A Privacy Enhancing Architecture for Collaborative Working Environments

Jasone Astorga, Purificacion Saiz, Eduardo Jacob, Jon Matias
{jasone.astorga, puri.saiz, eduardo.jacob, jon.matias}@ehu.es

Department of Electronics and Telecommunications

Universidad del País Vasco Euskal Herriko Unibertsitatea

PRO-VE'10, 11-13 October 2010, Saint-Etienne

Agenda

- Introduction
- Privacy and Security Concerns
- Collaborative System Architecture
- Proposed Solution
- Formal Validation of the Proposed Security Protocol
- Architecture Deployment in a Real Environment
- Conclusions

Introduction

- Architecture of the considered target scenarios:
  - Distributed applications consisting of different devices and software modules that interact with each other.
  - Ubiquitous access to the system:
    - Use of PDAs, laptops, etc.
  - Heterogeneous application or information servers:
    - Sensors and other low capacity devices used to collect data and real-time information.
- Main characteristics: invisibility and pervasiveness
  - Huge potential value.
  - Key challenges: **PRIVACY!**

Privacy and Security Concerns (I)

Privacy: "…the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others…" [Westin]

- The considered collaborative environments present important challenges to protect end-users' privacy:
  - Unprecedented data collection coverage.
  - Invisibility of the collection process.
  - Amount of data collected.
  - Envisioned system connectivity.

Privacy and Security Concerns (II)

- Main objective of our work:
  - Develop an infrastructure that allows the construction of privacy-aware collaborative applications integrating low capacity devices.
- Privacy vs Security:
  - *Privacy*: implies the possession of some kind of information and the subsequent terms and conditions by which it may be used, retained and disclosed to others.
  - *Security*: describes the capacity of a technical system to protect and maintain the privacy of the information within that system.

Privacy and Security Concerns (III)

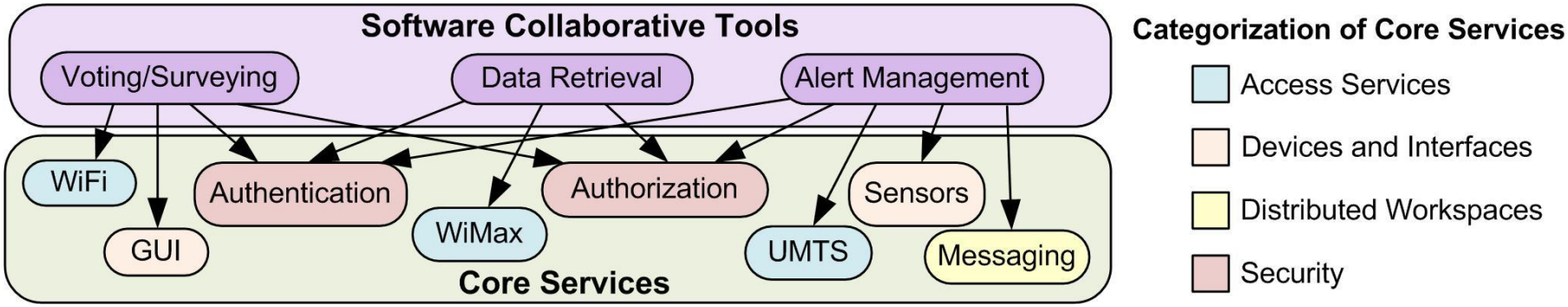
Privacy-aware architecture → Implementation of security mechanisms → Cryptography

