

Roger Levy Presentation for NIST/CSWG Smart Grid Privacy Group  
December 21, 2012

Could you please answer the following questions, whichever ones are applicable to your research, as they relate to privacy ramifications of smart meters and HANs.

- a. Can you provide an overview of the Lawrence Berkeley National Lab HAN assessment?

Roger:

The HAN assessment project is funded by DOE and the California Energy Commission. The project has been underway for about one year. It was motivated by two issues: (1) during many regulatory business case proceedings the HAN was considered an integral component of the smart meter and it was assigned very high expectations for producing customer education, energy savings, and system operation benefits, and; (2) implementation and opening the smart meter HAN for customer use has been substantially delayed which adversely impacts expected benefit streams.

The purpose of the Lawrence Berkeley Lab project is to assess the technical and policy status of the smart meter integrated HAN and identify options to address potential problems.

- b. What are the possible ways that electricity customers can get access to the current HANs? Via their laptop? Tablet computer? Smart phone? Directly through smart appliances? Etc.

Roger:

Smart meter HAN data is sent from meters via a radio embedded in the meter that communicates data using ZigBee SEP 1.x. There are two mechanisms to communicate with devices: one is via a direct link established between the particular device and the (utility controlled) HAN ZigBee radio and the other is via a gateway device that has previously established a secure connection with the HAN ZigBee radio. In the first case, each device would have to be approved by the particular utility (different processes at different utilities). In the second case, only the gateway device would have to be approved, and it would then provide the interface and information to other devices. Under the second scenario, there is no inherent reason why the information could not be displayed on any WiFi (or other well established secure communication protocol) enabled or Internet enabled device.

The smart meter integrated HAN is only accessible through utility authorized and certified devices, which to-date has been limited to in-home displays (IHDs) and programmable communicating thermostats (PCTs). While there have been many utility pilot projects, only Texas (<10,000 devices) and Oklahoma (about 40,000 devices) have actual implementation programs. As far as we know access to HAN based information is not available through devices other than those provided by or certified by the host utility or

retail energy service provider. Other than a few pilots, we know of no (none) smart appliance applications.

- c. Do you anticipate these possibilities changing with next generation HANs that may be in consideration?

Roger:

The next generation of smart meter HAN implementations anticipate implementation of ZigBee SEP 2.0. ZigBee SEP2.0 is not yet finalized and there are outstanding technical concerns regarding when it will be available, whether it can be retrofitted into existing smart meters, and how it might perform. We do know that SEP 2.0 is not backward compatible with SEP 1.x. SEP 2.0 is expected to be more secure SEP 1.x, however that won't be established until it is implemented and fully tested.

There are existing technical alternatives to the utility provided smart meter integrated HAN that are and should be capable of providing a wide range of connection, information, and automation options. Whether those options make it to the market is a function of regulatory policy and market factors. Without a customer value function (why invest in HAN devices and why change behavior) it is unlikely that a HAN market will develop. In fact, at least one major appliance manufacturer has already retreated from their smart appliance initiative.

- d. Is such HAN access hardwired or wireless, or various combinations of both?

Roger:

Existing smart meter integrated HANs are 'hardwired' and physically integrated into the circuit boards in the meter. The smart meter HANs use wireless communication to devices in the customer premise. Non-utility HANs are available that provide wireless, powerline, and other communication options but those were not the focus of our study.

- e. What are the types of data elements you are seeing collected and maintained within the HAN?

Roger:

The smart meter HAN is not collecting any data from inside the customer premise other than that necessary to register a customer device. To link a consumer device to the HAN the customer has to provide the utility with the device MAC address and an install code. This information is verified by the utility before the device is allowed to connect to the HAN. The capability to collect specific device operating information is part of the Smart Energy Profile (SEP 1.x) application set, however we aren't aware of any utilities collecting this information. The smart meter collects and stores premise time-interval usage information which is accessible to the HAN.

- f. Which data elements come from smart appliances?

To link IHDs, PCTs, and smart appliances to the HAN customers must provide the MAC address and an install code that uniquely identifies the device. Once matched to a list of

approved devices within some utilities, the particular appliance would be allowed to join the HAN network.

g. Which data elements come from the smart meter?

Roger:

Currently, it is our understanding that smart meters provide utilities only with interval usage data.

h. Do any data elements get fed into the HAN from a remote location, such as from a smart appliance vendor, a social network, a managed electricity services vendor, or some other type of entity?

