Wireless Networking

(hosted at http://utahgeeks.sourceforge.net)

I. OBJECTIVES

The University of Utah has a need to provide near seamless secure wireless access across campus without impacting or hindering local organizations. This wireless network should:

- Be accessible to all faculty, staff, students, and University affiliates.
- Be accessible to affiliates of other universities after the establishment of a trust relationship with their authentication servers.
- Follow the EduPerson ID format (username@domain) to allow federation of identities between organizations and institutions.

This document is designed to illustrate how this type of wireless network could be deployed in a decentralized heterogeneous environment with various organizations owning and maintaining parts of the wireless network.

The goal of this document is to provide direction to local organizations in making their wireless networks secure and available to the university community without the need to take over wireless networking campus wide or to prevent local organizations from deploying their own restricted wireless networks.

II. CONTENTS

III. WRITTEN BY (alphabetical order)

Chris Hessing
chris.hessing@utah.edu
Marriott Library – University of Utah

Bret Jordan
bret.jordan@utah.edu
College of Engineering - University of Utah

Terry Simons
terry.simons@utah.edu
Marriott Library – University of Utah

Appendix 1 – Wireless Implementation Reasoning, Goals, and Plans

I. REASONING

The focus of this section is on wireless networks that are beneficial to the entire university community. This information may or may not be pertinent to private departmental wireless networks.

Even though 802.11 based wireless networking is very popular, it is difficult to provide secure connectivity. Wireless networking has security considerations that wired networks do not have. The main consideration is that wireless traffic travels through the air unencrypted. The Wired Equivalency Protocol (WEP) was introduced to provide secure connections by encrypting the wireless traffic with a shared encryption key. Unfortunately, it has been proven that WEP is insecure (http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html). Another consideration is that some wireless cards, especially older ones, do not support WEP.

In a campus setting, wireless security is even more difficult. Closed networks, while hiding the SSID, offer no real protection that cannot be socially engineered. Encryption with WEP only offers quasi protection as every user in this community-accessible wireless network will have the same encryption key. This would allow any user on the network to gather and decrypt everyone else's communications and thus defeat the purpose of the security. Clearly closed networks and encryption with WEP do not provide any real security and, in fact, only add a level of complexity to end user's configurations that would make it impractical for a campus wide solution.

Currently most of our public wireless networks provide security by authenticating the end user with a mechanism such as WAAC (provided and developed by the Marriott Library) or WANA (provided and developed by Netcom). While these do not provide encryption they do restrict network access based upon verified affiliation with the University.

Due to these limitations it is necessary to periodically re-evaluate new technologies, as they emerge, to provide a more secure environment for authenticating and encrypting wireless networks connections.

The next generation wireless authentication committee has agreed that 802.1x should be looked at as a potential replacement for other, less secure, authentication mechanisms on campus.

II. GOALS

The primary goal of this wireless network is to provide a scalable and secure wireless network with seamless connectivity that can be departmentally managed.

A. Scalability

Scalability is inherent in 802.11a and 802.11b/g networks with load balancing, radio hand-off, zoning, and multicast rates. The only real issue is the cost of the wireless Access Points and their Radios.

B. Security

As previously mentioned, current wireless security has various limitations and does not meet the needs of a secure campus-wide wireless solution.

Implementation of 802.1x is necessary to provide per-user/per-session rotating WEP keys that would allow every user to have their own WEP key that is dynamically changed at a given interval.

C. Seamless Connectivity

The most problematic area of true campus wide wireless networking is Seamless Connectivity. Different SSIDs, authentication methods, and network addresses currently prevent users from seamlessly roaming from building to building and in some cases users are even required to reconfigure their computer as they move from building to building. To use WANA as an example: A user that authenticates to a WANA-enabled building, even though they might be able to roam to another WANA-enabled building, could quite possibly have to re-authenticate. They would also, more than likely, get a new IP address which would break all persistent connections. Although WANA may be available in multiple places due to the use of non-routed networks and on-site servers, true roaming is not currently possible.

1. SSIDs

Create a campus naming standard for secure and insecure wireless networks. The secure network name should be used in conjunction with the current University of Utah best practices for wireless networks (i.e. Currently 802.1x). The insecure network is optional and should reflect insecure wireless networks that do not provide data security. (I.E. WAAC and WANA)

Both networks should be able to coexist with each other. The secure network should be generic enough for future compatibility.

It should also reflect the function of the network name (i.e. secure.utah.edu). The insecure network should not be department or protocol specific so that it may also be adapted for future purposes (i.e. insecure.utah.edu).

