Security Landscape

The Smart Grid Realm

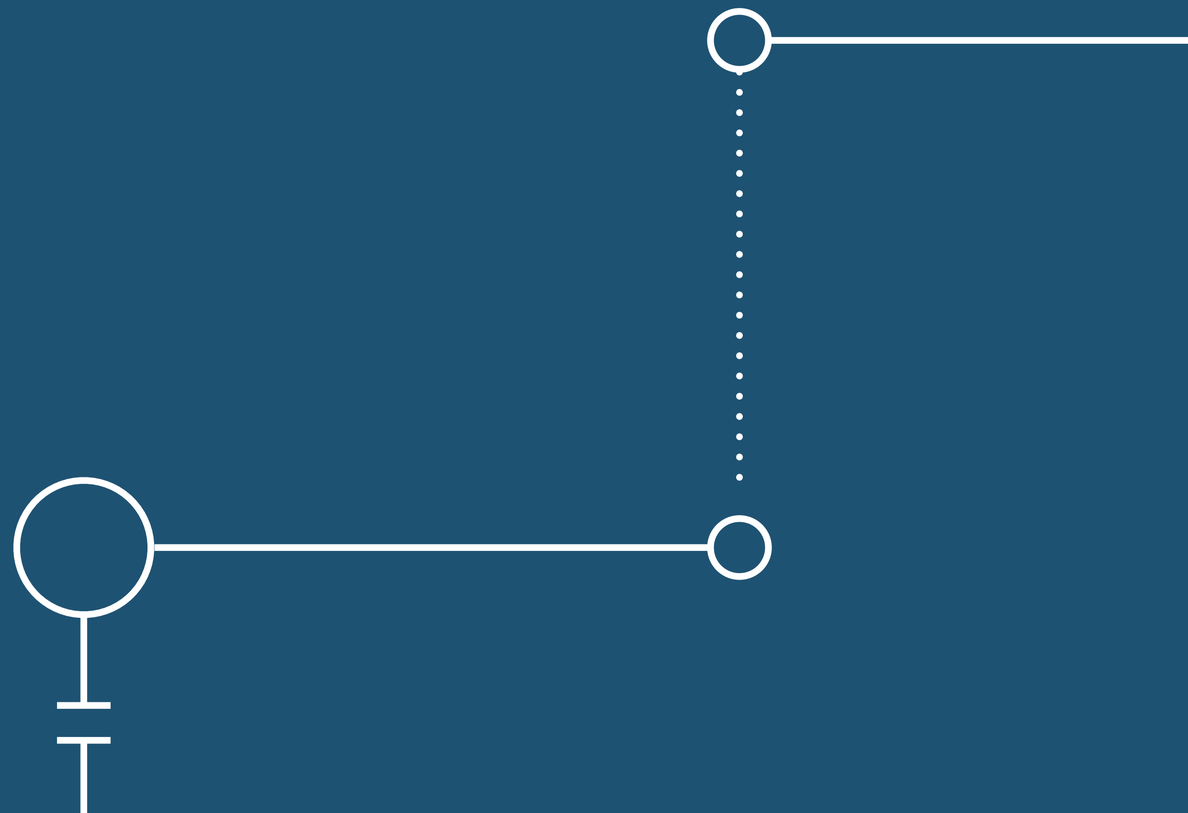
25/5/2016

++

MWR InfoSecurity

+ 13 years of Cyber – Offensive and Defensive
+ Global
+ Research-led
+ Working with ADSC among others to improve the security of Singapore’s Smart City aims.
+ Financial/Government/Critical National Infrastructure
+ Singapore since 2014

- **What is Smart Grid**
- What does this mean in practice
- Case studies
- Security considerations
- What we typically see
- How we review
- Questions?



++

What is Smart Grid?

+ Moniker for applying information technology to improve the ‘electric grid’
+ Make energy usage and distribution greener and more intelligent
+ Cost saving and increased reliability
+ Allows real-time reaction and automation of response to consumer demands

++

What is Smart Grid?

+ Similar concepts as smart-everything in terms of implementation

+ ‘Smart Grid’ is one utilization of ‘Smart Technology’

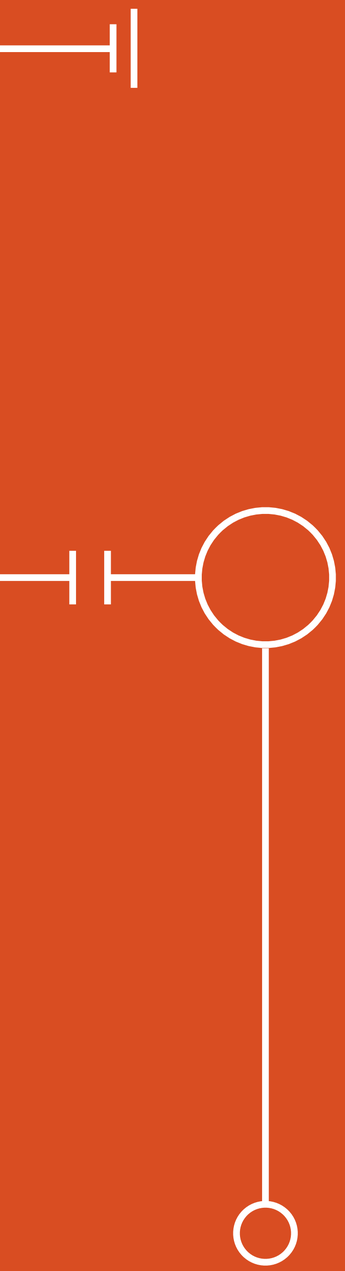
+ About automation

+ Similar security concerns

++

Primary aims of Smart Grid

+ Smart Grid defined in Energy Independence and Security Act of 2007 (EISA-2007)
+ Approved by the US Congress in January 2007
+ Signed to law by President George W. Bush in December 2007
+ Details interoperability/communication standards
+ Aims to increase efficiency
+ Mandates security



+ What is Smart Grid
+ **What does this mean in practice**
+ Case Studies
+ Security implications
+ What we typically see
+ How we review
+ Questions?

++

What does this mean in practice?

+ Connect everything
+ Make everything remotely controllable
+ Information reporting
+ Increased efficiency in terms of energy usage
+ Power grids
+ Industrial systems
+ Consumer devices:
  Kettle, car, fridge, air con, locks, healthcare devices, lights

++

What does this mean in practice?

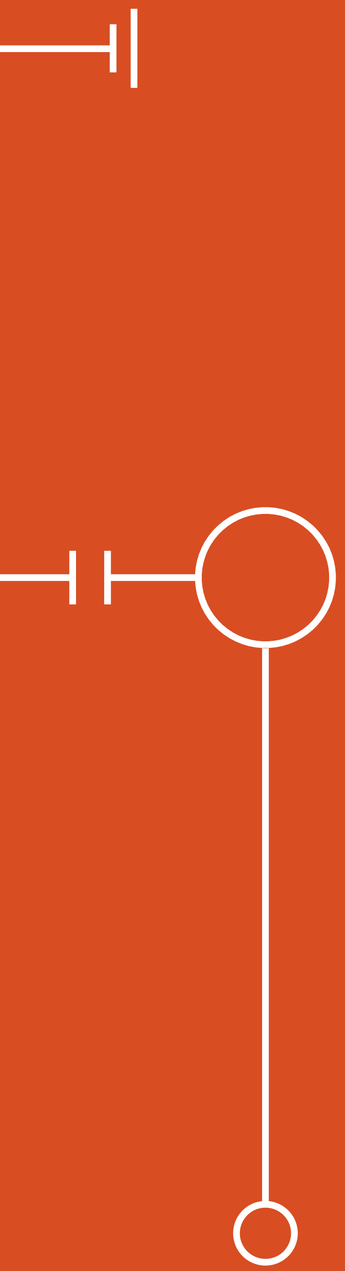
+ Remote access

+ Remote reporting

+ Applications for control in many guises
  - Thick clients
  - Custom protocols
  - Mobile/Web Applications

+ Cloud

+ Huge amount of information available



+ What is Smart Grid
+ What does this mean in practice
+ **Case Studies**
+ Security implications
+ What we typically see
+ How we review
+ Questions?

