COMPUTER SECURITY AND CYBER LAW (CSCL)

LECTURER: ROLISHA STHAPIT/ DIKSHYA SINGH

Unit 10

Policy and Procedures LH3

- Computer Crime and Categories, Cyber Crime, Digital Forensics (overview of (Digital Evidence, Investigation Procedures, Categories of evidence (Impressions, Bioforensics, Trace evidence, Material evidence)), Intellectual Property Rights, Copyrights, Trademarks, Patents Licenses, Agreements, Plagiarism, Digital rights management, Privacy protection, Cyber Law, Electronic Transaction Act, Electronics Transaction Rules, IT Policy, Information Security and policies

Computer Crime

- Computer crime refers to any crime that involves a computer and a network.
- The computer may have been used in the commission of a crime, or it may be the target.
- Netcrime refers to criminal exploitation of the Internet.
- Cybercrimes are defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)".
- Such crimes may threaten a nation‘s security and financial health. Issues surrounding this type of crime have become high-profile, particularly those surrounding cracking, copyright infringement, child pornography, and child grooming.

- There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise.
- Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes.
- Activity crossing international borders and involving the interests of at least one nationstate is sometimes referred to as cyber warfare.
- The international legal system is attempting to hold actors accountable for their actions through the International Criminal Court.

Categories

- Computer crime encompasses a broad range of activities. Generally, however, it may be divided into two categories:

  1. Crimes that target computers directly

  2. Crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device.

- Crimes that primarily target computer networks or devices include:

  - Computer viruses
  - Denial-of-service attacks
  - Malware (malicious code)

- Crimes that use computer networks or devices to advance other ends include:
  - Cyberstalking
  - Fraud and identity theft
  - Information warfare
  - Phishing scams

Cyber Crime

- Cybercrime is criminal activity done using computers and the Internet.
- Cyber crime encompasses any criminal act dealing with computers and networks.
- It also includes traditional crimes conducted through the Internet. For example; hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be cyber crimes when the illegal activities are committed through the use of a computer and the Internet.
- It includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts etc.
- Cybercrime also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet.

Digital Forensic

- Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime.
- The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data.
- Digital forensics is a branch of computer science that focuses on developing evidence pertaining to digital files for use in civil or criminal court proceedings.
- Digital forensic evidence would relate to a computer document, email, text, digital photograph, software program, or other digital record which may be at issue in a legal case.

- Digital evidence encompasses any and all digital data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its agent.
- Intrusion Detection Systems are a great source of digital evidence. They collect information from a variety of system and network sources then analyze the information for signs of intrusion and misuse.

Forensics vs. Security

Security

- wants to preserve the digital system the way it is – observing the policy that has been defined
- Focus is on (security) policy enforcement and the adequate roles are dressed up in hierarchy of access rights

Forensics

- attempts to explain how the policy came to be violated, which may eventually lead to finding flaws and making improvements in the future.
- Risk assessment

Computer/data/cyber forensics

- The lawful and ethical seizure, acquisition, analysis, reporting and safeguarding of data and meta-data derived from digital devices which may contain information that is notable and perhaps of evidentiary value to the trier of fact in managerial, administrative, civil and criminal investigations (L. Leibrock, 1998)

Digital Evidence

What is evidence?

- Evidence in its broadest sense includes everything that is used to determine or demonstrate the truth of an assertion

What is digital evidence?

- Digital evidence or electronic evidence is any information stored or transmitted in digital form that a party to a court case may use at trial.
- Before accepting digital evidence a court will determine if the evidence is relevant, whether it is authentic, if it is hearsay and whether a copy is acceptable or the original is required.
- Digital evidence encompasses any and all digital data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator. Intrusion Detection Systems are a great source of digital evidence. They collect information from a variety of system and network sources then analyze the information for signs of intrusion and misuse.

- The evidence is accurate and reliable if the substance of the story the material tells is believed and is consistent, and there are no reasons for doubt.
- Evidence is complete if the story that the material purports to tell is complete. That is, there are no other stories that the material also tells that might have a bearing on the legal dispute or hearing.
- Digital evidence can be classified, compared, and individualized in several ways. One of those ways is by the contents of the evidence. For example, investigators use the contents of an e-mail message to classify it and to determine which computer it came from.

