Internet of Things (IOT)/Bring your own devices (BYOD)

Discovery and Recommendation Report

Background & Introduction

Our current network on campus does not support the plethora of authentication mechanisms used by IoT devices connecting to it. IoT provisioning is being handled by different units across campus, with little consistency, emphasis on security, or accountability of devices. Instead, individual departments do what is needed to allow instruction and research to occur using these devices.

Project Goals

- Research device self-registration for Faculty, Staff, and Students connecting to the campus wifi network.
- Research how a device will reach out to cloud-based controllers and be controlled from other devices as necessary.
- Research using zero-trust security model to layer appropriate access levels to these devices, associate them with known in-person owners, and allow them to exist on our network, use our network, but not interfere with other users on the network.
- Capture device ownership
    - Endpoint Management tie-in
- Recommend optional tools to meet requirements.

Project Deliverables

- White paper with solution recommendations.

Key Recommendations

- Extend access.services.wisc.edu
    - Bulk device management
    - Endpoint management integration
    - Departmental security group membership management
    - PSK management
- Develop new multiple pre-shared key network for departmental IOT access
    - Each department/service gets a unique key but all devices share the same SSID.
    - Vlans/subnets connected to campus MPLS backbone allowing departments to manage firewall policy for individual networks.
- Conversion of UWNet into (or replaced by) a true guest network with clients treated as external devices with respect to access to campus services.
- Develop improved network access security. If possible this will be layered on top of the existing Eduroam network so local devices and users would be able to leverage the newer authentication and authorization mechanisms while eduroam guests would still get access using the current eduroam authentication infrastructure.
- Promote campus customer engagement with our wireless vendors to encourage use of compatible IOT devices.

<u>Intro</u>

We have been tasked with researching the needs of campus wireless customers with respect to access for devices that do not conform to the standard model of authenticating a single device with a specific user's credentials. Many of the devices falling into this broad category can be classified as “IOT” devices but this definition does not comprehensively describe the broad scope of types of devices and associated broad scope of device management needs desired by our campus customers.

In addition to gauging the relative priorities of these kinds of devices we were also asked to research:

- device self-registration expansion
- access to cloud-based controllers for IOT devices

- Zero Trust model in relation to IOT devices
- Endpoint Management integration

One of the methods used was to survey campus customers in order to assess the relative priorities of different wireless access technologies and methodologies. If we average the scores for each category across all responses we arrive at the following list arranged from most desired to least:

Cloud/Internet access (Outbound)
Static IP addressing
MAC Auth registration
Network Isolation,customer/device specific networks
2.4 only
Campus AD EAP-TLS certificate support
BLE
Z-Wave
Zigbee

<u>Survey Analysis</u>

The customer survey attempted to assess the level of need for specific wireless access technologies and to place them in a list of relative priorities. We asked for customers to score their perceived need for:

- *Access for 2.4 Ghz only devices.*
    - Responses indicate that there is a continued desire for Campus to offer ubiquitous 2.4 GHZ wireless. No change required
- *Access for Zigbee devices*

    - Survey responses indicate limited interest in this currently. This technology will be supported starting in the Aruba 500 series access points. Support on campus will come as access points are upgraded to newer hardware. If support is needed sooner we can look at targeting access point replacement to facilitate support or explore deploying USB zigbee management equipment.
- *Access for Z-Wave devices*
    - There is currently limited industry support for this technology and there was little interest from survey respondents.
- *Access for Bluetooth Low Energy (BLE) devices*
    - Support for BLE devices is built into the Aruba AP 340 series. Interest is limited but if resources are available, a more targeted solicitation for interested customers can be performed.
- *Devices that require Mac Authentication (not capable of Captive Portal) without an associated NetID*
    - There is widespread interest for expansion of the existing MAC address registration system, access.services.wisc.edu. Further solicitation of input from customers is advisable to identify key application requirements but it can be surmised that rapidly onboarding large numbers of devices, departmental/service account authentication, asset reporting, and longer registration times are among the expressed improvements.
- *Devices requiring host based EAP-TLS certificates (Machine Certs) issued by Campus AD Certificate Services*
    - There is clear interest from customers to provide a certificate based authentication system for departmental owned computing assets. This system would allow the devices to access (and be accessible from) the network prior to user authentication to the device.
        - ClearPass has the ability (with additional licensing purchases) to serve as a CA for this type of service.