++

Case Studies

+ Nissan LEAF cars
+ Stuxnet
+ Smart meters
+ Steel Mill, Germany
+ Yale Smart Locks

++

Nissan LEAF cars

+ Electric ‘smart’ car
+ Control car features via mobile application
+ Talks to Cloud web API
+ No authentication

++

Nissan LEAF cars - IMPACT

+ Retrieve driving history

+ Control car components (AC, charging)

+ No life threatening impact

Stuxnet

- Iran
- State sponsored
- Highly targeted attacks
- Rewrote PLC controls via infected control machines
- Air Gapped
- Infected USB sticks to infect air gapped machines
- Lateral movement using Windows Odays once on the network
- Rewriting of PLC control software on one of these machines

++

Stuxnet - IMPACT

+ Delayed progress

+ Damage to critical centrifuges

+ Financial loss

+ Global embarrassment

++

Smart Meters

+ Targeted research
+ Deployed to automate meter reporting and reading
+ Same AES keys used across all devices
+ Flawed cryptography

++

Smart Meters - IMPACT

+ Financial fraud
+ Shut down power
+ Loss of integrity to the data generated
+ Rendered ineffective

++

Steel Mill, Germany

+ Spear-phishing
+ Malicious attachments
+ Lateral movement on the network
+ Attacking ICS from corporate network
+ Attackers had specific industry knowledge

++

Steel Mill, Germany - IMPACT

+ Significant equipment damage

+ Operations interrupted

+ Financial loss

++

Yale Home Locks

+ Man in the middle
+ Cryptography integrity flaws
+ Remote command execution against the Android phone application
+ Well known mobile attack methodology
+ Discovered and reported by MWR

++

Yale Home Locks - IMPACT

+ Mobile device compromised

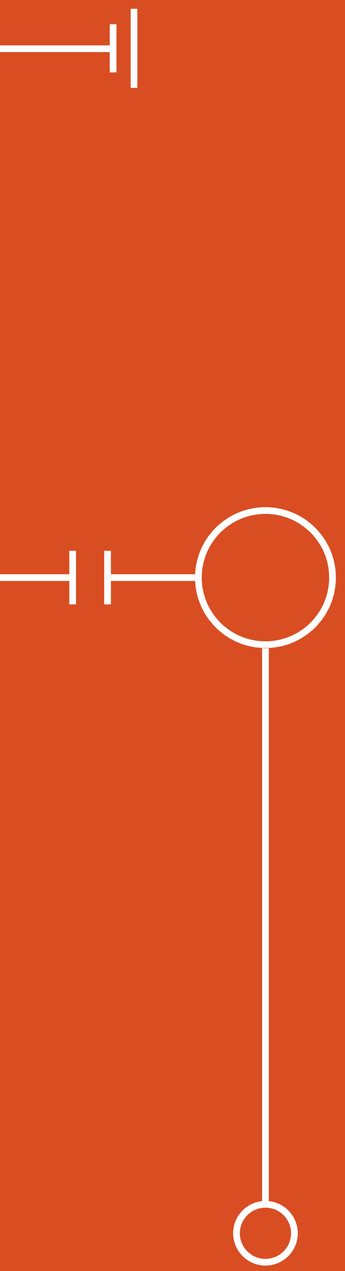
+ Can unlock home locks

+ Physical security compromised

++

Case Studies Summary

+ Common attack methods and mistakes made
+ Weak authentication
+ Large risk surfaces
+ Lack of separation
+ Lack of controls
+ Lack of secure development processes
+ Goal of attacker varies greatly and thus skill required



+ What is Smart Grid
+ What does this mean in practice
+ **Security implications**
+ Case Studies
+ What we typically see
+ How we review
+ Questions?

++

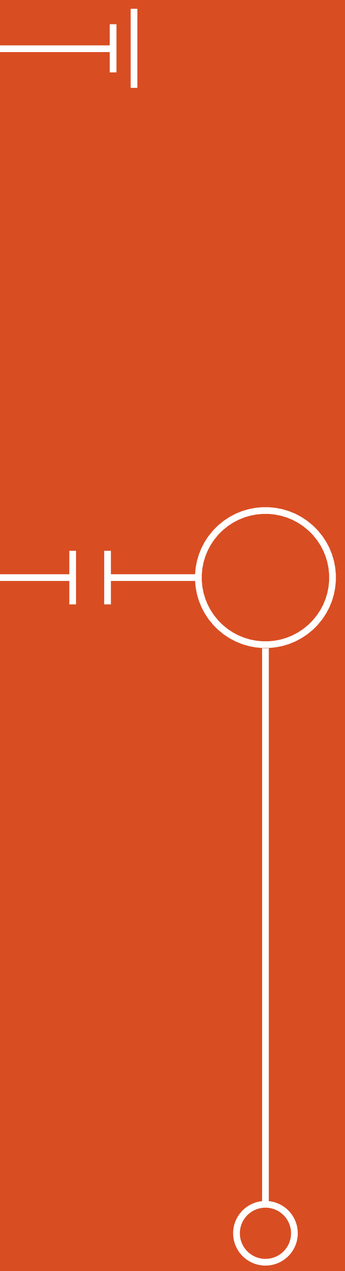
In the past

+ Information access
+ Espionage
+ Immediate consequences vary but typically no life threatening or physical damage consequences

++

Security Implications

+ Cities turned off
+ Pre-emptive strikes before war
+ Power grids/stations compromised
+ Buildings and offices unlocked
+ Fatalities
+ Mass amount of data



+ What is Smart Grid
+ What does this mean in practice
+ Case Studies
+ Security implications
+ **What we typically see**
+ How we review
+ Questions?

++

What we typically see

+ Issues at multiple levels
+ Software
+ Hardware
+ Controls

++

Software level

+ Unauthenticated protocols

+ Poorly implemented cryptography

+ Typical software vulnerabilities:
  Buffer Overflows
  OWASP Top 10
  MITM
  etc

+ Security implications of features not considered

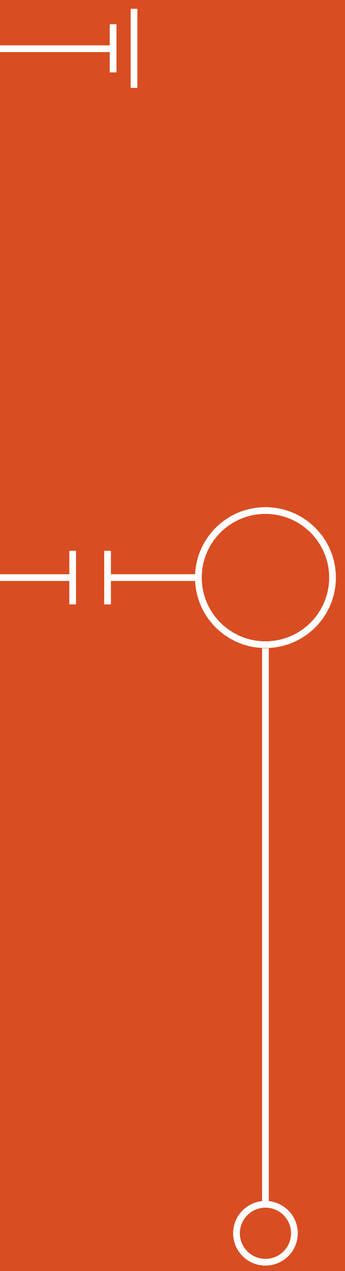
Hardware level

+ Level of sophisticated attack not considered
+ Does your environment expose network connectivity? (‘does your substation have a locked door?’)
+ Air gaps/clean environments
+ Policies around air gaps however, fail

++

Controls

+ Hardware and software security in place
+ Lack of policy controls renders these measures ineffective
+ Stuxnet
+ Human element always the weakest link



+ What is Smart Grid
+ What does this mean in practice
+ Case Studies
+ Security implications
+ What we typically see
+ **How we review**
+ Questions?

++

How we review

+ High level Threat modelling

+ Secure Design and Architecture Reviews

+ Typical software/security assurance activities but with specialized knowledge of smart technologies and environments (PLC programming, protocols, etc)

Threat modelling

+ Understanding specific concerns
+ Identifying ‘Threat Actors’
+ Mapping out usage and input vectors
+ Workflows
+ Attacker-centric threat modelling
+ Attack scenarios
+ Building in protections to defend against those attack scenarios with specific threat actors in mind.

++

Threat modelling

+ Vary based on scenario

+ Vary based on attacker
  - Scriptkids with Metasploit
  - Hacktivism/Hacktivists
  - Opportunistic Criminals
  - Organised Crime
  - Nation State (APT)

++

Secure Design and Architecture Review

+ Validate the security-related design features

+ Review:
  - Trust boundaries
  - How data flows
  - Entry points
  - Where privileged code resides

++

Software/Security Assurance Activities

+ Goal based penetration testing

+ Source code review

+ All informed by threat intelligence from community + GOVT

+ Threat modelling scenarios tested

+ TAS experience

MWR INFOSECURITY

+ What is Smart Grid
+ What does this mean in practice
+ Case Studies
+ Security implications
+ What we typically see
+ How we review
+ **Questions?**