- Another way to classify digital evidence is by function. This is when investigators examine how a program functions to classify it and sometimes individualize it. For example, a program that appears to do something amusing or useful but actually does something else is classified as a Trojan horse program. In addition, digital evidence can be classified by characteristics like file names, message digests, and date stamps.

Digital investigation

- Both computer and network forensics methodologies consist of three basic components that Kruse and Heiser both call the three As of computer forensics investigations.
- These are as follows: acquiring the evidence, taking care to make sure that the integrity of the data is preserved; authenticating the validity of the extracted data – this involves making sure that the extracted data is as valid as the original; and analyzing the data while keeping its integrity.
- A digital investigation is a process to answer questions about digital states and events. The basic digital investigation process frequently occurs by all computer users when they, for example, search for a file on their computer. They are trying to answer the question "what is the full address of the file named important.doc?". In general, digital investigations may try to answer questions such as "does file X exist?", "was program Y run?", or "was the user Z account compromised?"

General Process

- There is no single procedure for conducting an investigation. An intuitive procedure is to apply the same basic phases that are used by police at a physical crime scene, where we instead have a digital crime scene.
- The first step is preservation, where we attempt to preserve the crime scene so that the evidence is not lost. In the physical world, yellow tape is wrapped around the scene. In a digital world, we make a copy of memory, power the computer off, and make a copy of the hard disk. In some cases, the computer cannot be powered off and instead suspicious processes are killed and steps are taken to ensure that known evidence is copied and preserved.

- The second step is to survey the crime scene for the obvious evidence. The "obvious" evidence is the evidence that typically exists with investigations of this type. For example, at a physical crime scene where a violent crime has occurred, then the "obvious" evidence may have blood on it or be damaged. In a digital crime scene, the obvious evidence may be found based on file types, keywords, and other characteristics.
- After the obvious evidence has been found, then more exhaustive searches are conducted to start filling in the holes. With each piece of evidence that is found, there could be questions about how it got there. Questions such as "which application created it?" or "what user caused it to be created?". If so, then event reconstruction techniques are needed to determine which application-level event occurred. This is similar to reconstructing where a bullet was shot from.

Where to focus and how to start

- What are we going to work with:
  - Policies, technical procedures, permissions, billing statements, system utilities, applications, and various logs
- Whom and what we want to monitor:
  - Employees, employers, access rights, email, surfing logs, and chat room records.

Case assessment and requirements

- Situation – local and global environment
- Nature of the case
- Specifics
- Types of evidence
- Operating system – working environment
- Archive storage formats
- Location of evidence

Handling evidence

- Includes extraction and establishment of a chain-of-custody, which also involves packaging, storage, and transportation
- Who extracted the evidence and how?
- Who packed it?
- Who stored the evidence, how and where?
- Who transported it?

Handling evidence

- Case
  - Number
  - Investigator/institution/organization
  - Nature of the case
- Equipment
  - For all computers and devices involved – manufacturer, vendor, model, and serial number
- Evidence
  - Location
  - Recording entity
  - Time and date of recording

All of this sometimes is qualified as a chain-of-evidence.

Evidence recovery

- Extraction depends on the nature of the incident and the type of equipment or system involved (computer, operating environment, network)
- Rule of thumb – extract and collect as much as you can (avoid going back – most of the time it is impossible)
- Compress the evidence with lossless compression tools
- Some hashing (MD5, CRC, or SHA-1/2/3) should be done for integrity after storage and transportation

Preserving evidence

- No single standard
- Packaging and extra storage measures – digital evidence may be a disappearing act
- Back-ups
- Document
- Control access
- Validate and/or authenticate data based on standard procedures

Transporting evidence

- One has to protect the chain-ofcustody
- Strong data hiding techniques – encryptions, passwords, steganography
- Assurance of the preserved content
- Test possible changes and modifications

