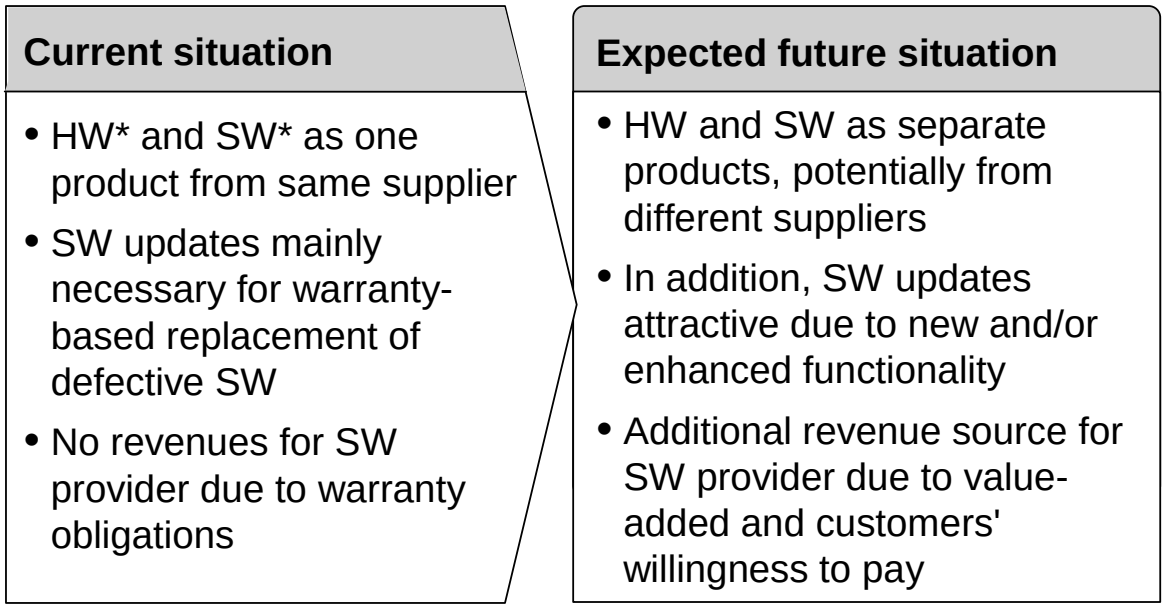
Secure Software Delivery and Installation in Embedded Systems

André Adelsbach, Ulrich Huber, Ahmad-Reza Sadeghi
Horst-Görtz-Institute, Bochum, Germany

ISPEC 2005 Presentation
Singapore, April 13, 2005

HW* and SW* will become separate products within an embedded system, thus providing an additional revenue source to SW providers

CHANGES IN THE ROLE OF SW IN AN EMBEDDED SYSTEM



* HW: hardware, SW: software

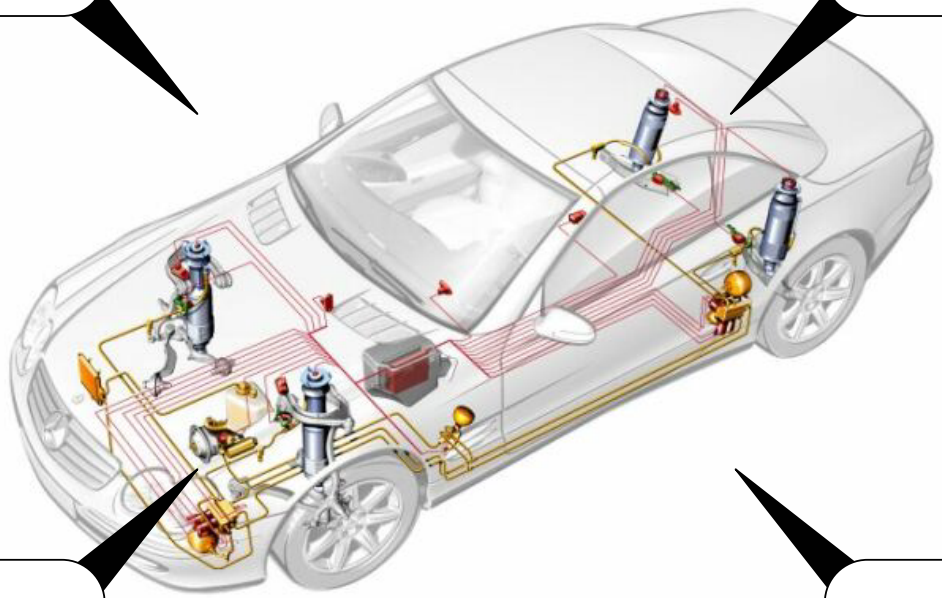
Source: Technical Report "Secure Software Delivery and Installation in Embedded Systems", http://www.prosec.rub.de/

There are four major difficulties when a provider installs a SW update in a vehicle

