Network Security Authentication of Power System Operations

Authors: Helen Cheung, Alexander Hamlyn, Cungang Yang

Presenter: Qin Yan

Submitted in Partial Fulfillment of the Course Requirements for
ECEN 689: Cyber Security of the Smart Grid
Instructor: Dr. Deepa Kundur

Outline

- Introduction and Motivation
- Smart grid role-based authentication
- Security authentication procedures
- Security authentication of stability control
- Conclusion
- My assessment
- Reference

Introduction and Motivation

- Operations of electricity power distribution systems have become fairly complex, due to
  - -- Distributed generations and microgrids
  - -- Open access competition
  - -- Network-controlled devices
- Computer network therefore turns into a key integral of modern power-grid operations.

Introduction and Motivation

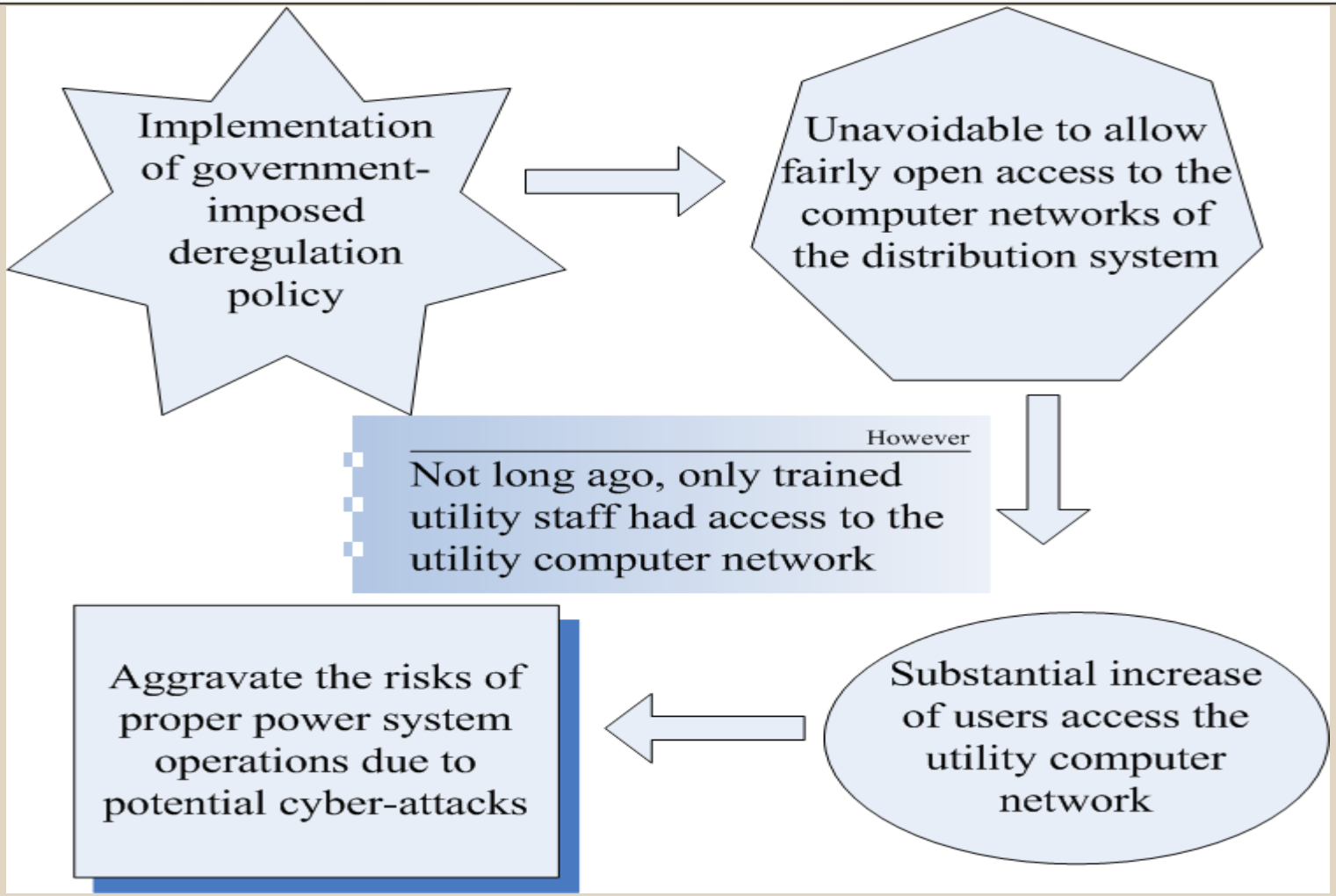


Figure. 1 Cause and Effect

Introduction and Motivation

- Therefore, security and reliability concerns of computer networks rising rapidly and demands for secure computer-controlled power system automation increasing tremendously.
- The paper proposes a **new strategy** for computer network security authentication of requests for actions/ commands in the smart-grid operations.
- The authentication covers multiple security domains in a new security architecture designed for smart power grids.

