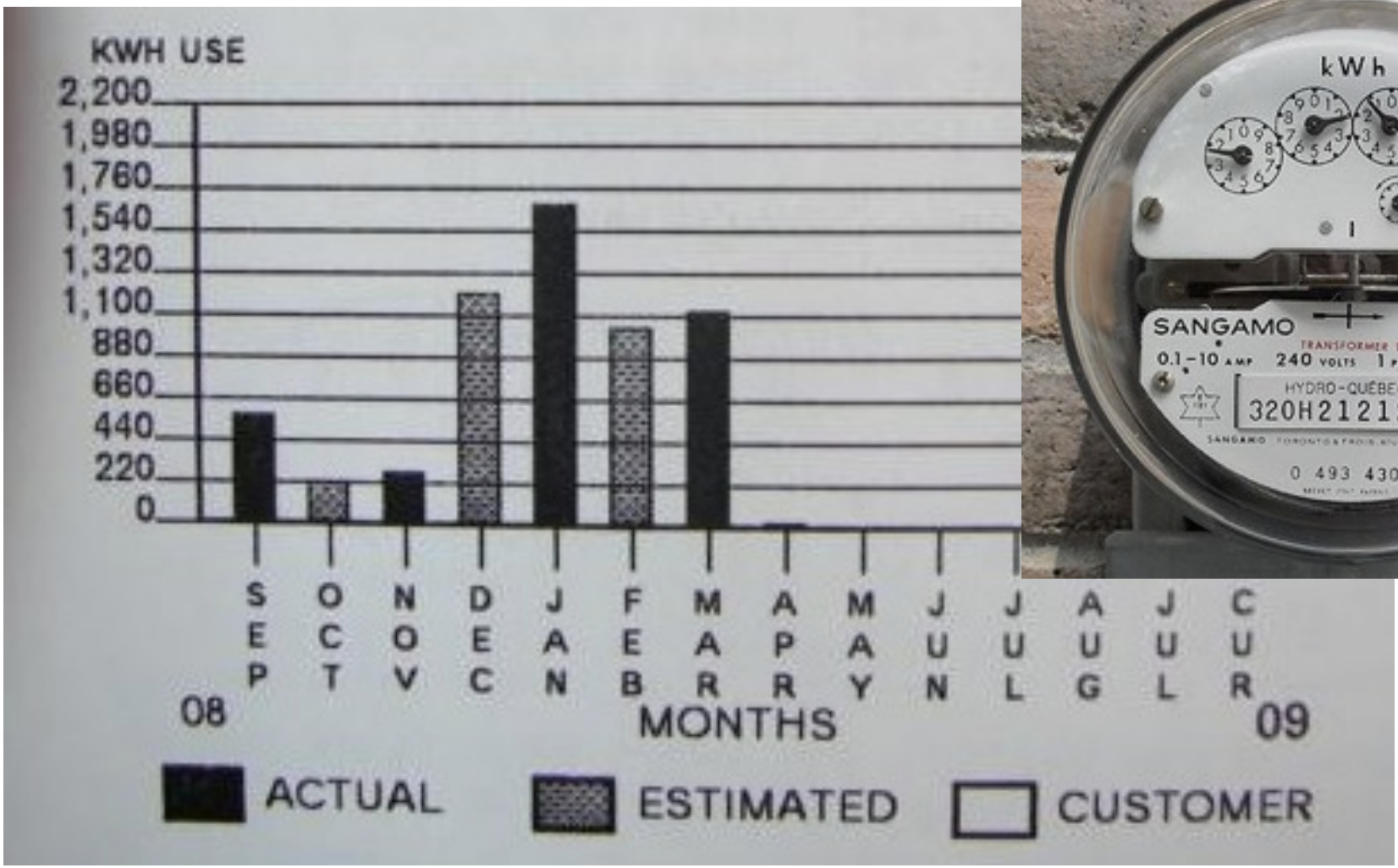
Multi-vendor Penetration Testing in the Advanced Metering Infrastructure: Future Challenges

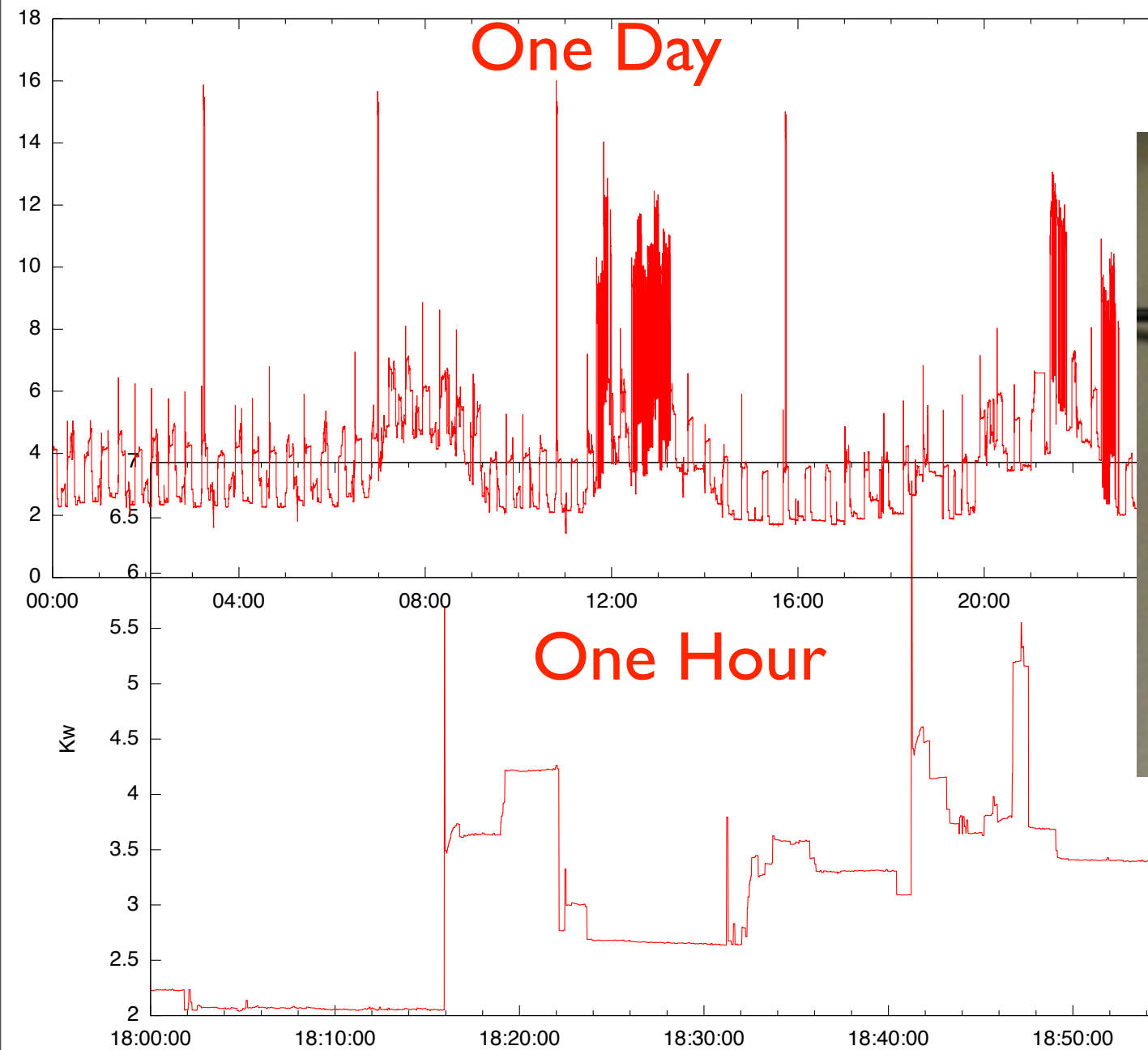
DIMACS Workshop on Algorithmic Decision Theory for the Smart Grid

Stephen McLaughlin - Penn State University

Meter Data Management (for the last 100 years)



Meter Data Management (now and in the near future)



Meter Data Management (now and in the near future)

