RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: TECH-W02

The Mother of All Pen Tests

Robert Hawk
Principal Consultant
RBH Enterprises
www.LinkedIn.com/in/IronManRBH

Steve Vandenberg
Senior Managing Consultant
IBM Canada
www.LinkedIn.com/in/SteveVandenberg

Disclaimer

This presentation reflects the experience and observations of the presenters with Advanced Metering Infrastructure technology on multiple programs. It does not represent information or positions specific to any project, utility, its vendors or partners.

It is not a representation of the BC Hydro SMI program.

A tidal wave of complexity…

Smart Meters, Zigbee, IPv6, C12.22, Field Area Routers, PKI, IHD…

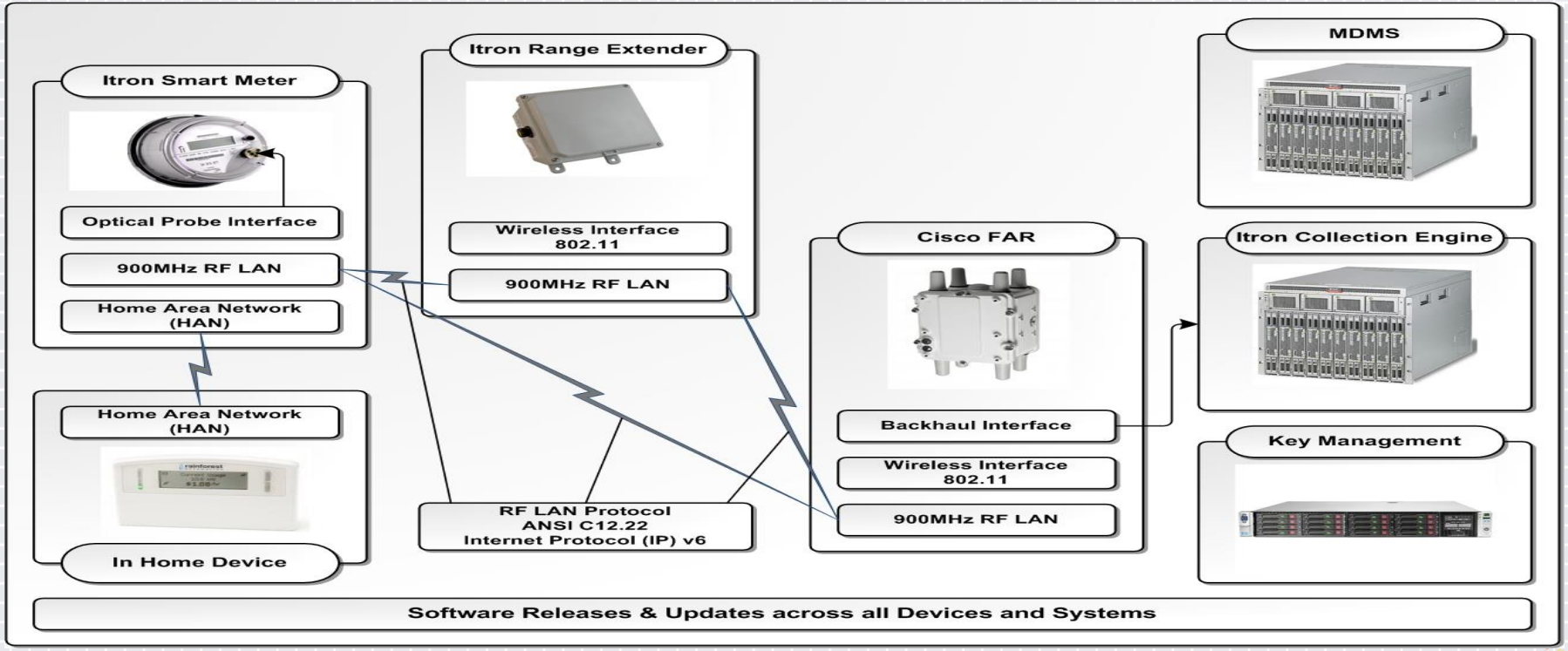
An Example: BC Hydro's AMI Deployment

- British Columbia is larger than CA, OR and WA combined
- 1.9 million Itron Smart Meters
- Thousands of Cisco Field Area Routers (FAR) and IPv6 Cisco Network
- Cost: $$$
- Deployment: 2011 through 2014

IT vs AMI Projects

Information Technology	Advanced Meter Infrastructure
3 to 5 year lifespan	Multi-decade lifespan field devices
1 to 3 fiscal quarters for deployment	2 to 5 year deployment
10’s of servers	100’s of servers
100’s of network devices	1,000’s of network devices
1,000’s of end nodes	1,000,000’s of end nodes

Security Test Scope



Standards Based Security Test Plans

- Common set of principles the client, vendors and service providers will accept and act on
- Standards based approach: AMISec & NIST IR 7628
- Interfaces and controls are the primary focal points
- Determine risk rating based on use case for each test. Prioritize testing based on this rating
- Be prepared to change test plans and priorities during test cycle in response to results

