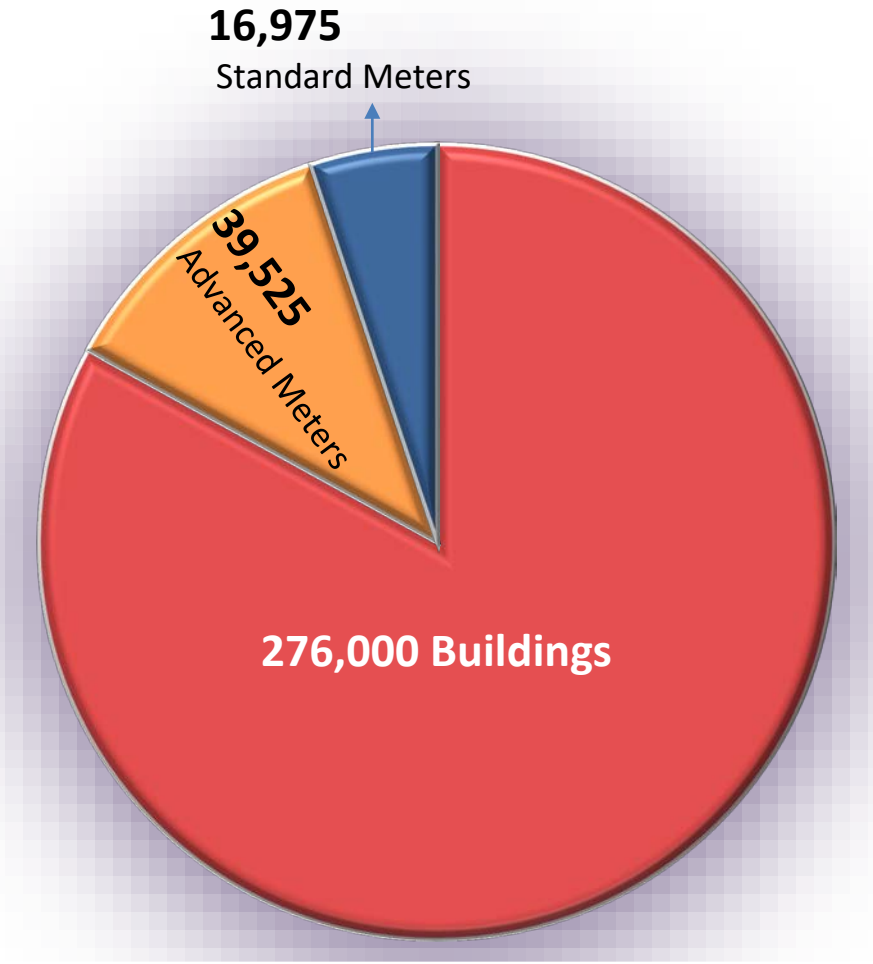
Interagency Sustainability Working Group

Cyber Security Challenges for Metering and Enterprise Systems



Currently: 33% Advanced Meters

Minimum 60% with goal of 85% by 2020

How Vulnerable Can They Be…

Serious vulnerabilities in smart electricity meters continue to expose both consumers and electric utilities to cyberattacks.

Attacks can be prevented with proper encryption, by implementing network segmentation and by monitoring smart meter networks.

Claims that hackers can cause these devices to explode.

http://www.securityweek.com/smart-meters-pose-security-risks-consumers-utilities-researcher

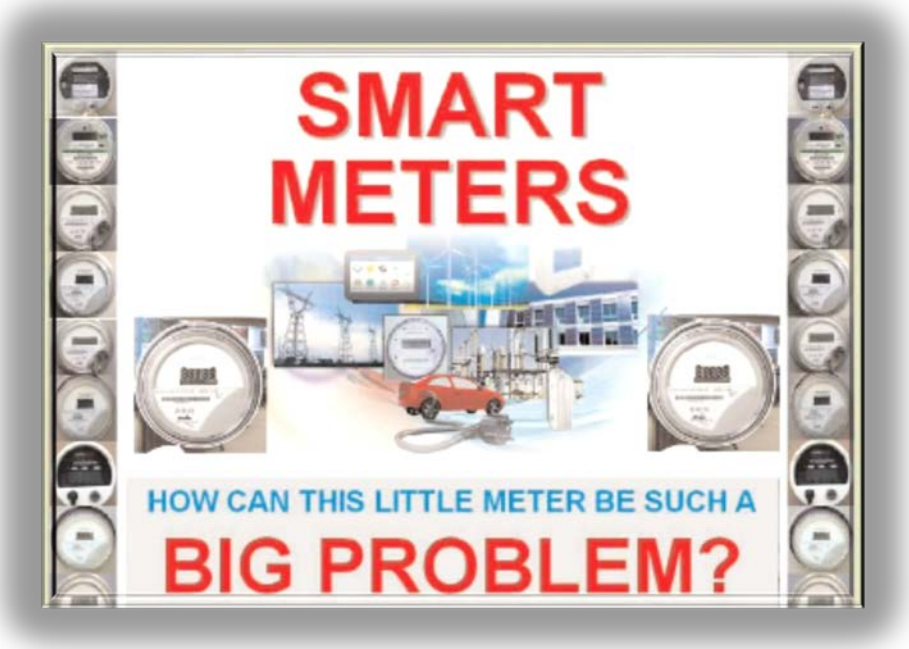
DHS ICS CERT Alert

Researchers have discovered several vulnerabilities affecting smart meters from Schneider and Feniks Pro.

Vulnerabilities include: security issues related to power and energy monitoring systems access control, cross-site requests forgery, weak credentials management, unauthorized configuration changes, weak default passwords and password recovery.

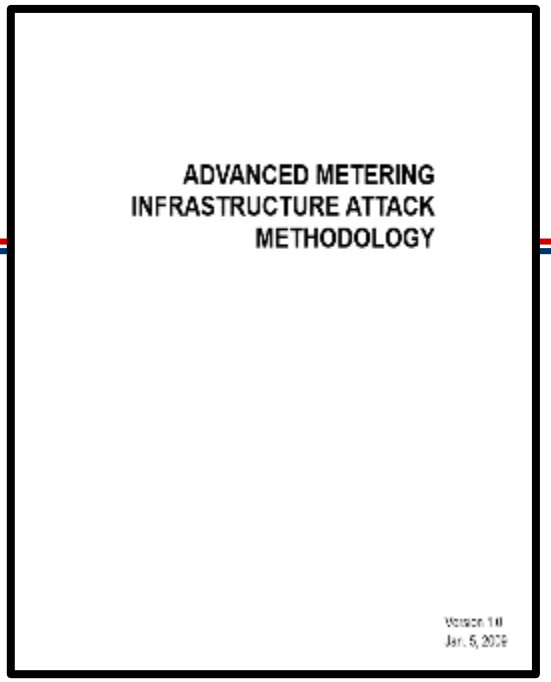
http://www.securityweek.com/ics-cert-issues-alerts-after-expert-discloses-power-meter-flaws

Challenges and Considerations



- Implementation of a “Kill Switch” on smart meters could cause instability and cascading failures.
- Other smart devices located in a home or facility could easily be hijacked if smart meters are hacked.
- Lack of comprehensive investigation and sharing of lessons learned.
- Electric utilities have suffered millions of dollars in losses due to smart meter fraud.

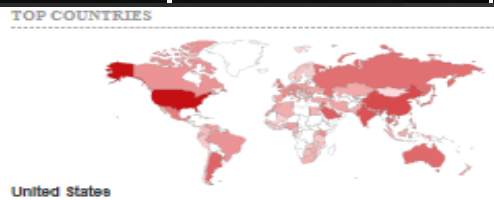
Published AMI Attack Methodology



Document describes AMI Security Acceleration Project (ASAP) Red Team approach to security testing of different AMI architectures. Specifically focuses on external equipment employing embedded computer architectures, not physically protected by utility-premise security measures.

http://www.inguardians.com/articles.html

Locating Connected Devices



TOP COUNTRIES

United States	7,351
China	2,281
India	1,506
Saudi Arabia	1,481
Argentina	1,263

TOP SERVICES

Telnet	23,567
HTTP	4,179
FTP	3,357
HTTP (8080)	1,058
HTTP (81)	445

TOP ORGANIZATIONS

NTT America	2,739
Telecom Argentina S.A.	1,109
SaudiNet	839
TATA Communications	585
Comcast Cable	489

TOP OPERATING SYSTEMS

Linux 2.6.x	15

Total results: 33,575

161.58.142.58
va20175.securesites.net
NTT America
Added on 2016-03-16 11:19:56 GMT
United States, Englewood
Details

220-
220-##
220-Welcome to your FTP server!
220-
220-Root login via FTP is disallowed by default. Please use an SFTP client
220-(or other secure protocol such as SSH) to connect as root for file
220-transfers.
220-
220-If you are...

