Building "Secure" Wireless Networks

Summary

With the recent surge of wireless devices like smart phones, tablet computers, netbooks, and even laptops, networks are expanding to let these portable devices access the Internet via WiFi. There are a host of potential challenges and problems with this concept, and this article will try to address many of them with easy ways to solve them.

Applies To

SecureSchool, ISBossBox, LibraryDoor

More Information

Access Methods

There are a few different ways you can deploy WiFi networks:

- Encrypted and access restricted using WPA2 encryption
- Unencrypted, but access restricted using a WiFi "gateway" or "hot spot controller"
- Unencrypted and unrestricted

The method you choose is based on what your goals are. For example, if your goal is to allow any wireless device access to the Internet for a "community hotspot" type service, then you would probably want to use no encryption and no authentication since the goal is to make it easy for someone with an unconfigured device to gain access.

If you're trying to allow only trusted & known devices on the network, then you will probably want to use encrypted & restricted access by deploying WPA2 security. This method requires the administrator to configure the device with a WPA2 passphrase before it has access to the WiFi network. You generally want to keep your WPA2 passphrase "secret" to prevent unauthorized devices from getting on the network. The more people that know the passphrase, the harder it is to keep control of it. Most WiFi card drivers will give you the option to hide the passphrase, so the user cannot see it or retrieve it once it's been entered, making it even more secure.

If the goal is to allow anyone with an account to use any device, then using a WiFi gateway or hot spot controller is your best option. This (typically) does not require any configuration on the client side, but when the client first launches a browser, the controller will stop the

request for the site that was asked for and instead present the user with a page to login with, and then grant them access to the wired network.

Each method has it's own advantages and disadvantages. If you choose not to use an encryption method like WPA2, all WiFi traffic is unencrypted. This means that anyone that has a device (authorized or not) that can run a packet sniffer like Wireshark can easily watch traffic and grab usernames and passwords "out of the air", not to mention data like email messages and files that are being transferred.

If you choose to use a gateway or hot spot controller, these devices are not inexpensive and usually require certain brands of access points to be used, which can raise your cost even more. However, this adds accountability to network access since the users have to login before they are granted access to the "wired side" of the gateway.

If you go with a simple deployment requiring WPA2 on all devices without a gateway, then you must configure the WPA2 passphrase in every device manually, but you then know all the devices that are on your wireless network (unless someone steals the WPA2 passphrase from a Post-It note).