Authentication
Authorization
Integrity
confidentiality

Highly resource consuming algorithms
vs
Severely limited devices

Traditional security mechanisms and asymmetric cryptography not applicable

Collaborative System Architecture



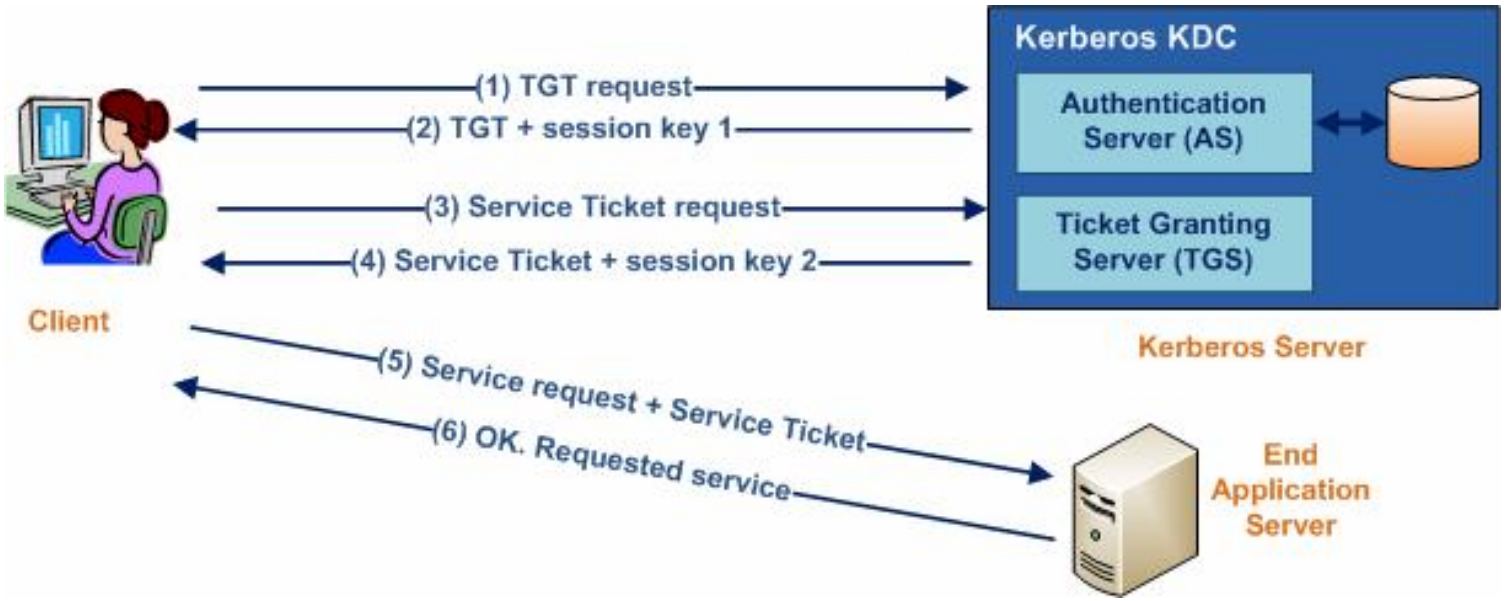
- Core Services:
  - Reusable software modules implementing basic or core functionalities.
- Software Collaborative Tools:
  - Offer aggregated functionalities by exploiting one or more core services.
- Necessity of centralized management of identity and access rights related information:
  - Neutrality and independence of core services.
  - Different trust relationships in different collaborative applications.

