Network Buddy-WLAN Monitoring on Android Phones

[1.] Anuradha S . Raut, [2.]Mayur S. Kakad, [3.]Prachi R. Mardhekar, [4.]Tanvi U. Kapadia
[1,2,3,4.] (Department of computer engineering, PVPIT, Pune)

***Abstract*— Many studies on measurement and characterization of wireless LANs (WLANs) have been performed recently. Most of these measurements have been conducted from the wired portion of the network based on wired monitoring (e.g. sniffer at some wired point) or SNMP statistics. More recently, wireless monitoring, the traffic measurement from a wireless vantage point, is also widely adopted in both wireless research and commercial WLAN management product development. Wireless monitoring technique can provide detailed PHY/MAC information on wireless medium. For the network diagnosis purpose (e.g. anomaly detection and security monitoring) such detailed wireless information is more useful than the information provided by SNMP or wired monitoring. In this paper we have explored various issues in implementing the wireless monitoring system for an IEEE 802.11 based wireless network. We identify the pitfalls that such system needs to be aware of, and then provide feasible solutions to avoid those pitfalls. We implement an actual wireless monitoring system and demonstrate its effectiveness by characterizing a typical computer science department WLAN traffic. Our characterization reveals rich information about the PHY/MAC layers of the IEEE 802.11 protocol such as the typical traffic mix of different frame types, their temporal characteristics and correlation with the user activities. Moreover, we identify various anomalies in protocol and security of the IEEE 802.11 MAC. Regarding the security, we identify malicious usages of WLAN, such as email worm and network scanning.**

***Keywords*— SNMP,AES Encryption, WLAN**

I. INTRODUCTION

A. Purpose

The main objective of this project is to provide maximum details about the computer in network to the administrator on their mobile phone, so that he can view and monitor all the machines in the network.

B. Project Scope

Today, the world is rapidly changing the statement “We are in the world” to “World is in our hands”. The main aim of our project is to control and monitor the LAN network from our wireless handheld device i.e. cell phone from anywhere irrespective of distance. Say, you have a LAN setup at your office. Sitting at home you want to learn the LAN status. You can do so by storing this project in your cell phone and executing the same. Extending the Wireless LAN (WLAN) to be a core technology will mean providing granular WLAN authorization and access control. In this guide, learn about Wireless LAN access control, as well as managing users on guest wireless networks and controlling Wi-Fi embedded devices on the WLAN. While WLANs were once used to offer network access to guests or employees in common areas, they are now often extended to reach every laptop and desktop in the enterprise. What's more, they also support both corporate and personal smart phones and tablets, as well as embedded Wi-Fi devices, such as copy machines and surveillance cameras. With all these users and clients, network managers must implement granular WLAN access control and network authorization.

C. Wireless LAN access control: Managing users

WLAN security using access control and encryption is much more solid than it was in years past, but WPA2-Enterprise is still no slam dunk. Using 802.1 x authentications requires integration of a number of components from multiple vendors. A successful WLAN access control plan will include the creation of user access policy that touches both corporate and personal devices. Once that policy is established a number of third-party tools can help with device fingerprinting and automated client provisioning for enforcement. In this expert tip on WLAN access control, learn about integrating wireless access control with other Network Access Control (NAC) tools, as well as information about device fingerprinting and automated provisioning.

D. Securing guest wireless networks

More on UK wireless LAN implementation Wireless LAN testing and troubleshooting guide .An indoor and outdoor WLAN revived the town of Black pool UK wireless technology trends: Tablets take hold in the enterprise Virtual WLANs enable schools to share learning materials Old methods of securing guest wireless networks are no longer sufficient. Once upon a time, wireless guest networks were given their own service set identifiers (SSIDs) and mapped onto an isolated Ethernet VLAN. HTTP requests from newly connected clients were sometimes redirected to a captive portal, where guests had to accept "terms of service" before being released onto the Internet. This left the door open for infected devices to access the guest SSID and the VLAN. It also left that captive portal open for attack. As a result, enterprises must consider other methods for securing these networks. A number of companies sell equipment that comes with built-in guest management. This equipment requires users to sign in and create accounts, and allows enterprises to create walled-gardens of access depending on their own user policy. These tools also allow enterprises to control how guests sign in. Captive portals can require guests to run anti-virus programs, and they allow the IT team to configure permitted destinations, ports and URLs tied to bandwidth limits and priorities. Companies can also integrate a NAC or IDS product to do checks on wireless guest networks.

E. Managing embedded Wi-Fi devices on the WLAN

As if managing guest devices weren't enough of a headache, increasingly network managers find themselves managing and securing Wi-Fi embedded devices on the WLAN. These devices range from wireless printers to barcode scanners and point-of-sale terminals. One way of controlling these devices is through WPA2-Personal: Pre-Shared Key (PSK) authentication and AES encryption. “Personal" suggests that this is not a strategy designed for enterprise wireless LANs, and PSKs are not preferred for devices that can be controlled effectively with WPA2-Enterprise. However, for consumer electronics that do not support WPA2-Enterprise or device certificates, PSKs can be a viable alternative. Enterprises could also opt to acquire devices that come ready with Wi-Fi Direct, a peer-to-peer Wi-Fi Alliance specification that enables devices to speak directly to each other. Wi-Fi Direct-capable devices discover each other and form Wi-Fi Direct "groups" composed of two or more devices that make management and visibility simpler.

