Daintree™

Network Security Primer

GE current
a Daintree company

Daintree™ Network Security Primer

System Architecture

The Daintree control system consists of on-site equipment (including the Wireless Area Controller or WAC, sensors, lights and other actuators) and software hosted in the cloud. The cloud software is currently hosted on the Amazon Web Services (AWS) and Microsoft Azure platforms.

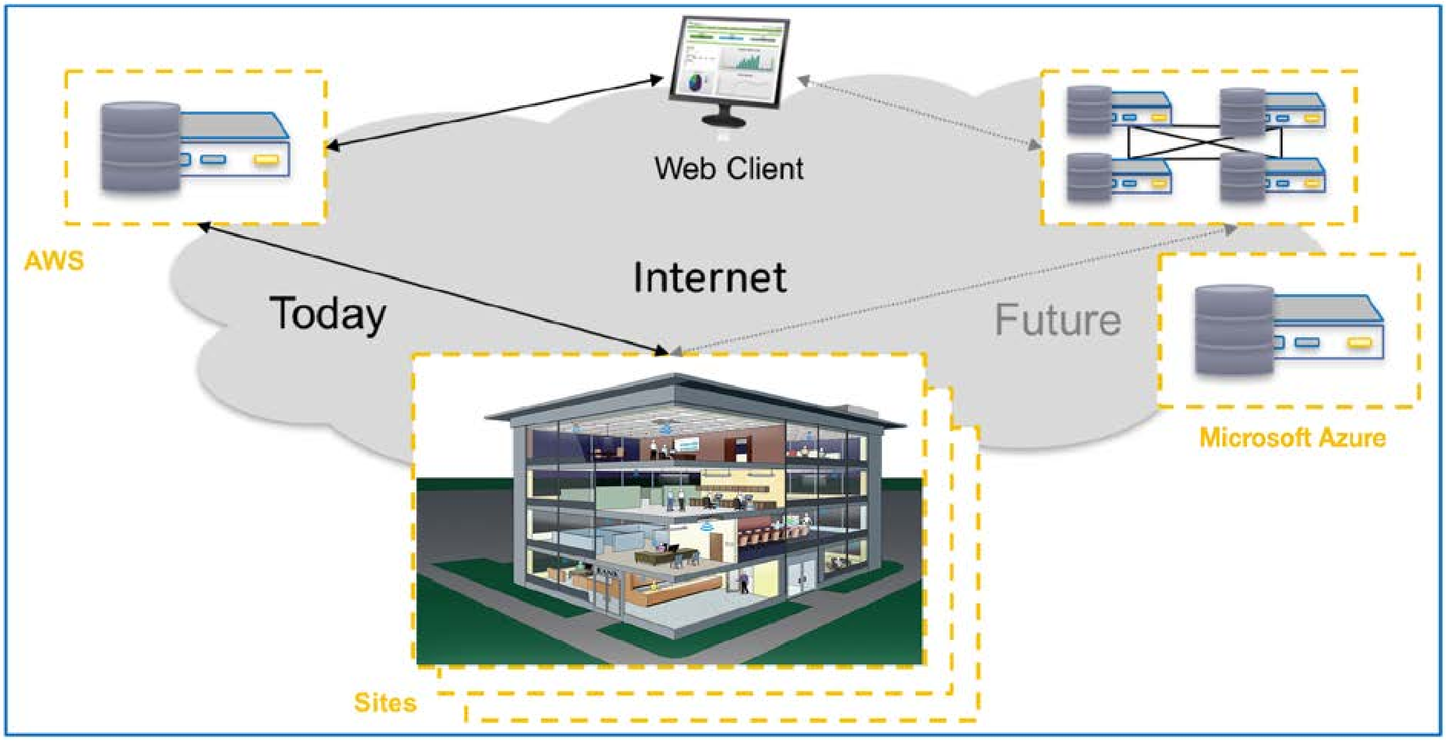

Figure 1: System Architecture

Regarding security, there are four main areas for discussion:

1. Cloud Security;
2. Edge-to-Cloud Security - including IP-side security between the WAC, Internet, and cloud software;
3. Wireless-side Security - between the WAC and the wireless sensors, lights and other actuators;
4. Network Isolation.

It should be noted that the WAC is the only device on-site that has connectivity to the Internet. All other devices on-site (wireless thermostats, lights, sensors, etc.) communicate with the ZigBee protocol, and cannot be accessed from the Internet.