DIFFICULTIES WITH SW UPDATES IN A VEHICLE

Service provider needs specific equipment, e.g., diagnostic tester, and skills

Service providers have different skill sets



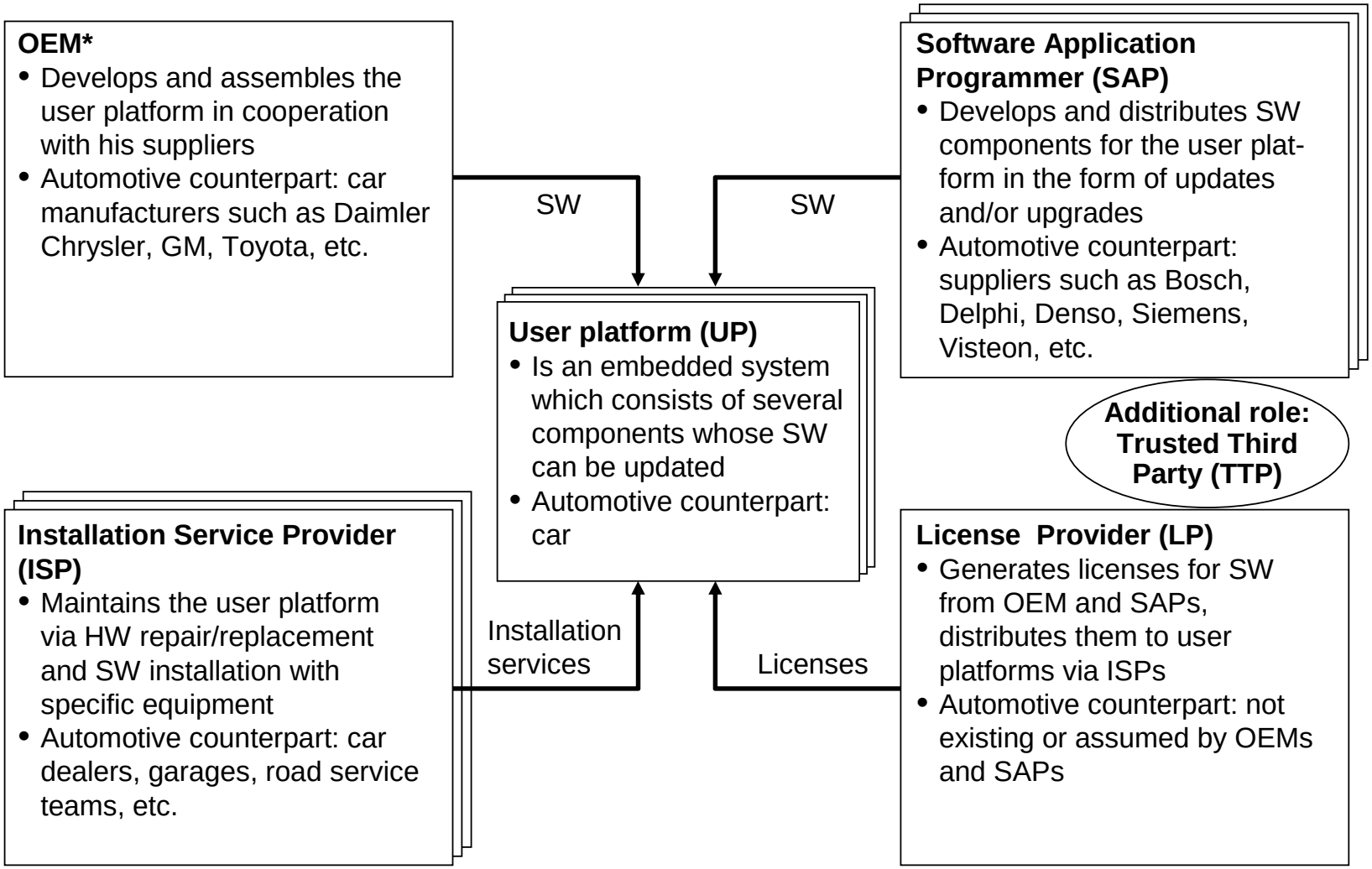
Compatibility among SW components is not self-evident due to number of ECUs

High economic value of vehicle and failure consequences induce tough requirements

Source: Technical Report "Secure Software Delivery and Installation in Embedded Systems", http://www.prosec.rub.de/

The system model contains five different roles which correspond with current players in the automotive industry

ROLES IN THE SYSTEM MODEL AND THEIR COUNTERPARTS IN THE AUTOMOTIVE INDUSTRY



* Overall Equipment Manufacturer

Source: Technical Report "Secure Software Delivery and Installation in Embedded Systems", http://www.prosec.rub.de/

There are many scenarios which lead to damage to an innocent party, four of which we detail