PENNSTATE

Peak Transient

One Day

Peak Usage

Hourly Average

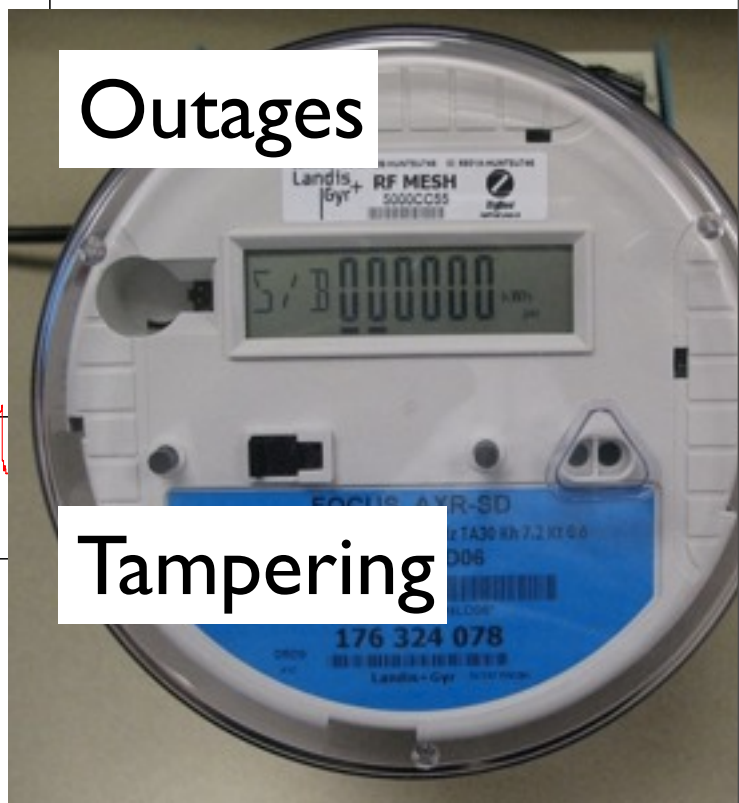
Time of Use

Repetitive Features

One Hour

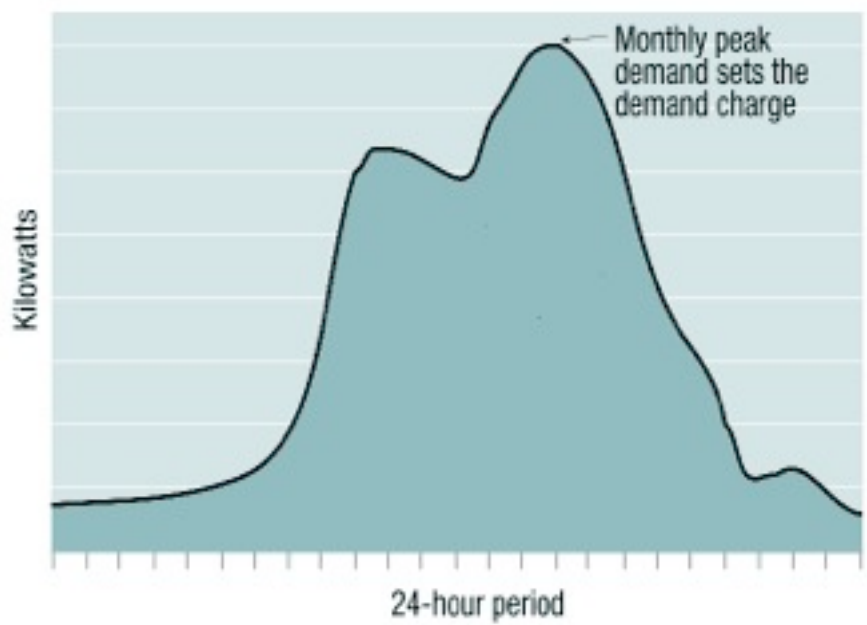
Power Quality over time

Types of appliances



AMI - the justification

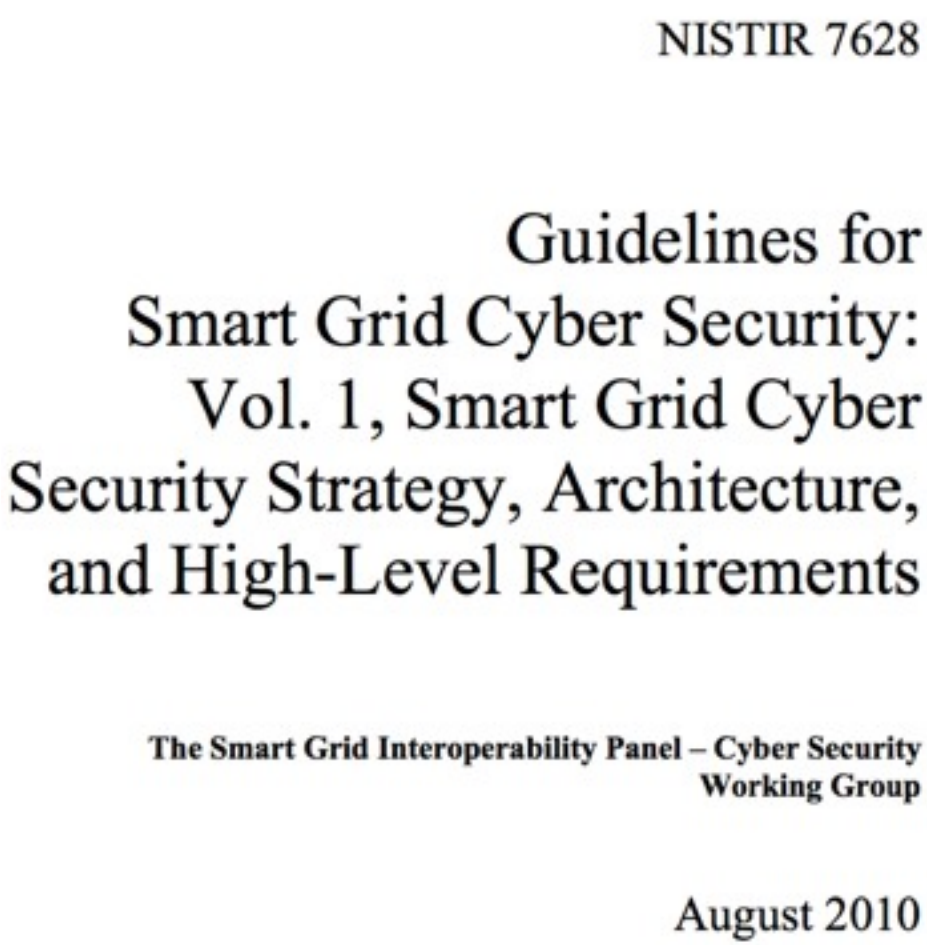
- Automated Meter Reading
  - Pre-smart meter automated reading and outage notification
  - Now expanding to Internet-connected SCADA systems
- Dynamic pricing schemes
  - Time Of Use (peak load management)
  - Maximum demand
  - Demand response
- Flexible energy generation
  - Enable consumer generation
  - Alternate energy sources



AMI - the concerns

- What should we be concerned about?
  - Accuracy/Fraud
  - Consumer privacy
  - National security

Penetration Testing AMI


NISTIR 7628

Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements

The Smart Grid Interoperability Panel – Cyber Security Working Group

August 2010

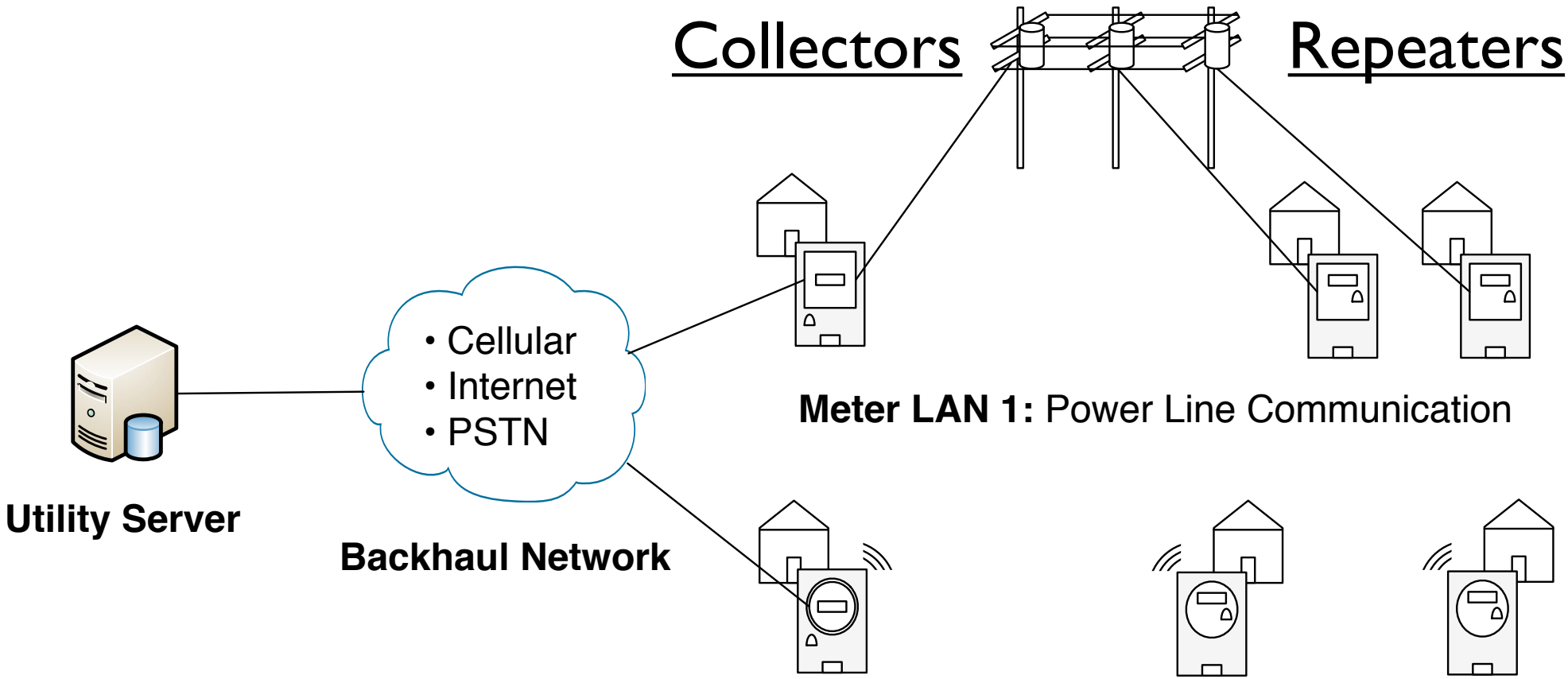
"The organization assesses the security requirements in the Smart Grid information system on an organization-defined frequency to determine the extent the requirements are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the Smart Grid information system."

