Lecture Notes on Jan/16/2023

Chapter 2:
Network Communications Protocols and Built-in Security (Part 01)

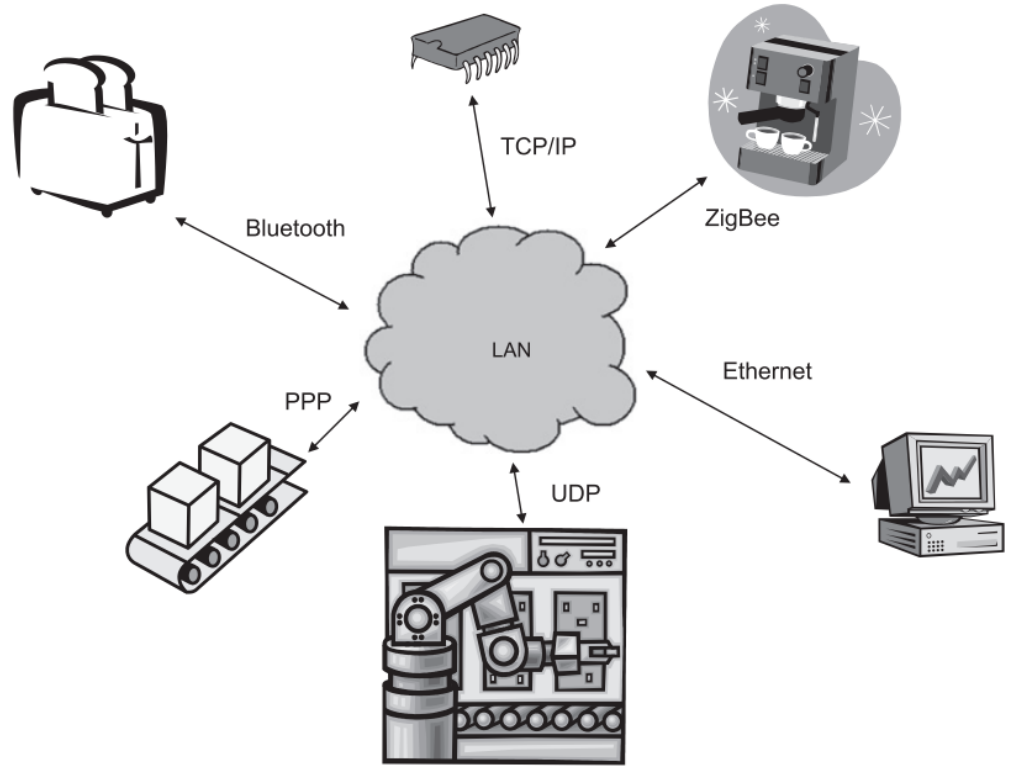
CYENG 351: Embedded Secure Networking

Instructor: Dr. Shayan (Sean) Taheri

Gannon University (GU)

Overview

- Embedded systems that are connected to any network, be it the full Internet or a small LAN, have to conform to the various protocols that have been designed and implemented to keep the network running.
- **Communications Protocols** → They can be used fully and partly depending on our needs → Provide the vast array of services available from networked devices. → Suitable for different failures and attacks.
  - Low-level (such as Ethernet or wireless technologies).
  - Medium level (such as TCP and IP).
  - High-level (HTTP, FTP).



Embedded Devices on a Local Area Network

Low-Level Communications

- **Low-Level Protocols** → These technologies are often hardware-based, very low-level software, or a combination of both (usually assembly code or some form of driver are needed to communicate between the hardware and higher-level protocols).
- **Types:**
  - Wired protocols such as PPP and Ethernet.
  - Wireless technologies such as Wi-Fi and Bluetooth.
- Each type has specific security requirements and each deals with security in its own way (which may be to have no security options at all).

The Network Stack Model with Example Protocols

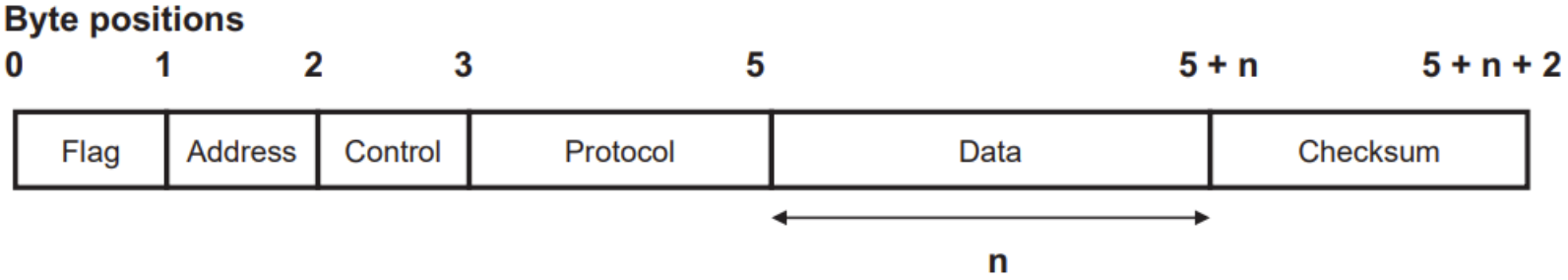
Application	
Transport	
Network	IP, ARP, IPSEC
Link	Ethernet (software), 802.11 MAC, PPP
Physical	Ethernet (physical), 802.11 radios, RS-232

