

UNIVERSITY OF ARKANSAS- FAYETTEVILLE

# CSAW 2008 Hardware Challenge

---

Report of Trojans

Anish Philip

10/10/2008



## Contents

1. Introduction	- 3
2. Trojan 1	-3
3. Trojan 2	-5
4. Trojan 3	-6
5. Counter measure and Conclusion	-7

# CSAW 2008 Hardware Challenge

## Introduction

Orange Army has developed a solid state cryptographic device “alpha” that will be mass produced and deployed into the field. The device uses a 128 bit private key block to encrypt message before they are transmitted. The main objective is to break this cipher device, without it being visible to inspection before deployment. The assumptions made are

1. Being under army control, the hardware device will not be physically available for manipulation or observation once deployed.
2. No specialized external hardware is available for use.
3. The transmitted cipher text can be intercepted by the attacker.

Considering these assumptions, the optimum method to break the device would be to insert an “Information Leakage” Trojan. This would involve exposing either the master key of the device or the private message that is meant to be encrypted. The device uses the master key and a key index to generate the private keys that encrypt the message. If the master key is obtained by the attacker, the private key can be generated with the help of the first byte of the cipher text. The first byte contains the chosen private key out of the 256 possible private keys.

## Trojan 1

Trojan 1 takes into consideration, the fact that Alpha makes use of an RS232 port to transmit the encrypted data. This port is configured as an output port. This Trojan reconfigures the output RS232 port to an input/output port. When alpha is in the “Clear Buffer” state, the Trojan observes the input RS232 port for the character “a”. This logic prevents the Trojan from activating when the circuit is in use, thus leading to its discovery. On reception of the character “a”, the Trojan is activated and the master key is transmitted out via the output RS232 port. During this period, the intended receiver is not aware of the Trojan as he/she does not listen for an incoming transmission. Once the master key is transmitted, the Trojan resets the device to the “Clear buffer” state and thus any user of the device alpha is also completely ignorant of the Trojan. Figure 1 shows the output of device when the Trojan is activated. It can be observed the cipher text contains the master key of the device.

```
Ciphertext:
    00FB7915BDF1E5C8B84BB718DD34D733A5FFFFFFFFFFFFFFF
Using Key:
    FB7915BDF1E5C8B84BB718DD34D73300
Plain Text:
    0P008~083R0z0
```

Figure 1- Cipher text containing master key

This Trojan can definitely pass the inspection procedure of the Orange Army. Detection using exhaustive test cases would not yield results, as the test case scenarios would not include an input RS232 port. Also the power consumed by the Trojan circuitry fails to leave any noticeable change on the 146 mA consumption during the “Clear buffer” state. The receiver clock is turned off when the device is not in the clear buffer state to reduce any overhead power consumption during the encryption and transmission states. Thus this Trojan is virtually impossible to detect by any normal inspection process.

The Trojan however requires an increased utilization of the four input look up tables. The increase however is by a small margin of 4 percent. Considering the huge design of the device, this would be a negligible increase in utilization. The device utilization summary is shown in figure 2

Device Utilization Summary				<a href="#">[E]</a>
Logic Utilization	Used	Available	Utilization	Note(s)
Number of Slice Flip Flops	1,517	4,896	30%	
Number of 4 input LUTs	4,208	4,896	85%	
<b>Logic Distribution</b>				
Number of occupied Slices	2,425	2,448	99%	
Number of Slices containing only related logic	2,425	2,425	100%	
Number of Slices containing unrelated logic	0	2,425	0%	
<b>Total Number of 4 input LUTs</b>	<b>4,373</b>	<b>4,896</b>	<b>89%</b>	
Number used as logic	4,208			
Number used as a route-thru	165			
Number of bonded <a href="#">IOBs</a>				
Number of bonded	47	108	43%	
IOB Flip Flops	5			
Number of RAMB16s	8	12	66%	
Number of BUFGMUXs	4	24	16%	
Number of DCMs	3	4	75%	
Number of MULT18X18SIOs	2	12	16%	

Figure 2

Trojan 1 would be the optimal Trojan for the attacker, as it would enable him/her to listen in to all further communications without any additional effort. The damage is not visible to the user of the device and cannot be undone by resetting the circuit or toggling the power.

## Trojan 2

Alpha can be used for encrypting and sending all kinds of information. The attacker might be overwhelmed if he/she decides to eavesdrop on each and every bit of communication taking place. Instead the attacker would only be interested in the message, if it contains certain key words. Thus this Trojan takes into consideration the nature of messages send by the user. The attacker would only be interested in messages if it contains a predetermined key word.

This Trojan monitors the input text to the device for the keyword “war”. If this pattern is not found, the device works as its intended function. If the particular pattern of characters is found by the Trojan, then all text in the vicinity and after the word war is transmitted without encryption. The receiver shall get a message containing plain text followed by erroneous plain text, as he/she tries to decrypt a decrypted message (Figure 3). The attacker can convert the hex ASCII characters to plain text to observe the message (Figure 4).

```
Ciphertext:
 1F985E03C94E0034B577E574DD32BB40CBDDC2A430DB2AEDFBEDBAF090D4B10C43697320
697320612074657374207761722077697468206F752020656E656D6965730404040404040404
0404040404FFFFFFFFFFFFFFF
Using Key:
 E47915BDF1E5C8B84BB718DD34D73305
Plain Text:
 this is a test this is a test th 0^0V00#000V0 +0 0 000 00 0|000] |%L 0
```

