ASHB
Association for Smarter Homes & Buildings

Ken Wacks' Perspectives

Recent international standards for energy management support the transformation of the power grid from centralized generation to distributed energy resources including local solar, wind, and stored energy in homes and buildings.

These are voluntary industrial standards developed to promote world trade by a committee I chair for ISO[1] and IEC[2]*. They are part of a family of standards for interconnected consumer electronics (home automation) called the "Home Electronic System" (HES)* [3]*. I welcome your comments and participation in developing these standards; please visit kenwacks.com for contact data.*

Cybersecurity provided by the HES Gateway

As energy management responsibility shifts from the public utility to the occupants of homes and buildings, users become more dependent on reliable and resilient automation. The automation centerpiece facilitating this shift is the international standard Energy Management Agent (EMA). My previous *CABA Journal* article, "The Home Sentry," introduced the HES Gateway as a communications interface that provides connectivity between different networks outside and inside homes and buildings. (WANs – Wide Area Networks are outside and LANs – Local Home Area Networks are inside; home-based LANs are also called HANs – Home Area Networks.)

The primary function of the HES Gateway is to provide translation between different communications protocols. This translation function is performed within the gateway by constituents called HES service modules. The design of the HES Gateway using service modules provides a flexible and extensible architecture accommodating additional specialized service modules for:

- Cybersecurity protection
- Interoperability among incompatible home and building networks
- Hosting applications control in the gateway

[1] ISO is the *International Organization for Standardization*, founded in 1947, www.iso.org.
[2] IEC is the *International Electrotechnical Commission*, founded in 1906, www.iec.ch.
Both ISO and IEC are headquartered in Geneva, Switzerland.
[3] The *Home Electronic System* (HES) is the name of the international standards committee officially designated as ISO/IEC JTC 1/SC 25/WG 1:
JTC 1 = Joint Technical Committee 1, entitled *Information Technology*
SC 25 = Subcommittee 25, entitled *Interconnection of Information Technology Equipment*
WG 1 = Working Group 1, entitled *Home Electronic System*

The cybersecurity services of the HES Gateway constitute a home and building *sentry* to protect applications including energy management. This article explains the cybersecurity (CS) features of the HES Gateway.

The HES device registry

With the proliferation of non-wired networks such as radio, infrared (typically used in remote control units), and power-line carrier it is easy to insert rogue devices into a building LAN. Therefore, the HES Gateway can include a registry of legitimate devices. The gateway validates cybersecurity certificates presented by attached devices to determine if the device belongs on this network. A certificate is a digital message to verify that a device was provided by a known company and operates according to agreed rules. It is analogous to a driver's license issued by the government attesting that the holder has demonstrated driving competency.

The certificate contains an encrypted code that the gateway uses to validate the authenticity of the certificate. The gateway validates this certificate code by consulting a known certificate authority, which maintain a database of legitimate devices. After the device certificate has been validated, the gateway can then establish a secure link with the device and an application controller by distributing encryption keys to the communicating parties so they can exchange encrypted messages. Since the device certificate registry is maintained in the HES Gateway, a loss of external communications would not impact cybersecurity, as would a cloud-based cybersecurity service.

HES message server screening

The HES Gateway has the option of examining message headers to determine if local devices are communicating with the intended cloud-based servers. To accomplish this, the HES Gateway maintains a list of servers with which each local application could be communicating for accessing remote services. Users would be warned of attempts to reach unauthorized servers.

Many applications encrypt the data payload in communication messages. Nevertheless, we can still protect the home environment by examining packet header data, the frequency of packets, the size of packets, and the sequence of packets. Research is underway to distinguish bogus packets from legitimate packets containing encrypted data[4].

[4] https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.html
https://research.nccgroup.com/2021/12/02/encryption-does-not-equal-invisibility-detecting-anomalous-tls-certificates-with-the-half-space-trees-algorithm/
https://blog.alphaprep.net/detect-malicious-encrypted-traffic/

HES privacy and safety protection

Privacy protection is established by an agreement between service providers and customers or by policies (rules, sometimes laws) regarding what personal data may be collected and how such data are handled. There may be restrictions on:

- How customer data will be used.
- Who is allowed to access customer data.
- Whether customer data can be transferred or sold to third parties.
- Whether customer data can be aggregated and anonymized.
- How long customer data will be retained.
- When customer data will be deleted.

Establishing privacy protection may use tools of cybersecurity such as encryption, but these tools do not create privacy protection. Privacy protection may require that readily available personal data that has been securely transmitted from customer equipment to a service provider not be stored because the customer did not give explicit permission. For example, some smart phone applications have been gathering location information for each customer without their permission and selling this information to third parties as a source of revenue for application developers. Therefore, privacy protection requires specialized services beyond the tools of cybersecurity.

