TCS332 Fundamental of Information Security and Blockchain

B. Tech CSE III Semester

Instructor:

Dr Mohammad Wazid

Professor, Department of CSE,

Head of Cyber security and IoT Research Group

Graphic Era (Deemed to be University), Dehradun, India

(Research h-index: 43, i10-index:71)

Email: wazidkec2005@gmail.com

Homepage: https://sites.google.com/site/mwazidiiith/home

About the instructor

Qualification:

1. Postdoc from Cyber Security and Networks Lab, **Innopolis University, Innopolis, Russia.**

2. Ph. D (CSE) from Center for Security, Theory and Algorithmic Research of the **International Institute of Information Technology (IIIT), Hyderabad, India.**

3. M. Tech. Computer Network Engineering from **Graphic Era Deemed to be University, Dehradun, India.**

4. B. E. (CSE) from **KEC, Dwarahat, (Regional Engineering College (REC) Uttarakhand, India.**

About the instructor

Research background:

- ❖Published 133 papers in international journals and conferences in the fields of
- ❖ Filed/published/granted 13 patents

Research areas:

Cyber Security

Authentication

Internet of Things (IoT)

Cloud Computing

Big Data

Blockchain

About the instructor

Research background:

❖Some of the research findings were published in top-cited journals, such as the IEEE TIFS, IEEE TDSC, IEEE Transactions on Smart Grid, IEEE Internet of Things Journal, IEEE Transactions on Industrial Informatics, IEEE Journal of Biomedical and Health Informatics, IEEE Consumer Electronics Magazine, Future Generation Computer Systems, and Journal of Network and Computer Applications.

Awards:

- University Gold Medal in M. Tech program
- Young Scientist Award by UCOST, Department of Science and Technology, Government of Uttarakhand
- Dr. A.P.J Abdul Kalam innovator of the year award
- ICT Express (Elsevier) Best Research Reviewer Award for 2019

Course Outcomes

- After completion of the course, students will be able to:
- 1. Explain information security and blockchain
- 2. Know the working of information security techniques
- 3. Analyse the different information security protocols
- 4. Use blockchain to implement information security protocols
- 5. Apply information security techniques in different applications
- 6. Develop blockchain-enabled information security protocols

Grading scheme

- **As per the University scheme.**

Contents of this course

- ❖Introduction to information security.
- ❖Linux basics and scripting for information security.
- ❖Basics of network and web security.
- ❖Overview of blockchain.
- ❖Blockchain mechanisms.

Reference Books:

- Georgia Weidman, “Penetration Testing: A Hands-on Introduction to Hacking”, No Starch Press, 2020.
- George Icahn, “Blockchain: the complete guide to understanding blockchain technology”, 2020.
- Antony lewis, “The basics of bitcoins and blockchains: an introduction to cryptocurrencies and the technology that powers them”, 2020.

Unit 1. Introduction to information security

Topics for this lecture

- **What is Cyber security**
- **Why we need Cyber security**
- **The Zero Trust Model**

Overview: Cyber security

- “Cyber” keyword came from “Cybernetic”, from the Greek for “skilled in steering (governing)”,

- Cyber is a **“prefix”** used in a growing number of terms to describe new things that are being made possible by the use of computers.

- Anything related to the **“Internet”** also falls under the cyber category.

Overview: Cyber security

- **Cyber security is a process of protecting and recovering networks, devices, and programs from any type of cyberattack.**

Overview: Cyber security

- Cyber security is often confused with the definition of information security.
- Information security, often referred to as ‘IT security’, looks to protect all information assets, whether as a hard copy or in digital form.
- **Cyber security is a subset of information security.**
- It specifically focuses on protecting computer systems and their components i.e., hardware, software and data.

Overview: Cyber security

- Overall protecting the digital infrastructure from attack, and unauthorized access.
- In recent years, cyber security has come under focus of the society because of rapid development of cyber risks (i.e., attacks) and the degree of impact on individuals, governments organizations and other organizations.