Role-based Authentication

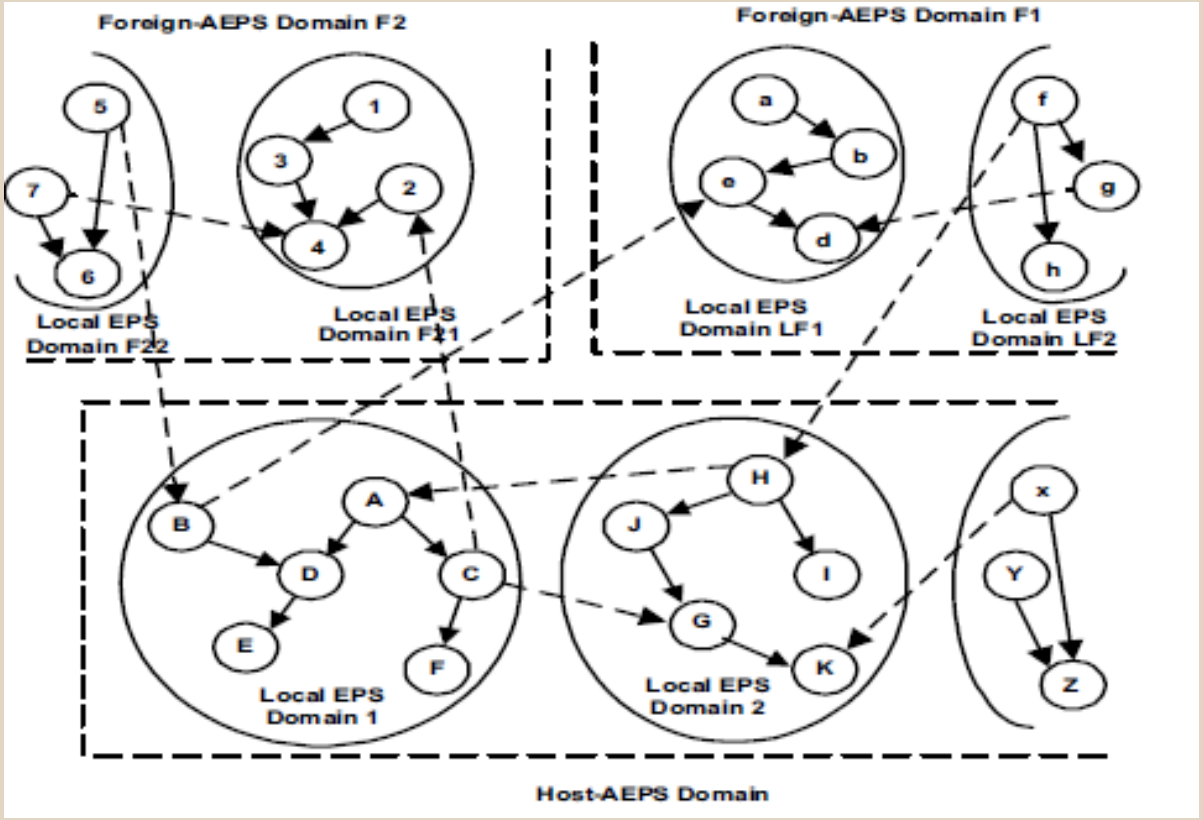


Figure. 2 Power Grid Security Architecture[1]

- Host-AEPS and interconnecting neighboring AEPS
- Network control center operates as an administrator and communicates with other users
- Each circle in the local security domain represents a role

Role-based Authentication

- A role is defined as collection of privileges that can be executed by the authorized users of certain job positions
- A privilege can be exercised on objects such as monitoring power system performance, trading electricity, operating substation equipments, etc.

Role-based Authentication

1. Authentication w.r.t Role Constraints

- The network controller is responsible for carrying out an authentication evaluation for constraints to the role operations defined with qualifications.
  - Cardinality constraints
  - Separation-of-duty constraints
  - Prerequisite constraints

Role-based Authentication

- Cardinality constraints
  - Have a limited number of users
  - Execute a limited number of roles
  - Limited number of roles that can be linked

e.g. In a typical electricity substation, the role of circuit breaker operator assigned to:

- substation operation on duty
- substation supervisor
- control center operator

Role-based Authentication

- Separation-of-duty constraints
  - managed by the network controller to enforce conflict of interest prevention policy

  e.g. electricity transaction monitor & power flow controller in power enterprise systems
- Prerequisite constraints
  - ensure that a user can perform a prerequisite operation if and only if the user has already been a member of prerequisite role

Role-based Authentication

e.g. The role with a privilege to trip substation bus-tie breaker must be a substation operator with a specific training and operating experience

- Other constraints

e.g. time constrains that defines how long the role can be activated that may be changed

Role-based Authentication

2. Authentication w.r.t Foreign Domain Interfacing

- A foreign-user network access policy to verify the trust relationship between users of host domain and those of foreign domain
- Digital credentials used to manage the trust establishment efficiently and verify the network access request to the power-grid computer networks
  - ➢ Properties and values for each type

Role-based Authentication

e.g. a substation circuit-breaker operator-- the user's profession credential, required training, specific equipment operating experiences, etc.

