

AN INTEROPERABLE INFORMATION INFRASTRUCTURE (III) MODEL

Dr Kay Fielden
UNITEC Institute of Technology
kfielden@unitec.ac.nz

ABSTRACT

In this paper design of an interoperable information infrastructure (III) model is discussed as a potential solution to the escalating problem of malicious use of the existing Global Information Infrastructure (GII). The III is a potential subset of the existing GII. The III model is an abstract specification designed to ensure that the total GII complexity does not overwhelm its human operators. A proposed architecture to provide seamless trans-coding of information between platforms is also described. Future implications for a GII that is underpinned by the III model for automated governance, political, social and economic issues are areas identified as requiring further research.

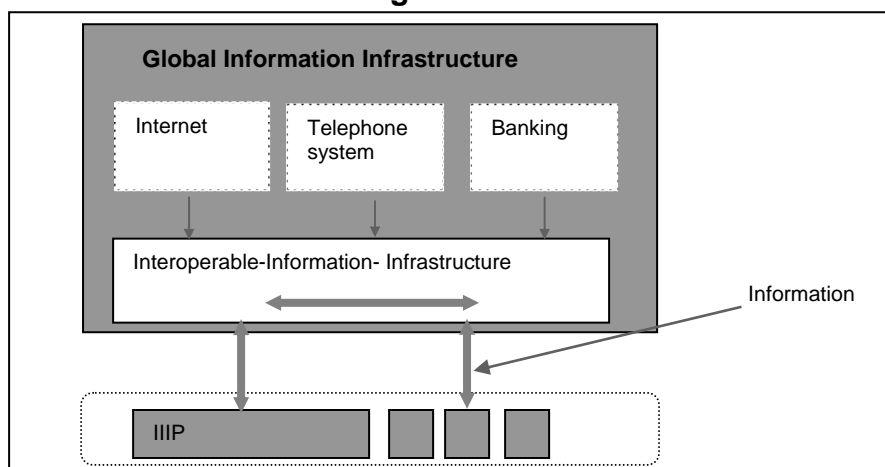
INTRODUCTION

The research carried out to date on the design of an interoperable information infrastructure model at Manabars Internet Technology suggests that a sound business platform based on an III is not only credible but economically viable. A holistic business view has been adopted in exploring feasibility of an III that includes technical concepts (peer-to-peer, grid, ubiquitous computing, utility computing, abstraction, virtualisation), political concepts (terrorism and crime management, implementation of legislation in a digital environment such as wiretaps and banning of illegal information) and economic concepts (trading of autonomous software agents, automated taxation and accountancy and embedded charging). These concepts have been developed into the Interoperable-Information-Infrastructure (Figure 1).

A CALL FOR A MORE VIABLE III

Figure 1 shows the relationship between the Global Information Infrastructure (GII) that includes the Internet, telephone and banking systems, all of which may be connected to the Interoperable Information Infrastructure (III). The III is a subset of the GII and represents the centralised platform on which digital businesses may operate in a seamless and orderly manner. An individual Interoperable Information Infrastructure Provider (IIIP) is an implementer of the abstract III specification (a behavioural model containing rules and properties) that the IIIP implementation must possess to enable interoperability. Individual organisations may profit from the development of an IIIP.

Figure 1 III Model



Global Information Infrastructure (GII)

The Global Information Infrastructure (GII) (Figure 1) is the inevitable framework that results from the economic, social and political need for information to be exchanged in an agreed and acceptable manner. It is the resulting collection of platforms, protocols and interfaces that can be identified as a GII. Research into a GII from political, social, economic (Blakely, 2002) and technical points of view have been conducted. Whilst there have been attempts to establish global alliances (Magee, 2002, OECD,2002,

Shaw, 1999, *P2P, Web Services, Wireless, and Beyond: O'Reilly Emerging Technology Conference*, 2002), this has not been achieved so far. The III (a subset of the GII) is an abstract specification that represents the highly coordinated and initially centralized effort to enable legislation to operate seamlessly for all information. When the III is completed, it is anticipated that it will drive efficiencies in a digital economy over a peer-to-peer network of computers that execute a common platform that allows for the representation of all information and provides legislative boundaries through which people and business can trade digital assets in a completely secure and accountable way.

