TECHNISCHE UNIVERSITÄT MÜNCHEN

Security Modelling for Electronic Commerce: The Common Electronic Purse Specifications

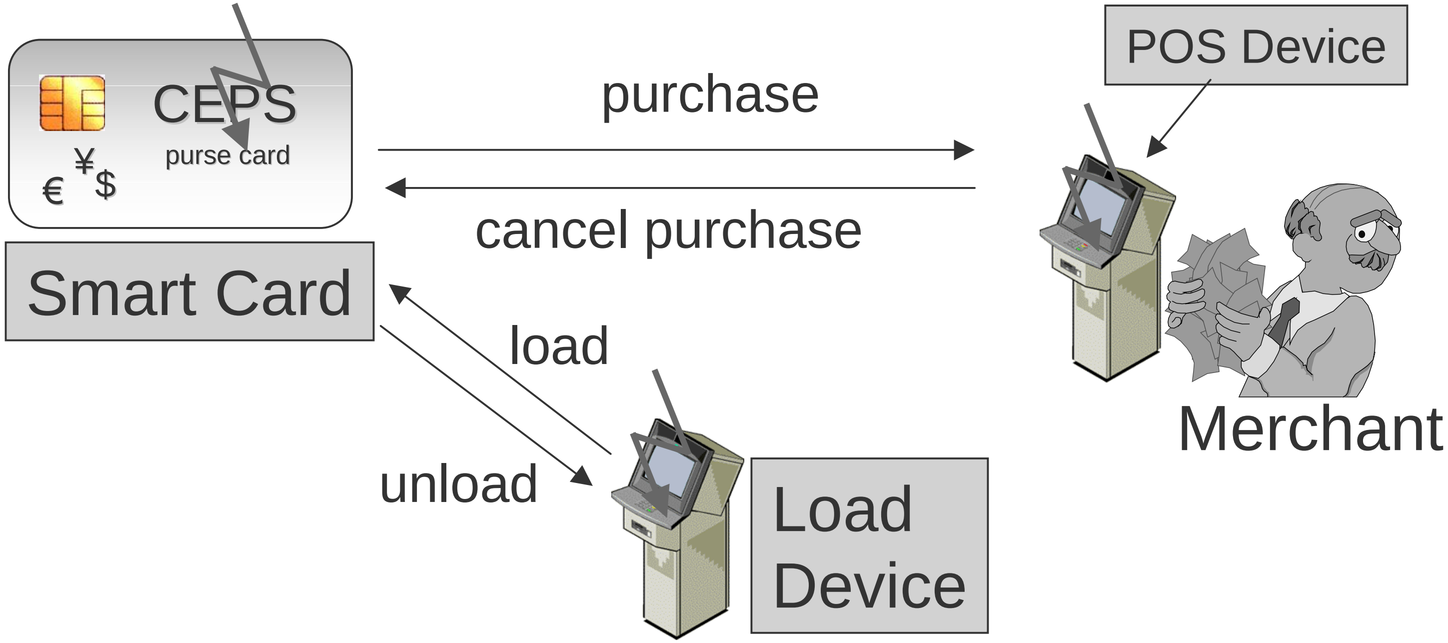
Guido Wimmel
Software & Systems Engineering
Technische Universität München

(with Jan Jürjens, University of Oxford)

Overview

- E-Commerce and Security
- AutoFocus
- Formal Model of Electronic Purse System
- Verification of the Protocol
- Conclusions / Further work