-p 117

Vulnerability Assessment

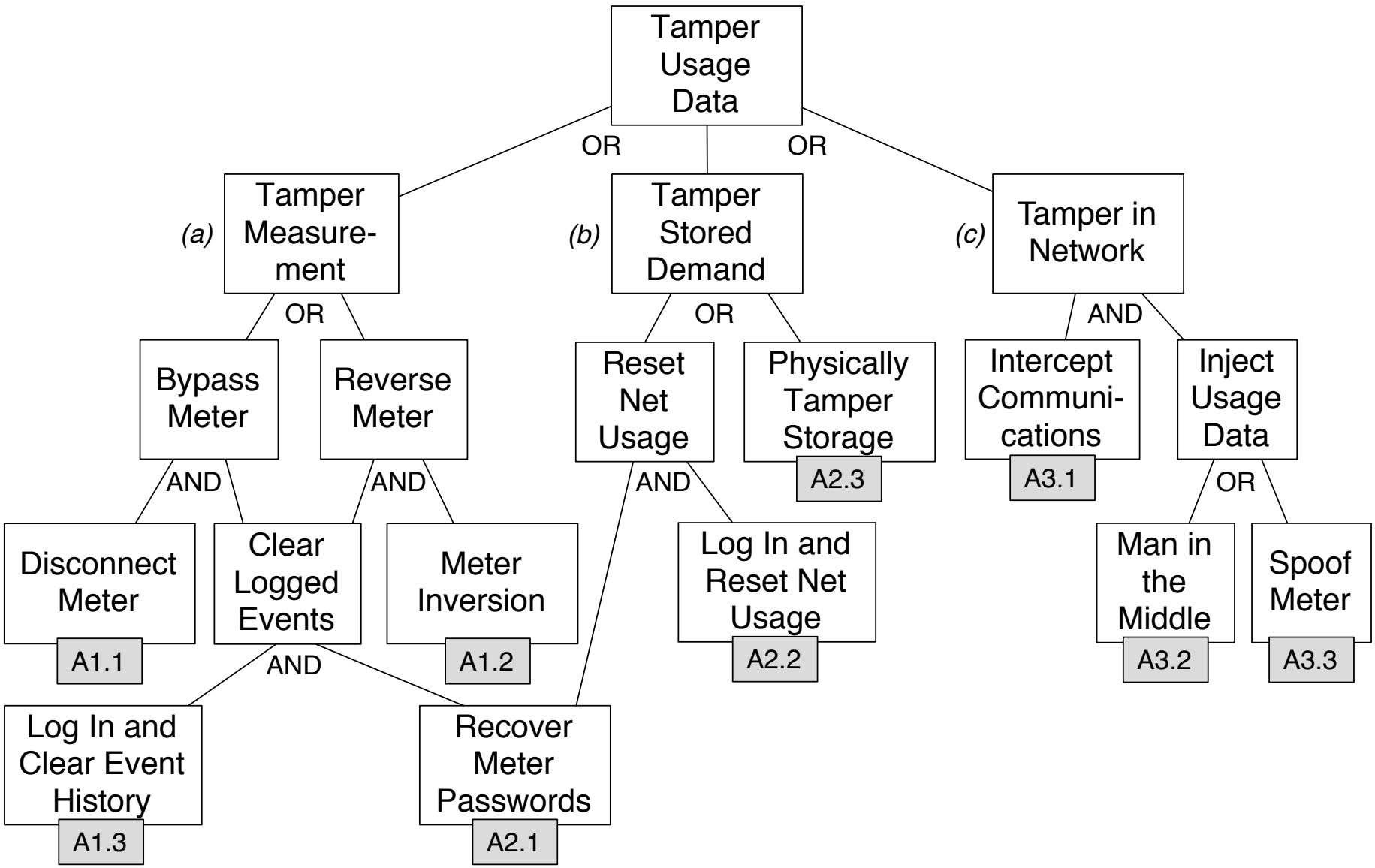
- Penetration testing: the art and science of breaking systems by applying attacker tools against live systems.
  - *Destructive research* attempts to illuminate the exploitable flaws and effectiveness of security infrastructure.
- Bottom line Q/A
  - Q: why are we doing this?
  - A: part of Lockheed-Martin grant to aid energy industry in identifying problems before they are found "in the wild".
  - Q: what are we doing?
  - A: evaluating a number of vendor products in the lab that are used in *neighborhood-level* deployments, i.e., we only look at the meters and collectors.

AMI Architectures



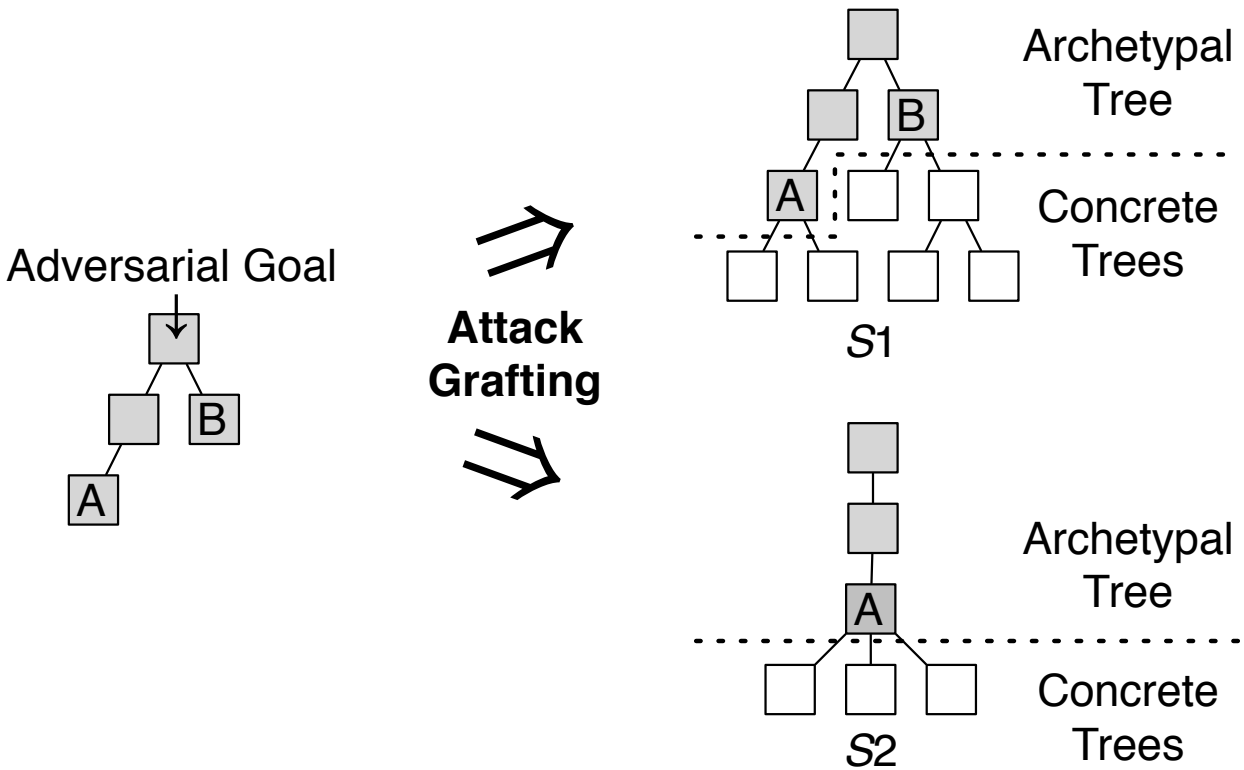
Attack Trees

A means for pen-testing planning



Archetypal Trees

- *Idea*: can we separate the issues that are vendor independent from those that are specific to the vendor/ device, e.g., access media?



- ... then reuse an archetypal tree as a base for each vendor specific *concrete tree*.

