Autumn 2018 Volume 15, Number 3

iHOMES and BUILDINGS

THE MAGAZINE OF THE CONTINENTAL AUTOMATED BUILDINGS ASSOCIATION

CABA™ Connect to what's next™

www.caba.org/ihomesandbuildings

iHOMES and BUILDINGS

THE MAGAZINE OF THE CONTINENTAL AUTOMATED BUILDINGS ASSOCIATION

Autumn 2018, Volume 15, Number 3

Contents

iHOMES and BUILDINGS

THE MAGAZINE OF THE CONTINENTAL AUTOMATED BUILDINGS ASSOCIATION

Autumn 2018
Volume 15, Number 3

CABA Connect to what's next™

Association Office
Continental Automated Buildings Association
1173 Cyrville Road, Suite 210
Ottawa, Ontario, Canada
K1J 7S6

Tel: 613.686.1814; 888.798.CABA (2222) Fax: 613.744.7833

Ken Wacks' Perspectives

Gateway Enhancements for IoT Privacy

By Ken Wacks

Introduction

In my previous *iHomes and Buildings* article I introduced the gateway as a sentry between customer equipment and outside service providers. These sentry features enable the gateway to ensure that a customer's expectation for privacy is implemented according to agreements with service providers. International standards are being developed that specify technology to check data flowing between customer equipment and external servers in order to ensure compliance with a service contract. Since this screening function is programmable, it would become practical for service providers to offer customers various privacy options. Customers might be provided extra services in exchange for disclosing additional personal data as part of a menu of privacy options. Gateway sentry technologies can enforce privacy choices thereby creating market opportunities for gateway manufacturers and service providers.

Technology for managing privacy

The United States proposed a series of international standards for a communications gateway and product interoperability that could be extended to monitor and manage data flows into and out of a house or building. These proposals were offered to an international committee of ISO and IEC that I chair consisting of experts from about 40 countries. We develop standards for the interconnection of electronic equipment and products for homes and small buildings[1]. The primary markets for these standards are manufacturers and installers of products and services for these markets. International standards organizations were established in the twentieth century to foster commerce as a productive alternative to commercial and military conflicts among nations.

So far we have published two gateway and two interoperability standards. At our March 2018 meeting we worked on an additional gateway standard to address customer privacy, data security, and safety, and standards to enhance product interoperability.

A gateway is a communications device providing an interface between a network inside a building and an external network such as the Internet. For example, a router and modem constitute a gateway. A set-top box for a TV may include a communications gateway.

The ISO/IEC gateway standards[2] extend the conventional communications gateway that interconnects a local network (called a LAN – Local Area Network[3]) to an external network (called a WAN – Wide Area Network) with some unique features. These additional gateway features are options that could be implemented with modular elements. Manufacturers might offer a variety of gateways with different combinations of optional modules providing the following functions:

1. Support for multiple LANs

As home automation evolved from a hobby to an industry, there were attempts nationally and internationally to create standards for a uniform communications infrastructure to interconnect devices such as sensors, actuators, controllers, and user interfaces. These standards were completed and were technically sound. However, they were not adopted; instead the market fragmented into specialty networks such as ZigBee, Z-Wave, Wi-Fi,

1 This international standards committee is officially designated as ISO/IEC JTC 1/SC 25/WG 1:
ISO = International Organization for Standardization
IEC = International Electrotechnical Commission
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*

2 ISO/IEC 15045-1, *Information technology – Home Electronic System (HES) gateway – Part 1: A residential gateway model for HES*
ISO/IEC 15045-2, *Information technology – Home Electronic System (HES) gateway – Part 2: Modularity and protocol*
ISO/IEC 15045-3, *Information technology – Home Electronic System (HES) gateway – Part 3: Privacy, security and safety* (under development)

3 A LAN inside a house is often called a HAN (Home Area Network).

LonTalk, KNX, etc. With this reality, we decided to focus on enabling interoperability among disparate LANs. We are adapting existing standards to specify the Gateway Link module, which translates messages among LANs, as illustrated in Figure 1. During our March 2018 meeting, we learned that an expert from Canada (Ludo Bertsch of Horizon Technologies) had built a prototype demonstrating the feasibility of this approach. He has proposed a protocol for the Gateway Link called the *Common Language Internal Protocol* (CLIP).

2. Support for application processing

The primary function of the gateway is a communications interface. Our gateway standard includes the option for embedding application processors. This option reflects common implementation practices in gateways such as set-top boxes and security panels. The Service Modules in Figure 1 support applications.