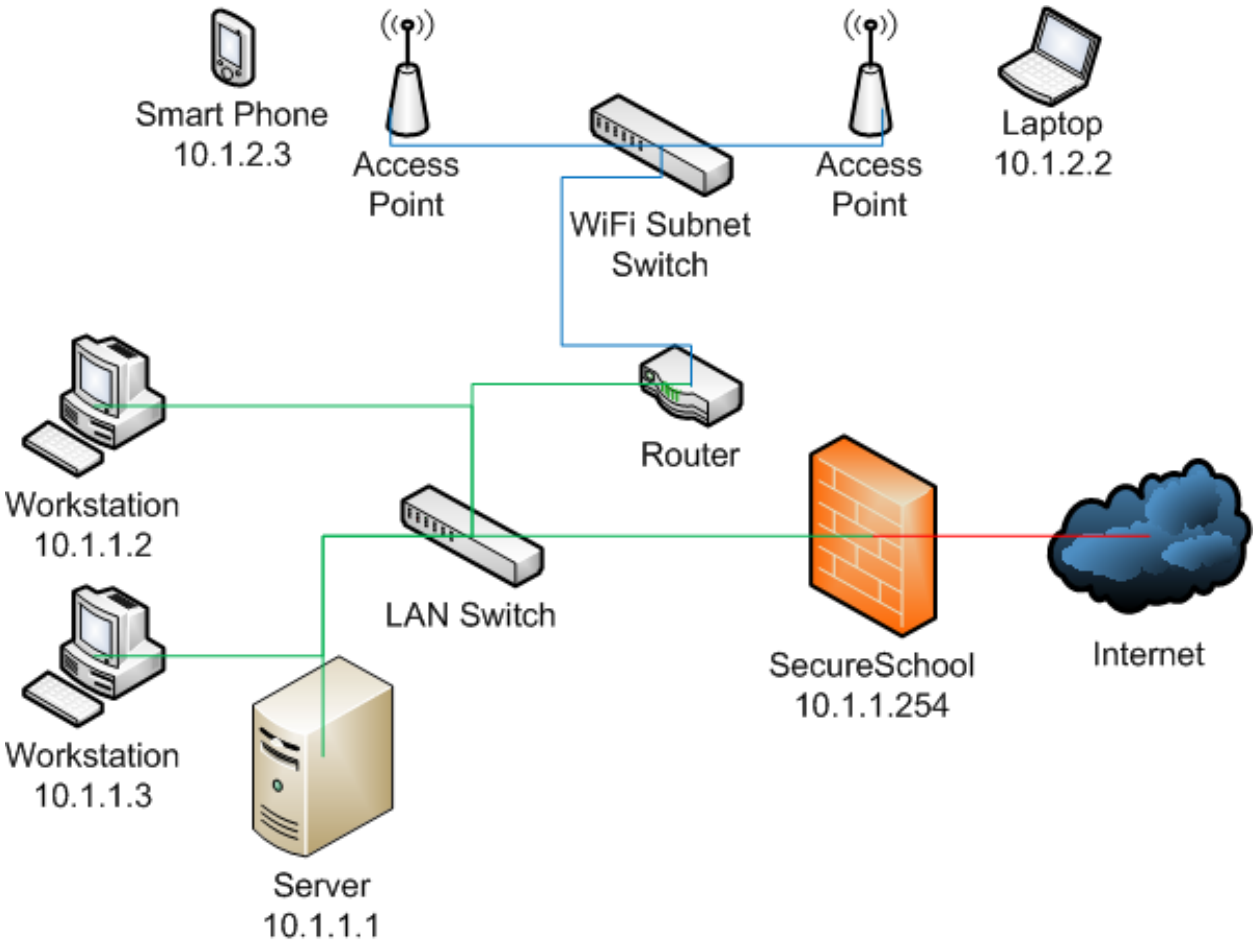
Other encryption methods like WEP and WPA have been cracked already and are flawed, and should not be used. Even some forms of WPA2 have weaknesses. The best encryption mechanism at the time this article was written is WPA2-AES. WPA2-TKIP has some weaknesses and has been exploited in lab environments.

Access Control

Where the WiFi devices have access to is something that must be considered early on in your design goals. If you're goal is to give any device access to your WiFi network, you're probably going to want to restrict WiFi devices to allow access only to the Internet (via SecureSchool). This is because not all WiFi devices may be trustworthy. Consider a student that brings in a laptop from home to the school WiFi network. While the student is at home, they can download and install tools to scan and hack Windows servers. When that laptop is now on the WiFi network at the school, that student can use those tools against your network. You want to limit (as much as possible) what places these devices have access to, while letting them do what has to be done. In most environments, the goal is to simply allow filtered access to the Internet.

To do this, the easiest and best way is to segment your WiFi network from your wired network using a simple two port router like a Cisco 861 router. Using the router, you would

create a new subnet off of your existing network:



In this example, your existing LAN is 10.1.1.0/24. You would add a new router, with one interface plugged into the 10.1.1.0/24 subnet, and it's other interface would be a new 10.1.2.0/24 subnet. This router would also have a DHCP relay agent configured on it, so you can still use your single DHCP server on 10.1.1.1, just add a new scope. The important thing this gives you is the ability to create Access Control Lists, or ACLs, on the router. You can create a rule at allows 10.1.2.0/24 to access only 10.1.1.254, and deny all other traffic from 10.1.2.0/24. Also, you can create a rule denying access from 10.1.1.0/24 to 10.1.2.0/24, except for 10.1.1.254. These simple rules will keep WiFi computers from accessing anything except SecureSchool, and prevent any wired computers from accessing any WiFi computers.

