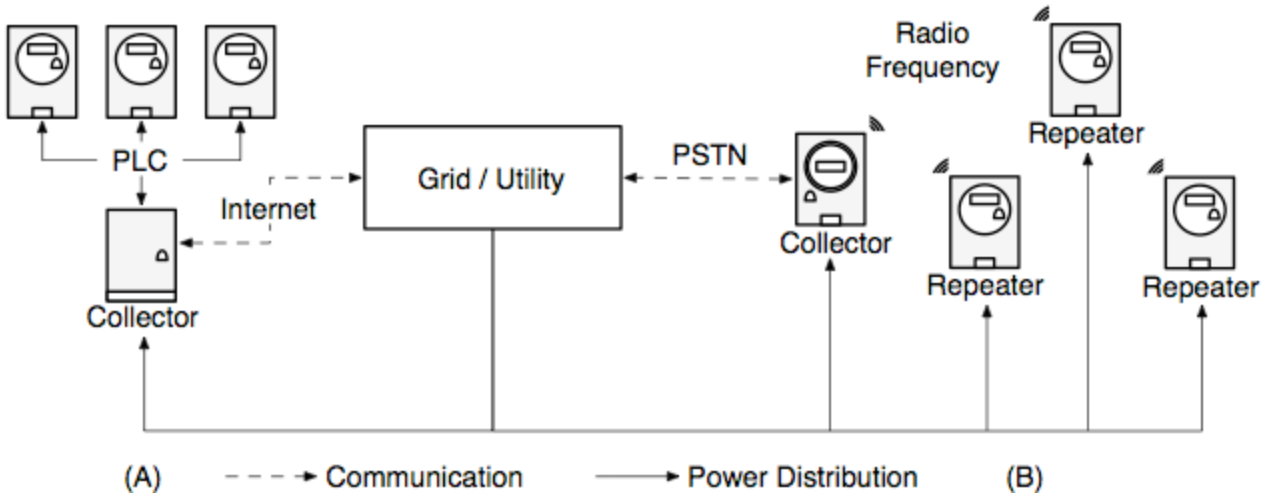
Identifying (and Addressing) Security and Privacy Issues in Smart Electric Meters

Patrick McDaniel and Steve McLaughlin
February 15, 2011
Los Alamos National Laboratory

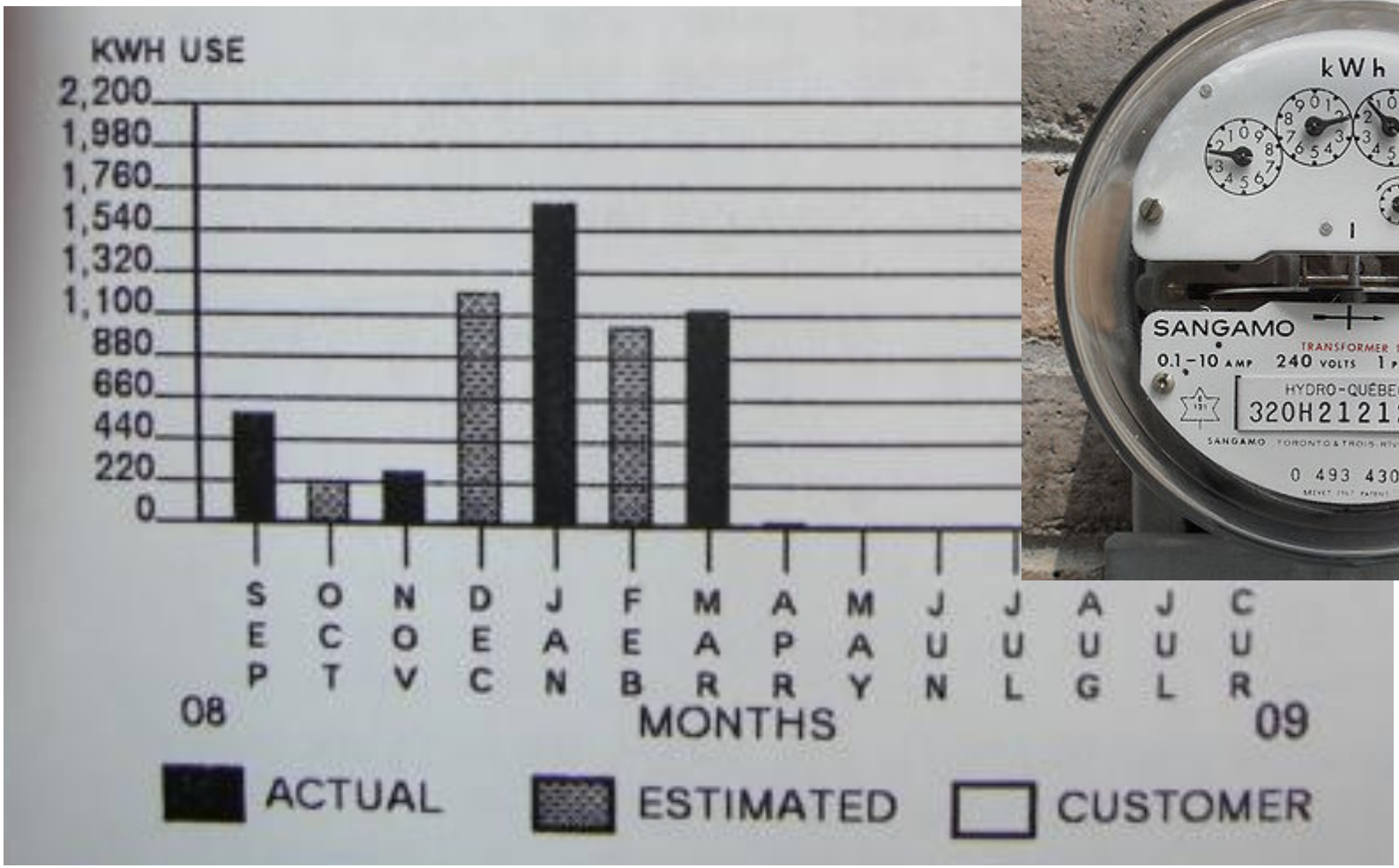
Smart Grid

- Digitization of electrical grid "control plane"
- Changes everything about how energy is consumed
  - accounting
  - event detection
  - recovery
  - planning
  - ...



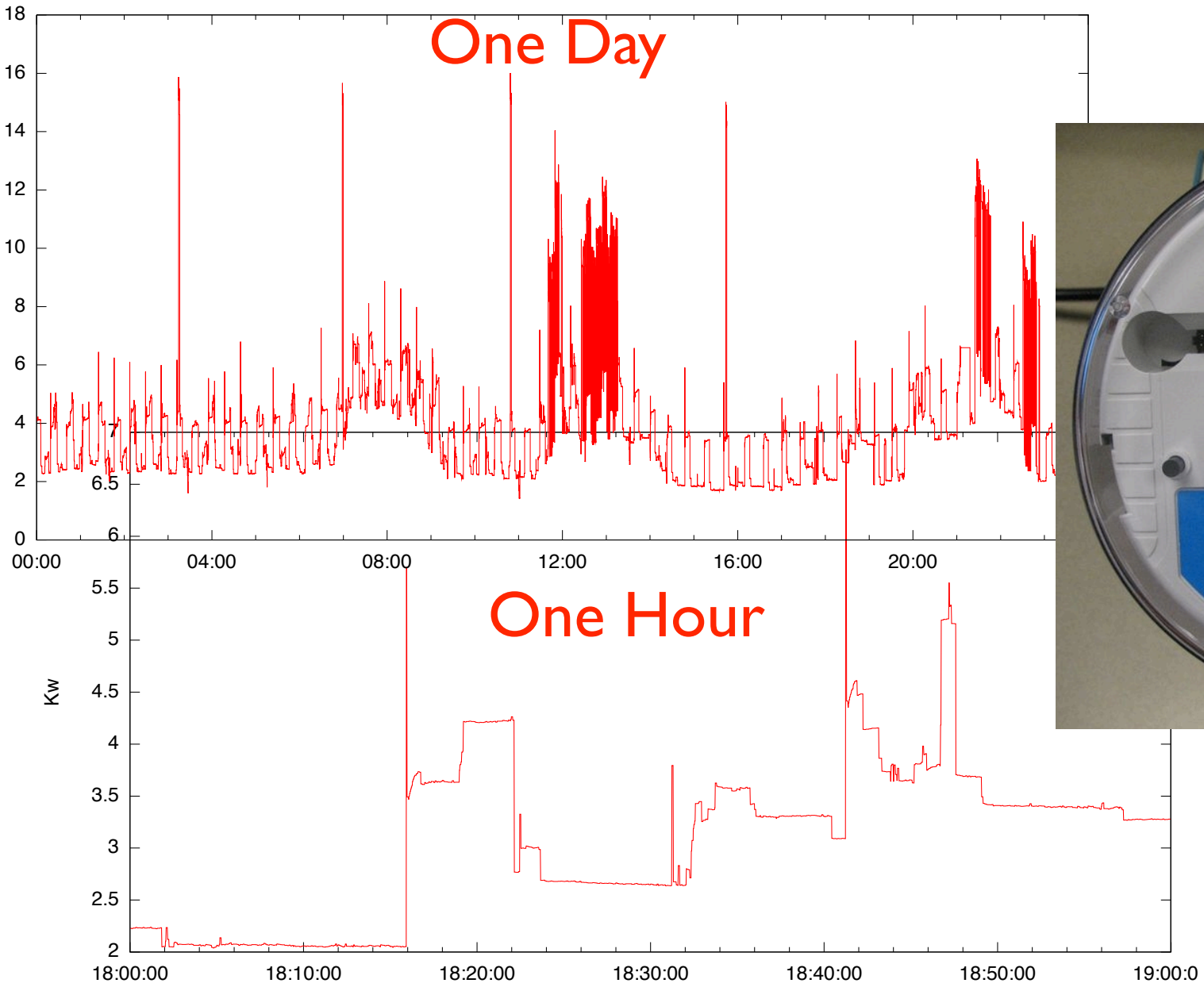
- At the micro scale, smart grid reaches into the home to "help" control appliances, lighting, etc.
- U.S. Deployment increasing, large scale deployments in Europe and Asia (particularly China) ...

Meter Data Management (for the last 100 years)



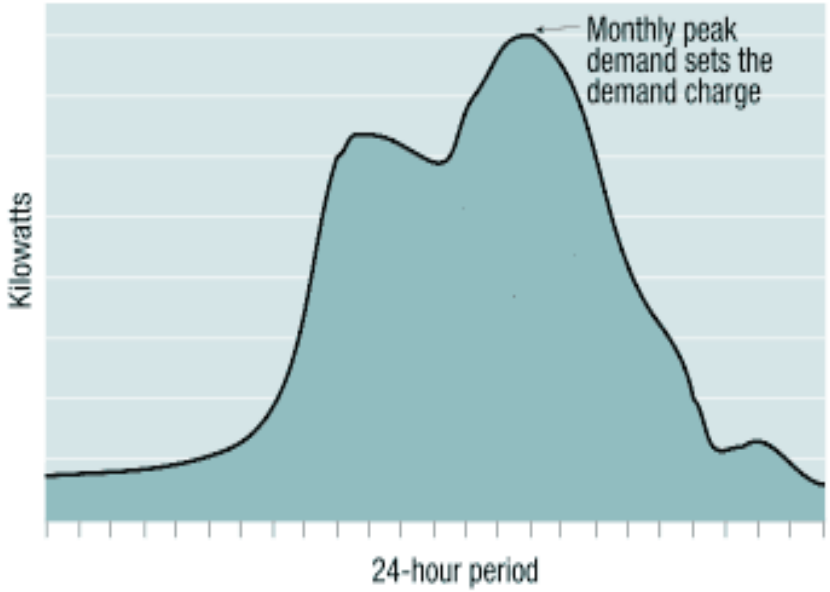
Meter Data Management (now and in the near future)

