National seminar On

Cyfo – 2019

January 16-18

(Cyber Security and Digital Forensics)

2019

Organized by

Department of information Science & Technology

Mangattuparamba Campus

Kannur University

[Accredited by NAAC with 'B' Grade]

Kannur District , Kerala -670567

Ph:

Table of Contents

Sl.no	Contents	Page No
1.	About Seminar	
2.	Programme Schedule	
3.	Sessions	
4.	Abstract of Papers	

Kannur University

Kannur University was established by the Act 22 of 1996 of Kerala Legislative Assembly. The University was inaugurated on 2nd March 1996 by E K Nayanar ,the Hon. Chief Minister of Kerala . The objective of the Kannur University Act 1996 is to establish in the state of Kerala a teaching, residential and affiliating University, promoting the development of higher education in Kasargod and Kannur revenue districts and the Mananthavady Taluk of Wayanad District.

Kannur University is unique in the sense that it is a multi-campus university with campuses spread over at Kannur , Kasargode , Mananthavady , Payyannur , Thalassery and Kanjangad. In 2016 March NAAC accredited the University with B grade.At present the university has 34 departments and 105 affiliated colleges

Department of Information Technology

Department of Information Technology , Kannur University campus is situated near Kerala Armed Police IV Battalion, dharmasala , Mangattuparamba. It was established in the year 2000.The department has come long way since its establishment.The department of information technology currently offers MCA, MPhil and PhD in Computer Science and allied fields.The research areas are Digital Speech and Image Processing, Pattern Recognition, Artficial Intelligence, Data Science, Natural Language Processing, Data Mining, Visual Crptography etc.The department has state of art facilities in Intelligent Computing and Signal Processing. The department has produced 14 Phd’s and conducted conferences/workshops on different areas of computer science.

About the seminar

The seminar will solicit a national forum for investigators , researchers and application developers to present their findings.Some of the major objectives are

- To introduce importance of cyber space in present scenario
- To familiarize the importance of cyber intelligence
- To equip participants to identify thrust areas of cyber intelligence research
- To provide an opportunity for the participants to share their experience and ideas in this area enabling individuals to enhance their knowledge, expertise and abilities with regard to the development

Course Coverage

The workshop will discuss various aspects of Cyber Intelligence which include:

- Cyber Security
- Security Threats, Challenges and Vulnerabilities
- Secret Sharing Schemes
- Data Protection
- Social Media Security
- Critical Information Infrastructure Protection
- Cybercrime Investigation Tools
- International Cybercrime Investigation Standards and Procedure
- Digital Evidences
- Cyber Forensics Tools and Techniques
- Digital Image Forensics/ Mobile Forensics/ Cloud Forensics
- Digital Image processing techniques
- AI and machine learning Applications
- Data analytics

Image Transforms for Image Forensic Application

Dr.Essakirajan S ,Professor ,Department of Instrumentation and control Systems Engineering ,PSG college of technology.

Forensic image processing (FIP) involves the computer restoration and enhancement of surveillance imagery. The goal of FIP is to maximize information extraction from surveillance imagery, especially imagery that is noisy, incomplete, or over/under exposed. Although this definition is with respect to surveillance imagery, FIP techniques can be applied to other types of images, such as retinal images, shoe impression images, UAV (unmanned aerial vehicle) infrared images, and more.

Often, for a variety of reasons, the quality of surveillance imagery is very low. The low imagery quality can be caused by poor lighting, poor media quality (analog systems), excessive motion of the subject, a camera in need of calibration, and noise introduced by the imaging/recording system. With digital filtering, image restoration, de-noising, and enhancement techniques, information can often be extracted from low quality imagery.

Forensic imaging processing is a method of improving a digital image (surveillance, closed circuit TV, infrared, etc.) using a variety of computer techniques. These techniques often involve digital "filters" that can suppress noise in the digital image, aid in the extraction of detail from shadow, and provide image sharpening. As will be discussed in a later article, the distribution of image pixels (histogram) can also be optimized for information extraction.