Perfect Encapsulation

Perfect encapsulation incorporates both scope and resource protection. Perfect encapsulation prevents two separate objects that have never encountered each other from affecting one another. Perfect encapsulation also requires that an object utilize only a single storage area, thus preventing software from leveraging on alternate storage points to gain access. Perfect encapsulation is a necessary condition required to protect the reference membrane (Figure 5). The reference membrane is constructed as software within Layer 3.

E-security

There is an ever-increasing need for more secure distributed systems and much has been written on this topic. (Camp, 2002) suggests that marketplace incentives to prevent piracy and hacking need to be researched. This is indicative of the international direction for research in this field. The III model described in this paper focuses on redesign to obviate the need for preventative measures. (Cybenko, Giani, & Thompson, 2002) have researched the economic value of hacking and explored cognitive profiles as a strategy to reduce the economic effects of hacking. This is research into strategy and direction after a security breach has taken place (Drozdova, 2002). There appears to be no research that has been published in the public domain about similar revolutionary operating systems design. (Blum, 1994) and (Bohr, 2001) have researched prototyping, implementation and testing to provide a secure interoperable distributed operating system. (Blakely, 2002) however, suggests that traditional security models do not work with Internet security. He suggests that most IT security systems fix the 'broken bits'. (Gehring, 2002) has explored the loss of intellectual property and the economic value associated with this. (Hann, Hui, Lee, & Png, 2002) has also explored economic issues involved with e- security. (Lipson, 2002) has written a major report on tracking and tracing cyber attacks.

E-security, provided by the reference membrane (Figure 5) and perfect encapsulation is a core design feature of this III.

Acceptance Factors for Radical Redesign

(Fisk, 2002) has explored social acceptance of extreme security measures. (Agre, 2003) has explored social, political and economic factors influencing the acceptance of innovative design. (Young, 1977) has taken a whole systems approach to radical redesign and proposed a theory of temporary structures. Young's theory is the only

whole systems theory in this literature review that took a whole systems view of radical redesign. Dominant paradigm thought and research in providing trusted and secure digital business facilities, and technical global networked infrastructure rules against acceptance of radical redesign.

Managing Complexity

(Ganek & Corbi, 2003) have explored managing complexity in large distributed systems from the point of view of autonomic computing. Exploration from a whole systems point of view for large virtual networks has been carried out by (Bolosky et al., 2002). (Landwehr, 2002) explores how to improve information flow in a secure virtual market place. (Park & Willinger, 2002) have researched the Internet as a complex system – but have no solutions on how to deal with the complexities. (Seel, 2000) has explored complexity issues from a whole organization point of view. (Willinger, 2002) has explored the issues of scale, complexity and control with large distributed systems. A key element in reducing complexity is addressed in this proposed III model by providing stable building blocks that will not change after initial implementation.

Conceptual Model Development for Global III

(Linger, 2000) has researched lifecycle models for survivable systems. This appears to be the academic approach being taken by the CERT Center at Carnegie Mellon University in the USA. The approach adopted with the III model described in this paper does not use this heavily engineered approach.

III DESIGN OBJECTIVES

Design objectives for an Interoperable Information Infrastructure (III) model include holistic, (rather than evolutionary) design, manageable complexity, freedom from malicious use, seamless information interchange, economic accountability, cost-effective security, low critical mass for adoption, self-preservation and computational completeness. Malicious use of the existing GII is the motivating force in this radical redesign.

A revolutionary redesign on an III is proposed that incorporates the following design features:

Holistic Design

Holistic design is one of the main design objectives. It is anticipated that with intelligent holistic design underpinning global digital business, both economic and political stability at a global level is more likely to be achieved. By avoiding an evolutionary design approach, the negative properties of stickiness and complexity can be avoided. Stickiness is encountered when protocols or standards have become embedded as standard within the industry. These standards or protocols are then extremely difficult to change. Complexity becomes a negative property when the economic cost of managing the system escalates faster than the level of complexity due to the time taken to understand system procedures and/or outcomes.

Manageable Complexity

As the dimensions of complexity increase so the potential for human operators to manage the III successfully decrease. People must be able to manage whatever III is in place. By adopting a revolutionary redesign, the inherent complexities of evolutionary operating system design can be minimised.