FOUR EXEMPLARY SCENARIOS LEADING TO DAMAGE TO INNOCENT PARTIES

EXAMPLES

1 SW is not authentic

- An honest garage installs a supposedly correct SW component for the ABS
- The adversary has replaced the SW component with a defective one
- The car fails, leading to an accident

2 ISP* is not qualified

- An unqualified garage installs SW for the airbags
- Due to wrong parameterization, the airbags do not trigger off properly
- The victim sues the OEM*

3 Innocent ISP is accused

- A SW component has a known error which might lead to a short circuit and set fire
- A malicious car owner burns his car and accuses his innocent garage of having installed the SW component

4 SAP* is discriminated

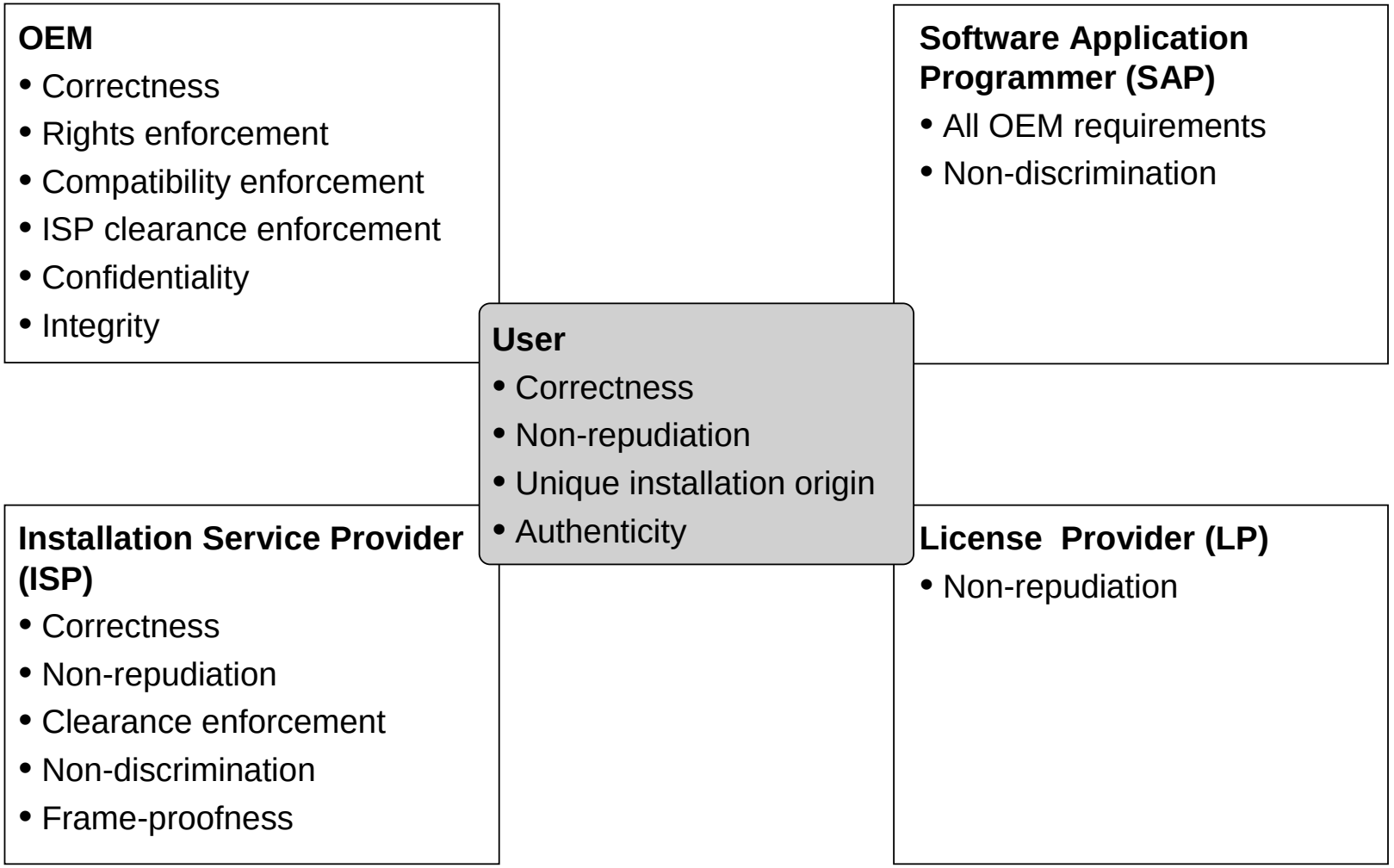
- An honest SAP develops a SW component
- The OEM has a SW component with identical functionality, but higher price
- The OEM configures each car such that only his SW can be installed

* ISP: Installation Service Provider, OEM: Overall Equipment Manufacturer, SAP: Software Application Programmer

Source: Technical Report "Secure Software Delivery and Installation in Embedded Systems", http://www.prosec.rub.de/

