SEMPER
Secure Electronic Marketplace for Europe

Project overview

TEN-Telecom Workshop
Brussels, 4 March 1998

Gérard Lacoste, IBM France
Michael Waidner, IBM Research
Project Objectives

Establish an open and generic security architecture for the global marketplace

- Define a model of the marketplace
- Specify an architecture and associated services
- Evaluate the architecture and the services
  - Develop a prototype
  - Run realistic trials
  - Evaluate security and consumer response
- Disseminate the results
  - Publish architecture and specifications
  - Contribute to standardisation efforts
- Exploit project results
1. Project Overview

Service provision
- Otto Versand
- Eurocom
- Fogra
- Maris

Banking
- Europay
- Commerzbank

Telecom operators
- France Télécom
- Intracom
- KPN Research

Social sciences
- Freiburg Univ.

Security engineering
- Cryptomathic
- CWI
- Digicash
- GMD
- IBM
- r³
- SINTEF
- Dortmund Univ.
- Hildesheim Univ.
- Saarbrücken Univ.
Internet Security: Goal

- Secure OS & hardware
- "Global" public-key infrastructure
- Mutual entity authentication
- End-to-end encryption

Internet
Secure Electronic Commerce

- More than Secure Communication
  - Multi-party problems: payments, notarized contract signing, auctioning, copy protection, ...
  - Multi-party security: limited trust in others
  - Processes: Systems must be securely linked, e.g., contract with payment with delivery

- More than electronic payments

- More than just integrity
  - Privacy and anonymity; availability; accountability

- More than just a technical question
  - A lot of open legal questions ...
Model

2. Achievements

- Offers
- Contracts
- Invoices
- Deliveries

- Registration authority
- Certification authority
- Banking gateway
- Fair exchange
- Time stamping
- White board
- Secure archiving

Transfers and fair exchanges of payments, certificates, signed statements

Applications

API

SEMPER

Orders

Contracts

Payments

Receipts

Applications

API

SEMPER
Service Architecture

2. Achievements

- **Commerce Layer**
  - Generic and standard business processes

- **Transfers & fair exchanges**
  - Documents, fair contract signing, certified mail, etc.

- **Payments**
- **Certificates**
- **Statements**

- **Supporting services**
  - Communication, crypto engine, trusted user I/O (TINGUIN), archive, preferences, access control
Service Blocks

2. Achievements

Manager

external interface

internal interface

Module for Service X, Type 1
Adapter
Implementation

Module for Service X, Type n-1
Adapter
Implementation

Module for Service X, Type n
Adapter
Implementation

etc.
3. Future Plans

Positioning of SEMPER

Unique properties:
- symmetric design
- large set of services
- commerce layer
- fair exchanges
- trusted user interface
- dispute handling
- anonymity
- SECA

Support standards:
- Standard formats and protocols: SET, X509, ...
- Message frameworks and protocols: OTP, OBI, ...
- Service frameworks: JavaSoft’s JECF, ...
- Specific and proprietary solutions: IBM, HP, Microsoft, ...

Exploit synergies:
- Service frameworks: JavaSoft’s JECF, ...
- Specific and proprietary solutions: IBM, HP, Microsoft, ...

Support specific modules:
- Service frameworks: JavaSoft’s JECF, ...
- Specific and proprietary solutions: IBM, HP, Microsoft, ...

Support standards:
- Standard formats and protocols: SET, X509, ...
- Message frameworks and protocols: OTP, OBI, ...
- Service frameworks: JavaSoft’s JECF, ...
- Specific and proprietary solutions: IBM, HP, Microsoft, ...

26-Feb-98
3. Future Plans

Internet Bargainer

- Well-defined & automatically verifiable forms
- Set legal context (+ SECA)
- Assisted negotiation of context
- Signed offer / signed order
- Secure delivery / receipt
- Secure payment / receipt

or

Dispute
Conclusions

SEMPER:
Blue-print of the Global Secure Marketplace

- Foundations of secure electronic commerce
- Strategic contributions towards an agreed e.c. framework
- A global, open solution with a European implementation