Cloud Security

Access to the cloud-based user interface is secured via the HTTPS protocol, protecting customer information using server authentication and data encryption. The Daintree platform supports integration with 3rd party Single Sign On (SSO) providers and other two-step verification authentication services. This ensures that customer data is safe, secure, and available only to registered users. Using role-based authorization, users enter a unique user name/password combination on login, with only system administrator roles having the ability to manage user accounts. System data is completely inaccessible to unauthorized users.

AWS Implementation

Customer data is further protected by the complete segregation of each customer's data. Daintree system administrators may intermittently access the cloud instance to ensure uptime and accessibility.

Edge-to-Cloud Security

After physical installation and initial setup, the WAC and cloud software establish trust with X.509 certificate-based mutual TLS authentication. Authentication occurs from client to server, as well as server to client (Figure 4). Thereafter, TLS encryption with the recipient's public key is applied to all messages sent between the WAC and the server.

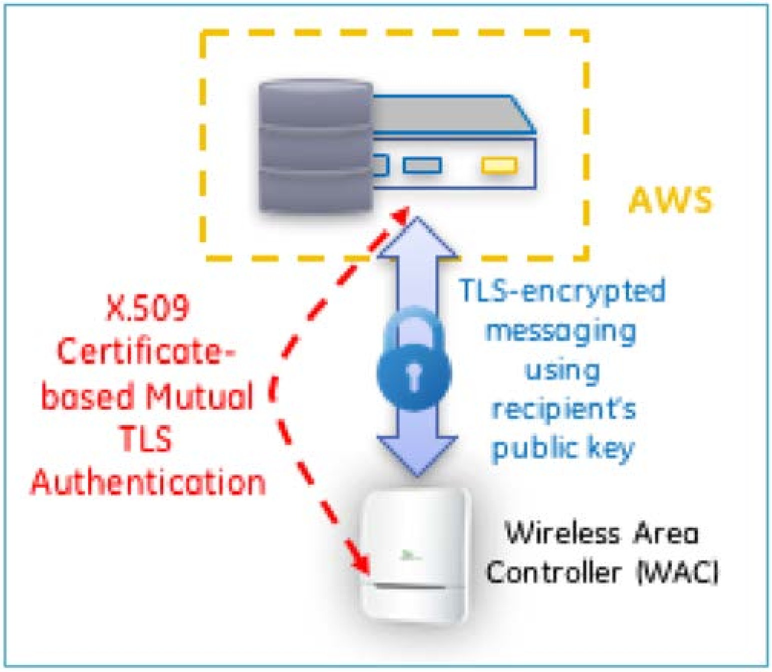
AWS
X.509 Certificate-based Mutual TLS Authentication
TLS-encrypted messaging using recipient's public key
Wireless Area Controller (WAC)

Figure 2: Authentication and encryption between WAC and cloud software text.

The Daintree control system uses best practices for TCP/UDP port management. Specifically, the WAC only requires outbound TCP/UDP ports (from the WAC to cloud). Full details of how the Daintree control system can be deployed can be found in the "ControlScope IT Networking Guide".

Wireless-side Security

The on-site wireless network is ZigBee, a global standard for Internet of Things (IoT) application. Used in a wide range of applications by hundreds of companies, ZigBee has been deployed in connected lighting, utility and retail applications, and the Smart Home.

The ZigBee standard currently being used in the Daintree control system is ZigBee Pro. ZigBee Pro defines the security standard to ensure interoperability between products from different vendors. Within this standard, there is a single trust center which manages access and trust. In the Daintree control system, the trust center resides in the WAC.

Security Keys and Encryption

The ZigBee Pro security specification has a symmetric key exchange protocol that is used by the trust center to distribute a common network key. This network key is used by all devices on the wireless network to encrypt (and decrypt) their messages while communicating on this network.

This process occurs during initial setup, when the WAC initiates connection with the network to allow devices to join the wireless network. On the Daintree system, this act of establishing the network connection(s) can only be executed by a user with administrative privileges on the web GUI.

A known security exposure exists in ZigBee Pro systems during this initial setup phase. The ZigBee Pro standard calls for this key exchange protocol (to distribute the common network key) to be encrypted with a well-known key.

This means that with some significant effort, an intruder could successfully decrypt the key exchange protocol during this brief period with the well-known key and obtain the common network key, thereby allowing them to decrypt all communications on that specific wireless network.