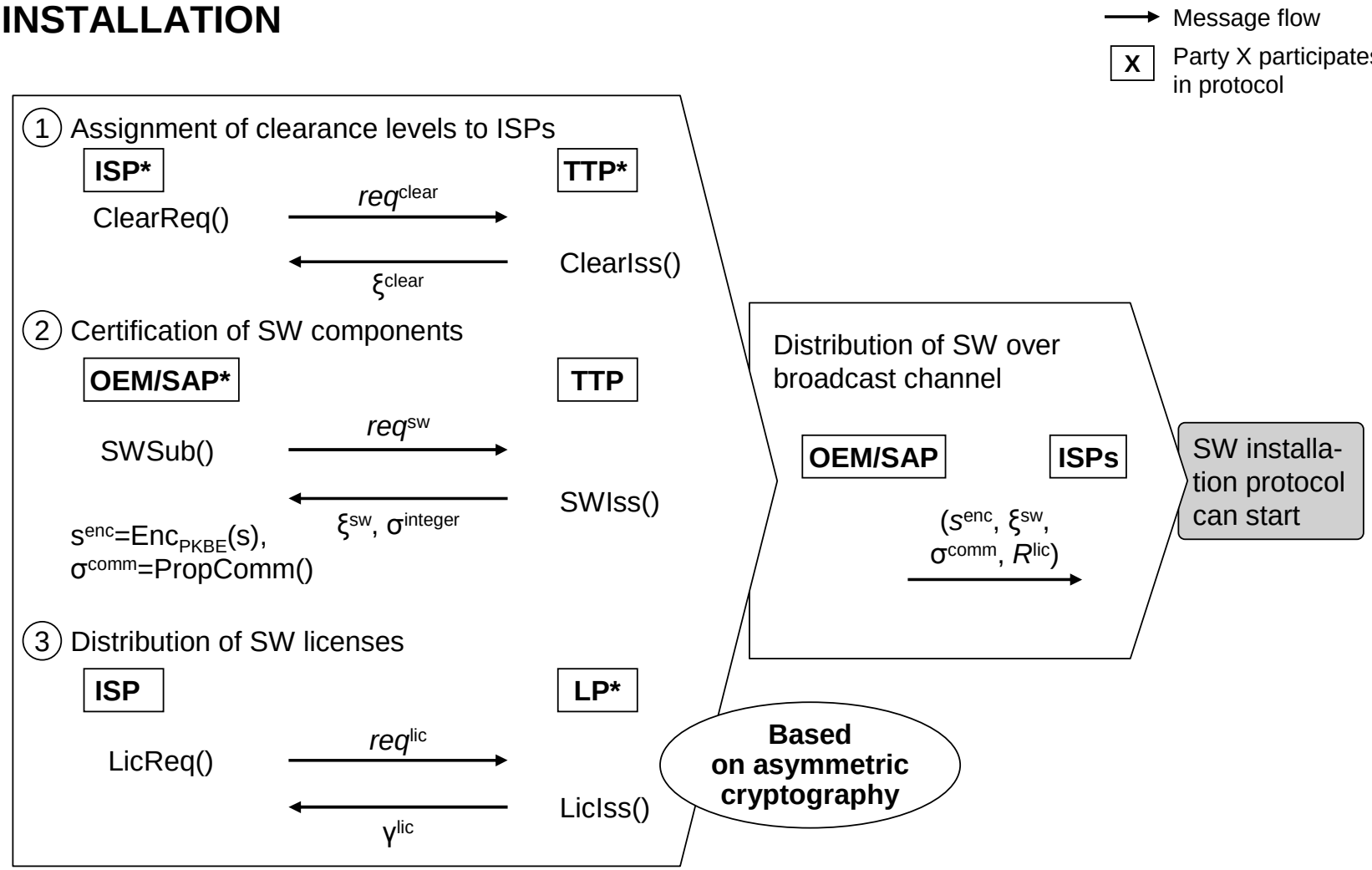
Each role in the system model has specific requirements regarding any software installation