3. Support for interconnected gateways

Gateways are embedded in many products ranging from set-top boxes to Internet access equipment to monitored security systems to smart TVs. A hallmark of an automated house is integration to deliver whole-home services. For example, a home theater room might include coordination among the entertainment equipment, shade control, and lighting. Our standard specifies methods shown in Figure 2 for establishing communication channels among multiple gateways directly or via the home LAN.

4. Support for cyber security

With the proliferation of non-wired networks (such as radio, infrared (typically use in remote control units), and power-line carrier) it is easy to insert a rogue devices into a building LAN. Therefore, the gateway might be designed to contain a registry of legitimate devices. The gateway would validate cyber security certificates presented by attached devices to determine if the device belongs on this network. A certificate is verification 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.

After the device certificate is validated, the gateway could then establish a secure link with the device and an application controller by distributing encryption keys. Since the device registry would be maintained in the home gateway, a loss of external communications would not impact cyber security, as would a cloud-based security service.

5. Support for message screening and filtering

We are planning optional features in a gateway that allow it to screen data traffic for compliance with policies that protect consumer privacy. Privacy issues are discussed in the next section. Also, appliance control messages impacting safety might be screened and blocked by the same mechanism. Figure 3 illustrates the elements in the gateway for protection of Personally Identifiable Information (PII) and safety: the PII & Safety Controller contains

Figure 1 – International Standard Gateway

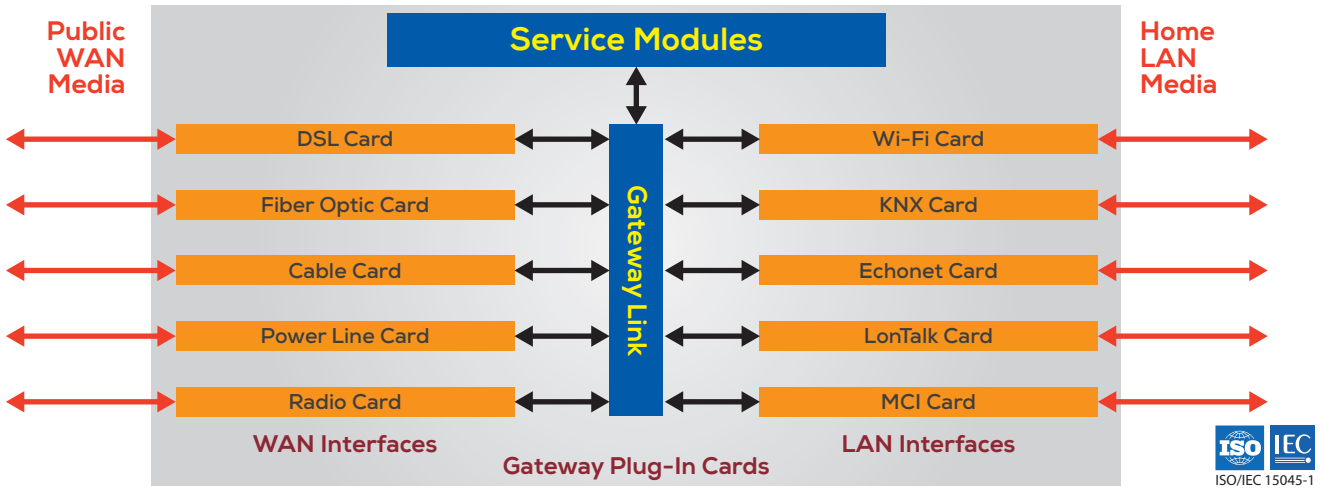
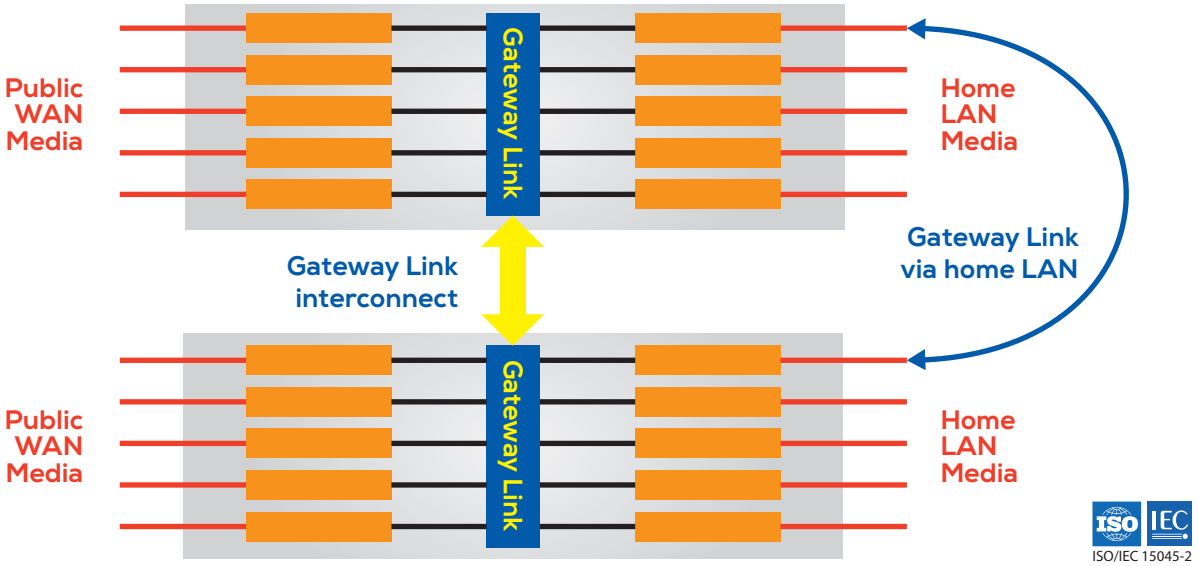