61.19.28.98
The Communication Authority of Thailand, CAT
Added on 2016-03-16 11:18:54 GMT
Thailand
Details

Cisco Configuration Professiona
This feature requires the one-tim
password "cisco". These default

60.173.217.8
China Telecom Anhui
Added on 2016-03-16 11:18:40 GMT
China, Hefei
Details

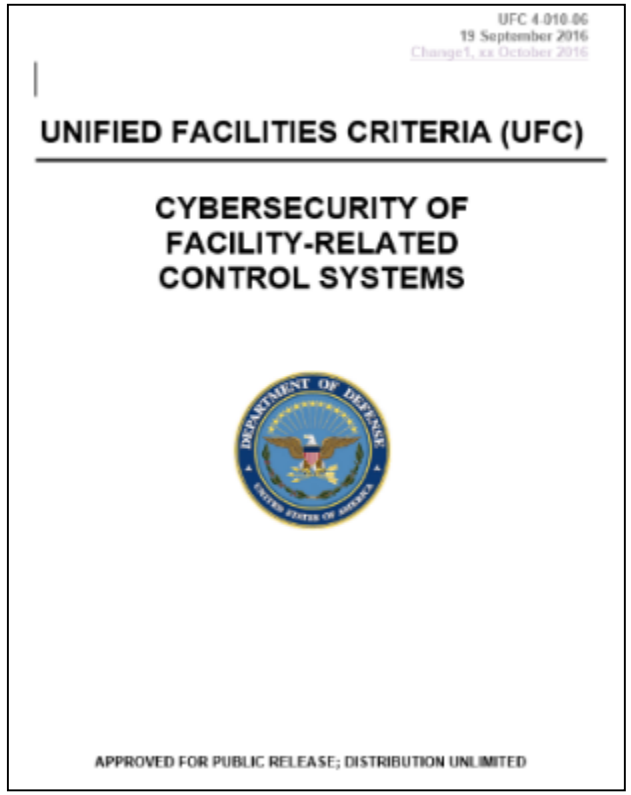
Cisco Configuration Professiona
This feature requires the one-tim
password "cisco". These default

61.16.177.1
mum-static-1-17[illegible]
Direct Internet
Added on 2016-03-16 11:18:25 GMT
India, Mumbai
Details

Cisco Configuration Professional (Cisco CP) is installed on this device.
This feature requires the one-time use of the username "cisco" with the
password "cisco". These default credentials have a privilege level of 15....

UNCLASSIFIED

Cybersecurity Controls Apply to New Construction


UFC 4-010-06
19 September 2016
Change1, xx October 2016

UNIFIED FACILITIES CRITERIA (UFC)

CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

1. Define new Design and Construction Methodology to apply RMF & NIST SP 800-82 ICS Security Guide
2. Define IT / CS Reference Architecture as it applies to Control Systems
3. Verify controls @ 50-75% construction: conduct Factory Acceptance Testing (FAT) of major components
4. Verify controls @ 100% construction complete: conduct Site Acceptance Testing (SAT)

Standards/Question Sets in CSET	Short Name
NIST Special Publication 800-53 Rev 3	800-53 R3
NIST Special Publication 800-53 Rev 3 App I	800-53 R3 App I
NIST Special Publication 800-53 Rev 4	800-53 R4
NIST Special Publication 800-53 Rev 4 App J	800-53 R4 App J
NIST Special Publication 800-82	SP800-82
NIST Special Publication 800-82 Rev 1	SP800-82 V1
NIST Special Publication 800-82 Rev 2 (Draft)	SP800-82 V2
Consensus Audit Guidelines (CAG)	CAG
Components Questions Set	Components
CFATS Risk-Based Performance Standards Guide 8-Cyber	CFATS
CNSSI No. 1253 Baseline	CNSSI 1253
CNSSI No. 1253 Industrial Control System (ICS) Overlay V1	CNSSI ICS
Catalog of Recommendations Rev 7	COR 7
DOD Instruction 8500.2	DOD 8500.2
INGAA Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry	INGAA
Key Questions Set	Key
NIST Framework for Improving Critical Infrastructure Cybersecurity V1	NCSF V1
NEI 0809 Cyber Security Plan for Nuclear Power Reactors	NEI 0809
NERC CIP-002 through CIP-009 Rev 3	NERC Rev 3
NERC CIP-002 through CIP-009 Rev 4	NERC Rev 4
NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 1	NISTIR 7628
NRC Regulatory Guide 5.71	NRC 5.71
TSA Pipeline Security Guidelines April 2011	TSA
Universal Questions Set	Universal