- When a foreign user requests to engage in a sensitive transaction without sufficient pre-established trust and such a request involves essentially every aspect of the ecommerce in the power systems.
- An enterprise's network access policy may allow foreign users to access to certain data files but such access may limit to the authorized users.

Security Authentication Procedures

Typical procedures of security authentication of requests for actions/commands in smart grids operations:

- A procedure handles the user access to its own local domain
  - Most frequent: utility staffs use the computer network to carry out daily tasks:

    obtain monitoring data of substation bus voltage and current, feeder voltage and current, breaker status
- A procedure handles the user access to another local domain

Security Authentication Procedures

- Specific: some utility staffs use another local network to carry out specific tasks:

  obtain monitoring data of neighboring substation power flow, breaker status on the high voltage transmission system

- A procedure handles the foreign user access to host AEPS domain
- Occasional: staff of other AEPS or personnel makes access to the host domain to carry out some tasks:

  request for transfer of power, sequence of events records, power flow data

Security Procedures Pre-execution

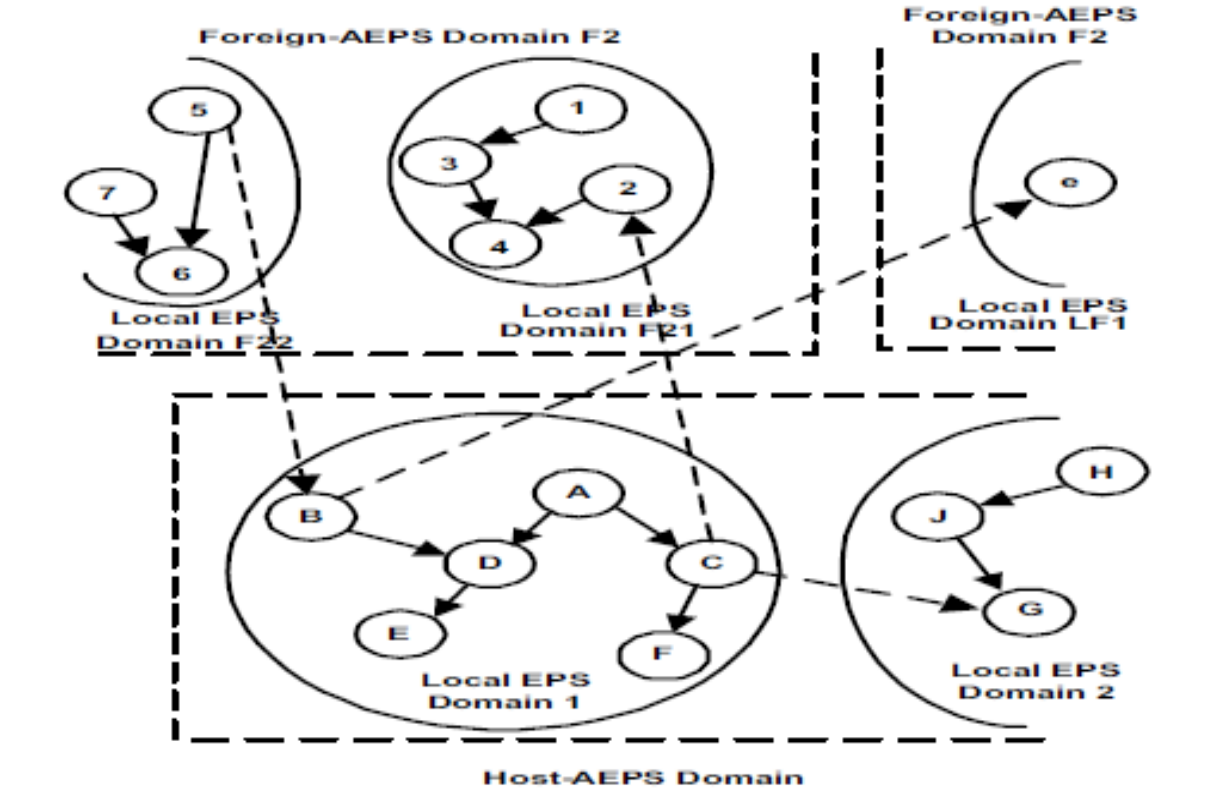


Figure. 3 Role Hierarchy for Inter AEPS Domains[1]