PENNSTATE 1855



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

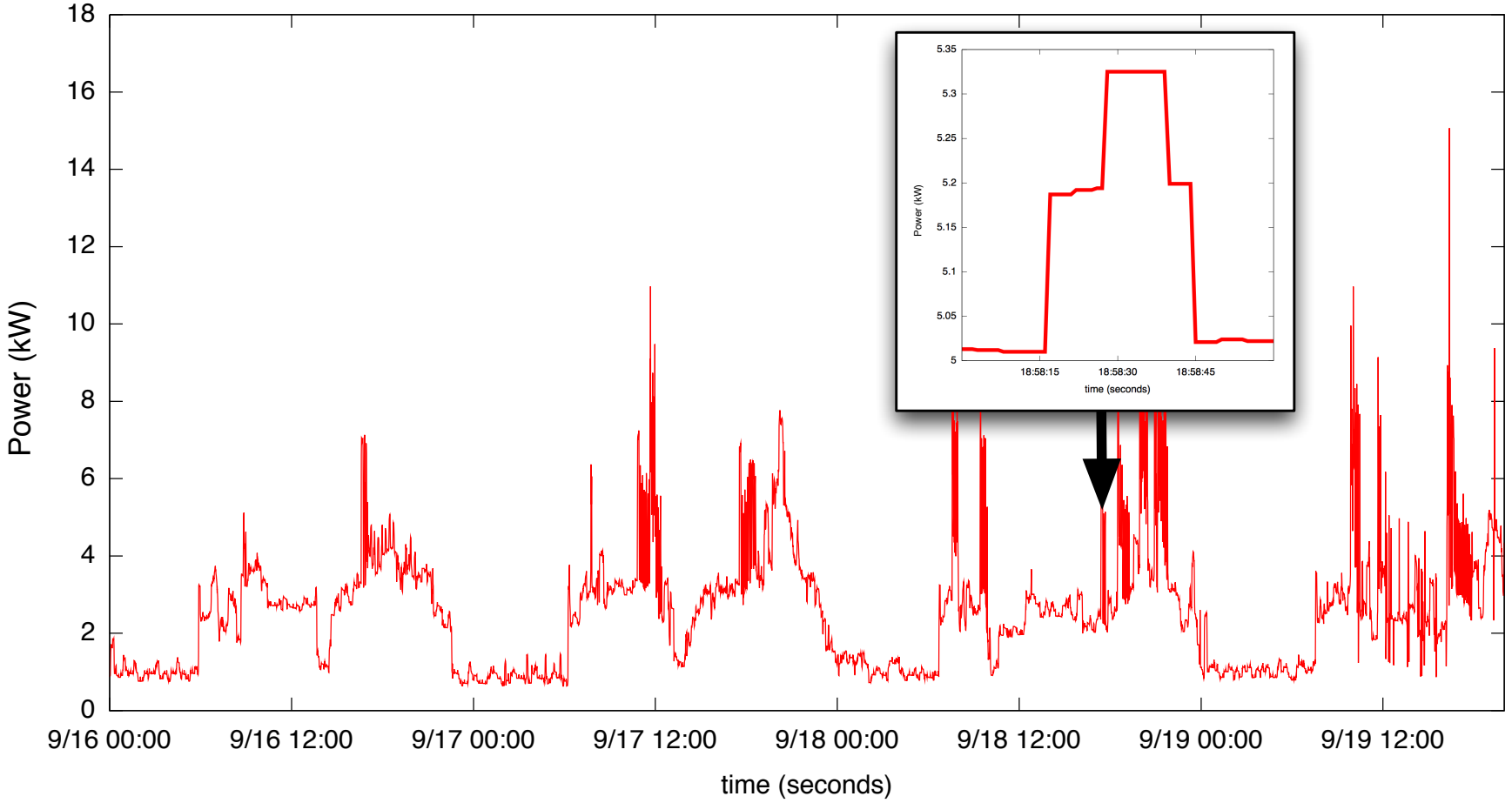


AMI - the concerns

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

AMI - the concerns

- What should we be concerned about?



Today

1. Horizontal penetration testing
   - National security
   - Accuracy/Fraud
2. Protecting consumer privacy
   - Consumer privacy

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

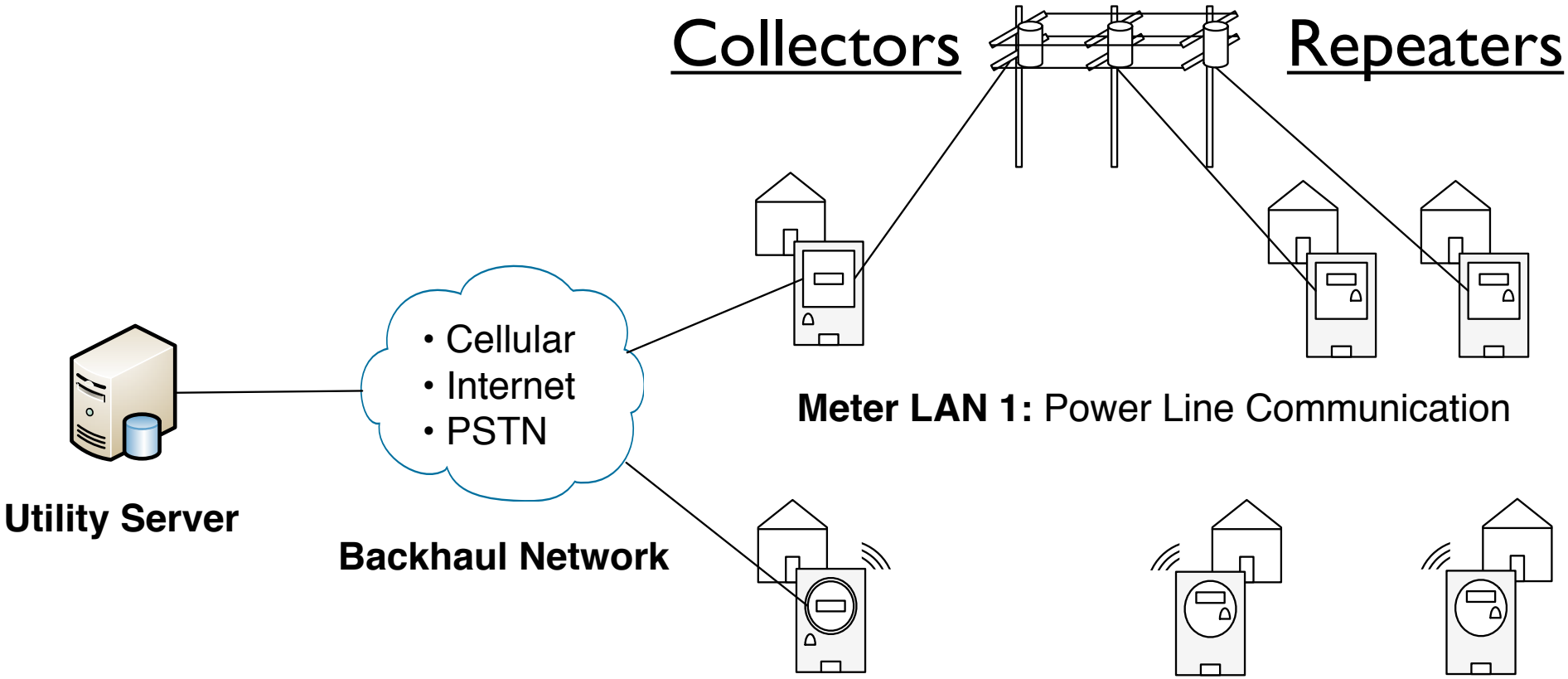
"The organization assesses the security requirements in the Smart Grid information system on an organization-defined frequency to determine the extent the requirements are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements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

-p 117

Vulnerability Assessment

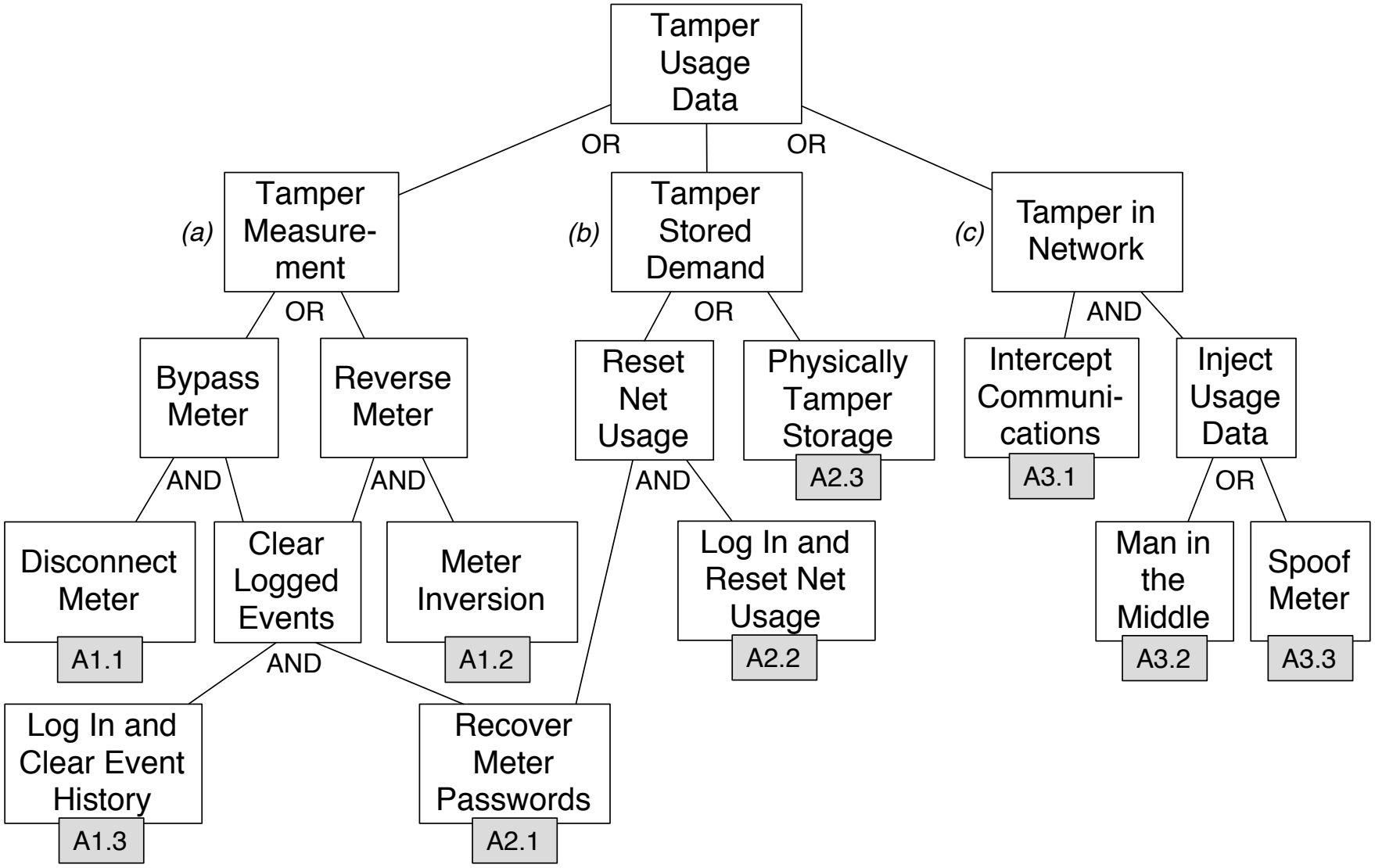
- Penetration testing: the art and science of breaking systems by applying attacker tools against live systems.
  - *Destructive research* attempts to illuminate the exploitable flaws and effectiveness of security infrastructure.
- Bottom line Q/A
  - Q: why are we doing this?
  - A: part of industrial 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