Analysis of evidence

- Fairly long and painstaking process
- Diversified
  - From shortcuts to recycle bins and registries
  - Every data medium and data type
  - All encrypted and archived files
- Hard drive physical analysis
- Hard drive logical analysis
- Depends on the platforms and the tools used

Categories of evidence

- When dealing with computer forensics, the only thing to be sure of is uncertainty. So the investigator should be prepared for difficulties in searching for bits of evidence data from a haystack. The evidence usually falls into the following categories:
- Impressions: this includes fingerprints, tool marks, footwear marks, and other types of impressions and marks.
- Bioforensics: this includes blood, body fluids, hair, nail scrapings, and bloodstain patterns.
- Infoforensics: this includes binary data fixed in any medium such as on CDs, memory, and floppies.
- Trace evidence: this includes residues of things used in the committing of a crime like burning, paint, glass, and fibers.
- Material evidence: this includes physical materials such as folders, letters, and scraps of papers.

Intellectual Property

- Intellectual property (IP) is a controversial term referring to a number of distinct types of creations of the mind (intangible property created by individuals or organization) for which a set of rights are recognized under the corresponding fields of law.
- Intellectual property refers to rights in creations of the human mind which arise under the laws of patents, copyrights, trademarks, trade secrets, unfair competition and related laws. Article 2 of the Convention Establishing the World Intellectual Property Organization (WIPO) defines intellectual property as follows:
  - *(viii) "intellectual property" shall include the rights relating to:*

- *literary, artistic and scientific works;*
- *performances of performing artists, phonograms, and broadcasts;*
- *inventions in all fields of human endeavor;*
- *scientific discoveries;*
- *industrial designs;*
- *trademarks, service marks, and commercial names and designations;*
- *protection against unfair competition; and*
- *all other rights resulting from intellectual activity in the industrial, scientific, literary or artistic fields.*

- Intellectual property rights (IPRs) are the legal rights given to creators of intellectual property.
- IPRs usually give the creator of intellectual property the right to exclude others from exploiting the creation for a defined period of time.
- Intellectual property laws provide the incentives that foster innovation and creativity, and strive to ensure that the competitive struggle is fought within certain bounds of fairness.
- The protection of IPRs contributes significantly to technological progress, competitiveness of businesses and our country's well-being.

- IP is divided into two categories:

–Industrial property, which includes inventions (patents), trademarks, industrial designs, etc.

–Copyright, which includes literary and artistic works such as novels, poems and plays, films, musical works, drawings, paintings, photographs ,architectural designs, etc

Copyright

- A copyright is a law that gives the owner of a written document, musical composition, book, picture, or other creative work, the right to decide what other people can do with it.
- Copyright laws make it easier for authors to make money by selling their works.
- Because of copyright, a work can only be copied if the owner of the copyright gives permission.
- When someone copies or edits a work that is protected under copyright without permission, the owner may sue for the value of the violation.
- Most such cases are handled by civil law. In more serious cases, a person who copies a work that is protected under copyright could be arrested, fined or even go to prison.

- As soon as a work is created and is in a tangible form (such as writing or taping) the work automatically has federal copyright protection
- stating the word copyright, or copy or "c" in a circle, with the name of the creator, and the date of copyright

Trademark

- A trademark, or trade-mark is a recognizable sign, design or expression which identifies products or services of a particular source from those of others.
- The trademark owner can be an individual, business organization, or any legal entity.
- A trademark may be located on a package, a label, a voucher or on the product itself.
- The period of protection varies, but a trademark can be renewed and Trademark protection is legally enforced by courts.
- Trademark protection also hinders the efforts of unfair competitors, such as counterfeiters, to use similar distinctive signs to market inferior or different products or services

- Trademark protection ensures that the owners of marks have the exclusive right to use them to identify goods or services, or to authorize others to use them in return for payment.

