USAID
FROM THE AMERICAN PEOPLE

Smart meters and security

South Asia Regional Energy Partnership (SAREP)

Dr. Shailendra Fuloria
Nagarro
https://www.linkedin.com/in/sfuloria/

Introduction

- Shailendra Fuloria
- Managing security for Nagarro
- PhD in Information Security, 2012. University of Cambridge

- Worked at Cisco, ABB, Eaton and Nagarro
- Experience in security engineering across IT and OT
- Building security products
- Building products securely
- Managing security operations
- Selling security

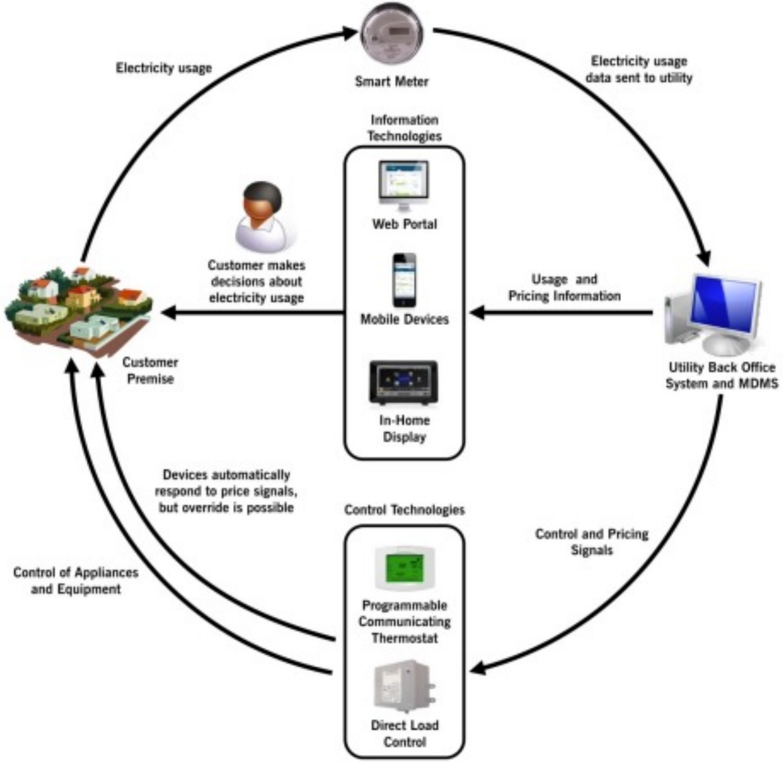
- Contact: https://www.linkedin.com/in/sfuloria/
  sfuloria@gmail.com

“You shall not pass…”

Agenda

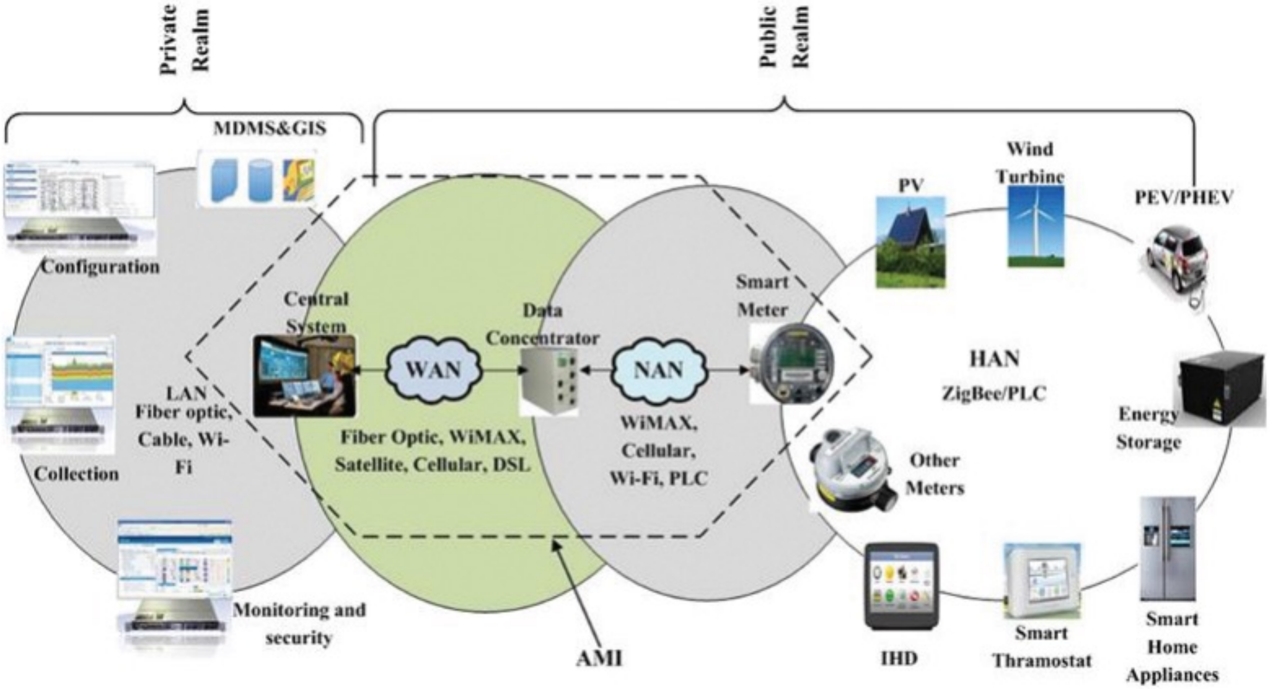
- High level AMI design and components
- Typical AMI architectures across the world
- Threat actors and motivations
- Attack points
- Specific security challenges and solutions