UFC 4-010-06 Published 19 Sept '16

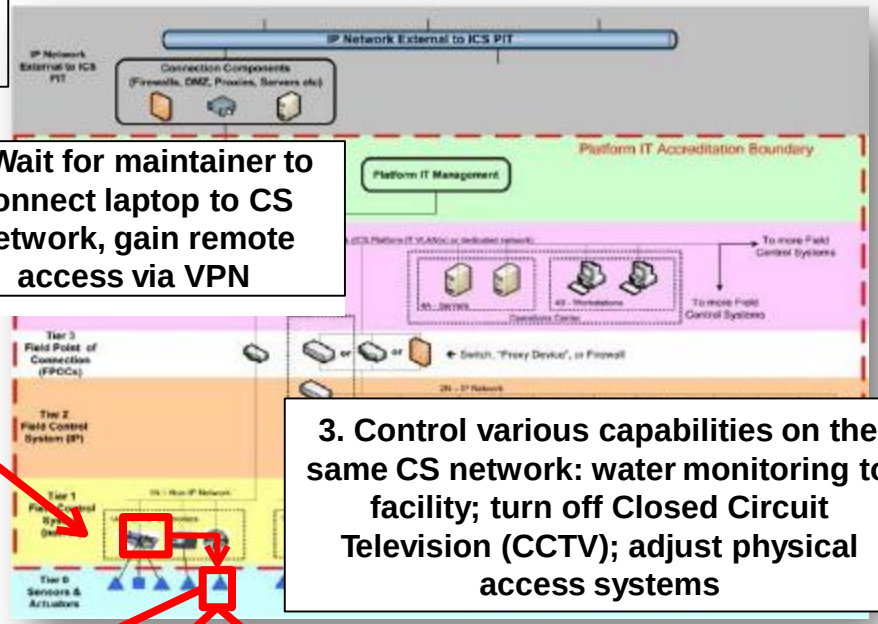
Cybersecurity Guidelines

https://serdp-estcp.org/Investigator-Resources/ESTCP-Resources/Demonstration-Plans/Cybersecurity-Guidelines

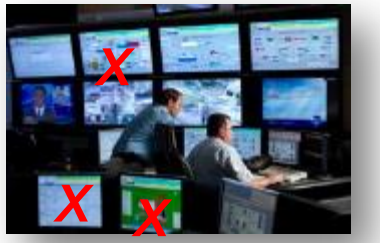
Illustrative Scenario: Remote Control of Systems Sharing Network

1. Target an internet connected maintenance laptop with malware

2. Wait for maintainer to connect laptop to CS network, gain remote access via VPN



3. Control various capabilities on the same CS network: water monitoring to facility; turn off Closed Circuit Television (CCTV); adjust physical access systems



Results in

4. Results in preparations for unauthorized entry to enable physical theft and/or damage to facility

- Specific Attack: Exploit Windows 7 maintenance laptop for VPN access to CS networks
- Level of Effort: DSB Tier 2; novice capability to access CS network and breach the controlled facility
- Impact: Targeting a maintenance worker's system can allow internal access to facility CS

A Note From Our Sponsor…

DoD facilities transitioning to smart buildings; increased connectivity has increased threat and vulnerability to cyber-attacks, particularly in ways existing DoD regulations were not designed to consider. Therefore, SECDEF deliver a report:

(1) Structural risks inherent in control systems and networks, and potential consequences associated with compromise through a cyber event;

(2) Assesses the current vulnerabilities to cyber attack initiated through Control Systems (CS) at DoD installations worldwide, determining risk mitigation actions for current and future implementation;

(3) Propose a common, DoD-wide implementation plan to upgrade & improve security of CS and networks to mitigate identified risks;

(4) Assesses DoD construction directives, regulations, and instructions; require the consideration of cybersecurity vulnerabilities and cyber risk in preconstruction design processes and requirements development processes for military construction projects; and

(5) Assess capabilities of Army Corps of Engineers, Naval Facilities Engineering Command, Air Force Civil Engineer Center, and other construction agents, as well as participating stakeholders, to identify and mitigate full-spectrum cyber-enabled risk to new facilities and major renovations.

CS include, but are not limited to, Supervisory Control and Data Acquisition Systems, Building Automation Systems Utility Monitoring and Energy Management and Control Systems. Such report shall include an estimated budget for the implementation plan, and delivered no later than 180 days after the date of the enactment of this Act.

Non Partisan "We Care!"