Pen Testing via Archetypal Trees

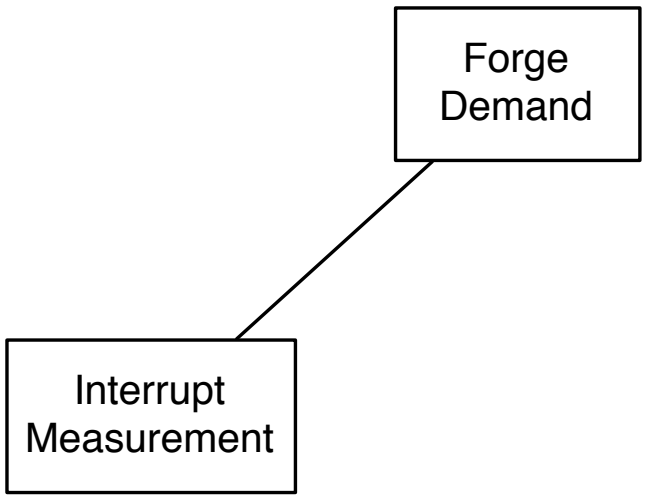
PENNSTATE

1. capture architectural description
2. construct archetypal trees (for each attacker goal)
3. capture vendor-specific description (for SUT)
4. construct concrete tree
5. perform penetration testing and graft leaves toward goals

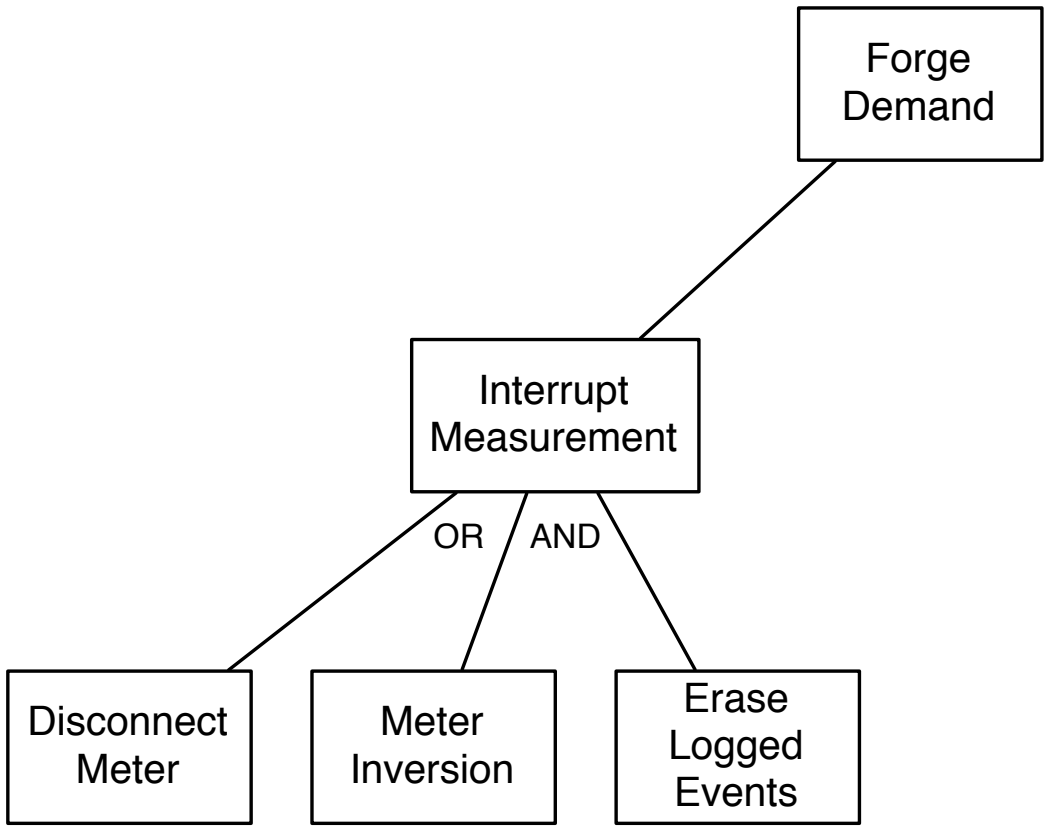
This paper: 3 Attack trees: fraud, DOS, disconnect, 2 "systems under test" (SUT)

