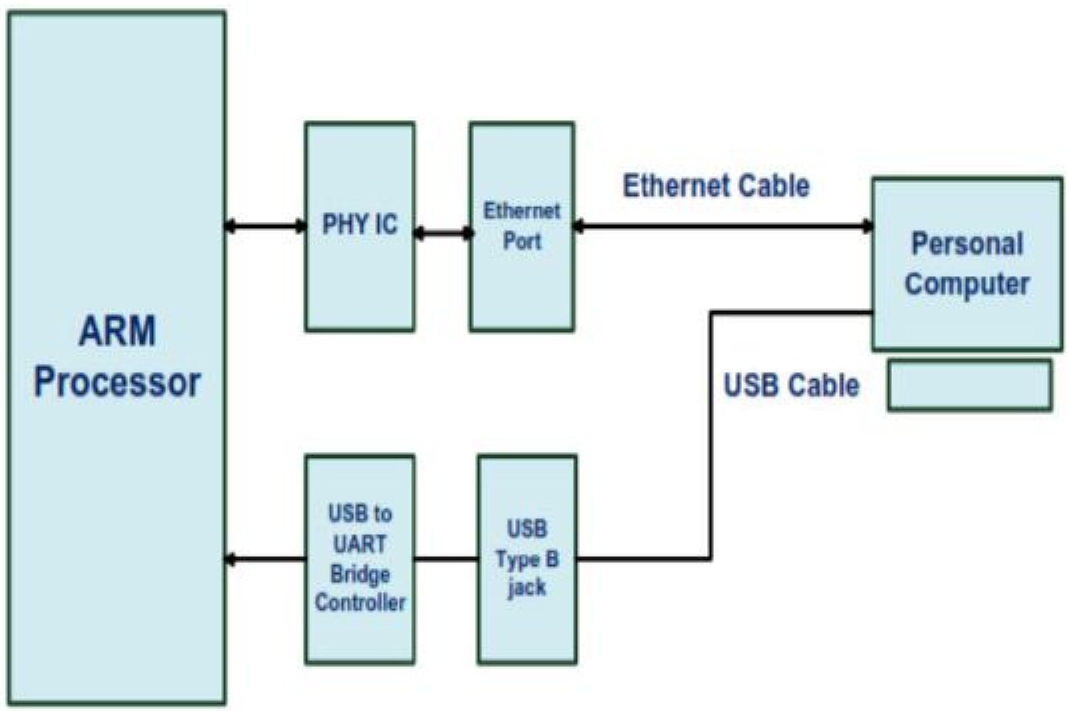
(USNA) Mission Overview

(USNA) Army week is coming up and tensions are higher than ever. The cadets have already paraded their mule down Stribling Walk and defaced Tecumseh. What will they do next?? Your company officer has made you responsible for having Army week run smoothly and without incident or she will **reject your leave chit for winter break** . Your mission is to figure out what your adversary is planning and put a stop to it. We're all counting on you!

(USNA) Luckily, a hardware device has been swiped from an exchange cadet that happens to be an ARM Cortex M3 NXP LPC1768 based embedded device. It allowed him to communicate back to Westpoint and plan the dastardly deed. The captured device when executed has messages encrypted and stored in memory. You will need to decrypt the message and send it to an analyst for interpretation.

(USNA) The ARM Cortex M3 processor is instrumental in coordinating the actions of our Westpoint adversaries. If we can decode and exfiltrate (EXFIL) the messages out of the network to our forces that will help safeguard Army week. Figure 1 illustrates the adversarial network [1] the detailed schematic is illustrated in figure 2 [1].