PROPOSED SOLUTION

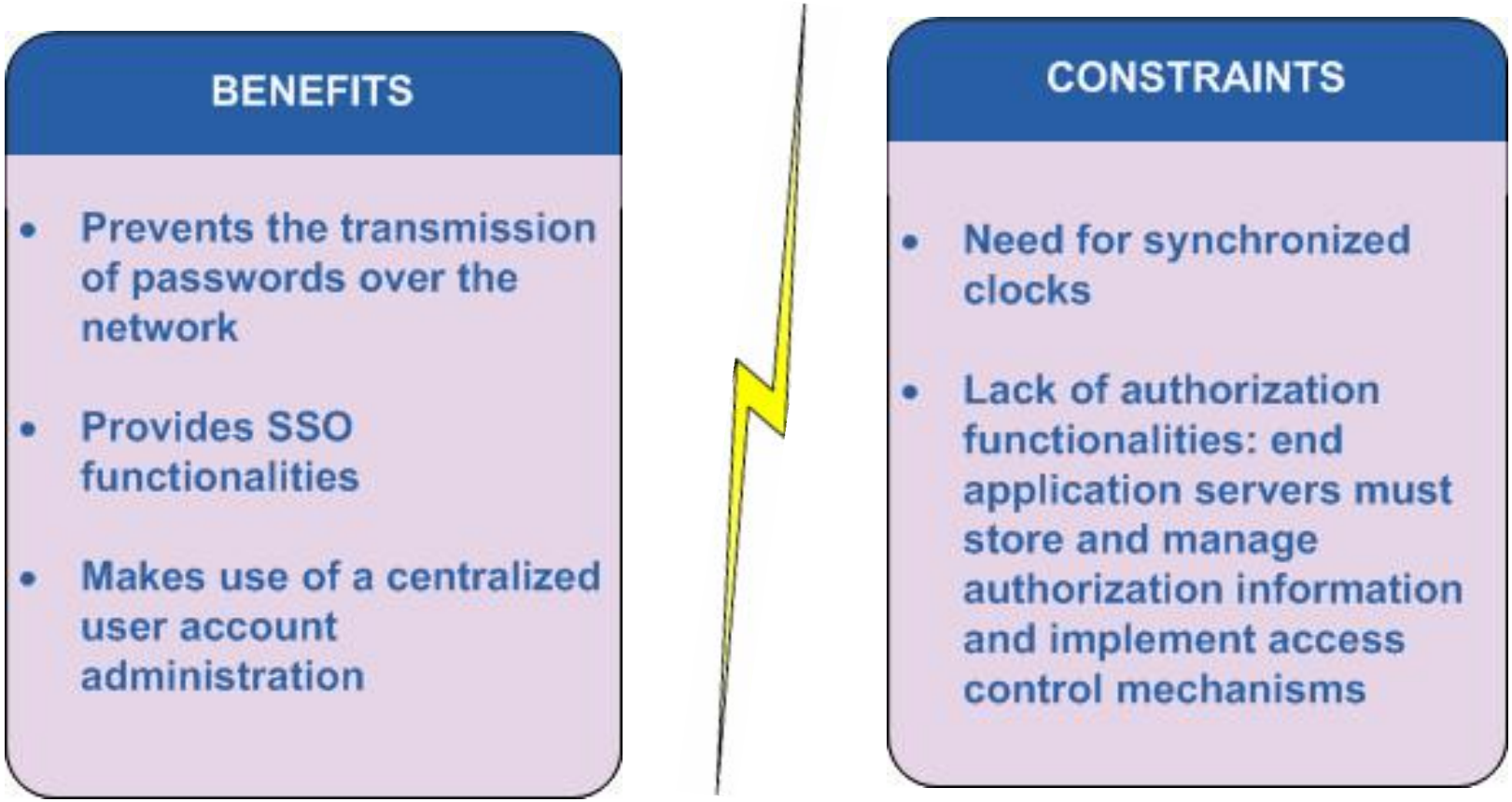
- Security protocol that deals with the two major constraints of the considered environments:
  - Resource limited devices
    - Minimize communication and computation overhead.
  - Dynamic creation of collaborative applications:
    - Centralized authentication and authorization processes.
- Kerberos-based approach:
  - Extension of the protocol with authorization functionalities.
  - Avoid the need for synchronized clocks.

PROPOSED SOLUTION:
Why a Kerberos-Based Approach?

- Kerberos: time-tested, widely-deployed system for authentication and establishment of secure channels.



PROPOSED SOLUTION:
Why a Kerberos-Based Approach?



