ARES PROJECT

Advanced Research on Information Security and Privacy

Prof. Josep Domingo-Ferrer

Universitat Rovira i Virgili, Tarragona

February 27, 2009

Research Team

- ARES is composed of research groups from:
  - Universitat Rovira i Virgili
  - Universitat Politècnica de Catalunya
  - Universidad de Málaga
  - Universitat Oberta de Catalunya
  - Consejo Superior de Investigaciones Científicas
  - Universitat de les Illes Balears

Research Team

- Formed by **78** researchers
  - Out of which **51** holding a Ph.D.
  - Average age: **35** years
- Project duration
  - From October 2007 to September 2012

Research Themes

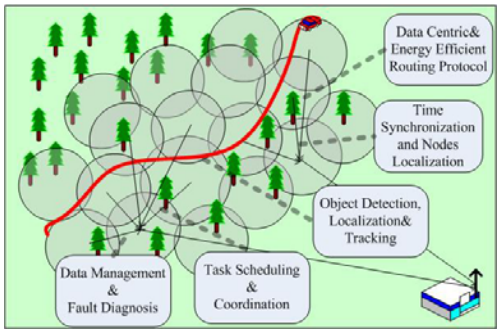
- Main Objective
  - “Develop new technology for **protection of privacy** in the **information society**”
- Research Lines:
  - Critical infrastructure protection
  - Ubiquitous computing
  - Electronic transactions
  - Digital rights management
  - Private data management

Critical Infrastructure Protection

- Priority for homeland and corporate security:
  - Airports, power plants, hospitals, financial facilities, etc.
- They depend on the safe operation of the information systems that control them

Critical Infrastructure Protection

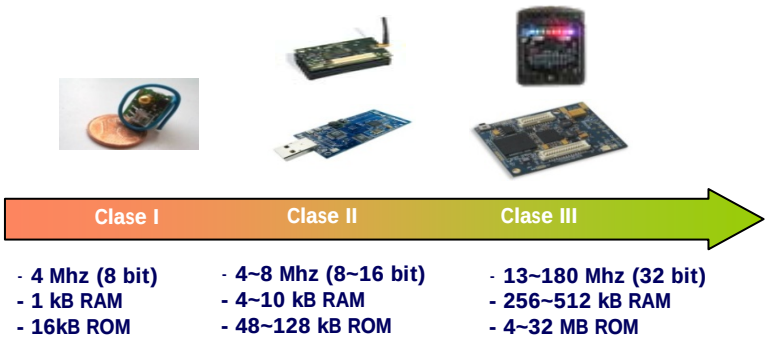
- Infrastructure protection by means of sensor networks
  - Constrained computational power
  - Hostile environment solutions
    - Key management
    - Node failure detection



A. Viejo, F. Sebé and J. Domingo-Ferrer, "Secure and Scalable Many-to-One Symbol Transmission for Sensor Networks". Computer Communications . Vol. 31, pp. 2408-2413. Jun 2008. ISSN: 0140- 3664.

Critical Infrastructure Protection

- Security primitives in sensor nodes
  - Classification of sensor nodes
  - Analysis of suitable security primitives for sensor nodes



R. Roman, C. Alcaraz and J. Lopez, "A Survey of Cryptographic Primitives and Implementations for Hardware-Constrained Sensor Network Nodes" Mobile, Networks and Applications (MONET) Vol. 12, pag 231-244, Springer, 2008, ISSN 1572-8153.

