ANNAPOORANA COMPUTER SCIENCE INCUBATION CENTRE (ACSIC)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Department of Computer Science and Engineering, AEC started an incubation centre as **Annapoorana Computer Science Incubation Centre (ACSIC)** in association with Avatar Academy on **05.06.2018** with the heavenly blessings of Dr.S.Shanmugasundaram our founder chairman . The centre was inaugurated by Mrs. Annapoorani Shanmugasundaram, Madam Founder Chairman in the presence of Mr. N. V. Chandrasekar Vice-President, Vinayaka Missions University, Dr.A.Anbuchezian, Principal, Dr.S.Sharavanan, Vice Principal and Dr.O.Saravanan, Dean-First year. ACSIC aims to excel in the field of networking and network Associate routing,switching types and other CSE Engineering works. WAN,network security,network media,TCP/IP,OSI models are carried out. The objective of the center for excellence is to provide best world class practices and to facilitate in research, exchange ideas, solutions to practical problems. The department of Computer Science and Engineering has signed MoU with many companies to enhance industry institute interaction such as internships, Field visits, Guest lectures, Seminars, workshops, placement are provided to students. Practical training is given for faculty members. Students are being exposed to have practical knowledge in the Computer Science and Engineering field through this centre

AEC Rd
ANK
Google
Kombadipatti, Tamil Nadu, India
Annapoorana Engineering College, Periya Seeragapadi, Tamil Nadu, Kombadipatti, Tamil Nadu 636308, India
Lat N 11° 34' 49.3374"
Long E 78° 2' 50.38872"
27/01/21 11:22 AM

Report on Hands-on Training Program on "Networking and Security " by Mr.P.K Amarnath, Operation Head ,Avatar Academy ,Erode on 07.06.2018 and 08.06.2018

Network security

Network security is a broad term that covers a multitude of technologies, devices and processes. In its simplest term, it is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies. Every organization, regardless of size, industry or infrastructure, requires a degree of network security solutions in place to protect it from the ever-growing landscape of cyber threats in the wild today.

Today's network architecture is complex and is faced with a threat environment that is always changing and attackers that are always trying to find and exploit vulnerabilities. These vulnerabilities can exist in a broad number of areas, including devices, data, applications, users and locations. For this reason, there are many network security management tools and applications in use today that address individual threats and exploits and also regulatory non-compliance. When just a few minutes of downtime can cause widespread disruption and massive damage to an organization's bottom line and reputation, it is essential that these protection measures are in place.

How does network security work?

There are many layers to consider when addressing network security across an organization. Attacks can happen at any layer in the network security layers model, so your network security hardware, software and policies must be designed to address each area.

Network security typically consists of three different controls: physical, technical and administrative. Here is a brief description of the different types of network security and how each control works.

Physical Network Security

Physical security controls are designed to prevent unauthorized personnel from gaining physical access to network components such as routers, cabling cupboards and so on. Controlled access, such as locks, biometric authentication and other devices, is essential in any organization.

Technical Network Security

Technical security controls protect data that is stored on the network or which is in transit across, into or out of the network. Protection is twofold; it needs to protect data and systems from unauthorized personnel, and it also needs to protect against malicious activities from employees.

Administrative Network Security

Administrative security controls consist of security policies and processes that control user behavior, including how users are authenticated, their level of access and also how IT staff members implement changes to the infrastructure.

Types of network security

Network Access Control

To ensure that potential attackers cannot infiltrate your network, comprehensive access control policies need to be in place for both users and devices. Network access control (NAC) can be set at the most granular level. For example, you could grant administrators full access to the network but deny access to specific confidential folders or prevent their personal devices from joining the network.

Antivirus and Antimalware Software

Antivirus and antimalware software protect an organization from a range of malicious software, including viruses, ransomware, worms and trojans. The best software not only scans files upon entry to the network but continuously scans and tracks files.

