Computer Security

Syllabus

Chi-Yu Li (2023 Fall)
Computer Science Department
National Yang Ming Chiao Tung University

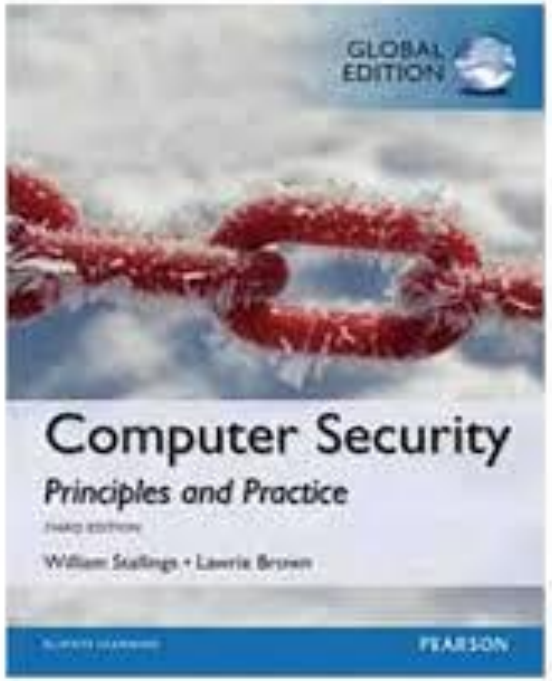
Course Information

- Course Name: Computer Security
  - Lectures: Mabc
  - Location: TB435
- Instructor: Chi-Yu Li (李奇育)
  - Email: chiyuli@cs.nctu.edu.tw
  - Office: EC529
  - Office hours: by appointment
- TA: Ping-Tsan Liu (劉炳瓚)
  - Email: meow.cs07@nycu.edu.tw

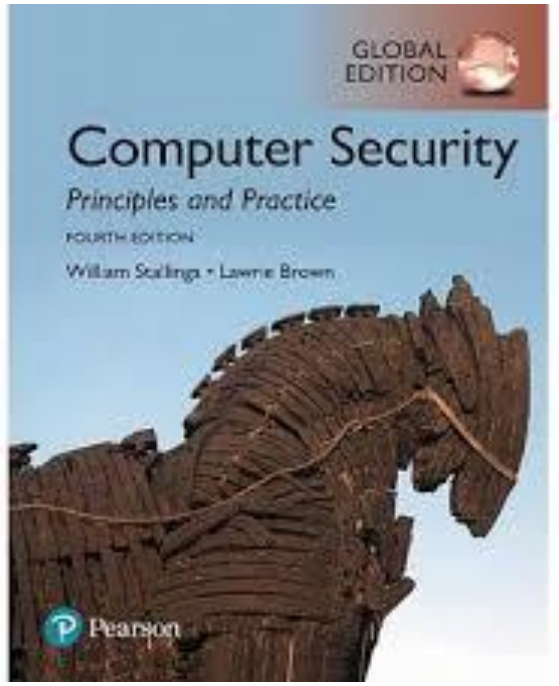
Textbook

- Computer Security: Principles and Practice
  - William Stallings and Lawrie Brown, Pearson

3rd Global Edition, 2014



4th Global Edition, 2018

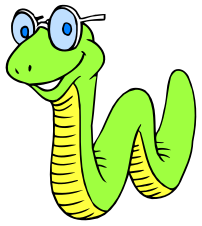


What this Course is About …

- Part I: an introduction to a variety of topics in computer security
  - Computer security technology and principles
    - Cryptographic tools, user authentication, access control
    - Database security, malicious software, DoS, intrusion, firewalls
  - Software and system security
    - Buffer overflow, software security, OS security, cloud and IoT security
  - Network security
    - Internet security protocols and applications
    - Wireless and cellular network security

Honeypots

Virus



Worm

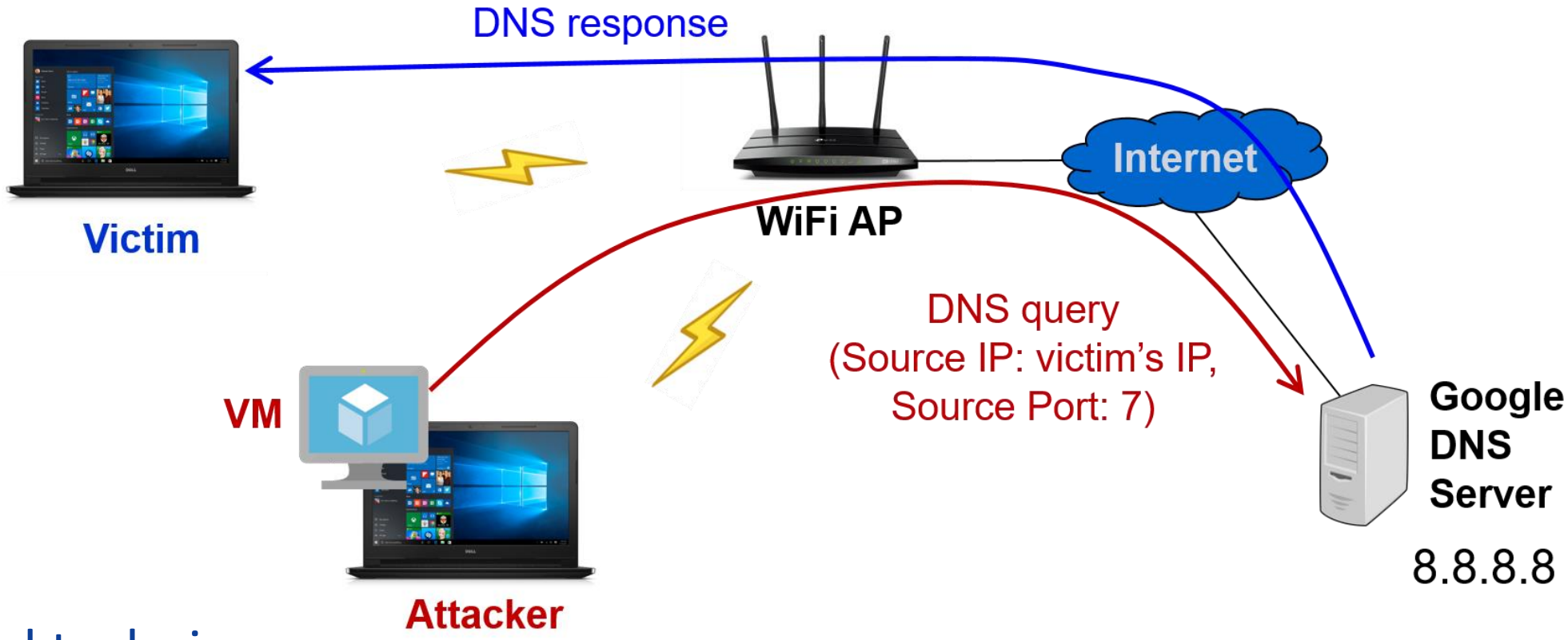
What this Course is About … (Cont.)

