

EE3220 System on Chip Design

Team Based Learning (TBL) on
Secure SoC Design & Wi-Fi Hacking

Prof Patrick HUNG and Ray CC CHEUNG

7 April 2025

Course Overview

- Lecture 1: Course Overview
- Lecture 2: Intro to Modern Microprocessor (CPU Architecture)
- Lecture 3: Embedded System Software (Software Architecture)
- Lecture 4: ARM Cortex-M4 (ARM Hardware)
- Lecture 5: From C to ARM Assembly (C Language, ARM Firmware)
- Lecture 6: Team Based Learning #1 (USB Firmware)
- Lecture 7: AAPCS (ARM Firmware)
- Lecture 8: Exceptions & Interrupts (ARM Firmware)
- Lecture 9: Intro to Verilog HDL & FPGA Design (HDL Design)
- Lecture 10: FPGA based SoC (FPGA based SoC)
- Lecture 11: SoC Integration & Emerging ISA (AMBA, RISC-V)
- Lecture 12: Team Based Learning #2 (Secure SoC Design & Wi-Fi Hacking)

Team-Based Learning

- Each Team functions as a Research Group
 - **COLLABORATING** with Other Members
 - Solving Real-World Problems
 - Competing Against Other Teams
- Healthy Academic Competition
 - Learning from **EACH OTHER'S STRENGTH**
 - Sharing Insights
 - Sharpening your Technical and Analytical Thinking
 - Learning How to Present

TBL: Secure SoC Design & Wi-Fi Security Hacking

WI-FI ROUTER SOC

Interfaces:

- Ethernet, Wi-Fi

Functions:

- Ethernet MAC
- Wi-Fi MAC
- Security Engine
- Switching & Routing

Examples:

- Broadcom BCM6750
- Broadcom BCM6764
- MediaTek MT7621



USB 3.0 WI-FI DONGLE SOC

Interfaces:

- USB 3.0, Wi-Fi

Functions:

- USB 3.0 MAC
- Wi-Fi- MAC
- Security Engine
- Data Buffering

Examples:

- Atheros AR9271,
- Realtek RTL8188EUS
- Realtek RTL8812AU



TBL: Secure SoC Design & Wi-Fi Security Hacking

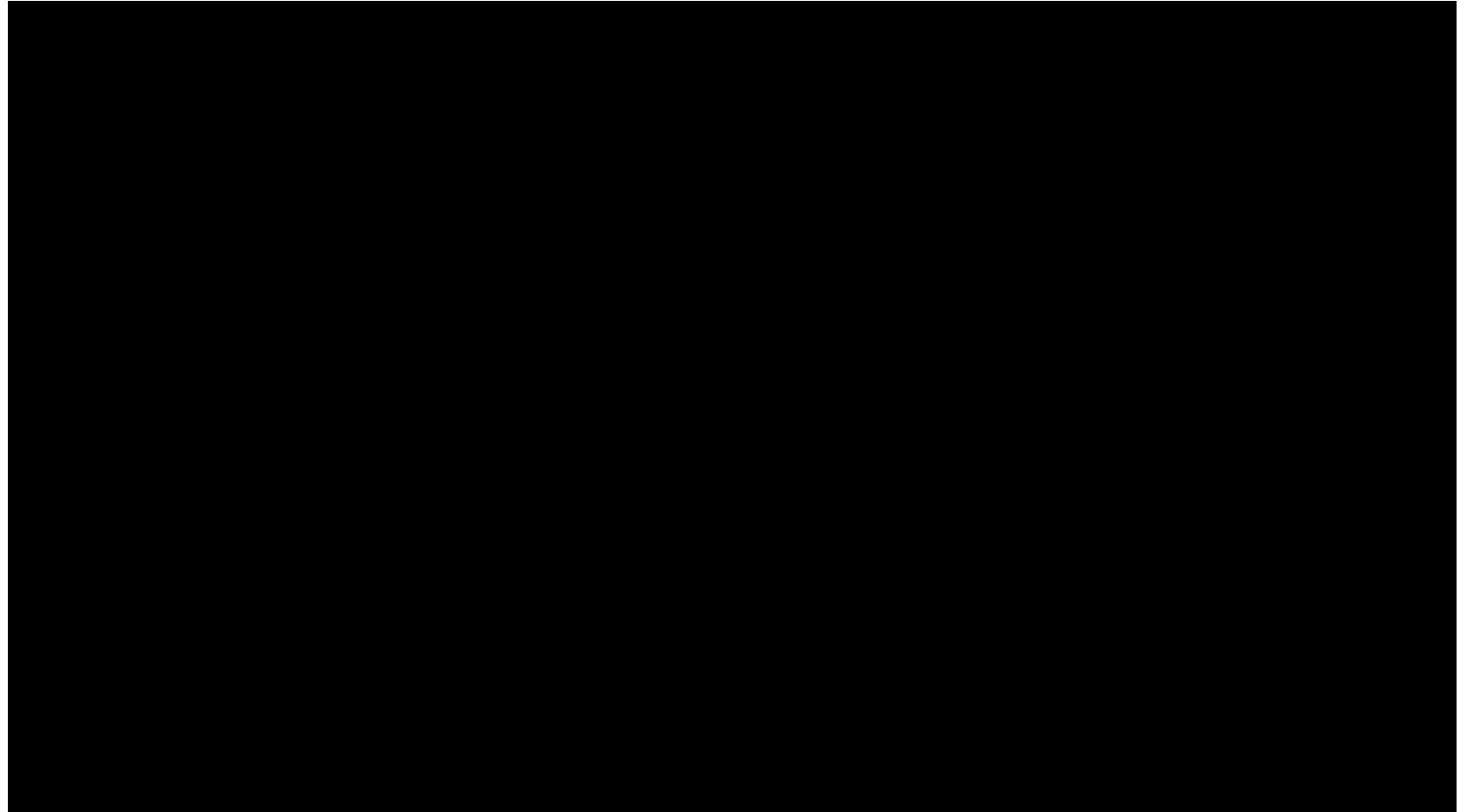
MONITOR
ENCRYPTED TRAFFIC
TO HACK WEP PASSWORD