Electronic Purse Systems



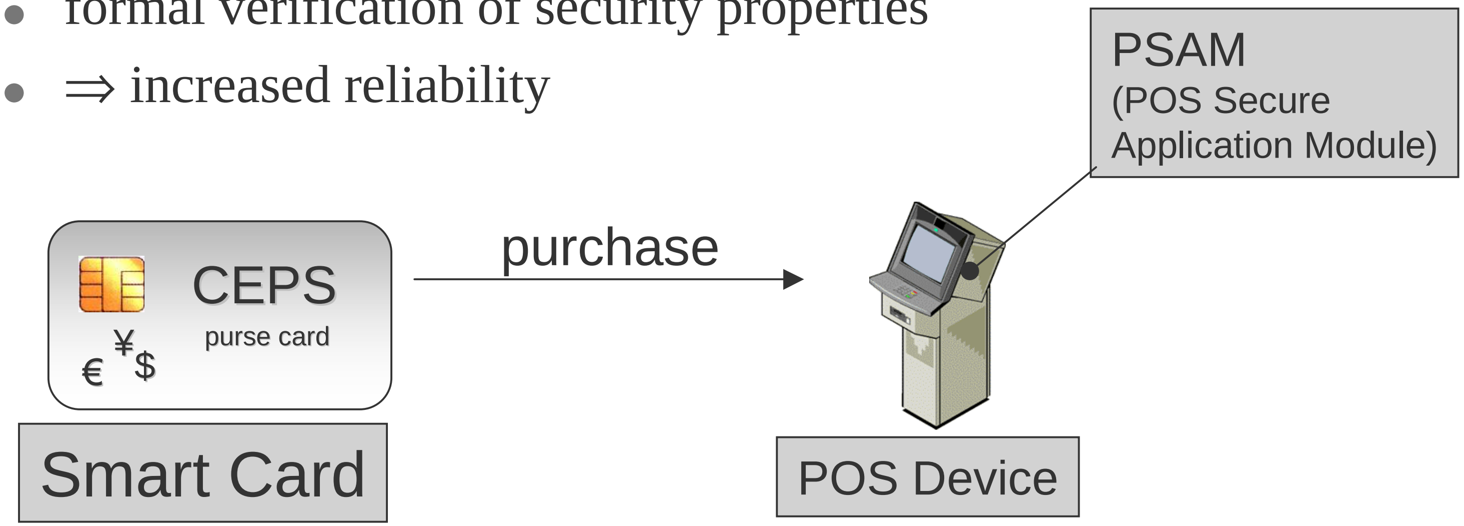
- ... will become globally interoperable (CEPS standard)
- ... are complex distributed e-commerce applications
- ... are highly security critical

Security Engineering

- Integration of security aspects into development process
  - Supports specification, design and implementation of secure e-commerce systems
- Characteristics of security critical systems:
  - Possible attacks (threats) against assets
  - Security objectives to protect assets
  - Security functions to prevent attacks
  - Security depends critically on assumptions about environment