Harm Minimisation

The nature of revolutionary or holistic redesign provides opportunity to close entry points for malicious uses or processes in evolutionary systems.

Interoperability

Information exchange without trans-coding or conversion has both economic and data protection advantages. In the III, Common-Factor-Interoperability (where a platform is capable of emulating other platforms) is the design objective. Semantic-Interoperability (in which meaning is assigned to interfaces) is beyond the scope of the III.

Accountability

Accountability is a primary property of the III. Both measurement and enforcement of payment for resources used is a primary design requirement and a necessary requirement for a digital economy. Digital businesses have both costs and income and economic gains within a digital economy are subject to taxation.

Global Trading of Digital Assets

Assets on the III are intellectual or computational machines rather than material. Intellectual (or information) assets can be represented, protected and sold within the III. Music, video, games, software, designs and processes are all examples of intellectual assets. Trading by digital businesses in these assets only requires automated legislative rules. Computational machines support the III generate revenue for their owners and in doing so form the foundation of a global trading platform. Static-Content, such as music or movies can be protected through rules applied at the Governance-Layer (Layer-3) whilst Active-Content, which is information that is interactive and contains process, is protected by hidden processes (Layer-4) (Figure 6).

Security

Security is paramount to the successful operation of the III. Basic factors that drive the security features are (1) the probability of a security failure and (2) the cost of the failure. Combining the III design objectives of security and accountability creates a dynamic and efficient environment. Software components should be able to choose their own level of security. This level of security is related only to the amount of money software is prepared to spend. This foundation philosophy prevents rogue processes from launching any meaningful attack. If an attack can be launched then it will most probably not be worth attacking.

Minimal Migration

It is important that introduction of the III does not require a critical mass for adoption to take place. Whilst this is technically more difficult the rewards are greater. The non-requirement of critical mass helps the III become a self-fulfilling prophecy as businesses can commit with the knowledge that the platform will not collapse because of critical mass issues. Businesses are more likely to commit to migration if they know that the platform is robust with minimal industry uptake. Early adoption for mobile computing reduces implementation costs and eases the hurdles of entry that accelerate adoption. Virtualisation of legacy technology is another factor that supports minimal migration.