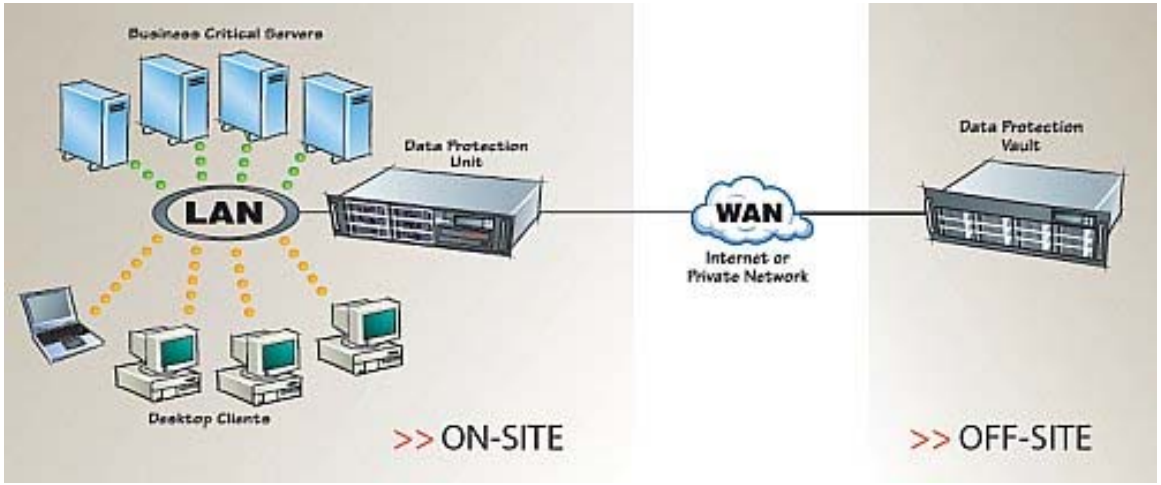
Critical Infrastructure Protection

- Protecting Critical Infrastructures through WSNs
  - Analysis of characteristics and operations of WSNs for the protection of CIs
    - Support for *Early Warning Systems* (EWS) & *Dynamic Reconfiguration Systems* (DRS)
  - New challenges: support services, trust/security management, secure control systems and assessment mechanisms

- J. Lopez, C. Alcaraz and R. Roman, "On the Protection and Technologies of Critical Information Infrastructures". En Foundations of Security Analysis and Design Tutorial Lectures, pp 160-182. LNCS 4677. Springer, October 2007, ISBN 978-3-540-74809-0.
- C. Alcaraz, R. Roman and J. Lopez , "Análisis de la Aplicabilidad de las WSN para la protección de Infraestructuras Críticas", VII Jornadas de Ingeniería Telemática (Jitel 2008), Alcalá de Henares, Spain, September 2008.

Critical Infrastructure Protection

- Remote integrity checking of backup data
  - Cost-efficient solutions
  - Data privacy concerns



F. Sebé, J. Domingo-Ferrer, A. Martínez-Ballesté, Y. Deswarte and J.J. Quisquater, "Efficient remote data possession checking in critical information infrastructures". IEEE Transactions on Knowledge and Data Engineering. Vol. 20, pp. 1034-1038. Aug 2008. ISSN: 1041-4347.

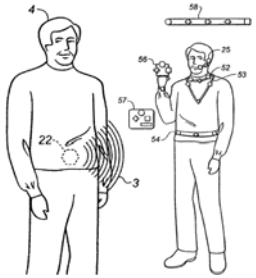
Critical Infrastructure Protection

- Intrusion Detection Systems
  - Analysis of network traffic for attack detection
  - Data collection preserving user privacy
  - Agent-based solutions

- J. Garcia-Alfaro and G. Navarro. "Prevention of Cross-Site Scripting Attacks on Current Web Applications". Lecture Notes in Computer Science. Vol. 4804 (On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS), pp. 1770-1784, Nov 2007, Portugal. ISSN: 0302-9743.
- R. Páez, J. Tomàs-Buliart, J. Forné, M. Soriano, “Securing Agents against Malicious Host in an Intrusion Detection System”, 2nd International Workshop on Critical Information Infrastructures Security (CRITIS), 2007.

Ubiquitous Computing

- Privacy in RFID-tagged shopping
  - Tagged products can be traced thus jeopardizing buyer privacy
  - Research on privacy-preserving tag identification



A. Solanas and J. Manjón, "Deployment of RFID Readers for the Scalable Identification of Private Tags: a Simulation Study". RFID Security: Techniques, Protocols and System-On-Chip Design . 2008. ISBN: 978-0-38776-480-1.

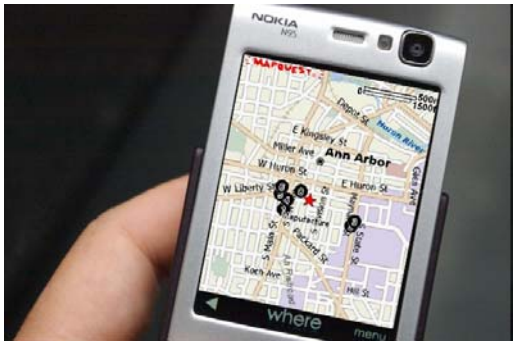
Ubiquitous Computing

- Security and privacy in RFID-enabled personal documentation
  - RFID in traditional paper-based documentation provides advanced features and a seamless link to the information system
  - Advanced security mechanisms required to protect the identity and the personal information of bearers.