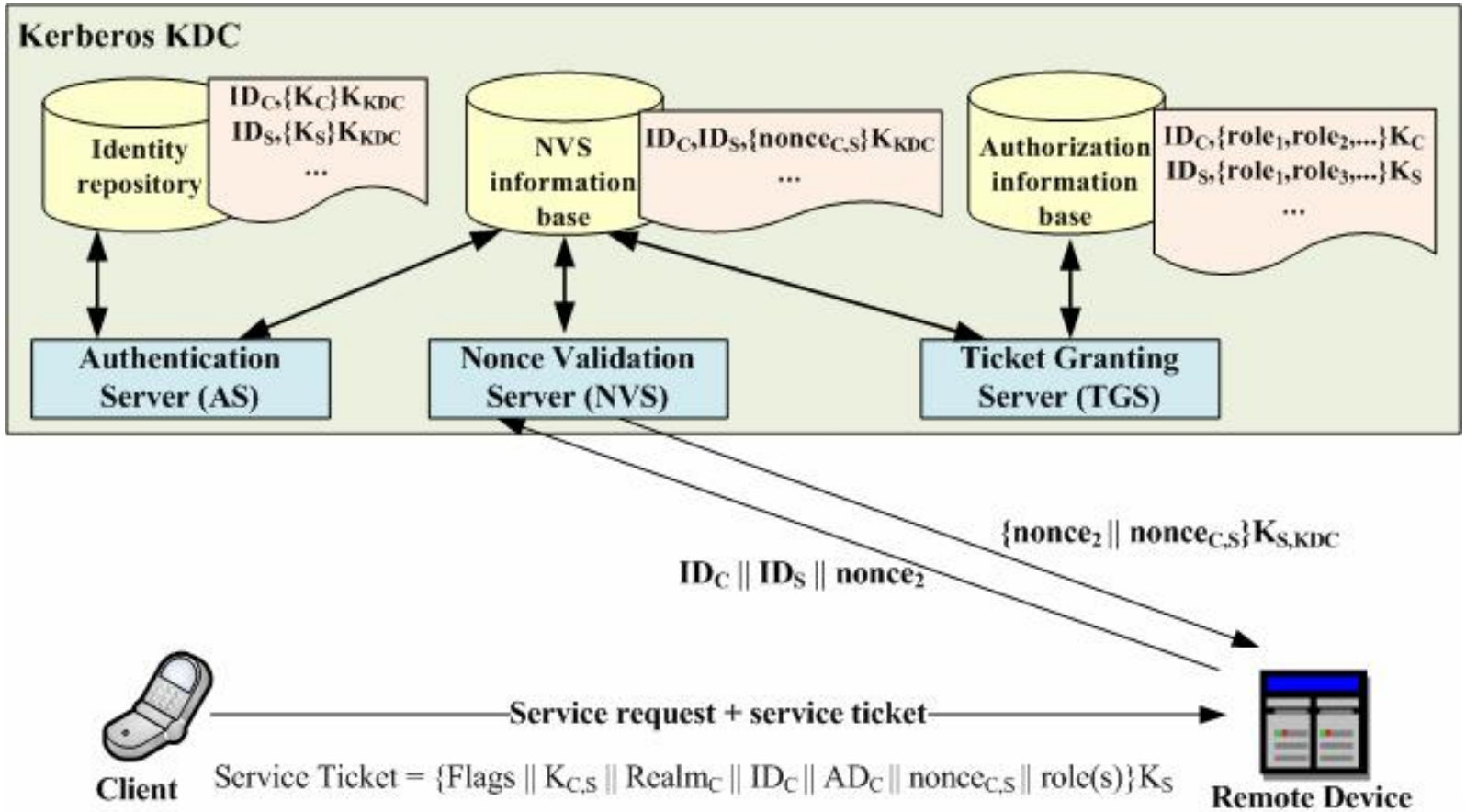
PROPOSED SOLUTION:
Related Work

- Adding authorization support to Kerberos is not a new idea, other protocols have been proposed:
  - SESAME.
  - IDfusion.
  - Proxy-based authorization and accounting.
  - Microsoft's implementation of Kerberos protocol.
- Drawbacks:
  - Use of public key technology.
  - No centralized management of users' privileges.

PROPOSED SOLUTION:
The Time Synchronization Problem

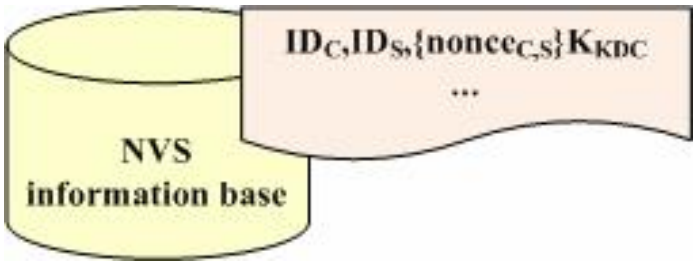
- Kerberos makes use of timestamps:
  - Need for synchronized clocks.
  - Statelessness.
- nonce-based implementation of Kerberos:
  - Stateful, but state information is only maintained in the KDC.
  - Nonce values included in the *authtime* field of Kerberos tickets and protocol messages.
- New Service: NVS (Nonce Validation Service)
  - Located in the Kerberos KDC, along with the AS and the TGS.

