

RNSA Sponsored U.S. Visit Report:

Jason Smith, Research Fellow, Information Security Institute, Queensland University of Technology

Trip Itinerary

The 10 day trip to the United States, from April 20th through until April 30th, 2007 incorporated:

- visits to two Universities with extensive information security and critical infrastructure protection programmes
 - Purdue University's Center for Research in Information Assurance and Security (CERIAS)
 - University of Illinois' Urbana-Champaign Information Trust Institute (ITI)
- attendance of the Second Workshop of the EU/US Summit Series on Cyber Trust: System Dependability & Security.

Summary of Meetings and Outcomes

Purdue University CERIAS

In addition to meetings with key faculty members within CERIAS I was able to attend the Third Annual Midwest Security Workshop which was being hosted by Purdue. The programme included presentations in the areas of software systems security, privacy and information flow, and policies. The full programme is provided as an appendix (Appendix A) to this report.

Meetings relating to information and network security research were held with:

- Professor Eugene Spafford, Executive Director of CERIAS
- Associate Professor Sonia Fahmy
- Assistant Professor Cristina Nita-Rotaru

During these meetings, current research directions and priorities were discussed. Current research priorities within Australia are closely aligned with efforts being undertaken at Purdue, with the differences being related more to scale than substance.

On hearing of current research projects in Australia relating to incident response and forensics in control systems, Professor Spafford recommended the Chief Scientist of the Cybersecurity programme (Prof. Frincke) at the Pacific Northwest National Labs (<http://www.pnl.gov>) as a contact who would be able to help progress the project.

University of Illinois ITI

The Information Trust Institute at the UIUC campus is involved in the Trustworthy Cyber-Infrastructure for the Power Grid Project (<http://tcip.iti.uiuc.edu/tcip/>). During my visit to ITI was able to meet and discuss research directions and potential for collaboration with a number of key research academics, including:

- Professor William Sanders, Director of the Information Trust Institute
- Professor Carl Gunter, Department of Computer Engineering
- Dr Zbigniew Kalbarczyk, Principal Research Scientist, Coordinated Science Lab
- Professor Klara Nahrstedt, Department of Computer Engineering
- Professor David Nicol, Department of Computer and Electrical Engineering

The TCIP research program is focused on a broad range of efforts that seek to secure next generation control systems in a manner that extends from trusted hardware components, through to secure and trustworthy networks of systems. The Trusted ILLIAC program seeks to increase the trustworthiness of systems by integrating trusted hardware components, hardware accelerated run-time execution monitoring of applications, and security and reliability techniques to facilitate the rapid recovery of systems subject to both malicious and non-malicious failures.

The research academics I met with were keen to hear about current research efforts in Australia to secure critical infrastructure and the potential for collaboration.

EU/US Summit Series on Cyber Trust

The final activity undertaken on this visit to the US was attendance at the Second EU/US Summit Series on Cyber Trust. This event was attended by approximately 40 researchers from the US, EU, Japan, and Australia.

The focus of this second meeting was to identify critical areas for international collaboration that would advance efforts to model, design, implement and evaluate secure and dependable next generation systems. The summit was attended by representatives from both the European Commission and the US National Science Foundation with the expectation that the ideas developed during this workshop would be useful in establishing significant collaboration between researchers from both the EU and the US.

Jacques Bus, European Commission

Jacques Bus described the current research funding arrangements for cybersecurity in Europe. In particular the upcoming call in September for "Trusted security for critical infrastructure protection" which will allocate approximately \$40 million euro's to research projects.

Jacques Bus expressed directly the ECs desire to collaborate with Australian researchers and requested that (political) avenues for this collaboration be explored.