ENCRYPTED TRAFFIC
WITH WEP PASSWORD

TBL: Secure SoC Design & Wi-Fi Security Hacking

- *Step 1:*
 - Listen to Video
- *Step 2:*
 - Read Documents
- *Step 3:*
 - Individual RAT
- *Step 4:*
 - Team RAT
- *Step 5:*
 - WEP Hacking
- *Step 6:*
 - Presentation



TBL: Secure SoC Design & Wi-Fi Security Hacking

- Step 1:
 - Listen to Video
- Step 2:
 - Read Documents
- Step 3:
 - Individual RAT
- Step 4:
 - Team RAT
- Step 5:
 - WEP Hacking
- Step 6:
 - Presentation

EE3220: Team-Based Learning Session 2 (Secure SoC Design & Wi-Fi Security Hacking)

1. Team-Based Learning: Secure SoC Design & Wi-Fi Security Hacking
 - 1.1 Overview

This team-based learning (TBL) session provides hands-on experience in secure SoC design and Wi-Fi security hacking. The session lasts 3 hours (from 3 to 6pm) and requires full participation from each team member to earn points.
 - 1.2 Session Objectives

By the end of this session, students should be able to:

 1. Identify the role of SoCs in Wi-Fi routers and USB dongles.
 2. Understand the security vulnerabilities of WEP encryption in Wi-Fi communication.
 3. Discuss the importance of ethical hacking.
 4. Conduct a hands-on hacking experiment to exploit WEP vulnerabilities.
 - 1.3 Team Structure

Each team consists of six students, each assigned a specific role:

 - Team Leader (1): Organizes the team, ensures collaboration, and communicates with the instructor. Works with the other team members to prepare a PowerPoint presentation.
 - Computing/Hacking Experts (2): Handle hands-on technical tasks such as setting up packet sniffing and cracking encryption.
 - Reviewers (2): Validate and cross-check results, ensuring accurate documentation of findings.
 - AI Specialist (1): Uses LLM tools such as DeepSeek or ChatGPT for research, troubleshooting, and optimizing strategies.

Important Rule: All six members must actively participate, or the team will receive no points.
 - 1.4 Session Flow
 - 1.4.1 Preparation (30 min)
 - Students review a short pre-recorded lecture (~15 min) on:
 - Basics of SoCs in Wi-Fi routers and USB dongles
 - WEP encryption and its weaknesses
 - Secure SoC design principles
 - Reading materials:
 - Review this document and some research papers.
 - 1.4.2 Readiness Assurance Test (RAT) (30 min)
 - Individual Quiz: Each student takes a RAT quiz to test pre-class knowledge.

7 April 2025 1 Revision 1.0

International Journal of Information Technology (IJIT) – Volume 4 Issue 6, Nov-Dec 2018

RESEARCH ARTICLE OPEN ACCESS

Ethical Hacking

Azhar Ushmani
Cyber Security
Western Governor University
Salt Lake City, Utah
USA

ABSTRACT
Hacking is common process which results in the breaching of one's privacy and confidential information. The weaknesses of a system or loopholes in a network are identified and private details are accessed. Therefore, hacking is also known as unauthorized intrusion ("What Is Hacking?" | Ethical Hacking"). However, hacking was not always perceived as theft and used for productive causes. Such type of hacking that involves good intentions is known as ethical hacking.
Keywords: Ethical Hacking, Hackers

I. DEFINING ETHICAL HACKING

The term hacking is divided into two types depending on the intention behind hacking process. The two types are white-hat hacking and black-hat hacking. According to CDN, white-hat hacking refers to ethical hacking which is performed with the target's agreement to discover system's vulnerability from a hacker's perspective. Such type of hacking is done to secure the system from black-hat hackers who have malicious intentions of stealing and exploiting personal information. The tools and tricks used to hack the system are the same for both types of hacking processes ("Cdn.tgtmedia.com"). Therefore, the white-hat and black-hat hackers think alike. The difference between these two categories is the idea or purpose behind hacking any system. If this purpose is to serve greater good like reducing security issues and stabilize organizational systems, the hacker is known as an ethical hacker. On the other hand, hackers with malicious intentions of stealing personal details and hurting privacy are not considered as ethical hackers.

Ethical hacking is legal since it is performed after acquiring the target's consent. According to CDN, the process of ethical hacking confirms the claim of multiple vendors about the security of their products. The significance of ethical hacking is boundless since it comes in handy for protecting crucial systems, networks, and accounts from data thieves by thinking exactly like them. It provides full control to the information owner, detects system flaws, strengthens computer security, prevents system attacks, and respects

II. ETHICAL HACKERS AND THEIR PURPOSE

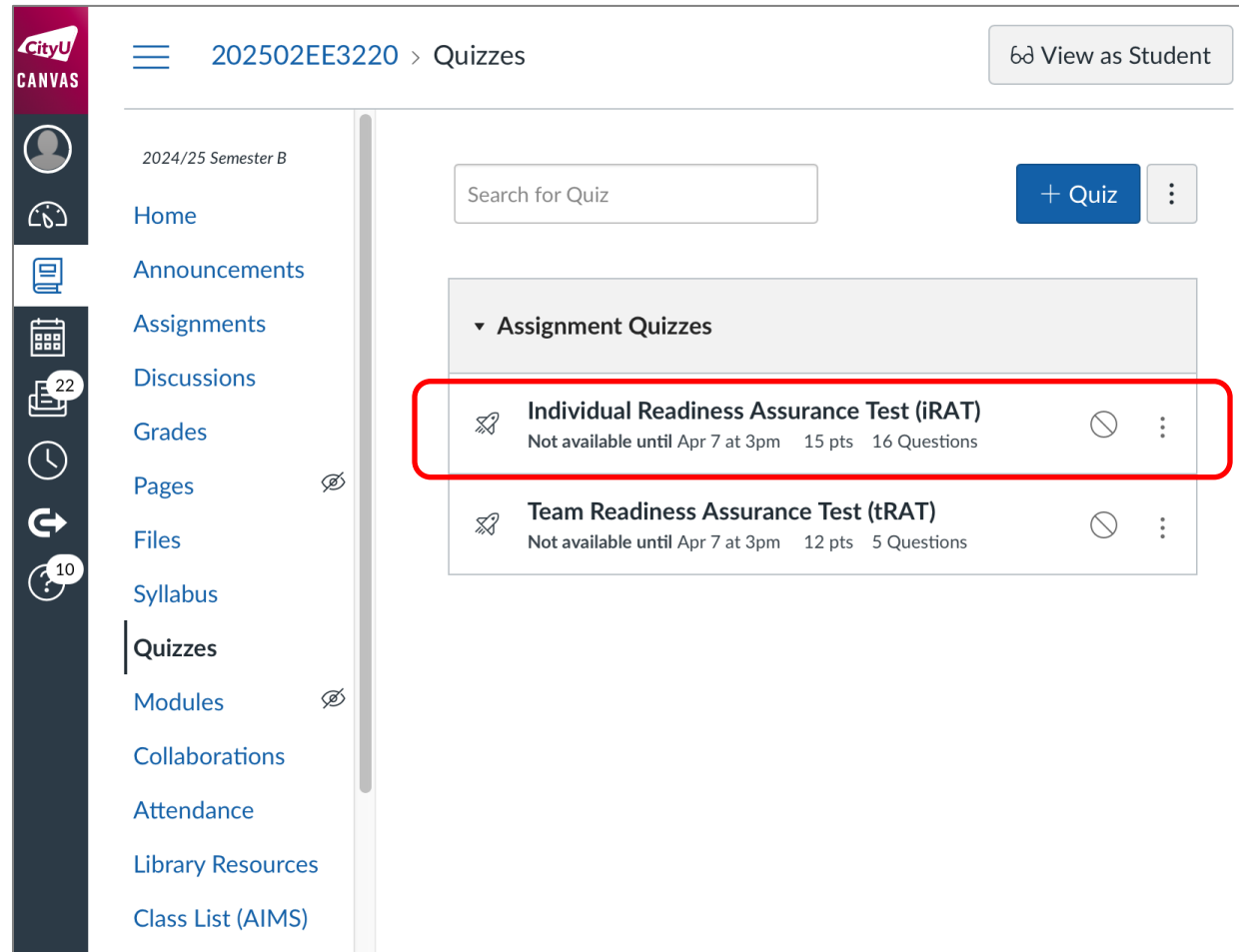
The people who specialize in ethical hacking process are known as ethical hackers. They are the professionals who hack into a system or network to locate possible faults, pitfalls, and vulnerabilities that may be exploited by black-hat hackers or crackers (Babbar, Jain and Kang). The skills and mindset of ethical hackers are equal to hackers with malicious intentions but they can be trusted. Ethical hackers are certified and authorized for performing hacking on target systems ("Certified Ethical Hacker - CEH Certification | EC-Council"). An ethical hacker has legal permission to access target's personal details and modify target system. The talents possessed by an ethical hacker can be used to limit cyber crime.

Along with the white-hat and black-hat hackers, another category of hackers was also discovered who work in close affiliation with ethical hackers yet face some social consequences. These hackers are known as gray-hat hackers who hack technical and network systems for good causes like helping organizations to fix security issues, but are unauthorized (Radziwill et al.). Gray-hat hackers implement ethical hacking but their unauthorized approach leads to lack of social acceptance. Ethical hackers are hired by agencies,

ISSN: 2454-5414 www.ijitjournal.org Page 1

TBL: Secure SoC Design & Wi-Fi Security Hacking

- *Step 1:*
 - Listen to Video
- *Step 2:*
 - Read Documents
- *Step 3:*
 - Individual RAT
- *Step 4:*
 - Team RAT
- *Step 5:*
 - WEP Hacking
- *Step 6:*
 - Presentation



TBL: Secure SoC Design & Wi-Fi Security Hacking

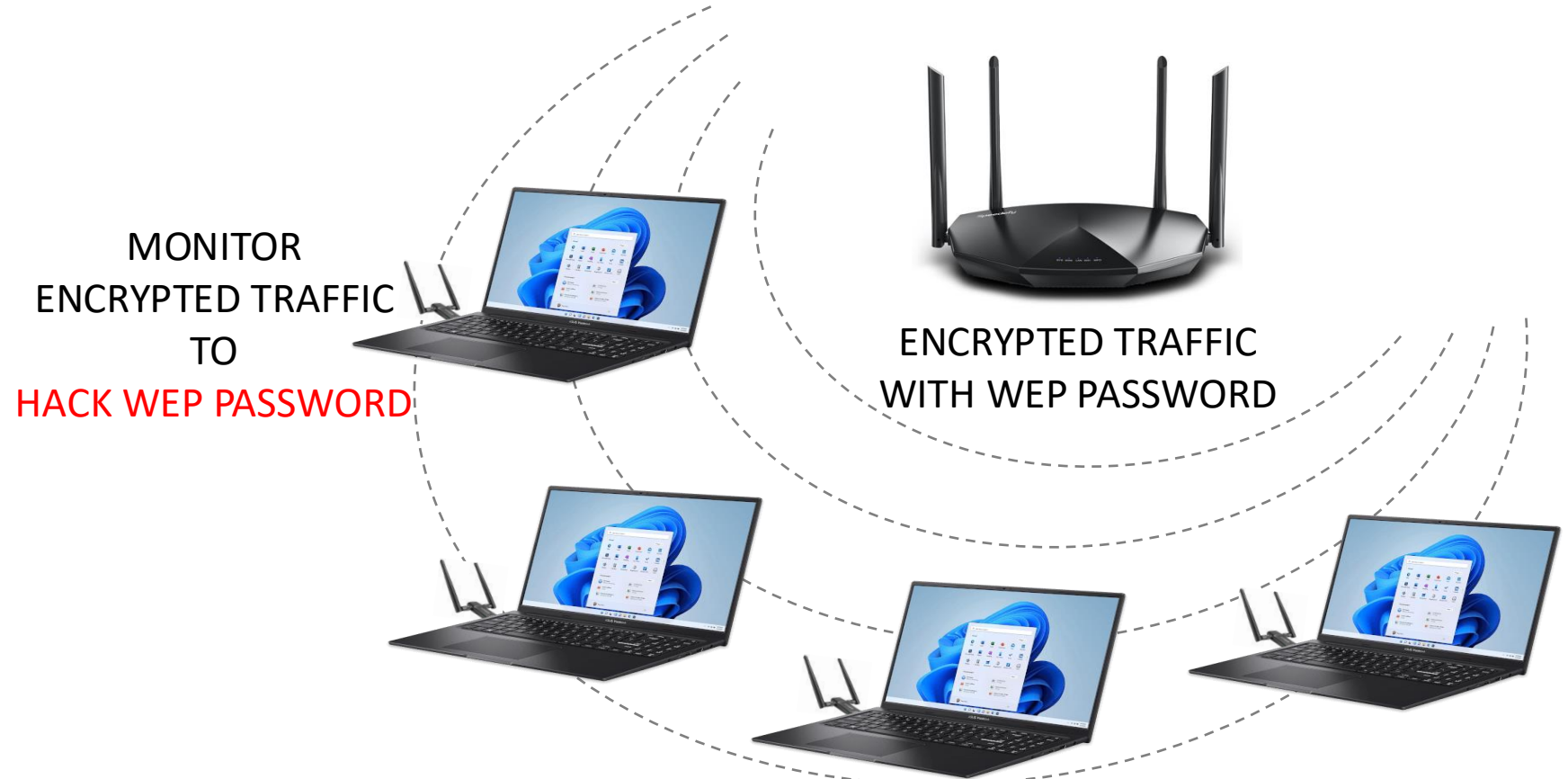
- *Step 1:*
 - Listen to Video
- *Step 2:*
 - Read Documents
- *Step 3:*
 - Individual RAT
- *Step 4:*
 - Team RAT
- *Step 5:*
 - WEP Hacking
- *Step 6:*
 - Presentation

The screenshot shows the Canvas LMS interface for course 202502EE3220. The left sidebar contains navigation links: Home, Announcements, Assignments, Discussions, Grades, Pages, Files, Syllabus, Quizzes (selected), Modules, Collaborations, Attendance, Library Resources, and Class List (AIMS). The main content area displays the 'Quizzes' page with a search bar and a '+ Quiz' button. Under the 'Assignment Quizzes' section, two quizzes are listed: 'Individual Readiness Assurance Test (iRAT)' and 'Team Readiness Assurance Test (tRAT)'. The 'tRAT' quiz is highlighted with a red box. It is noted as 'Not available until Apr 7 at 3pm', has 12 pts, and 5 Questions.

Quiz Name	Availability	Points	Questions
Individual Readiness Assurance Test (iRAT)	Not available until Apr 7 at 3pm	15 pts	16 Questions
Team Readiness Assurance Test (tRAT)	Not available until Apr 7 at 3pm	12 pts	5 Questions

TBL: Secure SoC Design & Wi-Fi Security Hacking

- *Step 1:*
 - Listen to Video
- *Step 2:*
 - Read Documents
- *Step 3:*
 - Individual RAT
- *Step 4:*
 - Team RAT
- *Step 5:*
 - WEP Hacking
- *Step 6:*
 - Presentation



TBL: Secure SoC Design & Wi-Fi Security Hacking

- *Step 1:*
 - Listen to Video
- *Step 2:*
 - Read Documents
- *Step 3:*
 - Individual RAT
- *Step 4:*
 - Team RAT
- *Step 5:*
 - WEP Hacking
- *Step 6:*
 - Presentation



TBL: Secure SoC Design & Wi-Fi Security Hacking

- Zoom Link:
 - <https://cityu.zoom.us/j/3735797590>