II. ENCRYPTION AND DECRYPTION ALGORITHM

Encryption is a process of coding information which could either be a file or mail message in into cipher text a form unreadable without a decoding key in order to prevent anyone except the intended recipient from reading that data. Decryption is the reverse process of converting encoded data to its original un-encoded form, plaintext. A key in cryptography is a long sequence of bits used by encryption / decryption algorithms.

There are two primary approaches to encryption: symmetric and public-key. Symmetric encryption is the most common type of encryption and uses the same key for encoding and decoding data. This key is known as a session key. Public-key encryption uses two different keys, a public key and a private key. One key encodes the message and the other decodes it. The public key is widely distributed while the private key is secret. There are a number of algorithms for performing encryption and decryption, but comparatively few such algorithms have stood the test of time. The most successful algorithms use a key. A key is simply a parameter to the algorithm that allows the encryption and decryption process to occur. There are many modern key-based cryptographic techniques. These are divided into two classes: symmetric and asymmetric (also called public/private) key cryptography. In symmetric key cryptography, the same key is used for both encryption and decryption. In asymmetric key cryptography, one key is used for encryption and another, mathematically related key, is used for decryption.

III. PRODUCT PERSPECTIVE

In a concern, computers are grouped together to form a network. To manage and control the activities of the network while in office is an easy task. But, while you are outstation / away from office, how do you go about with monitoring and controlling of network? Instead of depending on third party information, you can always have your cell phone serve the purpose. Just load the project in your cell phone, login anytime to the application and see who is busy with what in the office.

IV. PRODUCT FEATURES

- User doesn’t have to sit in lab for controlling and monitoring LAN.
- User should be able to control LAN using cell phone.
- Can control multiple PC’s by phone. Don’t have to monitor individual PC’s.

A. Features controlled from cell phone

- Net View: It will show list of Computer in network.
- Process List: It will display list of processes in computer.
- Activate Process: It will run new process on client machine
- Kill Process: It will kill process on particular client machine.
- Shutdown: It will shutdown the client machine.
- Image Capture : It will take the screen shot of the Desktop on phone
- Send Message: We can send message to the machine selected.
- View Screenshot – View Remote Computer Screenshot
- Detect Removable drives – detect external devices connected to client computers

Consider a LAN setup with the server machine connected to Android phone. The interaction between the clients and the wireless media happens through this server.

V. ARCHITECTURE

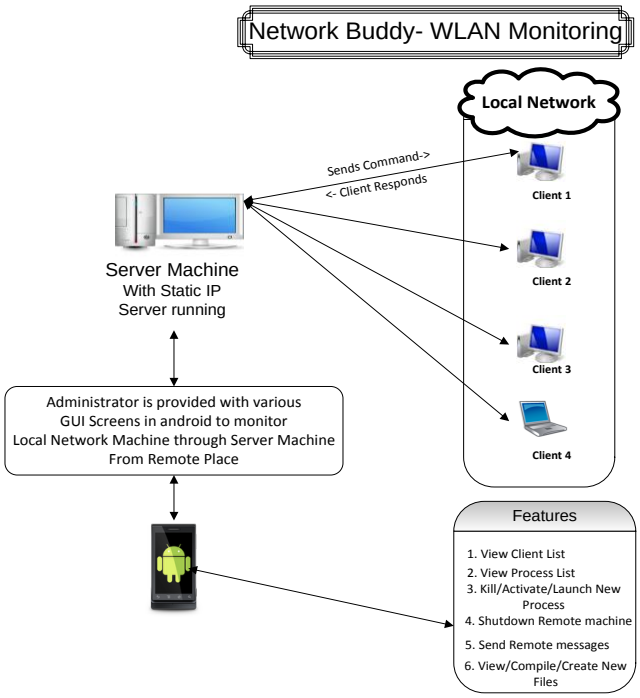

Fig 1. Architecture

VI. RESULTS

Thus using this project we are trying to provide maximum details about the computer in network to the administrator on their mobile phone, so that he can view and monitor all the machines in the network.

In a concern, computers are grouped together to form a network. To manage and control the activities of the network while in office is an easy task. But, while you are outstation / away from office, how do you go about with monitoring and controlling of network? Instead of depending on third party information, you can always have your cell phone serve the purpose. Just load the project in your cell phone, login anytime to the application and see who is busy with what in the office.

REFERENCES

[1] M. Raya, J-P. Hubaux and I. Aad. DOMINO "*A System to Detect Greedy Behavior*" in IEEE 802.11 Hotspots. In Proceedings of the 2nd international conference on Mobile systems, applications, and services, Boston, MA, June 2004.

[2] IEEE Computer Society LAN MAN Standards Committee. "*Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specications*". In IEEE Std 802.11-1999, 1999.

[3] IEEE Computer Society LAN MAN Standards Committee. IEEE 802.11 Management Information Base In IEEE Std 802.11-1999, 1999.

[4] THE IMAP Connection." *http://www.imap.org/*"

[5] D. Kotz and K. Essien. "*Analysis of a Campus-wide Wireless Network*". In Proc. the Eighth Annual International Conference on Mobile Computing and Networking (MOBICOM 2002), Atlanta, GA, September 2002.

[6] P. Kyasanur and N. Vaidya. "*Selsh MAC Layer Misbehavior in Wireless Networks*". In IEEE Transactions on Mobile Computing, April, 2004.