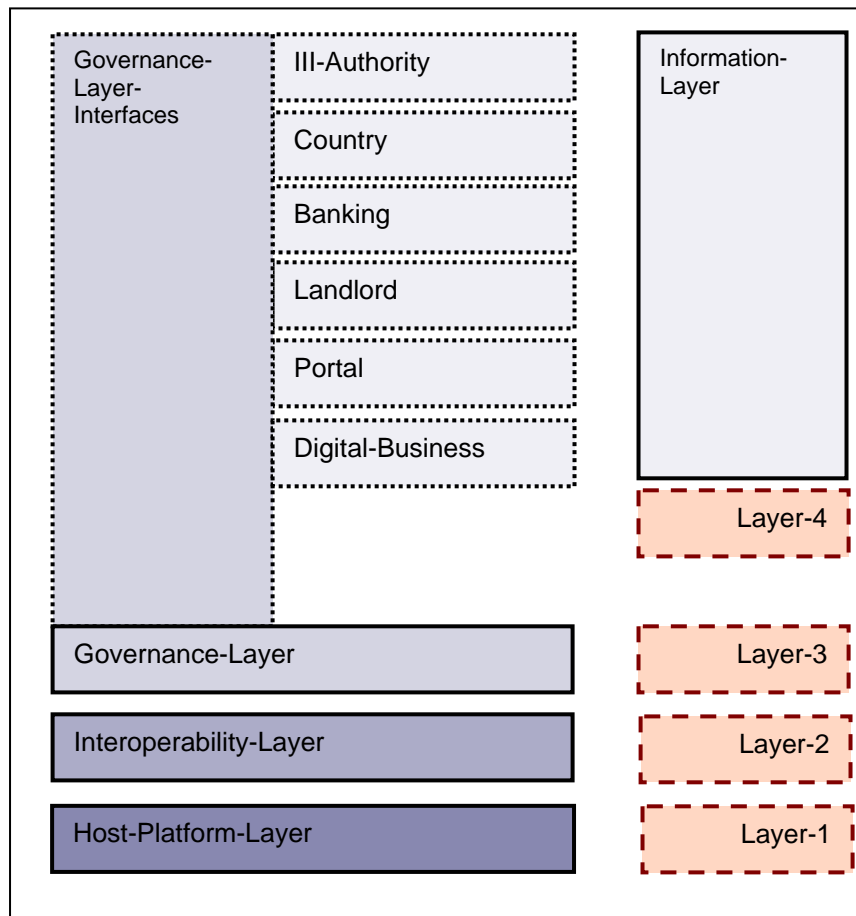
Self-preservation

Self-preservation design features adopt a two-tier strategy. Firstly, the III should be complete so that new infrastructure is not required and secondly, the III should be able to prevent other non-compliant networks from being able to establish themselves. Logical rather than physical governance is required to support this strategy.

Inflexibility

Ideally, holistic design incorporates the whole architecture at design time. Such systems are inflexible as the model that defines the structure is completely separate from the system, leaving limited options for an intelligent real-time response when the environment diverges from the original operating parameters.

Figure 2 Four-Layered View



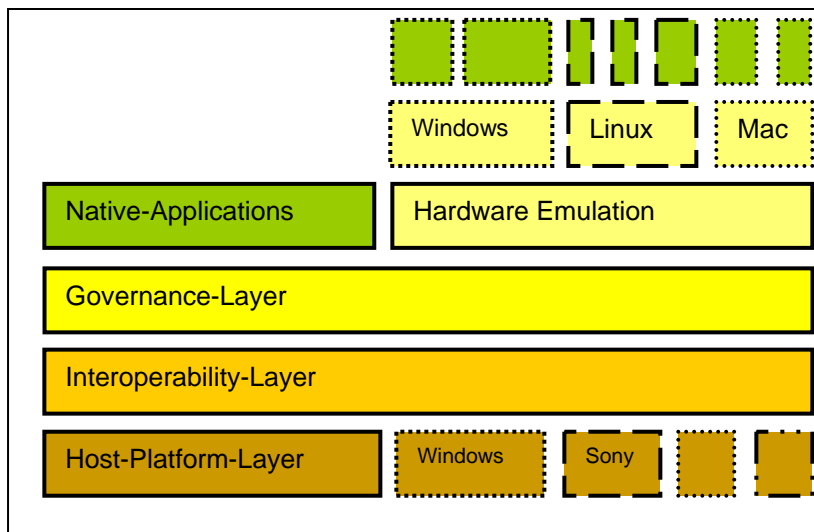
PROPOSED III ARCHITECTURE

In adhering to the established design goals to reduce complexity, the III is broken down into four layers (Figure 2).

Four-Layered View

Layer-1 is the platform on which the Interoperability-Layer (Layer-2) executes. This can be hardware and/or software. The only requirement is that Layer-1 can execute or implement software and is therefore computationally complete.

Figure 3 Interoperability View



Layer-2 is the Interoperability-Layer. It is the only software required for each specific target platform in Layer-1. The remaining architecture in Layer-3 and Layer-4 is virtual and is constructed entirely from the Interoperability-Layer.

Layer-3 is Infrastructure and is concerned with governance both legally and mechanically. This software is supplied by the entity responsible for the management of the III and is known as the III-Authority.

Layer-4 is any information in the form of a digital business. All information that exists as a digital business must communicate with the underlying infrastructure through the Governance-Layer-Interfaces (Figure 2) that enable their action to be meaningful in a legislated environment.

Interoperability View

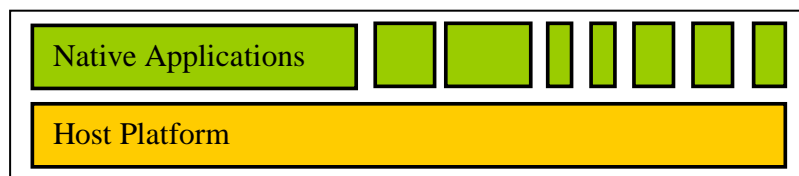
The III model enables Common-Factor-Interoperability by porting the Interoperability-Layer (Figure 3) to multiple platforms that within the Host-Platform-Layer. Common-Factor-Interoperability arises when a platform is capable of the emulation of other platforms and behaves as the lowest common denominator. All information on the III is

constructed from a finite set of components. Documents originating from different operating systems such as Linux and Windows can therefore be observed in parallel views at the same time.