- P. Najera, F. Moyano and J. Lopez, "Security mechanisms and access control infrastructure for e-Passports and general purpose e-documents". Journal of Universal Computer Science, Special Issue on Data Security and Privacy Protection in Pervasive Computing environments. To appear
- P. Najera, F. Moyano and J. Lopez, "Secure Integration of RFID Technology in Personal Documentation for Seamless Identity Validation" in 3rd Symposium of Ubiquitous Computing and Ambient Intelligence 2008. pp. 134-138. Series: Advances in Intelligent and Soft Computing , Vol. 51, Springer. 2008. ISBN: 978-3-540-85866-9

Ubiquitous Computing

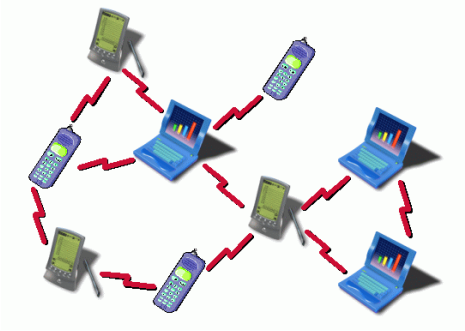
- Location Based Services
  - User devices receive information depending on their location
  - Technology solutions protecting users from tracing are needed



A. Solanas and A. Martínez-Ballesté, "A TTP-Free Protocol for Location Privacy in Location-Based Services". Computer Communications . Vol. 31, pp. 1181-1191. Apr 2008. ISSN: 0140-3664.

Ubiquitous Computing

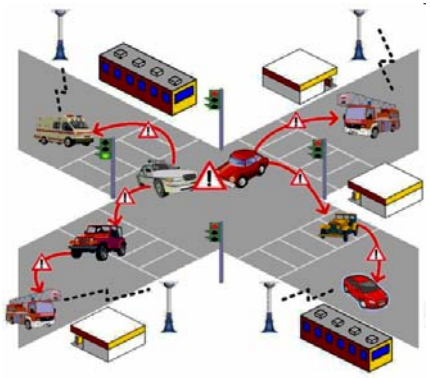
- Mobile Ad-Hoc Networks
  - Decentralized networks
  - Research on
    - Routing technology in hostile environments
    - Certificate Validation
    - Trust models

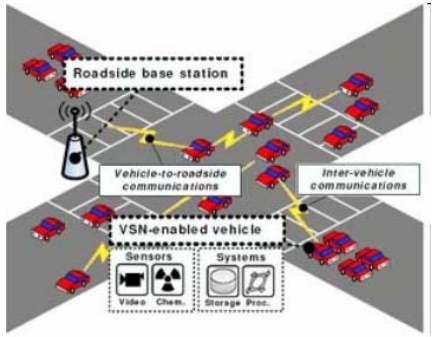


- J. Forné, J. L. Muñoz, F. Hinarejos, O. Esparza, "Certificate status validation in mobile ad hoc networks". IEEE Wireless Communications, February 2009.
- M. Mejia, N. Peña, J. L. Muñoz, O. Esparza, "A review of trust modeling in ad hoc networks". Internet Research, Vol. 19 No. 1, pp. 88-104. 2009

Ubiquitous Computing

- Vehicular Ad-Hoc Networks
  - Car-to-car communications permit:
    - Real-time alerts about dangers (braking, lane changes, etc.)
    - Announcements about traffic conditions (jams, icy roads, etc.)
  - Privacy must be kept by preventing driver tracking





V. Daza, J. Domingo-Ferrer, F. Sebé and A. Viejo, "Trustworthy privacy-preserving cargenerated announcements in vehicular ad hoc networks". IEEE Transactions on Vehicular Technology. To Appear.