Definition and Enhancement of a Digital Image

An image can be considered as a two-dimensional function, $f(x,y)$, where x and y are plane coordinates such as latitude/longitude in the case of a UAV image, and the value of f at any location (x,y) is the intensity or gray level of the image at that point. The intensity or gray level is directly related to the brightness of the subject that was imaged. Forensic image processing techniques can then be considered to be a transformation that is applied to an input image to produce an output image, such as:

g(*x*,*y*) = *T* [*f*(*x*,*y*)]

f(*x*,*y*) refers to the input image and can specify the gray level for any pixel *x*,*y*, *g*(*x*,*y*) is the output image produced by the forensic image processing technique, and *T* is an image enhancement technique

Fourier Transform

Fourier Transform is an important image processing tool which is used to decompose an image into its sine and cosine components. The output of the transformation represents the image in the Fourier or frequency domain, while the input image is the spatial domain equivalent. In the Fourier domain image, each point represents a particular frequency contained in the spatial domain image.

The Fourier Transform is used in a wide range of applications, such as image analysis, image filtering, image reconstruction and image compression.As we are only concerned with digital images, we will restrict this discussion to the *Discrete Fourier Transform* (DFT).

The DFT is the sampled Fourier Transform and therefore does not contain all frequencies forming an image, but only a set of samples which is large enough to fully describe the spatial domain image. The number of frequencies corresponds to the number of pixels in the spatial domain image, *i.e.* the image in the spatial and Fourier domain are of the same size.

For a square image of size N×N, the two-dimensional DFT is given by:

$$F(k,l) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} f(i,j)\ e^{-\iota 2\pi\left(\frac{ki}{N}+\frac{lj}{N}\right)}$$

where *f(a,b)* is the image in the spatial domain and the exponential term is the basis function corresponding to each point *F(k,l)* in the Fourier space. The equation can be interpreted as: the value of each point *F(k,l)* is obtained by multiplying the spatial image with the corresponding base function and summing the result.

The basic functions are sine and cosine waves with increasing frequencies, *i.e. F(0,0)* represents the DC-component of the image which corresponds to the average brightness and *F(N-1,N-1)* represents the highest frequency.

Cyber Security and Ethical Hacking

-Ms. Suma Rangappan. CEO Grace Cyber Solutions , Kochi

The need for more effective information security practices is increasingly evident with each security breach reported in the media.Ethical hacking offers an objective analysis of an organization’s information security posture for organizations of any level of security expertise. Hackers must scan for weaknesses, test entry points, priorities targets, and develop a strategy that best leverages their resources. The objectiveness of this kind of security assessment has a direct impact on the value of the whole evaluation.

People who spent most of the day online are not really bothered of the traps hidden in cyber world. By providing their personal details without any hesitation, they make their own way to be the victim of cyber-crimes. So many incidents are there where people turned to be victims of cyber-crimes by sharing their details and every activity through social media such as Facebook . She also made well awareness within the listeners about how to secure our information . Demonstrations on hacking were also carried out. The lecture ended well and like her motive, Ms. Suma could make the audience alert about the threats in cyberworld.

Current Trends in Cyber security and Critical Infrastructure Protection

Mr.DittinAndrews ,Senior Technical Officer ,Banglore.

If you know the enemy and know yourself, you need not fear for the result of a hundred battles. If you know yourself but not the enemy , for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, yow will succumb in every battle

-Sun Tzu(Sunzi)(The Art of War)

Challenging aspect in today's world is 3S- technology Synchronize (Collaboration), Store (Storage) and Secure(Security). Each person uses many devices. Wireless devices permits easy use of installed local
Infrastructure. The basic scenarios regarding these issues vary little: it comes down to defending the confidentiality, integrity, and availability of data belonging to individuals and companies against repeated attacks by cybercriminals who try to access, use, and/or steal these data.

