

Modelling and Verification of Layered Security Protocols: A Bank Application

Johannes Grünbauer,

Jan Jürjens, Guido Wimmel

Helia Hollmann

Software & Systems Engineering
Informatics, TU Munich
Germany

secaron AG
Munich

A Need for Security

Society and economies rely on **computer networks** for communication, finance, energy distribution, transportation...

Attacks threaten **economical** and **physical** integrity of people and organizations.

Interconnected systems can be attacked **anonymously** and from a safe **distance**.

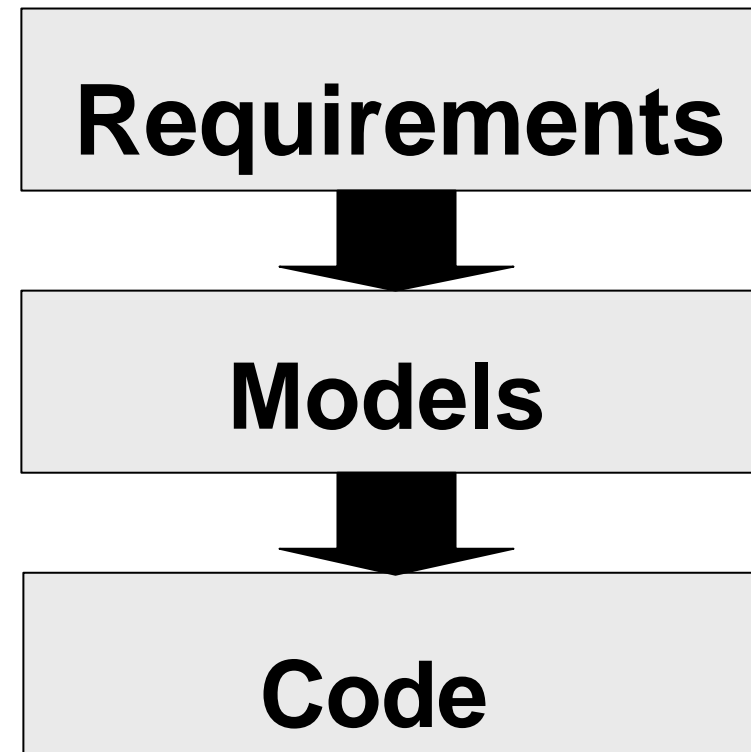
Networked computers need to be **secure**.

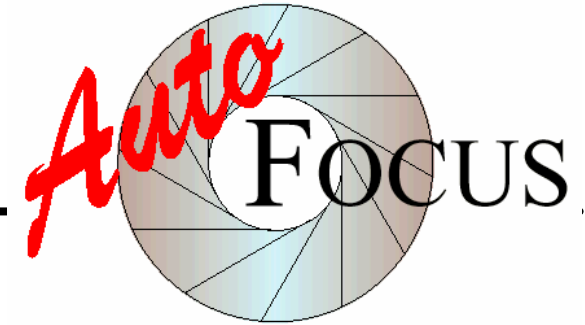
Need **secure software engineering**.

Model-based Development

Goal: ease **transition**
from human **ideas** to
executed **systems**.

Increase **quality** with
bounded **time-to-**
market and **cost**.





CASE-Tool with formal basis

Graphical, **view oriented** modelling (UML-like).

