Incenergy

Security in Internet-Connected Building Automation and Energy Management Systems

Executive Summary

Thermostats, lights, meters, and sensors are joining the "Internet of Things", increasing the power and ease of use of Building Automation and Energy Management Systems. The transition from isolated systems operated from a computer in the basement, to internet-connected systems accessed from a phone is well underway. The greatest advantages of this revolution are mobility and portfolio view, both of which increase ease of use and operational efficiencies. Internet connectivity also allows the correlation of a variety of data sources and the coordination of controls across disparate devices enabling increasingly sophisticated systems.

In the rush and excitement of internet connecting everything, security has not been a top priority. Serious security and privacy vulnerabilities exist in some systems placing infrastructure at risk to malicious intent. Building Automation and Energy Management System (BAS and EMS) vendors must take these concerns seriously and offer secure solutions. The security of BAS and EMS systems must not rest solely on the shoulders of the end users. Customers cannot be burdened with, or trusted to, ensure the security of these systems. However, end users do have the responsibility to consider security as an important criteria when evaluating BAS and EMS systems.

Ensuring the security of controls, monitoring and automation systems is as simple as adhering to standard IT best practices. Decades of experience in IT offers well-established best practices for securing internet-connected devices. Cutting edge technology trends including cloud computing and wireless communication offer new capabilities and security solutions. Facilities Managers and Building Engineers often have little interaction with IT, but as internet technology permeates the world of facilities, the high security standards long customary in IT need to be implemented in BAS and EMS systems.

Internet Connectivity is a Must, but Security Concerns are Real

Getting an alert on your phone when an HVAC zone is too hot is efficient. Viewing what you spent on cooling your portfolio of buildings yesterday offers great insight. These powerful features depend on internet connectivity. Facilities Managers and Building Engineers are more productive when they can work from anywhere. Internet connectivity allows problems to be recognized and solved faster by orders of magnitude.

As Building Automation and Energy Management Systems go online bringing power and convenience to users, there are increased security risks. Malicious intent directed at internet-

Incenergy
1135 W. 6th Street Suite 140
Austin, TX 78703
USA

512.327.2020
sales@incenergy.com
www.incenergy.com

connected controls systems is a real problem. According to Robert O'Harrow Jr. of The Washington Post, "Over the past two years, hackers and cyberwarriors who once focused primarily on traditional computers and networks have put control systems in their crosshairs, damaging machinery, stealing information from networks and spying on facilities."[1] Hackers are drawn to these systems because they often contain sensitive information and they offer the ability to affect the physical world. BAS and EMS systems may contain usernames and passwords, contact information, addresses and building layouts. If that is not alluring enough, these networks offer control of myriad of devices including pumps, HVAC, lighting and even door locks.

A case in point, revealed in an FBI memo[2], was the illegal hack into the heating and air-conditioning system of a New Jersey based company. Widely reported security vulnerabilities in the Niagara Framework, a prevalent building automation software platform, allowed the hack to occur and were serious enough to warrant a Department of Homeland Security alert[3]

The current state of vulnerability is not surprising because many of these BAS and EMS platforms were not originally internet connected. The security infrastructure which is standard in enterprise software architecture was not included in the original design of many Building Automation and Energy Management Systems. As technology progresses, these systems are being extended to add internet connectivity after the fact. As a result, too many systems have backdoors, weak password requirements, feeble encryption, and attempt to rely on "security through obscurity".

When vendors fail to provide secure solutions, they place that burden on the customers. For many end users, Facilities and IT departments are worlds apart, and IT is sometimes left out of the BAS or EMS installation leaving little opportunity to improve security at that stage. Even if IT is involved, they are likely to be ill-equipped to deal with this sort of equipment. There is no Microsoft or Cisco certification for the secure configuration of the "black box" connected to the HVAC system. The IT department may reasonably assume the BAS or EMS vendor has ensured the security of the system. The ambiguity as to who is responsible for securing the BAS or EMS is itself a problem. Obligating the customer's IT department to secure these systems is not only burdensome, but unreliable. As BAS and EMS move down market to less sophisticated organizations the issue becomes more and more problematic. Relying solely on customers to secure these systems is asking for trouble.

