

## 2012 recommended TAIS research topics

The following topics are recommended as areas of study for TAIS because they cover the most important assumptions of the theory and do not expand the scope too quickly. These topics are ideal for publication or masters topics.

All participants will have access to pre-release versions of the Blueicon-CDN (IDE) whose alpha release has not yet been scheduled. Write to [admin@blueicon.com](mailto:admin@blueicon.com) for more information.

### **(A) Practical application of TAIS to secure cloud deployments using budget mobiles phones**

This topic applies the TAIS-Beta-Environment to solving the machine security problem by way of a firewall and single communication port. The security proposition is straightforward: Nothing can connect to the server, so the content distribution system remains safe. The single communication port is secured by firstly verifying that the port bind passed correctly and secondly by encapsulating the management of the communication protocol at a level of scope that prevents it from interfering with the node host running on the machine being firewalled. This topic does not cover information security (TAIS-Zeta-Environment) and so does not attempt to secure the end-points that host the content being consumed. This topic is current because the majority of cloud providers today will legally remove any warranty relating to the security of the Virtual Machine. Industry protocol is to push the responsibility of security to the customer. This topic shows that security can now be bundled with cloud providers directly with no additional risk when using the TAIS approach.

### **(B) The exploration of TAIS as a robust framework in the securing of both machines and information**

This topic addresses all 6 TAIS security environments. It provides a broad analysis of how TAIS can provide security for both machines and information in robust architecture that can be partially implemented in a manner that results in a security profile that can be measured. The topic explores the TAIS methodology that considers 3 primary independent and related aspects of security: Theory, Specification and Deployment; and compares this to the industry standard of penetration testing of a specific deployment that lacks a supporting security model that is complete and yet defines a secure system. This topic explores the ever growing threat of targeted attacks by the installation of Trojans in spear-phishing type exploits. The topic examines the advantages of the TAIS model and resulting deployment that remain unchanged and secure over its use; and is compared to today's shifting IT landscape where Trojans can render previous penetration testing worthless. Finally, the topic assesses the feasibility and challenges of obtaining a formal proof for TAIS at some point in the future.

### **(C) Evaluating the TAIS Security Rating (TSR) as an effective corporate wide security metric**

This topic explores the effectiveness of a single dimensional rating system for information security. It explores the accuracy of the metric as well as its usefulness inside organisations where non-IT personnel may be required to understand security decisions without understanding the detail itself, such as in a budgeting scenario. This topic explores how TAIS represents a budding new approach to information security because an idealistic fully secure model can be easily modified to make it easier to implement and yet retain a high security profile.

**(D) A novel way to secure processes residing on an unbounded distributed computing system whose nodes may be compromised**

This topic is groundbreaking because it shows for the first time how a network containing some compromised machines can still be used securely to run distributed computing tasks. This topic studies the TAIS-Gamma-Environment in detail to show how compromised machines can still be used as part of the transport layer, provided they are never used to hold private asymmetric keys or the symmetric encryption keys themselves. The topic goes further to show how these compromised machines cannot corrupt other peer machines in the distributed network. The implications for science and business are huge because today's grids are centrally managed and code running on these machines needs to be carefully verified as trusted. The grid network deployed in this topic is unbounded and decentralised. Nobody owns it, yet it is secure and stable. The topic is supported by the Blueicon-CDN network on which experimental deployments can be run using web-browsers or mobile phones installed with a secure "Blueicon-CDN player".