Point to Point Protocol (PPP)

- **PPP** is a relatively old communications protocol, described in 1994 in RFC 1661,1 and was designed to provide connectivity over serial hardware channels.
- PPP was originally developed to allow higher-level protocols to utilize these serial channels in a consistent manner.
- This protocol, though losing out to newer, faster technologies, is still used widely for embedded systems due to the fact that simple serial hardware is much less expensive than the hardware that some of the newer standards require.
- PPP consists of a few protocols designed to establish the serial link, encapsulate the higher-level data, and to control each of the high-level protocols that can be used.
- Many different high-level protocols are compatible with PPP, such as the Internet Protocol (IP).
- PPP, as with many low-level protocols, is designed to be the connection between the network hardware and the application.
- Link establishment in PPP is controlled by the **Link Control Protocol (LCP)** → **The LCP divides the link establishment procedure into 4 distinct steps**:
  1. Establish the serial link using the hardware.
  2. Optionally, test the quality of the link to determine if the hardware can handle the communication level desired.
  3. Negotiate and configure the higher-level protocol for transmission.
  4. Terminate the link and release the hardware.

Point to Point Protocol (Cont.)

- **In LCP** → It is needed to have a hardware connection in order to communicate with the remote device. → It is optional to have a link quality test because leaving it out may result in subpar communications, while it will definitely save on code size, and the link can be established faster.
- PPP is an inherently configurable protocol, allowing for many implementation options.
- For each network-layer protocol, there is a corresponding Network Control Protocol (NCP) that allows the protocol to utilize PPP as the link-layer transport mechanism.
- Each NCP is designed to provide the correct functionality to allow PPP to transport the higher-level packets.
- This functionality includes any security protocols inherent to the higher-level protocols, such as IPSEC (security for IP).
- The selection of NCP's to support is another option we have to conserve code space.
- If we know that our application will only need to support one higher-level protocol (such as IP), then we only have to implement the functionality specific for the NCP for that particular protocol.



PPP Structure

Point to Point Protocol (Cont.)

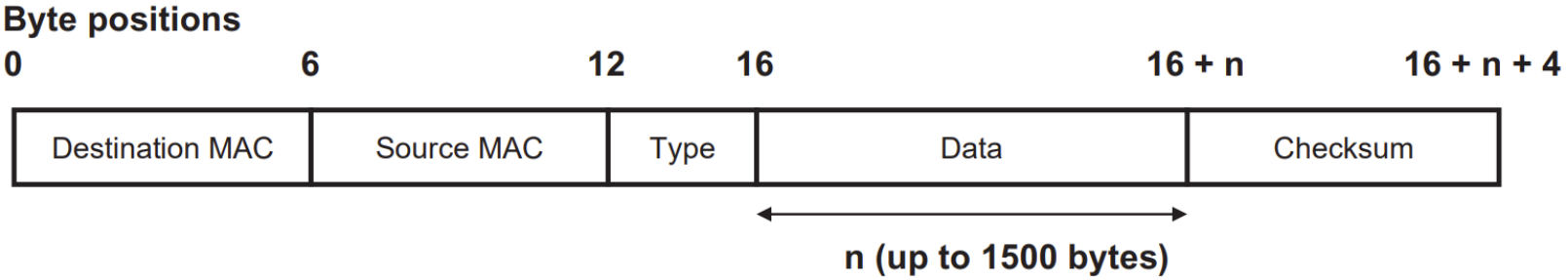
- We can tailor the implementation to fit the protocol, and since we do not have to support the other NCP's, we can simply reject any protocols that we do not support. → Robust Rejection Denial-of-Service or Buffer Overflow
- PPP has its own security mechanisms that we can use to authenticate connection requests, allowing the implementation to protect the device from unauthorized use.
- The security mechanisms supported by PPP are password authentication and a challenge-handshake. Again, we can choose to support either of these mechanisms.
- The password mechanism will have a simpler implementation, since the challenge-handshake will require additional states in the PPP state machine to handle the additional messages.
- Depending on the application, the no-security option may be more desirable. → If the network is not secure, sending a password would allow anyone eavesdropping on the network to read the password.
- The challenge-handshake protocol, though more complex, is also more secure than the password protocol.
- The common challenge-handshake protocol for PPP is defined in RFC 1994 (written in 1996), and is referred to as the Challenge Handshake Authentication Protocol, or CHAP.
- CHAP provides decent security for devices with a previously defined trusted relationship, but since it requires shared secret keys (cryptographic keys stored on each end), it is not practical for general-purpose security (connecting to arbitrary remote systems).
- Without an established relationship, the secret for the challenge mechanism must be sent plaintext over the network - which is obviously not secure at all.