Advance Metering Infrastructure (AMI) highlights


Smart Meter
Electricity usage
Electricity usage data sent to utility
Information Technologies
Web Portal
Mobile Devices
In-Home Display
Customer makes decisions about electricity usage
Usage and Pricing Information
Utility Back Office System and MDMS
Customer Premise
Devices automatically respond to price signals, but override is possible
Control Technologies
Control and Pricing Signals
Control of Appliances and Equipment
Programmable Communicating Thermostat
Direct Load Control

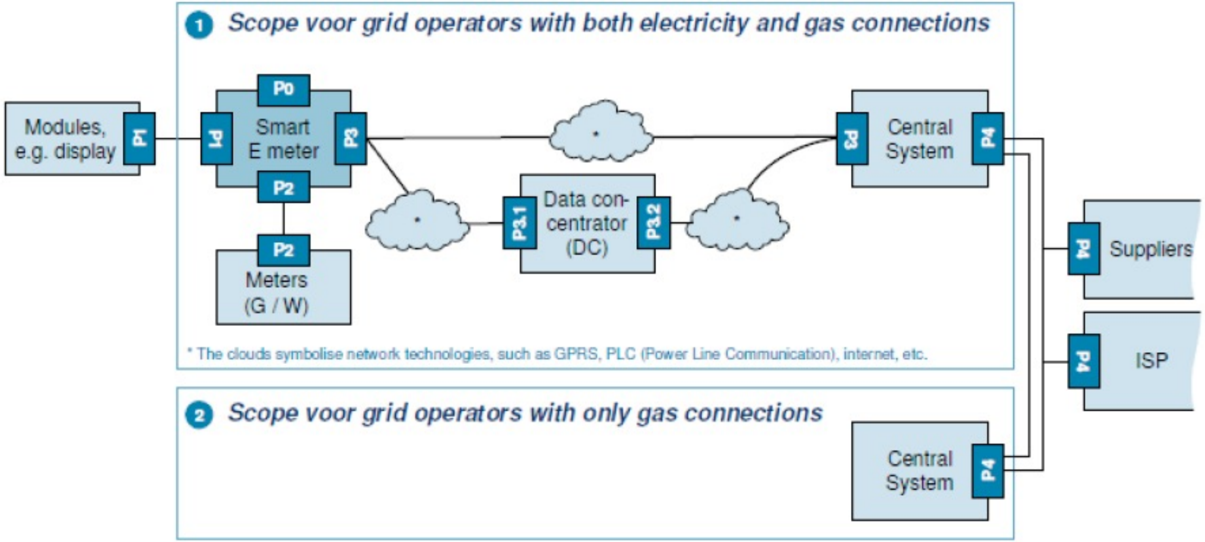
- Many countries adopting a smart meter or AMI deployment program
- Beneficial for the consumer, the energy supplier, the utility company, the environment…
- Two-way channel taking meter readings and sending pricing signals for a more responsive electrical grid
- Reduced electricity bill through better pricing signals
- Choice of electricity (green/brown)
- Reduced emissions, better environment
- Peak-demand shaving
- Better integration of distributed energy resources