PROPOSED SOLUTION:
The Authorization Issue

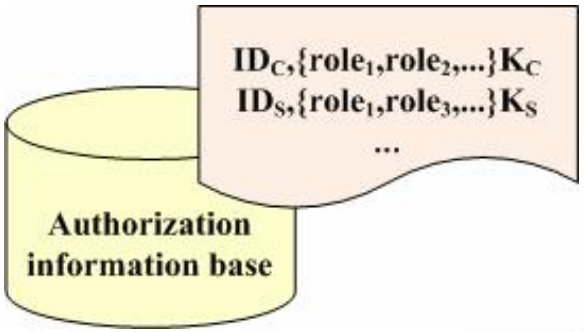


PROPOSED SOLUTION:
Additional Information Stores

- NVS information base
  - Information base in which each entry corresponds to a client and service principal and their associated nonce value.



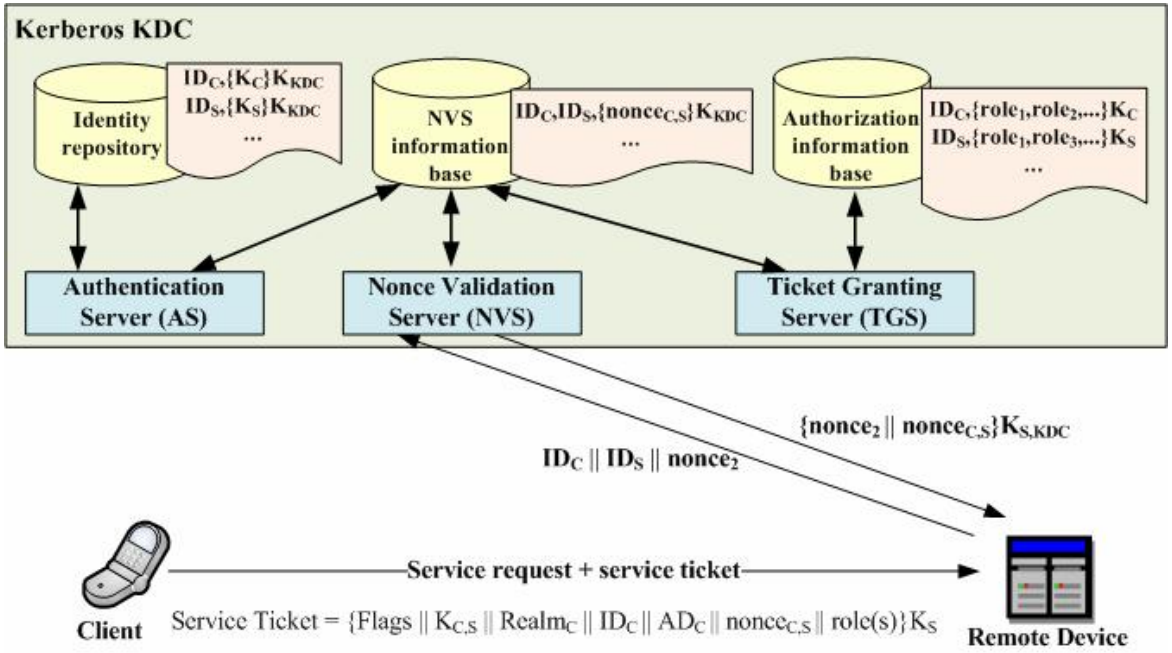
- Authorization solution based on RBAC
  - Entries associating client and service identities with their corresponding roles.



PROPOSED SOLUTION: The Authorization Issue

- The authorization decision is performed by the KDC whenever a client principal requests a Service Ticket.
  - Issues a query to its local authorization information base.
- Only authorized clients are provided with the requested Service Tickets.
  - The authorization payload field contains the identifier of the role undertaken by the client principal.

PROPOSED SOLUTION:
The Service Access Phase



- Validation of Service Tickets:
  - Successful decryption with the service principal's secret key.
  - Nonce validation against the Kerberos KDC.
  - Verification of the existence of a role identifier in the authorization field.

