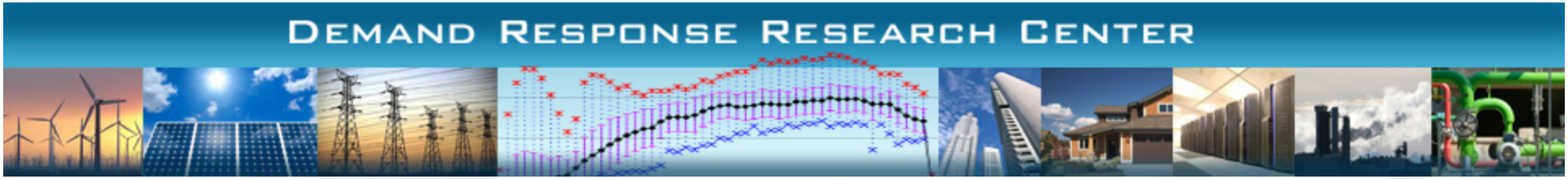


HAN Attack Surface and the Open Smart Energy Gateway Project

Justin Searle

Managing Partner – UtiliSec

justin@utilisec.com // @meeas

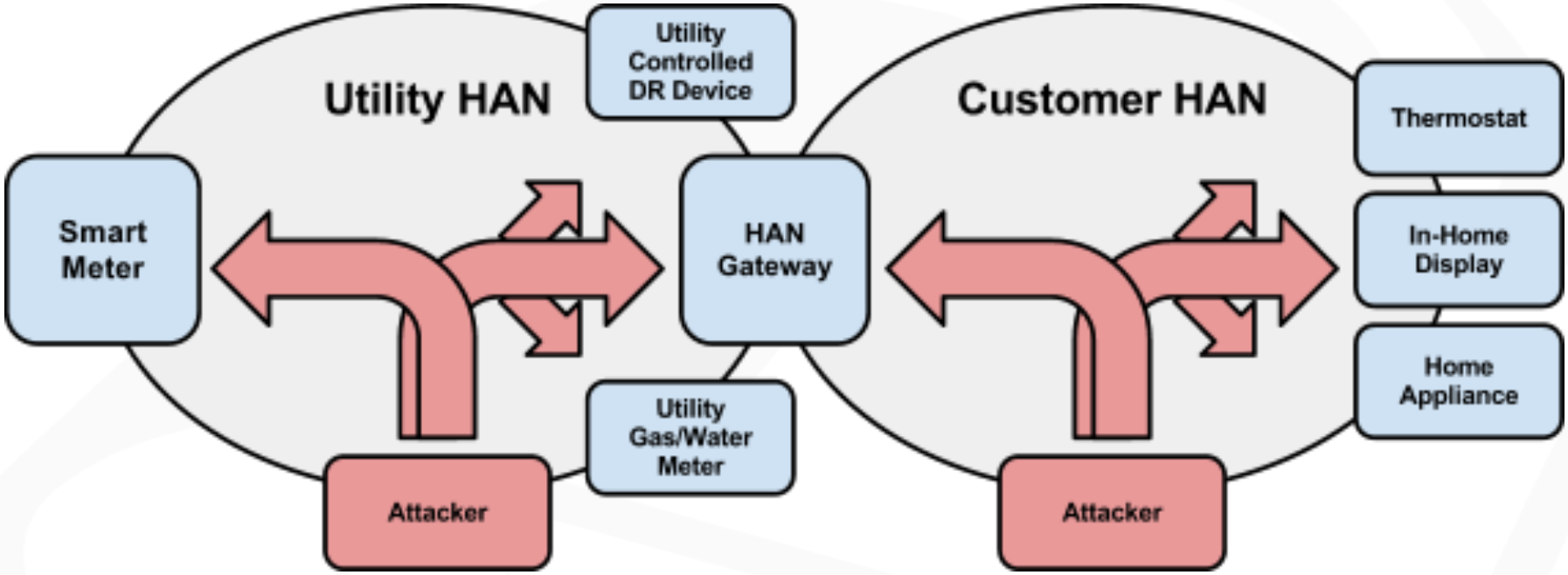
Who is UtiliSec?

