



EPRI

ELECTRIC POWER
RESEARCH INSTITUTE



Smart Energy Profile (SEP) 1.x Summary and Analysis



Annabelle Lee

Technical Executive – Cyber Security
alee@epri.com

December 7, 2011

Agenda

- Background
- Task scope
- White paper summary
- Representative architectures
- Cryptography
- Vulnerabilities, mitigations, and best practices



Background...

- Smart Energy Profiles (SEP) 1.0 and 1.1 deployed throughout the world
 - Implemented in the home area network (HAN)
 - Millions of smart meters implement SEP 1.x
- Deployment of SEP 2.0 delayed
- Initial assessment of SEP 1.x performed by
 - Carnegie Mellon
 - Cyber Security Working Group (CSWG)
 - Identified potential vulnerabilities



Task Scope...

- Joint effort by...
 - The National Electric Sector Cybersecurity Organization Resources (NESCOR)
 - The CSWG
 - Other experts
- ZigBee Alliance provided access to all requested documents
- *Goal – augment previous assessments*
 - *Provide a “user-friendly” overview*
 - *Add potential impacts, mitigations, and best practices*



Overview of SEP 1.x Summary and Analysis White Paper

- Addresses both SEP 1.0 and SEP 1.1
- Summarizes the differences between the two specifications
- Includes SEP 1.x reference architectures
 - Provides information on the Texas and California initiatives
- Provides an overview of SEP 1.x
 - Security functionality
 - Cryptographic functionality
- Identifies the applicable NIST Interagency Report (NISTIR) 7628 security requirements



Overview of SEP 1.x Summary and Analysis White Paper (2)

- Identifies potential vulnerabilities, mitigation strategies, and best practices
 - SEP 1.x specification
 - Cryptography
 - Implementation specific
 - Access control
 - Devices leaving the network
 - Key updates
 - Best practices
 - Trust Center
 - Certificate management
 - Functions outside the scope and in the environment
 - Physical tampering
 - AMI/HAN interface exploitation



Agenda

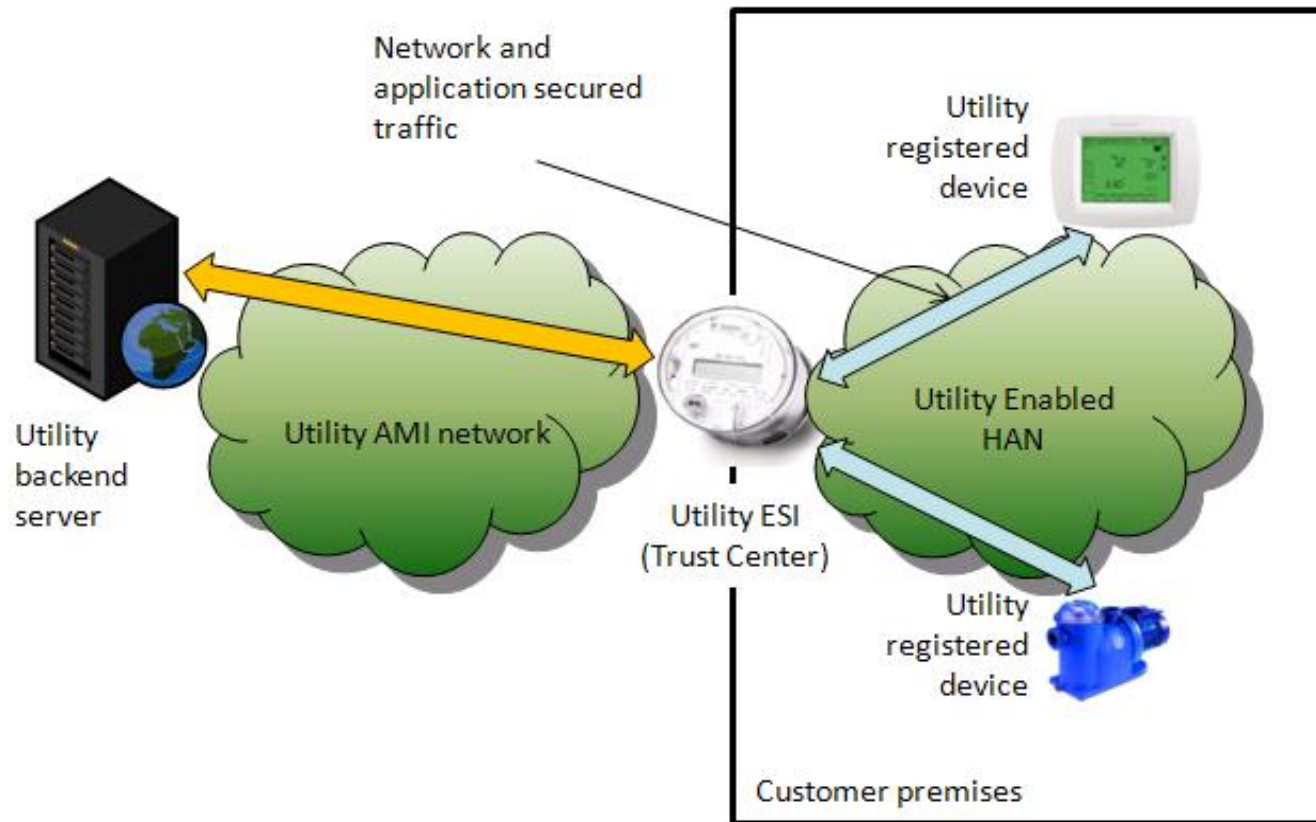
- Background
- Task scope
- White paper summary
- Representative architectures
- Cryptography
- Vulnerabilities, mitigations, and best practices