Network administrator defines functions of roles:

A: supervising role

B: monitoring role

C: power-flow controlling

D: substation designing

E: analyzing role

F: substation operating

G: power-flow monitoring

2: controlling role

4: bus-voltage analyzing

Illustration of Authentication of Requests

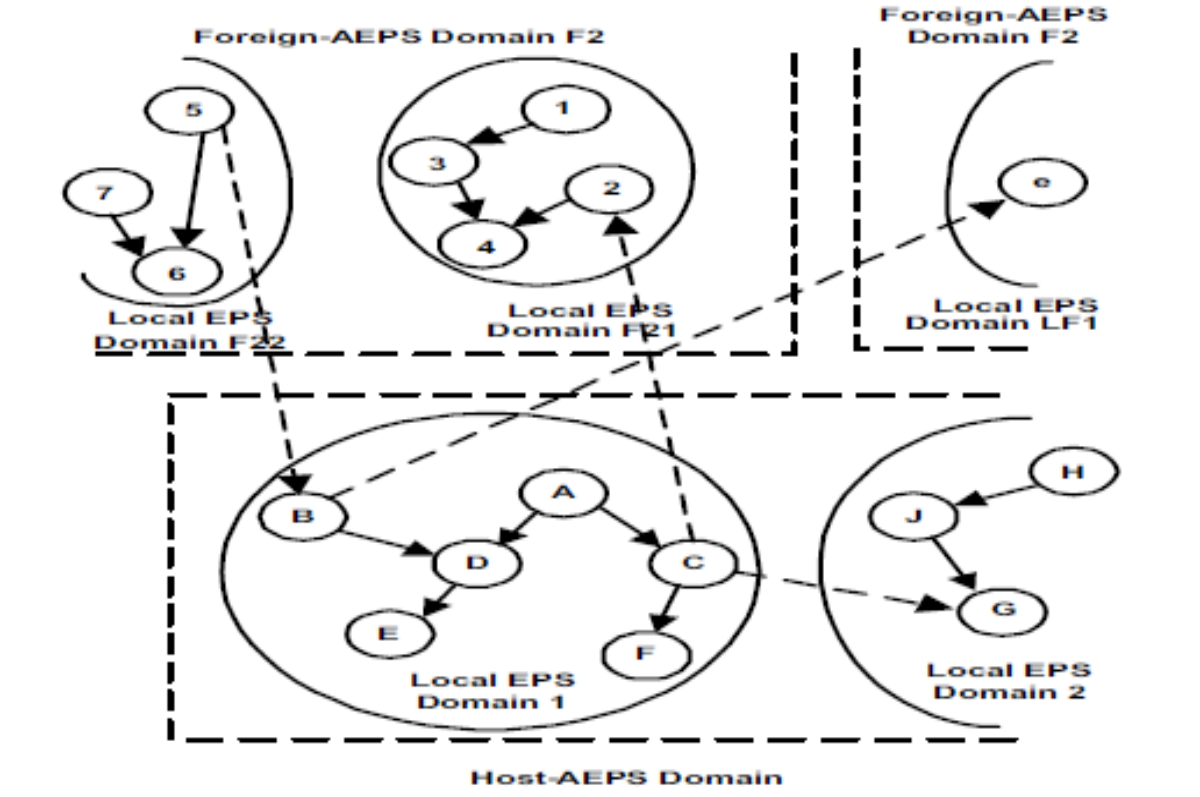


Figure. 3 Role Hierarchy for Inter AEPS Domains[1]

Request 1:

Reduce the power flow in Local EPS Domain 1 of Host-AEPS

Security Execution:

Accepted. User has role C that can directly implement the control of power flow in Domain 1 of Host-AEPS