- Part II: a training of hand-on skills in computer security
  - Two of the following three projects
    - Project 1: Network security
    - Project 2: Wireless network security
    - Project 3: System (Linux) security

Projects

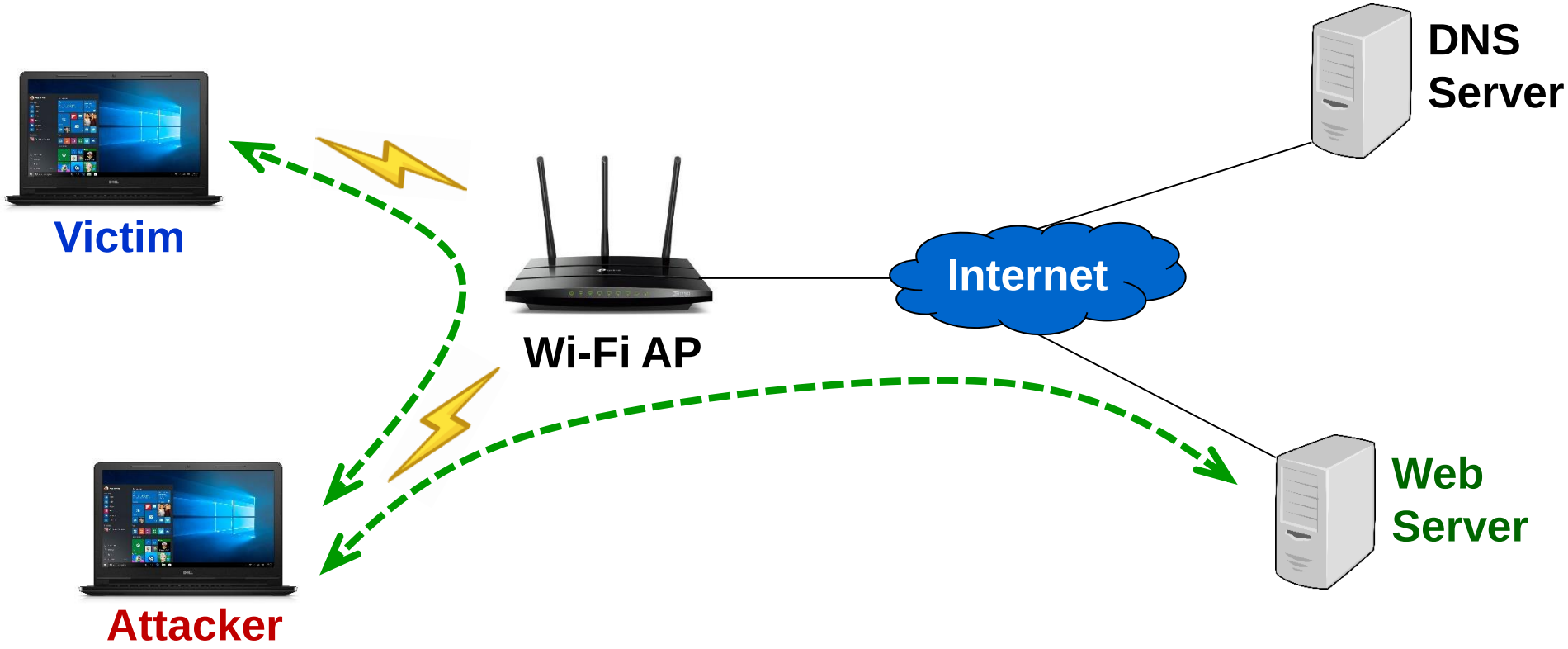
- Project 1: DNS Reflection and Amplification Attacks
- Project 2: Phishing Attacks in Wi-Fi Networks
- Project 3: Worms Replication through SSH and Its Detection

Project 1: DNS Reflection and Amplification Attacks



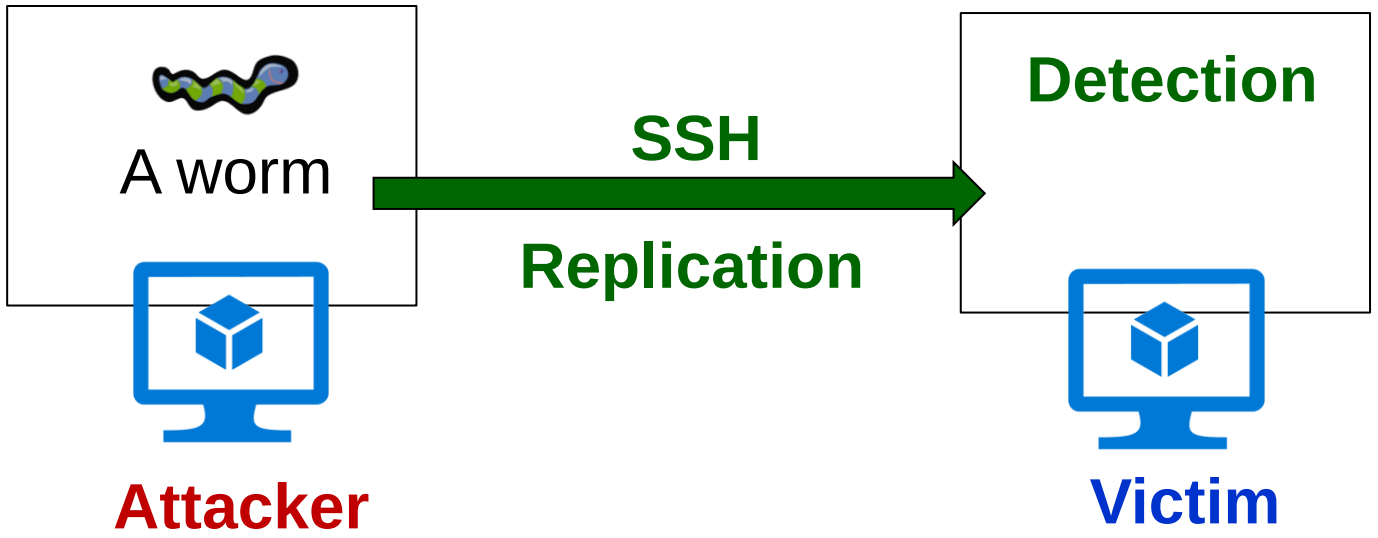
- Learned techniques
  - (1) Raw socket programming; (2) IP packet spoofing; (3) packet tracing; (4) DNS query fabricating