- Support for security in the development process
  - Consider security issues at each step of development
  - Integrate security requirements and assumptions into system models
  - Use formal methods for maximum confidence

CEPS Case Study

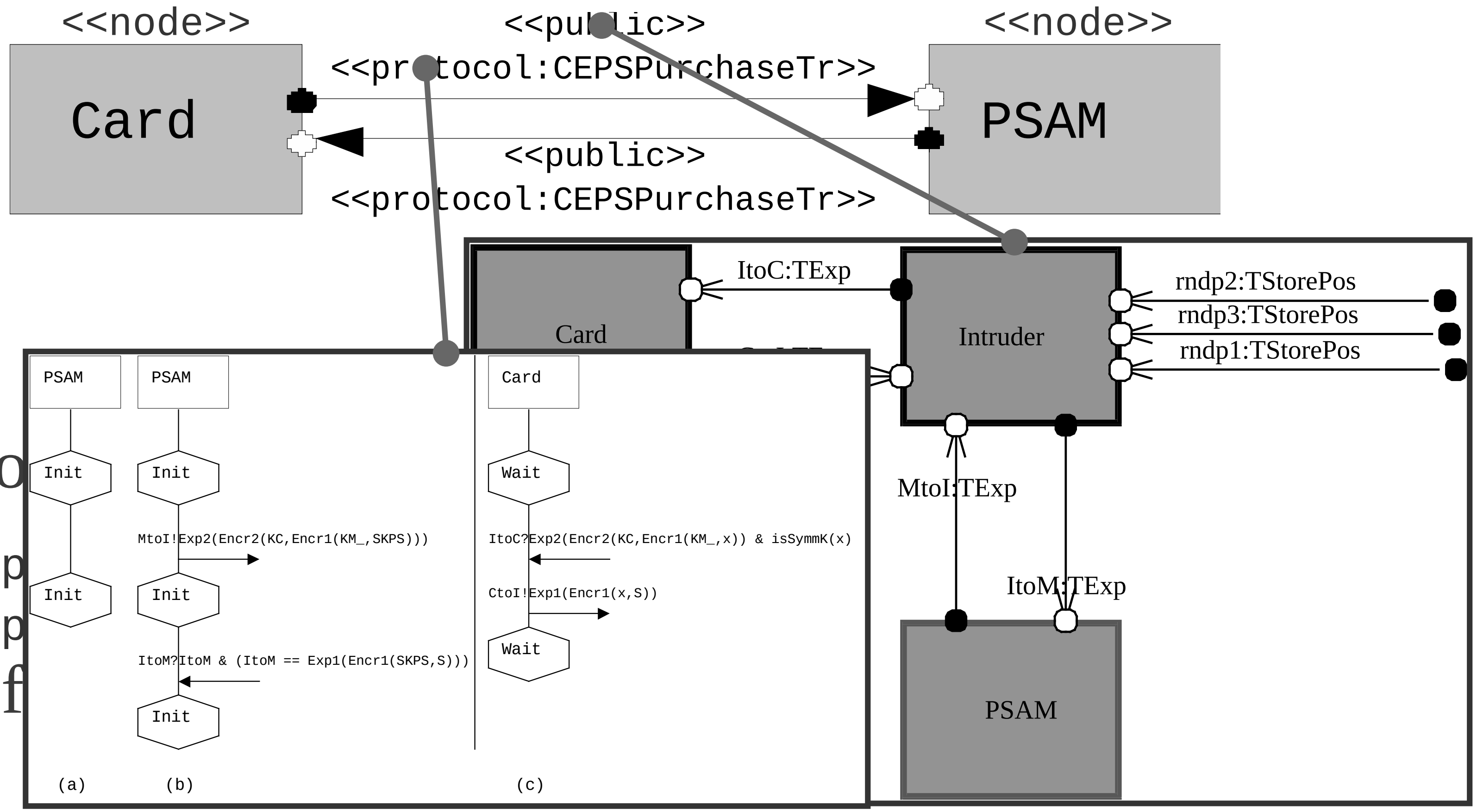
- Formal Modelling of CEPS Purchase Transaction
  - with the general-purpose formal CASE tool AutoFocus
  - using intuitive, standard graphical models
  - formal, precise specification avoids ambiguities and enables verification
  - integrated security analysis through extended description techniques
  - formal verification of security properties
  - ⇒ increased reliability