All private departmental networks should not broadcast their SSIDs and should use SSIDs names that resemble their organization (i.e. their DNS domain name) to avoid confusion for users trying to access the Public Wireless Network.

2. Authentication

Implement 802.1x and campus wide a Radius Mesh for all public wireless networks. This Radius authentication mesh will use the EduPerson ID (http://www.educause.edu/eduperson/) format for departmental name space and uNID name space.

With 802.1x authentication and Radius proxying (realms) it is possible to have an authentication mesh such that users from separate departments would be able to access the network on another part of campus with a valid username from their own department. This methodology, given that 802.1x is client-based and Radius proxying is server-based, would allow a user to configure their authentication client once and then roam from building to building without needing a new account for each network.

This authentication mesh, via Radius proxying, would also allow authentication pairing with other universities. Visiting affiliates of other universities would then be able to use the wireless network after presenting a valid authentication credential from their university.

3. Network Address Space

Various potential technologies are currently being evaluated to solve this problem. 802.1x does not provide the ability to roam without dropping persistent connections and large layer 2 networks are problematic due to issues with broadcast domains and VLAN spanning issues.

D. Departmental Manageability

Given the distributed nature of campus computing, the wireless network needs to interoperate with existing departmental infrastructures. These

departmental infrastructures often have their own IT staff, authentication methods, user accounts, and physical infrastructure. The goal is to design a campus wide wireless solution that will work with these existing departmental infrastructures so that departments wishing to maintain control over their own users can do so and still allow inter-operability with the rest of campus.

III. PLAN

In order to accomplish the above mentioned goals, the following must be done:

- Establish campus-wide secure and non-secure SSIDs
- Deploy a campus-wide radius proxy mesh
- Deploy PKI infrastructure for server and user certificates
- Identify vendor hardware/software compatibility issues
- Campus Awareness
- Deploy 802.1x authentication and DHCP
- Continue testing future technologies

A. Establish campus-wide secure and non-secure SSIDs

The next generation wireless committee has agreed that two common SSIDs should be established for any public wireless networks providing wireless network access to faculty, staff, students, and University Affiliates (i.e. secure.utah.edu and insecure.utah.edu).

B. Deploy a campus-wide radius proxy mesh

A proxy radius mesh should be established between Netcom and the various departmental networks using the EduPerson ID format (user@domain) for the realm delegation. One Netcom radius server should be located at each distribution node for redundancy. Radiator (a Radius server) has been purchased for campus-wide use and can be used for such a purpose. Departments that do not wish to use Radiator may use another Radius server that can provide proxy capability and campus recommended 802.1x authentication mechanisms.

Each organization that maintains their own user accounts or maintains their own Access Points and wants to interface with campus, should run their own Radius server to interface with the Radius Mesh.

The reason for this is both one of security and expandability. Access Points can usually only name a few Radius servers to try and authenticate against and departments can have control of their user space and can easily add users.

This proxy Radius Mesh will allow departmental user accounts to be used at other locations across campus to gain access to the wireless network. It will also allow for pairing with other schools, such as Salt Lake Community College or Brigham Young University.

See diagram 1.

C. Deploy PKI infrastructure for server and user certificates

The upcoming campus PKI infrastructure should be used to provide user and server certificates for Wireless Network Authentication purposes. This would allow users to take advantage of 802.1x authentication methods that can use digital certificates for the client and the server. This would also limit social engineering and security problems that are inherent with maintaining password files.

D. Identify vendor hardware/software compatibility issues

Continue testing various vendor hardware and software for compatibility issues. This will allow the creation of a "known to work" and "known not to work" web site.

See Appendix 5.

E. Campus Awareness

Provide notice and documentation to faculty, staff, students, and university affiliates about the migration from the current wireless network to the new 802.1x campus wireless network.

F. Deploy 802.1x authentication

1. Upgrade Wireless Access Points to support 802.1x if needed

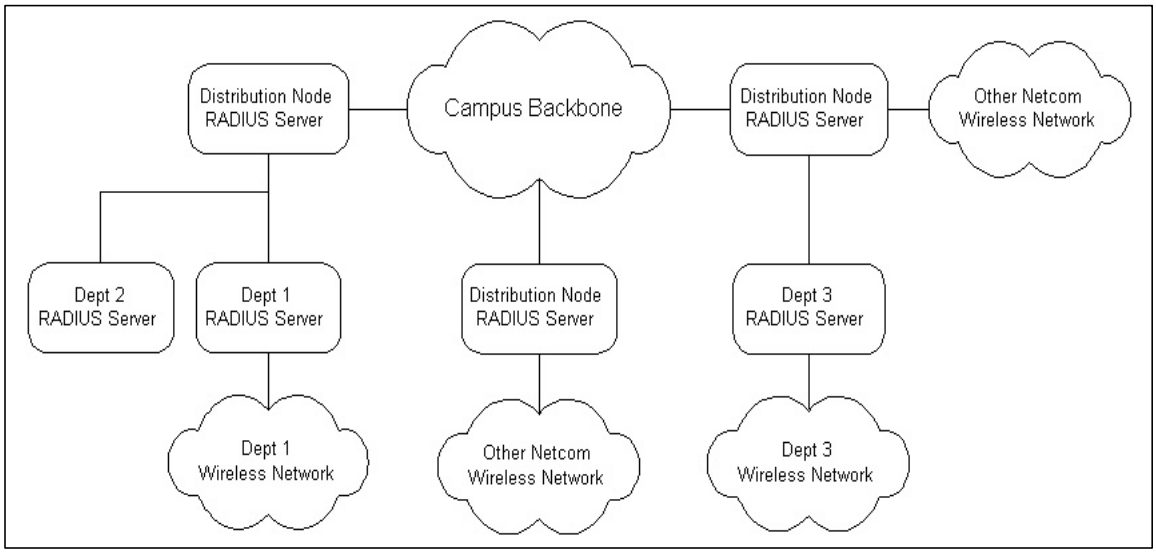
2. Build Wireless Networks with dynamic DHCP.

3. Provide client software.

G. Continue testing future technologies

As new technologies continue to surface, the Wireless Network Group needs to continue testing these new technologies in an effort to make access to the network more stable, secure, and seamless.

Diagram 1


Distribution Node
RADIUS Server
Campus Backbone
Distribution Node
RADIUS Server
Other Netcom
Wireless Network
Dept 2
RADIUS Server
Dept 1
RADIUS Server
Distribution Node
RADIUS Server
Dept 3
RADIUS Server
Dept 1
Wireless Network
Other Netcom
Wireless Network
Dept 3
Wireless Network

Appendix 2 – Proposed Wireless Policy

I. PURPOSE

To provide a base guideline for University Public and Private Wireless Networks.

II. REFERENCES

PPM 1-15, Information Resources Policy

University Information Technology Resource Security Policy
http://www.it.utah.edu/IT_Security_Policy.pdf

III. DEFINITIONS

A. Wireless Network: A network technology that uses radio frequencies to connect wireless devices together or connect them to a Local Area Network (LAN).

B. Wireless Network Device: A computer, printer, PDA, or other electronic device that uses radio frequencies to connect to a Wireless Network.

C. Access Point: A device used as a connecting point between a Wireless Network Device and a LAN.

D. Private Wireless Network: A Wireless Network that is restricted and limited to a certain organization.

E. Public Wireless Network: A Wireless Network that is available to all Faculty, Staff, Students, and University Affiliates.

F. Encrypted Session: A Wireless Network Session where all communications (authentication and data traffic) are encrypted.

IV. SCOPE

This policy applies to and governs all Wireless Network Devices connecting to a University of Utah network and all Wireless Networks and their frequencies located within the geographical boundaries of the University.

V. POLICY

A. All Wireless Network Devices and Access Points must abide by all federal, state, and local laws, rules or regulations pertaining to wireless networks.

B. Acceptable use of Wireless Networks is governed by Policies and Procedures Manual 1-15 (Information Resource Policy)

1. Interference or disruption of other authorized communications that result from the intentional or incidental misuse or misapplication of Wireless Networks or Wireless Network Devices is prohibited.

C. All frequencies to be used in a Wireless Network must be registered with the University prior to implementation of the Wireless Network. If an organization has exclusive use of a building they may register that building in place of individual frequencies.

D. It is the responsibility of the IT Steward for an organization that maintains a wireless network to register and maintain a current "Point of Contact" for that wireless network with the University.

E. Security

1. Access Points should be physically secure.

2. Management access to Access Points must be secure.

3. Wireless Networks are subject to the IT Security Policy.

F. Authentication

1. Access to any Wireless Networks must be authenticated by a currently acceptable secure method as defined by the Wireless Committee.

2. All authentication attempts must be logged and those logs should be kept according to University Policy.

G. Encryption

1. All user-sensitive authentication credentials (i.e. usernames and passwords) must be encrypted over the Wireless Network.

2. All wireless data traffic should be encrypted.

3. If wireless data traffic is not encrypted by choice or by design, users connecting to that wireless network must be informed and encouraged to use a secure alternative (i.e. VPN, SSH, SSL, etc.).

H. Private Wireless Networks

1. Private Wireless Networks should not broadcast their SSID.

2. Private Wireless Networks should use an SSID that reflects their Organization such as their Domain Name.

3. Private Wireless Networks must not use the official University of Utah public SSIDs (i.e. insecure.utah.edu or secure.utah.edu).

4. Private Wireless Networks should be designed and deployed to limit physical and logical interference with other Wireless Networks.

I. Public Wireless Networks

1. The SSID for Public Wireless Networks must be one of the official University of Utah public network names (i.e. insecure.utah.edu for non-encrypted sessions or secure.utah.edu for encrypted sessions).

2. Public Wireless Network traffic should be securely isolated from the Local Area Networks they connect to.

J. The local IT Resource Custodian or designee of the IT Resource Steward of the Organization (as defined in the University IT Security Policy) is responsible for the Wireless Network and user accounts owned and managed by the Organization.

K. Where more than one organization occupies a building the IT Resource Stewards will determine shared or delegated responsibilities in regards to the Public Wireless Network in that building if it exists.

L. In the event that one Wireless Network interferes with another Wireless Network and the IT Resource Stewards cannot resolve the issue after being notified of the problem, the issues will be escalated to the Information Technology Advisory Committee for a resolution.

M. Wireless networks are subject to the IT Security Policy and may be disconnected per that policy. Specific college and/or departmental policies may be more restrictive depending on the security requirements of the college and/or department.

N. Current best practices should be reviewed by a cross section of campus wireless network administrators under the direction of ITAC (Information Technology Advisory Committee) at least every 12 months and any changes implemented during the next summer term.

Appendix 3 – Current Best Practices

I. Hardware

A. Access Points must be field upgradeable of both software and radios.

B. Access Points must support 802.1x.

C. Access Points should support at least the following 802.1x authentication protocols: EAP-TLS and EAP-TTLS.

D. Users should be encouraged to buy multimode cards (A/B, A/B/G).

E. Access Points acquired with University of Utah Student Computing Task Force Funding must comply with these guidelines.

II. Security

A. Access Points should not be located in areas where they can easily be stolen or tampered with. Instead of locating the Access Point in the hallway of a building that is not secure, one might choose to put the Access Point in a corner of an adjacent secure office.

B. Management access (SNMP, HTTP, Telnet, etc.) should be restricted to wired ports and should be limited to a small number of machines.

C. All default Management passwords must be changed.

D. Wireless Networks should be on their own VLAN and Router ACLs or a Firewall should limit that VLAN from talking to other VLANs on that LAN.

E. Users should use SSH or a VPN solution to gain access to trusted VLANs.

F. Wireless Networks should restrict server software as much as possible through the use of Router ACLs and/or Firewalls (i.e. deny incoming SYN packets from the outside world).

G. Access Points should be configured to limit Broadcast Storms, all non IP traffic, and Ad-hoc connections.

III. Authentication

A. Only Wireless Networks that use a currently accepted dynamic keying authentication protocol (such as 802.1x) may use the secure SSID. (i.e.

secure.utah.edu). (Note: EAP-MD5 does not support dynamic keying, and is not acceptable.)

B. Current Public Wireless Networks that use WAAC or WANA for authentication may use the insecure SSID (i.e. insecure.utah.edu) if they are incapable of using 802.1x. However, these networks should be upgraded to support the current best practices (i.e. 802.1x).

C. Authentication should be handled at the local organizational level via RADIUS realms based on the domain part of the username.

D. All user names should be in the Edu-Person ID format (username@domain). The use of the Edu-Person ID format will ensure that collisions do not occur across the distributed wireless network and is required to facilitate proper proxying of authentication requests. This will also allow for future growth and ensure roaming within the University and between universities.

E. Radius servers may be setup by default to allow uNID authentication with and without the Edu-Person ID domain.

F. In order to add/remove a Radius server domain to/from the authentication mesh, the organization must have authoritative responsibility for that DNS domain.

IV. Private Wireless Networks

A. Private Wireless Network should make use of smaller zone sizes and larger multicast rates to limit possible interference with other Wireless Networks.

V. Configuration Example

A. Proxim AP2000 / Avaya AP3
http://utahgeeks.sourceforge.net/configExamples/

B. Radiator
http://utahgeeks.sourceforge.net/configExamples/

Appendix 4 – Proposed Administrative Responsibilities

I. ITAC

ITAC should be globally responsible for the Public Wireless Network and its Distributed Authentication Services.