High level AMI architecture



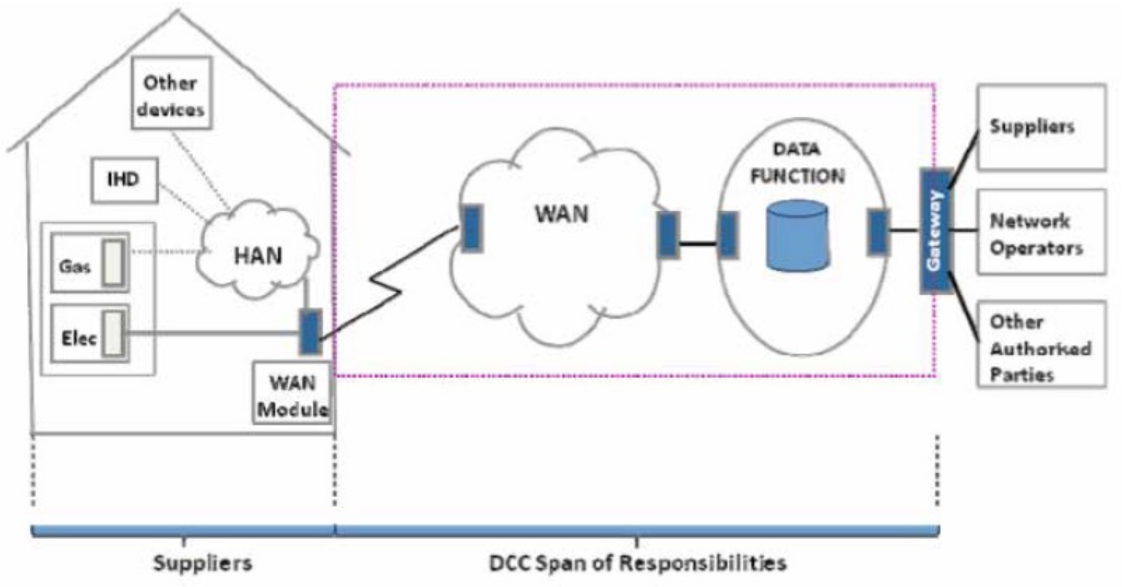
https://www.semanticscholar.org/reader/69eef4094aff56f34b87758d338cf7e80e8ae4ec

Global AMI deployment architectures – Netherlands


1 Scope voor grid operators with both electricity and gas connections
Modules, e.g. display
P1
P1
P0
Smart E meter
P3
P2
P2
Meters (G / W)
Data con-centrator (DC)
P3.1
P3.2
P3
Central System
P4
P4
Suppliers
P4
ISP
* The clouds symbolise network technologies, such as GPRS, PLC (Power Line Communication), internet, etc.
2 Scope voor grid operators with only gas connections
Central System
P4

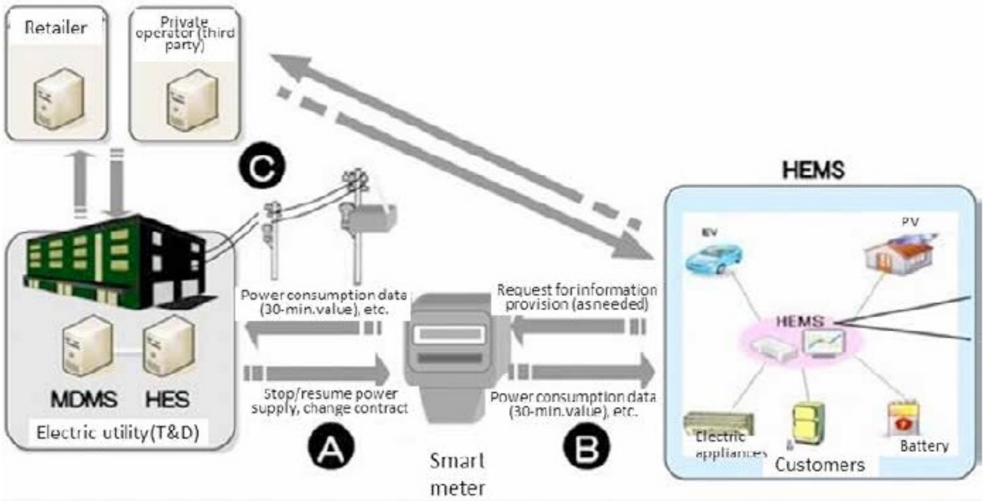
- Network operators responsible for maintaining a reliable advanced metering infrastructure
- Plan to deploy 15m smart meters across the country
- Suppliers and ISPs (Independent Service Providers) take meter data from a central system (Energie Data Services Nederland – EDSN)
- 15 min, hourly, daily, and monthly data recorded and stored
- ISPs can provide additional services (energy saving advice, visualization on mobile app…)

