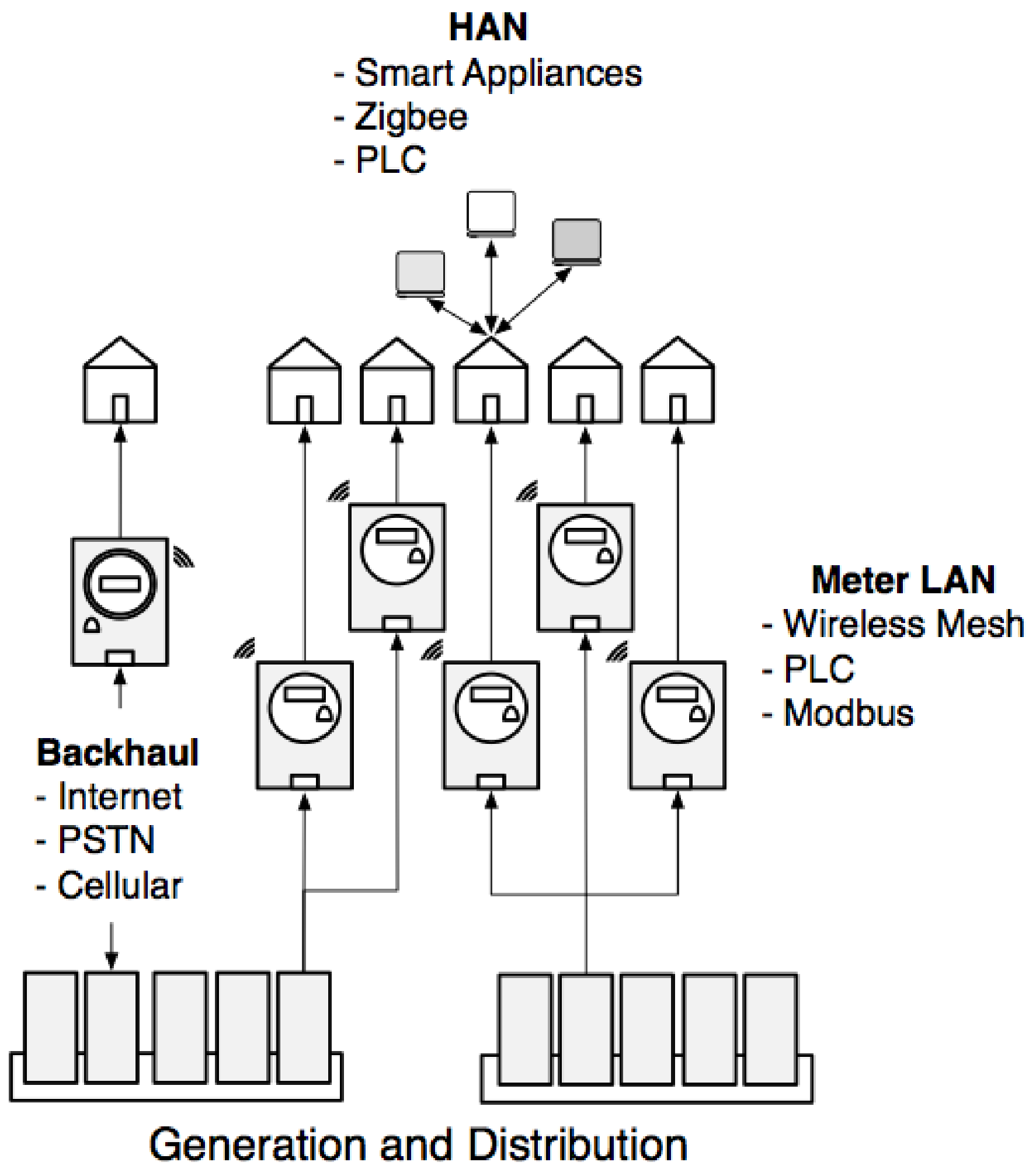
Energy Theft in the Advanced Metering Infrastructure

Stephen McLaughlin, Dmitry Podkuiko, Patrick McDaniel

The up and coming smart grid promises more cost effective generation and distribution for both utilities and consumers. The key component in the smart grid is the Advanced Metering Infrastructure (AMI). AMI is comprised of networks of *smart meters*, electric meters which remotely report energy demand over public networks. Theft of service is an understood problem in the current grid where the physical manipulation of electric meters is used to report erroneously low electricity demand. We posit and demonstrate that energy theft is likely to persist and even increase in the smart grid. We do this by constructing threat and attack models for theft of service in AMI which show how its complexity leads to the monetization of security flaws found in smart meters. We then implement a proof of concept attack against a commercially available smart metering system that allows energy usage to be forged.

