Trusted Infrastructures for Identities

Virtual Goods, Koblenz 2007

Barbara Fichtinger, Eckehard Hermann, Nicolai Kuntze, Andreas Schmidt
Barbara Fichtinger

University of Applied Sciences, Hagenberg, Upper Austria
- BSc in Computer and Media Security
- MSc in Secure Information Systems
  Master thesis in cooperation with Fraunhofer Institute for Secure Information Technology, Darmstadt

International experience
- Karlstad University, Sweden

Since October 2007
- Associate Consultant, Siemens AG, Munich
- CERT (Computer Emergency Response Team)
Agenda

- Problem description
- Basics
  - Trusted Computing
  - Identity Management
- Trusted Infrastructures for Identities
  - Requirements
  - Protocol sequence
  - Protocol messages
- Analysis
Problem description

- Increasing importance of Identity Management
- Identity Management Architectures
Problem description

- Trust relationships between the identifier domains
  - Traditional solutions
    - Cross certification
    - Spanning Certificate Authorities
    - Mirroring of user databases
  - Usage of already existing architectures:
    - Trusted Computing Group

- Identity provider
  - Authorization to issue tickets
  - Current system status during the authentication and authorization process
Trusted Computing

- Concept for attesting the trustworthiness of a platform
- Foundation of trust
  - Hardware chip: Trusted Platform Module (TPM)
- Transitive Trust
Trusted Computing

- Trusted Platform Module (TPM)
  - Integrity Measurement (Platform Configuration Register)
  - Cryptographic functions
  - Secure memory

- Cryptographic keys and credentials (certificates)
  - Endorsement Key (EK) und Credential
  - Attestation Identity Key (AIK) und Credential
  - Signing Keys
Identity Management - SAML

- Security Assertion Markup Language (SAML)
- XML-based security standard
- Transport of authentication- and authorization information
- Assertions
  - Authentication Statement
  - Authorization Decision Statement
  - Attribute Statement
Trusted Infrastructures for Identities

- **Goal**
  - Service providers trust decisions of identity providers in foreign identifier domains

- **Prerequisites**
  - Identity providers have to be equipped with a TPM
  - Adaptable infrastructure offered by the Trusted Computing Group

- **Tasks of the identity provider**
  - Authentication and authorization
  - Issuance of a trusted ticket

- **Tasks of the service provider**
  - Was the identity provider trustworthy at the moment of ticket issuing?
  - Is the identity provider authorized to issue tickets for the domain?
Trusted Infrastructures for Identities

- Trustworthy status of the identity provider
  - Integration of status information in the tickets
  - Measurements are compared with reference values

- Authorization of the identity provider to issue tickets
  - Adaptation of the request of identity credentials from the Privacy-CA
  - Privacy-CA decides based on the Endorsement Credential
    - Vendor certificate, Public Endorsement key
  - Creation of a special Attestation Identity Credential
Protocol sequence

1. Request + Credentials
2. Authentication Authorization
3. Ticket creation + status information + AlK credential
4. Service Request
5. Ticket validation - status information - AlK credential
Protocol messages

- **AIK Credential**
  - Format specified based on X.509 certificates
  - Extended key usage attribute (trustedTicketIssuing)

- **Trusted ticket**
  - SAML Assertion
  - Attribute statement for the transport of status information
  - Special XML structure
    - Values of the Platform Configuration Registers
    - Measurement log
    - AIK Credential (used to sign the status information)
  - Assertion is signed with a signing key
    - Signing key is certified with the Attestation Identity Key
<saml:Assertion
  MajorVersion="1"
  MinorVersion="0"
  AssertionID=number
  issuer="Identity Provider"
  IssueInstant=timestamp>
  <saml:Conditions
    NotBefore=timestamp
    NotOnOrAfter=timestamp />
  <ds:Signature>
  ... DzTJ4v1xz8QFn ...
  </ds:Signature>
  <saml:AuthenticationStatement
    AuthenticationMethod=method
    AuthenticationInstant=timestamp />
  <saml:AttributeStatement>
    <saml:Attribute
      AttributeName="QuoteValue"
      AttributeNameSpace="http://www.fh-ooe.at/ns">
      <QuoteValue>
        <ExternalData>... QFnR ...</ExternalData>
        <Data>... 9gi85 ...</Data>
        <ValidationData>... VB9gj ...</ValidationData>
      </QuoteValue>
    </saml:Attribute>
    <saml:Attribute
      AttributeName="EventLog"
      AttributeNameSpace="http://www.fh-ooe.at/ns">
      <EventLog>
        <Pcr_index=1>
          <PcrEvent_index=0>
            <TcTssVersion>x.x.x</TcTssVersion>
            <PcrIndex>1</PcrIndex>
            <EventType>12245</EventType>
            <PcrValue>... E4D21 ...</PcrValue>
            <Event>... 215TY ...</Event>
          </PcrEvent>
          <PcrEvent_index=1> ... </PcrEvent>
        </Pcr>
        <Pcr_index=2> ... </Pcr>
      </EventLog>
    </saml:Attribute>
    <saml:Attribute
      AttributeName="AikCredential"
      AttributeNameSpace="http://www.w3.org/2000/09/xmldsig#">
      <X509Certificate>... zTJ5QFnR ...</X509Certificate>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
Analysis

Advantages

- Usage of the infrastructure provided by the Trusted Computing Group
- Significant reduction of the initial implementation costs
- No additional PKI is required
- Embedding of status information in the tickets

Problems

- Scalability of the trust relationships between the identifier domains
- Adaptions of the original Trusted Computing architecture
- Size of the event log
Conclusion

Results
- Establishment of trust relationships with Trusted Computing technology is possible
- Successful reference implementation

Use cases in addition to the identity management area
- Anonymous usage of the tickets
- Combination with a payment system

Future research topics
- Verification of the service provider’s system status by the user
- Formulation of generic access-control policies
- Message replay attacks
- Implementation of integrity-measurement mechanisms in current operating systems
Questions?