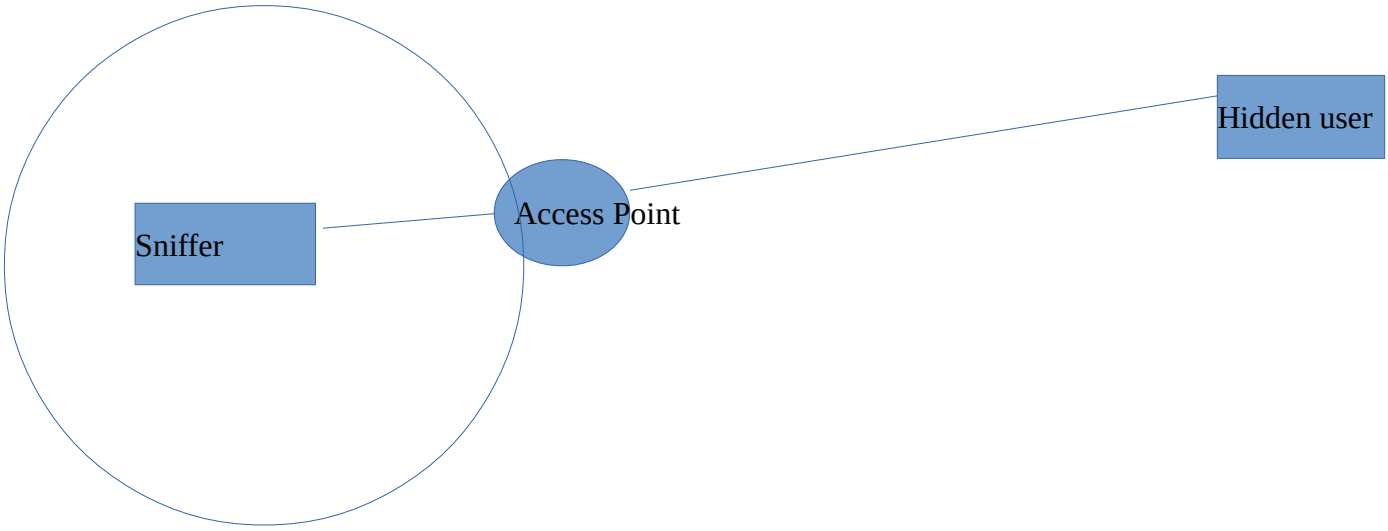
Hunter
Start Date: 9/12/2019

Objective:

The goal of this project is to produce a tool that will allow for the analysis of the dynamic nature of WiFi forests. On a campus or in an organization it is often difficult to define your perimeter, or even the nodes on your network. The very nature of the network is dynamic and in a constant state of change. The tool will be broken into two distinct parts. The first being the hunter. Its role is to locate and tag all of the nodes in the network. This will be accomplished through the tagging and locating of the nodes to a geographical region. This is where the use of mobile applications will come in. A mobile device will be used to sniff out wireless packets and tag them to a geographical location. This data will then be stored and uploaded to a remote server for analysis. From this point the second portion of the program takes effect. This program can then be used to analyze the data and produce a baseline map of the environment. From this baseline, an analysis can be made of the nature of the network and requirements for locking down the network. This information is then be passed back to the system for local investigation. Through this dynamic analysis of the network a better security model can be constructed.

The first component of the application is the sniffer element. The mobile application will go into promiscuous mode, allowing for the collection of traffic conforming to the IEEE 802.11 protocol. Instead of only looking at traffic that is meant for the mobile device, the device collects all transmissions in the area. From using the 802.11 protocol the application can extract information from these transmissions. The application will also be testing a prototype algorithm that will allow for hidden, and out of sight nodes.



In the above image the sniffer does not have the range on its own to reach the hidden user. Through the exploitation of the IEEE 802.11 protocol, the algorithm will attempt to use the router and the users own device to bridge the gap. The algorithm will not require that the hidden user's device be connected to the router being used. In addition this algorithm can be reversed so the hidden user who is using a private network can be exploited to expose the existence of the hidden access point. It is hoped that this algorithm will be compatible for integration with an existing tool called Hydra. If these tools can be integrated then the effective range of the system would cover the entire inter-networked area. This would mean that on the GMU campus IT could monitor for problems on everyone's devices for the entire campus. (This is of course not an objective of the project, for practical reasons. Bandwidth