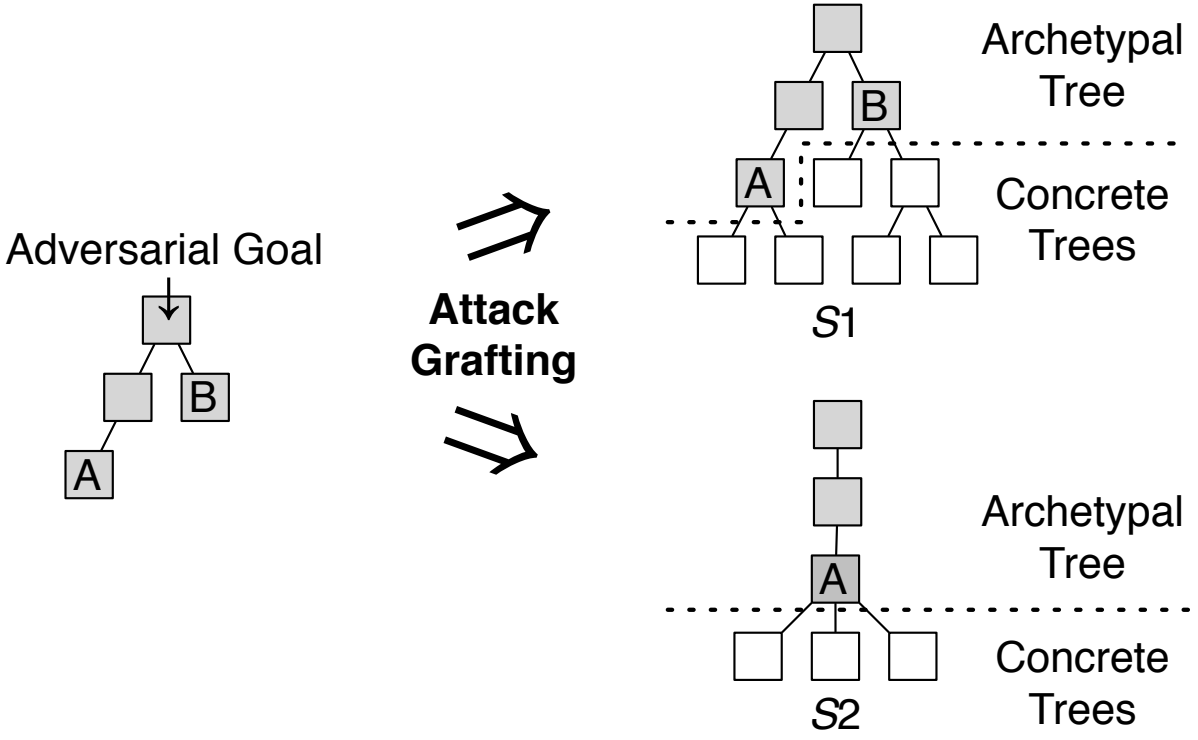
Attack Trees

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

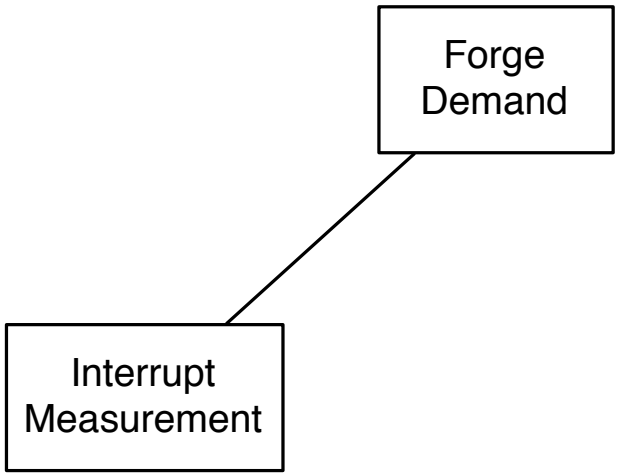
PENNSTATE 1855

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

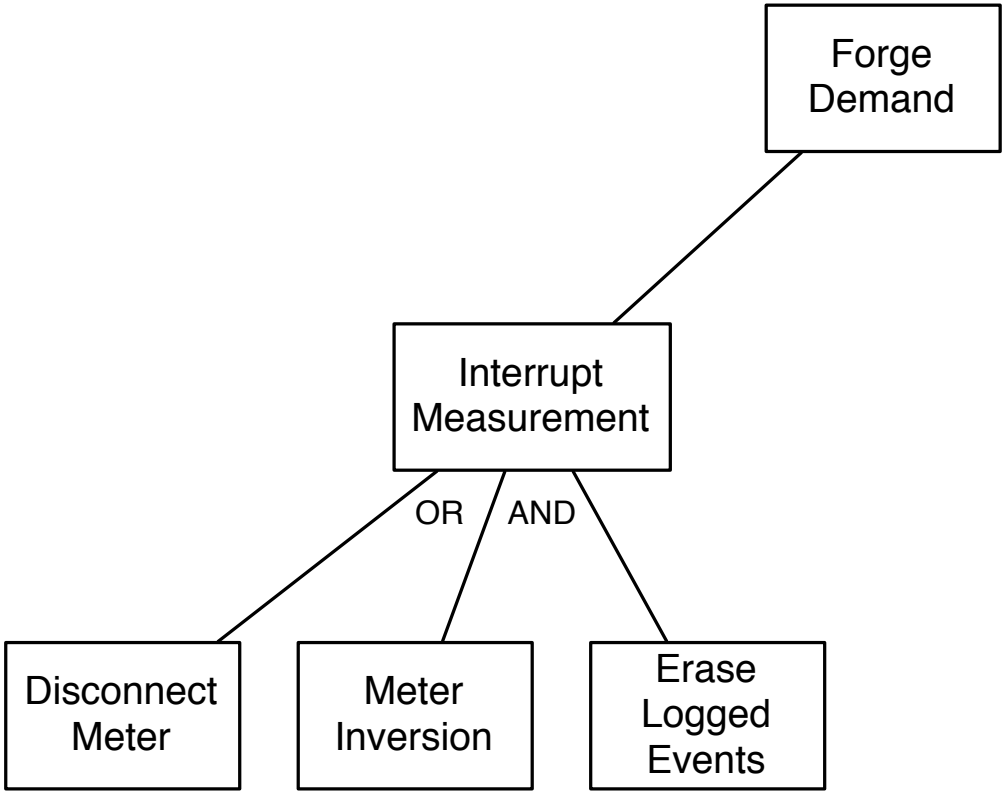
This paper: 3 Attack trees: fraud, DOS, disconnect, 2 "systems under test" (SUT)