The Interoperability-Layer emulates multiple platforms constructed from itself, allowing everything for which there are emulations to run on everything for which there are ports for the Interoperable-Layer.

This is in contrast to the traditional model, where specific applications must execute on a single platform, and there is no common context on which to share other software (Figure 4).

Figure 4 Traditional Model



Using Common-Factor-Interoperability, the III can allow software to exist within the same meta-context, although it does not allow software to interoperate at a semantic level, such as with XML.

The Scope View

The Scope View expands the virtual components of the III model (Figure 6).

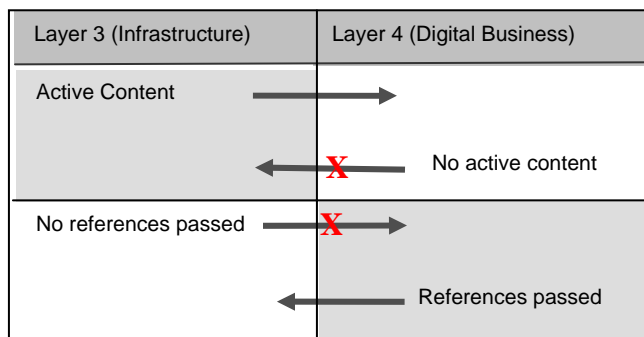
The Governance-Logic drives the behaviour of an III node. It is contained within the Governance-Layer (Layer-3) and is constructed from the Interoperability-Layer, so it is virtual. The Information-Layer (Layer-4) is contained within the Governance-Logic and is an array of digital businesses on the III node. An III node is defined as the integration of layers 1-4 operating as a node on the III network.

Each digital business is able to utilise the appropriate Governance-Layer-Interface to communicate with the outside world. During this communication process, all references and process should be stripped out at the Reference-Membrane to prevent the transfer of references from Layer-4 back into Layer-3 – which could corrupt the infrastructure and empower mal-ware.

The Reference-Membrane

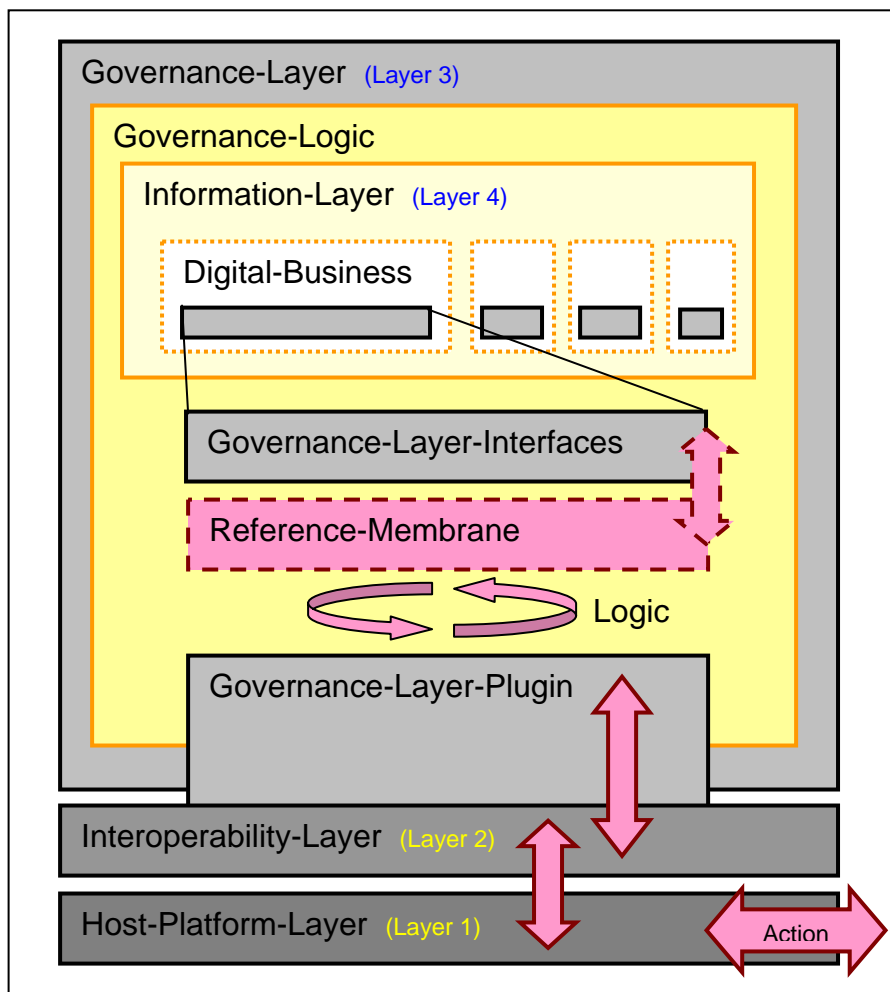
The Reference-Membrane preserves Layer-3 infrastructure integrity acting as a filter to strip out all Active-Content and references from communication between the Governance-Layer-Interfaces and the Governance-Logic. Active-Content also uses components from the Interoperability-Layer that enables computational completeness. The Reference-Membrane is critical in preventing the transfer of references between Layer-3 and Layer-4 as this transfer of references could otherwise lead to the corruption of the III-Node and to allow mal-ware to propagate.

