The C-DAX Security Architecture for Smart Grids

Florian Heimgärtner, Michael Höfling, Barbara Vieira, Erik Poll, Michael Menth

http://kn.inf.uni-tuebingen.de
C-DAX Project

EC FP7-ICT-2011-8 call project
- C-DAX: Cyber-secure Data And Control Cloud for power grids

Duration: 2012-10-01 – 2015-09-30

Total budget: 4,315,303 Euro
EU-funding: 2,931,000 Euro

C-DAX middleware
- Enables smart grid applications to exchange information securely
- Implements information-centric networking (ICN) paradigm
- Supports publish/subscribe across different administrative domains

Targeted use cases
- Future retail energy market (REM)
- Real-time state estimation based on PMU measurements
- Telecontrol (SCADA)

Project coordination: iMinds
Project website: http://www.cdax.eu

Project partners

C-DAX Components

► C-DAX client (publisher or subscriber)
  ▪ Produces or consumes information for a specific topic
  ▪ Provide access for smart grid applications to the C-DAX cloud (through an API)

► C-DAX cloud
  ▪ Network of C-DAX nodes

► C-DAX node
  ▪ Physical entity providing a specific set of functions to the cloud and the clients
C-DAX Communication Platform

C-DAX cloud

Security Server (SecServ)

Resolver

Data Broker (DB)

Designated Node (DN)

Designated Node (DN)

Client (Publisher)

Client (Subscriber)

SG application data to be published

: Control plane communication

SG application data to be consumed

: Data plane communication

C-DAX Monitoring/Management System

What do we want?

► Minimal trust in underlying infrastructure
  ▪ Nodes do not have to trust each other inside C-DAX cloud
  ▪ Clients do not have to trust C-DAX cloud for guaranteed end-to-end security

► Flexible match of security parameters to requirements of use cases, e.g., data rates, latency, confidentiality, integrity

How do we realize this in C-DAX?

► Authentication of clients and nodes based on asymmetric cryptography

► Symmetric cryptography for topic data

► Asymmetric cryptography for control data

► Central security component: Security Server (SecServ)
C-DAX Security Properties

Source authentication
- Mainly used for control plane messages
- Digital signatures

Topic access control
- Only legitimate publishers should be able to publish data to a topic
- Cryptography-based access control
  - Message Authentication Code (MAC) using a key shared among publishers and forwarding nodes

End-to-end integrity
- MAC using a key shared among publishers and subscribers

End-to-end confidentiality
- Control Plane (one-to-one)
  - Asymmetric encryption using recipient’s public key
- Data Plane (many-to-many)
  - Symmetric encryption using a key shared among publishers and subscribers

Forwarding nodes cannot decrypt or alter data
C-DAX Security Server

Services provided by the Security Server (SecServ)
► Managing and enforcing Access Control Lists (ACLs)
► Certification Authority (CA)
  ▪ Linking information to public keys of components (clients and nodes) using digital signatures → Certificates
    – Identity information
    – Roles and permissions
  ▪ Providing a Certificate Revocation List (CRL)
► Authentication of clients and nodes
  ▪ Verifying signatures of request messages
► Generating topic keys
► Distributing topic keys
  ▪ Asymmetric encryption of transmitted topic keys
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Associated with</th>
<th>Known by</th>
</tr>
</thead>
<tbody>
<tr>
<td>$K_c^-$</td>
<td>Component private key</td>
<td>Component $c$</td>
<td>Component $c$</td>
</tr>
<tr>
<td>$K_c^+$</td>
<td>Component public key</td>
<td>Component $c$</td>
<td>May be known by all components</td>
</tr>
<tr>
<td>$K_{SecServ}^+$</td>
<td>SecServ public key</td>
<td>SecServ</td>
<td>Must be known by all components</td>
</tr>
<tr>
<td>$K_t^{auth}$</td>
<td>Topic access control key</td>
<td>Topic $t$</td>
<td>Publishers, DNs, DBs for topic $t$</td>
</tr>
<tr>
<td>$K_t^{e2e}$</td>
<td>End-to-end security key</td>
<td>Topic $t$</td>
<td>Publishers and subscribers for topic $t$</td>
</tr>
</tbody>
</table>
SecServ distributes $K_t^{auth}$ and $K_t^{e2e}$ (1, 2).
Publisher encrypts message using $K_t^{e2e}$ and generates MAC using $K_t^{auth}$ and $K_t^{e2e}$ (3).
DBs and DNs verify MAC using $K_t^{auth}$ (4).
Subscriber decrypts and verifies MAC using $K_t^{e2e}$.

Key update triggers
- Join or leave events
- ACL changes
- Key lifetime expires

Secure key transition
- Backward secrecy
  - “old, previously used group keys must not be discovered by new group members”
- Forward secrecy
  - “new keys must remain out of reach of former group members”
- Asymmetric encryption required for topic key update

Topic key dissemination
- Push approach
  - Use topic-based pub/sub
  - SecServ sends topic keys encrypted with public keys of topic members
- Pull approach
  - SecServ sends key update notification via pub/sub
  - Topic members retrieve new topic key from SecServ
SecServ distributes updated keys via pub/sub (encrypted with each recipient's public key)

Problems
- Clients receive multiple keys but can only decrypt one
- SecServ needs to know current subscription state

Example: Update of $K_{t}^{e2e}$

1. SecServ sends update notification via pub/sub (plain text)
2. Clients send key retrieval request (signed using $K_{c}^{-}$)
3. Clients receive keys (encrypted using $K_{c}^{+}$)

Security architecture for C-DAX pub/sub middleware

- Based on standard cryptographic primitives
- End-to-end security
  - Ensuring message integrity and confidentiality between publishers and subscribers without the need to trust intermediate nodes
- Cryptography-based access control for publication to topics
- Certificates/signatures for source authentication (control plane)
- Key update mechanisms ensuring forward/backward secrecy
  - Asymmetric encryption using recipient’s public key
  - “Push” and “Pull” approach

Security concept implemented in C-DAX prototype

- EPFL’s real-time power network simulator
- Alliander Livelab smart grid test site
Contact

Dipl.-Inform. Florian Heimgärtner

University of Tübingen
Department of Computer Science
Chair of Communication Networks
Sand 13, 72076 Tuebingen, Germany

E-Mail: heimgaer@informatik.uni-tuebingen.de
http://kn.inf.uni-tuebingen.de/staff/heimgaertner

www.cdax.eu

Thank you for your attention!
Questions?