The HES Gateway supports an optional feature that screens data traffic for compliance with policies intended to protect consumer privacy. Also, appliance control messages impacting safety might be screened and blocked by the same mechanism. Figure 1 illustrates the elements in the gateway for protection of Premises and Personally Identifiable Information (PPII, explained in the next section) and safety. The “CS, PPII & Safety Controller” block in Figure 1 contains the rules about which data flows are allowed and which are blocked. The “CS, PPII & Safety Processor” block enforces these rules by examining the data to determine if the transmission of these data should be allowed or blocked.

As an example of safety protection, an HES Gateway service modules could be programmed to screen remote control commands sent to appliances from a smart phone app when away from home. This would prevent the smart phone app from starting a burner on a cook-top if nobody is at home to check that the appropriate pot with food is in place and nothing flammable is nearby. The functions of screening and filtering data extend the mission of the gateway to provide “data sentry” services for cybersecurity protection of customer data, privacy, and safety.

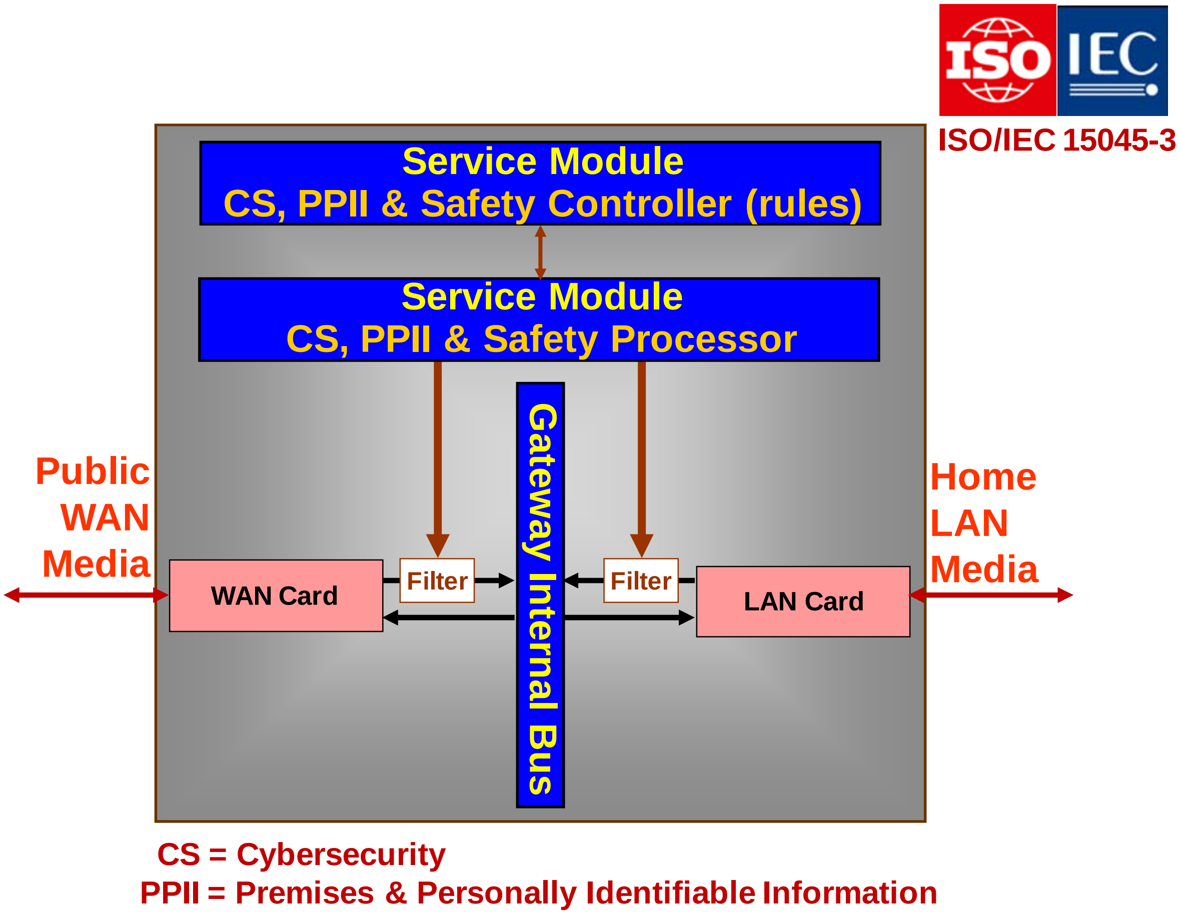

Figure 1– Gateway service modules

Privacy policies have focused on protecting PII such as name, address, government-issued identification numbers, facial photos, etc. ISO/IEC 29100[5] specifies a privacy framework for enterprise-level information technology (IT). This framework defines common privacy terminology, the elements that control and process PII, considerations for safeguarding privacy, and references to privacy principles that apply to IT. The scope of ISO/IEC 29100 states that these PII standards apply “to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII.”