Construction of Archetypal Trees

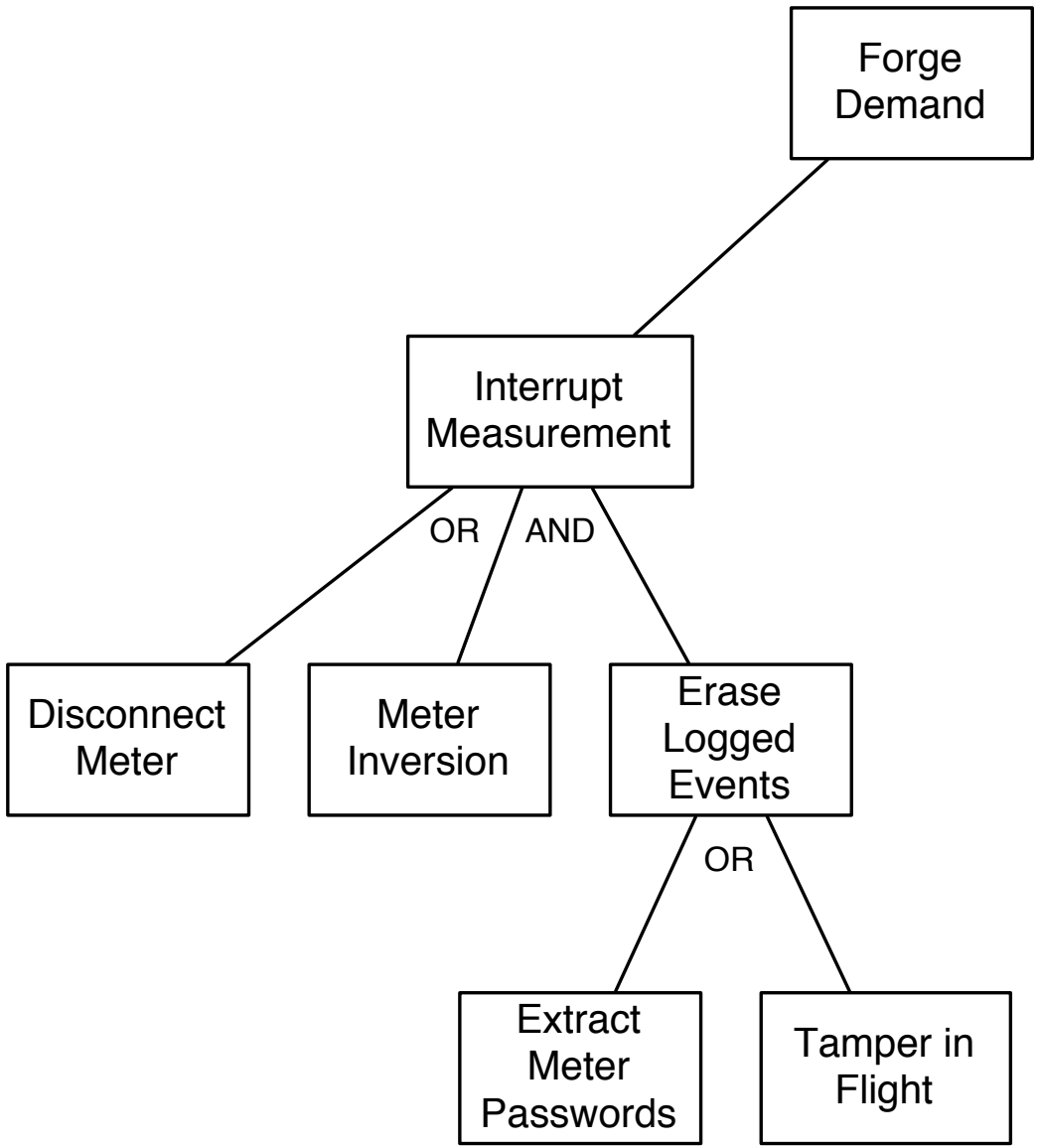
Construction of Archetypal Trees



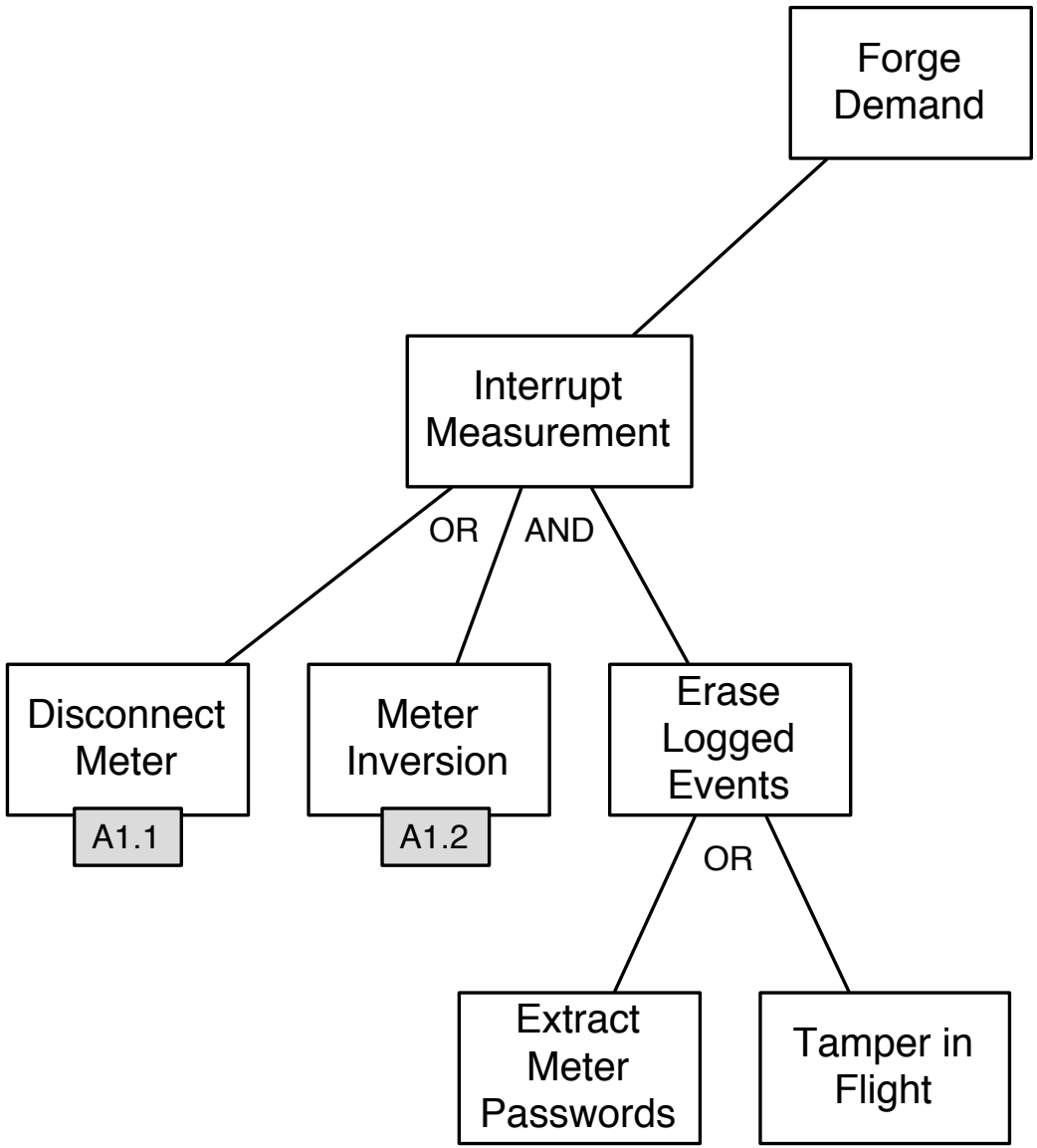
Construction of Archetypal Trees



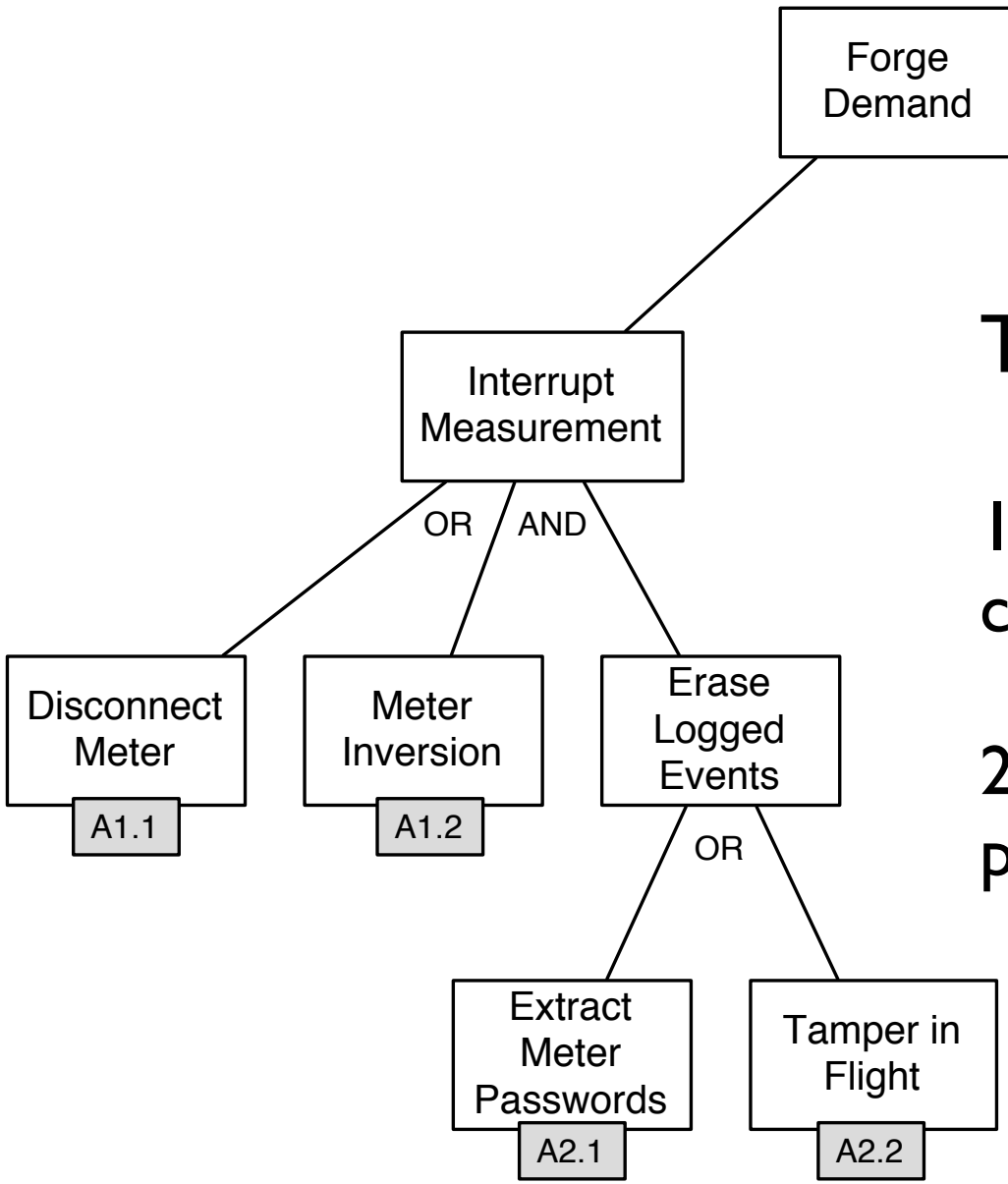
Construction of Archetypal Trees



Construction of Archetypal Trees



Construction of Archetypal Trees



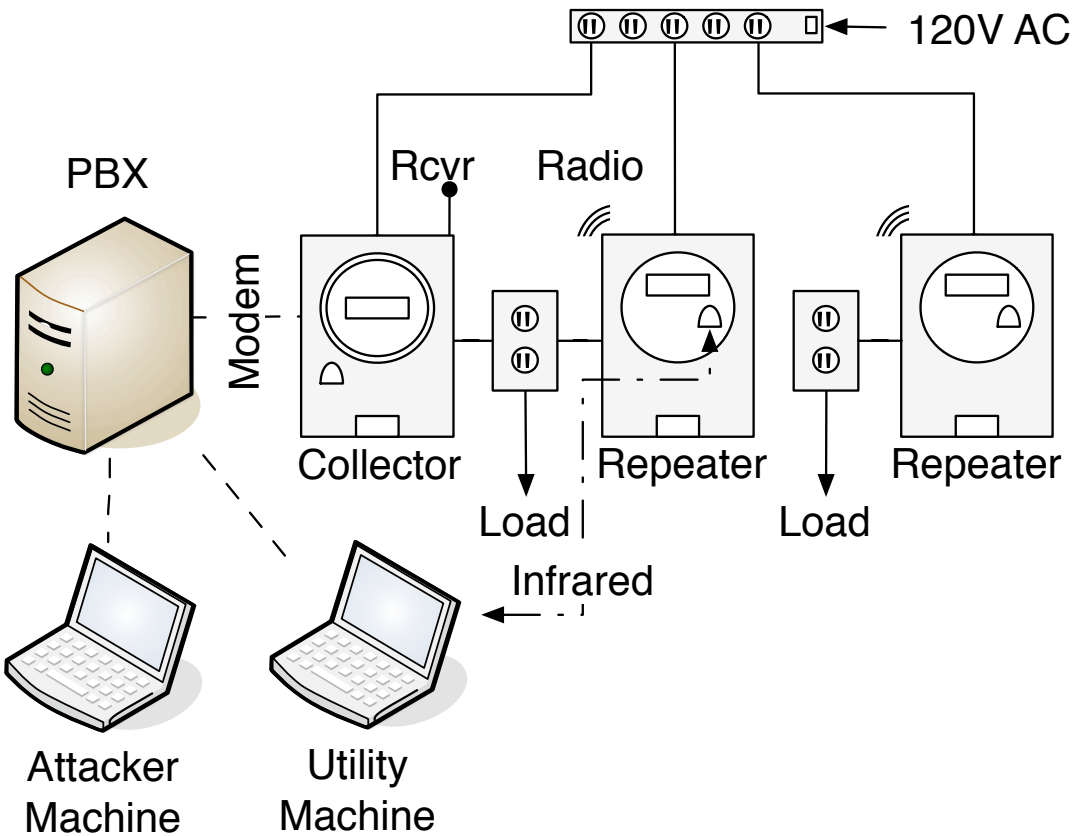
Two rules for termination:

1. Attack is on a vendor-specific component

2. Target may be guarded by a protection mechanism

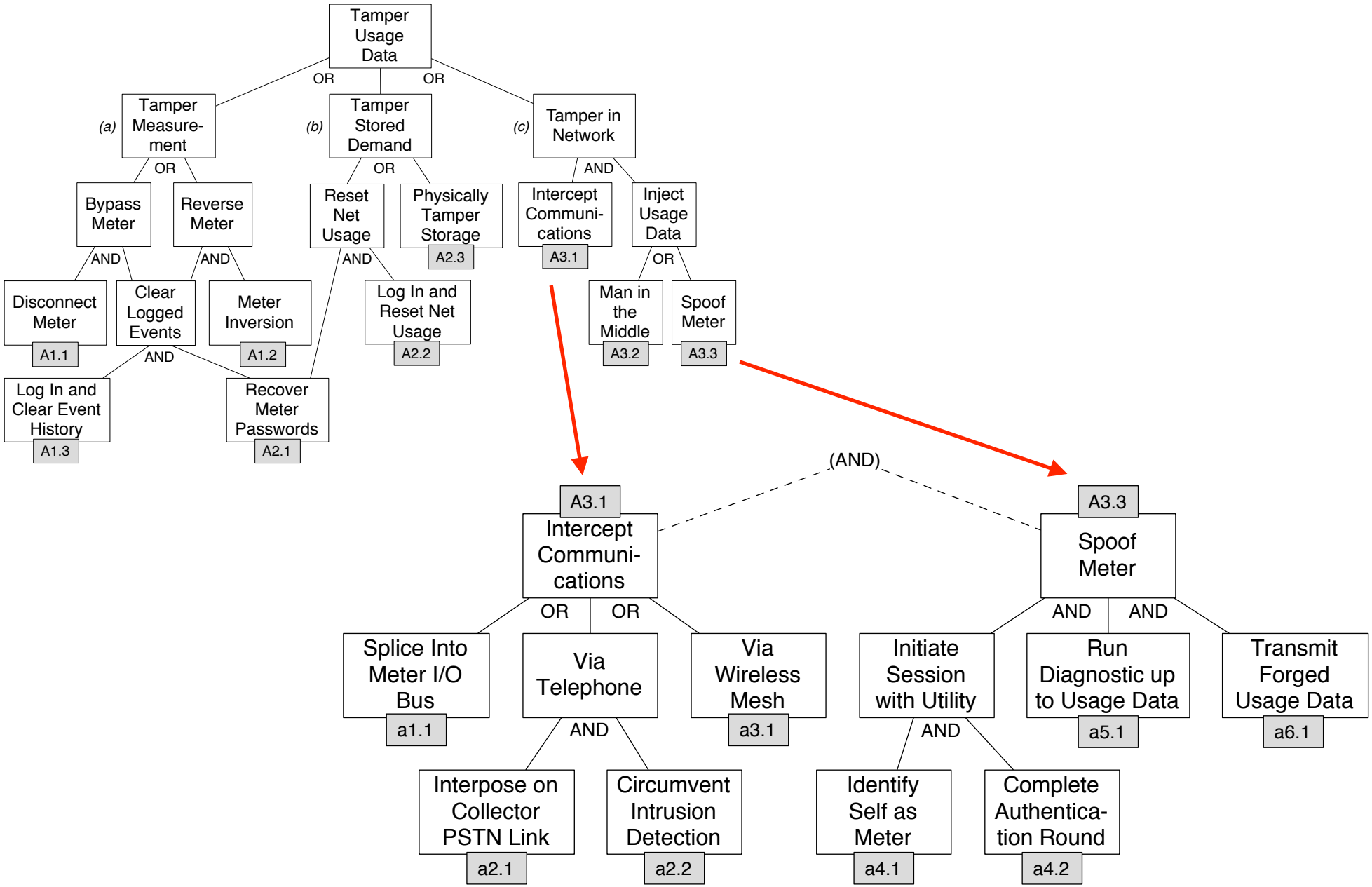
System Under Test

- PSTN connected collector
  - ANSI C12.21
  - "intrusion detection"



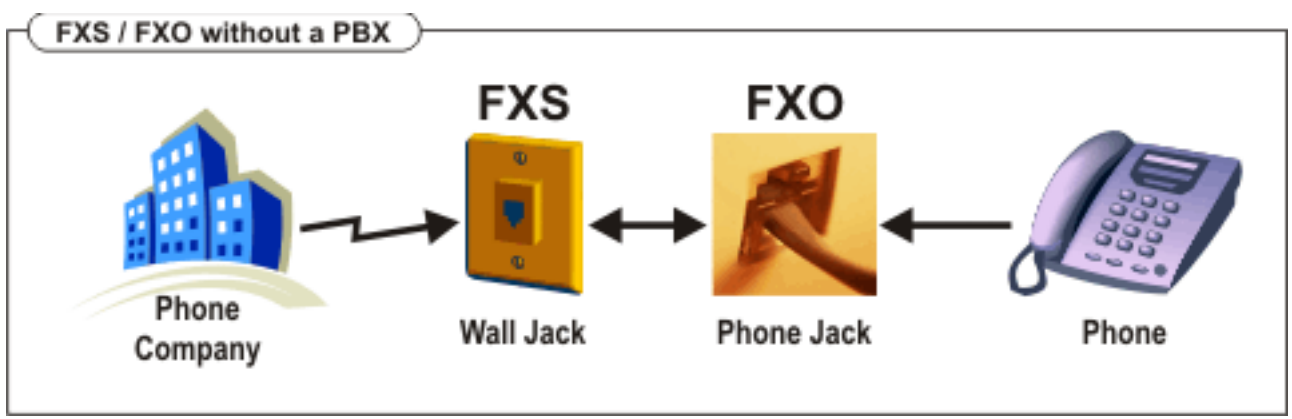
- 900 MHz wireless mesh collector/meter network
- Infrared "near-field" security for configuration port

Fraud Concrete

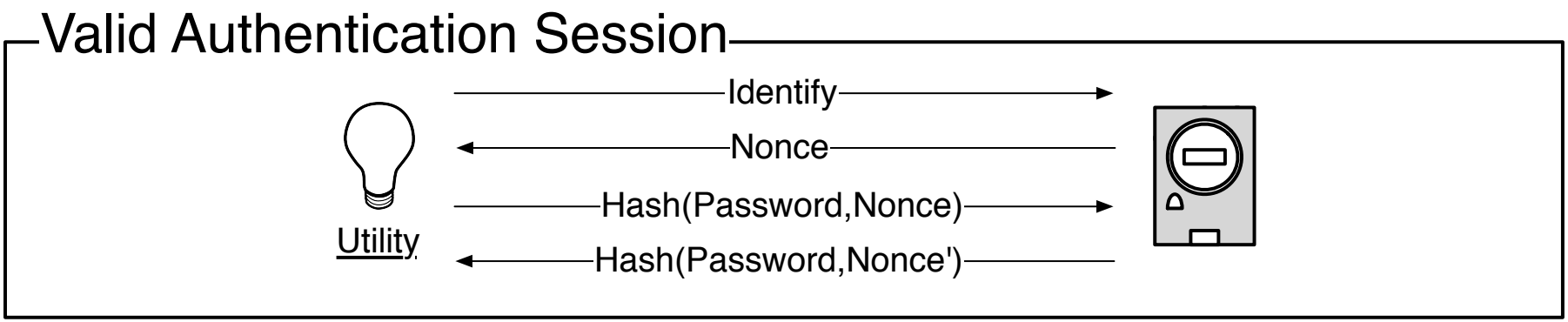


Enabling Attacks (Fraud)

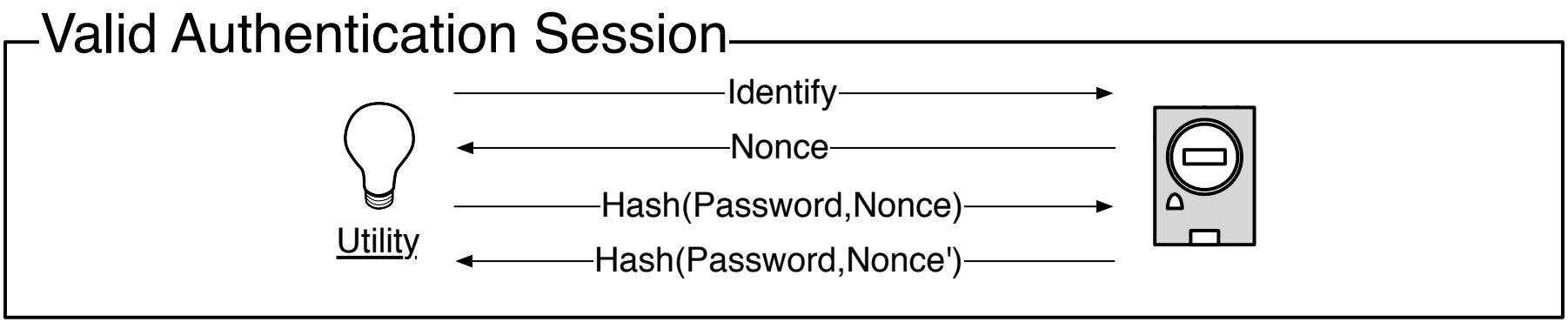
- Defeating modem "*intrusion detection*"
  - "off hook" events on the line are detected by sensing presence Foreign Exchange Office (FXO) of dial-tone voltage on the line.
  - current calls are dropped if off hook is detected
  - such events can simply be suppress easily by preventing voltage from arriving at the FXO