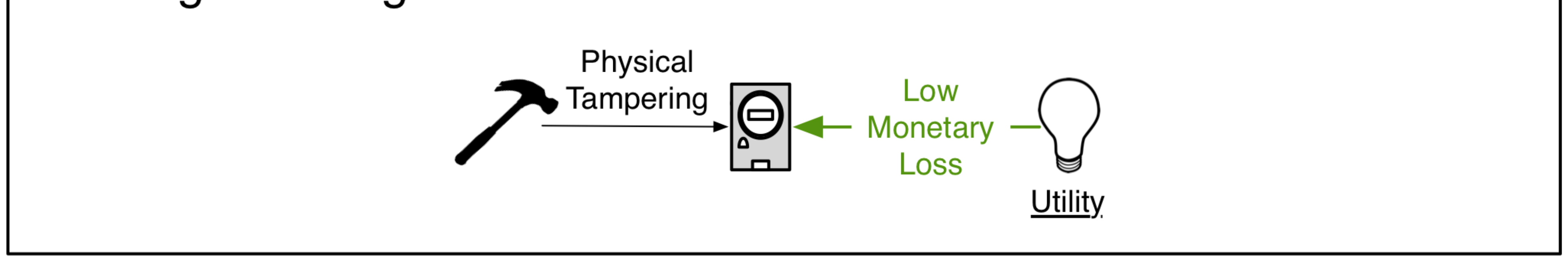


AMI Components

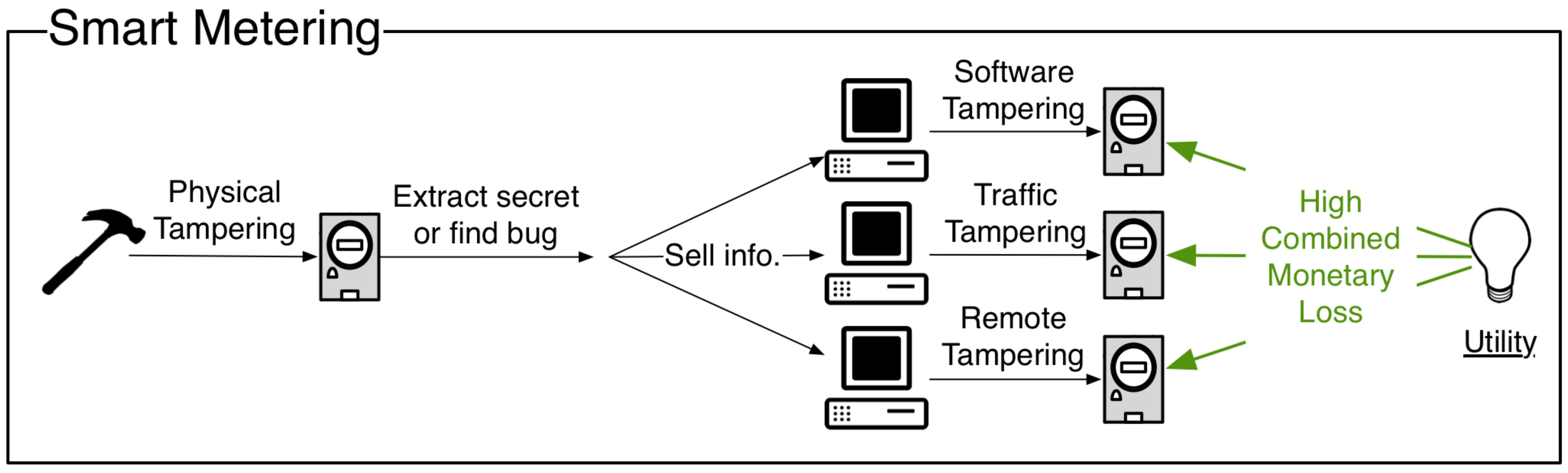
- The **backhaul network** connects gateway meters and utilities for remote meter reading.
- **Meter LANs** route demand and outage information to the gateway.
- Home area networks of **smart appliances** interact with meters to spread out peak demand

Impact of AMI on Theft of Service

Analog Metering

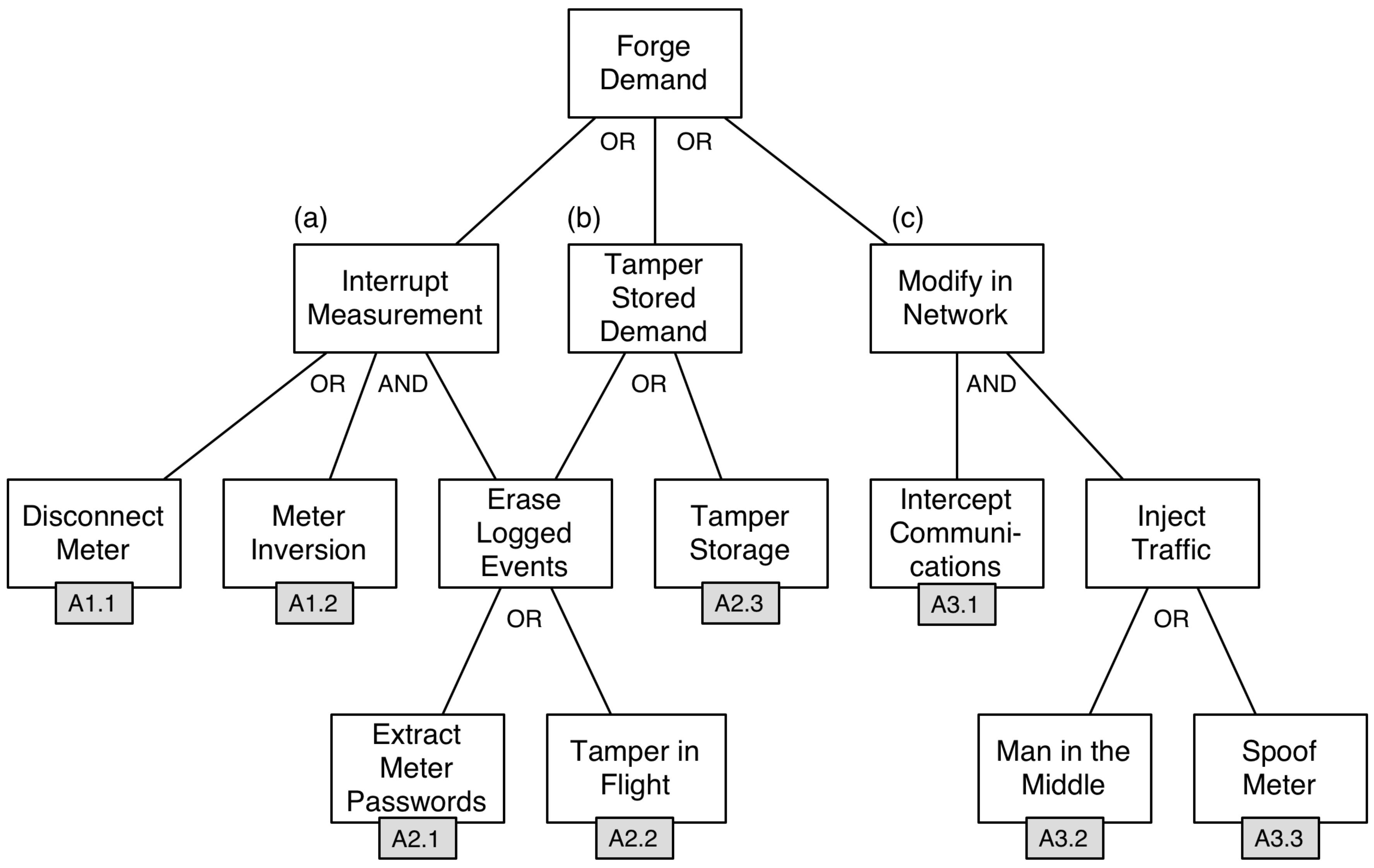


Smart Metering



The complexity of smart metering systems causes an amplification of adversary effort over analog meters. In the case of analog metering, a single high risk attack has little economic impact on the utility. Because smart metering systems rely on secrets such as passwords and keys, a single high risk physical compromise can lead to many low risk compromises. This monetization of security flaws in subscription based services has been seen before in the sale of stolen cell phone SIM unlock codes, and the distribution of cable TV descrambler devices.

Attack Tree Modelling



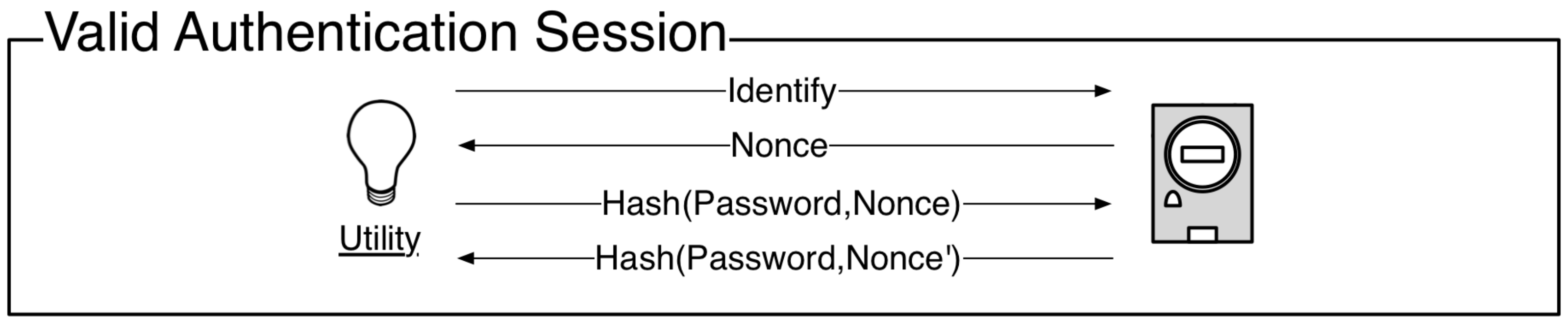
- Demand forgery (root node) is the goal of the tree
- Leaf nodes are the individual attacks needed to reach the goal