Utility Enabled Home Area Network (UE-HAN)

- All devices must be registered with the utility
 - Utility meter serves as the
 - ZigBee media access control layer
 - SEP 1.x Trust Center
 - Utility HAN's energy services interface (ESI)
- The white paper assessed the security functionality of the utility meter and all the ZigBee devices attached to the UE-HAN
- Outside the scope of the analysis and SEP 1.x
 - AMI domain in the smart meter and upstream of the physical utility meter
 - Utility backend environment
 - Security aspects of home appliances and displays not directly involved in ZigBee communications and control functions

Utility Enabled Home Area Network (UE-HAN) (2)

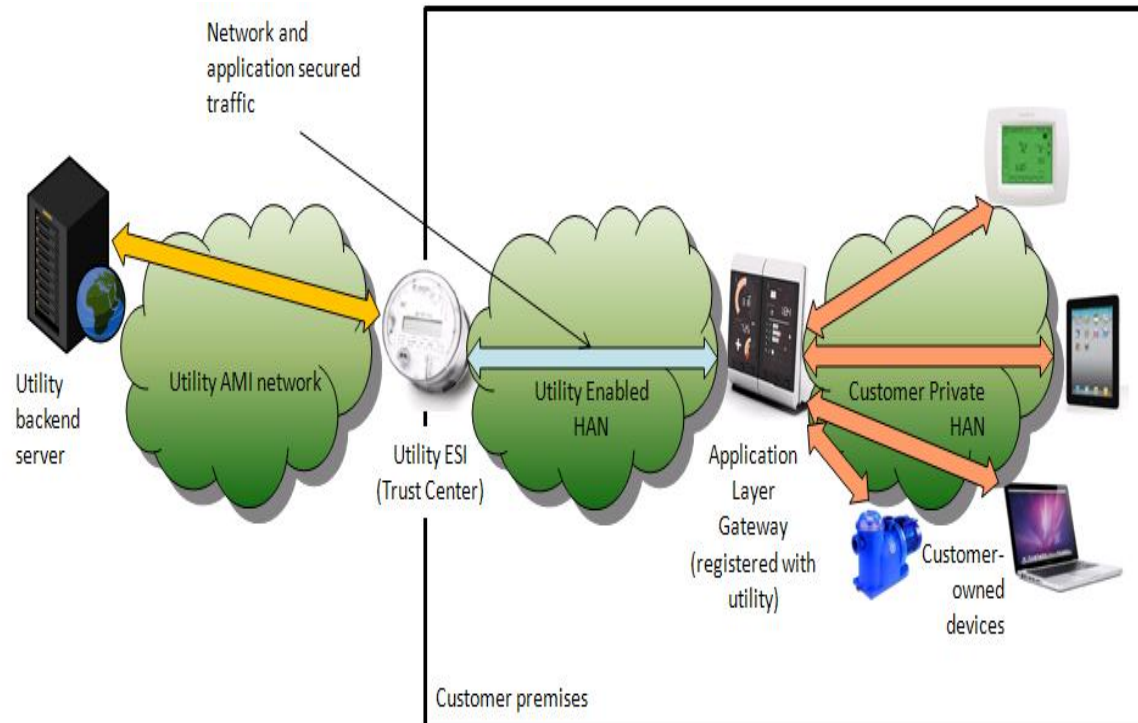


UE-HAN and its connection, through a utility meter, to a utility backend environment

Consumer Private HAN (CP-HAN)

- There is one device registered with the Utility - an application layer gateway (ALG)
 - Device must be a SEP 1.x compliant device
- There are two separate HANs in the premises, a UE-HAN and a CP-HAN, each with its own Trust Center
 - The devices on the CP-HAN do not have to be registered with the Utility
 - Their functionality is independent of the SEP 1.x specification
 - In scope: the UE-HAN and the devices registered with the utility (ALG in the figure)
 - Out of scope: the CP-HAN and the customer-owned devices on the CP-HAN are outside the scope of the white paper