Project 2: Phishing Attacks in Wi-Fi Networks



- Learned techniques
  - (1) Wi-Fi packet tracing; (2) ARP spoofing; (3) DNS spoofing; (4) MITM attack

Project 3: Worms Replication through SSH and Its Detection



- Learned techniques
  - (1) System login with public key authentication; (2) analysis of abnormal processes on Linux; (3) routine task scheduling on Linux

Tentative Schedule

Phase I

- Overview
- Denial-of-Service (DoS) attacks
- Cryptographic tools
- User authentication
- Wireless network security

Phase II

- Access control
- Internet authentication applications
- Malicious software
- Midterm Exam
- Buffer overflow
- Software security

Phase II

Phase III

- Database and data center security
- Intrusion detection
- Firewalls and intrusion prevention system
- OS security
- Cloud and IoT security
- Internet security protocols and standards
- Cellular network security
- Final Exam

How will We Proceed?

- I will not check attendance (no roll call)
- You can
  - raise questions anytime
  - feel free to give me feedback and suggestions
- Course Policies
  - No late turn-in accepted for credit!
  - No makeup exam! No cheating!
  - Homework: Discussion is allowed, but collaboration/plagiary/copy is prohibited

Workload & Grading Policies

- Projects: 40%
- Midterm exam: 30%
- Final exam: 30%

Why is Cyber Security so Important?

- Most computing devices are network-connected
  - All have risks: attacks from the network/Internet

Servers

Cyber (Network) Attack ➔ $1 trillion US dollars in Global Losses

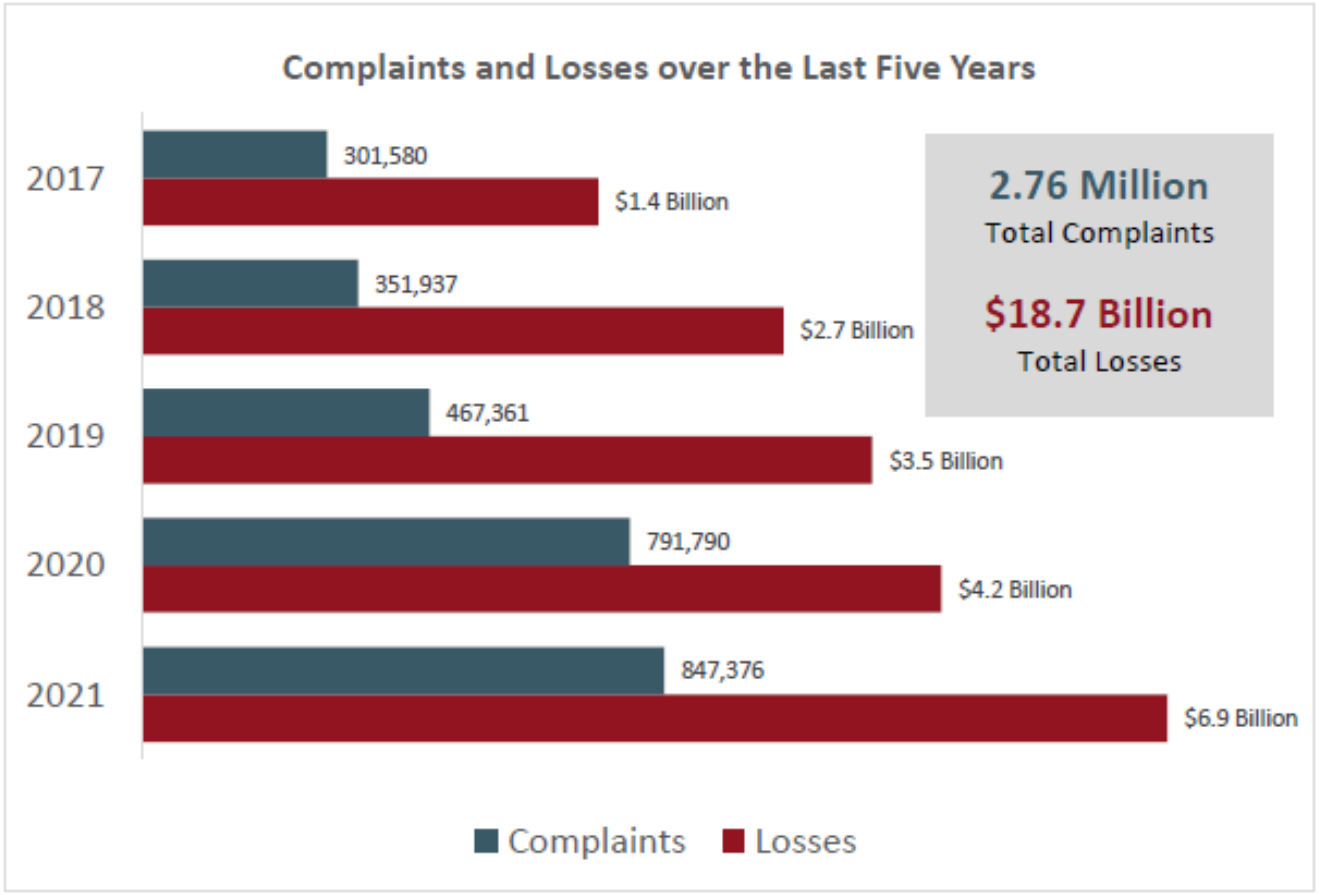
from US CSIS (Center for Strategic and International Studies) 2020 Report

Why are Cyber Attacks so Popular?