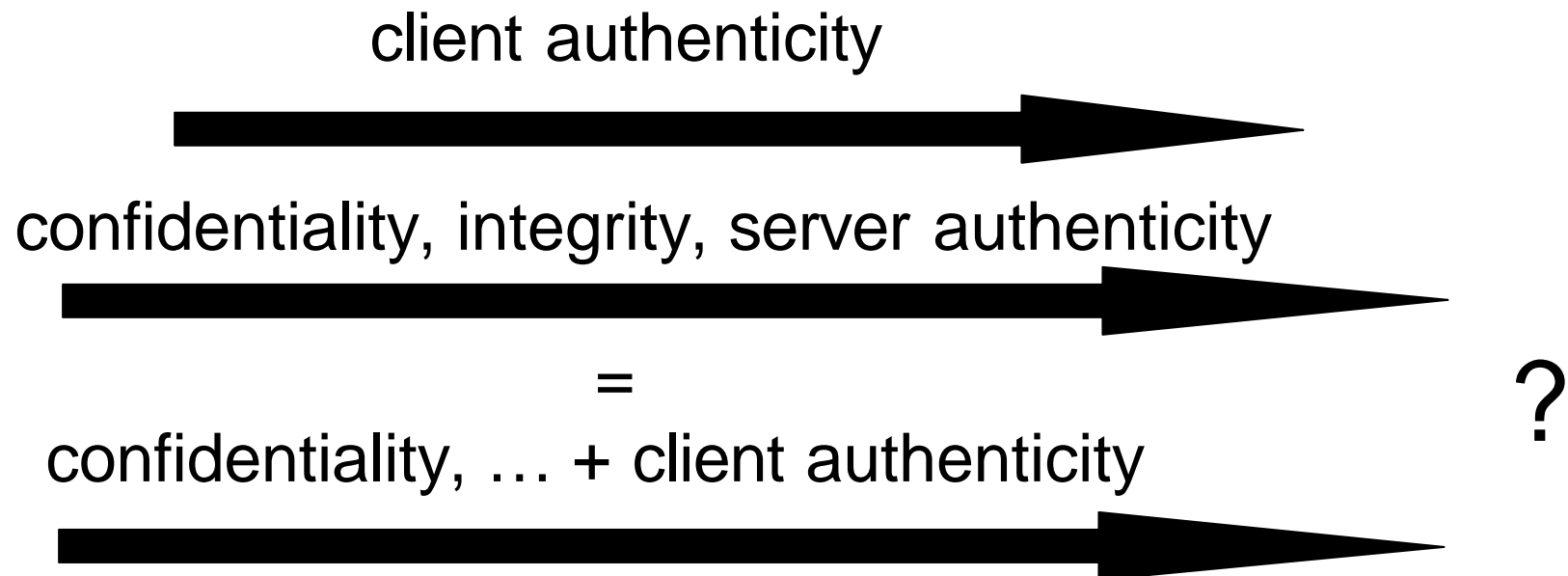
- System Structure Diagrams.
- State Transition Diagrams.
- Message Sequence Diagrams.
- Data Type Definitions.

Features:

- Simulation.
- Validation (Consistency, Testing, Model Checking).
- Code generation (e.g. Java, C).

Layered Security Protocols

- Protocol on **higher layer** uses services of protocol on **lower layer**.
- Big question: **security properties additive** ?
- Desirable: **secure channel abstraction**.



