Department of CSE, ISE, CSE[AI & ML], CSE[Cy Sec]

Global Alumni Connect – 3

TOPIC

Guardians of the Digital Realm: Exploring Cybersecurity in the Age of Smart Tech

Mr. Ankit Adiga

Senior Quality Development Specialist
CARIAD SE, Volkswagen Group
Erlangen, Germany

Graduated in 2012 (CSE)

15th November 2024   **1:30 PM**

Link for joining the session
https://meet.google.com/vsv-mzhu-yti

Staff & Students

Dr. D G Anand
PRINCIPAL

GLOBAL ALUMINI CONNECT-3

Online Workshop

On

Guardians of the Digital Realm: Exploring Cyber Security in the Age of Smart Tech

Organized by Department of CSE & ISE,

APS College of Engineering.

Venue: CSE Seminar Hall (Online)

APS College of Engineering

Date: 28th October 2024

GLIMPSES OF WEBINAR:

Guardians of the Digital Realm: Exploring Cyber Security in the Age of Smart Tech

No of registered students: 88

No of students attended: 72

Classes and section – 5th SEM CSE and 5th SEM ISE.

Details of resource person:

Mr. Ankit Adiga
Senior Quality Development Specialist CARIAD SE,
Volkswagen Group, Erlangen, Germany.

Brief report of the Alumni Connect-3

Introduction

The rise of smart technology has transformed the way we live, work, and interacts with the world. From smart phones and smart homes to wearables, autonomous vehicles, and industrial systems, smart tech is everywhere, creating a more connected and efficient world. However, with this increased connectivity comes an expanded attack surface for cyber threats, making cyber security a paramount concern.

Key Requirements for Cyber Security in the age of Smart Tech

Scalability of Security Measures: The sheer number of IoT devices being deployed across the world creates scalability issues. Each device may need to be individually secured, and ensuring that large networks of devices remain safe over time requires constant vigilance and updates.

Inconsistent Standards and Regulations: There is a lack of universal security standards for IoT devices, and regulations often lag behind technological advancements. Without clear guidelines, manufacturers and consumers alike struggle to understand the necessary security practices.

Device Lifecycle Management: Smart devices often have long lifecycles, but security updates may not be regularly provided. Many devices, especially in the IoT space, may continue to be used long after they become obsolete or unsupported, making them attractive targets for cybercriminals.

Vulnerabilities in Communication Channels: Smart devices typically communicate over networks, including Wi-Fi, Bluetooth, or 5G. These communication channels can be intercepted or hijacked if not properly secured, leading to man-in-the-middle attacks or data breaches.

The Future of Cyber security in Smart Tech

As the adoption of smart technology continues to grow, so too will the challenges of securing these devices and systems. The future of cyber security in the age of smart tech will likely involve:

Advanced Encryption Standards: The development and implementation of quantum-resistant encryption methods as quantum computing advances.

Unified Security Frameworks: Industry-wide collaboration to create standardized security protocols and regulations for IoT and smart devices.

Increased Automation: More reliance on AI and automation to secure devices, detect threats, and respond to attacks faster and more efficiently.

Privacy-First Design: A greater emphasis on privacy in the design of smart devices, ensuring that data is collected and used responsibly and securely.
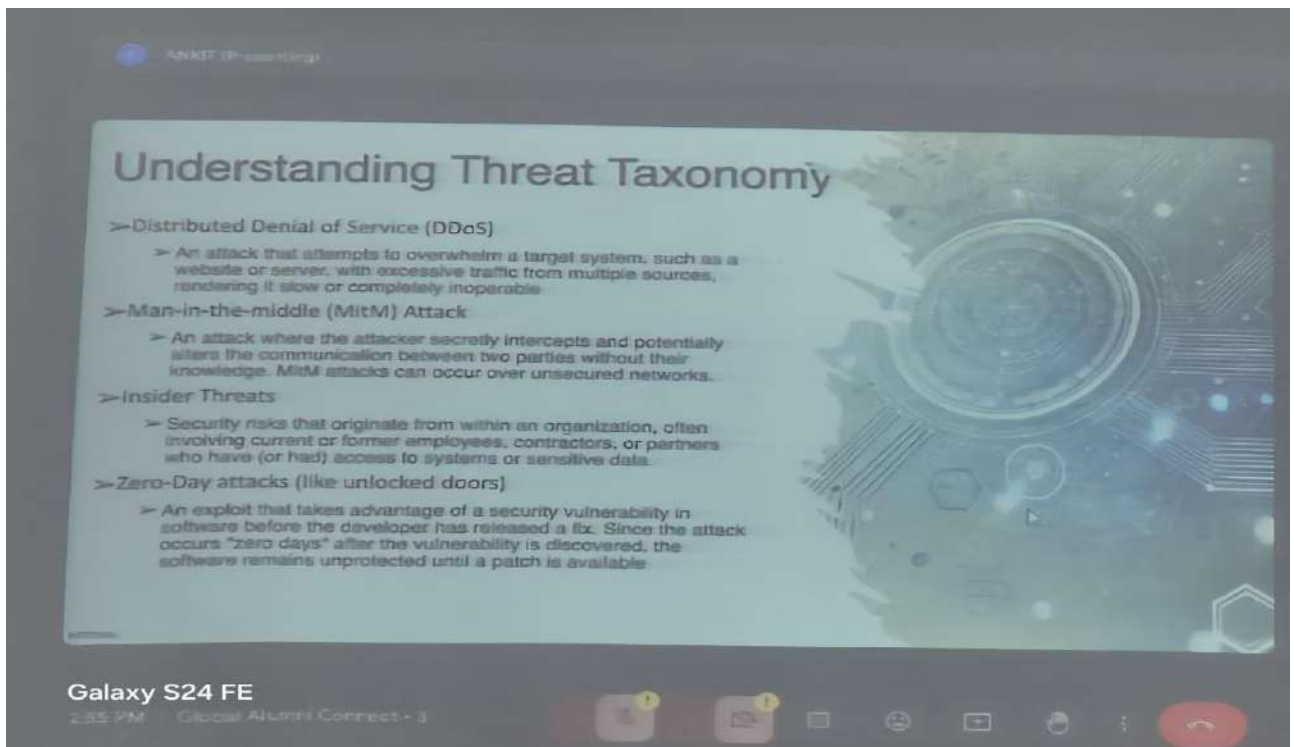
Conclusion

The proliferation of smart technology offers unprecedented benefits but also introduces new cyber security challenges that require careful attention. As we continue to integrate more intelligent devices into our daily lives and critical infrastructure, it's essential to adopt a proactive and holistic approach to cyber security. Manufacturers, developers, and users must work together to ensure that smart technology remains secure, reliable, and trustworthy in the face of evolving cyber threats.

Photos of the Event: