

## BI3 Ethical Hacking Challenge 2011

### Capstone style Industry Project Brief Summary

---

Information systems have made unprecedented gains in the last 100 years. In the past, critical documents could be locked in safes but today, system complexity and a proliferation of devices and technologies has caused a new problem of information insecurity. WikiLeaks is a clear example of the damage that can be incurred by using flawed security systems for mission critical information infrastructure.

The BI3 Ethical Hacking Challenge 2011 addresses information security head on with the Theory of Absolute Information Security. This project offers students an opportunity to make a real impact in the area of information security globally as they learn, help identify potential issues and verify the validity of this cutting edge security theory.

All knowledge and technology can be reused as it is free and open without restriction or warranty.

#### Prerequisites

Participants must

- be undergraduate or postgraduate at a recognised university, college or polytechnic
- enrol as individuals or in teams of up to 5 people
- have access to at least one relatively new PC and a good broadband connection
- understand the basics of networking and programming concepts

#### Student benefits

Although this Industry Project (Capstone style) has no direct financial incentive, the knowledge gained in the Theory of Absolute Information Security can be utilised throughout the student's career. Furthermore, Blueicon Technologies will publish student work and any contributions the student has made to the information theory, specifications or implementation on **www.blueicon.com**, which can be referenced on their CV.

Undergraduates can enjoy a clear framework (see workload) that introduces them to cutting edge security theory while postgraduates can research a groundbreaking approach to information leakage and extend the time they allocate to the project at will while benefiting from the online support provided by Blueicon Technologies.

#### Project level of difficulty

Undertaking the BI3 Ethical Hacking Challenge 2011 is not necessarily difficult. A strong framework and extensive resource base is made available to guide teams throughout the year. However, the project addresses one of the most difficult problems facing governments, military and corporations as they grapple with securing their information. The project therefore has the capacity for high achieves to demonstrate their true ability and possibly form the cornerstone of their career path as they utilise the open theory to build fully secure information systems.

## Qualifications

Blueicon Technologies will accept undergraduates and postgraduates that understand about networking, programming and object orientation (preferably an awareness of Java) and some basic security knowledge. Blueicon Technologies does not expect the student to have an expert understanding of security systems as the BI3 architecture is novel and will not have been encountered before. However, the student should be prepared for a project that can challenge them as it explores one of the most controversial aspects of Information Technology. Nonetheless, a rigid structure will be provided, so there is little chance that the student will become stuck and be unable to complete the project.

## Working remotely

The project involves collaboration from a number of universities from Europe, USA, China, Australia, India and New Zealand. As a result there is a rigorous framework for accessing information and presenting milestones.

- A comprehensive brief and software (Blueicon Development Kit) is provided that includes all deliverables, milestones and supporting tools.
- For general questions relating to the technology please email [admin@blueicon.com](mailto:admin@blueicon.com)
- You may post a question on the BI3 Technology Forum on **blueicon.com** (select the forum from navigation menu). You are encouraged to answer or help other students if you believe you know the answer to a question, otherwise Blueicon Technologies personnel will answer every question with 72 hours. You may post a question in Chinese – if the question is relevant it will be translated into English and answered in English by Blueicon Technologies personnel.
- You may try to connect with Skype name *blueicontechnologies* (not always available without a reservation) to speak with a technician in English. If you speak Cantonese or Mandarin, please request a Skype session by emailing [admin@blueicon.com](mailto:admin@blueicon.com) with your language of choice so we can arrange an appropriate translator/technician.
- You may call David Hughes on +64 9 4866884 for any technical or project enquiries in English
- The latest Blueicon Developer Kit (BDK) can be downloaded from the download page from **blueicon.com**
- The FTP server account details for uploading your deployment images will be assigned to you during the project.

## Workload

The project workload can vary depending on the number of people in the team but expect it to be around 400 – 500 hours per person for a 2 – 3 person team who are engaging a double semester project. Alternatively, the single semester project drops to around 200 – 250 hours for an equivalent 2 – 3 person team.

## Timeline

Please note that the times listed below are for the current semester intake only. Students are welcome to start later, outside this timeline and operate entirely at their own pace (ideal for postgraduate research). Please indicate on the registration form if this applies to your team.

**Note:** All files are released at 10h00 UTC+12. This New Zealand time zone lies next to the International Date Line, so the file will already be available by sunrise in your country. Files can be downloaded from the BI3 Ethical Hacker Challenge 2011 navigation menu link.