Figure 5 Reference Membrane



The Reference-Membrane prevents unknown software from establishing or gaining access to references within the Governance-Layer (Layer 3), even though information is exchanged. This is possible because an internal reference is never exchanged directly from the governance layer to a digital business (Figure 5). The Reference-Membrane also prevents any Active-Content from being exchanged from a digital business back to the governance layer, whether known at design time or not. All information structures within Layer 3 conform to both scope and resource principles of Perfect-Encapsulation

Figure 6 Scope View



that (1) prevents two separate objects that have never encountered each other from affecting the other; (2) allows only a single storage area for any object, thus preventing software from leveraging on alternate storage points to gain access; and (3) provides resource protection.

The inability of software to interfere with the infrastructure integrity prevents it from attaining privileges associated with the governing structure. This means that software can be handled safely and obviates destructive processes.

Governance-Layer-Interfaces

These interfaces force digital businesses to communicate with the outside world via the Governance-Logic rules.

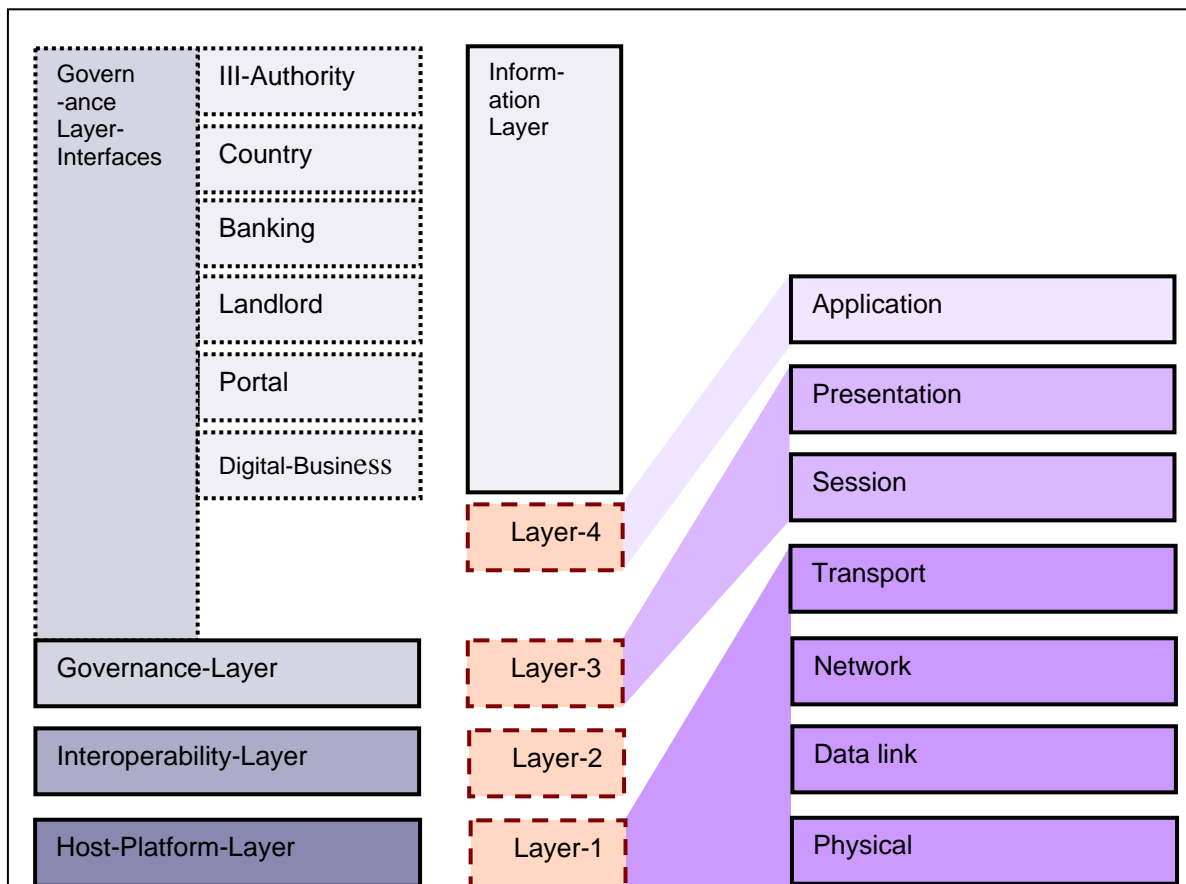
Digital Business

A digital business is only capable of accessing objects that it has references to on the Layer-2 Interoperability-Layer. Digital businesses do not access references on other III-Nodes directly.

Interoperability-Layer-Interface

The Interoperability-Layer-Interface is a reference within the Governance-Layer that allows the Layer-2 Interoperability-Layer to move information between the virtual Layer-3 Governance-Layer and the physical world via Layer-1 Host-Platform-Layer. This is

Figure 7 ISO View



where activity is translated between the real and the virtual realms. The Layer-2 Interoperability-Layer uses the Interoperability-Layer-Interface to: (1) move bandwidth content to partner on a peer-to-peer network; (2) communication with the Host-Platform display equipment; (3) communication with the Emulator on the Layer-1 Host-Platform to manage resource usage; and (4) execute virtual software in Layers 3 & 4 to enable computational completeness.