Patent

- A patent is a set of exclusive rights granted by a sovereign state to an inventor or assignee for a limited period of time in exchange for detailed public disclosure of an invention.
- An invention is a solution to a specific technological problem and is a product or a process.
- Patents are form of intellectual property.
- A patent protects an inventor’s intellectual property for a limited period of time usually 20 years.
- During the lifetime of the patent, it gives the owner the right to prevent others making or using the invention, unless the owner grants permission.
- To be patentable, an invention must be new and useful.

License

- formal permission from a governmental or other constituted authority to do something, as to carry on some business or profession.
- The certificate or the document itself that confers permission to engage such as a certificate, tag, plate, etc., giving proof of such permission; official permit: a driver's license.
- A license may be granted by a party ("licensor") to another party ("licensee") as an element of an agreement between those parties.
- A shorthand definition of a license is "an authorization (by the licensor) to use the licensed material (by the licensee)."
- In particular, a license may be issued by authorities, to allow an activity that would otherwise be forbidden.
- It may require paying a fee and/or proving a capability.

- The requirement may also serve to keep the authorities informed on a type of activity, and to give them the opportunity to set conditions and limitations.
- A licensor may grant a license under intellectual property laws to authorize a use (such as copying software or using a (patented) invention) to a licensee, sparing the licensee from a claim of infringement brought by the licensor.

Agreement

- A meeting of minds with the understanding and acceptance of reciprocal legal rights and duties as to particular actions or obligations, which the parties intend to exchange; a mutual assent to do or refrain from doing something; a contract.
- The writing or document that records the meeting of the minds of the parties. An oral compact between two parties who join together for a common purpose intending to change their rights and duties.
- An agreement is not always synonymous with a contract because it might lack an essential element of a contract, such as consideration.
- any meeting of the minds, even without legal obligation.
- in law, another name for a contract including all the elements of a legal contract: offer, acceptance, and consideration (payment or performance), based on specific terms.

Plagiarism

- Plagiarism is copying another person's ideas, words or writing and pretending that they are one's own work.
- It can involve violating copyright laws.
- College students who are caught plagiarizing can be kicked out of school, and writers who plagiarize will often be taken less seriously.
- Writing papers, many students practice plagiarism without knowing it by using other people's ideas without citing them (saying where they got them).
- Reading another article or book and taking an idea from it and putting it into one's own words is not plagiarism if the writer of the paper says where they got the idea.

Cyber Law

- IT Law is a set of legal enactments, which governs the digital dissemination of both (digitalized) information and software itself. IT Law covers mainly the digital information (including information security and electronic commerce) aspects and it has been described as "paper laws" for a "paperless environment“.
- Cyberlaw or Internet law is a term that encapsulates the legal issues related to use of the Internet. It is less a distinct field of law than intellectual property or contract law, as it is a domain covering many areas of law and regulation.
- Cyber law is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", (Internet).
- It is less a distinct field of law in the way that property or contract are, as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to apply laws designed for the physical world to human activity on the Internet.

Digital Rights Management (DRM)

- DRM refers to a collection of systems used to protect the copyrights of electronic media. These include digital music and movies, as well as other data that is stored and transferred digitally.
- For example, the Apple iTunes Music Store uses a DRM system to limit the number of computers that songs can be played on. Each audio file downloaded from the iTunes music store includes information about the owner of the file and how many times the file has been transferred. The protected files will not play on computers that have not been authorized to play the music.
- Digital Rights Management is important to publishers of electronic media since it helps ensure they will receive the appropriate revenue for their products.

- By controlling the trading, protection, monitoring, and tracking of digital media, DRM helps publishers limit the illegal propagation of copyrighted works.
- This can be accomplished by using digital watermarks or proprietary file encryption on the media they distribute.
- Whatever method publishers choose to employ, DRM helps them make sure that their digital content is only used by those who have paid for it.

The applications and methods are endless -- here are just a few examples of digital rights management:

- A company sets its servers to block the forwarding of sensitive e-mail.
- An e-book server restricts access to, copying of and printing of material based on constraints set by the copyright holder of the content.
- A movie studio includes software on its DVDs that limits the number of copies a user can make to two.
- A music label releases titles on a type of CD that includes bits of information intended to confuse ripping software.

