Trust Access Path Concept

Fangbin Liu Steffen van Loon

System and Network Engineering
Universiteit van Amsterdam

6 July, 2006

Outline

- Introduction and background of project
- Why “TAP”?
- The TAP-concept
- Application of TAP-concept
- Application in Proof of Concepts
- Conclusion and recommendations

Introduction and background of project

- A new concept “TAP” (Trust Access Path) from a large governmental organization
- The purpose of this project
- Project scope
- Main question for this project
- Mains steps within this project

Why TAP?

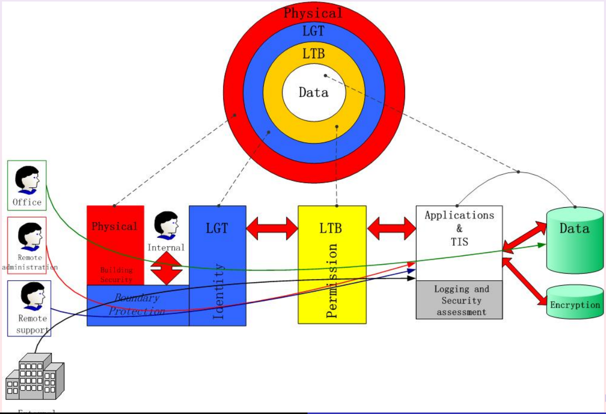
1. Development within the governmental organization (customer-pull)
2. Developments in market (market-push)
3. Impact

Development within the governmental organization

Current situation:

- “Onion” model
- Through multiple layers including: physical security, logical closed technical infrastructure and logical access control

Development within the governmental organization



Development within the governmental organization

- The control on these connections not practicable due to insufficient supervision
- Infrastructure not conform to the minimum security requirements:
  - Some hardware, software, data and users not known or trusted
  - Some access to data not through authorized applications
  - Some transmission of data through uncontrolled ports
  - ICT architecture not fully covered with physical security

Developments in market

- Current conditions not valid anymore
  - Traffic security control
  - Global provision of services
  - Services provided by third party
- Various techniques developed on the market
  - More awareness and attention for security risks
  - Security aspect divisions and products developed more intensively
  - Security become standard feature for services

Impact

Changing infrastructure and changing demands ask for a new security concept

$\longrightarrow$ TAP-concept

The TAP-concept

- Why TAP-concept introduced
- Description of TAP-concept
- Where TAP-concept applicable

Origin and description of TAP

- Main reason: an additional model for development and deployment to achieve the security again
- Demands on the development line
  - All obscurities regarding functions and responsibilities cleared
  - All dependencies on physical security combined and minimized
  - Data access only through authorized processes

Origin and description of TAP

- Key functions in secure infrastructure are: identification, authentication, authorization and verification
- Multiple implementations of these functions without a good model is ineffective and inefficient
- Trust relationships as a solution for the problems applied in many situations
- Foundation decisions for TAP-concept
    - Registration by one process
    - Authentication by one process
    - Authorizations granted to users (not to processes)
    - Complete chain verified (logged)

Origin and description of TAP

- Goal of TAP-concept: to define environment with single implemented security functions
- Easier overview for implemented functions
- explicit description of risk management

Primary achievements:

- Reduction of complexity
- Reduction of administration
- Better control
- Better reporting

What is TAP?

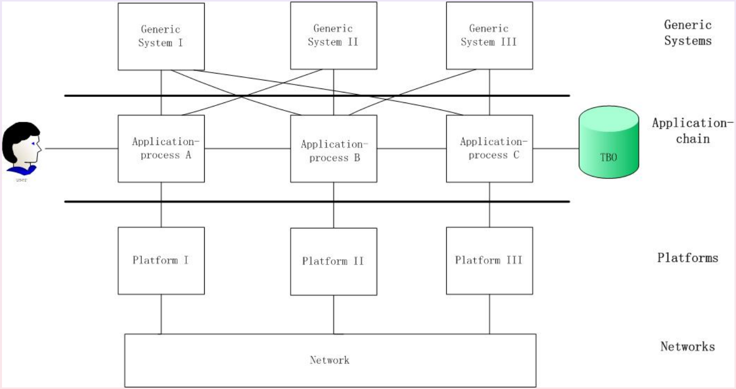


Figure: A figure of TAP-concept

What is TAP?

- Trust relations between secured processes
- Multiple security methods are deployed generically:
  - Invoked within the process chain
  - At the start and end points of the process chain
- Efficiency through security methods overall applicable

Where is TAP applicable?

TAP-concept requires:

- Components loosely connected with application
- Components clearly identified
- Function simply realized
- Data centrally stored

Business requirements

- Clear ownership of processes and data
- Clear granted authorizations
- Authorized users must be trustworthy
- Identifiable user roles
- Limited number of roles

Technical requirements

- Four components: identity, authentication, authorization, logging management
- Single Sign-On
- Role Based Access Control
- Link between users and processes

Identity Management

- Role based identity management
- Various products on the market: IBM, Sun, . . .
- Identity management for single sign-on feature as generic service
- Portal system through delegating the user to finish the job

Permission Management

- Identity verification through key exchange and connection parameter verification
- Certificate utilized among processes should be verifiable
- Permission granting on the basis of system environment
- Positions for authorization control

Encryption

- Various Encryption utilized for various communication paths
- Encryption management not part of TAP concept

Logging Management

- Logging records generated for the whole system environment
- Centralized record storage mechanism for auditing and analysis
- Records generated for different levels for various components

MijnUvA

- Authentication:

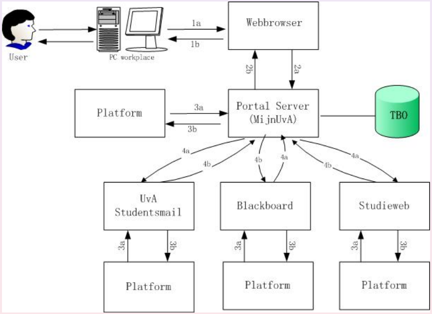


Figure: Trust-model for authentication with the use of a browser with MijnUvA Portal system

MijnUvA

- Authorization:

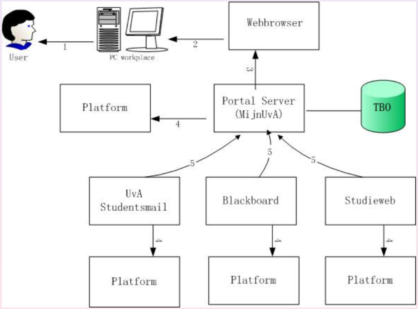


Figure: Trust-model for authorization with the use of a browser with MijnUvA Portal system

MijnUvA

- Logging:

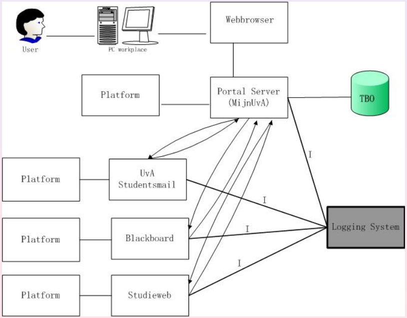


Figure: Trust-model for logging with the use of a browser with MijnUvA Portal system

Overview of Eduroam

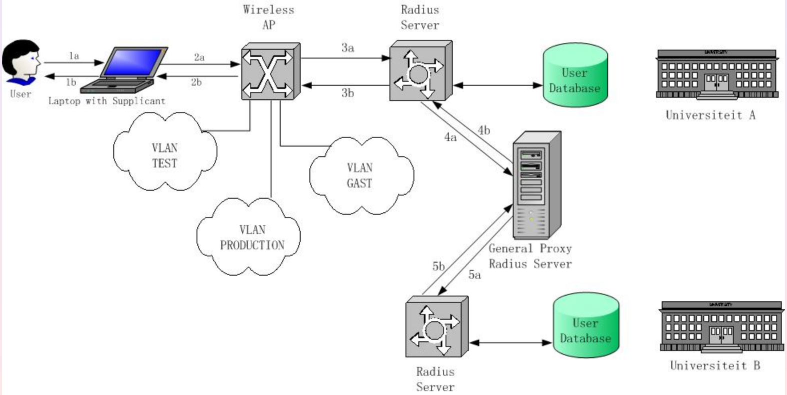


Figure: Working model for authentication in Eduroam

Overview of Eduroam

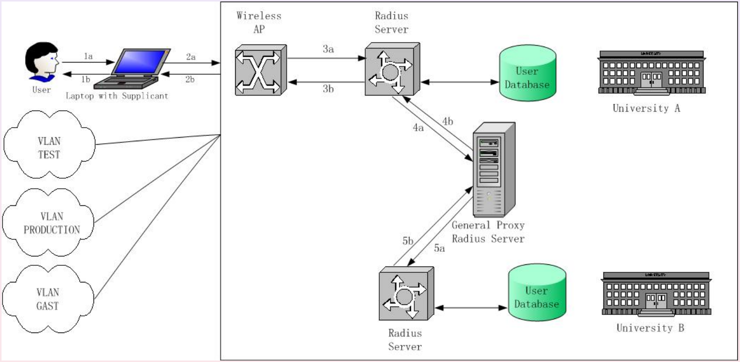


Figure: Working model 2 for authentication in Eduroam

Authentication an authorization

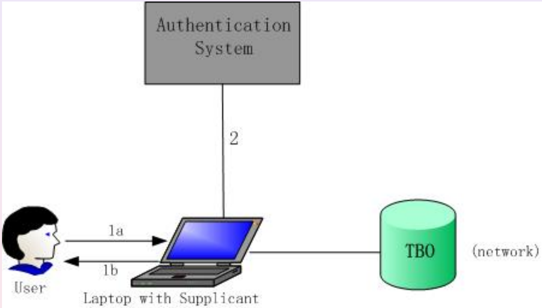


Figure: Overview of Trust relations for authentication between users and Eduroam System

Logging

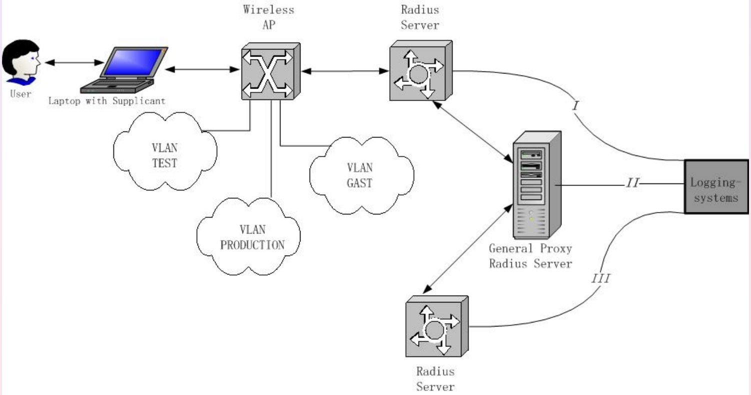


Figure: Trust relations for logging in Eduroam

Conclusion and Recommendations

- TAP is a successful addition at this large governmental organization, but
- Implementation probably takes a long period
- Extension of the TAP-concept is still necessary
- Business requirements more important for implementation

Question?

Discussion