



3rd Public Workshop IP Daidalos

**“Designing Advanced network Interfaces for the
Delivery and Administration of Location
independent, Optimised personal Services”**



**June 29, 2005
Brussels, (Belgium)**



3rd Public Workshop IP Daidalos

Overview of Security Related Activities in Daidalos

**Christian Hauser, Jochen Kögel,
WP1, University of Stuttgart, IKR**



Outline

- ▶ Security Evaluation: Challenge and Approach
- ▶ Example of Evaluation: A4C Server
- ▶ Summary of Results
- ▶ Outlook to Security Work in Phase II
- ▶ Cooperation with PRIME
- ▶ Conclusions





Challenge

Daidalos is not a single architecture instantiation

- ▶ Every operator can assemble its own architecture according to individual business needs
- ▶ Important aspects (for security) not similar for all possible instantiations
 - General evaluation not possible
- ▶ Examples
 - Varying trust domains
 - Deployment of IPSec depends on security of underlying network

Other peculiarities

- ▶ Research results → conceptual descriptions (no product stage specifications, no operational policies, ...)
- ▶ Value of assets not known → risk not quantifiable
- ▶ Huge system and not a full detailed model
 - formal evaluation not possible





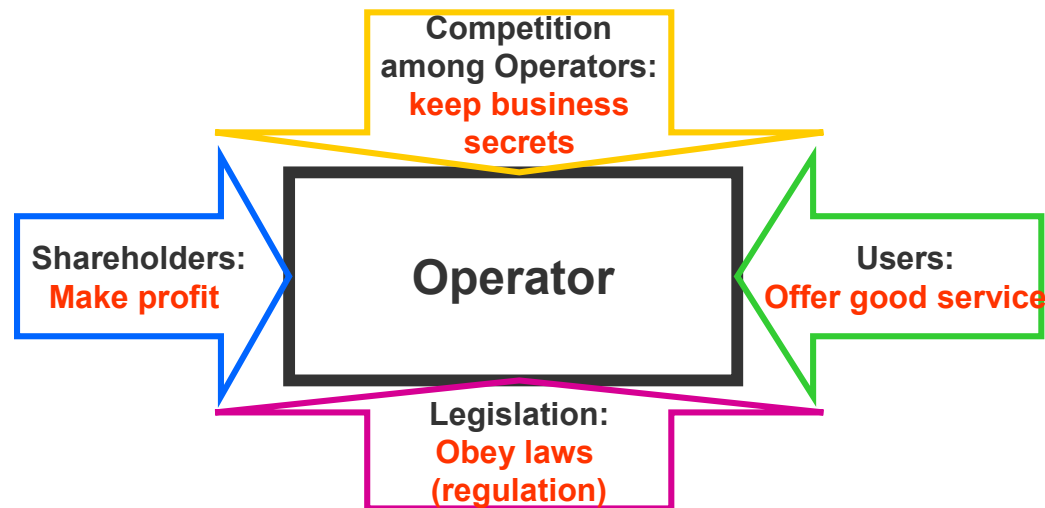
Approach

- ▶ Formal evaluation not possible
 - **well-structured** approach in order to assure
 - a certain degree of completeness
 - a common methodology among all evaluators and all components
 - a rating of the results
- ▶ Evaluation must be valid for all instantiations
 - **component-based** approach
 - Evaluate internal behavior of component by policies
 - Evaluate external behavior
 - Constraint: Interworking not fully covered
 - Requirements derived for possible instantiations
 - Focus on central components
- ▶ Team of (mainly) **independent auditors** not involved in design
 - objective evaluation, but misunderstandings possible





Deriving Policies



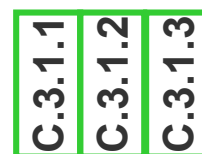
A-Level Policies
(business view)



B-Level Policies
(security centric)



C-Level Policies
(VID-specific)