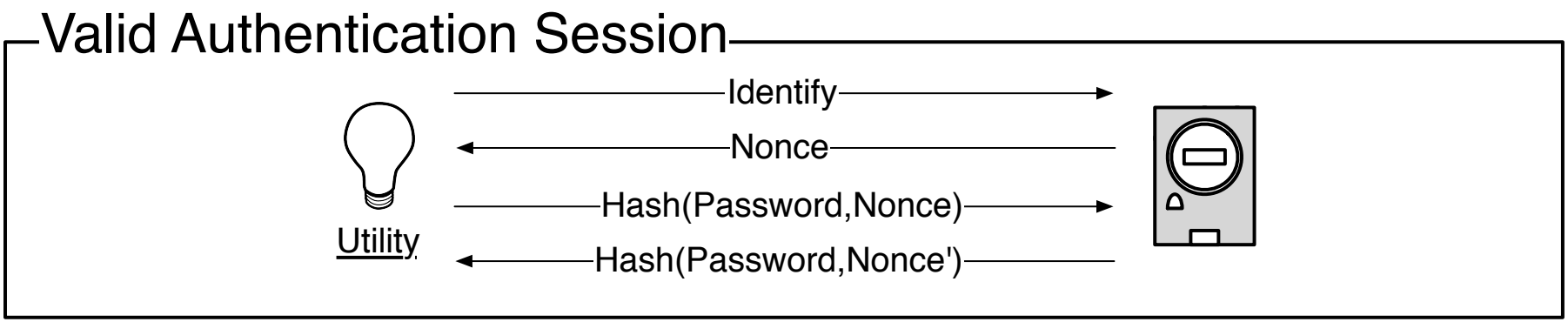
Enabling Attacks (Fraud)



Enabling Attacks (Fraud)

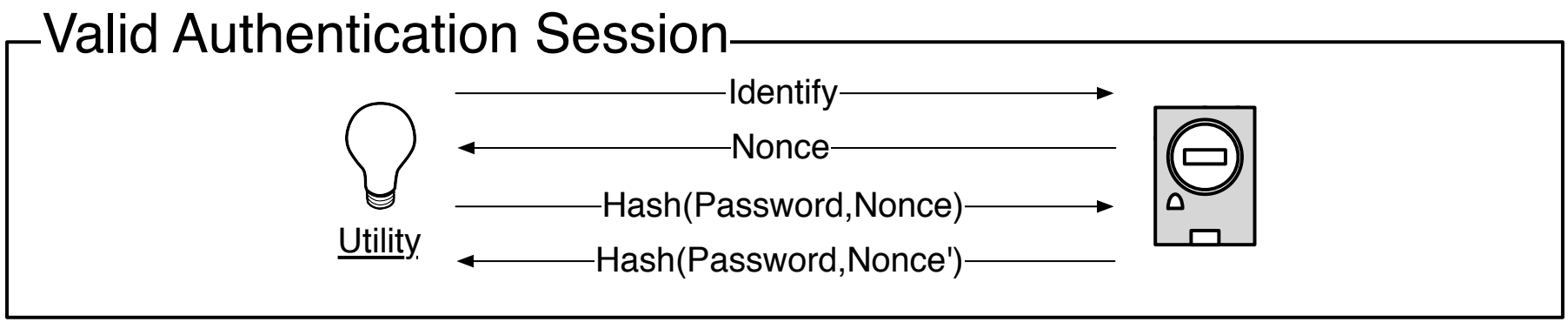


Enabling Attacks (Fraud)

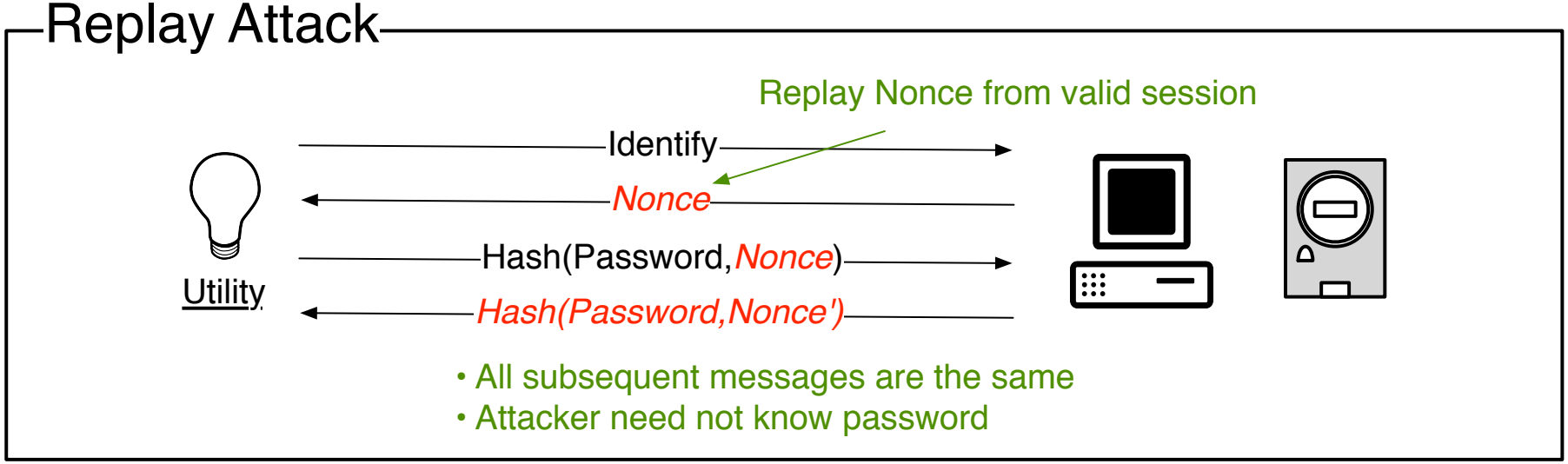


- *Replay attack*: I can replay the nonce from a previous session to impersonate the meter.

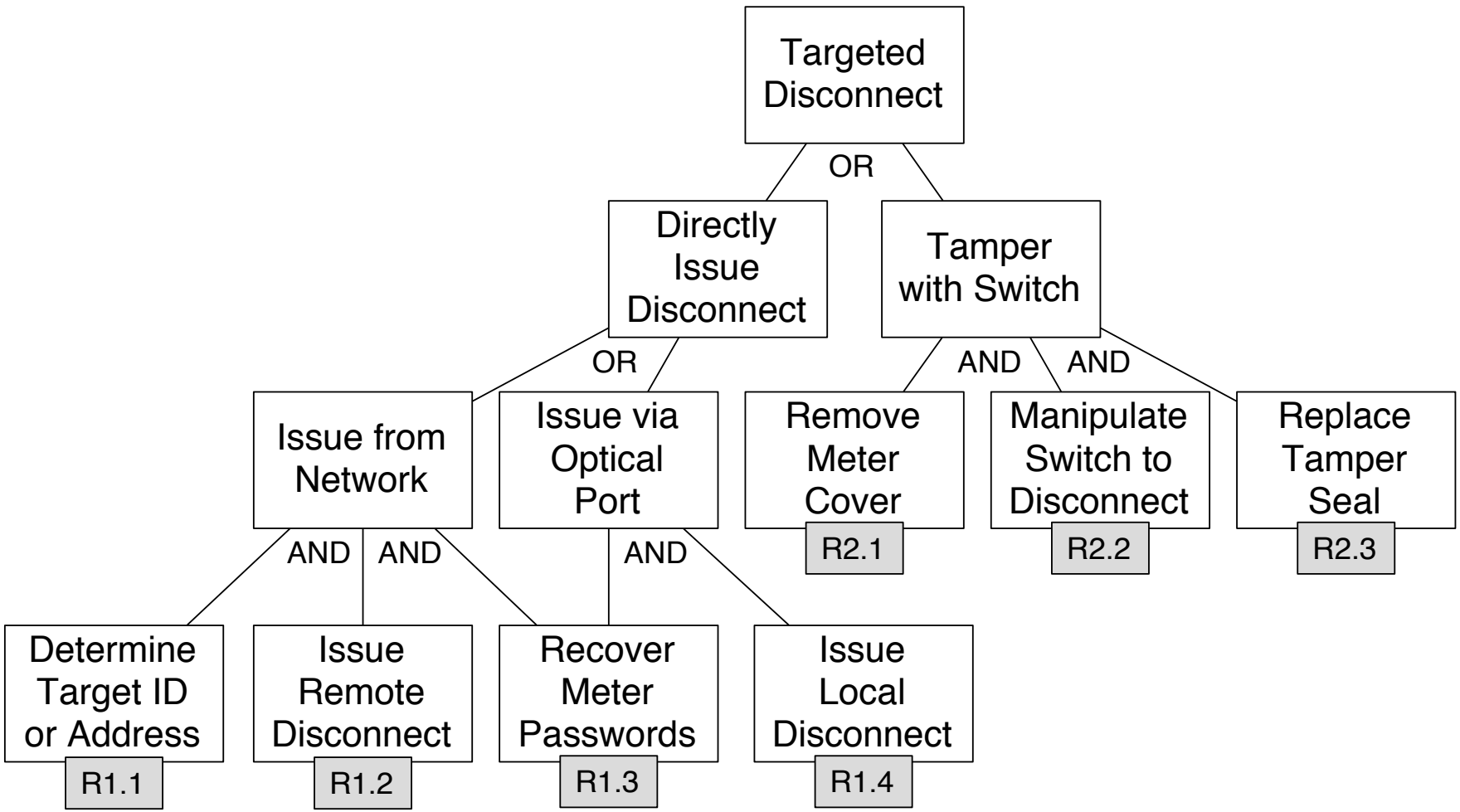
Enabling Attacks (Fraud)