Illustration of Authentication of Requests

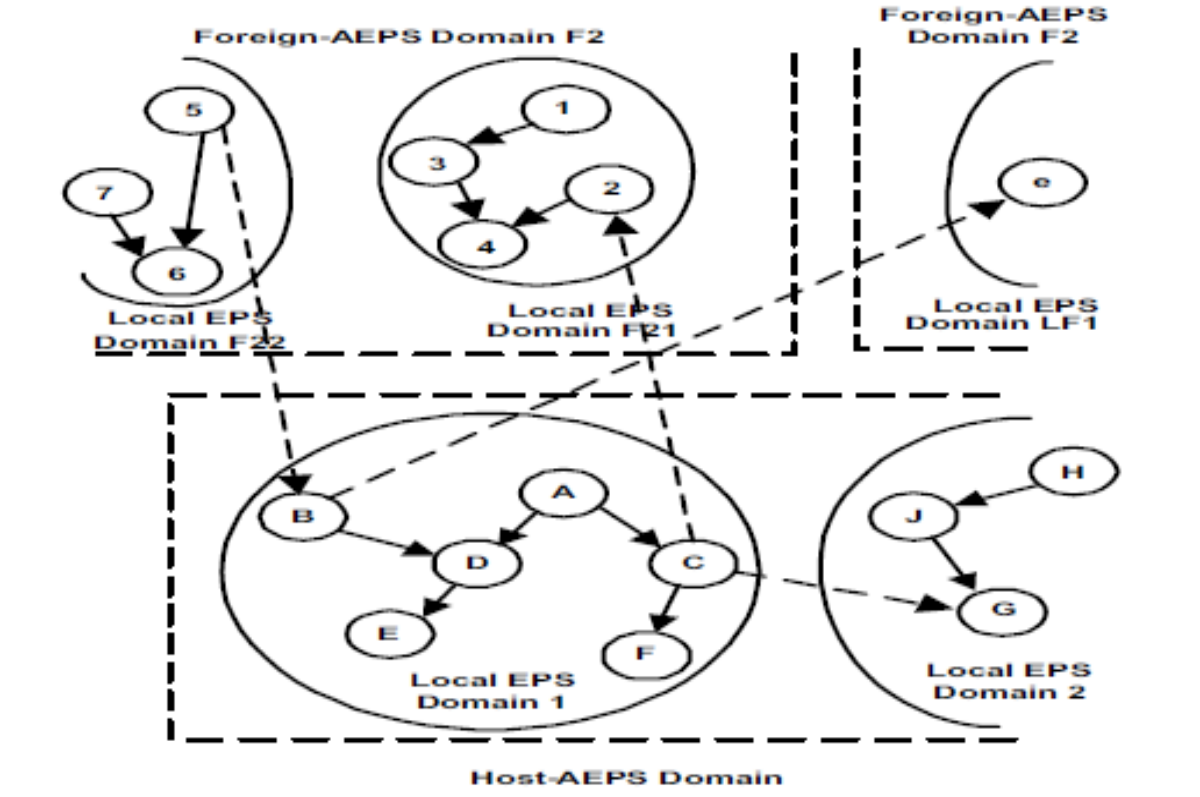


Figure. 3 Role Hierarchy for Inter AEPS Domains[1]

Request 2:

Analyze bus voltage fluctuation in Domain 1 of Host-AEPS

Security Execution:

Denied. All the roles user has cannot reach role E that is responsible for substation analysis in Domain 1 of Host-AEPS