Privacy Protection

- It is the ability of an individual or group to seclude themselves or information about themselves and thereby express themselves selectively.
- The boundaries and content of what is considered private differ among cultures and individuals, but share common themes.
- When something is private to a person, it usually means there is something to them inherently special or sensitive.
- The domain of privacy partially overlaps security, including for instance the concepts of appropriate use, as well as protection of information.
- Privacy may also take the form of bodily integrity.

ETA and more

- Electronic Transaction Act,
- Electronics Transaction Rules,
- IT Policy,
- Information Security and policies,

Information Security and policies

- A security policy is a document that states in writing how a company plans to protect the organization's physical and information technology assets.
- A security policy is often considered to be a "living document", meaning that the document is never finished, but is continuously updated as technology and employee requirements change.
- An organization’s security policy may include an acceptable use policy, a description of how the organization plans to educate its employees about protecting the organization’s assets, an explanation of how security measurements will be carried out and enforced, and a procedure for evaluating the effectiveness of the security policy to ensure that necessary corrections will be made.

Information Technology Policy,2010

- **Vision:** To place Nepal on the global map of information technology within the next five years
- **Objectives:** The information technology policy shall be formulated to achieve the following objectives:
    - To make information technology accessible to the general public and increase employment through this means,
    - To build a knowledge-based society, and
    - To establish knowledge-based industries.

Strategies:

The following information technology strategies shall be adopted to accomplish the above-mentioned objectives through rapid development and extension of information technology in a fair and competitive manner.

- The government shall act as a promoter, facilitator and regulator.
- High priority shall be accorded to research, development and extension of information technology with participation of private sectors.
- Competent manpower shall be developed with the participation of both the public and the private sectors for the sustainable development and extension of information technology.
- Domestic and foreign investment shall be encouraged for the development of information technology and the related infrastructures.
- Nepal shall be placed on the global map of information technology.
- E-commerce shall be promoted with legal provisions.

- Information technology shall be used to assist e-governance.
- Information technology shall be applied for rural development.
- Information technology industry shall be promoted.
- Speedy and qualitative service shall be made available at a reasonable cost by creating a healthy and competitive atmosphere among information technology service providers.
- Computer education shall be incorporated in academic curriculum starting from the school level.
- Professional efficiency shall be enhanced through the use of information technology.
- Information technology network shall be extended to rural areas.
- Nepal shall be placed on the international market through information technology.
- Export of services related to information technology (software and hardware) shall be increased to 10 billion rupees within the next five years.

Information Technology Policy

The following policies shall be followed up for the implementation of the aforesaid strategies:

• To declare information technology sector a priority sector,

• To adopt one window system for the development of information technology,

• To prioritize research and development in the field of information technology,

• To create an atmosphere conducive to attracting investment in the private sector, keeping in view the private sector's role in the development of information technology,

• To provide Internet facilities gradually to all Village Development Committees of the country,

• To assist educational institutions and encourage domestic and foreign training to fulfill the requirement of appropriate manpower at various levels pertaining to information technology,

• To computerize the system in all government offices and build their websites for the flow of information,

• To encourage the use of computers in private sectors,

- To develop physical and virtual information technology parks at various places with private sector's participation in the development of information technology,
- To use information technology to promote e-commerce, e-ducation, e-health among others, and to transfer technology to rural areas.
- To establish a National Information Technology Centre,
- To establish a fund at the national level by mobilising resources from Government of Nepal, donor agencies and private sectors so as to promote research and development of information technology and other related activities,
- To establish a venture capital fund with joint participation of public and private sectors,
- To include computer education in the curriculum starting from the school level and broaden its scope,
- To establish Nepal in the global market through the use of information technology,
- To enact necessary laws for providing legal sanctions to the use of information technology,
- To use information technology gradually in all government activities and provide legal sanctions to them.