The three pillars of cyber security:

- **Robust cyber security involves implementing controls based on three pillars:**
- People
- Processes
- Technology

The three pillars of cyber security:

- **People:**

Every employee needs to be aware of their role in preventing and reducing cyber threats, and staff dedicated to cyber security need to keep up to date with the latest cyber risks and solutions.

- **Processes:**

- Processes (process means day-to-day activates going in a organization).
- Processes are crucial in communicating the organization’s cyber security stance.

The three pillars of cyber security:

- **Processes:**
- Documented processes should also clearly define roles and responsibilities, and specify the procedure to follow when (i.e., reporting a suspicious email).
- Processes should be regularly reviewed to account for the latest cyber threats and responses.

- **Technology:**
- While organizational measures (i.e., protection methods) are a big part of cyber security, technical controls are just as essential.
- For example use of access controls, installation of antivirus software, and other technology can be deployed to protect against cyber attacks.

Need of cyber security

1. Increasingly sophisticated hackers

- Hacker (Internet attackers) are going smart day by day.
- They use novel tools and technique to get access into a system.
- Every organization has a website and **externally exposed systems** that could provide hackers a entry points into internal networks.
- With the common highly sophisticated attacks, business organizations need to assume that they will be breached at some point.
- So they need to implement controls which help to detect and respond to malicious activity before it causes damage and disruption.

Need of cyber security

2. The rising cost of breaches

- The fact is that cyberattacks can be extremely expensive for an organization to suffer.
- Recent statistics have suggested that the average cost of a data breach at a larger firm is £20,000.
- It is not just the financial damage suffered by the organization but also causes **untold reputational damage.**
- Suffering a cyberattack can cause customers to lose trust in the organization. So they try to spend their money elsewhere.

3. Rapid growth in the deployment of IoT devices

- More smart devices (i.e., smart home applliances, smart healthcare devices) than ever are connected to the internet.
- These are known as Internet of Things (IoT) devices and are commonly use in homes and offices.
- On the surface, these devices can simplify and speed up tasks, as well as offer greater levels of control and accessibility.

3. Rapid growth in the deployment of IoT devices

- Rapid growth in their deployment, however presents a problem.
- If their security is not managed properly, each IoT device which is connected to the internet could provide cyber criminals a entry point for unauthorized access.
- Such kind of unauthorized access can lead to information leakage or other serious issues.

4. Tighter regulations

- It is not just criminal attacks that mean organizations need to be more invested in cyber security than ever before.
- The introduction of regulations such as the GDPR (EU General Data Protection Regulation) means that organizations need to take security more seriously than ever, or face heavy fines.
- Among the requirements of the GDPR is the need for organizations to implement appropriate technical and organizational measures to **protect personal data**, **regularly review controls**, **plus detect, investigate and report breaches.**

The Zero Trust Model
(Ruled by the motto never trust, always verify)

- **Trust and trustworthiness**
- **Trust:** Firm belief in the reliability, truth, or ability of someone or something.
- **Trustworthiness:** The ability to be relied on as honest or truthful.
- Trusting someone means that you think they are reliable, you have confidence in them and you feel safe with them physically and emotionally **(In Cyber security: You feel safe technically).**

The Zero Trust Model

- When trying to create a safe network, organizations usually use a classic perimeter strategy.
- This strategy assumes that all users, devices, and endpoints inside the perimeter are trusted by default, and only outsiders are treated as a potential threat.
- But today, more and more companies are implementing Bring Your Own Device (BYOD) policies, hiring remote employees, using cloud services and storage, and granting access to their networks to third-party vendors.

The Zero Trust Model

- In such an environment, the real threats come from within the network, increasing the risk of access misuse and devastating data breaches caused by insiders.
- Therefore, securing remote access and ensuring a high level of perimeter protection isn’t enough anymore.

The Zero Trust Model

- One **possible solution to ensuring a better level of protection against insider threats is the so-called zero trust security model.**
- In contrast to the classic perimeter model, this model doesn’t identify trusted users, devices, or endpoints based on the network they belong to.
- Instead, the zero trust model is ruled by the motto never trust, always verify.
- It treats both **insiders** and **outsiders** as **untrusted** sources.