Global AMI deployment architectures – UK



- Centralized architecture through a Data Comms Company (DCC) to manage 53m meters
- 34 million smart meters installed by Dec 2023
- DCC acts as a central interface between energy retailers, network operators, the regulator, service companies and customers
- Meters owned by energy supplier. Customers can switch from one to another

Global AMI deployment architectures – Japan



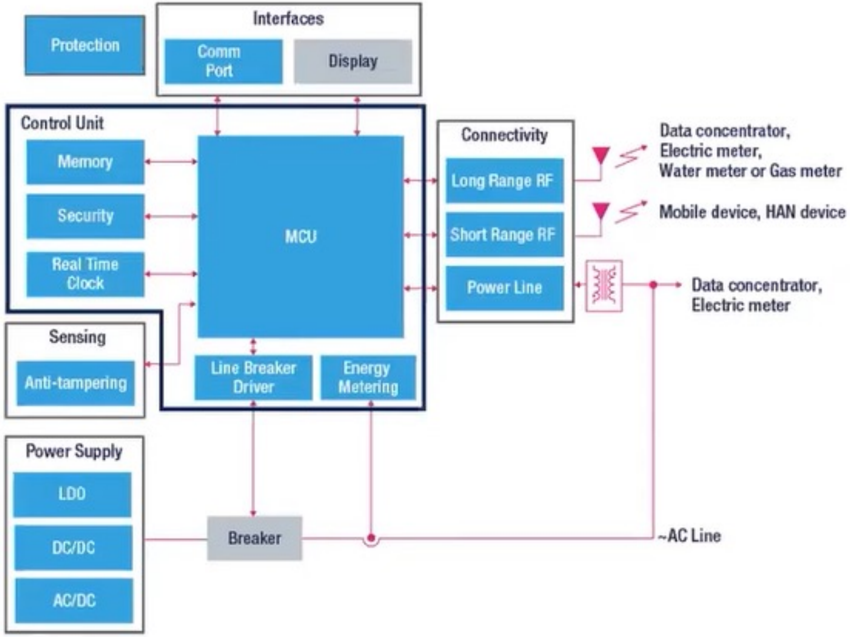
Retailer
Private operator (third party)
C
HEMS
EV
PV
HEMS
Power consumption data (30-min.value), etc.
Request for information provision (asneeded)
MDMS
HES
Electric utility(T&D)
Stop/resume power supply, change contract
A
Smart meter
Power consumption data (30-min.value), etc.
B
Electric appliances
Customers
Battery

- Japan has opted for a distributed architecture. 28m smart meters already deployed
- The data from smart meters can be shipped to the energy utility through two mechanisms:

Smart meter data is transferred to the Head End System (HES) and then to the Meter Data Management System (MDMS) both of which are owned and operated by the utility. The utility can share this data with a retailer or a third party with customer’s consent

Transfer of smart meter data to a Home Energy Management System (HEMS) which then transmits it to a third party over the internet. This third party then shares the consumer data with the utility according to predefined agreements

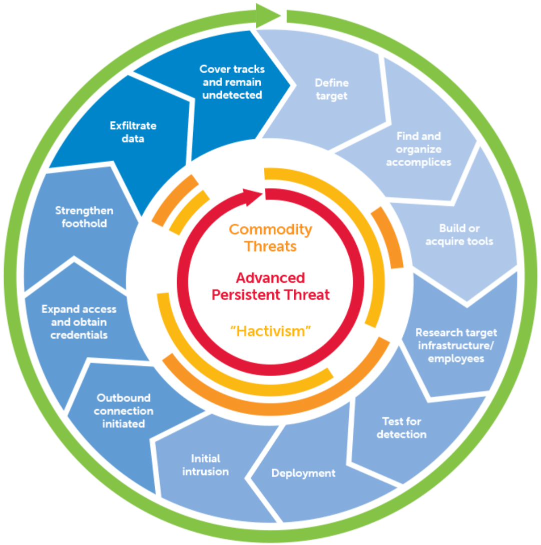
Smart meter architecture



- Three main parts: power supply, metrology unit, and comms unit
- Metrology unit:
  - Embedded Microcontroller Unit (MCU) has the metrology firmware
  - Runs embedded RTOS
- Communication Unit for bidirectional communication
  - Radio SoC (System on Chip)
  - RTOS/RT Linux
- Typical lifetime of 10 – 15 years
- Integrated load limiting, connect and disconnect switch
- Tamper event detection, recording and reporting
- Remote firmware upgrade
- On demand reading