Ethernet and ARP

- Where PPP is predominantly a software protocol, “Ethernet” is a combination of software and hardware.
- Although Ethernet is even older than PPP, it has gained widespread acceptance and is the de facto standard networking technology for LANs.
- The Ethernet standard describes both a physical hardware layer and a higher-level data encapsulation layer.
- Ethernet has been an evolving standard, and has kept pace with new developments in networking technology.
- The standard is now part of the IEEE 802 networking standards collection and newer versions support some of the highest speed hardware, capable of transmitting gigabytes of data each second.
- This Gigabit Ethernet is still relatively expensive since it requires expensive and powerful hardware. → Not well applicable for resource constrained systems.
- Ethernet is characterized by a physical layer that utilizes internationally assigned unique Medium Access Control addresses (MAC addresses) that are simply large numbers that are globally unique to a particular device.
- The data-link layer described by the Ethernet standard defines a frame that encapsulates both the MAC address and the data being transported.
- The Ethernet frame is used by the hardware to control where the data is going on the physical network.
- Ethernet Stack → How the addressing of each device is resolved (i.e., each device can have several addresses)? → These addresses include the hardware address (MAC), IP addresses, TCP ports, etc.

Ethernet and ARP (Cont.)

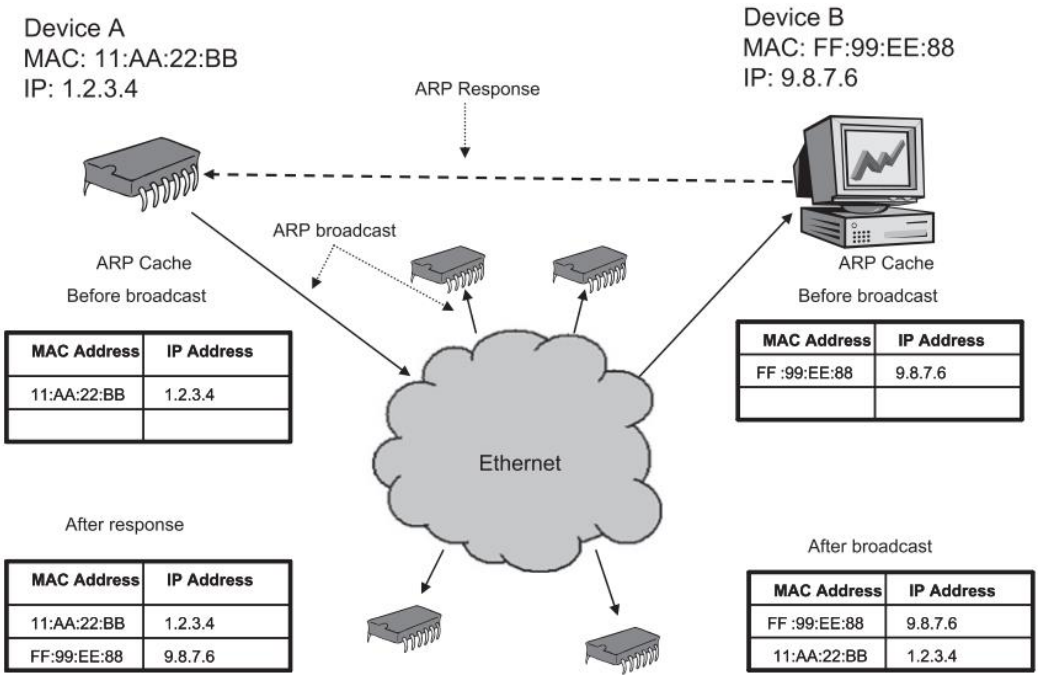
- The software layers need to be able to resolve the physical address of the destination device requested by an application so that the data can be communicated to the right receiver. The primary way this is done is to use the Address Resolution Protocol (ARP).
- ARP is responsible for associating hardware addresses with higher-level protocol address, primarily Internet Protocol (IP) addresses.
- Described in RFC 826, ARP facilitates the translation of higher-level protocol addresses, such as Internet Protocol (IP) addresses, into Ethernet hardware MAC addresses, and the reverse, associating a hardware address with a particular higher-layer address.
- ARP works by storing a table locally that contains the information about all of the known devices on the Ethernet network.
- This ARP table is updated only when a device is added to the network or a device attempts to contact a device not already in its table.
- ARP works by broadcasting a message to all the devices on the Ethernet network, asking if a particular device has the higher-layer protocol address and can speak the right protocol.



Ethernet Frame

Ethernet and ARP (Cont.)

- Once the target device receives the message, which contains the sender's hardware address, it updates its own ARP table and sends a reply back; this causes the sender's table to be updated.
- In this fashion, the ARP table does not have to be constantly updated, sending flurries of packets over the network whenever a connection is desired.
- The sender and receiver can contact directly using the stored hardware addresses.



ARP Broadcast Steps

Assignment

- **Reading Assignment:**
  - Stapko, T., 2011. **Practical embedded security: building secure resource-constrained systems**. Elsevier.
    - ✓ "Chapter 2: Network Communications Protocols and Built-in Security", Pages 23-30.

Questions?