Enterprises are under siege from a rising volume of cyber attacks. Threats are increasing by 62% in 2013.1 in 5 organizations have experienced an APT attack.71/2 is the average time an advanced threat goes unnoticed on victims network. At the same time ,the global demand for skilled professionals sharply outpaces supply. Unless this gap is closed,organization will continue to face major risk. Comprehensive educational and networking resources are required to meet the needs of everyone from entry level practitioner to seasoned professional. But the fact is that there are too few professionals.62% of organizations have not increased security training .83% of enterprises currently lack the right skills and human resources to protect their IT assets. At the same time1 million unfilled security jobs are worldwide. Cyber security professionals report an average salary of $116,000, or approximately $55.77 per hour. Nearly three times the national median income for full-time wage and salary workers (US statistics) . Almost all domains and critical networks need professionals Defense ,Communication, Financial, Infrastructure, Power grids, Every where and any where.

THREAT LANDSCAPE

- Nation states – Most capable actors in the cyber domain with political ,economical, military targets
- Crime groups -with international collaboration
- Corporate solutions- Defensive solutions like threat intelligence, network monitoring, penetration testing tools and services used for offensive capability
- Hacktivists- The use of computers and computer networks as a means of protest to promote political ends
- Insiders- Disgruntled insiders facilitating criminal Activity

GENERIC CYBER ATTACKS/CRIMES

- **Email spoofing**: Creation of email messages with a forged sender address eg:deadfake.com- kind of computer based social engineering
- **Spam**: use of electronic messaging systems to send unsolicited bulk messages (spam), especially advertising, indiscriminately.

  Other spams include mobile message spam, web search engine spam, online classifieds spam , spam in blogs etc.
- **Cyberdefamation**: Any sort of defamation or injury to reputation using internet
- **Cyberstalking and harassment**: use of the internet or other electronic means to stalk or harass an individual, a group of individuals, or an organization
- **Computer Sabotage** : Any deliberate action that compromises the confidentiality, integrity, or availability of a computer would be considered sabotage
- **Pornographic offense**: Any visual depiction that can be considered as obsene or unsuitable for the age.

- **Phishing**: act of attempting to acquire sensitive information such as usernames, passwords, and credit card details
  - Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

  - ▪ www.siteadvisor.com- by McAfee for testing websites, APWG-Antiphishing working group(antiphishing.org)

- **Spear phishing**: an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data especially for financial gain or trade secrets or military information.
- **Whaling**: phishing attacks directed specifically at senior executives and other high profile targets within businesses
- **Denial of Service** -Attempt to make computer resources unavailable
- **Password Sniffing**: Scans and records passwords that are used or broadcasted on a computer or network interface

- **Malware or malicious programs**-software designed to infiltrate a computer system without owners informed consent
- **Virus and worms**: Infectious malware-spread from one computer sytem to another
- **Trojan horse**-malware that appears to the user to perform a desired function but facilitates unauthorised acces to the user's sytem
- **Rootkits**-consists of one or more programs to obscure the fact that system is compromised
- **Backdoors**-method of bypassing normal authentication and securing remote access and attempts to remain undetected.
- **Spyware**-collects information from users without their knowledge, secretly installed in the user machine
- **Botnets/zombie network**-a set of compromised computers, automated program for doing some particular task over network

Recent Trends

Can your car be hacked?
You might be behind the wheel,but increasingly, computers control your car's every function.
Microprocessors direct breaking , acceleration and even the horn these days.Since they are hidden people don't understand that there can be

anywhere from 30 to 40 microprocessors in most cars and even upto 100 different ones running different functions in some vehicles.

STAGES IN CYBER ATTACK

PHASE 1-RECONNAISSANCE

- Passive reconnaissance - Involves acquiring information without directly interacting with the target For eg: searching public records or news releases
- Active reconnaissance – Involves interacting with the target directly by any means eg. Telephone calls to help desk or technical department

PHASE – 2 SCANNING

- Pre-attack phase when the attacker scans the network for specific information on the basis of information gathered during reconnaissance
- Includes the use of port scanners, network mapping, vulnerability scanners, ping sweep etc.
- Extract information such as computer names, IP address and user accounts to launch attack

PHASE 3- GAINING ACCESS

- Refers to the point where the attacker obtain access to the OS or application on the computer or network
- Attacker can again access at the OS level, application level, or network level
- Attacker can escalate privileges to obtain complete control of the system.
- Eg. Password cracking, buffer overflows, DoS,session hijacking etc.