The ISO View

Figure 7 (The ISO View) shows that the III model does not clearly fit into traditional structures.

The III model collapses the 7-layered ISO view into Layer-1, Layer-3 and Layer 4 as well as providing a superstructure outside of this traditional view.

IMPLICATIONS FOR THE FUTURE

Future implications for a GII that is underpinned by the III model for automated governance, political, social and economic issues are areas identified as requiring further research.

Automated Governance

The III should enable software to operate in a stable legislated environment thus providing automated governance. Legislation on the III should be kept solely to the trading of digital assets or judicial orders. Many issues arise concerning automated governance including: (1) the need to explore who should be responsible for the automated governance supplied to the Governance-Layer; (2) the impact on the open market for computational resources; (3) the effect of enforced accountability on the III; and (4) the impact of a mal-ware free, legislated, interoperable system.

Political, Social and Economic Issues

Research is needed into acceptance of such an interoperable information infrastructure on all levels including political, social and economic. There are many issues regarding legislation to be resolved for multiple views.

CONCLUSION

In this paper a revolutionary design for an III model has been presented. The proposed model has been designed holistically to address complexity and 'stickiness'. The critical requirement for a global system that is secure is also at the core of these design principles. This model has the potential to satisfy international needs for a secure, accountable, legislated virtual environment in which digital business may operate. Such a distributed trading environment provides a sound basis on which to base the world's digital economy.

This III model provides a starting point for further research into technical, political, economic and social views of this revolutionary concept.

Company Information

Manabars Internet Technology is a Joint Venture Partnership based in Auckland New Zealand. This privately funded Joint Venture was formed in December 2000. Any enquiries should be directed to the Chairperson, PO Box 46253, Herne Bay, Auckland, New Zealand.