- High returns at low risk and low cost
  - Low cost: Attacks require only network-connected devices; large-scale attacks
  - Low risk: difficult to be traced back; IP can be hidden or Botnet
  - Returns >> Cost
- Two major attack types
  - Social engineering
    - Tricking a user into granting access
  - Vulnerability Exploitation
    - Taking advantage of a design/implementation/operational flaw to gain access

IC3 Complaint Statistics

- IC3 has received an average of 552,000 complaints per year

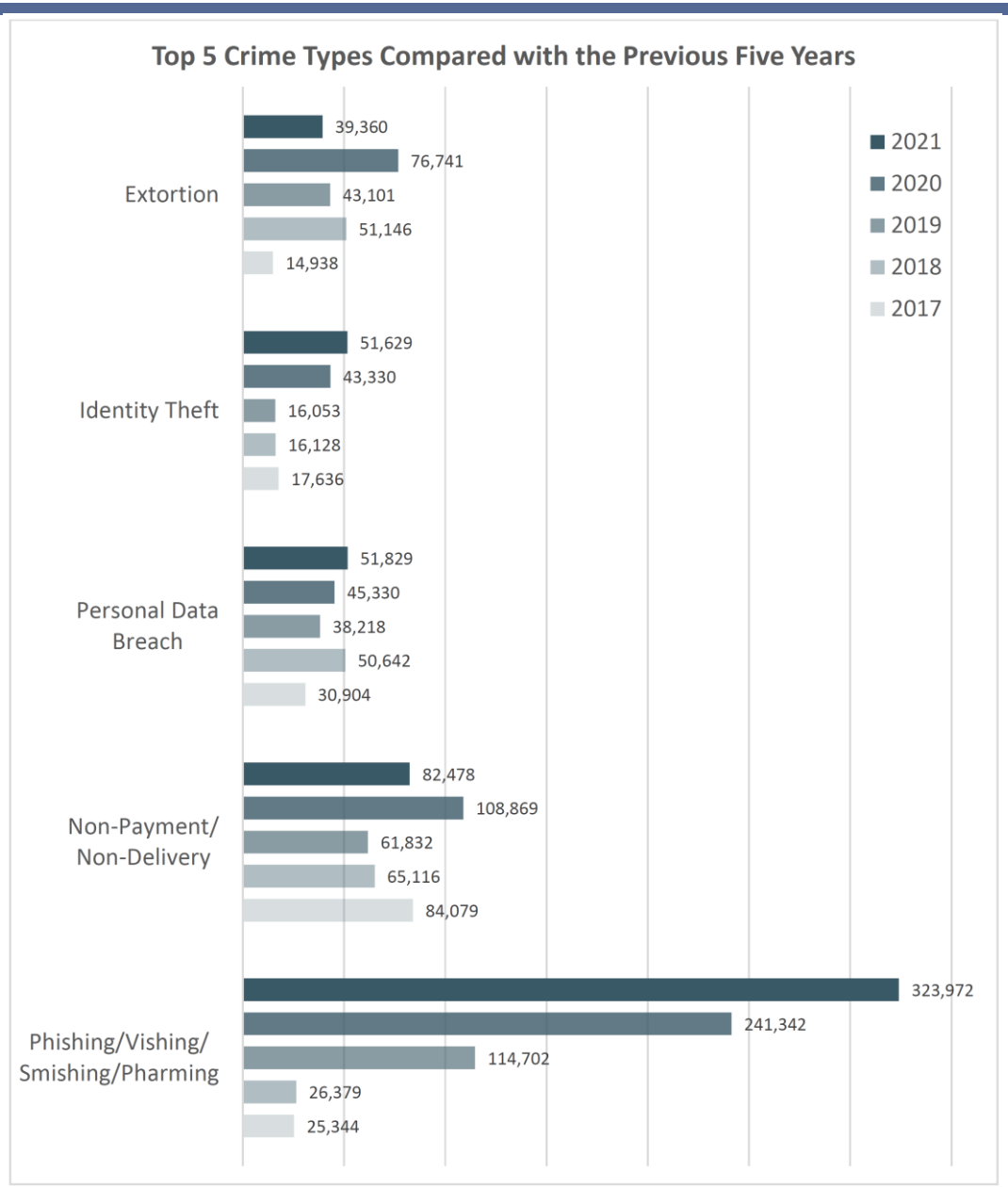


The FBI's IC3 (Internet Crime Complaint): providing the American public with a direct outlet to report cyber crimes to the FBI; it analyzes and investigates the reporting to track the trends and threats from cyber criminals and then share this data.

Source: "FBI Internet Crime Report," IC3 Annual Report 2021

Type 5 Crime Type Comparison

- Extortion: obtaining benefits through the act of process of persuading someone forcefully
- Vishing: Voice phsihing
- Smishing: SMS phishing



Source: “FBI Internet Crime Report,” IC3 Annual Report 2021

Threats Overviews for 2021

- Business Email Compromise (BEC)
- Confidence Fraud / Romance Scams
- Cryptocurrency
- Ransomware
- Tech Support Fraud

Source: “FBI Internet Crime Report,” IC3 Annual Report 2021

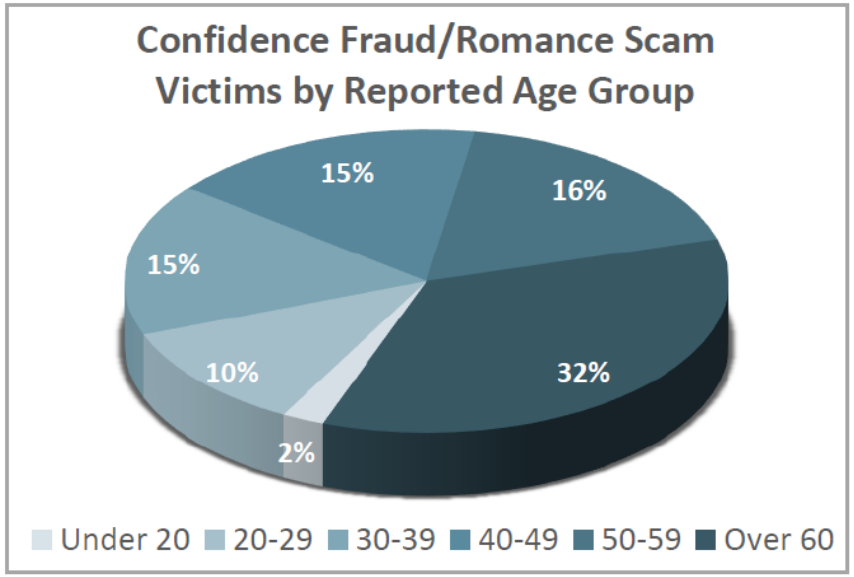
Business Email Compromise (BEC)

- In 2021, the IC3 received 19,954 Business Email Compromise (BEC)/ Email Account Compromise (EAC) complaints
  - Losses at nearly $2.4 billion
- BEC/EAC: a sophisticated scam targeting both businesses and individuals performing transfers of funds
  - frequently happening when an attacker compromises legitimate business email accounts through social engineering or computer intrusion techniques
- New BEC/EAS scheme from the increase of telework or virtual meetings
  - Compromising an employer or financial director's email
  - Using the email to request employees to participate in virtual meeting platforms
  - Inserting a still picture of the CEO with no audio, or a "deep fake" audio with claiming their audio/video was not working properly
  - Using the virtual meeting to directly instruct employees to initiate wire transfers

