VEL TECH®
Dr.RR & Dr.SR
TECHNICAL UNIVERSITY
VEL TECH RANGARAJAN Dr.SAGUNTHALA R&D INSTITUTE OF SCIENCE AND TECHNOLOGY
University u/s 3 of UGC Act, 1956
#42, Avadi-Vel Tech Road, Avadi, Chennai - 600 062, Tamil Nadu, INDIA.

OCTOBER 2014, ISSUE 1

Inside this issue:

CETA — NEWS LETTER

Department of Computer Science and Engineering

CETA – NEWS LETTER

(Computer Engineers Technical Association)

IEEE STUDENT CHAPTER

IEEE STUDENT CHAPTER (COMPUTER SOCIETY) INAGURATION

Vel Tech Dr.RR&Dr.SR Technical University take pride in informing that we have our own IEEE student chapter which was inagurated by Dr.N.R.Alamelu , chair madras section , principal sri Ramakrishna engg college 19th, September 2014 .

To start off the function we began with a prayer song and then followed lighting of kuthuvilaku by the chief guest, vice chancellor , registrar , IEEE student chair and by the student members of IEEE.

We then had the release of the approval letter which was approved by the IEEE head office. Which included details about the student chapter of veltech university. It also mentioned about the managing people of the IEEE student chapter namely:

Student Councellor : Dr.S.koteeswaran

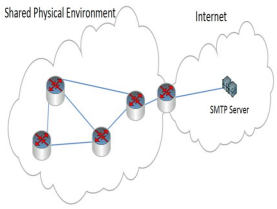
Student Chair : Sushmitha H

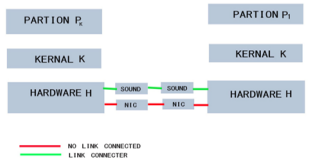
Then we had inaugural address by Our honourable Vice Chancellor Prof.Dr.Beela Satyanarayana , followed by a special address by our beloved registrar Dr.E.Kannan which briefed us what ieee is, then we had a special address by our respected proctor Mr.E.Kamalanaban where he listed out the privilege of being a IEEE member.

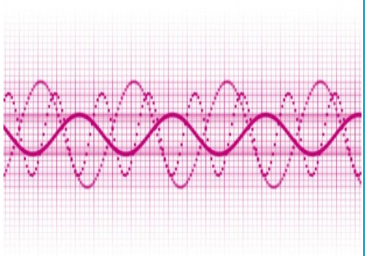
We then had a special address by our Chief Guest Dr.N.R.Alamelu , she being the chair of the madras section elaborated us about the offers and benefits that IEEE provides. She also discussed about the funds provided by IEEE for the current research projects. She made us clear about the privilege we get by being a member of IEEE.

Finally the inaugural festival was concluded by IEEE Student Chair, thanking the university management for starting up an IEEE student chapter in VELTECH UNIVERSITY and also thanking our chief guest Dr.N.R.Alamelu .

AIR-GAP MALWARE







AIR-GAP MALWARE is a malicious software program which infects computers without any internet connection by converting malicious code into high frequency sound waves
When a network admin finds that a system is trying to exploit a malicious code, the network connection for that particular system will be disconnected by the network admin to prevent rest of the device from the attack. So, that the malicious code has no path to be transferred. This process is called "roadblock". This technique can be cracked by "AIR-GAP MALWARE"

We can break a new ground, if we want to exploit a rigorously hardened and tested type of computing system. In operating system, channels are usually established by exploiting shared resource access between different processes. The communication shares both computing resource and pre-existing network interface. One can imagine a different computing system, where a new network interface based on a physical emanation is established completely. Communication can be done through radio, optical and sound waves.

Scenario:

The basic scenario for the air-gap malware is Two computers are neither connected to IEEE 802.3 ETHERNET nor IEEE 802.11 WLAN. They are prohibited to communicate with each other through a network interface. Nevertheless they are able to communicate with each other by using their audio input and audio output devices like microphones and speakers.

We assume a high-assurance setup where an operating system that consist of a small trusted computing base and individual service components . KERNAL always governs the reference monitor of an component-based operating system, which is an access control monitor that has always to be invoked in inter-partition communication (IPC) decisions.

Acoustical communication between p_1 and p_K is possible as long as audio input and audio output are under the hardware H accessible to both p_1 and p_k. Now the malicious code is generated and the code is converted into a high frequency sound waves. The converted malicious code is passed through ultrasonic waves from one device to other devices using Speakers and Microphones. Speaker in the system emits the converted malicious code and the microphone in the other device receives it and the virus is injected to that device.

In a covert acoustical mesh network, more than twocomputing systems in a shared physical environment (i.e. within the physical communication range between two connected nodes) can be connected to the mesh network and computing systems are able to communicate indirectly by following routing paths over multiple hops.