AutoFocus

- CASE tool, based on formal background (FOCUS)
- Graphical, view oriented modelling
  - System Structure Diagrams
  - State Transition Diagrams
  - Message Sequence Charts
  - Data Type Definitions
- Views related to UML-RT, support hierarchy
- Features:
  - Simulation
  - Validation (Consistency, Testing, Model Checking)
  - Code Generation (e.g. Java, C)

CEPS System Structure

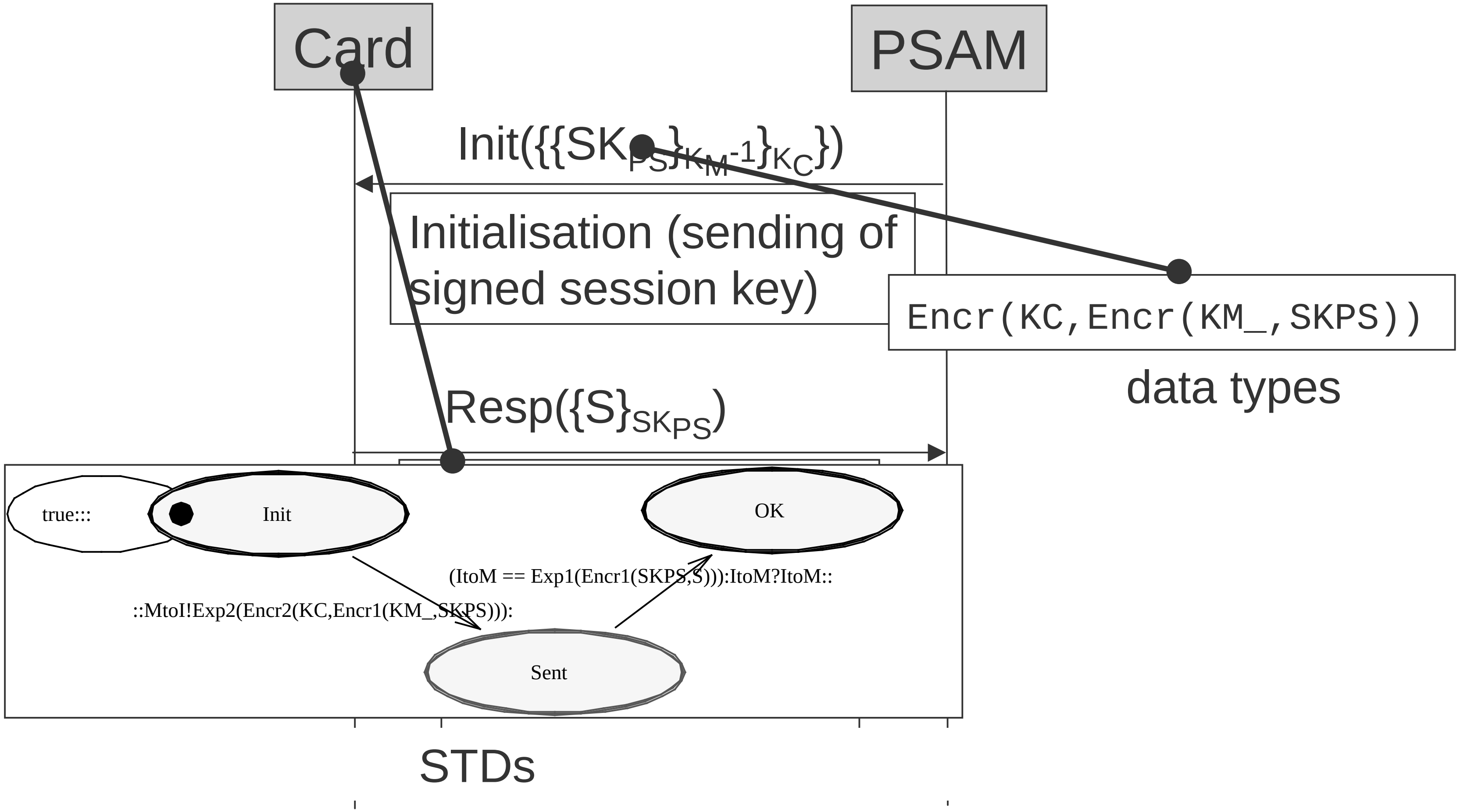


Protocol Specification

Threat model

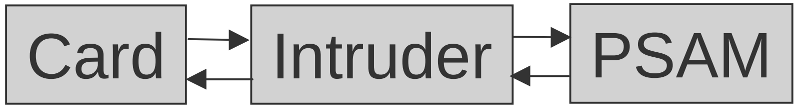
- Co…
  - <<p…
  - <<p…
    ref…

The CEPS Purchase Protocol

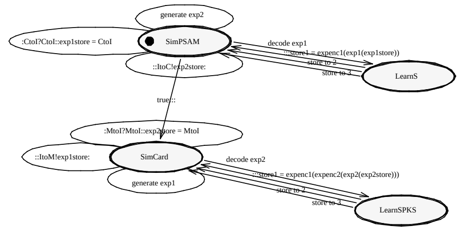


Intruder Model

- **Intruder** component models possible threats

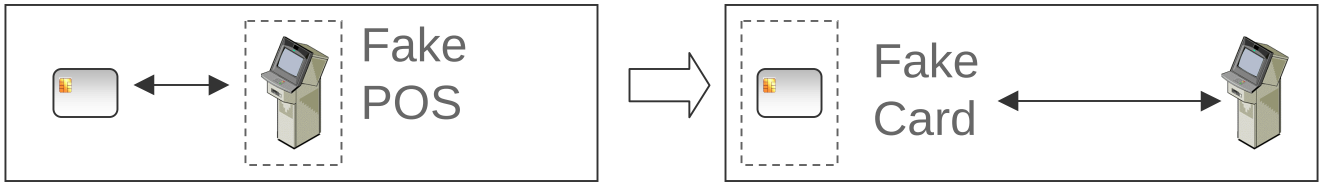


- Specified as an STD
  - Intercept and forward messages
  - Learn secrets
  - Generate own messages or replay messages

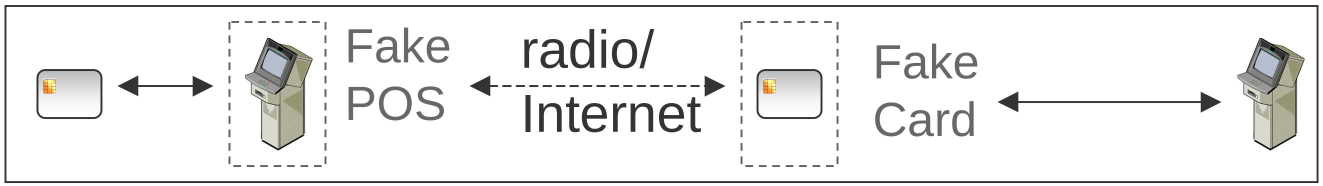


- Two scenarios: (variations of STD)

1.