If you plan on using a WiFi gateway or hot spot controller, these devices are typically routers as well that can have rules in them. You would put these rules in that device and accomplish the same things.

This does not mean however that you cannot access any internal "services" if you are on the WiFi network. For example, if you have a web based library card catalog, you can still access it through SecureSchool since you're not connecting directly to the library server.

Internet Access

The final challenge to the puzzle is how to get these devices to access the Internet. Unfortunately this is the hardest part of the puzzle since you are not always in control of these devices and the software involved. For starters, the best way to deploy proxy settings to devices that will be going between two locations (like work and home) is to configure and use Proxy Auto Detect. The instructions for this are at http://kb.k12usa.com/Knowledgebase/Proxy-Auto-Detect .

Proxy Auto Detect covers all devices that support it. Many devices only partially support it, and some do not support it at all. For the iPad and other iOS devices, see http://kb.k12usa.com/Knowledgebase/Proxy-Setup-for-Apple-iPad for help. Android based devices do not support proxy settings at all yet.

Once you get proxy settings deployed (manually or automatically) to your client devices, you now have to decide how to authenticate them, if at all. If you use authentication on SecureSchool, then the client device should pop-up a login box and ask them for their name and password. If you do not want your users to have to login when on WiFi, or if the people using WiFi will not have accounts (like when you are using WiFi to provide community access), then you'll have to setup an IP Group to force the WiFi computers into a particular filter set. To create an IP Group:

- Go to "User Auth" -> "IP Groups" -> "Add An IP Group". Select a Filter Set you want to use to filter the WiFi users, enter a name for the group, and click "Submit"
- Go to "User Auth" -> "IP Groups" -> "Add a Workstation IP". Enter the range of addresses you will be using for WiFi users (in our example, 10.1.2.0/24), enter a comment, select the IP group you just made, and click "Submit"

Other Considerations

You need to consider security for any services that you plan on deploying or using on the WiFi network. For example, if you have a web browser based student information system or accounting system, you want to use HTTPS to access it, instead of HTTP. This way, any communications between the client and the server are encrypted and no other users on the WiFi network will be able to capture packets and steal user credentials or data.

Building "Secure" Wireless Networks

In addition to WPA2, there is an extension called WPA2-Enterprize. With WPA2-Enterprize, you can "login" to the encrypted WiFi network, and do not have to put a passphrase in every computer. WPA2-Enterprize is not supported on all WiFi network cards, and not all access points support WPA2-Enterprize. WPA2-Enterprize uses 802.1x for authentication, so you need to configure and use a Radius server to handle the logins.

"WiFi Routers" are not the same as "WiFi Access Points". An Access Point (or AP) has one ethernet port, and simply "bridges" the wired connection to the wireless connection. A "Router" typically has a WAN port and at least one LAN port, but usually 4 LAN ports in a switch. A router performs a lot more tasks then is needed on a corporate LAN. For example, it has it's own DHCP & DNS server and runs NAT. It is designed to be a home router / Internet gateway. They typically also lack some feature that APs have (for example, WPA2-Enterprize). You can use a WiFi router as an AP however, by making sure you do a few things to it first:

- Disable its DHCP server
- Disable its NAT and routing options
- Disable its firewall
- If the router has an option to keep WiFi traffic separate from wired traffic, disable that as well
- Configure it's private / LAN address with an IP that is local to your network
- Change it's default passwords
- Setup it's wireless settings to match your environment (SSID, encryption type, channels, etc)
- Connect your network to one of the 4 LAN switch ports. This should be the ONLY connection to the device

If you are trying to re-use existing technology you may have been collecting over the years to build one unified WiFi network, or are trying to cut costs by using non-enterprize grade devices, you may be interested in DD-WRT (http://www.dd-wrt.com/). DD-WRT is an alternative firmware that runs on many WiFi routers to add functionality and make them more attractive. Using this firmware usually voids the factory warranty, but may be worth it depending on your use case.

K12USA Support Knowledge Base
https://kb.k12usa.com/Knowledgebase/50068/Building-Secure-Wireless-Networks