REQUIREMENTS OF ALL ROLES IN THE SYSTEM MODEL



Three basic protocols are a prerequisite of any SW installation

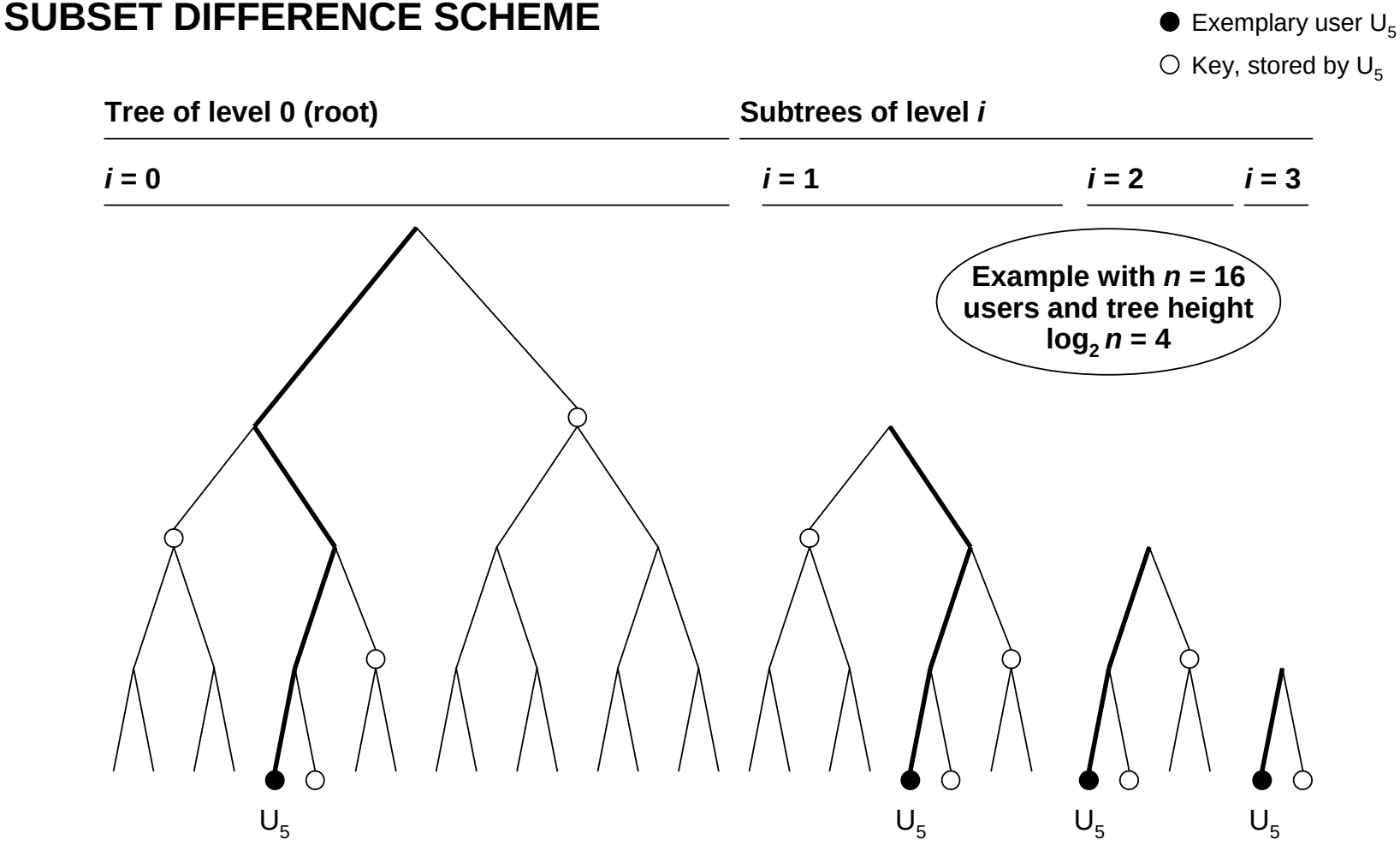
SYSTEM SETUP – THREE BASIC PROTOCOLS PRECEDING ANY SW INSTALLATION



* ISP: Installation Service Provider, TTP: Trusted Third Party, SAP: Software Application Programmer, LP: License Provider

In the SD scheme, each receiver obtains the keys just off his key path within each subtree

BROADCAST ENCRYPTION: KEYS OF AN EXEMPLARY USER IN THE SUBSET DIFFERENCE SCHEME



Source: The LSD Broadcast Encryption Scheme, CRYPTO 2002, LNCS 2442, pp. 47 - 60

Compared to SD*, the basic LSD scheme significantly reduces the storage requirements of the users by slightly increasing the message header length**