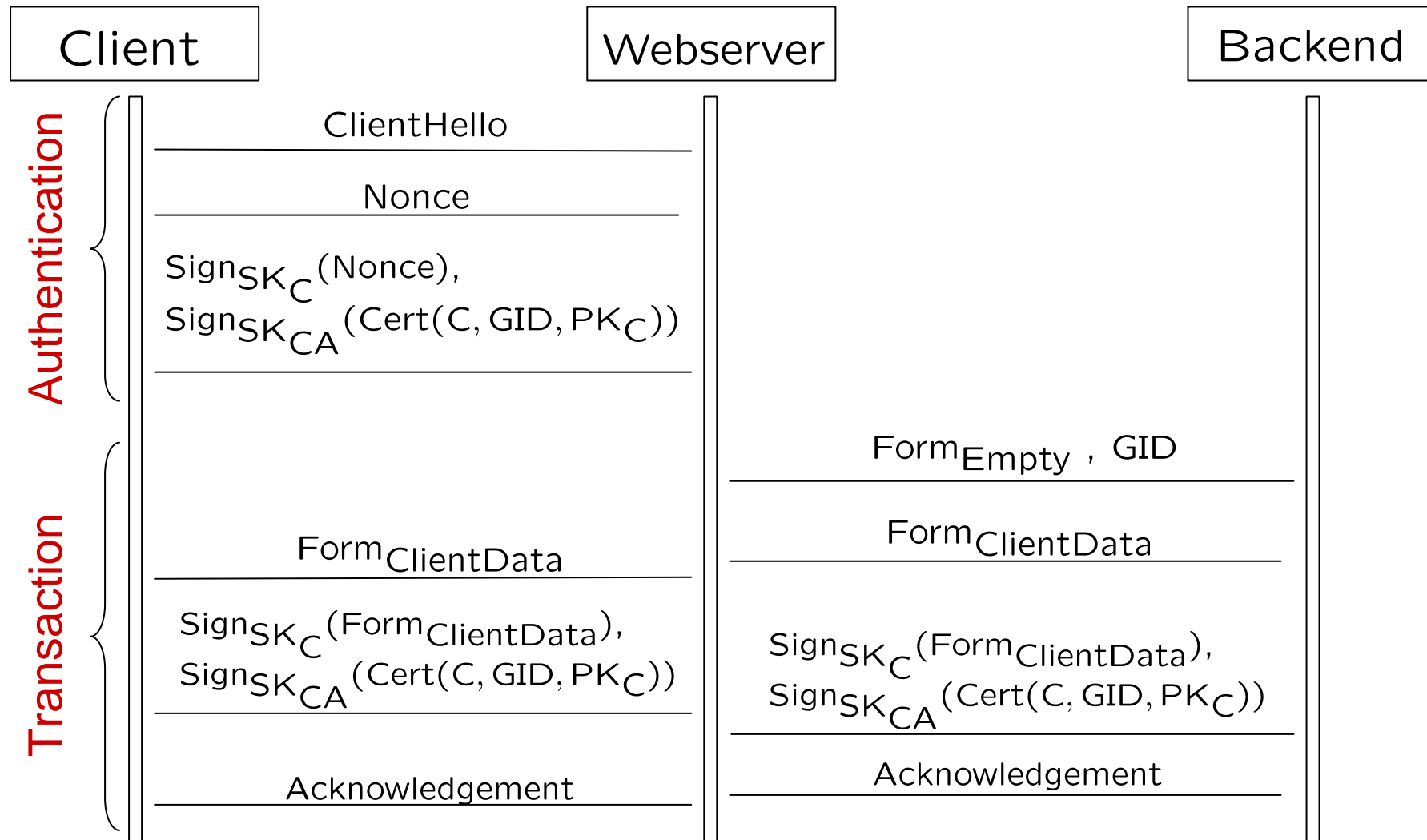
Here: Bank application

- **Security analysis** of web-based banking application, to be put to commercial use (clients **fill out** and **sign** digital order forms).
- In cooperation with major German bank.
- Layered security protocol
 - first layer: SSL protocol.
 - second layer: client authentication protocol
- Main security requirements:
 - personal data **confidential**.
 - orders not submitted in name of others.

The Application II

- **Two layer** architecture.
- When user logs on, an SSL-connection is established (first layer).
 - Provides **secrecy, integrity, server authentication** but no **client authentication** (this version).
- Custom-made protocol on top of SSL for **client authentication**.
- Session key generated by SSL used to encrypt messages on second layer.