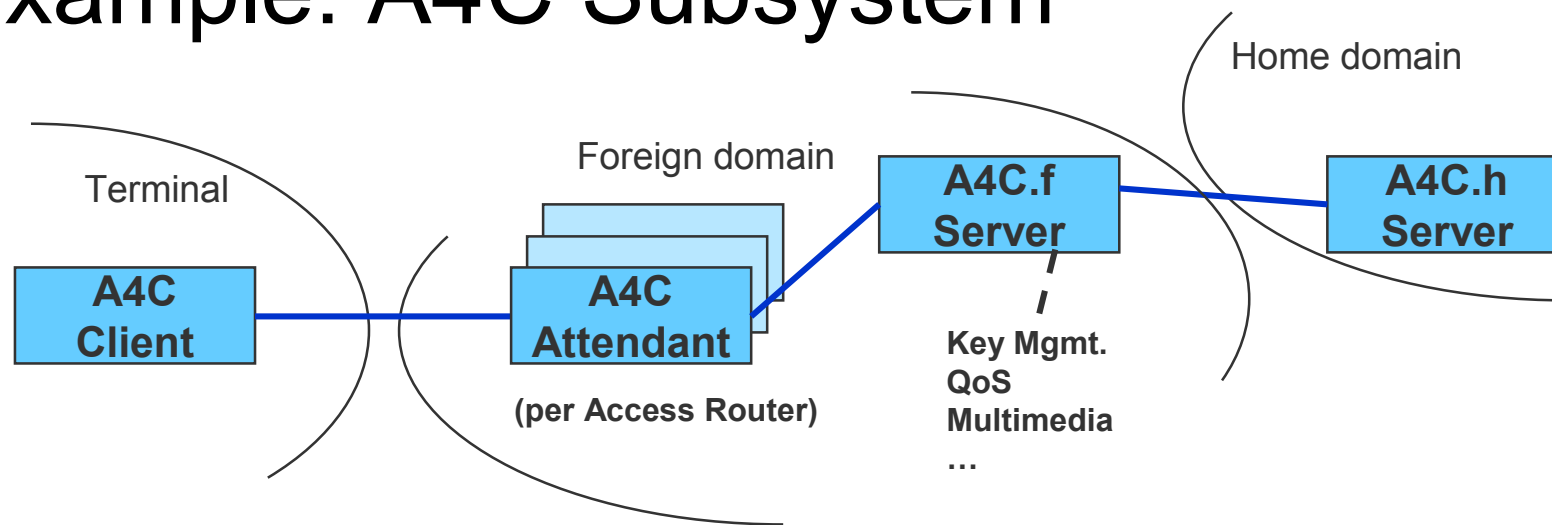


Basis for
evaluation





Example: A4C Subsystem



According to methodology

- ▶ Step through each component
A4C Server, A4C Attendant, A4C Client
- ▶ At each component
 - Check fulfillment of each policy
 - Derive security requirements for each interface





Example: A4C Subsystem

A4C Server - Policy B.1.1

“Any use/reservation of system resources that will be charged for according to the business model is accounted. (This also includes that accounting information is related to an (authenticated and authorized) user, and cannot be repudiated)”

- ▶ Architecture ensures that only accounting records **for authenticated and authorized users** can reach the A4C Server
- ▶ Records for **reservation of resources** (e.g. QoS) are considered
- ▶ Non-repudiation concept integrated
- ▶ **Issue:** No intermediate charging for post-paid
→ „endless calls“ are never charged
(high-level conceptual problem of „Service Interaction Phases“)





Example: A4C Subsystem

A4C Server - Policy B.1.2

“If the user is not willing to pay, enforcement mechanisms according to the contract apply. (e.g. the operator will deny further consumption of services)”

- ▶ **Issue:** Interface to other components lack enforcement functionality
 - No enforcement in case of post-paid
 - No immediate enforcement in case of pre-paid





Example: A4C Subsystem

Evaluation of Interfaces

Example: A4C interdomain interface

- ▶ Security of communication links for interfaces depends on instantiation
 - requirements on underlying communication networks are evaluated that have to be considered for securing certain functionalities
 - also derived from the policies
- ▶ Examples
 - B1.1 Accounting: **Integrity**
(possible realization: private network or digital signatures)
 - B1.2 Enforcement: **availability and integrity**
(possible realization: private network with resilience mechanisms)
 - C3.1.3 Prevention of VID linkage (for an outsider): **confidentiality**
(possible realization: private network or encryption)





Summary of A4C

- ▶ Main functionality (AAA) is working
- ▶ Minor design problems due to advanced privacy concept of VIDs
 - A4C Attendant can link VIDs based on IP Address
 - A4C.f must know link of VIDs to RegID
 - Certificates observable in registration phase:
attacker can link VIDs to terminals and observe e.g. denial of registration
- ▶ Some error cases not considered
 - No immediate enforcement
- ▶ Conceptual problem in very specific scenario
 - Charging of endless sessions