In our article, we describe how the complete concept of air gaps can be considered obsolete as commonly available laptops can communicate over their internal speakers and microphones and even form a covert acoustical mesh network. Over this covert network, information can travel over multiple hops of infected nodes, connecting completely isolated computing systems and networks (e.g. the internet) to each other.

This small bandwidth might actually be enough to transfer critical information (such as keystrokes). You don't even have to think about all keystrokes. If you have a keylogger that is able to recognize authentication materials, it may only occasionally forward these detected passwords over the network, leading to a very stealthy state of the network. And you could forward any small-sized information such as private encryption keys or maybe malicious commands to an infected piece of construction.

Harish.A (final yr CSE-A)

Kanmani.S (final yr CSE-A)

Dr.P.Visu (HOD-CSE)

STREAMING CLOUD

"'Streaming cloud'" computing is from multimedia aware-cloud. A multimedia aware-cloud which address how a multimedia cloud can perform distributed multimedia process and storage of the multimedia process and provide quality of service. To provide a High Quality of service for multimedia services we propose an architecture called media -edge colud (MEC) and in which storage, the central processing unit (CPU) and graphics processing unit (GPU) cluster are presented at the edge to provide distributed parallel processing and quality of service (QoS) adaptation for various types of devices.

Now we present a cloud -aware multimedia that how multimedia services and application such as storage, shaing,authoring,mash up and delivery, rendering and retrieval, can optimally utilize cloud computing resource for the better quality of services (QoS).

Cloud computing is an emerging technology providing various storage and computing services over the internet. Cloud computing is a platform and generally an incorporates infrastructure and software as service(SaaS). By using cloud computing users can store and retrieve their data, software, media and many in cloud using over the internet instead of storing their data in the local drives. The users can run their application more efficiently on cloud computing platform with software deployed in the cloud.

Media Cloud Computing Architecture:

We Handling multimedia computing form a quality of service(QoS) perspective of an MEC computing architecture. In cloud the server physically placed at the edge to provide media service with high quality of service to users. The MEC architecture is similar CDN Edge server architecture where CDN is for multimedia delivery and MEC for multimedia computing to the users. So that compare to all multimedia content in the centre of the server the multimedia computing is an MEC can produce less traffic.

There are two type of Architecture in MEC:

* 1st type: The all user data are stored in the MECs based on the user profile and content is location is communicated by its head through P2P.

* 2nd type: The central Administrator maintains all the associated users details and the content location where the MEC distributedly holds all the content within the MEC.

In P2P architecture each nodes a very important where the MEC has the high scalability and availability for media computing and media storage.

Cloud-aware applications :

In high professional organization the high quality media contents could only be acquired with efficient devices. The other distribution of media are used in hard copies like various compact disc. A low cost digital camera and camcorders has sparked an explosion of users generated media content. At new cyber physical systems made a new way of data Acquisting over sensor networks which increase the diversity and the volume of media data files. On the web 2.0 wave digital media data can be easly distributed through the internet connection. A biggest success for the youtube , gmail and other cloud storage services for demonstrates the popularity of the internet media. In early days the media storage are provided by the various service provider with there server farms ,but now every service provider have a choice to be user of public clouds. For small bussiness the pay as you go is the choice of the public cloud users.

A.Aravind (final yr CSE-A)

A.Hariprasath(final yr CSE-A)

S.B.Sibi Chakkaravarthy
(Asst.Prof-CSE)

WIRELESS DEAUTHENTICATION ATTACK

Wireless Deauthentication attacks are highly malicious which can be performed easily. This type of attack can target either in a specific station or multiple stations and prevent them from connecting to the wireless network. Attacker uses the access point of the client to disconnect the client's network. Attacker needs fair signal strength to launch the attack. The deauthentication frames are classified as management frames in the 802.11 specification, and are used to disconnect stations and access points. These attacks create a nuisance value; they can pose a security threat to a wireless network in the production environment.

CONCEPT OF DEAUTHENTICATION ATTACK:

- The connection between clients and access points is established by exchanging various frames.
- The communication between the client and the access point is established after probing the available wireless access points after that the exchange of a series of management frames, like authentication and association request frames, takes place. This attack is made at the Data-link layer which is associated with the MAC address.

BEHIND WIRELESS DEAUTHENTICATION ATTACKING:

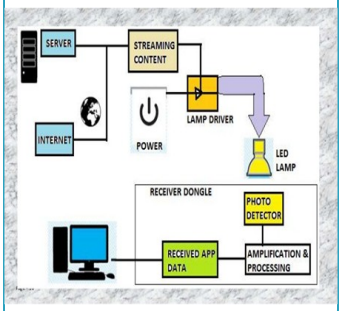
When a client uses a wireless network, their network can be attacked using the access point of their network. A wireless deauthentication attack is carried out by using the victims SSID (service set identification), AP (access point), BSSID: MAC address of the AP. Firstly, the attacker identifies the name of the wireless card. After the name is found, the attacker sets the wireless card on monitor mode. Then the attacker scans the clients monitor and identifies all its access points which are connected to the wlan. The important data like the MAC address, channel number and ESSID (Extended service set identification) of the AP is found. From the identified information the attacker will choose any one as his victim and mount the attack.