Source: "FBI Internet Crime Report," IC3 Annual Report 2021

Confidence Fraud / Romance Scams

- In 2021, the IC3 received reports from 24,299 victims
  - More than $956 billion
- Encompassing those designed to pull on a victim's "heartstrings"
  - frequently happening when a criminal adopts a fake online identity to gain a victim's affection and confidence
  - Using the illusion of a romantic or close relationship to manipulate and/or steal from the victim
- Many complaints from victims of online relationships resulting in
  - Sextortion: being threatened to distribute your private and sensitive material if their demands are not met
  - Investment scams: being pressured into investment opportunities, especially using cryptocurrency



Source: "FBI Internet Crime Report," IC3 Annual Report 2021

Cryptocurrency

- In 2021, the IC3 received reports from 34,202 complaints
  - involving the use of some type of cryptocurrency, such as Bitcoin, Ethereum, Litecoin, or Ripple
  - Reported loss: 0.24 B in 2020 → 1.6 B in 2021 (7 times)
- Cryptocurrency is becoming the preferred payment method for all types of scams
  - Cryptocurrency ATMs are popping up everywhere
  - Cryptocurrency support impersonators
    - Owners are alerted of an issue with their crypto wallet
    - Being convinced to either give access to their crypto wallet
    - Or, transfer the contents of their wallet to another wallet
  - Many victims of Romance scams are pressured into investment opportunities

Source: “FBI Internet Crime Report,” IC3 Annual Report 2021

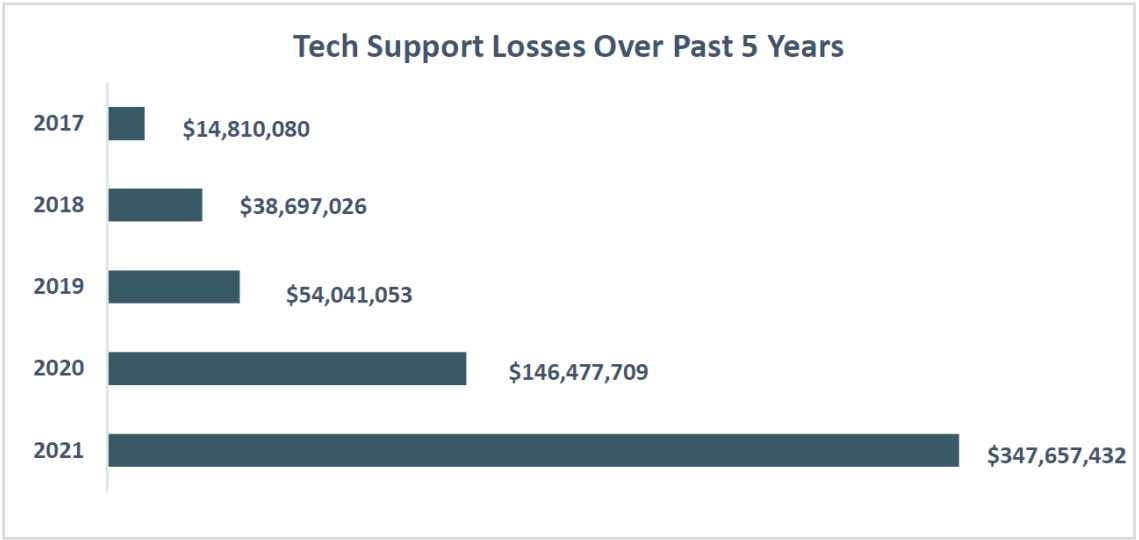
Ransomware

- In 2021, the IC3 received 3,729 complaints
  - Reported loss: more than $49.2 million
- Ransomware: a type of malicious software, or malware, that encrypts data on a computer, making it unusable
  - A malicious cyber criminal holds the data hostage until the ransom is paid
- Ransomware tactics and techniques continued to evolve
  - Phishing emails
  - Remote Desktop Protocol (RDP) exploitation
  - etc.
- Once a ransomware threat actor has gained code execution on a device or network access, they can deploy ransomware

Source: “FBI Internet Crime Report,” IC3 Annual Report 2021

Tech Support Fraud

- In 2021, the IC3 received 23,903 complaints from 70 countries
  - Reported loss: more than $347 million
- Tech Support Fraud: a criminal claiming to provide customer, security, or technical support or service defraud unwitting individuals
  - Criminals: posing as support or service representatives offering to resolve such issues as a compromised email or bank account, a virus on a computer, or a software license renewal
  - Victims: being directed to make wire transfers to overseas accounts or purchase large amounts of prepaid cards



Source: “FBI Internet Crime Report,” IC3 Annual Report 2021

Ghost Calls from Operational 4G Call Systems: IMS Vulnerability, Call DoS Attack, and Countermeasure