- UtiliSec team has been working with electric utilities, vendors, and Smart Grid community for years
- UtiliSec team has lead and participated in numerous "Smart Grid" security efforts:
  - Served in leadership positions some of the electric utilities largest community groups, including UCAIUG's AMI Sec, Smart Grid Security Working Group, Advancing Security for the Smart Grid (ASAP-SG)
  - Actively contributed to and lead several teams in the creation of NIST Inter-Agency Report 7628: "Guidelines for Smart Grid Cyber Security" (available at: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf, also see vol2 and vol3)
  - Continued participation in DOE's Smart Grid Interoperability Project (SGIP), new National Electric Sector Cybersecurity Organization Resource (NESCOR), and other DOE initiatives.

Smart Meters and the HAN

- Deploying smart meters provides benefits to both utilities and customers
  - Utilities receive operational benefits from automated meter reading and enhanced monitoring of the power grid
  - Customers benefit from services that allow readout of energy usage and automatic responses to energy price
- Many utilities have not yet enabled smart meter communications into the home preventing customers from realizing any benefits
  - Some reluctance is based on technical shortcomings of the currently selected communications technology
  - However, the overarching issue has been concern about the level of security provided by HAN technologies and their risk

What can Attackers Attack in a HAN?



- Attackers can potentially attack either the utility or the customer HAN
- Attackers attempt to exploit vulnerabilities in the way devices handle input
- The collection of all possible inputs in a system defines its attack surface
- Gateways between network provides a defensive barrier between networks
- If a device is compromised, an attacker could attack other devices from or through that compromised device, thus crossing network boundaries

ZigBee Smart Energy Profile (SEP)

- The most common HAN technology deployed in Smart Meters is the ZigBee Smart Energy Profile (SEP)
  - ZigBee is built upon the IEEE 802.15.4 standard
  - ZigBee Pro with SEP 1.0 is the most common HAN technology deployed in smart meters today
- ZigBee networks have a coordinator that sets up and controls the HAN
  - For utility HANS, this is usually the Smart Meter
  - For consumer HANs, this is a gateway or in-home display
  - Coordinators can limit which devices join the HAN through the use of a ZigBee network key
- Limiting which devices join the HAN can help decrease the HAN attack surface and related security risk

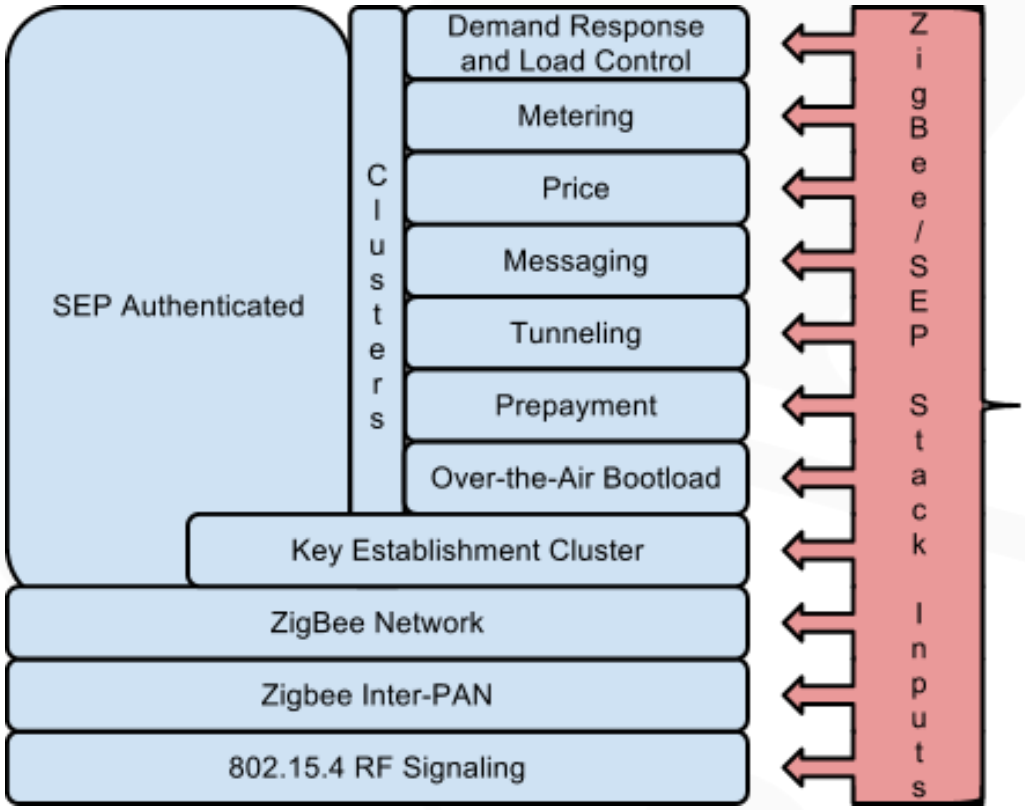
An Attacker's Primary Targets

- Because of the ZigBee coordinator's role, it becomes the primary target for attackers to compromise
  - compromise of the coordinator provides greater access to the other HAN devices
  - compromise of the coordinator can become a pivot point to attack other device on other networks
- Coordinators in ZigBee networks using SEP 1.x usually assume the roll of the SEP trust center
  - SEP trust centers provide a second layer of authentication, network management, and device whitelisting capability
  - Failure to authenticate to the SEP trust center prevents attackers from access most SEP functionality offered by HAN devices, which functionality can affect the physical world