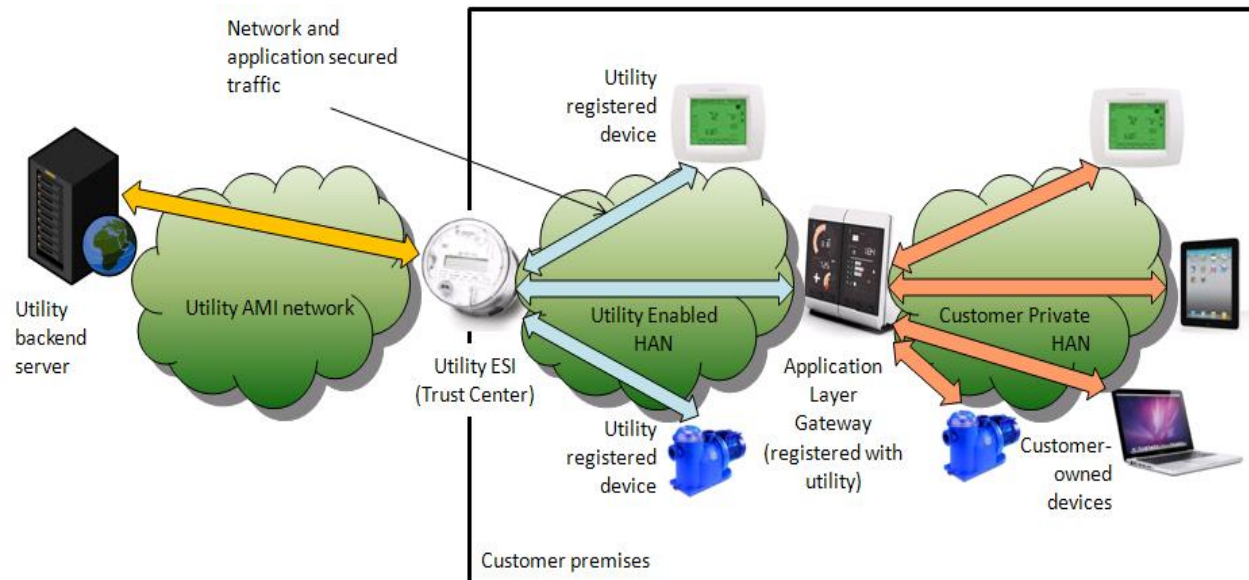
Consumer Private HAN (CP-HAN) (2)



Utility Enabled and Consumer Private HANs (UE-HAN and CP-HAN)

- Some devices in the premises are solely managed by the utility
- Must be registered with the Utility
- An additional ALG is owned by the customer
 - Must be SEP 1.x compliant device and registered with the utility
- There are two separate HANs in the premise
 - UE-HAN and a CP-HAN
 - Each HAN has its own Trust Center
 - The devices on the CP-HAN do not have to be registered with the utility
 - Their functionality is independent of the SEP 1.x specification

Utility Enabled and Consumer Private HANs (UE-HAN and CP-HAN) (2)



Security Controls - Cryptography

Key Name	Key Shared with	Related Protocol Stack Layer
Pre-configured link key	Trust center	Application layer
Trust center link key	Trust center	Application layer
Network key	Entire HAN	Network layer
Link key	Pair-wise device	Application layer

- SEP 1.x Network
 - SEP 1.x keys
 - Key updates
 - Cryptographic primitives
 - Random number generation
 - Key establishment
 - Key management

Agenda

- Background
- Task scope
- White paper summary
- Representative architectures
- Cryptography
- Vulnerabilities, mitigations, and best practices



Potential Vulnerabilities and Mitigations

- Cryptographic algorithms
 - Deprecated by NIST
- Link key and network key
 - If compromised – allows access
 - Potential vulnerability not unique to SEP 1.x
- Implementation specific vulnerabilities and mitigations
 - Each section includes
 - Background
 - Issues and vulnerabilities
 - Mitigations

Potential Vulnerabilities and Mitigations (2)

- Implementation Specific Vulnerabilities and Mitigations (2)
 - Access control
 - Malicious device joining the network
 - Devices leaving the network
 - Key updates
 - HAN security policies
 -

Best Practices

- Each section includes:
 - Background
 - Issues and vulnerabilities
 - Best practices
- Topics addressed include:
 - Trust center policies
 - Link key based on installation code
 - Key domain overlaps
 - Certificate management

Functions Outside the SEP1.x HAN Analysis Scope

- Customer privacy
- ZigBee radio physical tampering exploitation
- AMI/HAN Interface Exploitation

Summary and Conclusion

- Initial assessments focused on potential vulnerabilities
- Current assessment included
 - Sample reference architectures
 - Mitigations and best practices
- Take away...
 - All products contain potential vulnerabilities
 - Make an informed decision about deploying SEP 1.x
 - Analyze the potential vulnerabilities
 - Select mitigations and best practices
 - Determine residual risk



Discussion

Annabelle Lee

alee@epri.com

202.293.6345

Together...Shaping the Future of Electricity