Security in smart meters and AMI

Threat model



Cover tracks and remain undetected
Define target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Commodity Threats
Advanced Persistent Threat
"Hactivism"

- *Curious eavesdroppers:* Who just want to know about the activities of their neighbours
- *Motivated eavesdroppers:* Who want to gather information for malicious purposes
- *Unethical customers:* Who want to steal electricity and not pay for the services
- *Malicious insiders:* Who are disgruntled and want to cause harm to the energy company
- *Intrusive data management agencies:* Who want to gather private information and create user profiles for marketing and economic purposes
- *Active attackers:* Who want to perform large-scale attacks and sabotage. This would include nation states
- *Publicity seekers:* Who are more interested in getting famous rather than harming the users and gaining financial rewards

Source: Farid Molazem, Security and Privacy of Smart Meters: A Survey

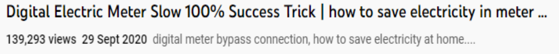
Threat vectors across AMI components

- Threats to meters
  - Unauthorized access compromising integrity and functionality
  - Physical tampering leading to inaccurate readings or disruption
  - Firmware manipulation
- Threats to the network hub
  - Sniffing, traffic analysis
  - MitM replay/fault injection attacks
  - Denial of Service (DoS) attacks, jamming

Threat vectors across AMI components

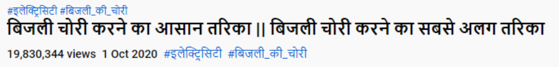
- Threats to remote management network
  - Unauthorized access gaining access to management systems
  - Data manipulation and altering meter configurations remotely
  - Eavesdropping for sensitive data
- Threats to distribution servers
  - Malware and ransomware infection
  - Insider threats

Approaching security at the meter level



Digital Electric Meter Slow 100% Success Trick | how to save electricity in meter ...

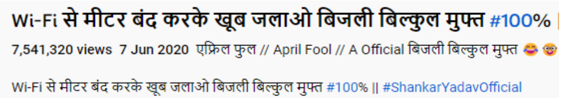
139,293 views 29 Sept 2020 digital meter bypass connection, how to save electricity at home....



#इलेक्ट्रिसिटी #बिजली_की_चोरी

बिजली चोरी करने का आसान तरिका || बिजली चोरी करने का सबसे अलग तरिका

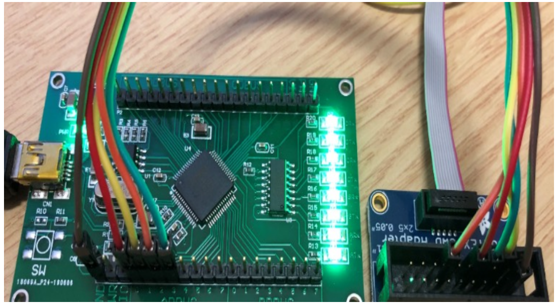
19,830,344 views 1 Oct 2020 #इलेक्ट्रिसिटी #बिजली_की_चोरी



Wi-Fi से मीटर बंद करके खूब जलाओ बिजली बिल्कुल मुफ्त #100%

7,541,320 views 7 Jun 2020 एप्रिल फुल // April Fool // A Official बिजली बिल्कुल मुफ्त 😂 🤓

Wi-Fi से मीटर बंद करके खूब जलाओ बिजली बिल्कुल मुफ्त #100% || #ShankarYadavOfficial



