrastructure
  - Configurable security policies
    - Audit and imputability policies
    - Granularity of security, adapt to a profile
  - Mobility = vulnerability, manage a secure mobility
  - Authentication of subjects and objects, secure architecture, alibis, tracability, web of trust
  - QoS access control





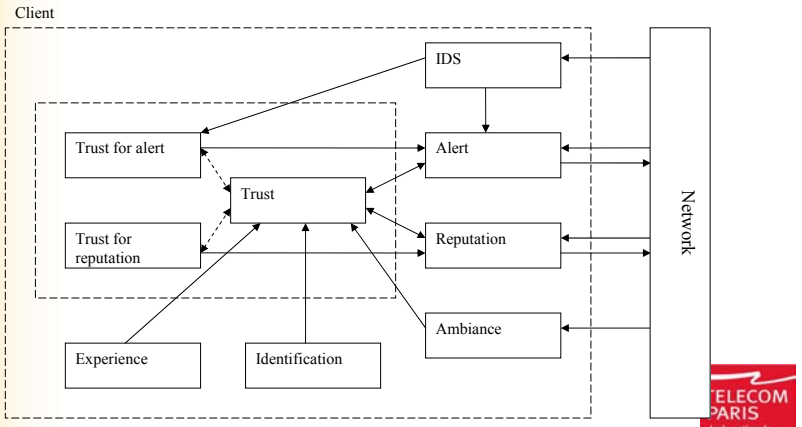
Deployment

- AP deployment
- Presentation of the service
- Network management
- Security delegation
- Certificates
- Hotspots
- Radius proxy to update the CA (site mobility possible)



Dynamic evolution of trust

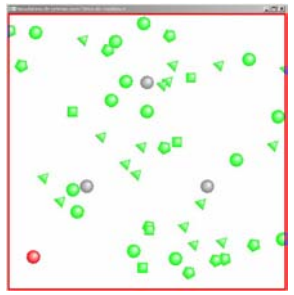
- Enhanced DIDS
- Each client computes its own trust => more robust

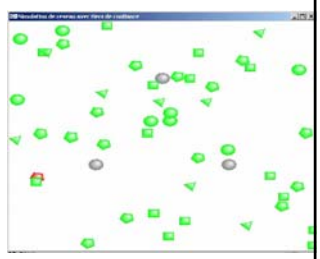


Dynamic evolution of trust

Evolution of trust

- Depending on the ambience



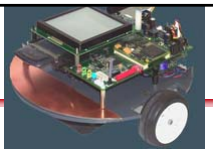


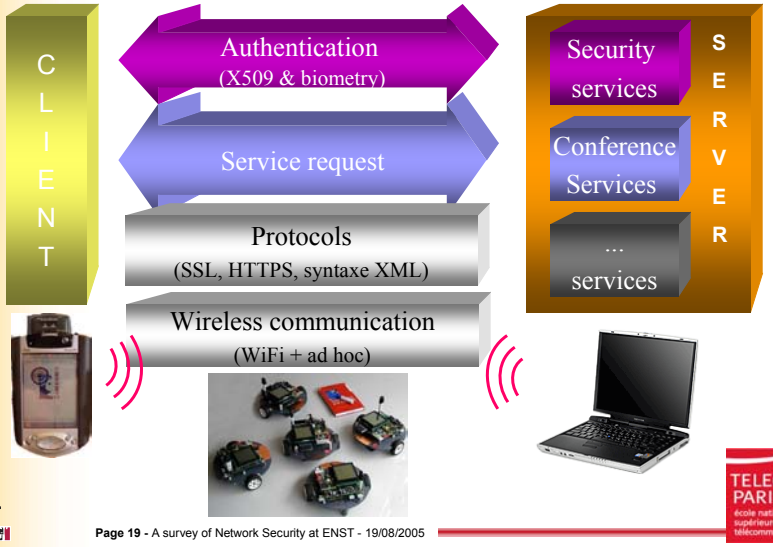
AMBIENCE (ITEA)

- Ambience Demo movie
  - http://perso.enst.fr/~legrand/Video/M1_Guide2Meeting.mpg
- Classical security objectives
  - Confidentiality
  - Authentication
  - Integrity
  - Access Control
  - Availability : network services resist DoS attacks

- New constraints for security
  - Unreliable wireless link
  - Physical protection of weak nodes
  - Limited resources (CPU, memory, batteries, …)
  - No centralized infrastructure (no trusted third party)
  - Secure routing to distribute secrets
  - Dynamic topology : maintain trust in a dynamic environment.