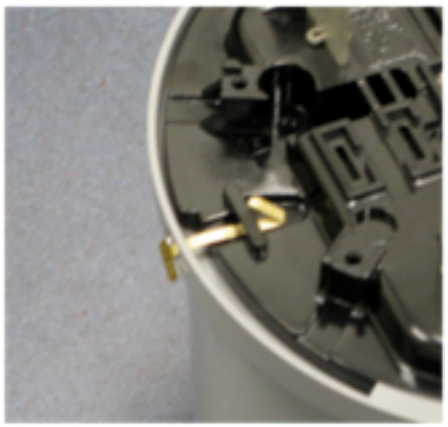
- *Replay attack*: I can replay the nonce from a previous session to impersonate the meter.



Targeted Disconnect AT



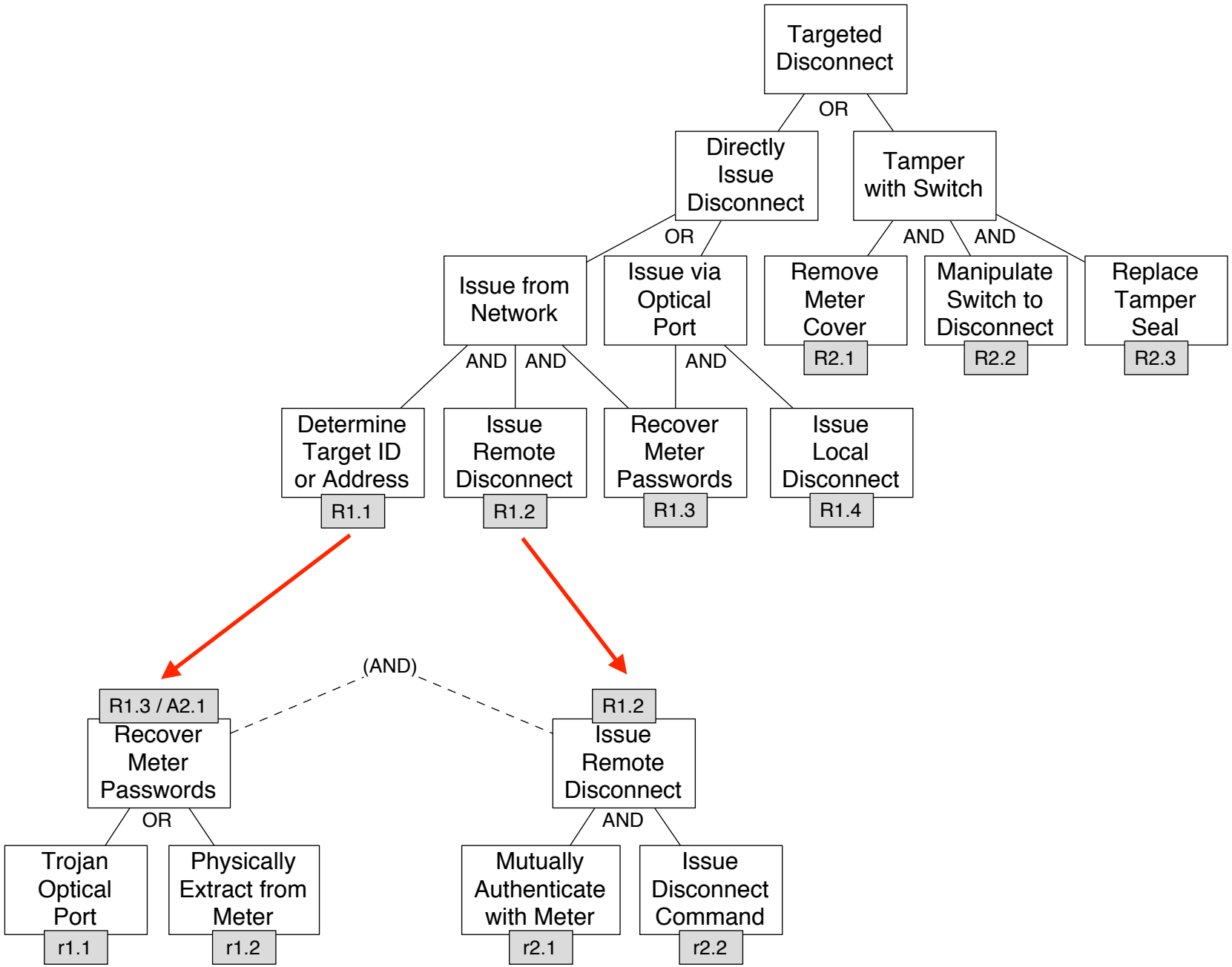
Enabling Attacks (Disconnect)



- Physical tamper "evidence"
  - Limited tamper seals, *which enables ...*
- Passwords are stored in EEPROM
  - Physical access to the device can yield all of the data held in non-volatile memory, *which enables ...*
- Authentication secrets derived from passwords
  - Bypass the authentication system, *which enables ...*
- Issue disconnect command.

Note: if you can break the dependency chain, you can prevent the attack, i.e., simple measures can often prevent complex attacks.

Disconnect Concrete



Attacks Summary

Table 1: Summary of concrete attacks and discovered vulnerabilities for each adversarial goal.

Ref.	Description	Enabling Feature or Vulnerability
	Energy Fraud in S1	
a2.1	Interpose between utility and collector	Telephone line may be accessible.
a2.2	Defeat modem intrusion detection	The mechanism cannot detect an FXS.
a4.1	Identify self as meter	A meter's ID is printed on its faceplate.
a4.2	Complete authentication round	Lack of nonce-tracking allows replayed authentication.
a5.1	Run diagnostic up to usage data	Protocol is standardized.
a6.1	Transmit forged usage data	Usage data is not integrity protected.
	Denial of Service in S2	
d1.1	Determine collector ID	The ID is transmitted in the clear.
d1.2	Initiate association with utility	Initialization uses a simple `HELLO` message.
d1.3	Receive and drop packets	The utility uses the IP address of the initiator of the most recent association.
d2.1	Determine meter listening port	The collector is responsive to port scanning.
d2.2	Allocate sessions until failure	The collector does not handle many sessions robustly.
	Targeted Disconnect in S1	
r1.2	Physically extract passwords	Passwords are stored in the clear in EEPROM storage.
r2.1	Mutually authenticate with meter	The encryption key is derived from passwords.
r2.2	Issue disconnect command	Administrative software is commercially available.

Challenges: Logistical

- Uncooperative meter vendors
- Establishing standards for pen-testing, e.g. collections of attack trees
- Pen testing products, not deployments

Challenges: Methodological

- Enumerating adversarial goals (security is largely reactive)
- Being comprehensive in attack tree construction
- Automation of the process using existing modeling techniques such as threat modeling

Summary

- Horizontal penetration is now essential
  - Transitions of major infrastructure and critical systems mandates *external review of by-sector vulnerabilities*.
- Archetypal trees are a way to get there
  - Focus energies on adversarial efforts leading to goals
  - Approaches goals of certifications like Common Criteria
- Smart grid: Deployments outstripping our ability to understand and manage vulnerabilities
  - Society must get ahead of problems before they lead to potentially devastating events
  - Needs more back-pressure to improve deployed solutions.

Questions?

PENNSTATE

- Patrick McDaniel (mcdaniel@cse.psu.edu)
- Stephen McLaughlin (smclaugh@cse.psu.edu)
- Project Page: http://siis.cse.psu.edu/smartgrid.html

- Papers
  - Stephen McLaughlin, Dmitry Podkuiko, Adam Delozier, Sergei Miadzvezhanka, and Patrick McDaniel. *Multi-vendor Penetration Testing in the Advanced Metering Infrastructure*. Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC), December 2010. Austin, TX.
  - Stephen McLaughlin, Dmitry Podkuiko, Adam Delozier, Sergei Miadzvezhanka, and Patrick McDaniel. *Embedded Firmware Diversity for Smart Electric Meters*. Proceedings of the 5th Workshop on Hot Topics in Security (HotSec '10), August 2010. Washington, DC.
  - Stephen McLaughlin, Dmitry Podkuiko, and Patrick McDaniel. *Energy Theft in the Advanced Metering Infrastructure*. In the 4th International Workshop on Critical Information Infrastructure Security, September 2009. Bonn, Germany.