Illustration of Authentication of Requests

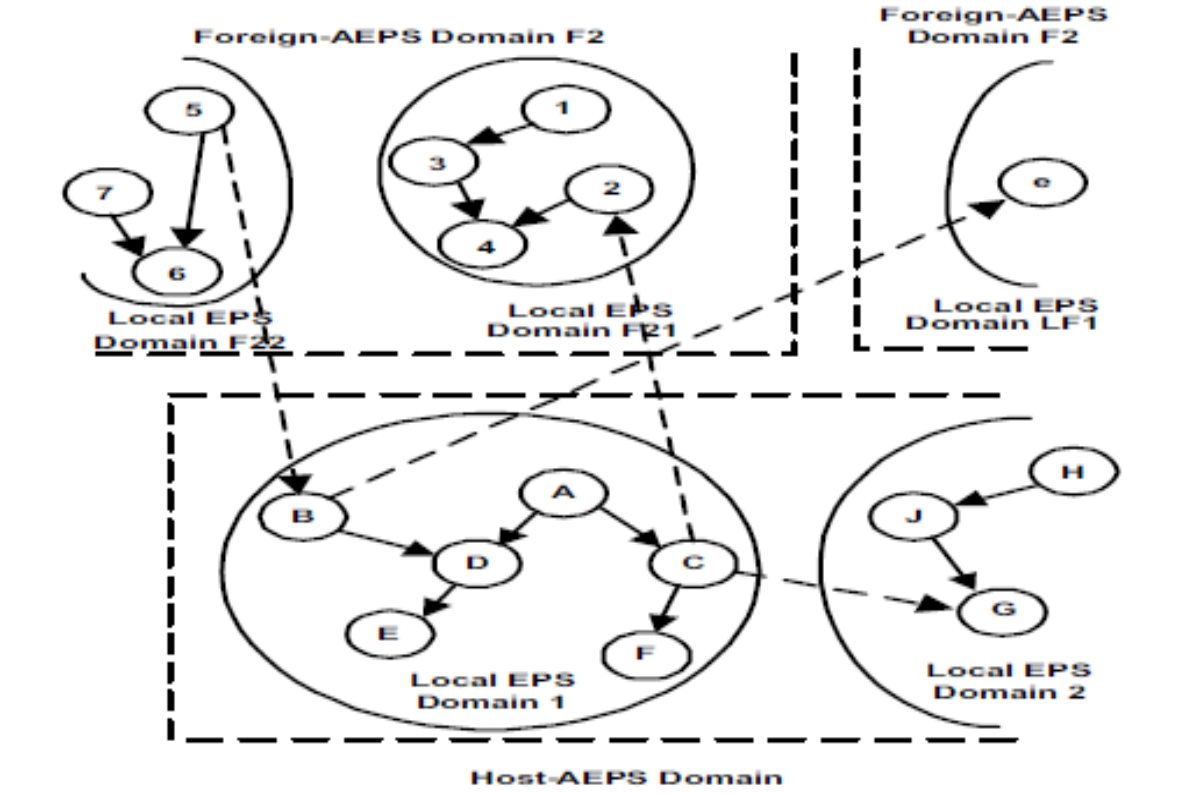


Figure. 3 Role Hierarchy for Inter AEPS Domains[1]

Request 3:

Obtain bus voltage data in Domain F21 of the neighboring Foreign-AEPS

Security Execution:

Accepted. User has role C with access privilege to role 2 of Domain F21, and role 2 is a parent role of role 4 in Domain F21

Security Authentication of Stability Control

1. Basic smart-grid stability control strategy:

- Continuously evaluate the power-grid real-time performance particularly regarding any contingencies, using state-of-art DSP and computer networking technologies
- Carry out corrective actions to restore a sufficient margin

increase of spinning reserve, reschedule of generation, decrease of allowed power transfer, shedding of non-critical loads, etc.

Security Authentication of Stability Control

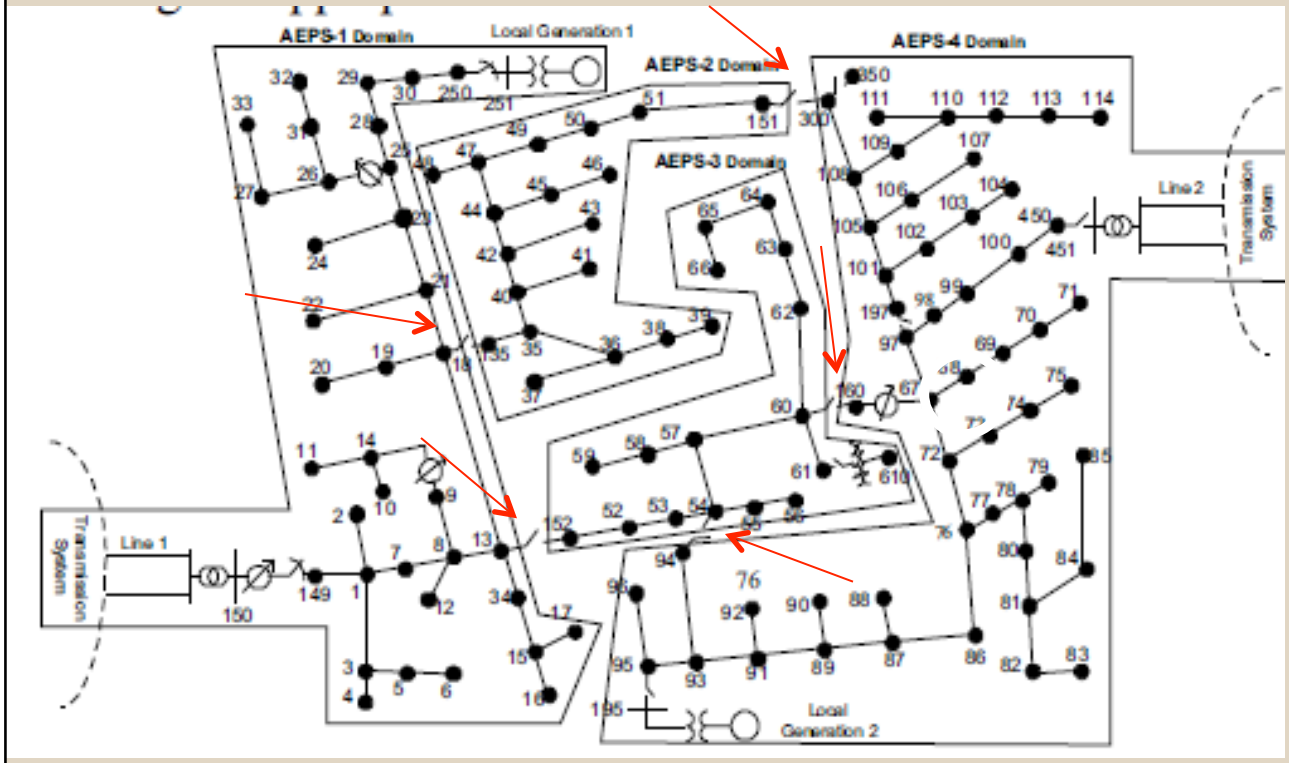
2. Security Authentication of Stability Control:

- The most important operations
- Prior to executing any requests or correcting instability conditions, all action requests must go through strict security checks for examining not only the reliability of the requests but also the trustworthiness of the issuers of the requests.