Demo architecture





Critical Infrastructure Protection

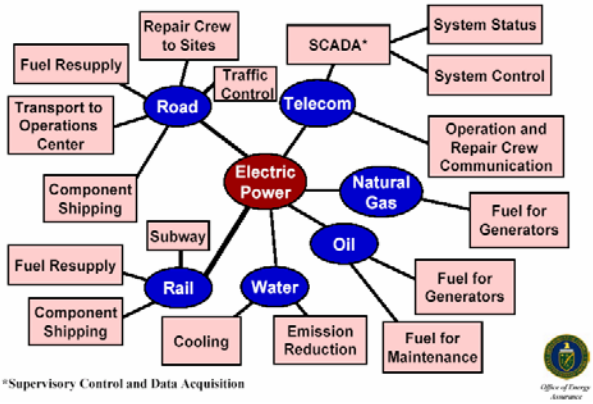
- IST projects : ACIP, CI2RCO, DESEREC, IRRIIS
- Celtic : BUGYO
  - ⇨ Roadmap, build network, design tools, models and solutions for CIIP
- ENISA (European Network and Information Security Agency)



Domains	Information & Communication	Bank & Finance	energy	Transportation	Vital HS	Governement



Complexity



*Supervisory Control and Data Acquisition

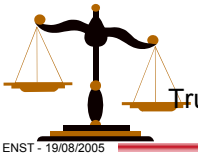
Classical Security

- Security models
  - ⇨ Alice & Bob share a secret (mutual confidence)
  - ⇨ They use classical (symmetric & asymmetric) cryptography
    - – To cipher a message (cryptography)
    - – To insert a subliminal mark in a content (watermarking)
- Cryptographic protocols : SSL, IPSec, …
- Trusted Infrastructures : Public Key Infrastructures, Certificates (X509)

Point-to-point

Alice

Bob



Cryptography

Trusted Third Party

New Models

- New requirements
  - ⇨ Urbanization
  - ⇨ Heterogeneity
  - ⇨ Mobility
- Restore
  - ⇨ Real world
    - trusted clock & position, …
  - ⇨ Semantics & context

The two classical Planes in 2005

Logical

Physical

Von Neum

New Planes for 2010

Communications & Computers

Introduction of new **complexity**

Virtual

Logical

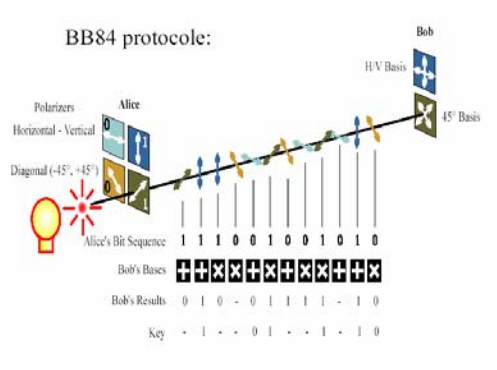
Physical

Emergence of **randomness**: the **Quantum** Age

Quantum

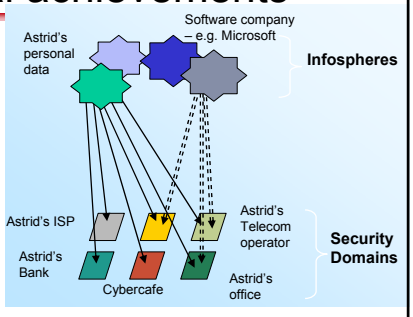
SECOQC (IST) : quantum cryptography

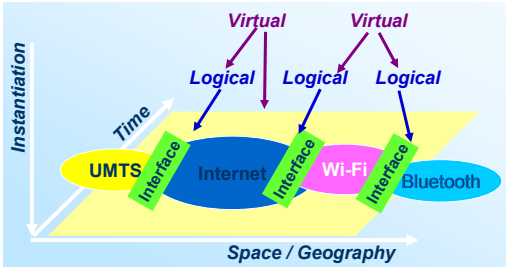
- Evolving **quantum cryptography** into an instrument that can be operated in an economic environment.



SEINIT (IST): Conceptual achievements

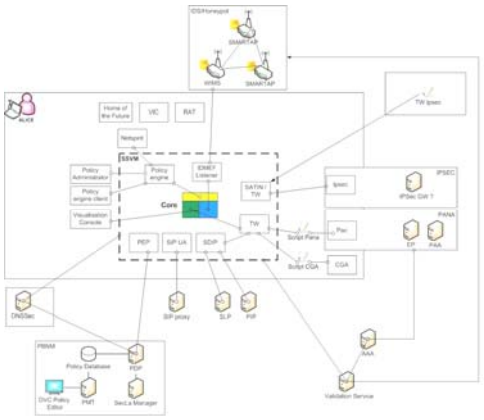
- The virtualisation of security
  - Negotiation among policies
- SEINIT achieved :
  - ✓ The Abstract Security Architecture
  - ✓ The definition of the SEINIT Virtualisation Engine



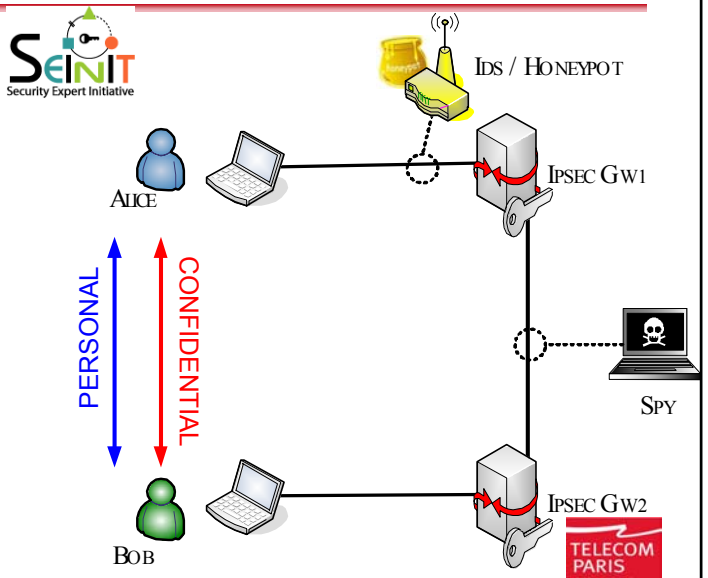


SEINIT: Architectural achievements

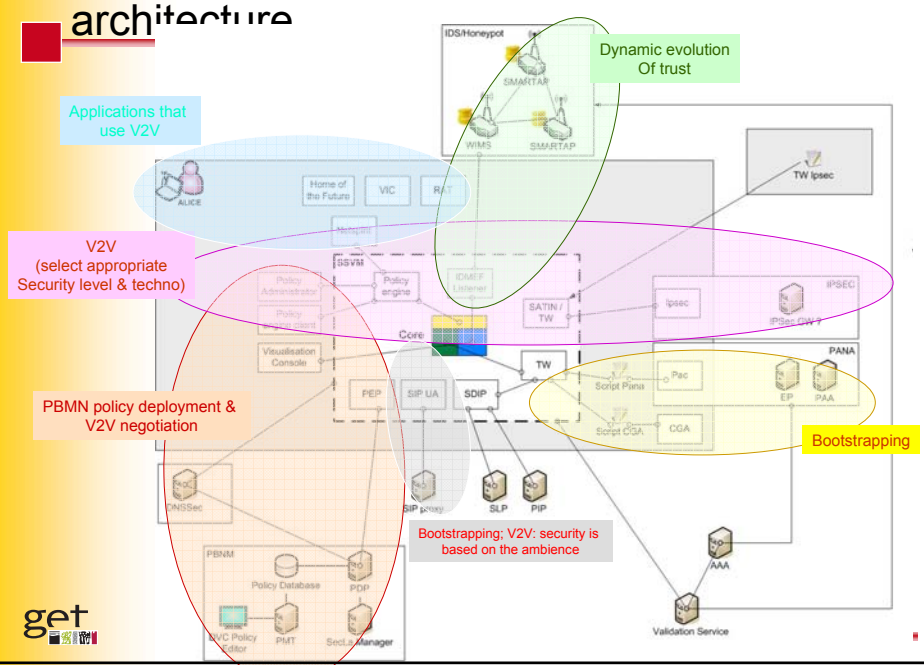
- A scalable architecture
  - ⇨ A SecLA-based security configuration
  - ⇨ The dynamic deployment of components and wrappers
  - ⇨ Secure repository and inter-domain Authority
- Towards mobility support
  - ⇨ Addressing the trust bootstrapping issue
  - ⇨ enhancing threat detection
    - In a distributed, wired and wireless monitoring system



SEINIT: Demo architecture



SEINIT: Concepts mapped on the architecture



Conclusion

- Research projects at the National (RNRT) and European (ITEA, IST) level
- Innovative work in key domains
- ENST is one of the European leaders in network security research