COMPARISON OF SD* AND BASIC LSD** PERFORMANCE PARAMETERS

Main difference

n Number of users

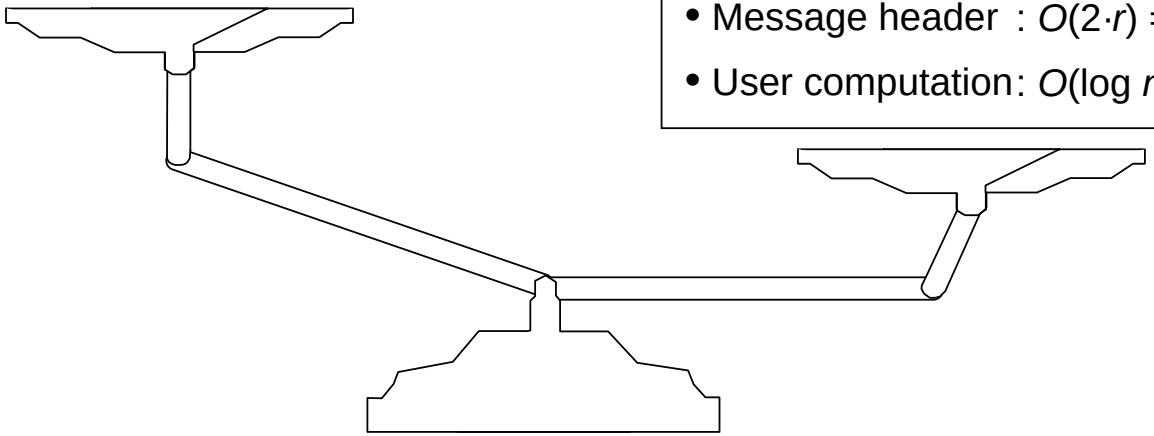
r Number of revoked users

SD

- User storage : $O(\log^2 n)$
  - Example : 406 keys for 2^{28} users
- Message header : $O(r)$
- User computation : $O(\log n)$

Basic LSD

- User storage : $O(\log^{3/2} n)$
  - Example : 146 keys for 2^{28} users
- Message header : $O(2 \cdot r) = O(r)$
- User computation : $O(\log n)$



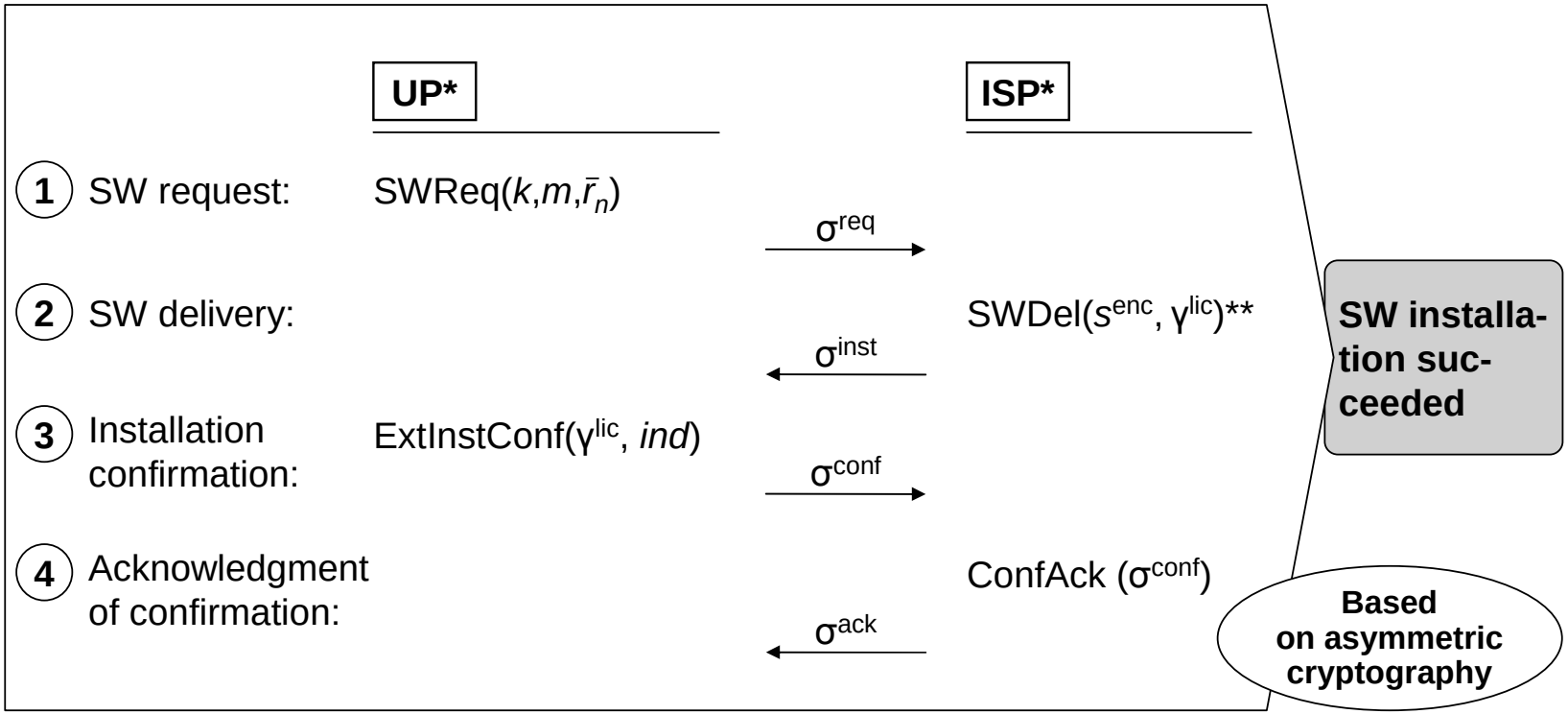
* Subset difference

** Layered subset difference, not lysergic acid diethylamide

Source: The LSD Broadcast Encryption Scheme, CRYPTO 2002, LNCS 2442, pp. 47 - 60

A SW installation consists of four basic steps

FOUR STEPS OF A SW INSTALLATION



* UP: User Platform, ISP: Installation Service Provider

** In order to execute SWDel(), the ISP must have executed LicReq() and received γ^{lic}

Source: Technical Report "Secure Software Delivery and Installation in Embedded Systems", http://www.prosec.rub.de/