Formal Validation of the Proposed Security Protocol (I)

- AVISPA: Automated Validation of Internet Security Protocols and Applications:
  - Based on HLPSL (High Level Protocol Specification Language).
  - Four different back-ends.
  - Dolev-Yao intruder model.
- Security goals:
  - The security analysis is performed against this goals and the results indicate if the protocol meets them or not.
  - Templates for *authentication* and *secrecy.*

Formal Validation of the Proposed Security Protocol (II)

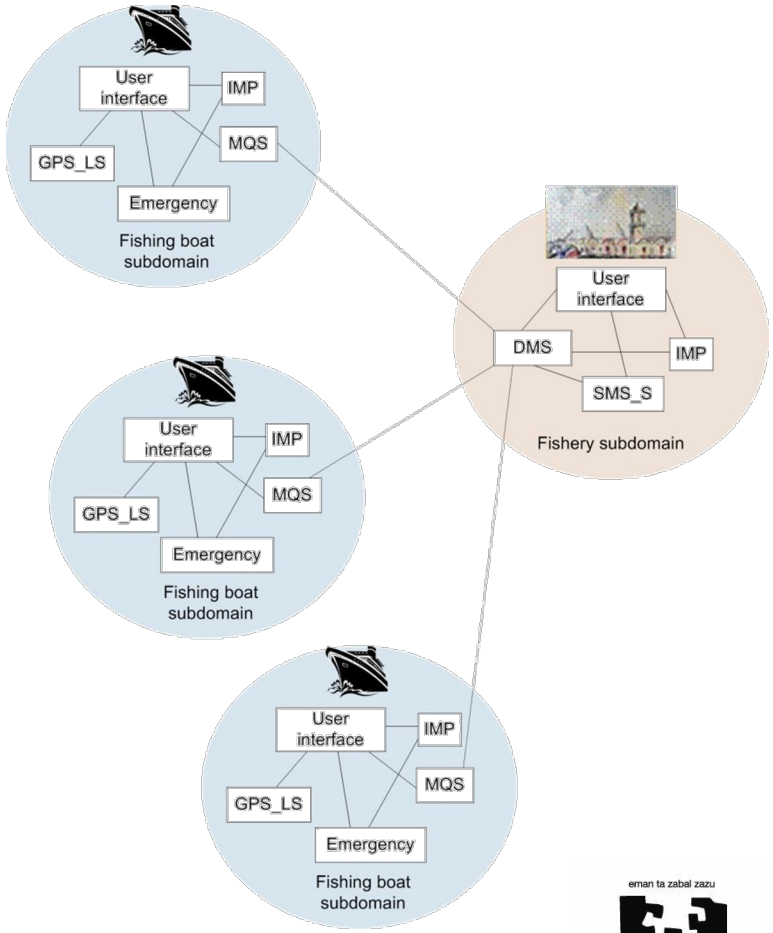
- Security goals defined for our protocol:
  - Authentication.
  - Access Control.
  - Data confidentiality and data integrity.
- Key parameter: initial knowledge of the intruder
  - Different scenarios:
    - Single session and the intruder playing the role of each legitimate agent.
    - Two parallel sessions and in one of them, one legitimate agent playing a role for which it is not intended to.
  - AVISPA reports the protocol to be secure in all cases.

Architecture Deployment in a Real Environment (I)

- C@R, “A Collaborative Platform for Working and Living in Rural Areas”:
  - Promote collaborative environments in rural areas in order to enable their development and permit their integration in the information society.
  - Development of a novel architecture for the composition of collaborative applications.
  - Integration of the introduced security model.
  - Validation based on Living Lab methodology.

Architecture Deployment in a Real Environment (II)

- Cudillero Living Lab:
  - Objective: quality hallmark with origin certificates for hake catches.
  - Fishermen and fishing boats equipped with different types of sensors (location, temperature, humidity, etc).
  - Data access restrictions vary depending on the situation:
    - Everyday work vs emergency.



Conclusions

- Privacy concerns regarding collaborative applications that involve low capacity devices.
- Requirements of a security model tailored to the target environments:
  - Lightweight cryptographic solution.
  - Centralized management of authentication and authorization processes.
- The presented security model:
  - meets above requirements.
  - allows the establishment of trust relationships between the different entities that compose a collaborative application.

THANK YOU FOR YOUR ATTENTION !