[5] ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework*

The HES Gateway ISOIEC 15045-3[6] series extends the enterprise privacy framework from persons to devices by introducing the term PPII to incorporate devices and persons. The data sentry screening functions are intended to:

- Prevent active inbound attacks and unsafe commands.
- Discover and classify outbound traffic.
- Mediate network traffic within homes and buildings.
- Manage mechanisms for privacy and security.
- Develop a dashboard for reporting gateway activities and status to a non-technical end-user.

HES Gateway data screening

For the gateway technology to enforce privacy and safety provisions, all messages to and from devices must be checked by the gateway for compliance with the provisions of the privacy contract. The gateway scans and filters messages in real-time as the messages pass through the gateway.

For data not needed in real time, the gateway might function as a repository where these data are buffered. For example, a thermostat could register with the gateway and be allocated storage of a specified number of readings. The remote user with appropriate permission to access this repository would then retrieve these temperature readings from the gateway.

A gateway hardened against unintended data flows is effective if the gateway is the sole data pipe into the home. However, mobile (cellular) operators have developed communication protocols to transport IoT (Internet-of-Things) data. Some of the emerging technologies for mobile IoT data are 5G (5th generation mobile technology), LTE-M (Long Term Evolution for Machines) and NB-IoT (Narrow Band IoT) offered by existing mobile operators. SigFox, a French company, rents space on mobile networks to transmit IoT data at 100 or 600 bits per second with a proprietary protocol called Ultra Narrow Band modulation and offers IoT data management services.

As mobile data transmission become cheaper, it is possible that manufacturers might install mobile-phone data transceivers inside appliances and IoT devices to report on

[6] ISO/IEC 15045-3-1, *Information Technology – Home Electronic System (HES) gateway – Part 3-1: Introduction to privacy, security, and safety* [In progress]
ISO/IEC 15045-3-2, *Information Technology – Home Electronic System (HES) gateway – Part 3-2: Privacy framework* [In progress]

usage and performance without informing the customer. At the 2023 Consumer Electronics Show (CES), a company called 1NCE (www.1nce.com) offered a product called "IoT Flat Rate," a SIM card (Subscriber Identity Module) for IoT devices to communicate via the T-Mobile network in 150+ countries for a flat fee of $10 total for 10 years. Roaming is included if the T-Mobile network cannot be accessed. This service includes 500 MB of data and 250 SMS (text messages). For $20, the data and text message volumes are doubled for 10 years. The service includes a secure data channel via a virtual private network (VPN) and support for 2G, 3G, 4G, LTE-M, and NB-IoT cell networks. For HES compliance, messages to be sent via such a mobile interface are pre-screened by the HES Gateway to enable customer cybersecurity protection.

Privacy protection

The HES Gateway cybersecurity services can provide protection for customer's data, privacy, and safety. This is important for energy data and applications since energy consumption patterns can reveal who is home, when they are home, and what they are doing.

We may be at a confluence of social, political, and technical events that make standards and technology specifications for privacy timely. Consumers are becoming aware that personal data can be misused. In May 2018 the European Union (EU) General Data Protection Regulation (GDPR) became law. It protects the personal data such as names, addresses, photos, and voice recordings of all EU residents regardless of where the data are processed. Explicit consent is required before processing personal data for one or more specific purposes.

Consumers need products with technology that can protect privacy. The HES Gateway ISO/IEC 15045-3 series specifies technology that allows consumers and service providers to choose and enforce privacy options. It is now up to designers and manufacturers to incorporate privacy technology into products and for service providers to offer privacy choices with opt-in provisions. Such choices might be presented as a menu of services based on how much personal data customers are willing to share. A menu of choices would replace a take-it or leave-it click-through agreement that allows implicit sharing of all customer data obtained directly from the customer or indirectly using data purchased from data brokers with no disclosure or transparency. Building in privacy protection during product design is less costly for manufacturers than fixing problems later and compensating customers for data breaches.

Market studies have shown that privacy concerns are impacting the sale of connected home products. Parks Associates, a market research firm that tracks home systems, surveys 10,000 broadband households periodically for "Smart Home Device Inhibitors." Privacy concerns have consistently ranked third after device cost and benefits for the past three years. More than 30% of those surveyed agreed, "I have data privacy and security concerns about having smart devices in my home.” [These survey results were provided courtesy of Parks Associates by President and CMO Elizabeth Parks.]

Therefore, privacy concerns are no longer just an abstract concept, but can impact business. The HES Gateway addresses these concerns with technology that can enforce privacy policies and agreements between service providers and customers to protect the consumer’s data by specifying what can and cannot be shared.

Dr. Kenneth Wacks has been a pioneer in establishing the home systems industry. He delivers clear and practical advice to manufacturers and energy companies worldwide on business opportunities, network alternatives, and product developments in IoT and AI for home and building systems. The United States Department of Energy appointed him to the GridWise® Architecture Council to guide the electric industry toward smart grids. For further information, please contact Ken at +1 781 662-6211; kenn@alum.mit.edu; www.kenwacks.com