SEMPER Field Trials and User Evaluation

Dale Whinnett
University of Freiburg, Germany
<dalew@iig.uni-freiburg.de>
Outline

1. Description of Basic/SME Trials
2. Security Services Tested
3. Buyer Reactions
4. Seller Reactions
5. Initial Reactions to Fair Internet Trader (FIT)
Trial Scenarios

Business contexts

- Mail order
- Tele-training
- Literature Service
- Database access
- Image distribution

Players

- Registration authorities
- Sellers
- Buyers
- Banks

Payment

- Credit cards
- SET
- stored value
- Customer accounts
Decision to make supervised *Basic & SME* Trials

**Problems:**

- computing skills of users, i.e. lack of confidence to install & configure a software prototype
- user understanding of security technologies, e.g. types of encryption, key lengths, public key infrastructure
- restricted “real life” opportunities for use
- necessary to explain SEMPER architecture to enable evaluation

**Solutions:**

- supervised interviews with pre-installed software
- additional information regarding security mechanisms provided by interviewer
- SME trial sites offered “live” testing of real sites
- supplementary information used to explain architecture (illustrations, etc.)
Trial Participants

- 80% have used the Internet for more than 2 years
- applications used:
  - WWW 93% daily
  - email 87% daily
  - FTP 57% weekly
- Average duration of trial + interview = 2 hours
  - local software initialised (login, password entry, key generation, registration with CA)
  - creation of 1 or more purses
- visit SEMPER trial site
  - authentication - customer by merchant, merchant by customer
  - transfer of signed statements - offer/order
  - payment - credit card (SET, SSL), generic purse, stored value with user device
  - online delivery of digital goods - offline delivery of hard goods
Secure Transfers & Exchanges

Customer

Certificates

Certificates

Signed Offer

Signed Order

Payment Authorization

Delivery

Registration/Certification Authority

Merchant Server

Payment Gateway

Dale Whinnett, November 1998
Participants & Connections

Customer

Browser

Semper Client

Seller

Server

Semper Server

Network

unprotected communication

local connection

secure communication

CA

Customer Seller

unprotected communication

local connection

secure communication
Phase I Trials

33 Trial Participants

EUROCOM customers

FOGRA customers

Trial Sites

EUROCOM trial site

FOGRA trial site

secure ID, signed offer/order, online delivery, generic purse
Phase II Trials

12 Trial Participants

“power users”
IIG Freiburg

Trial Site

FOGRA trial site

secure ID, signed offer/order, online delivery, generic purse

plus initialisation of software (registration, purse creation)
Phase III - SMEtrial

16 Trial Participants:
Customers of

Otto Versand + SET

Actimedia + credit card data via SSL, encrypted web pages, SET

ACRI + credit card data via SSL, encrypted web pages, SET

OPL + encrypted credit card data via SEMPER; stored value + user device, SET

secure ID, signed offer/order, online delivery, generic purse

plus initialisation of software (registration, purse creation)

plus new forms of payment
Phase III - SMEtrial

10 Trial Participants
invited “testers”
IIG Freiburg

Trial Sites
Otto Versand
Actimedia
ACRI
OPL

trial participants tested all SME trial sites and forms of payment from one computer
User Interface in Basic/SME Trials

A central element of Semper is the Trustworthy INteractive Graphical User Interface, “TINGUIN”.

trusted output

trusted input
### Trustworthy User Interface

<table>
<thead>
<tr>
<th>Connected to</th>
<th>ACTIMEDIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offer</td>
<td></td>
</tr>
<tr>
<td>BACH Suites for violin</td>
<td>250 FF</td>
</tr>
<tr>
<td>BEETHOVEN Trios</td>
<td>400 FF</td>
</tr>
<tr>
<td>BEETHOVEN Piano Sonatas</td>
<td>500 FF</td>
</tr>
<tr>
<td>Price</td>
<td>1150 FF</td>
</tr>
<tr>
<td>VAT tax</td>
<td>50 FF</td>
</tr>
<tr>
<td>Shipping</td>
<td>70 FF</td>
</tr>
<tr>
<td>TOTAL</td>
<td>1270 FF</td>
</tr>
<tr>
<td>Signed</td>
<td>May 25, 1998 14:00</td>
</tr>
</tbody>
</table>

