The Impostors Hardware Trojan

Casey Avila, Ben Kunkle, Noah Masten

CPE-426

Oct 31 2023

OVERVIEW

Our hardware trojan is implemented into an AES module. We have implemented a program to interact with the serial port on the Basys3 to allow sending plain text to be encrypted to the board and then receive the encrypted ciphertext back.

AES

AES is a block cipher algorithm. Many chips include hardware implementations of AES to improve its performance due to how popular it is.

AES supports multiple key sizes, our implementation uses a 128 bit key.

USAGE

The Vivado project including the Verilog source files are included as well as binaries to interact with the module.

To interact with our project you must download the Virtual COM Port drivers for the Basys3 found at https://ftdichip.com/drivers/vcp-drivers/

Once the drivers are installed you may synthesize the project and program the Basys3.

With the Basys3 programmed you can then run the provided binary for your computer's architecture.

The binary provides two main features

1. A nice way to interact with the board. When it runs it starts a server on port 8080. Navigating to localhost:8080 in your browser will present you with a simple web page to enter in a secret key and a message. Pressing submit will then send the information to the board to be encrypted.

2. Additional logic for interacting with the AES algorithm. Our AES module only handles encrypting a single block of plain text. The binary provides a simple wrapper around the connection to the board allowing messages of arbitrary sizes to be encrypted as well as providing decryption functionality.

Note that the binary has nothing to do with the trojan. It only provides an interface for interacting with the compromised module.

Also note that the binary is just a wrapper around communicating with the board through the COM (serial) port. You can Interact with the board directly by using `PuTTy` on Windows or the `screen` cli utility on Mac or Linux. Information on how to communicate with the board is given on the web page served by the binary.

The Impostors Hardware Trojan

Casey Avila, Ben Kunkle, Noah Masten

CPE-426

Oct 31 2023

TRIGGER

The trojan is implemented as a sequential trojan. Sending an input block to be encrypted with certain (trigger) bits set correctly will increment an internal counter by one. Once the counter reaches its max count (Q) the output of the counter will be 1. Therefore encrypting Q blocks sequentially with the trigger bits set correctly will activate the trojan for the next encrypted block.

The sequential nature of the trojan provides a level of stealth. The payload of the trojan modifies the output of the module potentially giving away the presence of the trojan or at the very least a problem with the AES module. However, the requirement for Q consecutive blocks with the specified bits set correctly to be passed during normal use for one block of output to be modified minimizes the chance of the trojan being activated during normal use.

PAYLOAD

The payload is delivered through a series of or gates between the output of encryption rounds 0 to n - 1 where n is the number of rounds. One of each of the gate inputs will be from the output of the previous rounds. The other is the output of the trigger counter. While the counter is not at its max count (Q) the output is 0, thereby making the payload or gates simply pass their inputs on unmodified. Once activated the inputs to the final round of encryption will all be 1.

With the inputs to the last round known, the returned ciphertext from the module can be used to decipher the subkey for the final round, as well as all the previous subkeys, and finally the original secret key. This is all done using relatively simple algorithms.

Knowing the inputs to the last round is important as the last round is the only round that does not include the “mix columns” layer. This makes it easier to decipher the final round’s subkey and subsequently the secret key as the matrix used to mix the columns does not have to be known by the attacker.