2.

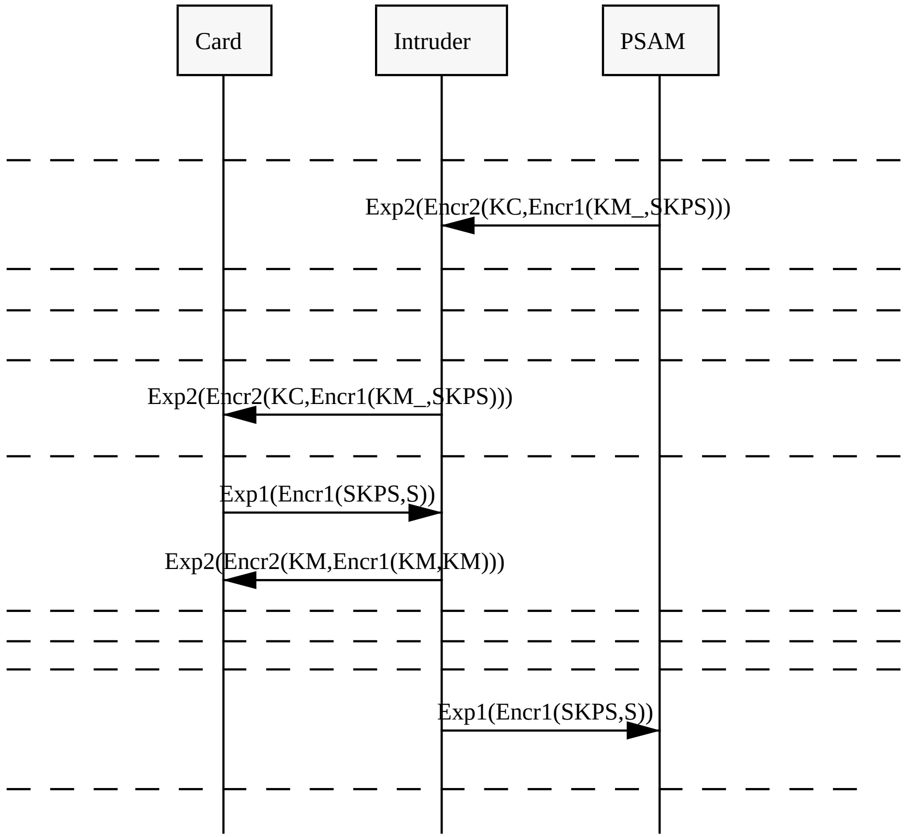


Analysis

- Security Objective:
  - Transactions must not be completed in presence of Intruder
- Verification using Model Checking
  - Property to check: AG $\neg$(PSAM.State = OK)
  - Performance: approx. 5 minutes to automatically verify all possible behaviours
- Results:
  - No attacks found for scenario 1 (Card$\leftrightarrow$Intruder; Intruder$\leftrightarrow$PSAM) except intruder knows ***both*** private keys
  - *No full proof*, because of abstractions in the model
  - In scenario 2 (Card$\leftrightarrow$Intruder $\leftrightarrow$ PSAM), objective can be violated
  - Computed attack trace shows simple middleperson attack

MSC for Attack Trace

- MSC shows violation
- Here, intruder acts as relay (middleperson attack)
- Only possible attack in the model, also considering cryptography
- Important when Internet is involved
- Shows significance of modelling assumptions



Conclusion

- General formal framework for specification and validation of security critical systems
- CEPS purchase transaction model in AutoFocus
  - System structure
  - Threat model and assumptions
  - Protocol behaviour
  - Security objectives
- Verification using formal techniques indicates vulnerabilities
  - E.g. insecure connection between POS-device and card enables attack
  - Guidelines necessary to find verifiable abstraction of system
- Integration of security analysis and design for e-commerce systems
  - Explicit statement of assumptions and objectives $\Rightarrow$ find errors early
  - Forces developer to consider protocols in context of the general system
- Future research directions: extend modelling possibilities for security aspects; extend tool support for verification and validation/testing