In each step of a SW installation, the party in charge verifies several necessary conditions

NECESSARY CONDITIONS FOR EACH SW INSTALLATION STEP (1/2)

Main criteria

(1) Conditions for a user platform to issue a SW request

- User platform and SW are compatible
- ISP* has sufficient clearance level
- All certificates match
- SW certificate ξ^{SW} is authentic, i.e., generated by the TTP*
- Property commitment σ^{comm} is authentic, i.e., generated by the SW provider
- Clearance level certificate is authentic, i.e., generated by the TTP

→ Compatibility, clearance enforcement, and authenticity

(2) Conditions for an ISP to deliver a SW installation package

- SW request is authentic, i.e., generated by the user platform
- The set of requested rights is a subset of the allowed usage rights of the SW, i.e., does not violate the terms and conditions
- License provider issues a valid license
- ISP possesses the requested SW
- User platform has a valid ID

→ Authenticity, rights enforcement, and soundness

* ISP: Installation Service Provider, TTP: Trusted Third Party

In each step of a SW installation, the party in charge verifies several necessary conditions

NECESSARY CONDITIONS FOR EACH SW INSTALLATION STEP (2/2)

Main criteria

③ Conditions for a user platform to deliver an installation confirmation

- SW installation package is authentic, i.e., generated by the ISP*
- License is authentic, i.e., generated by the LP, and grants the requested rights
- SW is integer, i.e., identical to the SW which the TTP certified
- Decryption of SW succeeds
- Internal installation in target component succeeds (details follow)

→ Authenticity, integrity and soundness

④ Conditions for an ISP to deliver an acknowledgment

- Installation confirmation is authentic, i.e., generated by the user platform
- Installation result was "success"

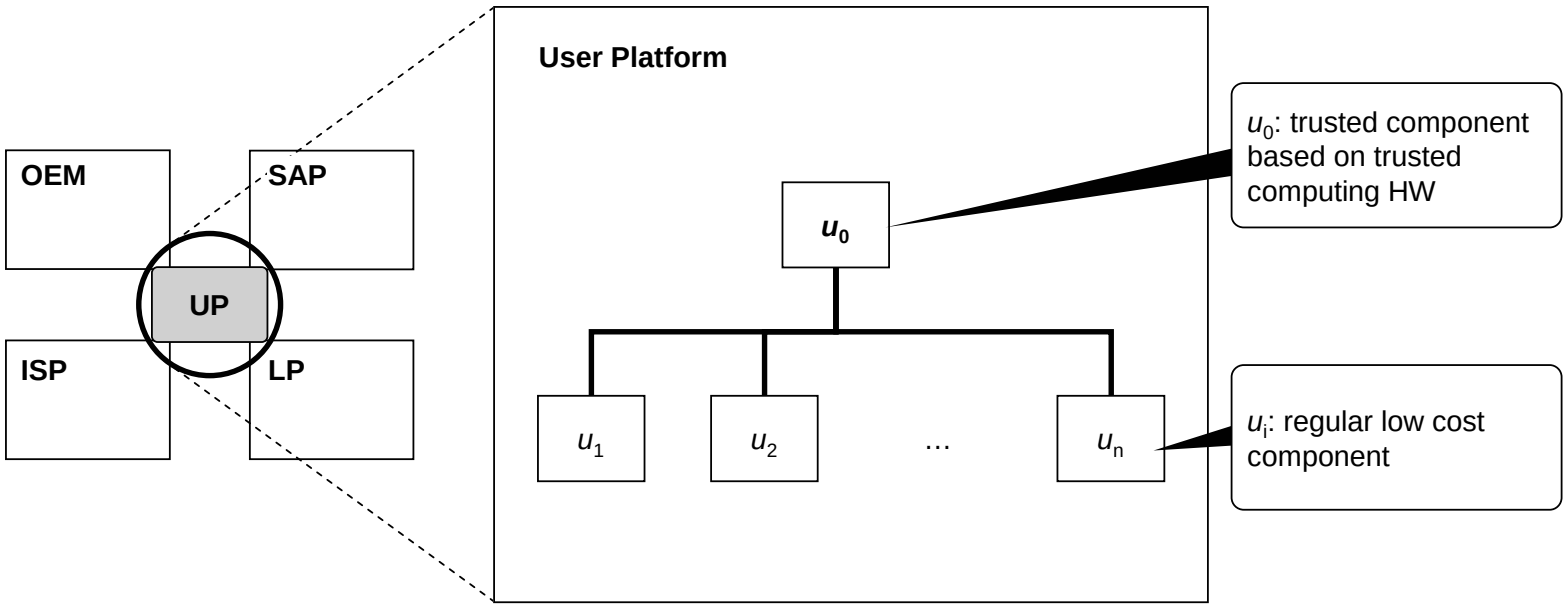
→ Authenticity and soundness

* Installation Service Provider

Source: Technical Report "Secure Software Delivery and Installation in Embedded Systems", http://www.prosec.rub.de/