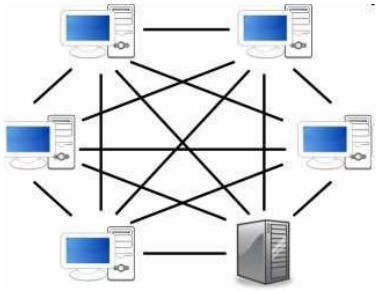
Secure Electronic Transactions

- Research on security and privacy of electronic transactions
  - Legal aspects of electronic transactions
  - Electronic payment systems
  - Electronic contracts
  - Formal validation of protocol security
  - Private information retrieval

- A. Martínez Nadal, “Comentarios a la ley 59/2003 de firma electrónica”. CIVITAS EDICIONES, S.L. ISBN: 978-84-470-2221-2.
- J. Castellà-Roca and A. Vives-Guasch, “Billetes electrónicos seguros”. Reunión Española de Criptología y Seguridad de la Información (RECSI) , pp. 141-150. 2008. ISBN: 978-84-691-5158-7.

Secure Electronic Transactions

- Private Information Retrieval
  - User queries to Internet search engines reveal user habits
  - Research on query anonymization:
    - Query masking
    - P2P-based query anonymization



- J. Domingo-Ferrer, A. Solanas and J. Castellà-Roca, "h(k)-Private Information Retrieval from Privacy-Uncooperative Queryable Databases". Online Information Reviews. To Appear.
- J. Domingo-Ferrer, M. Bras-Amorós, Q. Wu and J. Manjón, "User-Private Information Retrieval Based on a Peer-to-Peer Community". Data & Knowledge Engineering. To Appear.

Digital Rights Management

- Intellectual property of digital content has to be protected
- P2P file sharing makes content redistribution very easy

Digital Rights Management

- Research on Copy Detection Systems
  - Watermarking
    - Copyright information embedded into digital content
  - Fingerprinting
    - Security against collusion by dishonest buyers

- M. Fallahpour, D. Megías, “Reversible Data Hiding Based On H.264/AVC Intra Prediction”. Lecture Notes in Computer Science (IWDW 2008). ISSN: 03029743.
- J. Tomas-Buliart, M. Fernández, M. Soriano “Protection of mobile agents execution using a modified Self-Validating Branch-Based Software Watermarking with external sentinel” in CRITIS, Frascati, Oct. 2008.

Private Data Management

- Electronic transactions permit automatic collection of large amounts of personal data
- Sharing and publishing personal data must be compatible with individual privacy

- **Transfer Contracts: EUROSTAT, IDESCAT**
- **Spin-Off: STAITEC**

Private Data Management

- Secure Data Mining
  - Research on:
    - Data masking methods
    - Record linkage algorithms
    - Privacy preserving data mining

Name	Weight	Height
(…)	(…)	(…)
Anna	77	1,77
(…)	(…)	(…)

Age	Weight	Height	Result
25	63	1,55	Yes
35	70	1,68	Yes
32	77	1,77	No

- J. Nin, J. Herranz, V. Torra, "Rethinking Rank Swapping to Decrease Disclosure Risk". Data & Knowledge Engineering. Vol. 64, issue 1, Pages 346-364. Jan 2008. ISSN: 0169-023X.
- J. Domingo-Ferrer, F. Sebé and A. Solanas, “An anonymity model achievable via microaggregation”, LNCS 5159, pp. 209-218, Aug. 2008. Vol. 5th VLDB Workshop on Secure Data Management-SDM 2008, Berlin: Springer-Verlag

Conclusion

- Information society has to stay secure to survive.
- Security will progress even without public support …
  - … but privacy technology has less commercial appeal.
- Information society must respect privacy to stay human.

ARES Leitmotiv

“National and corporate security”

vs

“Individual Privacy”

First Year Scientific Indicators

	Objective	Actual
ISI JCR journal articles or LNCS	60	**81**
Book Chapter or ISBN conferences	60	**93**
Intergroup publications	12	**18**
Patents	1	**1**
Ph.D. Theses	5	**8**
New funded projects	10	**16**

First Year Scientific Indicators

- Researchers who have joined ARES:
  - Post-doctoral grant holders:
    - Qianhong Wu from China
    - Roberto Di Pietro from Italy
    - Guillermo Navarro from Spain
    - David Rebollo from Spain
  - Pre-doctoral grant holders:
    - From Spain: 8
    - From China: 1
    - From Cuba: 2
    - From Sweden: 1
    - From Romania: 1
    - From Iran: 1

ARES PROJECT

Advanced Research on Information Security and Privacy

Prof. Josep Domingo-Ferrer

Universitat Rovira i Virgili, Tarragona

February 27, 2009