That said, this initial setup runs quite briefly, and ZigBee, being a low power technology, can only be 'sniffed' and thus found by a radio receiver located very close to the system or site during this initial setup period, requiring both a precise knowledge of the system installation and commissioning schedule and access within the facility during the period. Furthermore, such a breach would be limited to a single WAC network (no more than 200 wireless devices) and limited only to the ZigBee side of the network.

After the brief key exchange, messages exchanged between all wireless devices are encrypted using the network key with AES-128 with CCM, which is a NIST approved cryptographic standard used to classify information up to the SECRET level.

For further detailed technical information, refer to **https://products.gecurrent.com/controls-and-sensors/daintree-enterprise-wireless-controls.**

ZigBee Light Link Exploit

In a recent article, a Philips Hue system was exploited using a drone that came into very close proximity to the Philips Hue system and managed to take control of the devices. Philips Hue uses a variant of ZigBee, called ZigBee Light Link (ZLL).

ZLL, which was designed around consumer lighting requirements, offered mechanisms to "bind" off-the-shelf products to each other by the consumer, using close-proximity between devices. The act of binding included the exchange of security material. A bug in the Philips Hue firmware allowed the drone to obtain the security material, and thereafter, exploit the system.

The Daintree control system neither uses the ZigBee Light Link, nor does it allow proximity as a basis of establishing trust. Rather, only the WAC will determine whether a new device can be allowed onto the network (and receive security material), and the WAC will initiate the network to allow this only when an administrator with the necessary privileges decides to do so. It is worth noting that Philips quickly fixed the bug and released the firmware.

Network Isolation

One of the strongest forms of security is isolation. Networks that are isolated from each other prevent compromises in one network from affecting other networks.

As shown in Figure 5, each WAC manages a separate ZigBee network. Devices on one ZigBee network cannot communicate with devices on another network. Furthermore, each WAC independently manages its own and its network's security credentials. This effectively isolates these wireless networks from each other.

Furthermore, when a device gains access to the ZigBee network, that device cannot gain access to the IP network connected to the WAC. This effectively isolates the ZigBee network from the IP network.

A further common practice is to isolate the data network used to move Daintree data (to/from the cloud) from the rest of the corporate network. Note that VLANs are often used to support this method.

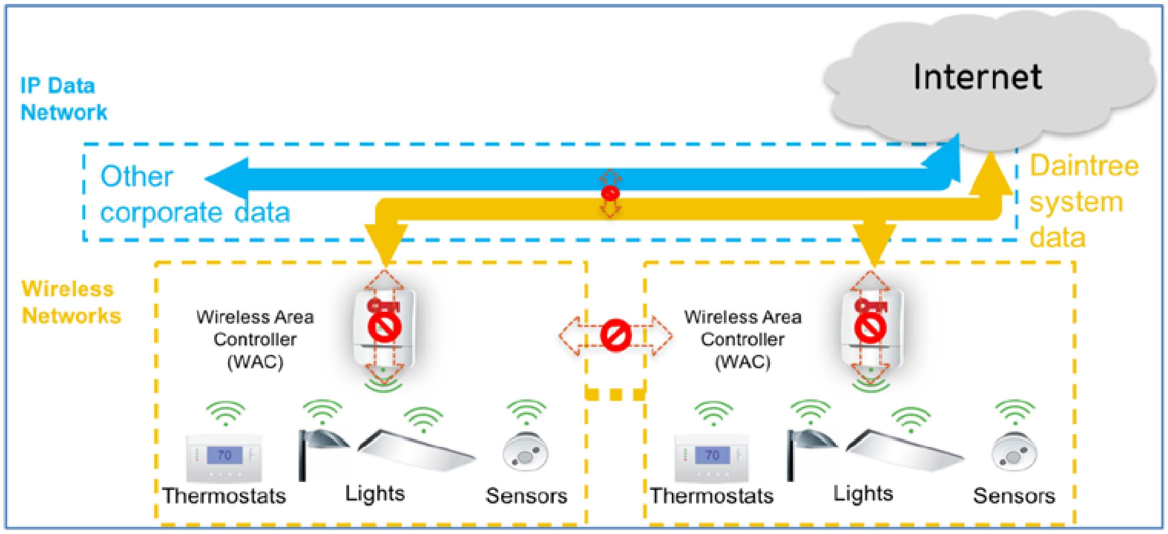

Figure 3: Network isolation