Computer and Network Security

MINI PROJECTS

Description

The project of computer and network security course is a precious opportunity to convert the acquired theoretical knowledge into practical solutions that enhance the security of information systems and face off the various existing security threats. Also, it will be an occasion to teamwork and cooperate with your peers to build solid solutions. This will allow developing your teamwork skills, as per management, task distribution, communication, and cooperation.

Preparation

To work on these projects, you must form teams of exactly 6 members, from the same academic groups. You are required to designate a team leader. The selected leader should send me an email, CCing the teaching team, stating the final members, and the selected topics, by Thursday, March 16th — 11:59PM. If you run out of classmates, and find yourselves with 5 members, then that is exceptionally fine (b.c., certain groups contain 22 or 23 students).

To Do

In this project, you must choose two topics: One from the primary list and another one from the secondary list (see Pages 2 and 3).

Requirements

You are required to do the following five tasks:

1. Finalize a primary and a secondary project.
2. Prepare some Latex slides to present the two projects,
3. Prepare a project report — choose whatever template you like from Overleaf — discussion your project problematic, your solution, implementation, and the obtained results,
4. Project submission: zip your project resources (report, slides, source code, link to videos, etc), upload the file to Google Drive, and share the link with the teaching team,
5. Prepare a demonstration (could also be recorded and uploaded over Youtube as backup).

Firm Deadline

The deadline is fixed for Friday, May 16th, 2025 — 11:59PM.

Presentation and Demos

You will present and demonstrate your work on Week 15 during lab sessions.

Primary Projects

- **[P001] DNSSec.** Implement a secure local DNS server that uses digital signature to resolve DNS requests. Demonstrate DNS spoofing when using a standard DNS server, and when using your secure DNS server.
- **[P002] Create a keyboard emulator using Arduino (Keylogger).** The product will be an Arduino keyboard emulator that once plugged into a computer it injects a set of commands, e.g., opening the cmd, running some commands, etc.
- **[P004] Encrypted chat application.** Create a secure messaging app with end-to-end encryption. Users can connect to the server and choose to securely access (using a password) a given chatroom to securely chat with peers. The app should be scalable.
- **[P005] Malware.** Here you will develop malware that can compromise various security services. The malware should evade most anti-malware tools.
- **[P006] Secure mail server.** Implement a secure local mail server where employees of a company can create their account and securely exchange emails. Your server should be able to detect spoofed emails using SFP, DKIM, ARC, and DMARC mechanisms.
- **[P007] Next-generation firewall (NGFW).** Implement a NGFW. The project could involve creating a firewall that incorporates key features such as web filtering, URL filtering, an Intrusion Prevention System (IPS), and deep packet inspection.
- **[P008] Blockchain-based authentication.** Implement a decentralized authentication mechanism where user credentials are stored on the blockchain, eliminating the need for centralized databases and reducing security risks.
- **[P009] Voice Recognition-Based Multi-Factor Authentication (MFA) System.** Implement a voice recognition-based Multi-Factor Authentication (MFA) system using an Arduino/RaspberryPI and a suitable microphone sensor. The system will require a user to repeat a unique (unpredictable), randomly generated sentence to authenticate and gain access (e.g., open a door 672). This prevents attackers from using a recorded voice to bypass the system.
- **[P010] Secure Quiz Application.** Here you will develop a client/server application, where the server (e.g., teacher) provides a quiz to connected clients (e.g., students), which securely answer the quiz questions and submit their work to the server. Clients use their student cards to authenticate to the server and securely submit their work to the server. The server automatically grades the quizzes and stores the answers and scores in a secure database.

Secondary Projects

- [**S001**] **Ad Blocker device.** Use Raspberry Pi along with OpenDNS and PiHole to implement a local DNS proxy that can block all sorts of ads.
- [**S002**] **Developing a secure authentication system using multi-factor authentication (MFA).** In this topic, you will design and implement a robust authentication system that requires users to provide multiple (at least 3 factors) forms of verification, such as passwords, biometrics, or OTP to access a web application.
- [**S003**] **Cybersecurity awareness game.** Develop an application (e.g., mobile app, or web-app) where employees of a company can use it to solve security challenges, to train themselves and become more aware and sensitive. Your application can be used in a company to develop its social aspect.
- [**S004**] **Password security checker.** Here you can develop an application, and preferably, a browser plugin, that helps people test the complexity/strength of their password before they really start using it.
- [**S005**] **Setting-up a basic intrusion detection system.** Use tools like Snort to define rules for detecting malicious traffic. You should verify your solution by running at least five (05) different attack scenarios.
- [**S006**] **Student Attendance.** Here you will develop a secure application (with GUI) that uses RFID technology to allow students to automatically mark their presence in a class by just tapping their student card to the RFID reader.
- [**S007**] **VPN Analysis.** Here you are asked to implement a VPN in your local network to secure communication to a server. You will use OpenVPN to create your virtual private network, and use Wireshark to demonstrate how packets are secured (i.e., authenticated, encrypted, etc) while demonstrating the different used protocols.
- [**S008**] **ARP poisoning detector.** Here you will set up a blackbox tool to detect ARP poisoning in your local network. The blackbox is connected to a computer, and it consists of an Arduino board with an alarm system that blinks when it detects poisoning. The engine of this system would be a script that runs on the computer and analyzes the ARP cache to detect the poisoning. When the poisoning is detected, the board is alerted.
- [**S009**] **DNS poisoning detector.** Here you will set up a blackbox tool to detect DNS poisoning in your local network. The blackbox is connected to a computer, and it consists of an Arduino board with an alarm system that blinks when it detects DNS poisoning. The engine of this system would be a script that runs on the computer and analyzes the DNS cache to detect the poisoning. When the poisoning is detected, the board is alerted.
- [**S010**] **Smart QR code scanner.** An ENSIA mobile app that allows people to scan QR code, verify their authenticity, before opening the pointed web-page.