Firewall Protection

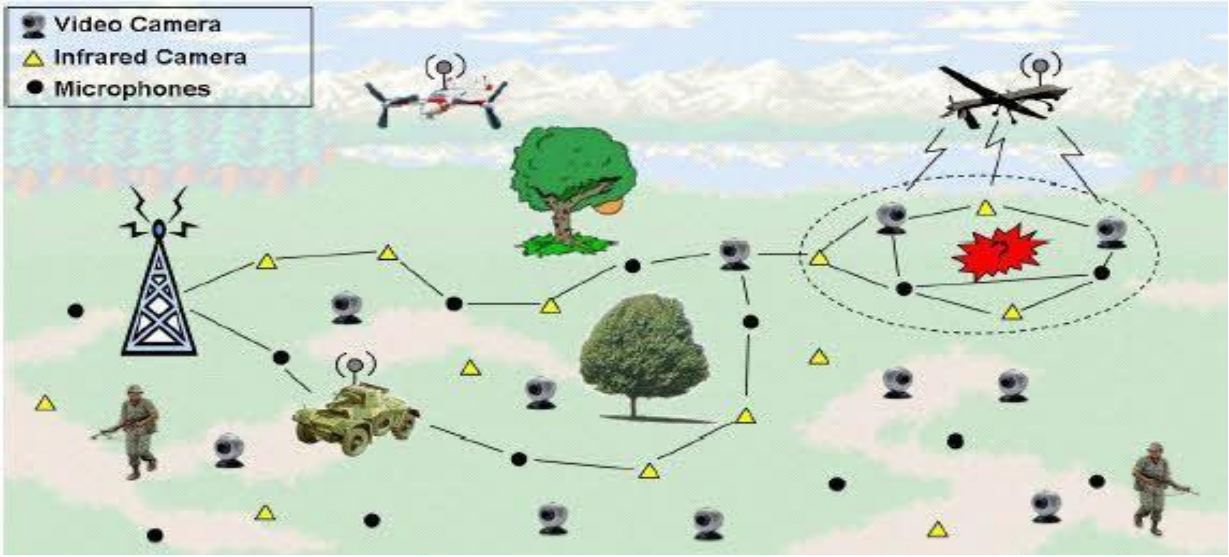
Firewalls, as their name suggests, act as a barrier between the untrusted external networks and your trusted internal network. Administrators typically configure a set of defined rules that blocks or permits traffic onto the network. For example, Forcepoint's Next Generation Firewall (NGFW) offers seamless and centrally managed control of network traffic, whether it is physical, virtual or in the cloud.

Virtual Private Networks

Virtual private networks (VPNs) create a connection to the network from another endpoint or site. For example, users working from home would typically connect to the organization's network over a VPN. Data between the two points is encrypted and the user would need to authenticate to allow communication between their device and the network. Forcepoint's Secure Enterprise SD-WAN allows organizations to quickly create VPNs using drag-and-drop and to protect all locations with our Next Generation Firewall solution.

Network security for businesses and consumers

Network security should be a high priority for any organization that works with networked data and systems. In addition to protecting assets and the integrity of data from external exploits, network security can also manage network traffic more efficiently, enhance network performance and ensure secure data sharing between employees and data sources.



Report on Hands-on Training Program on "Cyber Security " by Mr.P.K Amarnath, Operation Head ,Avatar Academy ,Erode on 18.07.2019 and 19.07.2019

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

Application security focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

Information security protects the integrity and privacy of data, both in storage and in transit.

Operational security includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.

End-user education addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

The scale of the cyber threat

The global cyber threat continues to evolve at a rapid pace, with a rising number of data breaches each year. A report by RiskBased Security revealed that a shocking 7.9 billion records have been exposed by data breaches in the first nine months of 2019 alone. This figure is more than double (112%) the number of records exposed in the same period in 2018.

Medical services, retailers and public entities experienced the most breaches, with malicious criminals responsible for most incidents. Some of these sectors are more appealing to cybercriminals because they collect financial and medical data, but all businesses that use networks can be targeted for customer data, corporate espionage, or customer attacks.