PHASE 4- MAINTAINING ACCESS

- Maintaining access refers to the phase when the attacker tries to retain his or her ownership of the system
- Attackers may prevent the system from being owned by other attackers by securing their exclusive access with Backdoors , rootkits or Trojans
- Attackers can upload , download or manipulate data, applications and configurations on the owned system
- Attackers use the compromised system to launch further attacks

PHASE 5 COVERING TRACKS

- Refers to the activities carried out by an attacker to hide malicious acts
- Intensions include continuing access to the victim system, remaining unnoticed and uncaught, deleting evidence that might lead to prosecution
- Attacker overwrites the server , system, and application logs to avoid suspicion

SECURITY AS A PROCESS

- **Anti-virus:**

  Necessary part of good security program.If properly implemented, can reduce organization's exposure to malicious programs.It Will not protect an organization from an intruder who misuses a legitimate program to gain access to a system.It Will not protect an organization from a legitimate user who attempts to gain access to files that should not have access to.

- **Access controls**

  If properly configured and file permissions are set , file access controls restrict legitimate users from accessing file, they should not have access to.It Will not prevent some one from using a system vulnerability.

- **Firewalls**

  Access control devices for the network.It Can protect an organization's internal network from external networks.It Will not prevent an attacker from using an allowed connection to attack a system.It Will not protect from an internal user in internal n/w.

- **Smart cards(some thing you have)**

  Alleviate the problem of passwords.It is Used for authentication.smart card Can reduce the risk of someone guessing a password.But Beware of stolen smart cards. Attack against a vulnerable system will not be prevented with smart cards

- **Biometrics(something you are)**

  Biometric authentication Reduce the risk of someone guessing a password.It is unique. Fingerprints, Retina/iris, Palm prints, Hand geometry, Facial geometry, Voice can be used for authentication.

- **Intrusion detection sytems**

A device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a Management Station.It Will not detect legitimate users who have many inappropriate access to information.

- P**olicy management**

Policy management system helps to make aware of any system that does not conform to the policy. Policy management may not take into account vulnerabilities in systems/ misconfigurations in application software.

- **Vulnerability scanning**

Scanning will help an organization to identify the potential entry points for intruders. VS will not protect computer sytems.Security measures must be implemented immediately after the identification of vulnerability.It Will not detect an legitimate users who have inappropriate access.And Will not detect an intruder who is already in the system as they look for weakness in configurations and patches.

- **Encryption**

Primary mechanisms for communications security. Protect information in transit. Protect information that is in storage by encrypting file.Encryption system will not differentiate between legitimate and illegitimate users if both presents the same keys to encryption algorithm

- **Physical security mechanisms**

  Physical security will not protect the systems from attack that use legitimate access.It will not protect the systems from attacks that come across the network instead of through the front door

“A technology that can give you everything you
want is a technology that can take away everything
that you have.” – Daniel Geer, CISO, In-Q-Tel

Network Security - Mr.MuraleedharanN ,Principal Technical Officer ,CDAC Banglore

With the explosion of the public Internet and e-commerce, private computers and computer networks, if not adequately secured are increasingly vulnerable to damaging attacks. Hackers, viruses, vindictive employees and even human error all represent clear and present dangers to networks. And all computer users from the most casual Internet surfers to large enterprises could be affected by network security breaches. However, security breaches can often be easily prevented. How? This white paper provides you an overview of the most common network security threats and its solution which protects you and your organization from threats, hackers and ensures that the data traveling across your networks is safe.

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.