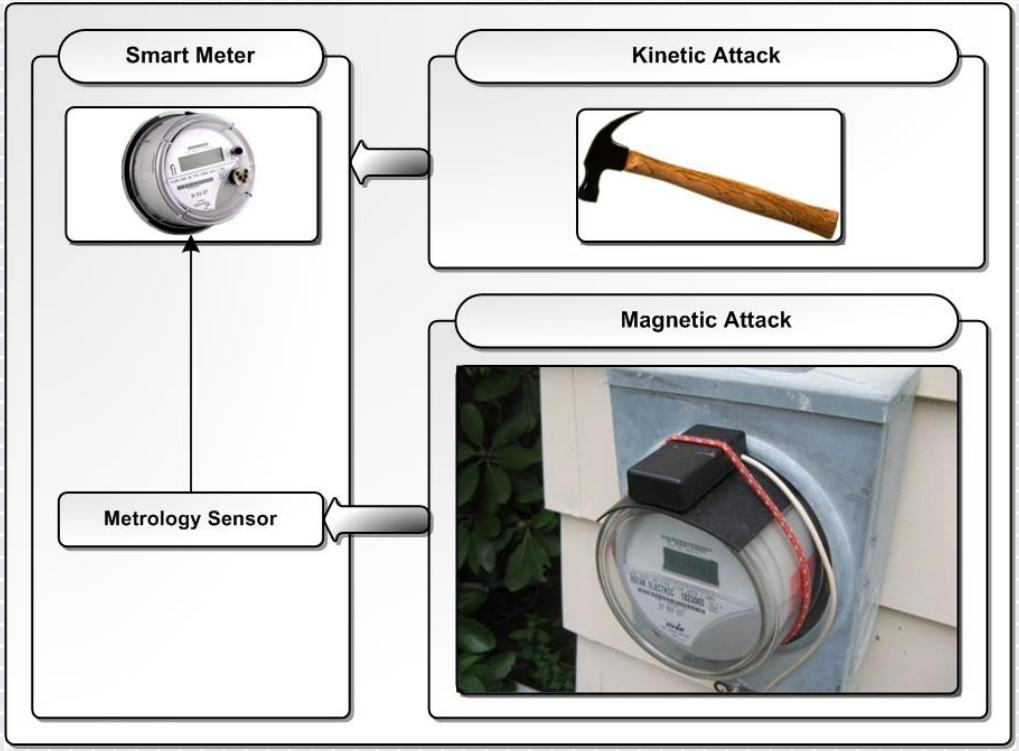
Security Test Plans for Complex Systems

- Create use case documents to shape the test plan
- Do a Security Assessment of the product to shape the test plan
- Must develop strategies to deal with:
  - Network latency
  - Embedded systems with specific encryption requirements
  - Tunnels e.g. GRE, L2TP, etc.
  - Security certificates
  - Simulate Public Key Infrastructure (PKI)
- Risk based approach to shape the security test plans