Authentication protocol



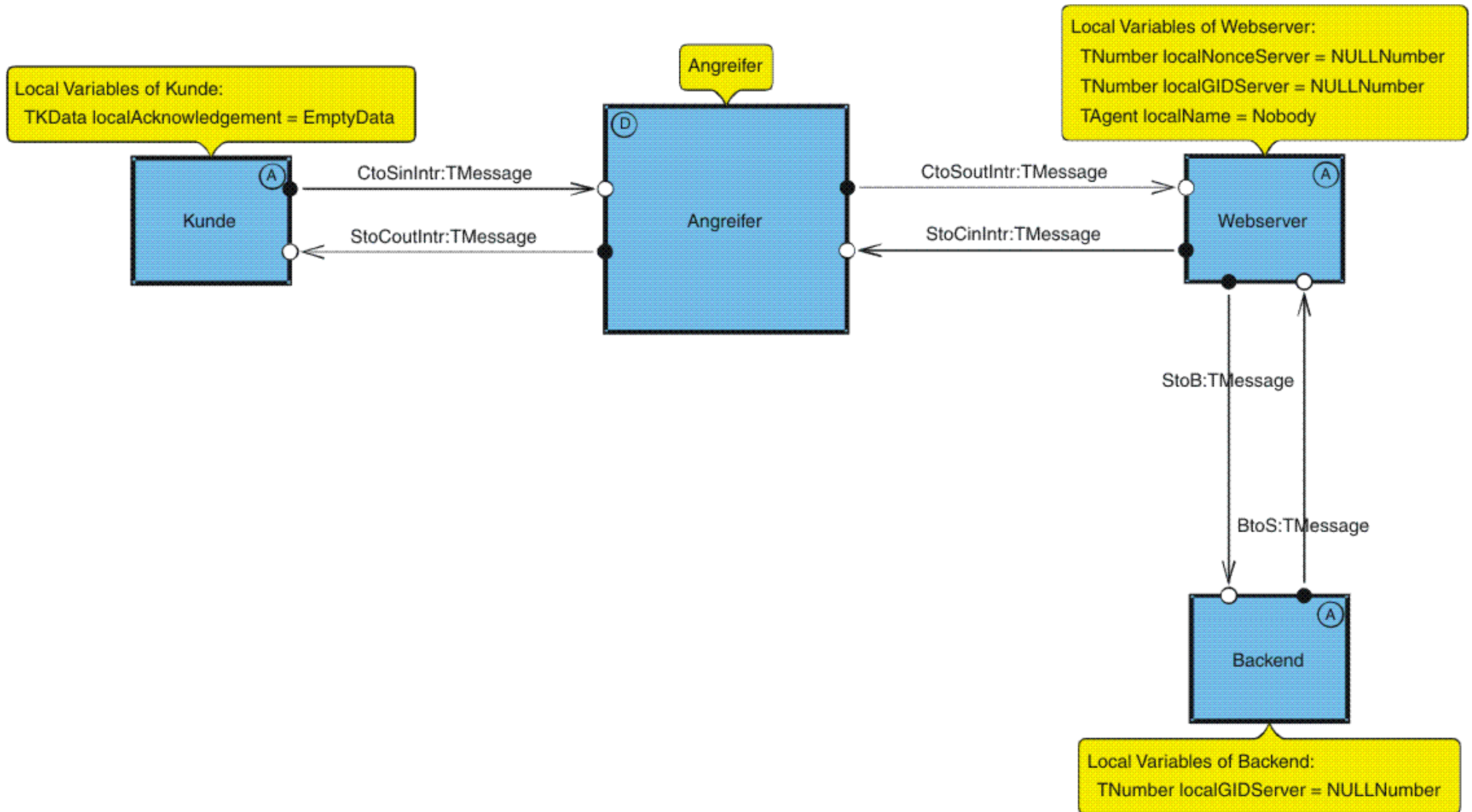
Generic Adversary (Dolev-Yao)

- May know some data in advance (but not private keys etc.).
- Can **read, modify, split, recombine, insert and delete** messages.
- Not able to **derive private key** from public key.
- Can only **read** encrypted messages with the **corresponding** key.
- Cannot break encryption, **fake signatures** etc.
- Cannot perform **statistical attacks**.