Figure 3

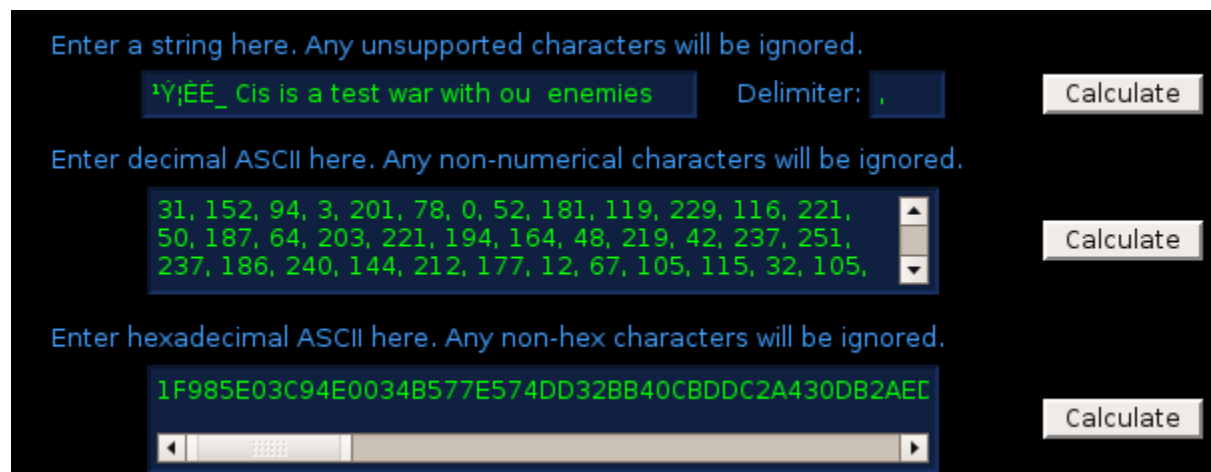


Figure 4

Device Utilization Summary				
Logic Utilization	Used	Available	Utilization	Note(s)
Number of Slice Flip Flops	1,473	4,896	30%	
Number of 4 input LUTs	4,184	4,896	85%	
<b>Logic Distribution</b>				
Number of occupied Slices	2,407	2,448	98%	
Number of Slices containing only related logic	2,407	2,407	100%	
Number of Slices containing unrelated logic	0	2,407	0%	
<b>Total Number of 4 input LUTs</b>	<b>4,337</b>	<b>4,896</b>	<b>88%</b>	
Number used as logic	4,184			
Number used as a route-thru	153			
Number of bonded IOBs				
Number of bonded IOB Flip Flops	46	108	42%	
Number of RAMB16s	8	12	66%	
Number of BUFGMUXs	4	24	16%	
Number of DCMs	3	4	75%	
Number of MULT18X18SIOs	2	12	16%	

Figure 5

If the Trojan is activated, it is possible for the receiver to deduce that the message has been tampered with. But this can be detected only after the device has been deployed and the damage has been done, as the attacker would have received his/her crucial information.

Trojans that observe for patterns are very hard to detect. It is again virtually impossible to detect them by exhaustive testing due to the large number of input patterns possible. The power consumed by the Trojan is negligible and any increase beyond the stipulated 144mA is not observable during the encryption state. However, it does consume 3% more LUTs. The device utilization summary is shown in Figure 5.

### Trojan 3

Trojan 3 is also an Information leakage Trojan. It transmits the master key of the device when activated. The Trojan is activated based on the number of bit one's present in the selection of input key. If the number of bit one's is equal to 5, then the master key is transmitted before the cipher text. Thus the attacker can observe the cipher text to

obtain the master key. With the help of the master key, the attacker shall be able to decipher the encrypted text.

This Trojan again does not consume a significant amount of power to make it greater than the reference levels. An example output and the device utilization summary of the device are shown below.

```

Ciphertext:
    1FFB7915BDF1E5C8B84BB718DD34D733A59ECDD4DF83C62226EB0A51F11873EEFBFFFFFF
FFFFFFFF
Using Key:
    E47915BDF1E5C8B84BB718DD34D73305
Plain Text:
    
```

Figure 6

Device Utilization Summary				
Logic Utilization	Used	Available	Utilization	Note(s)
Number of Slice Flip Flops	1,483	4,896	30%	
Number of 4 input LUTs	4,194	4,896	85%	
<b>Logic Distribution</b>				
Number of occupied Slices	2,396	2,448	97%	
Number of Slices containing only related logic	2,396	2,396	100%	
Number of Slices containing unrelated logic	0	2,396	0%	
<b>Total Number of 4 input LUTs</b>	<b>4,354</b>	<b>4,896</b>	<b>88%</b>	
Number used as logic	4,194			
Number used as a route-thru	160			
Number of bonded <a href="#">IOBs</a>				
Number of bonded	46	108	42%	
IOB Flip Flops	5			
Number of RAMB16s	8	12	66%	
Number of BUFGMUXs	4	24	16%	
Number of DCMs	3	4	75%	
Number of MULT18x18SIOs	2	12	16%	

Figure 7

### Counter measures and conclusion

These Trojans demonstrate that current methods of power analysis and exhaustive testing fail to detect the presence of minute Trojans. With larger circuits, exhaustive testing can be ruled out due to sheer number of input test vectors. Also as we go for smaller fabrication process, the process variation shall negate the effects of power analysis. An optimal solution would be deduce vulnerable portions of the circuit and introduce scan chains that can set the values on internal registers and observing the

Anish Philip

corresponding outputs. This would certainly yield a higher probability of finding Trojans that embedded deep into large circuits.