Proof of Concept Attack

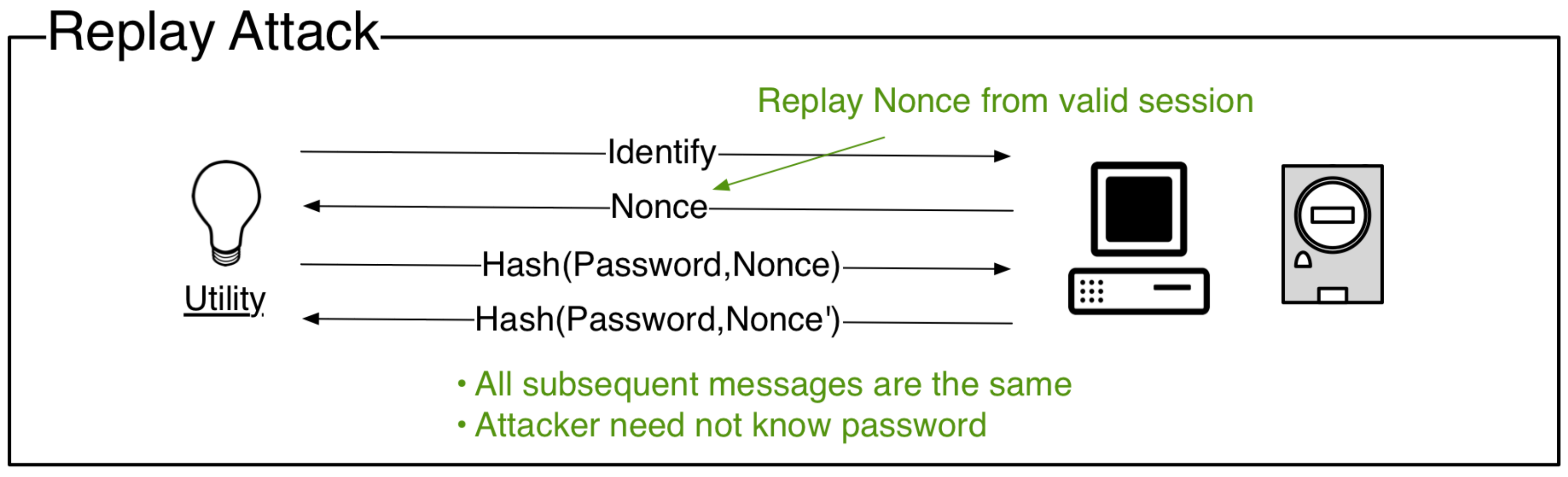
- We implemented a proof of concept attack for energy theft against a commercially available smart metering system.

- The attack uses a laptop computer to impersonate a meter during an automated meter reading.
- This is possible due to a flaw in the authentication protocol between utilities and meters.

Valid Authentication Session



Replay Attack


Replay Nonce from valid session
Identify
Nonce
Hash(Password,Nonce)
Hash(Password,Nonce')
Utility
• All subsequent messages are the same
• Attacker need not know password

- Once authenticated, the adversarial machine can forge demand values and eavesdrop on meter to utility communications.
- As the attack requires eavesdropping, we recorded the traffic on the utility side modem using bus snooping.
- In a real attack scenario, an adversary would interpose a device such as a private branch exchange in the meter's communication path and demodulate the intercepted signal.

Publications

Patrick McDaniel and Stephen McLaughlin, **Security and Privacy Challenges in the Smart Grid.** *IEEE Security & Privacy Magazine*, 7(3):75--77, May/June, 2009.

Stephen McLaughlin, Dmitry Podkuiko and Patrick McDaniel, **Energy Theft in the Advanced Metering Infrastructure.** *4th International Workshop on Critical Information Infrastructure Security (CRITIS 2009)*, Bonn, Germany. September, 2009.

Work Sponsored by Lockheed Martin