nano-tera.ch
swiss scientific initiative in health / security / environment systems

SmartGrid RTD 2013

FNSNF

Secure Architecture for Active Power Distribution Networks (ADNs)

Teklemariam T. Tesfay, Jean-Yves Le Boudec
Email: {tech.tesfay, jean-yves.leboudec}@epfl.ch

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

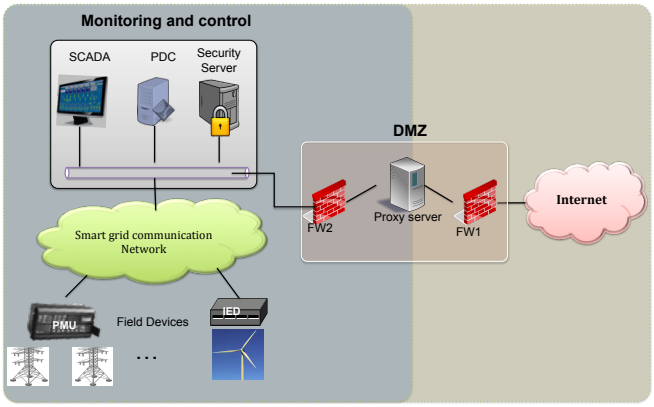
Context

Active power distribution network

- Highly distributed and more sophisticated monitoring and control strategy
- A large number of sensing (e.g PMUs) and actuating (IEDs) field devices
- Dispersed over a large unprotected geographic area

Cyber-security implications

- Opens lots of entry points for cyber-attacks
- Insider or outsider attackers



Secure network perimeter

- Physically separate network from the public network
- Firewalls filter outgoing and incoming traffic from/to the ADN
- A proxy server at the Demilitarized Zone (DMZ) serves as a relay node
- Proxy server performs further security checks for suspicious data before relaying traffic

Secure end-to-end message delivery

- Communicating parties mutually authenticate using their certificates
- Devices use their certificates to agree on a group encryption key
- Source authentication achieved using one-time-signature technique

Security Concerns and goals

Attacker's Goals

- Compromise the availability, integrity, confidentiality of sensor data or control signals

Security Goals

- Being *smart* should not translate to a *more fragile* system
- An Attacker should not have more power than a classical sabotage destruction

Security solutions

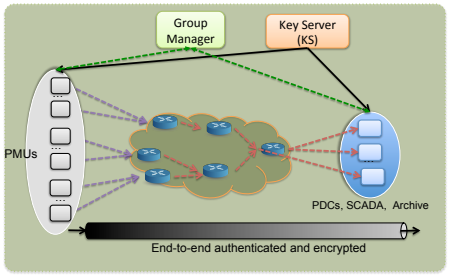
- Authenticated access to devices and network
- Secure network perimeter
- Secure end-to-end message delivery

Authenticated user access to devices

- Access to all devices in the ADN limited to only authorized personnel
- Centrally managed separate per-user credentials
- Activity logging and monitoring to held individuals accountable

Authenticated network access by devices

- A certificate authority (CA) issues digital certificates to all devices
- 802.1x protocol used to authenticate devices using their digital certificate
- Prevent rogue devices from accessing the ADN
- No device is able to stream traffic through the network before authentication



Secure end-to-end multi-cast communication

Reference: Teklemariam T. Tesfay, Jean-Pierre Hubaux, Jean-Yves Le Boudec, and Philippe Oechslin "Cyber-Secure Communication Architecture for Active Power Distribution Networks (ADN)", *Special Track on Smart Grid and Smart Technologies (SGST), March 24-28, 2014* Gyeongju, Korea