Construction of Archetypal Trees

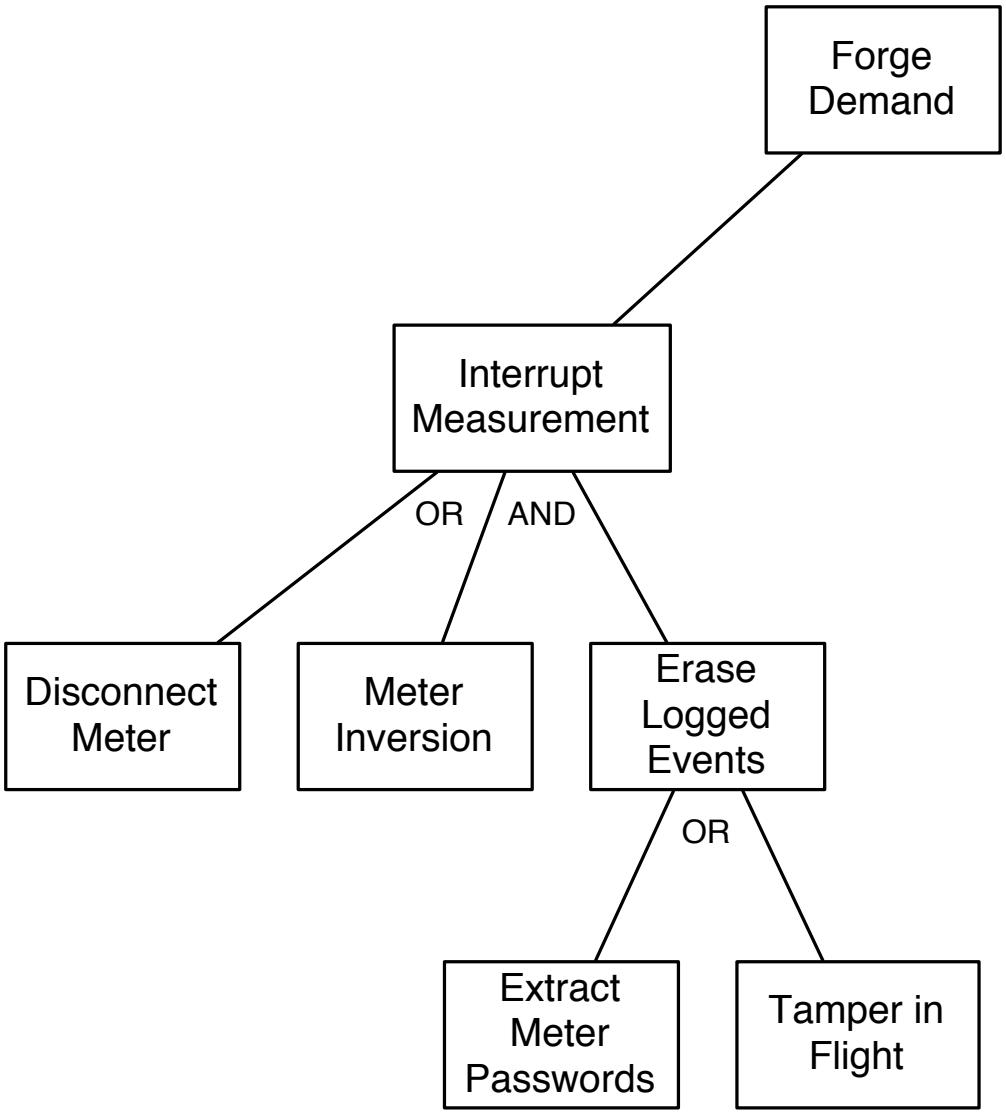
Construction of Archetypal Trees



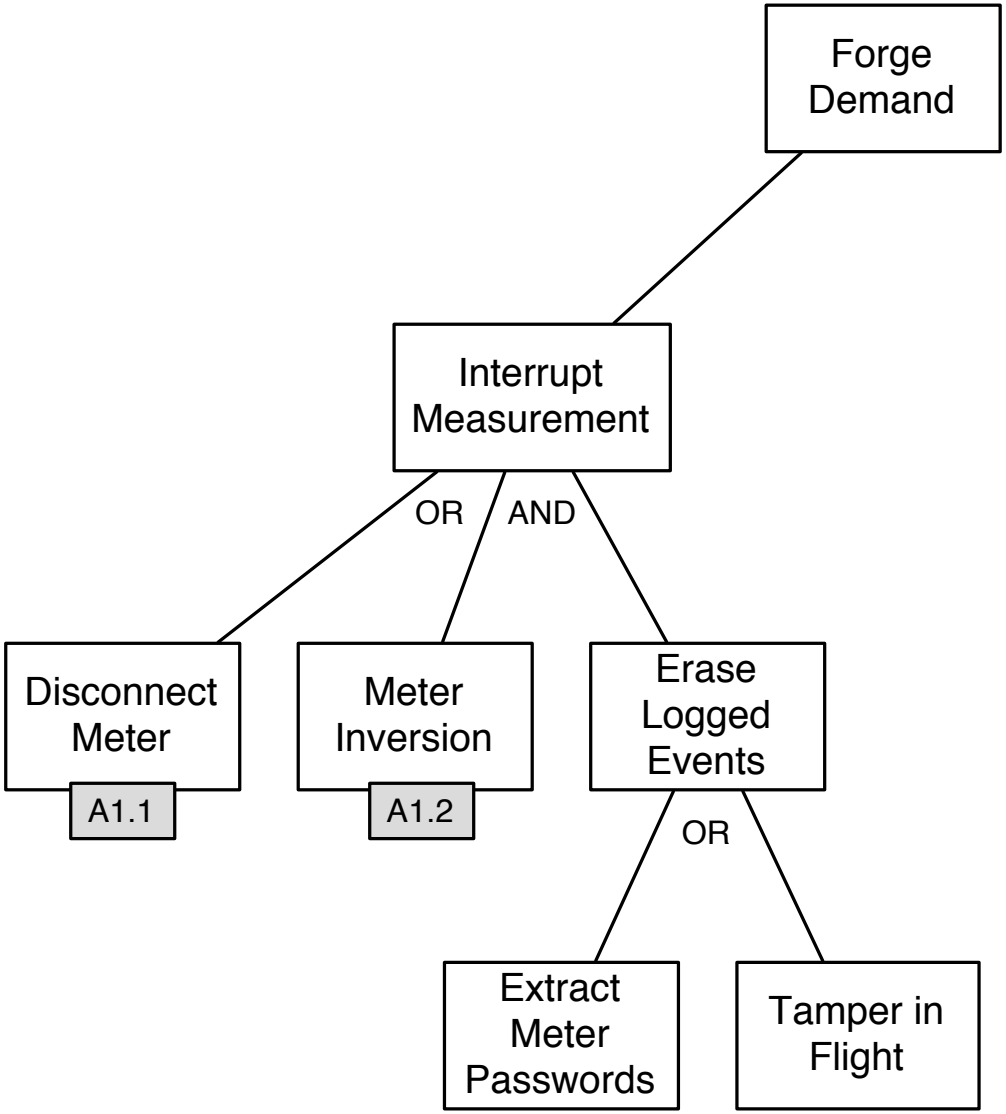
Construction of Archetypal Trees



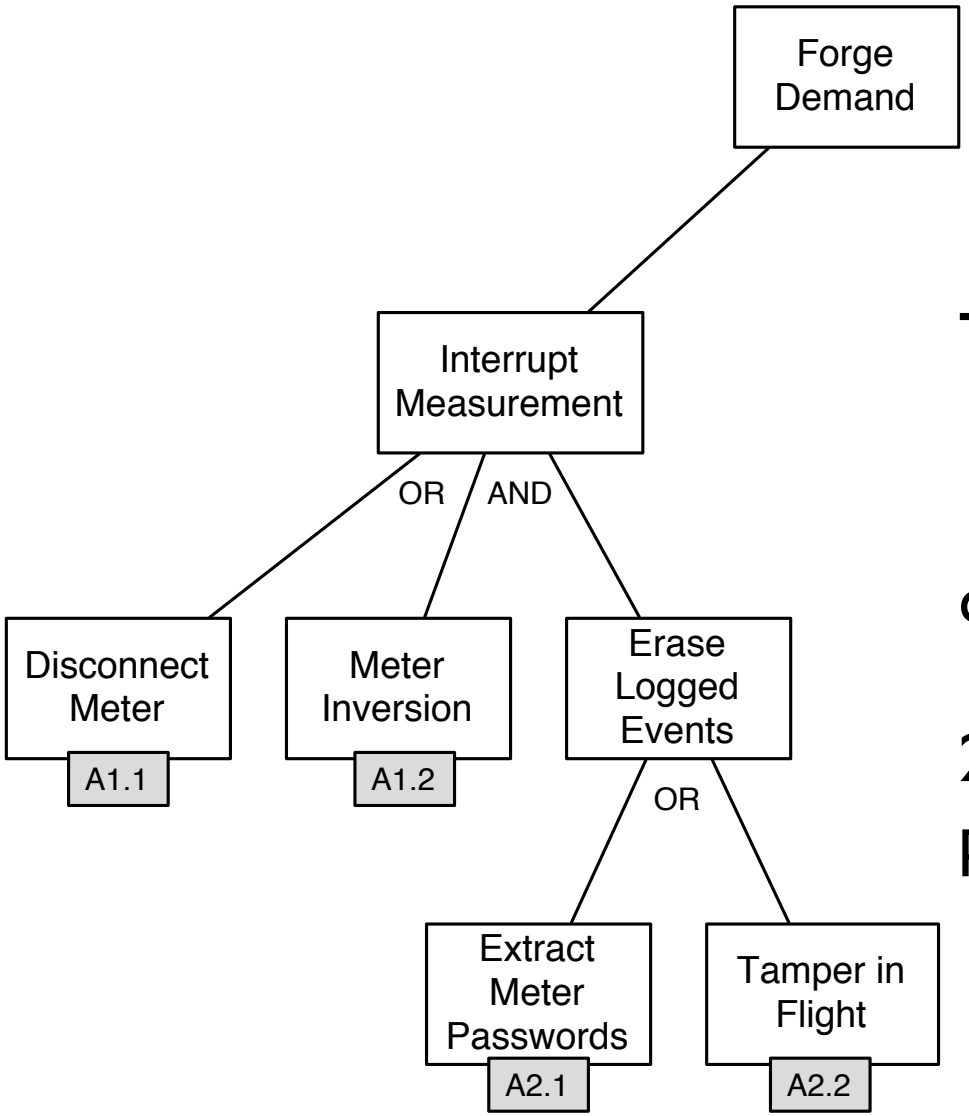
Construction of Archetypal Trees



Construction of Archetypal Trees



Construction of Archetypal Trees



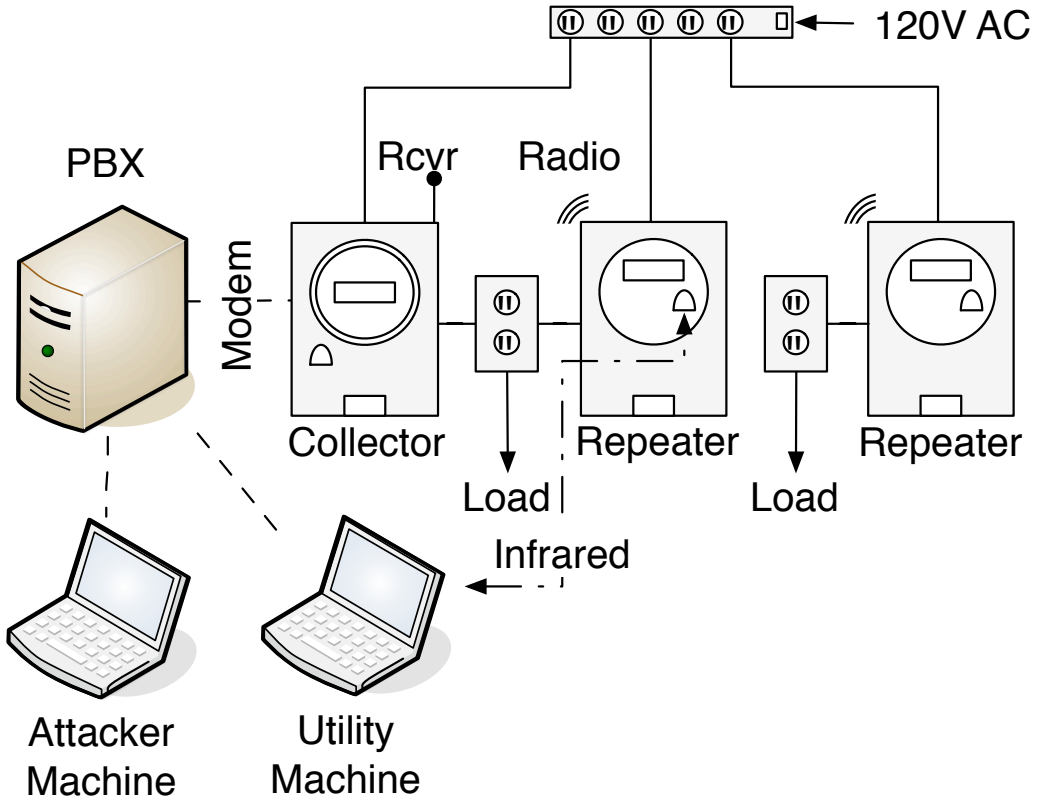
Two rules for termination:

1. Attack is on a vendor-specific component

2. Target may be guarded by a protection mechanism

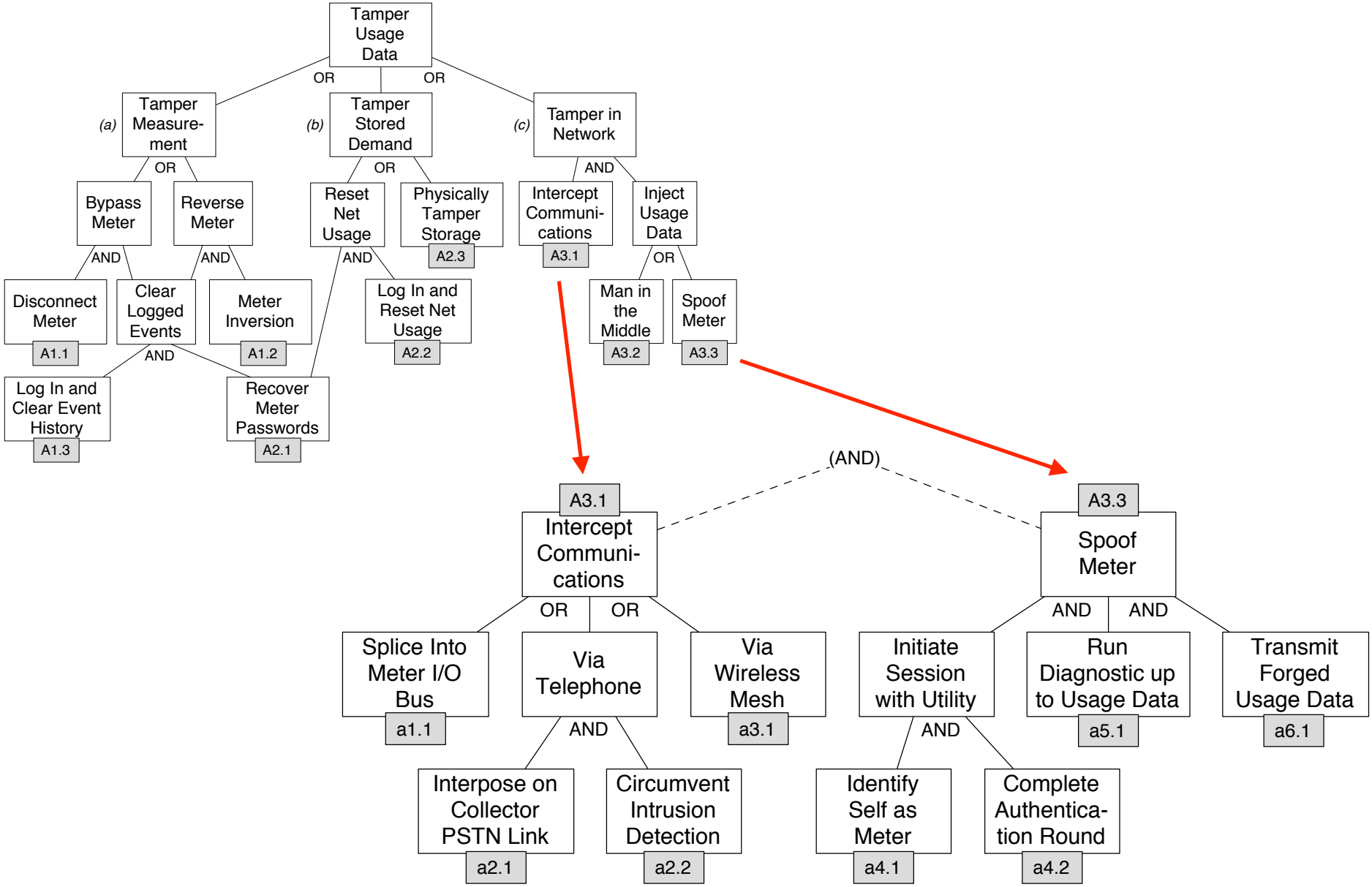
System Under Test

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

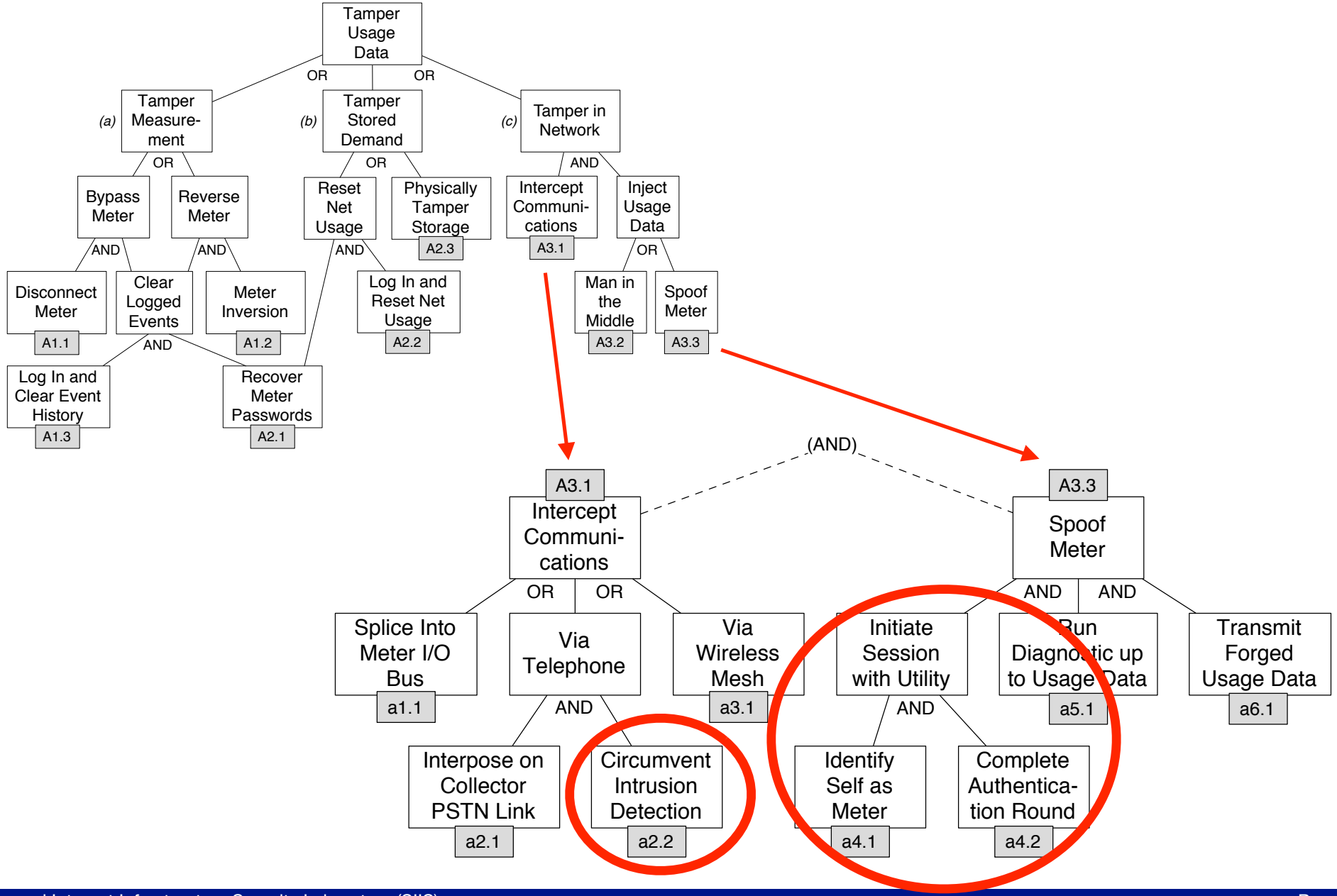


- 900 MHz wireless mesh collector/meter network
- Infrared "near-field" security for configuration port