ZigBee SEP Network Formation

- The ZigBee coordinator selects an unused, logical network identifier called a PAN ID and a network access password called the ZigBee network key
- The coordinator advertises the PAN ID to potential ZigBee devices
- A ZigBee device is configured to use the chosen PAN ID and network key and communications with the coordinator
- If the ID and key are correct, the device joins the network
- If the device needs access to SEP services, it must speak to the SEP Trust Center to perform a CBKE authentication using the ECC cryptographic certificate programmed into the HAN device at manufacture time or during flash updates
- If the device passes CBKE authentication, it can communicate securely with other SEP devices

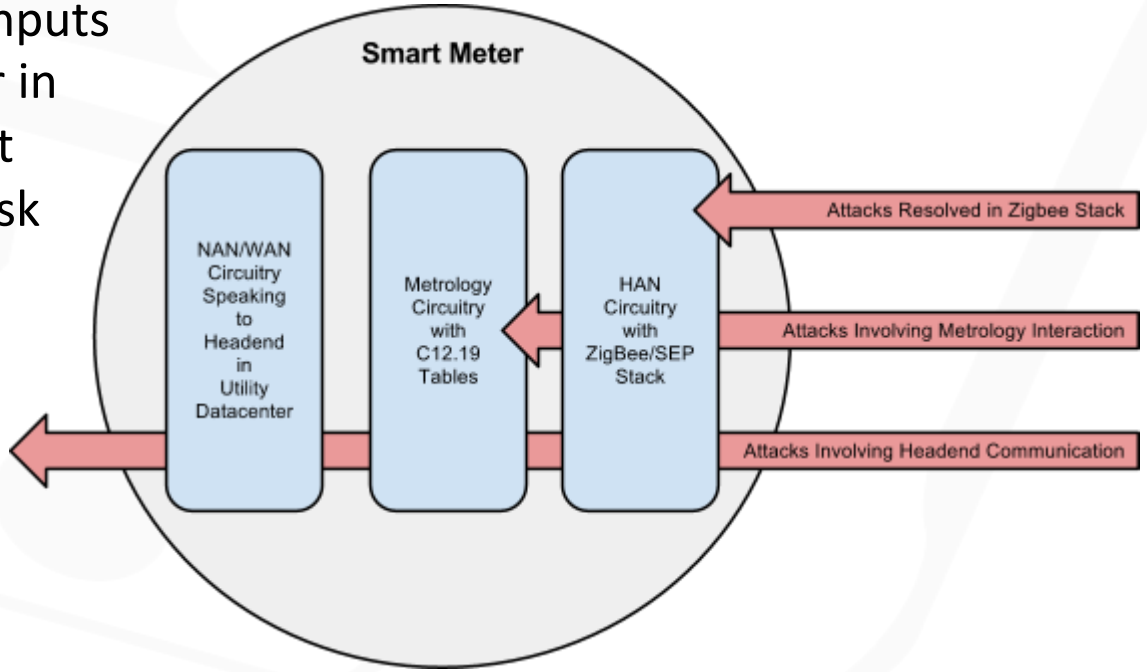
Smart Energy Profile's Attack Surface



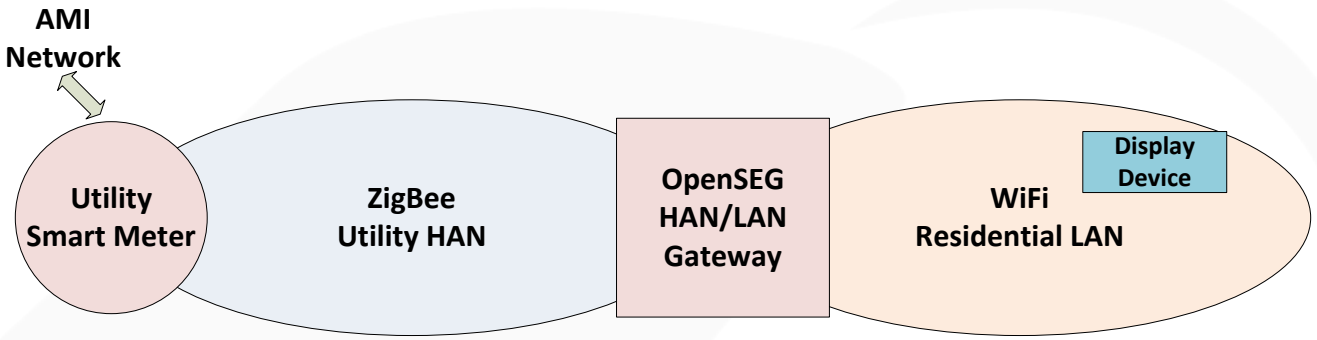
- Attackers must work their way up from the lowest level of connectivity to gain access to the higher level protocols
- With appropriate access, attackers can attack all inputs in the SEP protocol stack
- Once authenticated to the SEP trust center (via CBKE authentication), an attacker can attack any of the enabled SEP Clusters and their functionality

The Utility's Biggest Concerns

- Utilities are concerns about the potential attacks in the HANS they manage
- Utilities are more concerned about the potential attacks that the presence of a HAN creates for their Smart Meters
  - Most ZigBee inputs are handled by the HAN circuitry in the meter
  - Some SEP inputs interact with the metrology circuitry and data tables
  - A small number of inputs get passed through the meter all the way up to the Smart Meter and Demand Response management servers
- Vulnerabilities via these inputs in the metrology board or in the backend management servers create far more risk for utilities and issues in the HAN itself
- This attack surface and related exploit probability is very small, but it is also very real