Not only do many vendors shirk the security responsibility onto their customers, but they even refuse to patch known security issues creating "Forever Day" bugs.[4] In legacy systems, some vendors are unwilling to commit resources to fixing security problems, so the vulnerabilities remain, waiting to be exploited. Furthermore, even if a security patch is provided, it is unlikely many customers will deploy it, often because they are unaware of the patch's existence, or the patch installation is too complex, or patch installation on BAS and EMS systems is a low priority.

Cloud-Hosted Systems Take the Security Burden off the Customer

A secure cloud hosted system offers many advantages. Provided that the Building Automation or Energy Management System is designed with robust security, cloud based systems relieve customers of the burden of securing sensitive data and web services. It is more efficient and reliable to provide a single highly secured application in the cloud, than to attempt to secure thousands of individual instances at customer sites relying on IT teams of varying resources and ability.

Leading cloud service providers specialize in IT and security. Unlike many customer premises, physical access to cloud provider data centers is strictly controlled. State of the art cyber security and redundant physical security systems are employed to safeguard customer data and ensure reliability. A slew of cloud security certifications exist to validate the level of security provided. "There are many tiers of security validation, and programs such as FedRamp, ISO 27001, and SOC stand out as good benchmarks of operational security for cloud service providers," according to David Baker a Chief Security Officer. [5]

Cloud-hosted applications should include geographically separated redundancy, so in the event of a catastrophic event at a data center in one location, the system can continue to operate by rolling over to its servers in another location. Another advantage of cloud hosting is in security patch management. Customers can rely on the BAS or EMS vendor to keep the system up-to-date, whereas servers on customer premises often do not have the latest security patches. As new security concerns are identified, a cloud-based system can be continually updated and hardened, benefiting all customers while requiring no effort on their part.

Putting a system in the cloud does not make it secure. The system architecture must include security features at every layer. Secure passwords are the minimum, better yet is two-factor or multi-factor authentication.[6] Two-factor authentication requires users to authenticate with two of the following three types of proofs of identity:

- something they know (like a password)
- something they possess (like a phone or ATM card)
- something inherent about themselves (like a fingerprint)

Without two-factor security any "forgot password" retrieval system is vulnerable. Recently Apple followed Facebook, Google and Microsoft in offering the more secure two-factor authentication option to users.[7] All communication— interactions with the server to retrieve data or send commands — must require authentication as well as be encrypted. 2048 bit RSA public-key encryption is recommended because it is virtually unbreakable.[8]

The Customer Site Must Be Easy To Secure

A cloud-hosted system keeps the secure services and customer data out of the customer premises, but an internet gateway is still required. Minimizing the number of devices on the internet at the customer site to a single gateway is wise. Avoiding a proliferation of directly internet-connected devices makes security at the customer site much easier. The internet gateway should be secured behind a firewall or VPN and not directly on the customers' LAN. This is commonly accomplished with VLAN technology where devices are physically wired together, but the traffic is separated between segments of the network. Figure 1 shows how a VLAN setup isolates the gateway from the rest of the network.

