ENGIN 112: Module 12–Cybersecurity

Instructor: Prof. Tilman Wolf

Fall 2022

1 Internet

The Internet is a data communication network that connects many different end-systems so they can exchange information. Distributed applications require such information exchange to work correctly (e.g., an email client on a laptop communicates with an email server where the user's email is stored). The network consists of many links and "routers" that connect these links. Many different communication technologies can be used on the links and many different distributed applications can be built on the Internet. Unlike the telephone network, where a phone connection is pinned to a particular path for the duration of a phone call, data transmissions in the Internet use independent "packets." Each packet traverses the Internet independently and thus can take different routes.

"Protocols" are used to specify who different entities communicate with each other. A protocol specifies the types of interactions that can take place (e.g., format of messages), how to interpret these interactions, and what actions trigger or are triggered by interactions. Many ECE systems use a variety of protocols on interfaces between components.

An important aspect to the structure of the Internet is the use of "layering" to hide complexities and achieve scalability. For example, a network protocol that is concerned about how to route traffic from one system to the next does not need to be concerned how exactly a particular bit is encoded and transmitted on a given link. Two important protocols in the Internet protocol stack are Transmission Control Protocol (TCP) and Internet Protocol (IP).

Because protocols standardize the way communication is conducted, it is possible for malicious attackers to interfere with these interactions. The in-class demo shows an example of how traffic can be redirected to allow for a "man-in-the-middle" attack, where the attacker can observe the web requests sent by another user. Note that such interference, while technically possible, is unethical and illegal. In class, we only attacked our own computers and did not interfere with anyone else's communication.

2 Information Security

Information can be valuable and thus needs to be protected from unauthorized access and use. Information security mechanisms are used to provide such protection. There are a number of information security properties that are typically considered:

- Confidentiality: the information cannot be accessed by anyone who is not authorized (e.g., someone who does not have the keys to decrypt the information).
- Integrity: the information cannot be modified without the modification being noticed.
- Authenticity and non-repudiation: the information can be attributed to a source.
- Availability: the information is accessible (e.g., via network or server).

Attackers may launch Denial-of-Service (DoS) attacks using a single computer or Distributed Denial-of-Service (DoS) attacks using multiple computers. The goal of a DoS or DDoS attack is to exhaust the resources (network bandwidth, compute power, memory, etc.) of the victim and thus make it inaccessible to valid users (i.e., violating the "availability" property). Botnets can be used to coordinate a DDoS attack that is launched from many infected computers and controlled from a single command & control computer.

To achieve confidentiality, cryptographic algorithms can be used to encrypt data. There are a number of different encryption algorithms that vary in complexity and strength. The current Internet standard is the Advanced Encryption Standard (AES), which encrypts blocks of data using a secret key. The same key is used for decryption. Thus, this algorithm is a "symmetric" encryption algorithm. Asymmetric encryption algorithms use different (but matching) keys to perform encryption and decryption. The RSA algorithm is an example of a common asymmetric cryptographic algorithm.

Protocols can be used to achieve certain information security properties using cryptographic algorithms. For example, for authentication, a simple transmission of the identity or the identity and password is vulnerable to replay attacks. However, using a protocol, where the receiver challenges the sender to perform an operation that only the authentic sender can perform (e.g., encryption of a randomly chosen number using a secret, pre-shared key), can achieve authentication with protection from replay attacks.

Since establishing pre-shared keys between many entities is challenging, trusted intermediaries are used to establish a chain of trust. In the Internet, commercial websites can obtain certificates that trace their identity back to a trusted issuer of certificates (e.g., Symantec/VeriSign). The browser of a user can automatically check the validity of such certificates and display the information for the user.

3 Internet of Things

The Internet focuses on information exchange between computational systems. More recently, efforts have been made to also include physical components. In such an "Internet of Things" (IoT), three main actions occur:

- Sensing of physical world (e.g., temperature sensor, RPM sensor in motor, physical switch),
- Computation of response based on sensor input (e.g., control response to difference in actual temperature compared to set temperature),

- Actuation in physical world (e.g., turning on or off HVAC system)

This loop of sensing, computation, and actuation occurs in practically all control systems. In IoT, a large number of devices can contribute to these control loops.

One example of a sensor system in the physical world is Radio Frequency Identification (RFID), where small tags are powered through electromagnetic radiation from the reader. After being activated, RFID tags response with a short transmission that the reader can sense. This transmission can contain the identifier of the tag, sensor information, or results from cryptographic computations for secure authentication. RFID tags are widely used in practice (e.g., theft protection, supply chain management).

Home automation is another example of IoT. As shown in the demo, electric lights can be controlled wirelessly or via the Internet using a home automation system. In this case, different types of networking protocols are used to communicate via the Internet with the "bridge" that controls the home systems and within the home. The final example was a home that had its holiday lighting connected to the Internet, where any visitor can turn on and off the decorations and observe the results on a live camera feed.