The first comes from the victim's machine which contains the Deauthentication Flag. The second Deauthentication Flag frame is sent from the AP to the victim.

DETECTING DEAUTHENTICATION ATTACKS:

The Deauthentication frame will terminate communication between the two stations. Restarting the AP more than three times after the manual disconnection, the device will show the deauthenticated packets. If there are many deauthenticated packets, it's a sign that someone is attacking the device.

LI-FI (LIGHT FIDELITY)-THE FUTURE TECHNOLOGY IN WIRELESS COMMUNICATION



Most of us are familiar with Wi-Fi (Wireless Fidelity), which uses 2.4-5GHz RF to deliver wireless Internet access around our homes, schools, offices and in public places. We have become quite dependent upon this nearly ubiquitous service. But like most technologies, it has its limitations. While Wi-Fi can cover an entire house, its bandwidth is typically limited to 50-100 megabits per second (Mbps). This is a good match to the speed of most current Internet services, but insufficient for moving large data files like HDTV movies, music libraries and video games. The more we become dependent upon 'the cloud' or our own 'media servers' to store all of our files, including movies, music, pictures and games, the more we will want bandwidth and speed. Therefore RF-based technologies such as today's Wi-Fi are not the optimal way. In addition, Wi-Fi may not be the most efficient way to provide new desired capabilities such as precision indoor positioning and gesture recognition. Optical wireless technologies sometimes called visible light communication (VLC) and more recently referred to as Li-Fi (Light Fidelity) on the other hand, offer an entirely new paradigm in wireless technologies in terms of communication speed, flexibility and usability.

HOW LI-FI WORKS?

Imagine ourselves walking into a complex where GPS signals are unavailable but the complex is equipped with ceiling bulbs that create their own 'constellation' of navigation beacons. As the camera of our cell phone automatically receives these signals, it switches our navigation software to use this information to guide us to the ATM machine we're looking for. We conclude our ATM transaction and notice the Giga Spot sign for instant digital movie downloads. We pick out that new data using our phone's payment facility and then download within a few seconds the high-definition movie intothe Giga Link flash drive plugged into the USB port of our Smartphone. As we walk away, our phone notifies us that the leather jacket featured in the character of movie is on sale nearby. We walk over towards the show window and our image comes up on the screen, wearing that coveted jacket. You turn and pose while the image matches our orientation and body gestures for a 'digital fitting.' When we walk into the store, the clerk handover us the actual jacket in exactly size fitting.

Within a local Li-Fi cloud several data based services are supported through a heterogeneous communication system. In an initial approach, the Li-Fi Consortium defined different types of technologies to provide secure, reliable and ultra-high-speed wireless communication interfaces. These technologies included giga-speed technologies, optical mobility technologies and navigation, precision location and gesture recognition technologies. For giga-speed technologies, the Li-Fi Consortium defined Giga Dock, Giga Beam, Giga Shower, Giga Spot and Giga MIMO models to address different user scenarios for wireless indoor and indoor -like data transfers. While Giga Dock is a wireless docking solution including wireless charging for smart phones tablets or notebooks, with speeds up to 10 Gbps, the Giga Beam model is a point-to-point data link for kiosk applications or portable-to-portable data exchanges. Thus a two-hour full HDTV movie (5 GB) can be transferred from one device to another within four seconds.

COMPARISION BETWEEN Li-Fi & Wi-Fi

LI-FI is a term, one used to describe visible light communication technology applied to high speed wireless communication. It acquired this name due to the similarity to WI-FI, only using light instead of radio. WI-FI is great for general wireless coverage within buildings and li-fi is ideal for high density wireless data coverage in confined area and for relieving radio interference issues, so the two technologies can be considered complimentary.

CONCLUSION

The possibilities are numerous and can be explored further. If this technology can be put into practical use, every bulb can be used something like a Wi-Fi hotspot to transmit wireless data and we will proceed toward the cleaner, greener, safer and brighter future.

Sushmitha.H (Final year CSE-B)

Suseendran.V (Final year CSE-B)

Parandhaman (final year CSE-B)

Vel Tech Dr.RR & Dr.SR Technical University

42, Avadi - Vel Tech Road,
Avadi,
Chennai
Pin : 600 062.
Phone: 044 - 26840262
E-mail: pvisu@veltechuniv.edu.in

Www.veltechuni.edu.in
Www.vel-tech.org

Computer Labs