The Deep Web and Darknet

If we conceive of the Web as a data ocean, most of us are interacting with the wavy, transparent, easily navigable Surface Web .The Surface Web is the portion of the Web that has been crawled and indexed (and thus searchable) by standard search engines such as Google or Bing via a regular web browser. In the darkness below, beneath the electronic thermocline, are the abyssal depths of the Deep Web (also referred to as the Invisible Web or Hidden Web) – the portion of the web that has not been crawled and indexed, and thus is beyond the sonar reach of standard search engines. It is technically impossible to estimate accurately the size of the Deep Web. However, it is telling that Google – currently the largest search engine – has only indexed 4-16 percent of the Surface Web. The Deep Web is approximately 400-500 times more massive than the Surface Web . It is estimated that the data stored on just the 60 largest Deep Web sites alone are 40 times larger than the size of the entire Surface Web . Growing rapidly within the Deep Web is the Darknet (also referred to as the Dark Web, Dark Net, or Dark Internet). Originally, the Darknet referred to any or all network hosts that could not be reached by the Internet. However, once users of these network hosts started sharing files (often anonymously) over a distributed network that was not indexed by standard search engines, the Darknet became a key part of the Deep Web. Unlike the traffic on the Surface Web or most parts of the Deep Web, most Darknet sites can only be accessed anonymously.

How To Access The Deep Web And Darknet

Depending on one's overall goals, different tools and techniques will help reach different depths. For most users, there are generally two different but related approaches to access the Deep Web and Darknet:

■ Use special search engines accessed from regular browsers such as Internet Explorer, Firefox, Chrome, Safari, etc.

■ Use special search engines that can be accessed only from a TOR browser.

The research community and those familiar with technology can go even deeper by developing a custom-built crawling program using linkcrawling techniques and API programming skills.

One easy way to gain access to the Deep Web is to use alternative/special search engines that are designed specifically for the purpose. These alternative search engines are designed to access different parts of the Deep Web (see Table 1), but the challenge is that all search engines developed so far only crawl or index a small part of the Deep Web. Therefore, it is still necessary to visit the right online directory or hidden website listings(e.g.https:// sites.google.com/site/howtoaccessthedeepnet/ working-links-to-the-deep-web). Since these websites are not indexed, they will not be found using normal search tools. However, their URLs can be found using other means and, once the 8 URL is known, one can then access some of these sites on the Deep Web using regular browsers.

Image Forensics for Cyber Crime Investigation

Mr.Vijith T K ,Assistant Professor and Head ,Colllege of Engineering ,Vatakara.

Digital forensics is the science of identifying, extracting, analyzing and presenting the digital evidence that has been stored in the digital devices. Various digital tools and techniques are being used to achieve this. Computer forensics is the process that applies computer science and technology to collect and analyze evidence which is crucial and admissible to cyber investigations.

Network forensics is used to find out attackers' behaviours and trace them by collecting and analyzing log and status information. A digital forensic investigation is an inquiry into the unfamiliar or questionable activities in the Cyber space or digital world. The investigation process is as follows

Collection phase: The first step in the forensic process is to identify potential sources of data and acquire forensic data from them. Major sources of data are desktops, storage media, Routers, Cell Phones, Digital Camera etc. A plan is developed to acquire data according to their importance, volatility and amount of effort to collect].

Examination: Once data has been collected, the next phase is to examine it, which involves assessing .

Analysis: Extracted and relevant data has been analysed to draw conclusions. If additional data is sought for detail investigation will call for in depth data collection.

Reporting: This is the process of preparing and presenting the outcome of the Analysis phase.

Digital Forensic Science covers Computer forensics, Disk forensics, Network forensics, Firewall forensics, Device forensics, Database forensics, Mobile device forensics, Software forensics, live systems forensics etc.

It is one of the very important step to choose a right cyber forensic examiner or digital crime analyst, who must be trained, certified, court acceptable and experienced with the latest digital forensic examination techniques and recent advanced investigation software / tools. If your case related to court, police or legal matter, then selecting the right & correct Cyber Forensic Analyst or Cyber Crime

Investigator is just as important as choosing the right lawyer or advocate, otherwise there may be chances of negative effect on your case. Powerful Expert Opinion will help you win your case and save wastage of time & money. Please remember that many Cyber Experts, Ethical Hackers, IT Professionals, Cyber Security Experts Reports etc... are not acceptable in courts etc, so be aware during selecting right Cyber Expert.

Abstract of Selected Papers