Open Smart Energy Gateway (OpenSEG)



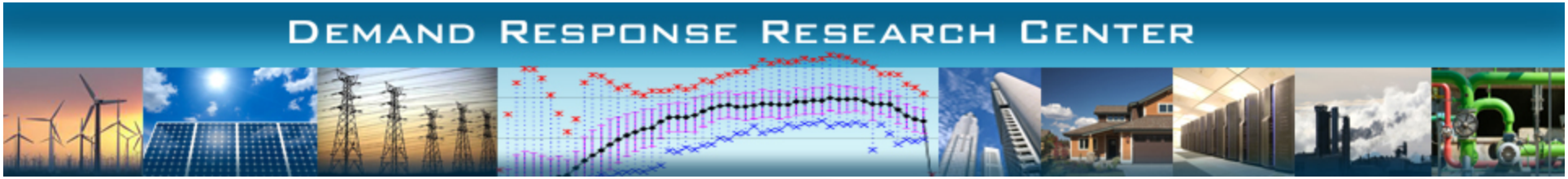
- Primary goal of the OpenSEG is to minimize the system-level risk when enabling residential smart meter communications on current SEP 1.0 meters
- OpenSEG requires an embedded platform that supports both ZigBee SEP 1.0 and Wi-Fi
- OpenSEG runs a simple gateway application that:
  - receives external Wi-Fi requests for smart meter data
  - presents a single SEP request to the smart meter for that data
  - conveys the resulting response back to the original requestor

How OpenSEG Gateway Helps

- OpenSEG decrease the HAN attack surface
  - Limits the number of utility HAN ZigBee devices requiring binding to the smart meter to only the OpenSEG gateway
  - Limits the SEP Clusters that can be accessed by HAN devices
  - Prevents HAN devices from leveraging InterPAN access
- Doesn't prevent direct wireless attack to utility HAN, rather it limits the number of devices that an attacker can leverage in an attack against the Smart Meter and beyond
  - Allows utilities to have very restrictive whitelists on their Utility HANs
  - Decreases compatibility testing between numerous different ZigBee SEP devices

Conclusion

- ZigBee SEP 1.x has several security risks, but many of these are not removed in later and future SEP versions
- The potential number of security weaknesses is related to the number services supported, and we currently support more services (SEP Clusters) than we need
- OpenSEG reduces the number of smart meter services exposed to the customer and third party HAN devices, thus decreasing the meter's attack surface
- OpenSEG helps reduce the relative security risk for utilities to enable the HAN interface on their smart meters and provide customers with the promised smart meter benefits



UtiliSec

www.utilisec.com
info@utilisec.com

Justin Searle
personal: justin@meeas.com
work: justin@utilisec.com
cell: 801-784-2052
twitter: @meeas