3. Formulation of AEPS Domain

- The computer network is divided into AEPS network domains

Security Authentication of Stability Control



- The division is based on the configuration of the circuit as each domain can be physically isolated when open disconnects around that domain

Fig. 4 AEPS domains defined for the IEEE circuit[1]

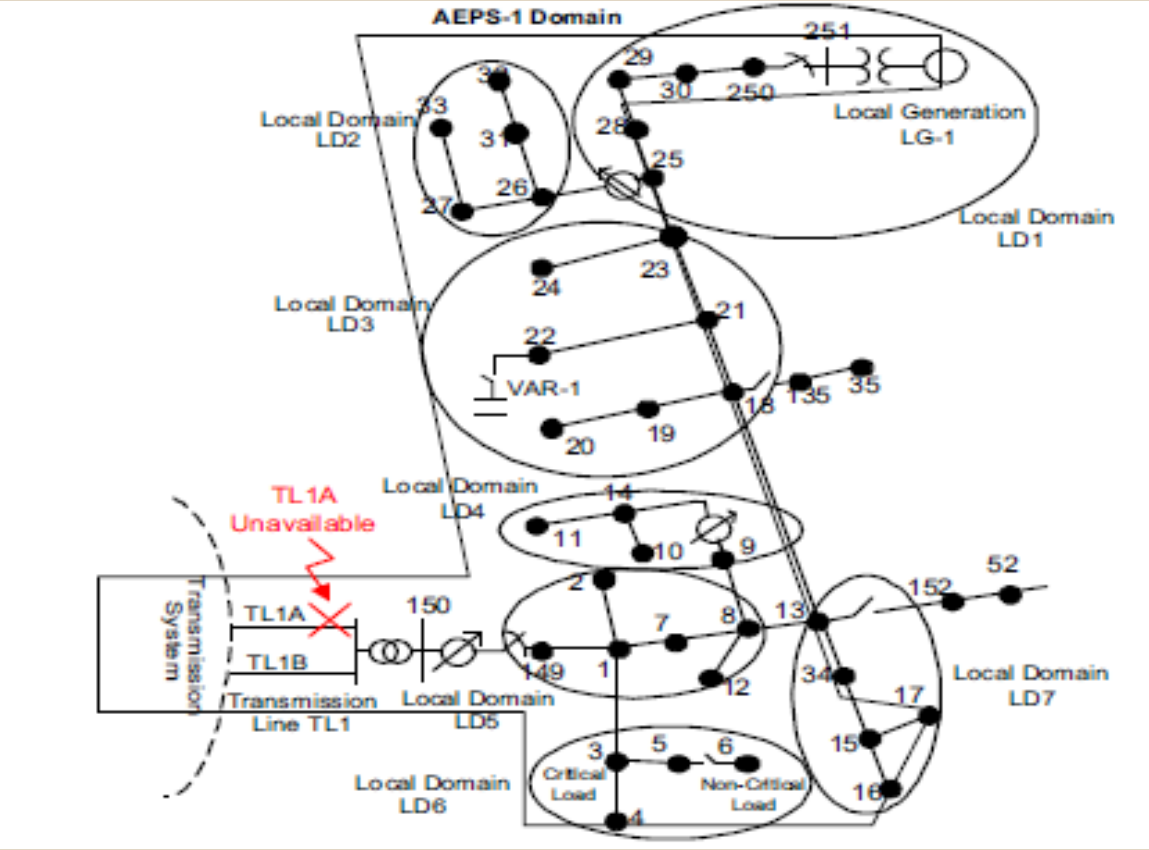
Security Authentication of Stability Control

4. Formulation of Local EPS Domains

- Each AEPS domain is subdivided into several local domains.
- This division is based on two aspects, the circuit specifics and the network design for stability control:

➢ A maximum of 7 circuits / nodes for one local domain is selected
➢ Each monitors the circuits that are located closely in one section
➢ Each should include circuits that are critical from the monitoring point of view, if physically feasible.
➢ For cost-effective implementation, the number of local domains should be minimized.