Yu-Han Lu, **Chi-Yu Li**, Yao-Yu Li, Sandy Hsin-Yu Hsiao, Wei-Xun Chen

Department of Computer Science
National Yang Ming Chiao Tung University

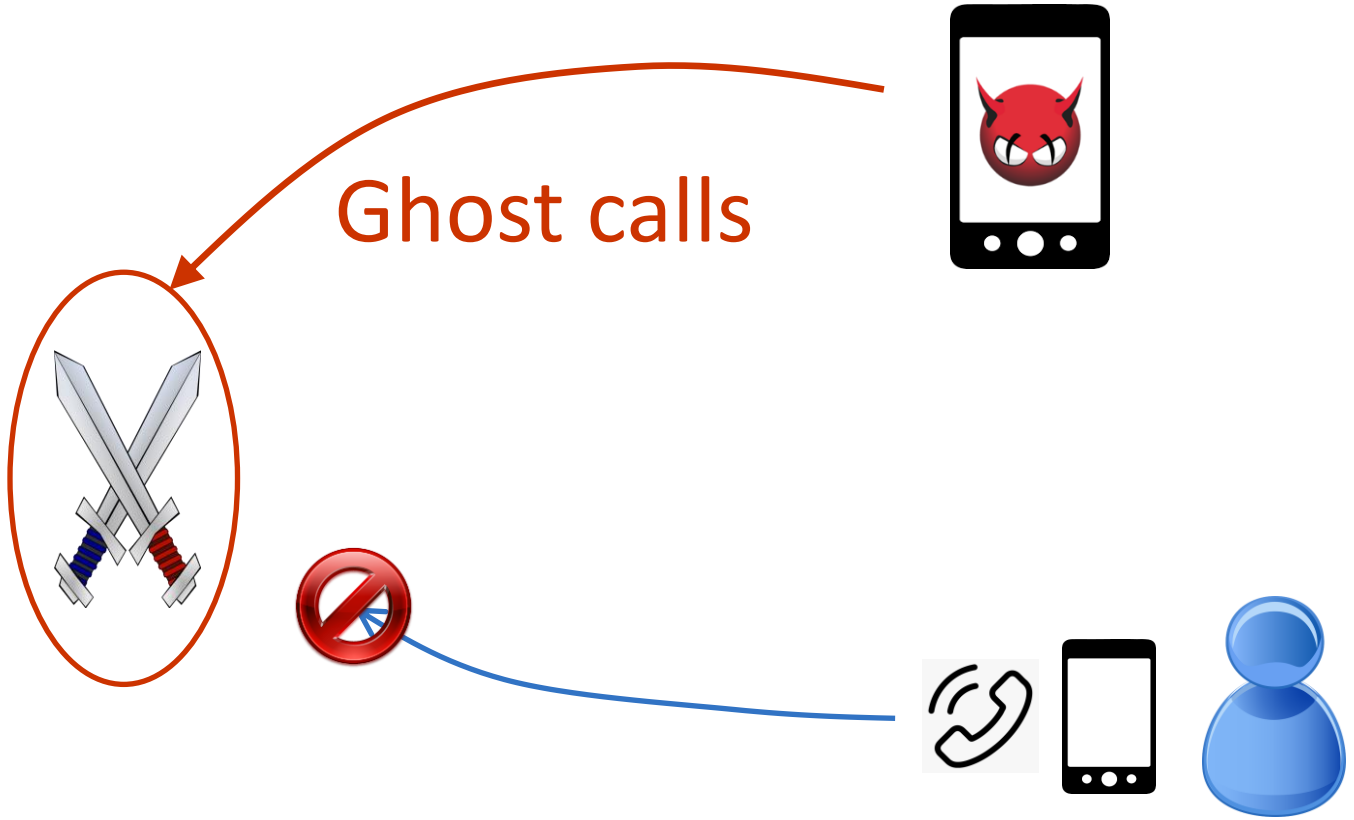
Tian Xie, Guan-Hua Tu

Department of Computer Science and Engineering
Michigan State University

No one is calling you.

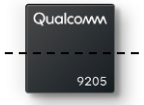
Is it always the case?

Probably, you are under attack.



Why May It Happen?

Former Voice Services



Circuit-switched voice

- ❑ Major call operations are hidden in the hardware modem

4G Voice Services

Packet-switched voice

- ❑ VoLTE (Voice over LTE) and VoWi-Fi (Voice over Wi-Fi)
- ❑ **VoWi-Fi**: major call operations are done by the mobile software ➔ *larger attack surface*

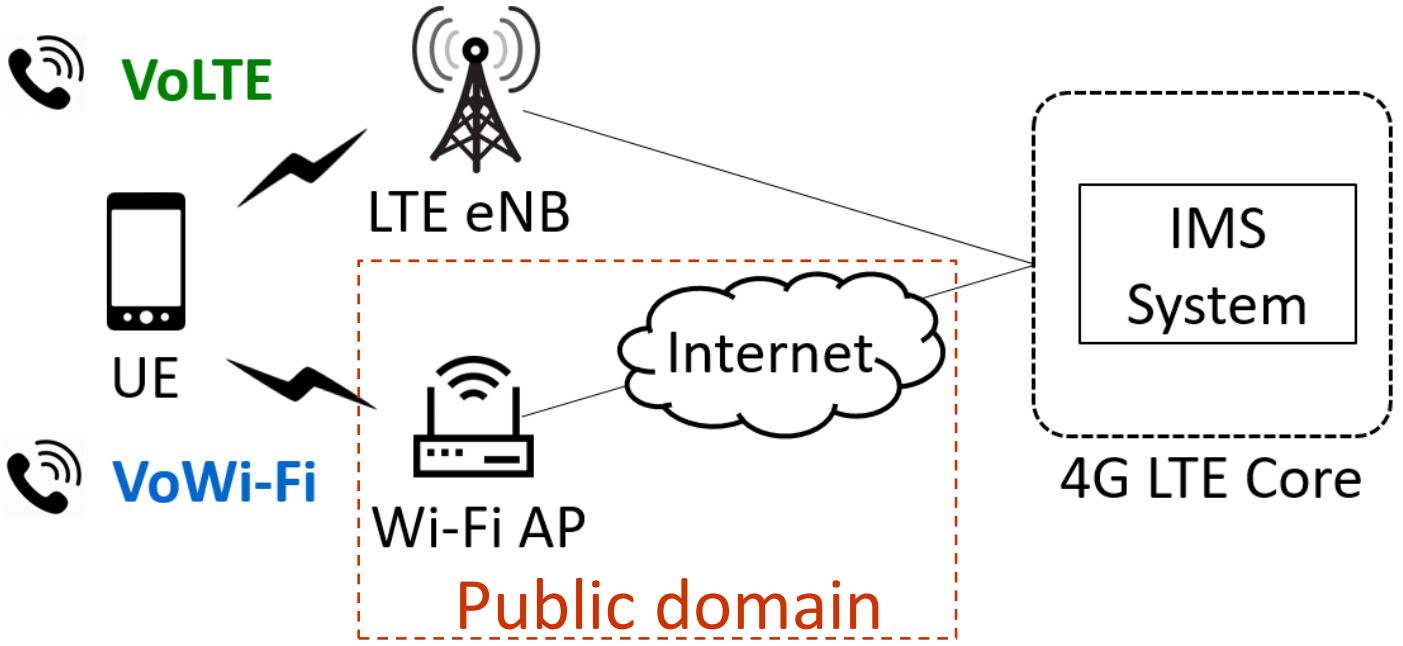
Why VoWi-Fi (aka WiFi Calling)?