Figure is USNA Sensitive

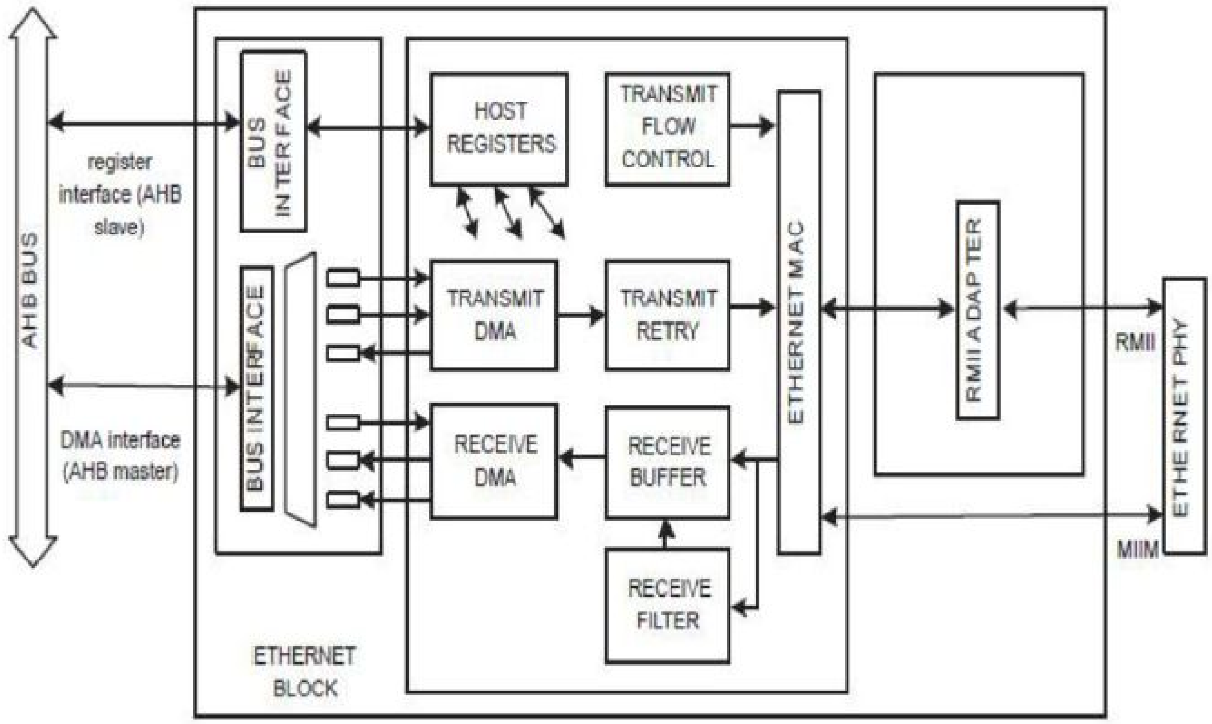


(USNA) Figure 1: Integration of the ARM Processor and the importance of adversarial communications [1].

(USNA) A **covert channel** is a type of attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy. (wikipedia)

(USNA) Reading the registers and then encoding the light sequence would give us the information advantage to foil any plans the cadets attempt to execute, giving us the upper hand in morale for the big game. Discover their plot and make Mother B proud!

Figure is USNA Sensitive



(USNA) Figure 2: Schematic of a futuristic ethernet communications device [1].

(USNA) Operational Needs Statement - Exploitation and EXFIL Requirements:

1. (USNA) (20 pts) Access the memory stored in the data registers prior to being overwritten
2. (USNA) (20 pts) Identify the language encoding set that is being used
3. (USNA) (20 pts) Decode the message from the encoding set
4. (USNA) (20 pts) Crack the encryption key
5. (USNA) (30 pts) Decrypt the message and thwart the Army plan

(USNA) Additionally, you were able to get your plebes to do recon in the exchange cadets' room to gather some useful intelligence. MIDN 4/C Namath was able to find the secret key scheme that could be used to decrypt the memory registers to reveal the encoded characters (consider known character encodings). It turns out that the encrypted bitstream is stored in the R0 register whenever LED2 is illuminated and the bits for the key to decrypt the ciphertext is gathered from the least significant bit of the R0 register whenever LED4 is lit . He is just in plebe cyber and has NO IDEA what this means. Luckily, you are an experienced Cyber Operations major and will have this case cracked in no time! Happy Hacking!

(USNA) Secret Key

(USNA) The secret key was EXFIL-ed over secure communications to your device as a 32-bit value (Format in Hexadecimal).

References:

[1] Kavya M.P., Thanuja T.C., Angadi N.G., “Development of a Prototype for Ethernet Port With ARM Cortex-M3 Processor for Web Applications” International Journal of Research and Technology Vol. 4., Issue 9, September 2015