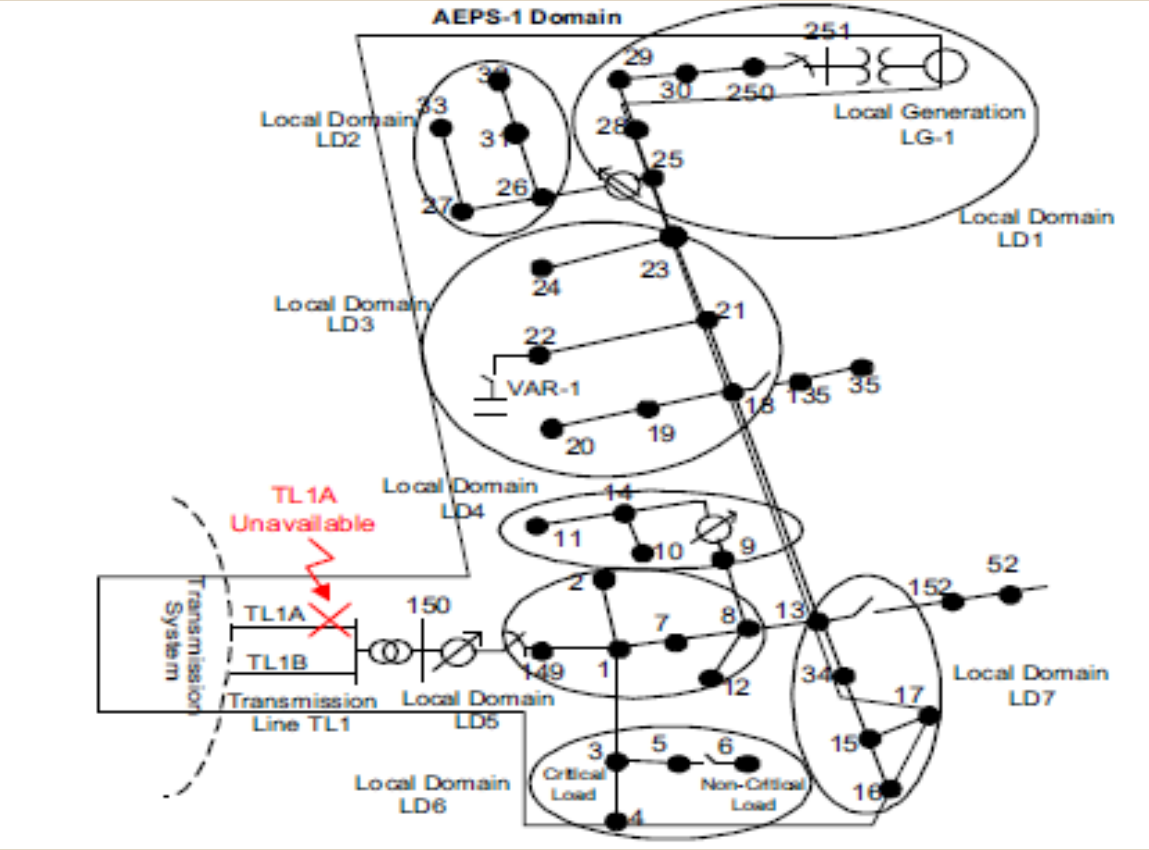
Security Authentication of Stability Control



- LD 1:
  - Five node circuits
  - Node 250 disconnect and Node 25 regulator are critical elements
- LD 3:
  - Seven node circuits
  - Node 18 connecting to AEPS-2 is critical element

Fig. 5 Local domains defined for AEPS-1 Domain[1]

Security Authentication of Stability Control



- Case studies
  - TL1A unavailable
  - Excite dynamics
  - Angle, voltage
- LG-1 excitation controller
- VAR compensator controller

Fig. 5 Local domains defined for AEPS-1 Domain[1]

Conclusion

- The paper proposed a new strategy for computer network security authentication of smart-grid operations. The authentication covers multiple security domains in a new security architecture designed for smart power grids.
- The paper presented the procedure of security checks and authentications of commands requests for operations in the host AEPS and neighboring AEPS. Also, it introduced the principles of dividing into the AEPS domains
- The paper presented network security authentication for requests of actions for smart-grid stability controls.

My Assessment

- Pros:
  - Analysis of the situation of current power system
  - Clear demonstration of the power grid security architecture
  - Quite a lot of examples and case studies, clearly presented the request and corresponding executions
- Cons:
  - Lots of case studies, less explanation
  - No details about how the strategy realize

Reference

- [1] H. Cheung, A. Hamlyn, C. Yang, Network Security Authentication of Power System Operations, 2008 IEEE
- [2] A. Hamlyn, H. Cheung, T. Mander, L. Wang, C. Yang, R. Cheung, Computer Network Security Management and Authentication of Smart Grids Operations, 2008 IEEE
- [3] T. Mander, F. Nabhani, L. Wang, R. Cheung, "Open-Access-Compatibility Security Layer for Enhanced Protection Data Transmission", 07GM0458, IEEE PES General Meeting, Tampa, Florida, USA, June 24-28, 2007.

TEXAS A&M UNIVERSITY

Thank you!!

Questions~