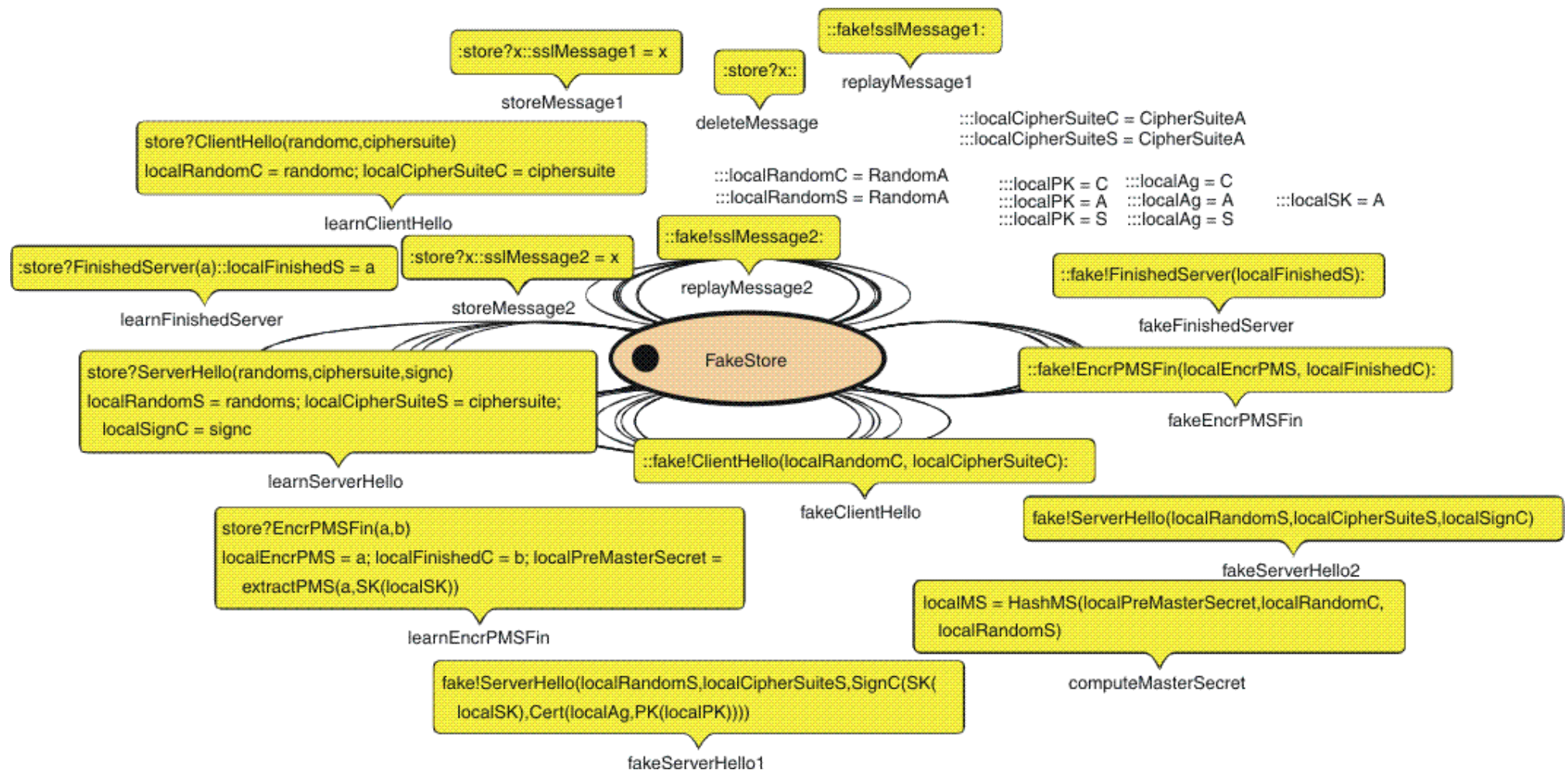
Layered Security Protocol

- Adjust adversary model to account for SSL security properties.
- Justify that specialised adversary model wrt. top-level protocol is as powerful as generic adversary wrt. protocol composition.
- Verify top-level protocol wrt. specialised adversary.
- Implies verification of protocol composition.

SSD Overview



Part of generated adversary model



Verification of the Auth. protocol 1

- Authentication:
 - It's not possible for the adversary to authenticate under a wrong identity against the web server.
 - $\neg(\mathbf{E}(\neg\text{Client in state } \textit{SentNonceCert} \mathbf{U} (\textit{Webserver in state } \textit{GotSignedNonce} \wedge \textit{nonce was signed Client}))))$
 - Used time: approx. 2 hours 40 minutes.

Verification of the Auth. protocol 2

- Transaction:

- It's not possible for the adversary to get the confidential client's data.

AG $((FakeStore \text{ doesn't get the GID}) \wedge$
 $(FakeStore \text{ doesn't get the Client's data}) \wedge$
 $(FakeStore \text{ doesn't get the acknowledgement}))$

- Used time: approx. 2 hours 50 minutes.

Conclusion & Future work

Protocol layering indeed additive wrt.
security properties in this particular case.

Future work: Generalize to classes of
protocols and security.

Some resources

Book: Jan Jürjens, Secure Systems Development with UML, Springer-Verlag, due 2003

Tutorials: Sept: FORTE (Berlin); Oct: GI Sicherheitstagung (Frankfurt), ASE (Montreal), SNDP (Lübeck), LADC (Sao Paulo); Nov: WWW/Internet (Algarve), FMOODS (Paris), ICSTEST-E (Bilbao) ...

Special SoSyM issue on Critical Systems Development with UML

CSDUML'03 @ UML'03 conference (Oct. in SFO)

More information (slides, tool etc.):
<http://www4.in.tum.de/~juerjens>