<b>BI3 Ethical Hacking Challenge 2011 Timeline</b>	
28 Feb	Orientation week starts (remote Skype, video broadcasts & more)
29 Feb	Blueicon Development Kit (BDK) released
7 Mar	Final enrolment and registration of academic teams
7 Mar	Project starts for single and double semester teams
7 Mar	Milestone 1 full brief released
11 Mar	Milestone 2 full brief released
18 Mar	"Isolated Bluebrick© Alpha" build available
18 Mar	Milestone 3 full brief released
28 Mar	Milestone 4 full brief released
1 April	Milestone 5 full brief released
8 April	Milestone 6 full brief released
15 April	Milestone 7 full brief released
15 April	"Secured 2 party communication" build available
22 April	Milestone 8 full brief released
6 May	Milestone 9 full brief released
13 May	Milestone 10 full brief released
27 May	Milestone 11 full brief released
3 June	Project ends for single semester teams
17 June	Milestone 12 full brief released
8 July	Milestone 13 full brief released
22 July	Milestone 14 full brief released
12 Aug	Milestone 15 full brief released
26 Aug	Milestone 16 full brief released
9 Sep	Milestone 17 full brief released
23 Sep	Milestone 18 full brief released
7 Oct	Milestone 19 full brief released
14 Oct	Project ends for double semester teams

\*Note: Dates are subject to change

## Deliverables

Deliverables are due throughout the project. The level of documentation required for each of the deliverables is deliberately not specified. You should include as much information as required to adequately comply with the brief. This naturally does not relate to any academic documentation that may be required by your educational institution, which is not covered by this brief – please check with your supervisor if you have additional academic requirements.

### Milestone deadlines

Please ensure that you upload your milestones with the FTP account details you receive when you register for the project. If you require an extension, email [admin@blueicon.com](mailto:admin@blueicon.com) with your team details and a reason for the extension.

Team milestone dates for 2011			
No	Milestone	Deadline single semester teams	Deadline double semester teams
1	Inspection of TAIS Alpha Environment	11 March	11 March
2	Inspection of BI3 Alpha Specification	18 March	18 March
3	Deploy "Isolated Bluebrick© Alpha"	28 March	28 March
4	Alpha compliancy assessment	1 April	1 April
5	Inspection of TAIS Beta Environment	8 April	8 April
6	Inspection of BI3 Beta Specification	15 April	15 April
7	Deploy "Secured 2 party communication"	22 April	22 April
8	Develop a TAIS Beta Environment exploit	6 May	13 May
9	Beta compliancy assessment	13 May	20 May
10	Invoke TBE exploit	27 May	10 June
11	Conclusions and recommendations	3 June	17 June
12	Inspection of TAIS Gamma Environment	N/A	8 July
13	Inspection of TAIS Delta Environment	N/A	22 July
14	Inspection of TAIS Epsilon Environment	N/A	12 Aug
15	Inspection of TAIS Zeta Environment	N/A	26 Aug
16	Case study: Preventing a WikiLeaks scenario with TZE	N/A	9 Sep
17	Use case: Protecting state secrets with TZE	N/A	23 Sep
18	Use case: Protecting mobile data with TZE	N/A	7 Oct
19	Conclusions and recommendations	N/A	14 Oct

### Change of scope

If the specification becomes subject to change then you will receive a notice for change of scope. This Industry Project involves a number of participants globally, so teams will be required to integrate changes to the material that may arise during the project into their results.

### Registration process

Teams are required to register via email to [admin@blueicon.com](mailto:admin@blueicon.com) before the 7 March 2011.

The email should including the following information:

- The name and country of the academic institution in which the team is enrolled
- The full name and email of the supervisor of this project from your academic institution
- Full names, mobile and email addresses where possible for each team member
- Identify if this is a single or double semester project being undertaken
- Including any feedback or marking assistance that may be required by your supervisor

### About the Theory of Absolute Information Security

TAIS is different from other security models because it provides a complete recipe to achieve zero risk security. Other models (at 2010) generally provide good advice on security policy and procedure in order to reduce risk, but never purport to be able to eliminate the information security breach. Other models focus only on system or machine security, but are vague on the topic of protecting information itself. Most worrisome is that a security breach is likely to go undetected, such as in the case of WikiLeaks where authorised personnel forwarded information to unauthorised parties. TAIS specifically prevents information being accessed by unauthorised persons, even if it has been forwarded to them because information is retained and accessed from the secured grid and is never copied to devices on which it is consumed. Although collectively, the existing security models may indeed help, they are more like an ambulance at the bottom of the cliff instead of extinguishing the source of the fire. TAIS is designed to provide a bullet-proof formula for the protection of state assets at a government or military level.

TAIS provides a clear roadmap for achieving total security, and where the implementation costs become too high, it enables engineers to objectively measure the accumulated risk when the deployment is degraded, and most importantly, TAIS allows information access to be governed by this risk function so that critical data, such as the diplomatic content in the WikiLeaks case, can be prevented from being handled by components that do not present a suitable risk profile.