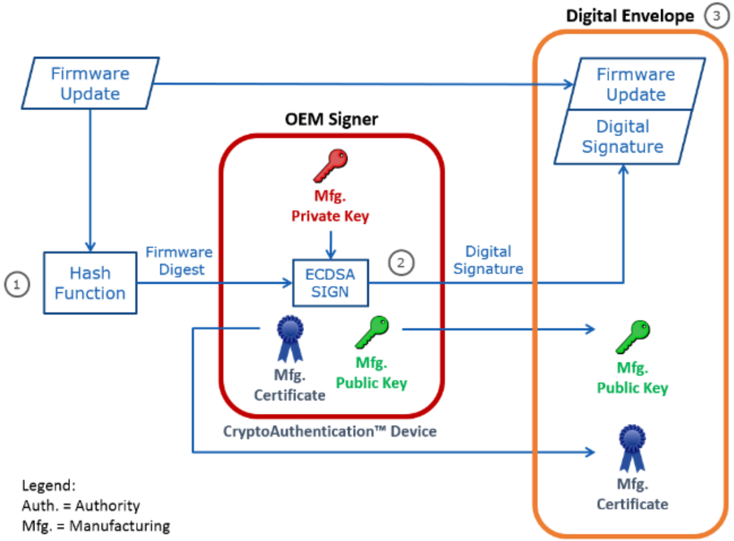
- Layered security
  - Secure access using optical codes
  - Protect settings through config access passwords
  - Ensure accurate config data through error correction
  - Encryption for firmware security
- Intrusion detection
  - Monitor optical and radio access through HIDS
  - Notify utility promptly through alerts and messages
- Physical tampering alerts
  - Tilt warning hall sensors (magnetic influences), physical tamper detection
  - Map consumption patters from transformers to meters

Remote management poses security challenges

- Motivations for a remote disconnect feature: demand response, pre-payment, curtailing fraud
- It can become a strategic vulnerability leading to extortion or sabotage
- Consider, for example, the UK smart meter system...
- Strong cryptography needed to ensure *bi-directional authentication and message integrity* between the utility systems and the meter
- The utility headend system itself becomes a critical information infrastructure
- Have proper Business Continuity Plans (BCP) and Disaster Recovery (DR) plans in place. Tested frequently

https://www.cl.cam.ac.uk/~rja14/Papers/meters-offswitch.pdf

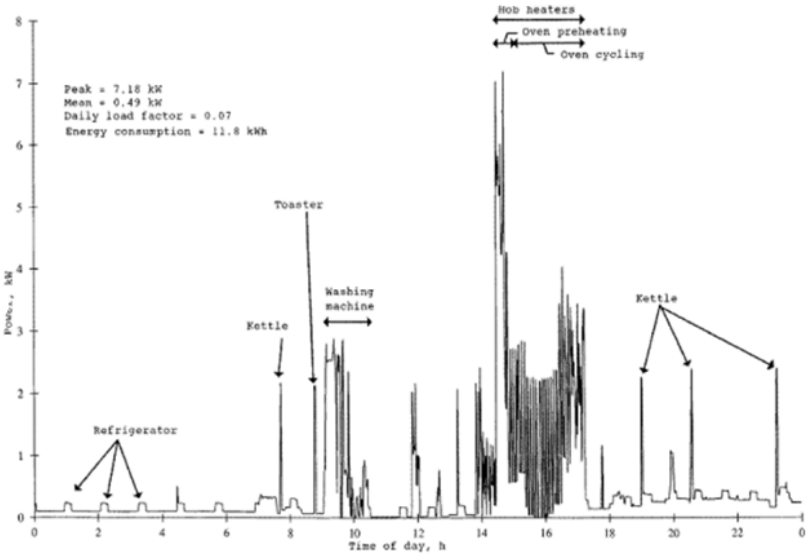
Security challenges with OTA upgrades



- Typical lifetime of a smart meter ~ 10-15 years
- Firmware upgrades needed
  - Improve meter performance
  - Enhance features, add new functionality
  - Achieve compliance to evolving standards

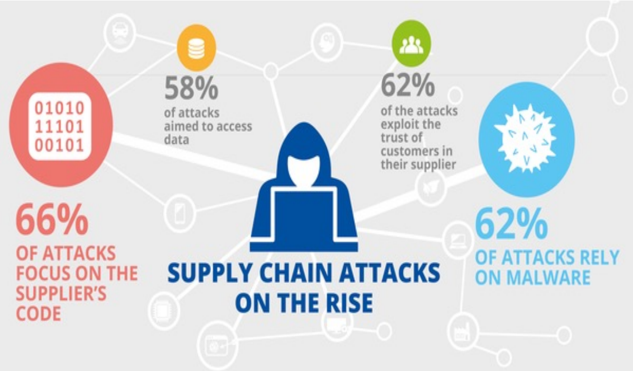
- Authentication/verification of new firmware before upgrade is essential
- Typical approach is to use digital signatures for authentication and verification
- Firmware may also be encrypted to ensure no sensitive data is leaked
- Proper key management with revocation protocols is essential
- Lightweight system essential

