

Potential Master and Doctorate topics relating to BI3 grid network

A model for the encapsulation of information within a secure network

By utilising the natural scoping properties of sets, information can be encapsulated so that it cannot be move beyond predefined zones. This method can be used to build on the user-model to provide a more robust authentication system that keeps information stored in the grid (or cloud) and prevents leakage at point of usage on the device.

A model to seamlessly migrate information from a private to public space

Information can be bounded and held securely in a grid (above), but allowing that information to be accessed publically presents many issues. Besides the economic management of resources in the public infrastructure, information presentation must be addressed. Provided the zone within the information is held is configured to allow public access, any information unit it contains can be released into the public domain. The thesis presents a model to transfer this

information while allowing each access to guarantee royalties to the user while appropriate taxation is applied. Information must be able to be restricted and conform to international surveillance legislation.

A model to operate a secure public grid network

A model is presented that enables an interconnected, unbounded and open grid network to operate as a secure fabric. The thesis explores how mobile agents on the grid can attain security while utilising resources that may be insecure. By adhering to a strict formula of launching processes only on trusted machines and using symmetric encryption to store or transmit data across non-trusted nodes, the grid fabric as a whole can be viewed as trusted.

A model to break the online payment deadlock

Users today expect information on the internet for free, partly because the transaction costs are too small and the risk

and effort of credit card use exceeds the value of the content. This problem is exacerbated due to the Web 2.0 architecture that requires repeated authentication for each web-site, instead of a single virtual desktop with global authentication. A new model is examined where computational resource is sold on a grid network to high usage customers (such as the Large Hadron Collider) and the credits used to establish a new content based economy. Discussion is also included as how this can solve the music and newspaper revenue problems relating to online payment.

Development of a grid and on chip architecture that avoids the von Neumann Bottleneck

As chip manufacturers battle the laws of physics to improve the performance of chips, they have begun to include more core processors in a bid to stave off physical limitation of data transmission at the bus. Although gains appear substantial, the bus connecting the on board cache with the main memory is the bottleneck by an order of

magnitude. This new computer architecture uses non-random access arrays to store memory so they can be cached at any point, either on chip or across a grid. Ultimately, an implementation in FPGA is discussed that could revolutionise chip design, increasing performance tenfold with an identical CMOS fabrication process as regular boards.

A model to enable forward and backward compatibility while enabling dynamic upgrades

Applications, Platforms and Operating Systems have traditionally posed the classic forwards compatibility problem where new applications cannot execute on older systems, and often without the correct architecture, old applications will not execute on newer systems. This model provides a Universal Virtual Computer (UVC) that can represent all information in a manner that doesn't require compulsory upgrades. However, to allow for future modifications, the model presents an architecture that enables the upgradability of the grid fabric piecemeal without service

disruption and without the need to convert information into newer formats.

A model to prevent Denial of Service attacks using a Point-to-Point routing infrastructure

The TCP/IP protocols are limited in their ability to manage the source address space and so are open for bogus header attacks such as denial of service. A new approach to networking using Point-to-point connections and routing agents prevents such attack by fully authorising the complete Point-to-Point route. Discussion is also made on how this can be used for surveillance legislation compliance.

A model to enable the seamless legislative compliance of content between nation states

A model is presented that allows users to publish information on a global platform while simultaneously allowing individual states to ban information at a national level. Additional provision is made to ban information globally if required. The model also allows for content to generate revenue on access. Copyright holders and patent infringements can be

addressed through banning or through the reclaiming of stolen revenue. Discussion is made as how the redistribution of nation state revenue through tax collection can be used to enforce international treaties such as Carbon Emission Trading by deducting the shortfall from the collective tax take generated by the nation state's citizens.

A model to prevent the Malicious Client Problem and remote attack of the host computer

The Malicious Client Problem and remote network attack can make machines vulnerable unpredictably. Once compromised, the machine presents the Malicious Host Problem and can re-infect other hosts. A novel model is discussed that can prevent the Malicious Client Problem as well as reducing the implementation footprint to ensure the deployment conforms to this theoretical model. Discussion is included to the broad reaching consequences that could be achieved by stabilising and securing Cyberspace.

Potential Research papers

A Novel Method for the Prevention of the Malicious Client Problem Using Segmented Memory Overlaid with Managed IO

This paper outlines an alternative approach to preventing an application from attacking the host execution layer by way of separating the memory of the Application and Operating System at the hardware level and enabling communication between these isolated memory segments by way of a communication channel (bus) that transports encoded Sets that contain predetermined API instructions.

A Model to Identify and Measure the Factors Required to Guarantee Absolute Information Security

This paper defines the factors required to preserve information integrity and shows that no other unidentified factor is necessary for protection. The paper highlights the limitations of the implementation on achieving this idealised outcome.

A Model for Designing Security Architectures that Reduce the Implementation Footprint

This paper discusses a technique to reduce the implementation footprint of appropriate security architectures so that the software can be manual verified by a small trusted team. The paper also discusses how applications can be developed securely in the context of spy or renegade developers.

A Model for the Secure Storage of Data on a Grid Network by way of the Selection of Trusted and Fully Secure Nodes

This paper examines a model for disparate database implementation on an appropriate grid network that guarantees security. The paper shows how data security is guaranteed only if the integrity of Nodes on which data is stored is also guaranteed. The paper also shows how the grid can be used to virtualise

the data store so that it can hold the effective capacity of the network while managing torrents, backups and redundancy simultaneously.

A Model for the Elimination of Data Debris through Active Storage

This paper explores how data can be absolutely destroyed by guarantying Node security and avoiding backups. By rotating the symmetric encryption keys and always holding data in an active form, deletion is absolute.

A Model for the Encapsulation of Information in the Context of Disparate Access Points.

A Novel Approach to Network Access Control by way of Overlaying an Encapsulating Zone Structure with a Directory Structure.