6.111 Final Project Abstract: Encrypted Communications over Ethernet

Hyo Won Kim, Mark Theng

2018

For our project, we will transmit AES-encrypted text over Ethernet. Ethernet is the most common data link layer networking protocol for Internet communictations, so using Ethernet as a base for our encrypted communications system would make our system portable to a large range of networks. Our goal will be to transmit a message from one FPGA to another (in a way impervious to a malicious middleman) and display it on a screen. This would be done over a single Ethernet cable, but could be extended to communicate over a larger network.

The Nexys 4 DDR board contains an Ethernet port behind an SMSC 10/100 Ethernet PHY exposing an RMII interface, allowing us to send and receive raw Ethernet frames directly without having to worry about the analog aspects of Ethernet communications. On the lowest level, our system will need to be robust to interrupted or corrupted packets, collisions and other issues that may arise in communication. To transmit long messages reliably, we may need to implement additional systems over Ethernet, or use temporary buffers for message reconstruction. Messages will then need to be split into blocks for the cryptographic processing.

Encryption would use the AES-128 standard, ultimately supporting encryption and decryption in CBC mode. We will initially establish a static key for the procedure, but may add a way to derive a shared key. At first, we will implement ECB mode, which encrypts each 16-byte block independently, and influences each block in place. Ultimately, we hope to be able to operate the cipher in CBC mode, which gives us additional security.