Roger:

We are not aware of any current implementations where smart appliance or other device information is "remotely" fed into the HAN. For a device to properly connect to the meter device information technically must go through the smart meter HAN or be provided over the phone or through a web site by the consumer or their agent. There are pilot and other small scale implementations that provide a "cloud-based" interface between the customer and utility where several different types of usage, price, cost, and message data is collected both from the meter and utility back-end systems and then provided to the customer through a computer, smart phone, or other interface. However, these 'cloud-based' implementations don't necessarily use the utility HAN.

i. What have you found with regard to PEV data being integrated within or loaded into consumer HANs?

Roger:

It is our understanding that the existing smart meter HAN is not currently being considered to support PEVs.

j. What types of access do you see utilities having into consumer HANs? Through what pathways? (E.g., via smart meters, directly to the HAN via a wireless connection, etc.)?

Roger:

The smart meter integrated HAN is fully controlled by the host utility. The utility is the only entity that can turn the HAN 'on' or 'off' and they are the only entity that can transmit messages, prices, costs, or other information through the HAN. Communication from the utility to the HAN is generally via wireless capability. Under certain tariffs and demand response programs utilities may directly control appliance setting, operating modes, and on-off status. While not a HAN function, many smart meters have capabilities to remotely set premise demand limits – for example during capacity shortages the kilowatt (kW) demand a premise can use will be limited to a fixed amount which if exceeded will cause a switch to turn off all power to the premise.

- k. What types of privacy vulnerabilities (e.g., those allowing access to consumer energy usage data, to smart appliances, etc.) have you found within the HANs you've researched?

Roger:

There have been numerous cyber security assessments and some privacy work focused on the smart meter with integrated HAN. Almost all of these studies have been privately prepared by host utilities and/or vendors where results are not publicly disclosed or coordinated. The levels of risk tend to be evaluated and assessed differently for each utility consequently there is no universal HAN risk assessment. What we know is that studies have documented threats with various aspects of HAN implementation, specifically with functions that require reaching back through the smart meter into the utility communication network or back-office management systems. We also know from confidential discussions that utilities have successfully hacked into their own meters and gained access to some of the meter functions. Those same sources indicated that as a result of that effort they have modified their systems to better detect external threats, however that does not mean that new threats might develop capability to bypass those mitigation measures.

- l. What are you finding with regard to smart meter integration with HANs? What are vendors looking to accomplish with this regard?

Roger:

Smart meters with integrated HANs have already been implemented on millions of meters throughout North America. Vendor objectives have generally been focused only on making certain the HAN meets utility specifications and that its operation does not jeopardize the primary data collection / billing functions the meter was designed to provide. In general we have documented technical problems that challenge the ability of the smart meter integrated HAN to fulfill many of its claimed expectations.

- m. How much control do consumers have for the connections made between smart meters and HANs?

Roger:

The smart meter integrated HAN is controlled by the utility, not the customer. The utility, not the customer, controls whether the HAN is activated (turned on) or deactivated (turned off). There is no status light or other capability which would notify customers regarding the on-off status of the HAN. Customer choice will be limited to voluntarily or otherwise choosing to connect an IHD, PCT, smart appliance or other control device to the HAN and then only under utility guidance. For some utility service areas customers will obtain all of their HAN devices from the utility. Customers could choose to disconnect their device from the HAN however that would have to be accomplished by (1) notifying the host utility or (2) physically unplugging the device. We know of no current IHDs, PCTs or smart appliances that provide customers with on-off switches on the device to activate or deactivate a HAN connection - that does not mean they don't exist.

- n. Based on your research, what are the emerging trends you are seeing with regard to smart meters, their data collection and storage capabilities, and their abilities to integrate with HANs?

Roger:

Our project focus was on HAN technical and policy issues that affect HAN implementation and its ability to provide the expected customer education, pricing, and energy management benefits. We did not specifically examine trends. Although our observation is that there are numerous technology options available to support different approaches to HAN functionality than that offered through smart meters. The data collection and storage issues with smart meters are well known, the systems to collect, use and manage that data are still evolving and probably will continue to evolve for years.

Smart meter integration with the HAN appears to have numerous technical and policy issues, some of which may create regulatory and operational problems.