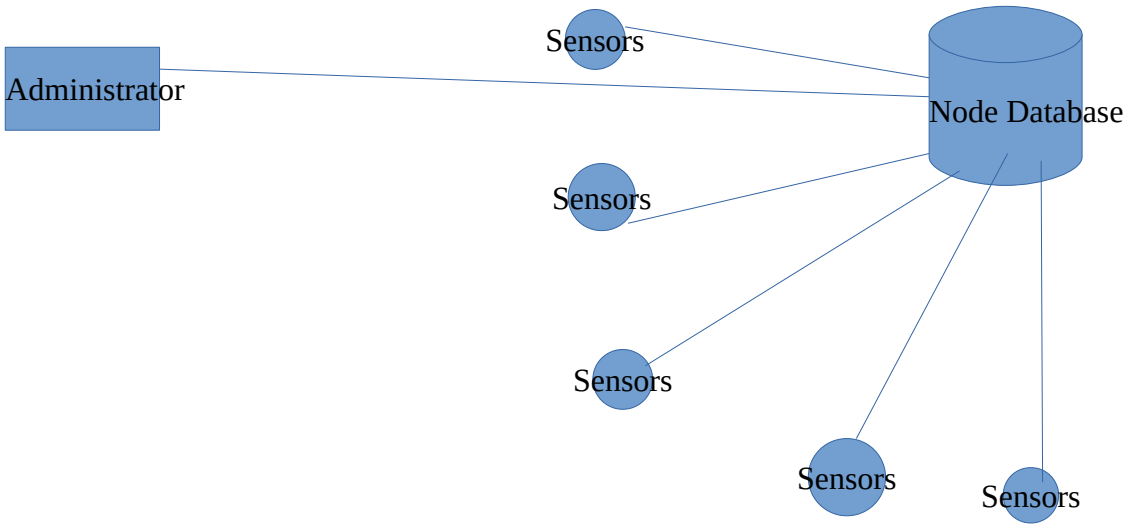
requirements, invasion of privacy, and Sub-netting). The primary goal of the first part of the application is the collection of information for the second part of the application.

Processing of this data is the next step of the application pipeline. This data is grouped into sort-able groups and processed. The information will be of the following structure:

{ MAC Address, GPS Location, {Were they went}, {Security Protocols}, {Security Violations}, {links to other contacts}}

The MAC address is the key that will be used to sort the devices by. This provides also a unique way of identifying users. The GPS location, will provide a type of home range for the device. This will also allow the user to identify known devices seen in the wild (ie. not on campus. Is this a device that a user brings from home? Does he/she only have it at work? Is the device a professors laptop, that never leaves the lab?) . While these questions on the surface do not seem to be important, the nature of the security that is needed to protect the devices differs with the way it is used. The next piece of information serves two purposes. The first is to notify the administrators of accesses to black listed locations (malware servers, pirate servers, inappropriate locations, and to link with the protocols used). The protocols is to identify nodes in the network that might need correction on security protocols. For example, going to a bank site and sending credentials un-encrypted. This information is then collected and added to the security violations, where it can be retrieved through a SQL search. This information is then processed and returned back to the mobile device as both a report, and tags.

This leads to the shared aspect of the project. Eventually the goal is to make this a distributed system. Deployable sensors can be logging nodes, and transmitting data to servers for analysis. This information can then be disseminated to company network administrators to take action. The quicker this loop in information can take place, the shorter the window for unauthorized access. There is also a plan for the integration of network security tools into the security package.



At this point the tags, can be used to track down the devices that need to be addressed. Through this process a better security model can be developed. The first element of security is to know what you have. In a dynamic network this is a challenge. Only when you know the environment being dealt with can you develop a plan to protect it. There is also an additional side effect of this project. If

people know what kind of information that they broadcast, they might take greater measures to secure the data. The primary goal of this system is to be able to detect and act on threats to the security of the network. The concept is to have a lightweight and mobile system, that can shift with the changing needs of the industry. In effect the searches on the database can be updated on the fly, to reflect the changing face of security. The reports and data flowing to the administrative staff can be changed at a server level allowing for quicker changes to the system. The real challenge of this system will be making tools developed for running on a laptop, and porting them down to an android device.

The goal is that a sensor or audit device will detect a violation of security policy, and forward it to the database. The database detects the violation and forwards it to the network administrator. The administrator quarantine the node, and takes action. This action is supported now by the sensors allowing the administrator to know the location of the offending device. This is where the name Janus comes from. Janus was the Greek god of portals and decisions. The program is to be a portal into the shifting nature of the wireless network, and make decisions to secure the network.

The testing of the final application will have two parts. The first will center around unauthorized users on the network. I am going to recruit a few people to play the part of unauthorized users. The goal of the system is to detect them and to locate them on campus. He next phase will be to define a set of websites, and actions as security violations. Then the goal will be to identify nodes on the network that are committing these violations. This will take the form of listing of a site like Amazon as a black listed server, and detecting nodes accessing the server.