Privacy challenges



- Many countries have enforced regulation for strict control on data ownership and protection
- User details such as customer name, address, location etc are not transmitted
- Most countries collecting data in intervals of 15 – 60 mins
- Fine-grained energy consumption of data can reveal personal information (which can be sensitive)
- Several countries have seen lawsuits
- Indian data privacy regulation recently released
- Best follow ‘privacy by design’ approach and proper privacy impact assessment and anonymization

Ensuring a sanitized supply chain (1/2)

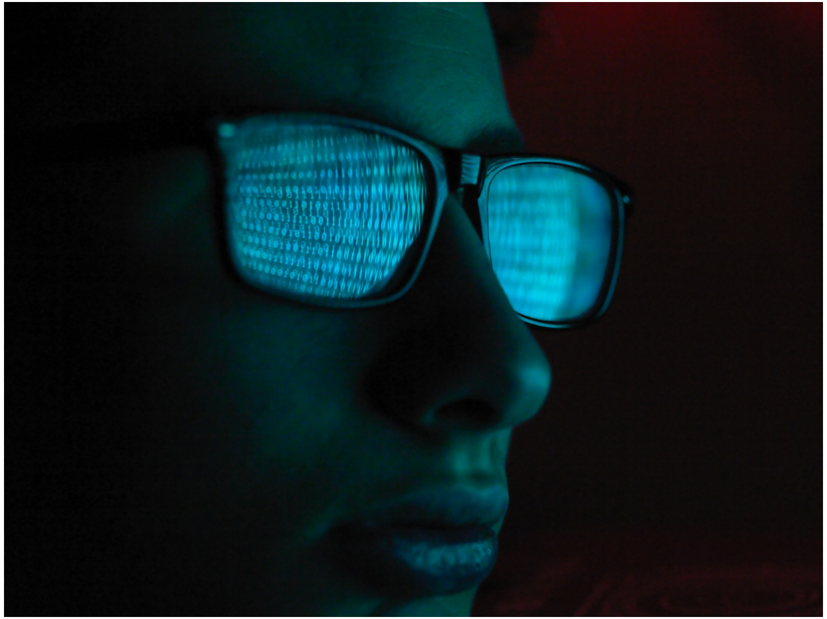

01010
11101
00101
58%
of attacks aimed to access data
62%
of the attacks exploit the trust of customers in their supplier
66%
OF ATTACKS FOCUS ON THE SUPPLIER'S CODE
SUPPLY CHAIN ATTACKS ON THE RISE
62%
OF ATTACKS RELY ON MALWARE

- Identity, data and device integrity key in ensuring supply chain security
- This involves complex Device | Supplier | Geography interactions that are hard to observe and control
- Opacity on supplier – component mapping. OEMs don’t monitor fully
- Security of open-source components is also complex
- Risk of sabotage by a malicious insider through a logic bomb in the firmware or hardware trojan
- Ensuring right protection

Ensuring a sanitized supply chain (2/2)

- Maintain SBOM with mappings
- Define clear lifecycle management process with ownership (even after EOL)
- Defined punitive action against suppliers for failing to meet security standards
- Setup independent testing facilities that work with utilities (and not meter manufacturers). Must test for fault attacks, side-channel attacks, firmware reverse engineering
- Declaration of all software components used by all suppliers. Helps in maintain licensing compliance and security

Threat-centric vs infrastructure-centric security



- Threat-Centric: Focuses on identifying and eliminating cyber threats
- Infrastructure-Centric: Prioritizes creating a robust, well-protected OT infrastructure
- Focus first on infrastructure-centric security
  - Secure the network: Network segregation, access controls
  - Secure the endpoints: Minimize software, have SBOM, minimize comms protocols, specify groups of endpoints having similar security needs and apply security policy

Summary

- AMI and smart meters would become a critical national infrastructure for any country
- Getting security infrastructure right the first time is critical since recalling and replacing field equipment is costly and time consuming
- Recycle technology that exists as it's likely to have fewer bugs. Desist the temptation to create something totally new
- Get architecture and systems reviewed by multiple experts. Frequently
- Prolonged field testing is critical to know real-world challenges and failure modes

Thank You!

https://www.linkedin.com/in/sfuloria/