The user platform has an internal structure consisting of three elements: a trusted component, regular components and an internal communication network

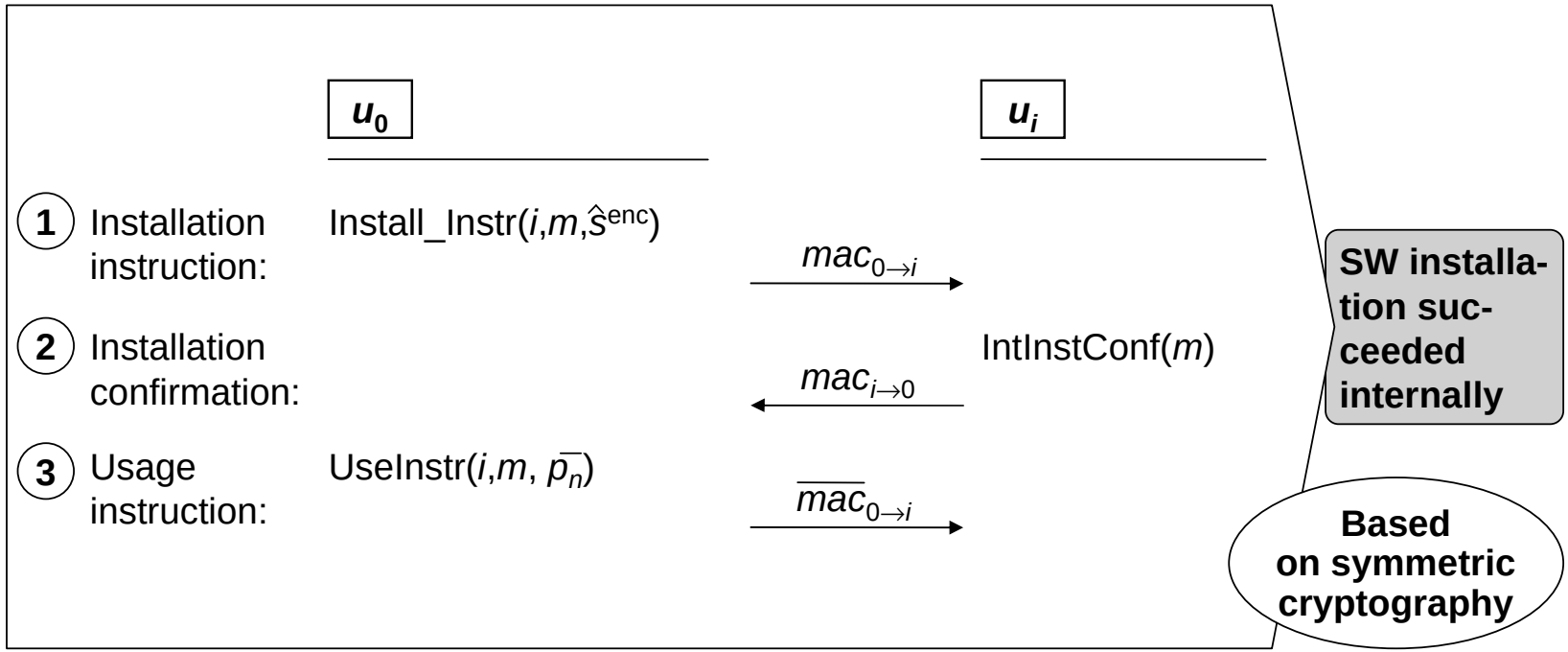
INTERNAL STRUCTURE OF THE USER PLATFORM



Internally, a SW installation within a user platform consists of three basic steps

THREE INTERNAL STEPS OF A SW INSTALLATION WITHIN A USER PLATFORM

u_0: Trusted component
u_i: Target component
$1 \le i \le n$



The paper makes two major contributions

CONCLUSION: TWO MAJOR CONTRIBUTIONS OF THE PAPER

Requirements model for SW installation in embedded systems

- Major roles included in requirements model
- Compatibility of SW components and skill set of ISPs considered
- Basic license and DRM scheme

Secure installation protocol meeting the requirements

- Public Key Broadcast Encryption (PKBE) for achieving non-discrimination
- Trusted Computing for achieving trust in user platform with little additional hardware
- Security analysis in Technical Report

Open Problem
Reduced need for TTP in setup phase by aggregating the PKBE key material bottom-up