The Zero Trust Model

- The term zero trust was first used by Forrester experts when describing a new security model in which users and devices were no longer split into trusted and untrusted groups.
- Basically, the zero trust model is designed to reduce the risk of insider threats.
- In the zero trust security model, you **grant access** to critical applications, data, and endpoints only to those **users** and **devices** that have already been **authenticated and verified**.

The Zero Trust Model

- **Summary:**
- This approach is based on three essential steps:
- **Verifying users** when they log in to the system **(Use of strong authentication mechanism).**
- **Validating devices** before they connect to the network **(Use of strong device access control mechanism).**
- **Managing privileged access (Use of strong user access control mechanism).**

The Zero Trust Model

Fig. 1: Zero trust model (Image source: https://www.ekransystem.com/en)

Possible suggestions

- User verification can be ensured with the help of such tools as multi-factor authentication (i.e., 2-factor or 3).
- Each time someone tries to access sensitive data, you have to make sure that the user requesting permission is who they claim to be **(check the genuineness of a user).**
- User behavior monitoring and analysis may also be helpful in verifying legitimate users and detecting insider threats.
- For example, a **login at an unusual time** or from a suspicious location should be treated as a sign of a possible **cybersecurity problem.**

Possible suggestions

- Also, **the least privilege approach** must be applied wherever possible in order to make sure that no one can access data or assets which they are not authorized to access.

Approaches for effective cyber security

1: Confidentiality

- Confidentiality means something which is secret and should not be disclosed to unintended people or entities.
- Confidentiality ensures that sensitive information is accessed only by an authorized person and kept away from those who are not authorized.
- Examples are Bank account statements, Personal information, Credit card numbers and Government documents.
- Any data security approach is used should ensure customer’s data remains confidential at all times.

Approaches for effective cyber security

1: Confidentiality

- **Solution: Use of data encryption techniques**
- Data confidentiality in the network begins at the physical layer, where fiber tapping devices can be used to steal sensitive data.
- To combat this, all your in transit data should be bulk encrypted from end-to-end which makes it undecipherable.

Approaches for effective cyber security

2: Integrity

- Integrity means that when a sender sends data, the receiver must receive exactly the same data as sent by the sender.
- Data must not be changed in transit i.e., if someone sends a message “Hi”, then the receiver must receive “Hi”.
- That is, it must be exactly the same data as sent by the sender.
- Any addition or subtraction of data during transit would mean the integrity has been compromised.
- Example are: Data modification attacks and Man-in-the-middle (MITM) attack.
- **Solution: Use of hashing algorithms i.e., SHA256.**

Approaches for effective cyber security

3: Availability

- Availability implies that information should be available to authorized parties whenever required.
- It is essential to have plans and procedures in place to prevent or mitigate data loss as a result of a disaster.
- A disaster recovery plan must include unpredictable events such as natural disasters and fire.

Approaches for effective cyber security

3: Availability

- **Solution:** A **routine backup job** is advised in order to prevent or minimize total data loss from such occurrences.
- Also, extra security equipment or software such **as firewalls and proxy servers** can guard against downtime and unreachable data due to malicious actions such as denial-of-service (DoS) attacks and network intrusions (i.e., malware).
- Example -Attacks that affect Availability: DoS and DDoS attacks (i.e., Hello flood attack)

References

- Zero Trust Model: Can Trusting No One Be the Answer to Your Cybersecurity Problems (Information available at: https://www.ekransystem.com/en/blog/zero-trust-security-model
- Textbook: Penetration Testing: A Hands-on Introduction to Hacking by Georgia Weidman
- Textbook: Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives by Sunit Belapure and Nina Godbole
- Michael E. Whitman and Herbert J. Mattord, Principles of Information Security, (2e), Thomson Learning, 2007
- psu.edu
- Pen test. Information available at: https://www.imperva.com/learn/application-security/penetration-testing/

❑ Identifying, Analyzing, and Evaluating Cyber risks. Information available at: https://www.securityforum.org/uploads/2017/05/ISF_c07.pdf