



Kevin Lawless  
Sanam Chaudhari  
Ken Teoh  
Adrian Armstrong  
Jonathan Walsh  
Kyle Tuckwell

## Milestone 8 – Team 112

### Part A

#### A.1

The TAIS Beta Environment's (TBE) Criteria of Abstraction (CA) is inherited from the TAIS Alpha Environment (TAE), as according to Beta 1 "the TAIS Beta Environment inherits the TAIS Alpha Environment". Now Alpha 1a states, "the execution substrate of the TAIS Alpha Environment is not compromised" and 1b states "the execution substrate of the TAIS Alpha Environment has no network access". Therefore, the TBE substrate is inaccessible directly due to there being no network access for the emulator or substrate. There should be no vulnerability that would allow an attacker to gain complete control of the substrate.

#### A.2

The value of analysing all of the Bluebrick code and searching for a bad implementation method that would allow a connection on port 10000 to occur would be very high. If a bad implementation method was found it would allow you to control the Bluebrick implementation and you could modify instructions. For example, at the end of every instruction it could be modified to transfer \$100,000 or steal important files. However, such research would be limited by time and the cost would be a waste due to the Bluebrick implementation being in the substrate.

#### A.3

It would be an impossibility to subvert the CRE unless you had a saboteur in place of where you wanted to subvert as in order to subvert the CRE you would need to modify the code, including methods of the Bluebrick implementation and the instruction set in the CRE to enable a malicious method to occur. This is because the CRE normally has formal methods and certain behaviours that every instruction is allowed to pass across the Reference-Membrane, thus preventing passive and backdoor attacks. There would be more point in focussing resources on analysing the Bluebrick code and searching for flaws before attempting this as it would be a bad use of resources.

#### A.4

We believe that due to the framework from TAIS to its working implementation on Bluebrick that there would be no successful attack method possible.

## Part B

Configuration booted up and log files were checked and the connections were successful.

## Part C

We used the free program Nmap to perform penetration tests on the provided defence template.

Using the IP address 192.168.56.101, all tests found port 10000 to be open but were unable to penetrate the target.

## Part D

D.1

All attacks failed, as expected

D.2

We think that there is no way to successfully attack the Bluebrick implementation from outside the system.

D.3

The internet would not be able to help in accessing the Bluebrick implementation due to the nature of the substrates security.