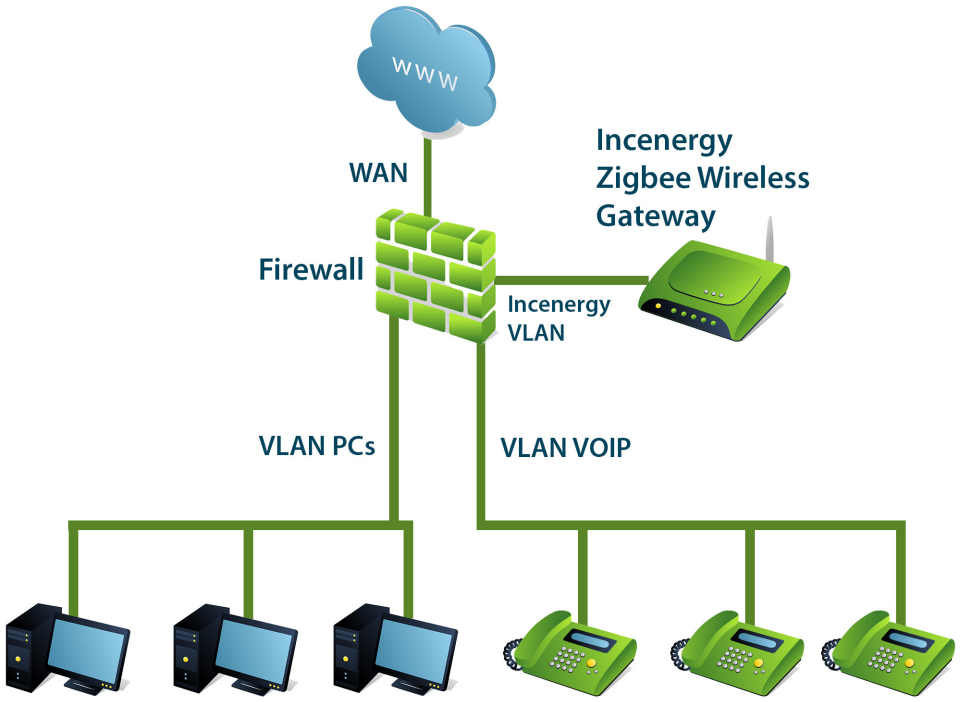

Figure 1: VLAN Setup

Another option is putting these gateways into DMZ zones of firewalls. The DMZ is a controlled WAN zone that can be configured to have no access to the LAN. These precautions make it impossible for a BAS or EMS internet gateway to serve as a jumping off point into the customer's network (or vice versa). Figure 2 shows how a DMZ setup isolates the gateway from the local network.

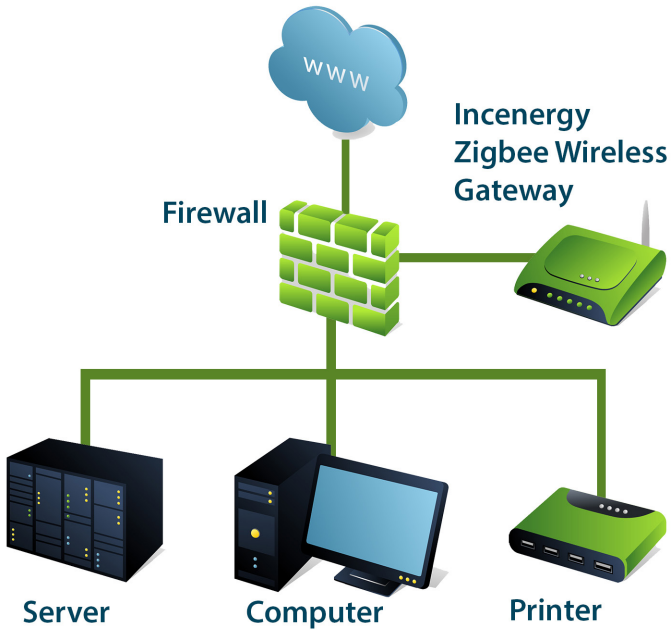

Figure 2: DMZ Setup

Customers cannot be relied on to configure the system security (as the Niagara example has shown), therefore the system must remain secure even in the worst case scenario where the gateway is not behind a firewall and has access to the LAN. Internet gateways with only outbound point-to-point communication are the most secure. This ensures that all communications travel from the gateway outbound to secure cloud servers and do not allow any inbound messages to be responded to by an onsite gateway. Gateways with no open ports, and no listening at all, thwart most hacking techniques. Moreover, gateways should not contain customer data or business logic, but rather function solely as communication facilitators, keeping logic and data in the secure cloud.