Overall Summary of Main Results I

- ▶ No consistent enforcement in case of denying service usage (non-repudiation function)
- ▶ Accounting problems of endless sessions
- ▶ Unchecked charging messages in MMSP
- ▶ No consistent protection of signaling traffic
- ▶ No consistent and clear specification of IPSec use
- ▶ Certain privacy leaks
 - E.g., non-credibility of user by observation of unsuccessful service requests
 - Suboptimal design of ID-Token
 - Non-consistent spreading of VID concept
- ▶ No A4C integrated in WP4





Overall Summary of Main Results II

Three classes

- ▶ Conceptual problems
 - No charging in endless sessions
- ▶ Technical details
 - ID-Token not optimally designed
- ▶ General technical issues
 - No full specification of IPSec use

Origin of main problems

- ▶ Known problems taken into account on purpose for risk and/or resource management reasons, e.g., no full spreading of VID concept, no A4C in WP4
- ▶ Different underlying attacker models and trust assumptions due to partly bottom-up approach
- ▶ Not a single architecture instantiation





Architectural Approach in Phase II

- ▶ Stronger top-down approach
- ▶ Common attacker model among all WPs, aligned with business actors
- ▶ Stronger focus on deployment of components
- ▶ Concrete sample architecture instantiations
- ▶ A4C activity also in WP4
- ▶ Refined VID concept
 - Wider spreading of VID concept
 - More implications of VID concept explored before start of detailed research
 - Get the basic lines of integration
 - Get a feeling about how far to go
- ▶ Exploitation of liaison projects to extend security work





Attacker Model

<---Attacker--->

	User	Term. Pr.	AgAPr.	PSPr.	VASPr.	NO	Outsider
<---Target---> User							
Term. Pr.							
AgAPr.							
PSPr.							
VASPr.							
NO							
Outsider							

- ▶ Domains according to (fragmented) instantiation
 - User
 - Terminal Provider (Term Pr.)
 - Aggregated Access Provider (AgAPr.)
 - Pervasive Service Provider (PSPr.)
 - Value-added Service Provider (VASPr.)
 - Network Operator (NO)
 - Outsider: Non-Daidalos entity (e.g. eavesdropper on the access network)





Attacker Model

<---Attacker--->

	User	Term. Pr.	AgAPr.	PSPr.	VASPr.	NO	Outsider
<---Target---> User	2, WP2/3/4		3, WP3	3, WP4	1, WP4	2, WP2/3	5, WP2/3/4
Term. Pr.							
AgAPr.	1, WP3		2, WP3	2, WP3	2, WP3/4	2, WP3	
PSPr.	1, WP4		2, WP4	2, WP4	2, WP4	2, WP4	
VASPr.	1, WP3/4		5, WP3/4	5, WP3/4	5, WP3/4		
NO	1, WP2/3			3, WP2	1, WP2/3		1, WP2/3
Outsider							

- ▶ Definition of project scope and priority
- ▶ Assignment to work packages
- ▶ To be evolved in future when gaining new insights
 - E.g., attacker power
 - E.g., further subdivision of actors





Security Evaluation in Phase II

- ▶ Jointly with (fully) external experts
 - Internal experts for explaining Daidalos
 - External experts for independency
- ▶ More iteratively
 - Several pre-evaluations during research process
 - Shorter feedback cycles
 - Regular dissemination of results
 - feedback at end of phase II is not enough as no third phase will exist
 - Basic lines of architecture seem to be stable enough earlier than in phase I





Cooperation with PRIME

External security evaluation

- ▶ Idea
 - Auditing of internal evaluations by PRIME partners
 - Consulting to help us to improve (process and results)
- ▶ Status
 - Proposal sent to PRIME for agreement
 - Administrative organization to be clarified

Other activities

- ▶ Daidalos contribution to “*Workshop on Standards for Privacy in User-Centric Identity Management*” organized by PRIME and FIDIS
 - Start to get deeper in touch with standardization bodies and external experts
- ▶ Evaluation of feasibility of PRIME concepts





Conclusions

Security evaluation in phase I

- ▶ Several flaws found
 - Mostly minor flaws identified
 - Big issues were known and because of risk management
- ▶ More flaws might be present
 - No formal evaluation → no proof
 - No full evaluation of architecture instantiation
 - No evaluation of “external” protocols
 - Not all components evaluated → will change anyway in D-II and major problems were already identified

Resulting adaptations in phase II

- ▶ Stronger top-down approach, e.g., by common attacker model
- ▶ Wider spreading of VID concept for privacy
- ▶ Expansion of A4C concepts on WP4
- ▶ Adaptation of evaluation process
- ▶ Integrated security knowhow and solutions from cooperating projects, e.g., PRIME





**3rd Public Workshop
IP Daidalos**

...end of presentation.

Thank you for your attention!