        - Many of our peer institutions are leveraging commercial services to deliver these features. One product name mentioned by many of our peers is SecureW2.
- *Devices that require a network isolated from other campus devices*
    - Respondents showed interest in this feature. We can currently expand our policy based vlan steering (used on Eduroam for participating customers) to other customers as well as other SSID's. Customer specific vlans/subnets can be delivered to clients on all existing Campus wireless networks. Consultation with interested customers as well as Cyber Security would be necessary to illuminate both desired features as well as security constraints.
- *Devices that require outbound Cloud/Internet access*
    - The campus wireless network can satisfy this need by delivering customer specific networks to departmental assets. The new wireless core is provisioned to participate in the mpls backbone across the UW Madison network core. Leveraging mpls attached, customer specific networks for each customer will allow customers to manage the firewall policy for their own devices and craft custom NAT/security policy to allow for cloud access to/from local devices. Each case will likely have to be considered uniquely as cloud-based management can vary widely between device vendors.
- *Devices that require a Static IP address*
    - This is another use case for customer specific networks where customers can manage the ip address entries for themselves. The main subnets for Eduroam and UWNet will never likely support static ip address assignment.

<u>Device Self Registration</u>

There is a clear desire for departmental customers to be able to deploy large numbers of devices that require little or no interaction from the user in order to obtain network access. These devices can range from classroom or checkout laptops or mobile devices to lab sensors and handheld inventory devices.

A service (access.services.wisc.edu) currently exists to allow anyone with a netid to register new devices, delete an existing registration, or renew an existing registration. All registrations are made using the netid of the user that has authenticated (UW Madison

netid) to the application. These registrations allow devices access to the UW Madison open network (UWNet). This existing system can be extended to accommodate departmental customers' requirements as well as integrate with campus endpoint management systems to leverage the additional device attributes available for authorization. There is some concern that unfettered access and unlimited (or at least extended) registration times will lead to a bloating of the device repository causing potential database bloat.

Zero Trust Model

At the current time there are many broad definitions of Zero Trust. In the most basic terms Zero Trust means not trusting any device connecting to the network. Access to services is not granted merely as a result of having network access. Access to services is then granted based on a client's ability to assert its permission to access.

How then do we assess the client's authorization for access and at what point in the system do we control the access? Every network vendor of course has their own solution that requires heavy investment, end to end, in their products.

In order to begin developing a working solution for this campus we will need to have some guidelines regarding what constitutes sufficient validation for accessing services and where we are going to assert our control. At the network access level? At the firewall level? At the application level?

Our current network vendors (HP/Aruba, Palo Alto, Cisco) have a variety of solutions that can be leveraged in whole or in part to implement greater access security and awareness.

Aruba's approach to zero trust involves leveraging the device profiling capabilities of the ClearPass Policy Manager as well as the role based Policy Enforcement engine of the wireless controllers to assign a policy to a given class of devices or group of users. Coupled with the platform's ability to integrate with many endpoint management systems (including BigFix and VMWare Workspace One) it looks like there is a lot of room to advance the amount of device profiling and policy assignment we are doing.

As an alternative to deploying policy on the wireless controllers we could use the device/user profiles to assign device traffic to specific segmented portions of the network and use our existing firewalls to enforce policy.

At the current time UW Madison is doing a limited amount of device profiling along with a very limited number of different device roles. Our experience using this system of management, while limited, has been successful so far. If the campus would like to expand this capability, the wireless team will need to participate in a broader effort with other interested campus parties in order to define Zero Trust requirements and to design implementation features to meet those requirements. If this discussion is ongoing as a part of other projects (NG2N? Something in security?) then it would be helpful to work with them to bring some clarity to the wireless engineering team.

Committee Members

Jeanne Skul, Executive Sponsor
Dennis Lange, Project Sponsor
David Crabb, Project Lead
Jeff Robertson, Chris Poser, Oakes Dobson, Project Team
Care Adametz, Project Manager