Electronic Transaction Act 2063

- An Act promulgated to make legal provisions for electronic transaction of digital data.
- This includes legal provisions for authentication and regularization for recognition, validity, integrity and reliability of production, processing, storage, communication and transmission of electronic record.
- This Act was declared on 24th Bhadra 2063 (2nd September, 2008)

Following are the Electronic Transaction rules:

Provisions Relating to Electronic Record and Digital Signature

- Authencity of Electronic Record:
- Legal Recognition of Electronic Record:
- Legal Recognition of Digital Signature:
- Electronic Records to be Kept Safely:
- Secured Electronic Records:
- Secured Digital Signature:

Provision Relating to Dispatch, Receipt and Acknowledgement of Electronic Records

- Electronic Record to be Authenticated to be from the Originator:
- Procedure of Receipt and Acknowledgement of Electronic Record:
- Time and Place of Dispatch and Receipt of Electronic Record:

Provisions Relating to Digital Signature and Certificates

- Certifying Authority may issue a Certificate:
- Certifying Authority may issue a Certificate:
- Certificate may be suspended:
- Certificate may be revoked:

Functions, Duties and Rights of Subscriber

- To Generate Key pair:
- To Accept a Certificate:
- To retain the private key in a secured manner:
- To Deposit the Private Key to the Controller**:**

Electronic Record and Government use of Digital Signature

- Government Documents may be published in electronic form:
- To Accept the Document in Electronic Form:
- Use of Digital Signature in Government Offices:

Provisions Relating to Network Service

- Liability of Network Service Providers
- Network Service Provider not to be Liable

Offence Relating To Computer

- To Pirate, Destroy or Alter computer source code:
- Unauthorized Access in Computer Materials:
- Damage to any Computer and Information System:
- Publication of illegal materials in electronic form:
- Confidentiality to Divulge:
- To inform False statement:
- Submission or Display of False License or Certificates:
- Non-submission of Prescribed Statements or Documents:
- To commit computer fraud:
- Abetment to commit computer related offence:
- Punishment to the Accomplice:
- Punishment in an offence committed outside Nepal:
- Confiscation:
- Offences Committed by a corporate body:
- Other Punishment:

Information Technology (IT) Security and policy

- An Information Technology (IT) Security Policy identifies the rules and procedures for all individuals accessing and using an organization's IT assets and resources.
- Information Technology (I.T.) Acceptable Use Policy

  -The use of computer accounts and passwords;

  -Confidentiality and privacy of information;

  -The use of computer hardware and software;

  -Backup of Information

  -Storage of information

- Electronic Communications Policy

-The confidentiality and privacy of email and fax messages;

-Access to restricted and blocked internet content;

Password Standards Policy

-The creation of secure passwords;

-Minimum password length;

-Composition and complexity of passwords;

Encryption Policy

-Minimum level of encryption;

-Approved Encryption Algorithms and Protocols;

Introduction to E-government

- E-Government (short for electronic government, also known as e-gov, digital government, online government, or connected government) is digital interactions between a government and citizens (G2C), government and businesses/Commerce (G2B), government and employees (G2E), and also between government and governments /agencies (G2G).
- The e-Government delivery models are

–G2C (Government to Citizens)

–G2B (Government to Businesses)

–G2E (Government to Employees)

–G2G (Government to Governments)

–C2G (Citizens to Governments)

Introduction to E-contract

- A contract is an agreement that is enforceable by a court of law or equity.
- An Electronic Contract...
  - is a well-structured document
    - From the perspective of formatting
    - Semantically
  - is edited/viewed in different contexts
    - Composition, Printing, Visualisation, Signing
  - consists of standard elements plus individual extensions
  - needs to be exchanged
  - may be manipulated in a collaborative session
  - is signed by attaching signatures in a standardized way

Type of online contract:

- **Business-to-business (B2B)** includes suppliers of raw materials, parts and components and wholesalers to retail. Electronic Data Interchange (EDI) systems may replace paper with the standards specified as part of the contract.
- **Business-to-consumer (B2C)** includes sites such as Amazon.com that use online catalogs and price lists. Purchases may be made online, via fax, phone or mail. Payments may be electronic or physical. Goods may be delivered or picked up.
- **Consumer-to-consumer (C2C)** includes sites such as eBay, online want ads, auctions or flea markets.