Figure 2 – Interconnected Gateways



the rules about which data flows are allowed and which are blocked; the PII & Safety Processor enforces these rules by filtering the data to allow or block transmission. For example, using a smartphone app when away from home to start a burner on a cook-top could be dangerous unless someone 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.

The gateway as a data sentry

Privacy policies have focused on protecting PII such as name, address, government-issued identification numbers, facial photos, etc. A series of international standards has been published that 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 these PII standards[4] 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."

The standards we are developing for the gateway extend the privacy framework from persons to devices. We have introduced the term DPII for *Device and Personally Identifiable Information*. 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.

The gateway data screening

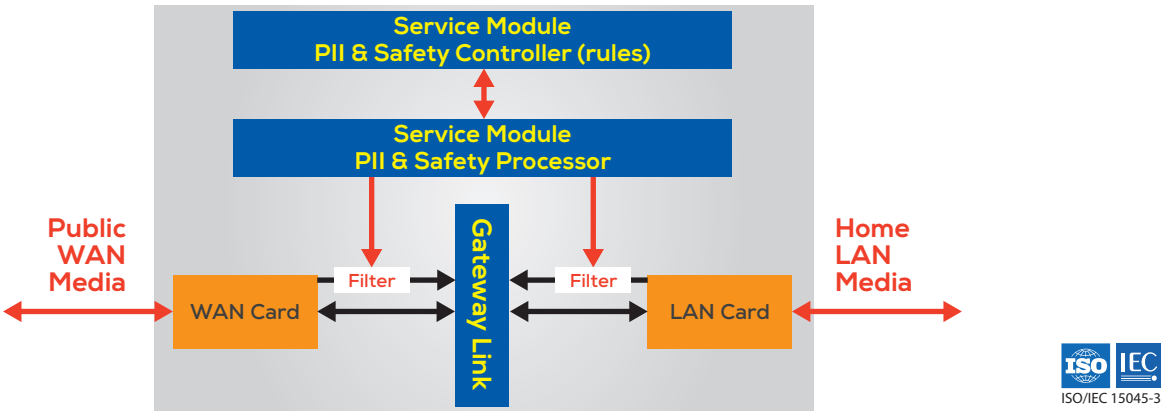
For the gateway technology to enforce privacy and safety provisions, all messages to and from devices must be checked by the gateway for compliance with the provisions of the privacy contract. The gateway scans and filters messages in real-time as the messages pass through the gateway.

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 are planning communication protocols to transport IoT

4 ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework*

Figure 3 – Gateway Filtering for PII and Safety



(Internet-of-Things) data. Some of the emerging technologies are 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 cell-phone data transceivers inside appliances and IoT devices to report on usage and performance without informing the customer. If the concept of a customer-controlled gateway becomes a marketable business proposition, there may be a parallel market for cellular-data gateways, or cellular data might first be sent to the home gateway for screening before transmission. However, if the unscrupulous gathering of covert data proliferates through channels that bypass the gateway, a market for mobile-data jamming products directed at IoT devices might develop.

From standards to products

The international standards described in this paper are all voluntary. They are intended to promote trade by offering a common infrastructure upon which applications may be developed. These are plenty of opportunities for innovation and competition.

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. The United States Congress held hearings in the spring of 2018 on data gathering by social networks for political influence. 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. As this article explains, there soon will be specifications for 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. Building in privacy protection during product design is less costly for manufacturers than fixing problems later and compensating customers for breaches. Privacy is no longer just an abstract concept, but can be enabled with appropriate policies, technology, and products. ●

Dr. Kenneth Wacks has been a pioneer in establishing the home systems industry. He delivers clear and practical advice to manufacturers and utilities worldwide on business opportunities, network alternatives, and product developments in 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