Building Automation and Energy Management Systems should avoid having directly internet-connected smart devices. Large installations can include hundreds of smart devices. If these are all internet connected, the chore of securing them becomes unmanageable. Many customers will not have the IT resources or sophistication to secure so many Internet Protocol (IP) devices. Systems should not rely on the internet for communication within the BAS or EMS, but rather should limit internet access to the gateway and cloud hosted web services.

Incenergy's cloud hosted EMS offering was designed with security precautions built in from day one. A seasoned team with deep roots in Telecom and Enterprise software systems ensured security was a top priority of the system architecture. To make securing the customer premises easy, Incenergy has only a single internet connected gateway. Moreover, Incenergy's robust security architecture protects customers even if that gateway was not deployed with optimal security.

The ZigBee Wireless Protocol is a Good Choice for BAS and EMS

ZigBee wireless smart devices can form a robust and secure mesh communications network completely separated from the internet and the customer's LAN. This security-amplifying reduction in the number of IP devices has the added benefit of a reduction in installation costs because wireless installations are more affordable. Incenergy's ZigBee mesh network of smart devices provides robust communications with none of the security hazards associated with IP devices.

ZigBee is based on the IEEE 802.15.4 standard which includes several security services. These security features prevent rogue devices from participating in, or eavesdropping on, the mesh communications. Table 1 names some of these services and shows how they contribute to data security.

Security Service	Contribution to Data Security
access control	Login credentials limit access to authorized users
data encryption	Converts data into difficult-to-interpret form, requires a key for interpretation
frame integrity	Provides authentication, key management and data transfer privacy
sequential freshness	Prevents replay attacks on the network
ZigBee Trust Center	single special device which other devices trust for the distribution of security keys
ZigBee security services	configures devices with keys and authorizes devices onto the network
Permit Joining	Allows restriction of device connectivity

Table 1

Building Automation and Energy Management System must function even in the unforeseen worst case scenario. Even having taken all the precautions, something totally unprecedented and unforeseen could occur. Vendors must ensure that smart devices operate appropriately in this scenario. HVAC and lights must stay on schedule. The building must function smoothly even in the event that the BAS or EMS is "headless".

Conclusion

Internet connectivity is highly desirable in Building Automation and Energy Management Systems, but comes with grave responsibilities. The responsibility to secure these systems cannot lay with the customers. By adhering to IT best practices, and taking advantage of cloud computing and wireless technology, our buildings can enjoy powerful, convenient

and secure BAS and EMS systems. Incenergy is committed to providing an Energy Management System with robust security while requiring minimal efforts from customers. Customers must insist upon these secure systems to meet their energy management and building automation needs. Building Automation and Energy Management Systems' rapid technical evolution has to include cutting edge security practices.

Endnotes

1 http://www.washingtonpost.com/investigations/tridiums-niagara-framework-marvel-of-connectivity-illustrates-new-cyber-risks/2012/07/11/gJQARJL6dW_story.html

2 http://www.wired.com/images_blogs/threatlevel/2012/12/FBI-AntisecICS.pdf

3 http://articles.washingtonpost.com/2012-07-13/news/35489028_1_user-passwords-hackers

4 http://arstechnica.com/business/2012/04/rise-of-ics-forever-day-vulnerabiliities-threaten-critical-infrastructure/

5 http://www.infosecurity-magazine.com/blog/2013/3/22/three-critical-features-that-define-an-enterprisegrade-cloud-service/841.aspx

6 http://www.wired.com/gadgetlab/2012/11/ff-mat-honan-password-hacker/5/

7 http://www.computerworld.com/s/article/9237845/Security_experts_applaud_Apple_s_new_two_factor_authentication

8 http://www.digicert.com/TimeTravel/math.htm

9 http://docs.zigbee.org/zigbee-docs/dcn/09-5378.pdf