II. Office of Information Technology (OIT)

The Office of Information Technology should be responsible for the following functions of the Public Wireless Network as they relate to Distributed Authentication Services:

A. Maintenance of Campus Core Radius Servers

The University of Utah's Systems Group under the direction of the Wireless Committee and Authentication Committee should maintain the campus core servers that are used for the Radius Mesh.

B. Maintenance of Campus Radius Mesh

The University of Utah's Systems Group in cooperation with Radius Mesh Members and under the direction of the Wireless Committee and the Authentication Committee should maintain, update, and upgrade the Radius Mesh as needed.

C. Negotiations with Other Universities

The Office of Information Technology in cooperation with The Institutional Security Office should be responsible for negotiations with other universities that wish to join the Radius Mesh and should verify that the guidelines are met and checklists are completed.

III. Wireless Committee

The Wireless Committee should be responsible for the following functions of the Public Wireless Network and Private Wireless Networks:

A. Guidelines and Checklist for Connecting to the Radius Mesh

The Wireless Committee along with The Institutional Security Office should develop guidelines and checklists for organizations desiring to join the Radius Mesh from internal or external sites.

B. Gathering Point of Contacts for Wireless Networks

The Wireless Committee should be responsible for developing a means of collecting and securely publishing a list of contacts for mesh-enabled and private Wireless Networks. It is important that this information be readily available to all Wireless Network Administrators and The Institutional Security Office.

IV. The Institutional Security Office (ISO)

A. Abuse Issues

The Institutional Security Office should be globally responsible for addressing all abuse complaints as directed by the University Security Policy. The Institutional Security Office, upon receiving a complaint, should inform the local Point of Contact for the Wireless Network where the abuse is originating from and inform the local Point of Contact for the organization that is authoritative for that user account so that the issue can be resolved. Blocks need to be processed at the authoritative radius server for the user, not as an IP block at a firewall or router, due to the use of dynamic IP address and roaming between IP networks.

V. Local Organizations

Local organizations that own and manage part of the Public Wireless Network should follow the best practices guide for maintaining their Access Points, Radius Servers, and DHCP Servers; create a support@domain.utah.edu email address to which support or authentication enquiries can be sent; and must maintain authentication logs per University Policy. Local organizations that are planning major outages to their Wireless Network should post to a global wireless-network-outage list that needs to be created

VI. Other Universities

Universities that wish to participate in this Wireless Mesh must satisfy the guidelines, checklists, and periodic reviews to be determined by The Institutional Security Office. At a minimum, an external organization must provide a Point of Contact for their Institution that can deal with configuration and abuse issues and must provide a detailed abuse policy.

Appendix 5 – Support and Known Issues

Support is one of the major obstacles with deploying and maintaining a distributed Wireless Network such as the one described by this paper. Below is a list of the major issues in supporting this kind of system.

I. Global Management of a Scalable and Decentralized Network.

The Radius Authentication Mesh was designed with distribution and flexibility in mind. Organizations that connect to the Radius Mesh should be responsible for supporting authentication issues with their organization level accounts, issues with access points that they own and maintain, and should base their end user support documentation and training off that of the central help facilities. The campus Wireless Committee and Authentication Committee should provide support on global core issues such as the Radius Mesh.

II. Support Documentation and Testing

The University of Utah campus is highly diversified with many talented computer support professionals and network engineers. The development of support documentation and testing should be a collaborative effort by all organizations that connect to the Radius Mesh and should be a priority for those organizations.

Some organizations currently have extensive troubleshooting and documentation relating to 802.1x. An official collection point for support documentation should be setup by the Wireless Committee to ensure fairness to all mesh participants. All support and testing documents submitted to the Official Support Documentation site should clearly identify and give credit to the writers and testers for their respective data. The Wireless Committee should routinely verify that all documents in the Official Support Documentation are current and correct.

III. End User Support

A central campus location should be responsible for providing direct support to students and affiliates that wish to receive help getting connected to the Wireless Network. The Marriott Library is currently providing this service and has a trained staff for walk-in support. However, an official location should be decided by the Wireless Committee to ensure fairness to all mesh participants. NetCom should provide telephone support via their help desk. All support documentation should be uniform to help prevent disparity.

For authentication support issues, the central help facilities will only be able to help with the campus wide accounts in the @utah.edu space. Users with organization level accounts will need to seek support from their respective organizations when it comes to authentication problems.

IV. Known Issues

Wireless hardware and software testing is an ongoing process. For current known issues with various operating systems, clients, radios, along with details of the testing environment, please go to the Troubleshooting Web Pages and the Card Compatibility Web Pages located at: http://www.laptop.lib.utah.edu/.