With the scale of the cyber threat set to continue to rise, the International Data Corporation predicts that worldwide spending on cyber-security solutions will reach a massive $133.7 billion by 2022. Governments across the globe have responded to the rising cyber threat with guidance to help organizations implement effective cyber-security practices.

In the U.S., the National Institute of Standards and Technology (NIST) has created a cyber-security framework. To combat the proliferation of malicious code and aid in early detection, the framework recommends continuous, real-time monitoring of all electronic resources.

The importance of system monitoring is echoed in the "10 steps to cyber security", guidance provided by the U.K. government's National Cyber Security Centre. In Australia, The Australian Cyber Security Centre (ACSC) regularly publishes guidance on how organizations can counter the latest cyber-security threats.

Types of cyber threats

The threats countered by cyber-security are three-fold:

1. **Cybercrime** includes single actors or groups targeting systems for financial gain or to cause disruption.
2. **Cyber-attack** often involves politically motivated information gathering.
3. **Cyberterrorism** is intended to undermine electronic systems to cause panic or fear.

So, how do malicious actors gain control of computer systems? Here are some common methods used to threaten cyber-security:

Malware

Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer. Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.

There are a number of different types of malware, including:

Virus: A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.

Trojans: A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.

Spyware: A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.

Ransomware: Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.

Adware: Advertising software which can be used to spread malware.

Botnets: Networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.

SQL injection

An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a databased via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

Phishing

Phishing is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information.

Man-in-the-middle attack

A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecure WiFi network, an attacker could intercept data being passed from the victim's device and the network.

Denial-of-service attack

A denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.

Latest cyber threats

What are the latest cyber threats that individuals and organizations need to guard against? Here are some of the most recent cyber threats that the U.K., U.S., and Australian governments have reported on.

Dridex malware

In December 2019, the U.S. Department of Justice (DoJ) charged the leader of an organized cyber-criminal group for their part in a global Dridex malware attack. This malicious campaign affected the public, government, infrastructure and business worldwide.

Dridex is a financial trojan with a range of capabilities. Affecting victims since 2014, it infects computers though phishing emails or existing malware. Capable of stealing passwords, banking details and personal data which can be used in fraudulent transactions, it has caused massive financial losses amounting to hundreds of millions.

In response to the Dridex attacks, the U.K.'s National Cyber Security Centre advises the public to "ensure devices are patched, anti-virus is turned on and up to date and files are backed up".

Romance scams

In February 2020, the FBI warned U.S. citizens to be aware of confidence fraud that cybercriminals commit using dating sites, chat rooms and apps. Perpetrators take advantage of people seeking new partners, duping victims into giving away personal data.

The FBI reports that romance cyber threats affected 114 victims in New Mexico in 2019, with financial losses amounting to $1.6 million.

Emotet malware

In late 2019, The Australian Cyber Security Centre warned national organizations about a widespread global cyber threat from Emotet malware.

Emotet is a sophisticated trojan that can steal data and also load other malware. Emotet thrives on unsophisticated password: a reminder of the importance of creating a secure password to guard against cyber threats.

End-user protection

End-user protection or endpoint security is a crucial aspect of cyber security. After all, it is often an individual (the end-user) who accidentally uploads malware or another form of cyber threat to their desktop, laptop or mobile device.

So, how do cyber-security measures protect end users and systems? First, cyber-security relies on cryptographic protocols to encrypt emails, files, and other critical data. This not only protects information in transit, but also guards against loss or theft.

In addition, end-user security software scans computers for pieces of malicious code, quarantines this code, and then removes it from the machine. Security programs can even detect and remove malicious code hidden in Master Boot Record (MBR) and are designed to encrypt or wipe data from computer’s hard drive.

Electronic security protocols also focus on real-time malware detection. Many use heuristic and behavioral analysis to monitor the behavior of a program and its code to defend against viruses or Trojans that change their shape with each execution (polymorphic and metamorphic malware). Security programs can confine potentially malicious programs to a virtual bubble separate from a user's network to analyze their behavior and learn how to better detect new infections.