### Classical Music CD Roms - Platform PC

- **BACH Suites for violin**: 250 FF
- **BACH Partitas**: 400 FF
- **BEETHOVEN Trios**: 400 FF
- **BEETHOVEN Piano Sonatas**: 500 FF
- **BEETHOVEN Sonatas**: 700 FF
- **COUPERIN**: 400 FF

### Browser Window

![Browser Window](image-url)
Trial Participant Reactions

- **valued**
  - all security relevant information in one window
  - one “security tool” to manage e-commerce needs
  - clear separation of secure window from insecure browser
  - variety of payment options
  - transaction archive/browser
  - ability to personalise according to individual needs
  - ability to extend with use (e.g. add purses, certificates)

- **criticised**
  - no status bar or symbol in TINGUIN to indicate connectivity
  - too many user confirmations required
  - information in transaction browser difficult to understand
  - no digitally signed receipts
  - not enough information about keys & key storage
  - no certificate browser
User Prerequisites for Electronic Commerce Tool
(questionnaire results)

- Essential in e-commerce tool
  - secure payment (93%)
  - ease of installation and maintenance (85%)
  - data privacy (81%)
  - ease of use (80%)
  - signed offers/orders (76%)
  - encrypted data transfer (73%)
  - choice of payment options (60%)
  - record-keeping (57%)

- Essential changes before willing to use SEMPER
  - legal acceptance of digitally signed evidence (69%)
  - used by broad range of suppliers (64%)
  - secure key storage (60%)
  - electronic receipts (57%)
Services in three trial phases

<table>
<thead>
<tr>
<th>Trial Characteristics</th>
<th>EUR</th>
<th>FOG</th>
<th>FRE Basic</th>
<th>OTV</th>
<th>ACRI</th>
<th>Acti</th>
<th>OPL</th>
<th>FRE SME</th>
</tr>
</thead>
<tbody>
<tr>
<td>secure identification of business partner</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>digitally signed offer</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>digitally signed order</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>generic purse (test payment system)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>digital goods delivered on-line</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>real goods delivered off-line</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>webpages encrypted / sent via SEMPER</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>credit card data transmitted via SSL</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SET payment protocol</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>encrypted credit card data via SEMPER</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>stored value - chipcard and user device</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>real credit card payment</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Seller Reactions

- infrastructure (financial/ legal) to support secure electronic commerce not yet in place
- customer base not yet experienced enough for transition
- future prospects for use good, all required the functionality in the SEMPER architecture, it needs to be exploited and refined
- consumer education essential
- businesses need easy way to create business applications, e.g. “module installer”
Advanced Trials
Fair Internet Trader (FIT)

- negotiation of contract content
- forms with fields
- warning of changes
- negotiation of security settings
- non-repudiation tokens (signed receipts)
- dispute handling (import/export)
- SECA (limiting liability)
Fair Internet Trader (FIT) - initial reactions

(9 demonstrations/interviews)

◆ appreciated similarities to traditional business documents
◆ for businesses signed order is more important than electronic payment
◆ ability to configure to suit different business processes valued
◆ want to be able to forward documents to other departments
◆ means of limiting liability important for private and business use
“The advantage of SEMPER is that the existing tools are incorporated into one tool that I can use for doing business. Its possible to assign meaningful roles to the various tools. I can say here is a databank, with goods and offers in it, and I can abstract an offer from it, digitally sign it and send it over as a container and that’s much more than just PGP and RSA and emails.”

“It is the only software I’ve seen which organises all the relevant issues in electronic commerce.”