Author Information

Associate Professor Kay Fielden is the Research Co-ordinator for the School of Computing and Information Technology at UNITEC Institute of Technology. She is also the academic adviser to Manabars Internet Technology on the development of the III model.

REFERENCES

- Agre, P. (2003). "Peer-to-Peer and the Promise of Internet Equality". **Communications of the ACM**, 46(2), 39-42.
- Blakely, B. (2002). "The Measure of Information Security in Dollars. Paper presented at the 1st Workshop on Economics & Information Security, University of California, Berkley, May 16-17.
- Blum, B. I. (1994). "A Taxonomy of Software Development Methods". **Communications of the ACM**, 37(11), 82-100.
- Bohr, A. (2001). "Software Component Testing Strategies" **Technical report No. UCI-ICS-02-06**, June 2001. Irvine: Dept of Information and Computer Science, University of California.
- Bolosky, W. J., Draves, R. P., Fitzgerald, R. P., Fraser, C. W., Jones, M. B., Knoblock, T. B., et al. (2002). "Operating Systems Directions for the Next Millennium" **Microsoft Research**.
- Camp, L. J. (2002). "Marketplace Incentives to Prevent Piracy: An Incentive for Security?" Paper presented at the **1st Workshop on Economics & Information Security**, University of California, Berkley, May 16-17.
- Cybenko, G., Giani, A., & Thompson, P. (2002). "Cognitive Hacking & the Value of Information." Paper presented at the **1st Workshop on Economics & Information Security**, University of California, Berkley, May 16-17.
- Drozдова, E. (2002). "Dealing With Low-Tech Terrorist Communications in the Hi-tech Age: Toward a Theory of Fault Intolerant Network Organizations." **23rd International Conference on Information Systems**.
- Fisk, M. (2002). "Causes & Remedies for Social Acceptance of Network Security". Paper presented at the **1st Workshop on Economics & Information Security**, University of California, Berkley, May 16-17.
- Ganek, A. G., & Corbi, T. A. (2003). "The dawning of the autonomic computing era." **IBM Systems Journal**, 42(1), 5-18.
- Gehring, R. A. (2002). "Software Development, Intellectual Property Rights and IT Security." Paper presented at the **1st Workshop on Economics & Information Security**, University of California, Berkley, May 16-17.

Hann, I.-H., Hui, K.-L., Lee, T. S., & Png, I. P. L. (2002). "Online Information Privacy: Measuring the Cost-Benefit Trade-off." **23rd International Conference on Information Systems.**

Landwehr, C. E. (2002). "*Improving Information Flow in the Information Security Market.*" Paper presented at the **1st Workshop on Economics & Information Security**, University of California, Berkley, May 16-17.

Linger, R. (2000). "Lifecycle Models for Survivable Systems". **US Department of Defence** and Carnegie Mellon University.

Lipson, H. F. (2002). "Tracking and Tracing Cyber Attacks: Technical Challenges and Global Policy Issues" (**Final No. CMU/SEI-2002-SR-009**). Pittsburgh: Software Engineering Institute, Carnegie Mellon University.

Magee, M. (2002). "Trusted Computer Platform Alliance is a Secret Cabal." *The Inquirer*.
OECD. (2002). "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security."

P2P, Web Services, Wireless, and Beyond: O'Reilly Emerging Technology Conference. (2002, May 13-16). Paper presented at **The O'Reilly Emerging Technology Conference**, Westin Santa Cara.

Park, K., & Willinger, W. (2002). "The Internet as a Complex System: Scaling, Complexity and Control" **Santa Fe Institute**.

Seel, R. (2000). "Culture and Complexity: New Insights on Organisational Change." **Organisations & People**, 7(2), 2-9.

Shaw, M. (1999). "Research Opportunities in the Virtual Agora: Market Aspects of Open Resources Coalitions." Pittsburgh: Computer Science Dept, Carnegie Mellon University.

Willinger, W. (2002). "The Internet as a Complex System: Scaling, Complexity and Control" **Santa Fe Institute**.

Young, T. R. (1977). "Radical Dimensions of Modern Systems Theory: A Theory of Temporary Structures, Parallel Structures, Underground Structures and Conflict Structures." **Transforming Sociology Series**, 020.