Fraud Concrete

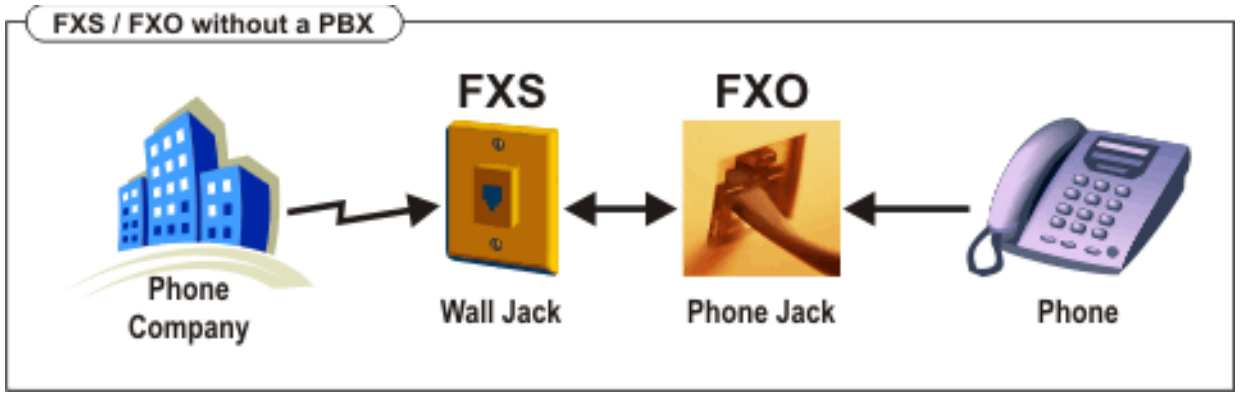


Fraud Concrete

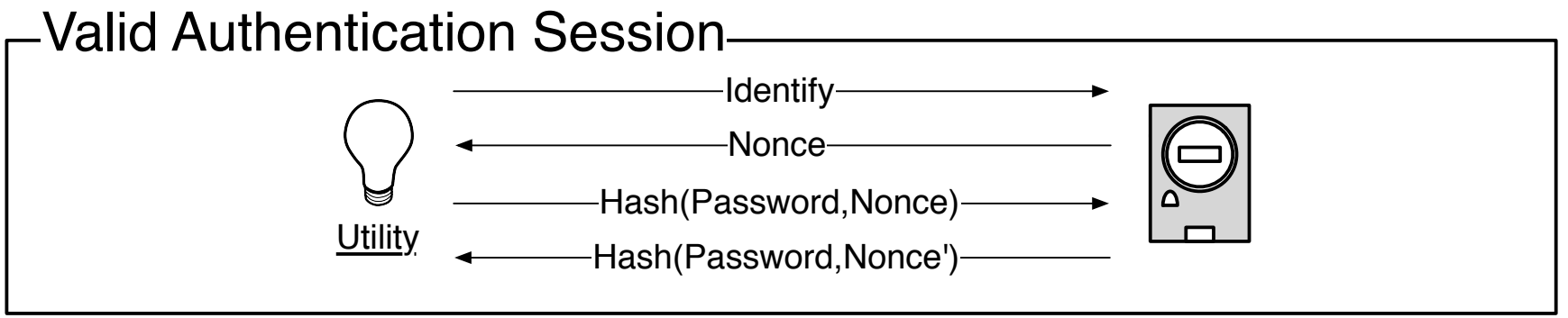


Enabling Attacks (Fraud)

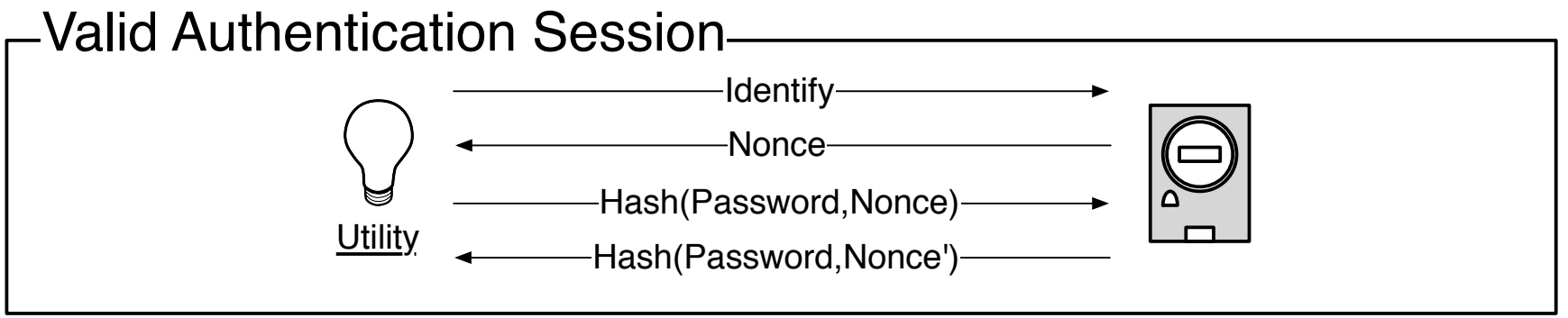
- Defeating modem "*intrusion detection*"
  - "off hook" events on the line are detected by sensing presence Foreign Exchange Office (FXO) of dial-tone voltage on the line.
  - current calls are dropped if off hook is detected
  - such events can simply be suppress easily by preventing voltage from arriving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



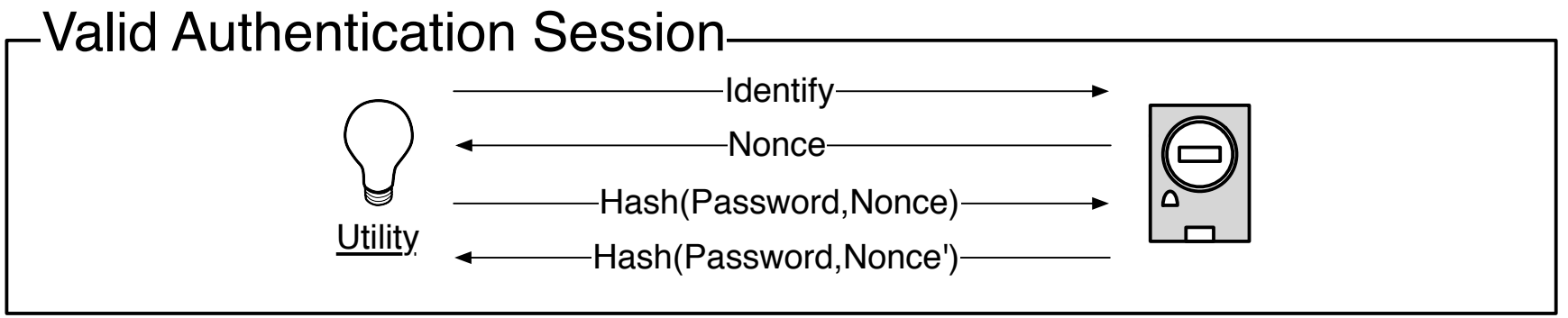
Enabling Attacks (Fraud)



Enabling Attacks (Fraud)

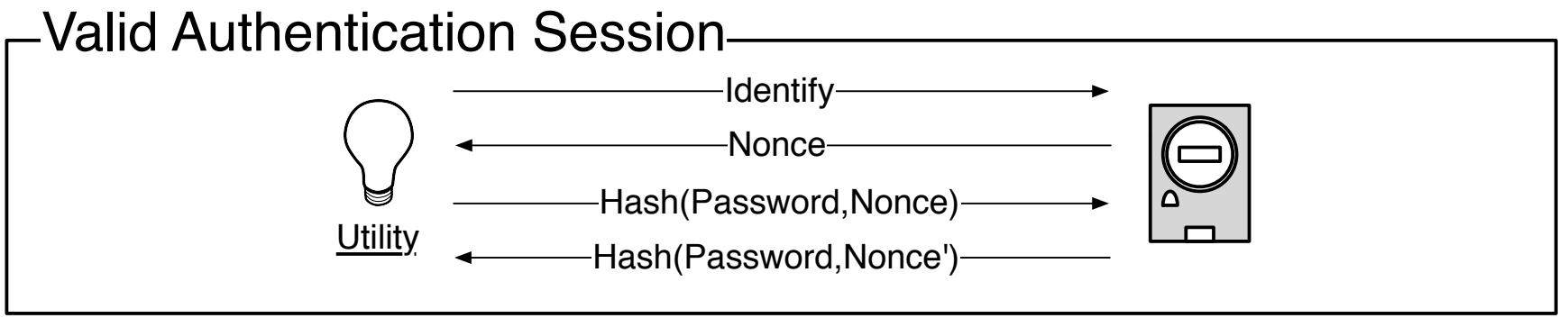


Enabling Attacks (Fraud)

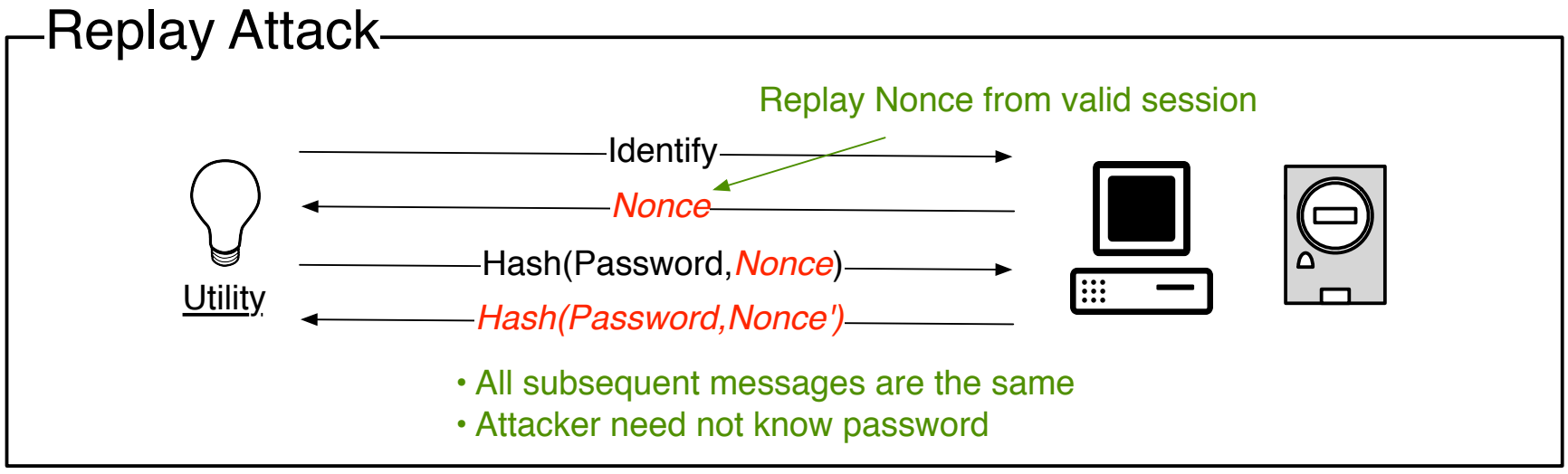


- *Replay attack*: I can replay the nonce from a previous session to impersonate the meter.

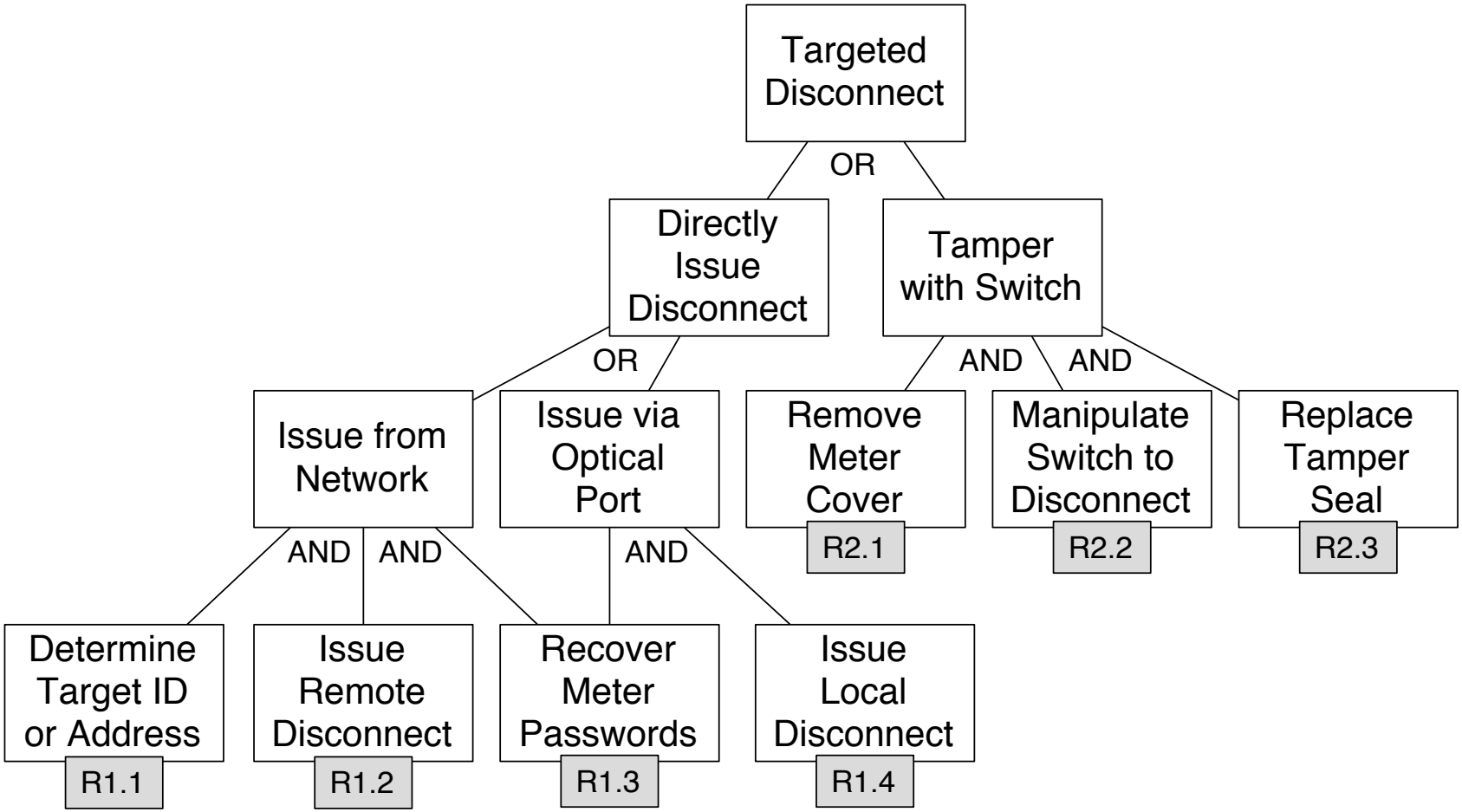
Enabling Attacks (Fraud)



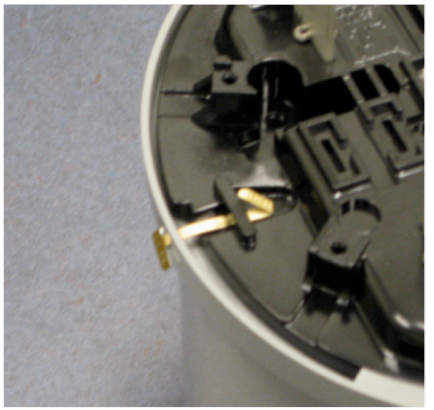
- *Replay attack*: I can replay the nonce from a previous session to impersonate the meter.



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.

Attacks Summary

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

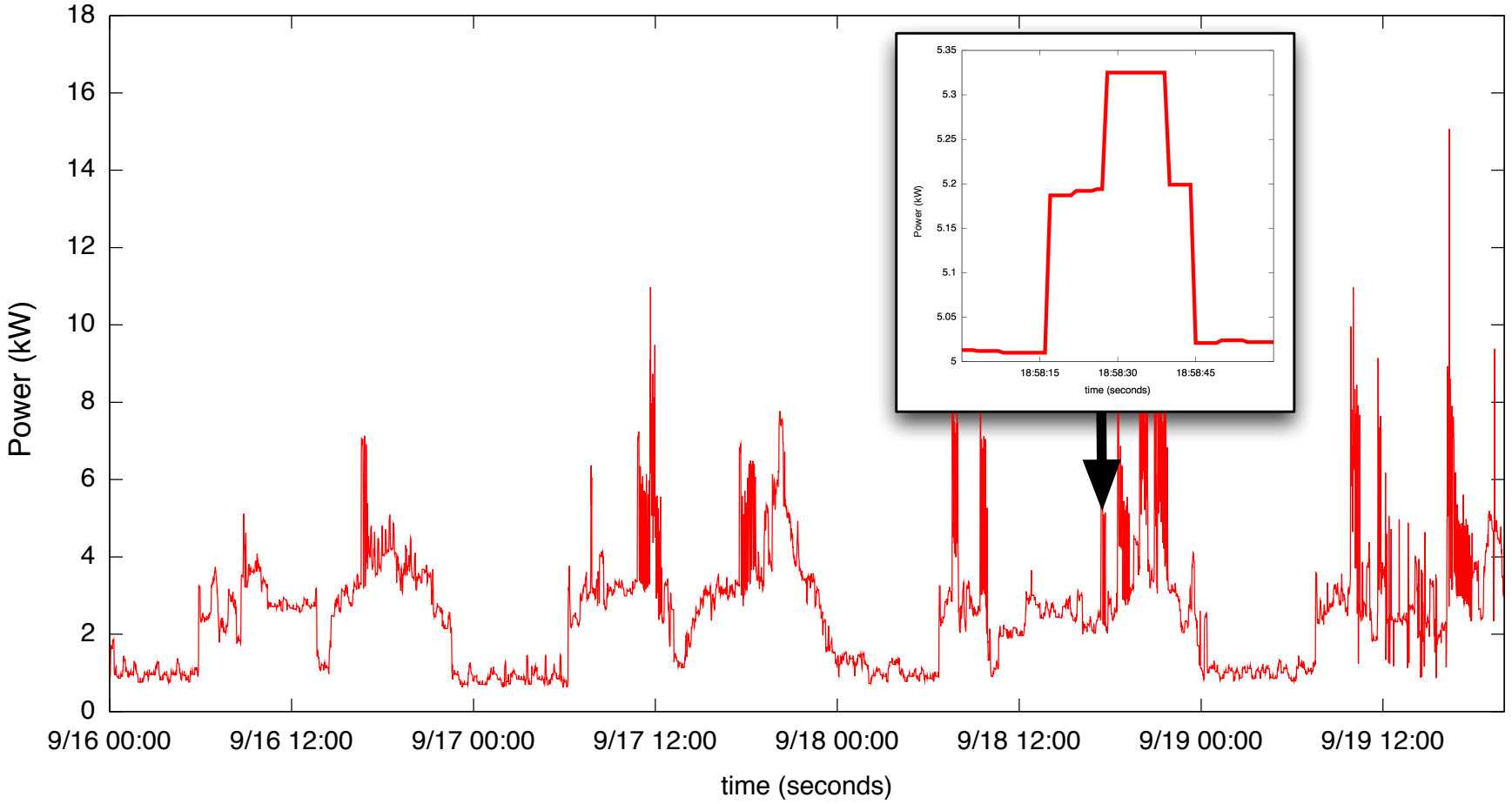
Ref.	Description	Enabling Feature or Vulnerability
	Energy Fraud in S1	
a2.1	Interpose between utility and collector	Telephone line may be accessible.
a2.2	Defeat modem intrusion detection	The mechanism cannot detect an FXS.
a4.1	Identify self as meter	A meter's ID is printed on its faceplate.
a4.2	Complete 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.

Consumer Privacy

- Recall the meter side channel ...

Consumer Privacy

- Recall the meter side channel ...