Security programs continue to evolve new defenses as cyber-security professionals identify new threats and new ways to combat them. To make the most of end-user security software, employees need to be educated about how to use it. Crucially, keeping it running and updating it frequently ensures that it can protect users against the latest cyber threats.

Cyber safety tips - protect yourself against cyber attacks.

ANNAPOORANA ENGINEERING COLLEGE

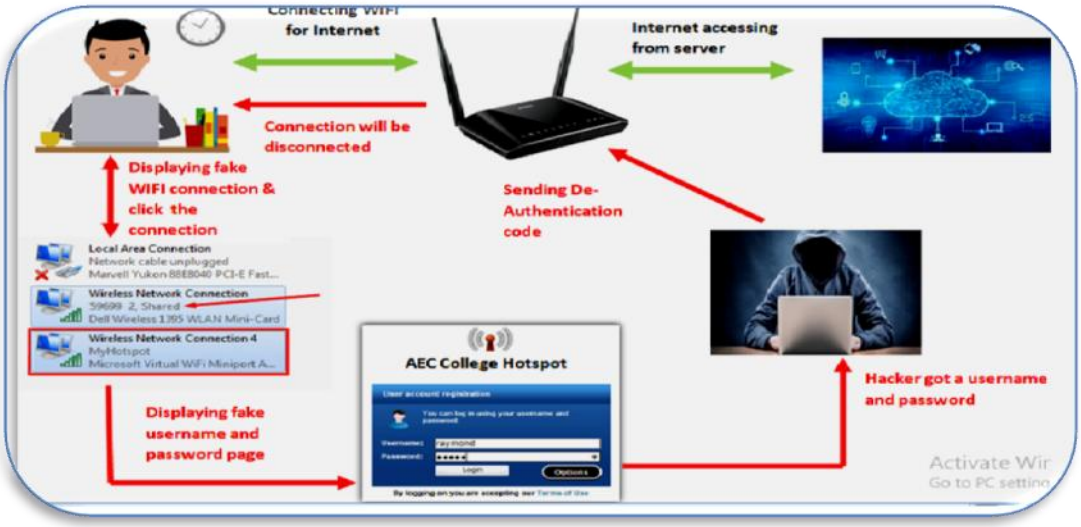
(Approved by AICTE-New Delhi, Affiliated to Anna University, Chennai)
NH-47 Sankari Main Road, Periyaseeragapadi, Salem-636308, Tamil Nadu.
ISO 9001:2015 Certified Institution
www.aecsalem.edu.in

INCUBATION CENTER PROJECT DESCRIPTION REPORT

IMPROVEMENT OFAUTHENTICATIONTECHNIQUES AND IMPLICATIONS OF COEVAL METHOD (1)

ABSTRACT

Login id creation is a mandatory process in today's internet era. Many levels of security measures have been taken to protect the user data both at the server and client side. (Eg: two-step verification, OTP verification, etc.,) but Twin Evil Attack (TEA) is common in nowadays due to exact matching of duplicate creation of popular sites (Eg: Google, face book, yahoo, Amazon).To reduce the Twin Evil Attack (TEA) this project is implemented on the client side. A third step verification appears while the user tries to login. Additional information has been gathered while the user creates the login id. Verification process is done on the user credentials and the additional information if both get mismatched then authentication gets failed.


Connecting WIFI for Internet
Internet accessing from server
Connection will be disconnected
Displaying fake WIFI connection & click the connection
Sending De-Authentication code
Local Area Connection
Network cable unplugged
Marvell Yukon 88E8040 PCI-E Fast...
Wireless Network Connection
59699 2, Shared
Dell Wireless 1395 WLAN Mini-Card
Wireless Network Connection 4
MyHotspot
Microsoft Virtual WiFi Miniport A...
AEC College Hotspot
User account registration
raymond
Login
Options
Displaying fake username and password page
Hacker got a username and password