- A HD voice service
  - Making and receiving calls over a Wi-Fi network

Source: https://u.com.my/plans/data-services/wifi-calling

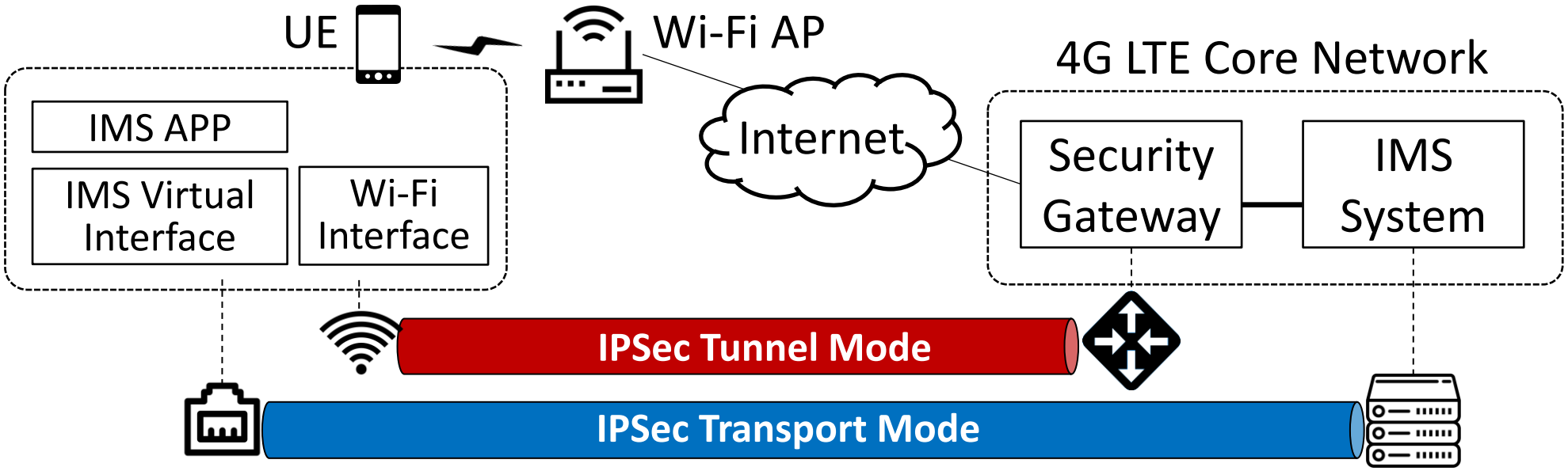
4G Voice Services from IMS System

- IMS (IP Multimedia Subsystem) supports multimedia services
  - Call operation: signaling (SIP) and voice delivery (RTP)

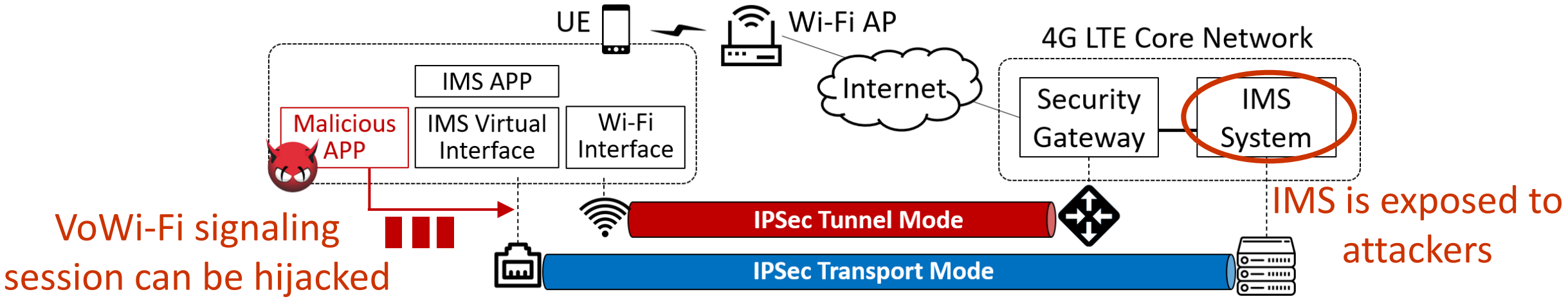


VoWi-Fi with IPSec Protection

- IPSec protection over VoWi-Fi traffic traversing public domain



However, they can be hacked!!



Attacker can manipulate IMS call service operation

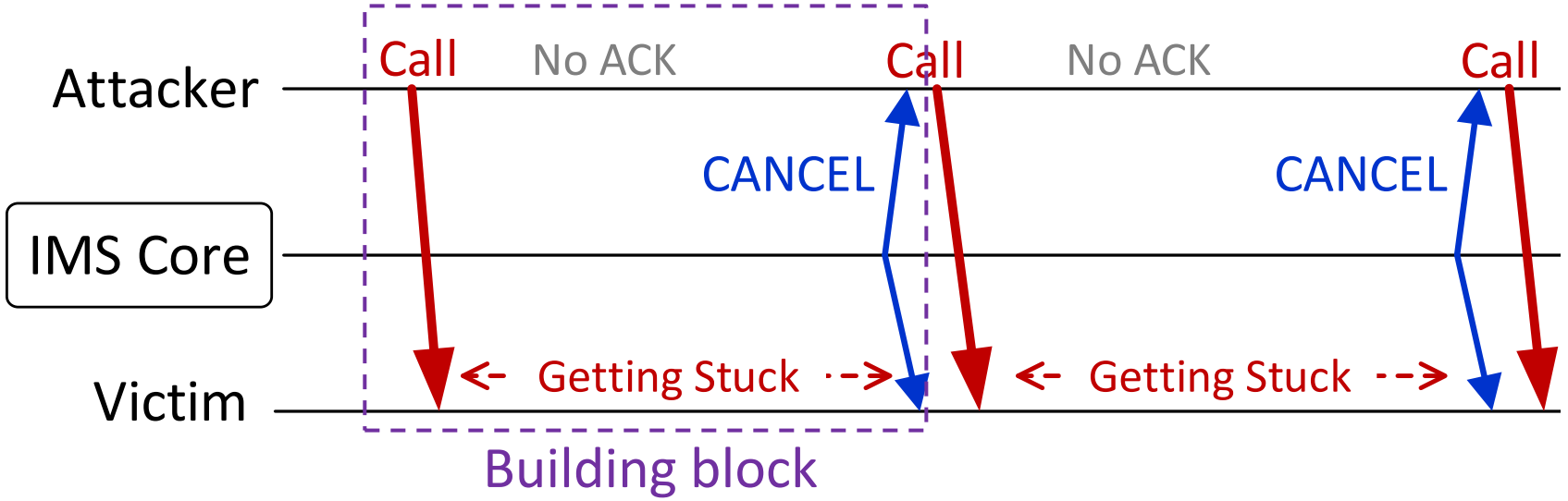
IMS vulnerabilities can be exposed!!

Three Security Vulnerabilities

- Hijacking VoWi-Fi signaling session
  - V1: no app-level data-origin authentication
- Manipulating IMS call service operation
  - V2: (call management) concurrent call attempts are allowed
  - V3: (call state machine) callee may get stuck

Validated in 2 Asia and 2 US carriers using
15 phone models with 7 phone brands

Stealthy Call DoS Attack



- Attack model
  - Attacker: only commodity smartphone and victim's phone number are required
  - Victim: using 4G call services
- Impact: up to 99.0% DoS time without user awareness in operational 4G networks

However, the DoS attack can work for
only **idle 4G users** with the **same carrier** as the attacker

When target users temporarily handover to 3G or
are with another different carrier, the attack fails!