The Basic Privacy Problem

Electricity usage encodes information about human behavior

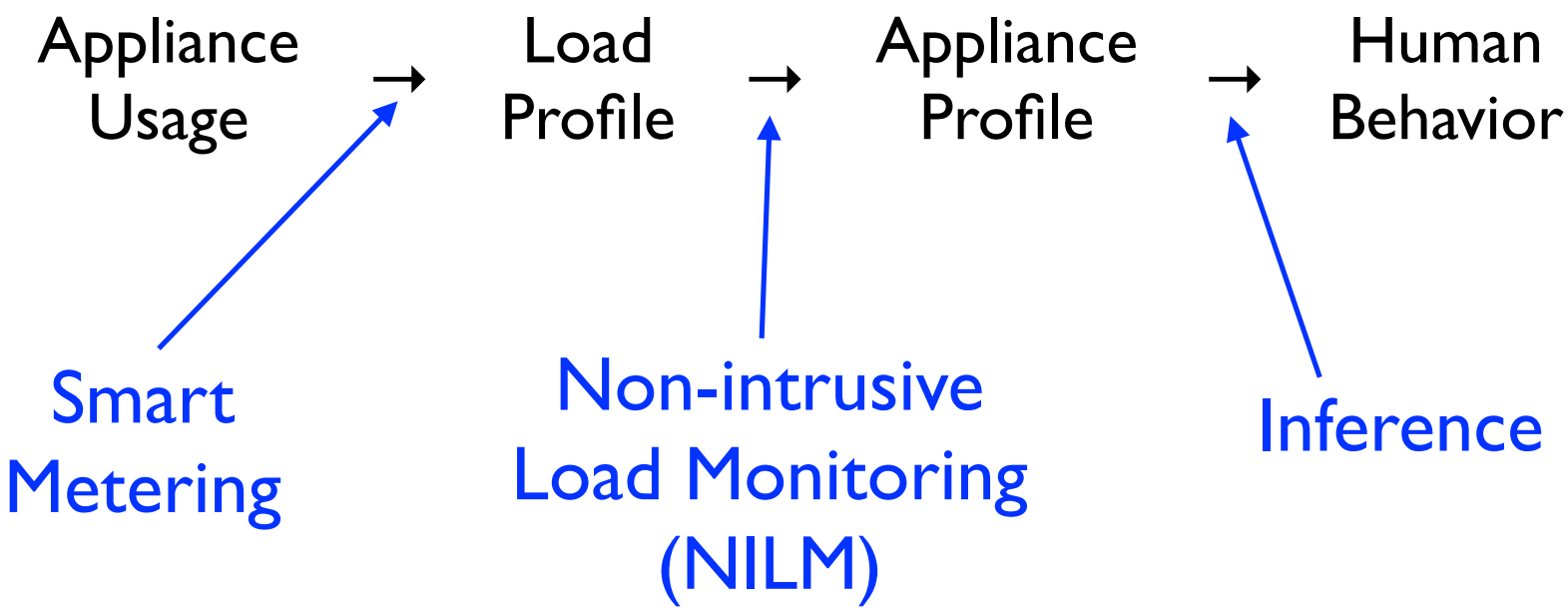
The Basic Privacy Problem

Electricity usage encodes information about human behavior

Appliance Usage → Load Profile → Appliance Profile → Human Behavior

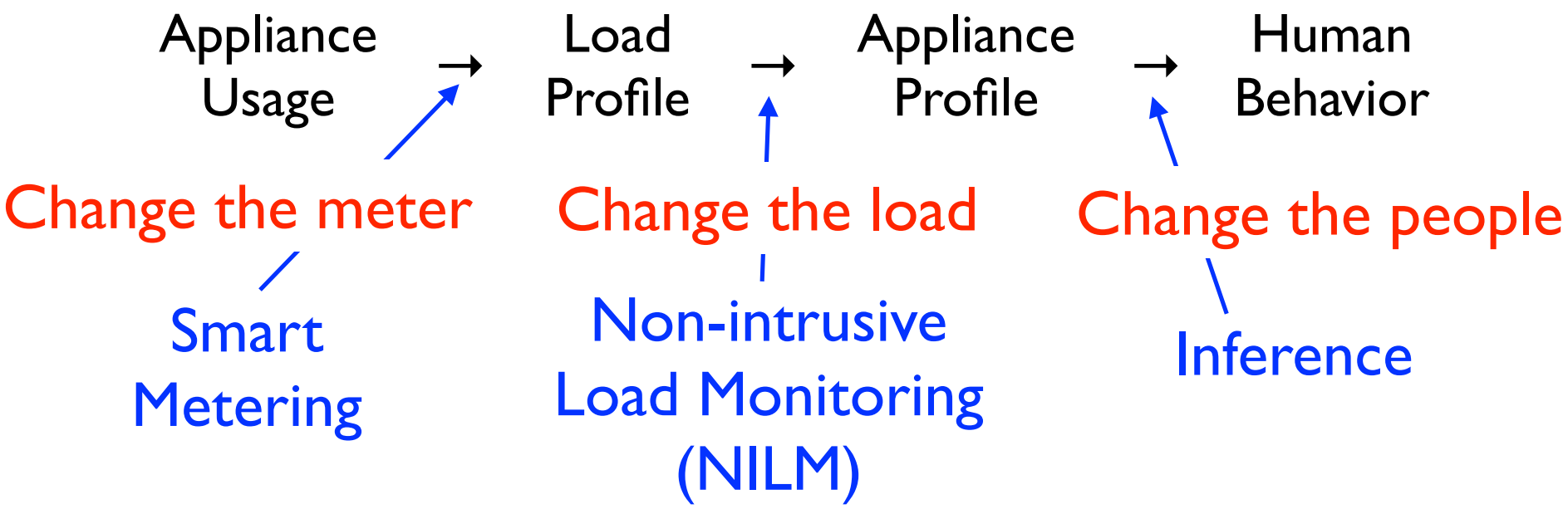
The Basic Privacy Problem

Electricity usage encodes information about human behavior



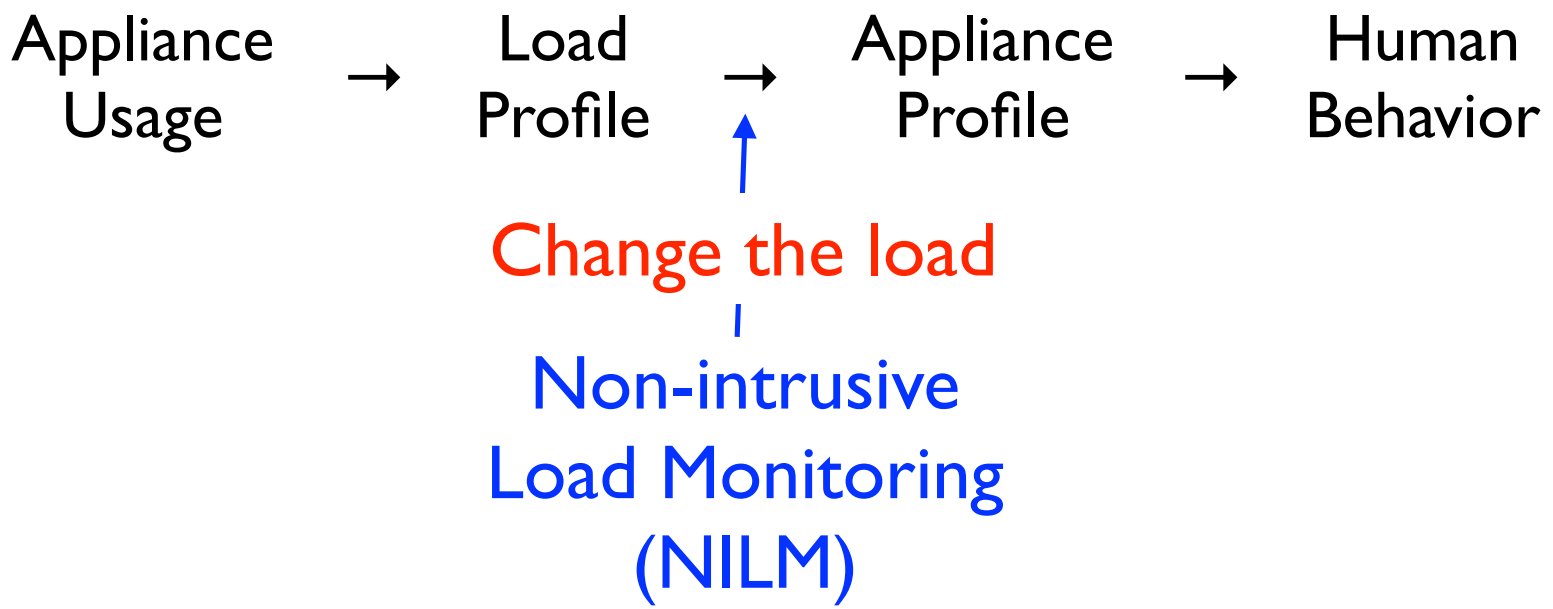
Three Potential Solutions

Electricity usage encodes information about human behavior



Three Potential Solutions

Electricity usage encodes information about human behavior

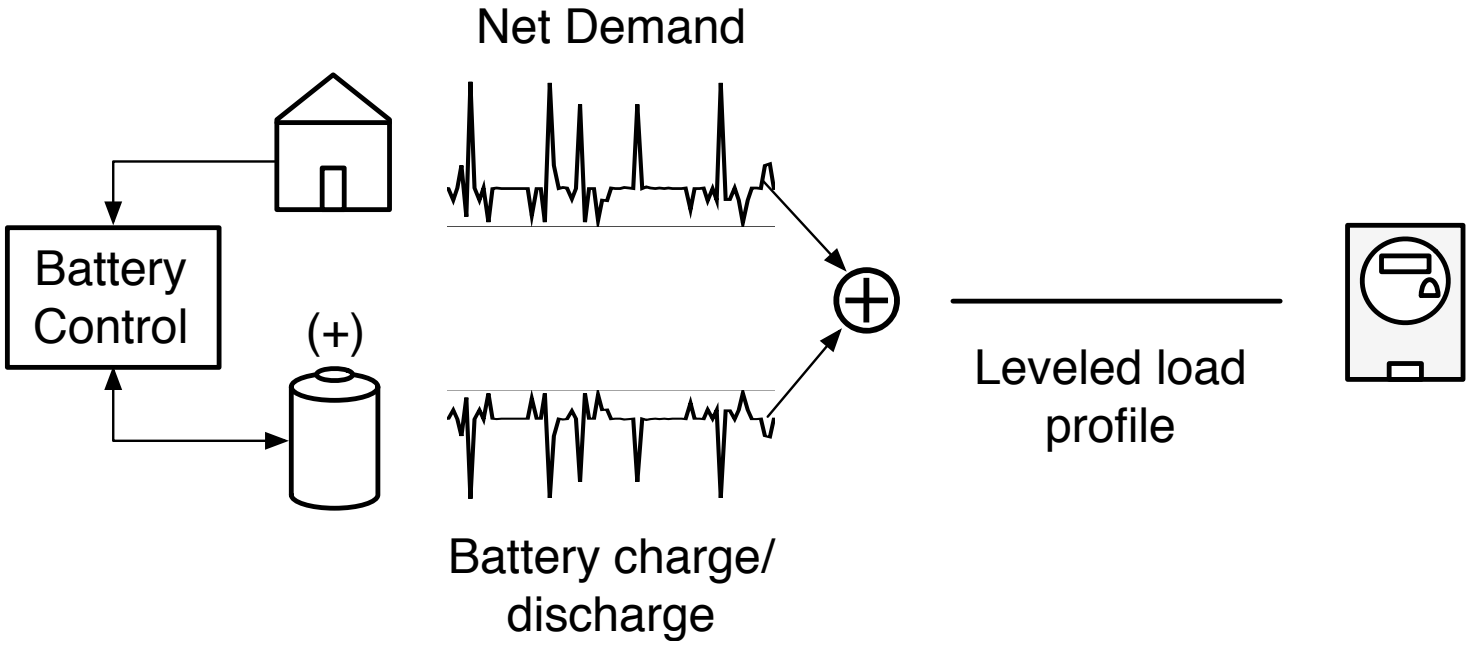


Non-intrusive Load Monitors

- NILMs translate a load profile into an appliance profile
  - Load Profile: High-resolution time series of energy usage
  - Appliance Profile: Set of appliances ON at any given time
- Two classes of NILMs
  - Steady State: Look for transitions in steady state load
  - Power Signature: Look for load features indicative of particular appliances

Non-intrusive Load Leveling (NILL)

- A battery is placed in parallel with house's electrical service panel.
- By charging and discharging at controlled rates, features can be removed from the house's load profile.



Definitions

PENNSTATE 1855

$d(t)$ Demand from house

$u(t)$ Utility-observable demand

$c(t)$ Battery state of charge

$b(t)$ Battery rate of charge

$b(t) > 0$ Charging

$b(t) < 0$ Discharging

H The upper limit on battery state of charge

L The lower limit on battery state of charge

K_{SS} The target steady state demand for $u(t)$

Definitions

$$u(t) = d(t) + b(t)$$ (Utility-observable demand)

$$c(t) = c(t_0) + \int_{t_0}^{t} b(t)\ dt$$ (State of charge)

$$= c(t_0) + \int_{t_0}^{t} u(t) - d(t)\ dt$$

$$= c(t_0) + K_{SS}[t - t_0] - D(t)|_{t_0}^{t}$$

NILL Constraints

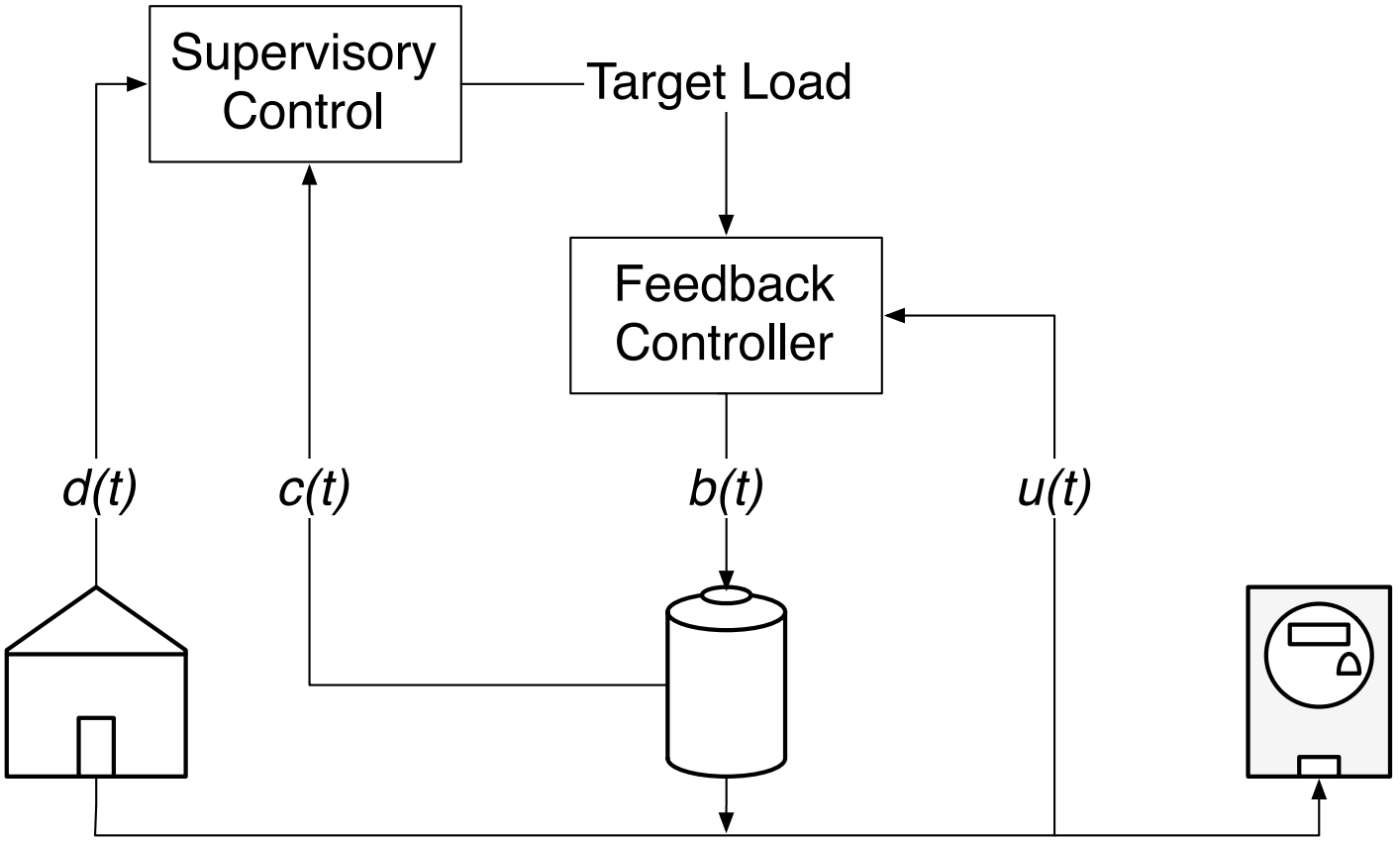
$$L < c(t) < H$$

(Safe state of charge)

$$u(t) = K_{SS}$$

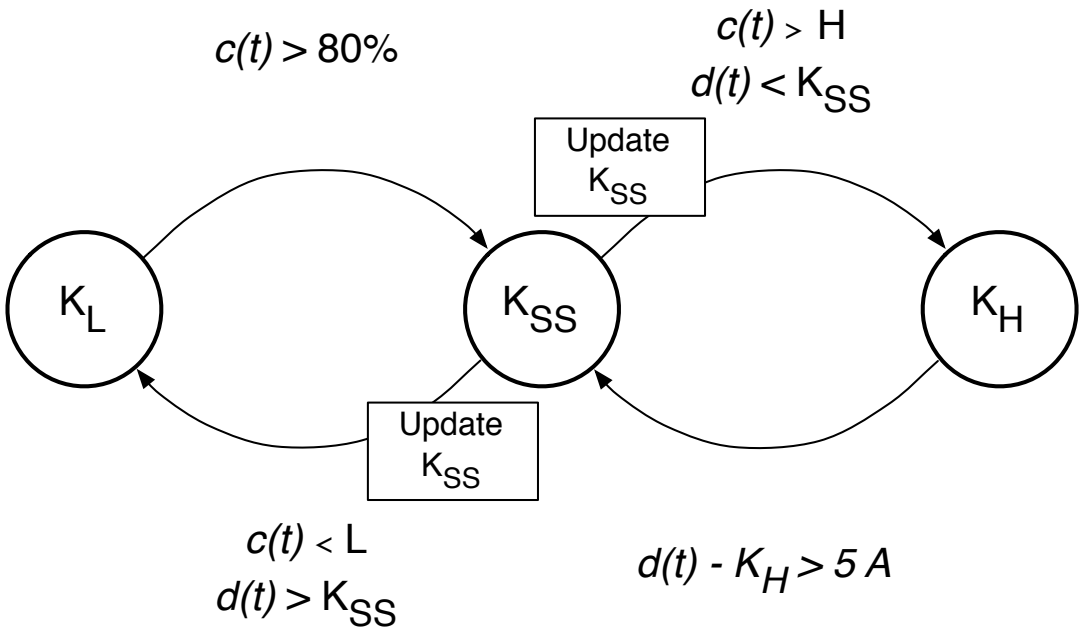
(Leveled load)

Control Model



Supervisory Control

- Attempts to choose a "good" target load given the demand and battery SoC.
- Currently very basic: method of learning is and EWMA of *d(t)*
- K_L chosen to be close to maximum amperage charge rate
- K_H chosen to be just below recent *d(t)*



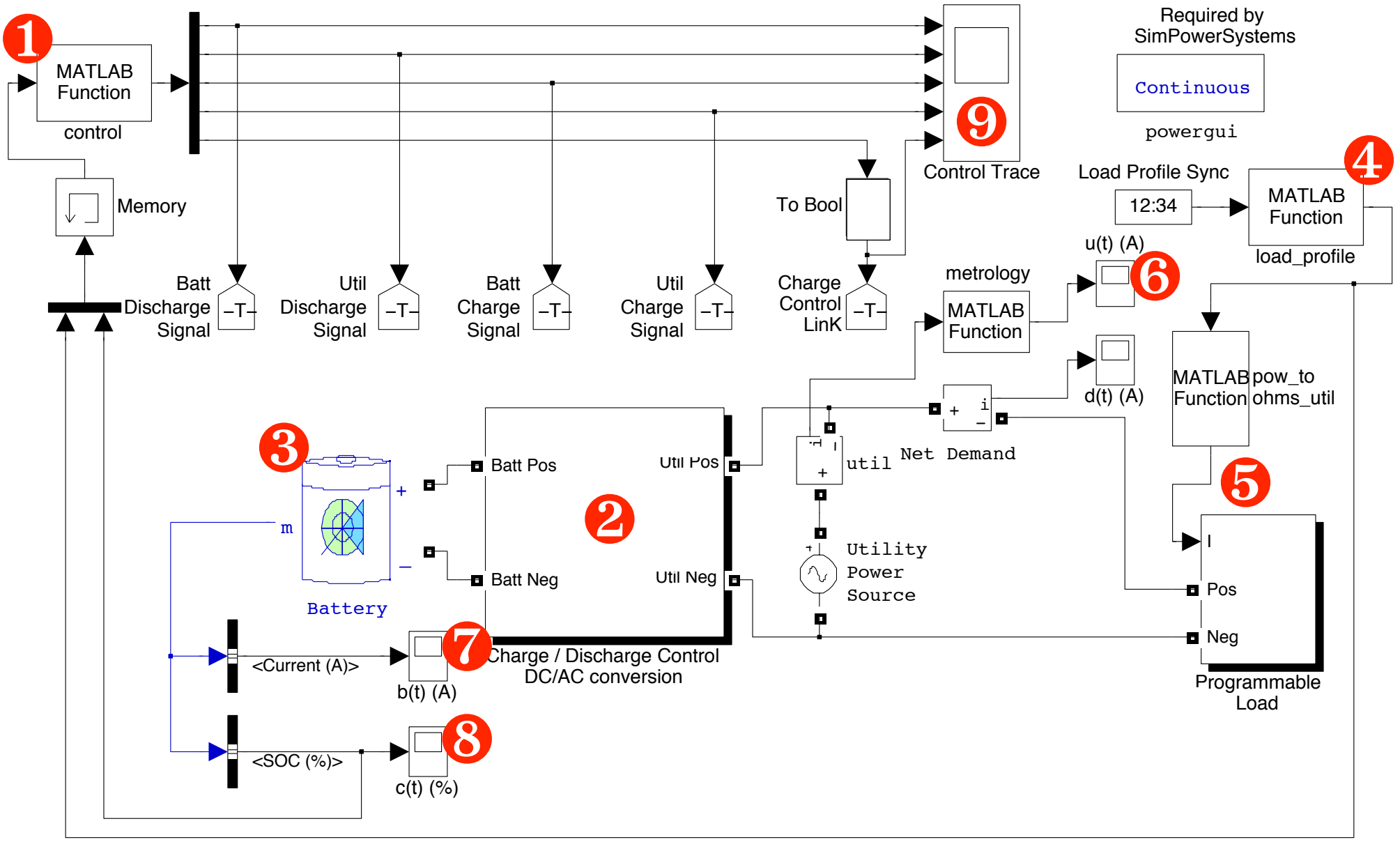
Initial target loads

1. $D \leftarrow \int_{t_0}^{t_{max}} d(t)\,dt$
2. $d_{max} \leftarrow \max_{[t_0, t_{max}]} d(t)$
3. Binary search K in range $[0, d_{max}]$
4. Check constraints for $c(t) = K|_{t_0}^{t} - D + c(t_0)$
5. Save minimal satisfactory K

Experiment

- One-second resolution load profile data was collected from two houses, one townhouse, and one apartment for at least one month each.
- We simulated a NILL installation in which the load profile for each was replayed under the influence of the NILL controller.
- The result is a pairing of original load profile and load profile under NILL for each house.

Simulation


1
MATLAB Function
control
Memory
Batt Discharge Signal
Util Discharge Signal
Batt Charge Signal
Util Charge Signal
To Bool
Charge Control LinK
9
Control Trace
Required by SimPowerSystems
Continuous
powergui
Load Profile Sync
12:34
4
MATLAB Function
load_profile
u(t) (A)
6
metrology
MATLAB Function
d(t) (A)
MATLAB Function
pow_to ohms_util
5
3
Batt Pos
Batt Neg
Util Pos
Util Neg
2
Battery
util
Net Demand
Utility Power Source
I
Pos
Neg
Programmable Load
<Current (A)>
b(t) (A)
7
Charge / Discharge Control
DC/AC conversion
<SOC (%)>
c(t) (%)
8

Load Profile Features

- A **feature** is any near-instantaneous change in demand
- **Sister features** are a pair of features in which the first feature is an increase in demand, and the second is a decrease of equal and opposite magnitude as the first

Feature Reduction

Residence	Non-NILL	NILL	Change
Total Features			
H1	1047099	61793	-94.10%
H2	286960	20713	-92.78%
A1	430214	24893	-94.21%
T1	384847	33413	-91.32%
Features per hour			
H1	358	21	-94.10%
H2	199	14	-92.79%
A1	289	16	-94.21%
T1	277	24	-91.32%
Sister feature pairs			
H1	340986	10552	-96.91%
H2	110994	4735	-95.73%
A1	176540	6030	-96.58%
T1	147982	8120	-94.51%

Quantifying Privacy Loss

- **Feature Mass:**

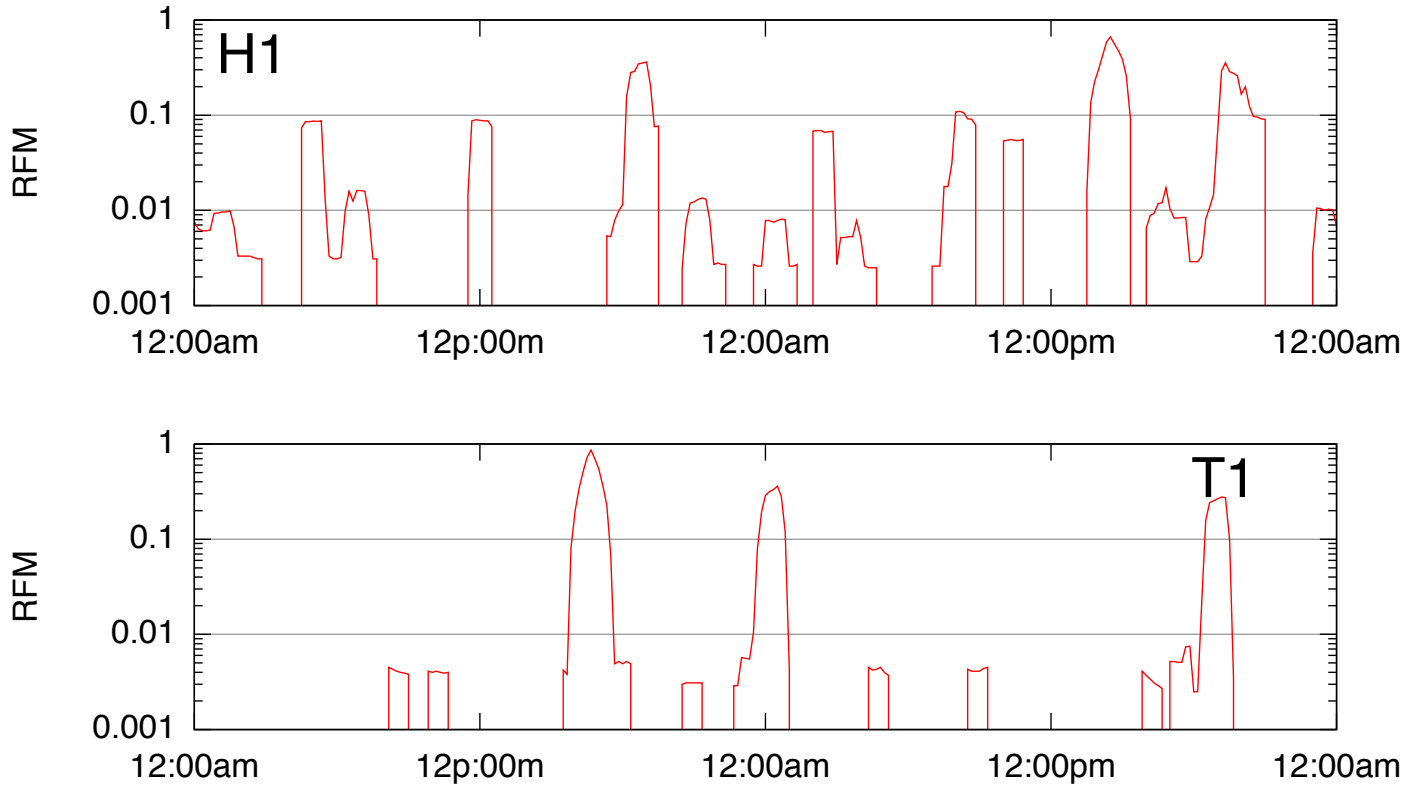
$$FM(w, D) = \sum_{i=0}^{w} (d_i \neq 0)$$

- **Relative Feature Mass:**

$$RFM(w, D) = \frac{FM(w, D_{NILL})}{FM(w, D_{NON\_NILL})}$$

RFM Results

- RFM of zero means perfect privacy
- Even for large loads, RFM is below 1% most of the time.



Residual Features

- **Residual Features:** Features that appear in both the NILL and Non-NILL load profiles at the same time

Residence	Sister features	Per Day
H1	359 (0.11%)	5.9
H2	33 (0.03%)	1.1
A1	93 (0.05%)	3.1
T1	128 (0.09%)	4.4

Conclusions

PENNSTATE 1855

- We have described both security and privacy challenges in neighborhood-level smart grids.
- Attack trees have proven to be a useful tool in finding vulnerabilities in real smart metering products.
- Non-Intrusive Load Leveling can significantly reduce the useful features in smart meter readings without cooperation from utilities.

Summary

- Horizontal penetration testing is 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
- Consumer Privacy
  - Enormous information exposure on signal provided by fine-grained energy usage, is exploitable
  - NILL algorithms provide a way to counteract exposure while not perturbing signal
  - NILL may lead to more efficient energy usage

Systems and Internet Infrastructure Security Laboratory

Prof. Trent Jaeger,(tjaeger@cse.psu.edu)

Operating Systems Security, Policy Design and Analysis, Source Code Analysis

Prof. Patrick McDaniel, (mcdaniel@cse.psu.edu)

Network Security, Critical Infrastructure, Security-typed Languages, Formal Security Policy

Prof. Adam Smith (asmith@cse.psu.edu)

Cryptography, Applied Cryptography, Information Science, Theoretical Computer Science

Systems and Internet Infrastructure Security

PENNSTATE

CSE

Funding:

National Science Foundation
Army Research Office/DOD
CISCO
Motorola (SERC)
Raytheon
IBM
Lockheed Martin
AT&T, ...

Ongoing Projects:

Systems and VM Security
Secure Storage Systems
Language Based Security
Telecommunications Security
Smartgrid Security
Voting Systems
Theoretical Cryptography
Practical Privacy

Factoids: Established September 2004 -- Location - 344 IST Building -- Contact siislab@cse.psu.edu

URL: http://siis.cse.psu.edu

Questions?

PENNSTATE 1855

- 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.
  - Patrick McDaniel and Stephen McLaughlin, Security and Privacy Challenges in the Smart Grid. IEEE Security & Privacy Magazine, (3):75-77, May/June, 2009.