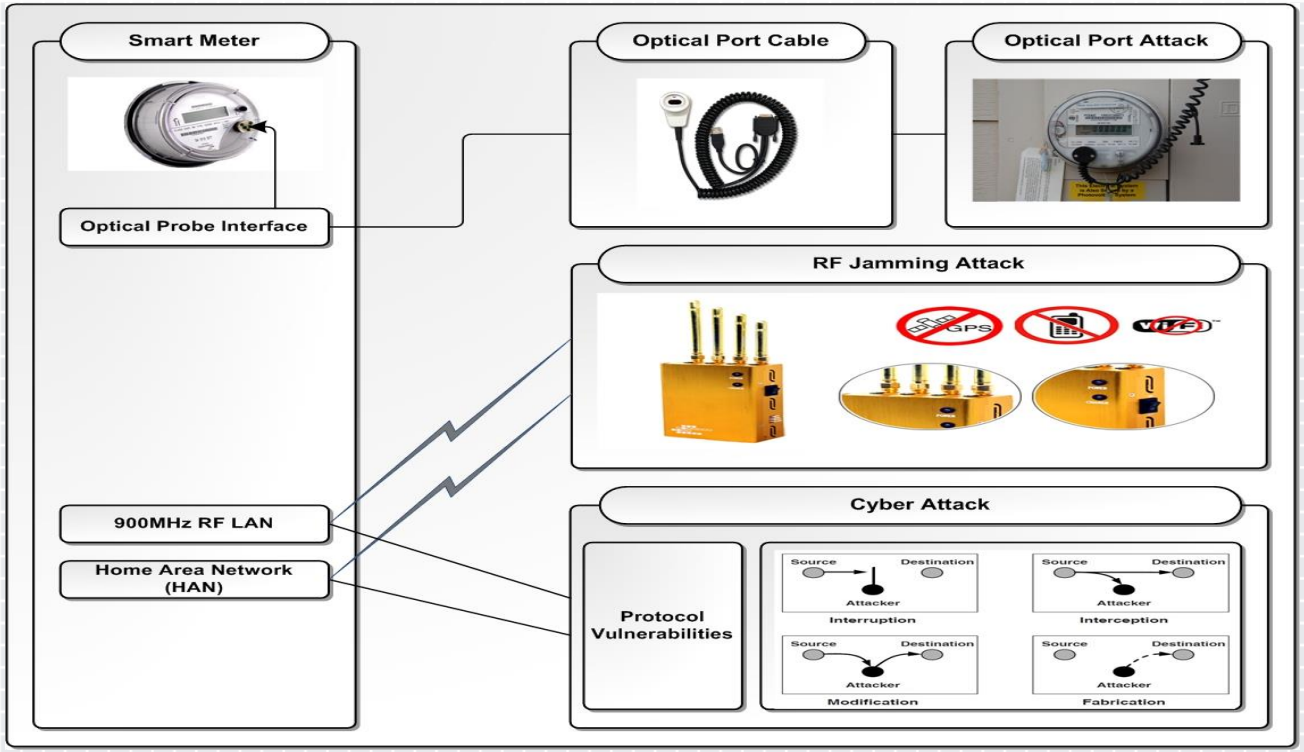
Tools & Results

- Successful penetration testing requires the use of tools.
  - Right tool for the job – Codenomicon, Nessus, nMap, Foundstone, etc.
  - Important to be result focus and pick the correct tool.
  - Having skilled/talented penetration testers to understand and make useful the results of the tools.
- The penetration testing project can discover vulnerabilities in devices, interfaces and systems.
  - Defects can be resolved by manufacturers producing code fixes
  - Vulnerabilities can be resolved by hardening and armoring the affected devices, interfaces and systems.

Threat Vectors



Threat Vectors



Threat Vectors

- Social Engineering Attack – against the ‘Utility Call Center’
  - Current meter status information
  - Improper or Inappropriate disconnect
- Combination Attacks – Physical, Cyber & Social Engineering
  - HAN device association to target home/business
  - SD Card Hack
- Why? - turn off the power, mess with billing, know when people are home and what they’re doing…

Before Starting…

- Get results of security testing carried out by others – vendor, 3rd party lab and other customers
- Eliminate redundant, expensive testing
- Pick up where others left off
- Further explore their findings
- Optimize the test plan

Ensure a Production-Like Environment

- These results are costly and resource intensive, be sure they are valid
- Production-like equipment is not enough, production-like configuration is needed
- Document the differences between production and test environments
- Confirm with the vendor and implementation team how these differences will impact results

Support Structure for Security Testing

- Complex security testing needs substantial support from the vendor and implementation team
- Test environment
  - Construction & Maintenance
  - Certification
  - Troubleshooting
- Information for white box testing
- Make this part of the contract

Defect Management

- Defect Management
  - Defect definitions
  - Defect mitigation criteria
  - Defect resolution – what evidence is acceptable for closure?
  - Residual defect management – harden, armor or monitor
- Engage the vendor beforehand to form a common understanding and make this part of the contract

Handling the Results

- Confidentiality vs. Availability
- How will the information be handled?
- How will the information be protected?
- Who will see the results and how?
- People, Process, Technology
- Data leakage could damage the public, the utility, the vendor, other users of the product

Setting an Achievable Goal

- What does done look like?
- All test findings will point to need for more testing
- Where to stop?

Transition to Production

- What if some defects survive the project?
- How to manage defects that cannot be resolved by the end of the project to closure?
- After deployment is over, patching and new versions of applications and devices will occur
- Maintaining and upgrading the security test environment
  - Keep it production-like

Apply this: Position your pen test for success

- Use a standards based foundation for test plan
- Prioritize the test plan with a risk based approach
- Get buy-in on the test plan from vendors and implementation team
- Build a production-like environment - equipment and configuration
- Arrange support for maintenance and upgrade of test environment, include Service Level Agreements
- Define Defect Management criteria at the start of the project i.e. defect definitions and mitigation strategies

Apply this: Position your pen test for success

- Get results of previous testing by others
- Arrange support for understanding and correction of defects, include Service Level Agreements
- Strategy required for correction and mitigation of defects - short term and long term
- Determine what done look like before starting
- Strategy for test program transition to production

References

- Security Profile for Advanced Metering Infrastructure v2.1

  http://osgug.ucaiug.org/utilisec/amisec/Shared%20Documents/AMI%20Security%20Profile%20(ASAP-SG)/AMI%20Security%20Profile%20-%20v2_1.pdf

- NISTIR 7628 Guidelines for Smart Grid Cyber Security

  http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf

- NIST SP800-115 Technical Guide to Information Security Testing and Assessment

  http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Questions?

Robert Hawk

Principal Consultant
RBH Enterprises
www.LinkedIn.com/in/IronManRBH

Steve Vandenberg

Senior Managing Consultant
IBM Canada
www.LinkedIn.com/in/SteveVandenberg