Can we detect attackable phones remotely and silently?

Inferring Phone Status based on SIP Messages

- Phone status **(Attackable)**
  - Call states: **idle**, calling, and talking
  - Voice technologies: 3G, **VoWiFi**, and **VoLTE**
  - Inter-carrier or **intra-carrier**

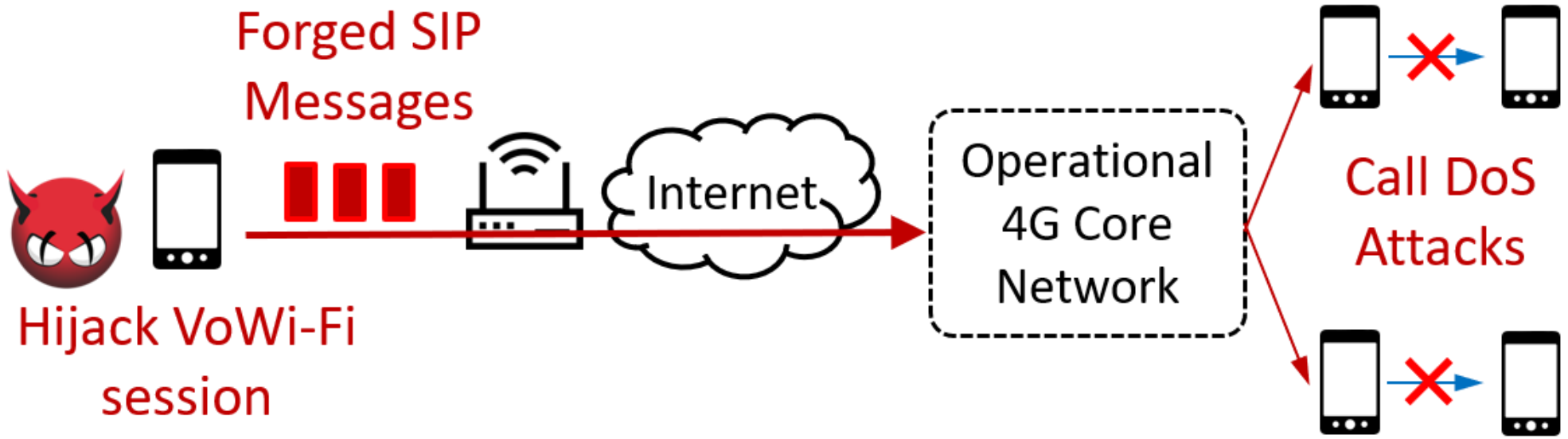
- Major idea: SIP message content/flow/interval may vary with different phone statuses
  - Their call attempts may be processed by different network entities/procedures

Each silent attack call can also detect the victim's phone status

Attack I

- Stealthy call Denial-of-Service (DoS) attack on personal phones
  - No ring tones to victims!!
  - 97.6% DoS time without user awareness

- Demo Scenario



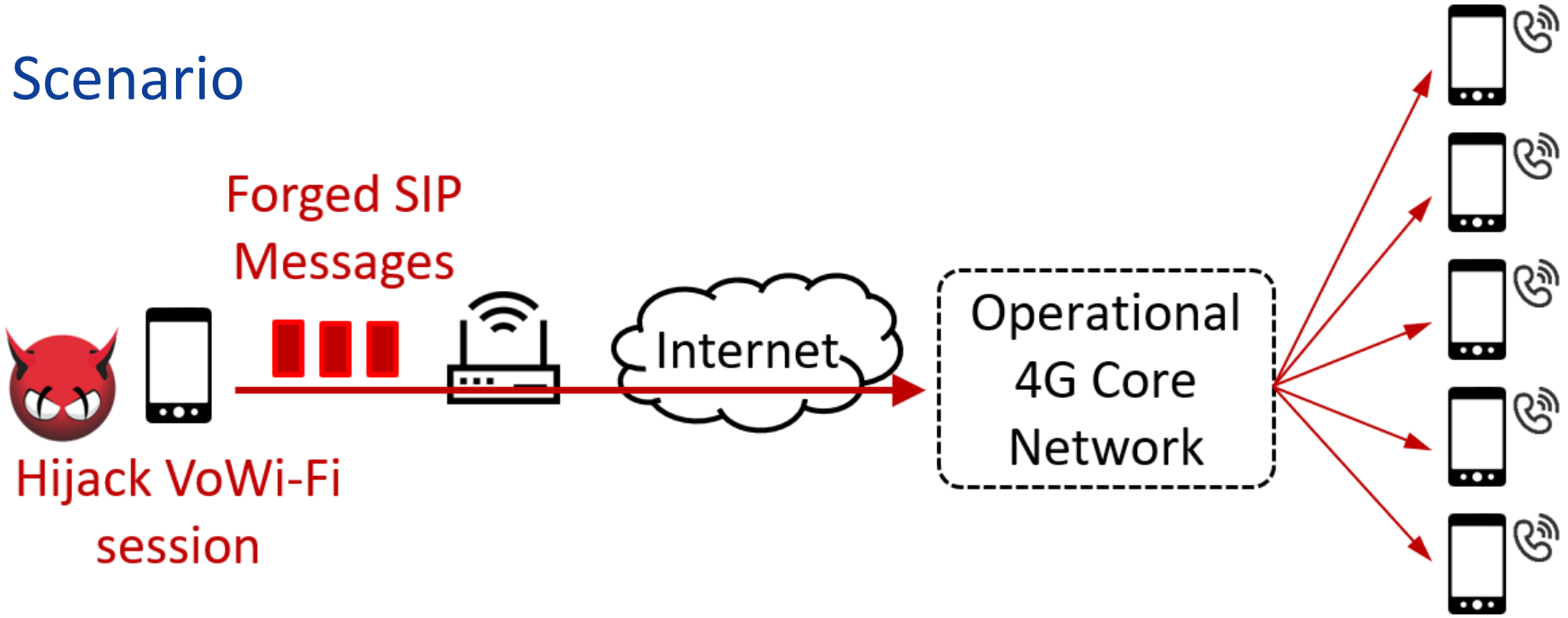
4G Call DoS Attack

National Chiao Tung University
NEtworking and Mobile Systems Lab

Attack II

- Ghost-call Attacks: large-scale concurrent call attempts
  - Social engineering with missed calls
  - DoS on multi-line telephony systems (e.g., enterprise, emergency)

- Demo Scenario



Concurrent Ghost Calls from an Attack Phone

National Chiao Tung University
NEtworking and Mobile Systems Lab

Questions?