Karl Levitt, National Science Foundation

Karl Levitt detailed the goals of the NSF's CyberTrust program, indicating that the program is necessarily broad. Strong candidates for collaboration and funding (in NSF's view) included:

- Next generation network security testbeds

- how such testbeds might be used for game theoretical analysis of network security and assist in determining the location of security components (on the edge or in the core of the network), and
- how existing testbeds could be interconnected - for example, how wireless and wired testbeds might be integrated to allow the modeling of heterogeneous network systems.
- “Future Internet Network Design” (FIND) research initiatives, involving
 - secure design, effective ID management, fault tolerance and recovery, and distributed trusted computing bases (TCBs)
 - the use of a “capabilities” based network architecture
 - the application of virtualisation technology to address dependability and security challenges
- Data confidentiality and integrity in research experimentation
 - how can large data sets be provided to facilitate research, while simultaneously preserving the confidential nature of information that such large data sets will invariably contain.
- NSF notes the success that DARPA has with the annual “Grand Challenge” it hosts
 - NSF considering a cybersecurity grand challenge. Candidate scenarios include:
 - e-voting security
 - secure network and systems design
 - SPAM prevention, detection and response
 - Worm defenses

Douglas Maughan, Department of Homeland Security

As program manager of the DHS Cyber Security Research and Development Center (<http://www.cyber.st.dhs.gov>), Douglas Maughan presented a summary of research efforts and achievements of DHS in recent times. Most notably:

- The requirement for US government agencies, through FISMA (<http://csrc.nist.gov/sec-cert/index.html>), to adopt DNSSEC
- Current efforts with APNIC investigating PKI based routing security
- Testbed development and support activities
 - DETER (<http://www.isi.edu/deter/>)
 - PREDICT (<http://www.cyber.st.dhs.gov/public/PREDICT/>)
- Upcoming project requests
 - Broad Agency Announcement for Cyber Security Research and Development (<http://www1.fbo.gov/EPSTData/DHS/Synopses/37711/BAA07%2D09/20070517143549%2Ezip>)

Workshop Overview

This second workshop aims to ensure progressive continuity of the consensus building achieved at the first workshop held in November 2006 in Dublin. The guiding principle was to identify and develop further those research areas that require and will benefit from international collaboration, while examining the structures and mechanisms (existing and/or future) that could potentially enable and fund the proposed work.

The approach is to identify a focused technical subset of interconnected themes. As a starting point, we propose two main S&D themes:

1. Architectures, Protocols and environments for the Security and Dependability (S&D) of future polymorphic networked Information and Communication Technology (ICT) systems
2. S&D attributes and mechanisms of future distributed services & content, future overlay networks & applications.

Delegates of the summit were required to provide written responses to pre-workshop questionnaire (QUTs response is provided in Appendix B) and during the summit were split into two groups with the task of identifying areas for collaboration in one of the two theme areas. Each group then provided a summary report back to the complete summit on the final day. A number of areas for collaboration, across both themes, were identified and will be pursued by the EC and the NSF. A report of the findings of the workshop is forthcoming and will be made available on the Information Trust Institute web page:

<http://www.iti.uiuc.edu/EU-US/>

Appendix A: Midwest Security Workshop Programme

9:00am to 10:00am

Breakfast and poster session (LWSN Commons Area)

10:00am to 10:10am

Opening remarks (LWSN 1142)

10:10am to 12:10 pm

Session 1: Software Systems Security (LWSN 1142)

- **Dynamic Malware Detection**
Somesh Jha (U. Winsconsin.)
- **The Search for Optimality in Automated Intrusion Response**
Yu-Sung Wu, Saurabh Bagchi. (Purdue)
- **Candid: Preventing SQL Injection Attacks using Symbolic Queries**
Sruthi Bandhakavi (UIUC), Prithvi Bisht (UIC), P. Madhusudan (UIUC), V.N. Venkatakrisnan (UIC)
- **An Architectural Approach to Preventing Code Injection Attacks**
Ryan Riley, Xuxian Jiang, Dongyan Xu. (Purdue)
- **Click fraud: slide effects of online advertising**
Mona Gandhi Markus Jakobsson. (IUB)
- **Usable mandatory integrity protection for operating systems**
Ninghui Li, Ziqing Mao, Hong Chen. (Purdue)

12:10pm to 02:10pm

Lunch and poster session (LWSN Commons Area)

2:10pm to 3:50pm

Session 2: Privacy and Information Flow (LWSN 1142)

- **TrustBuilder2: A Reconfigurable Framework for Trust Negotiation**
Adam Lee (UIUC), Marianne Winslett (UIUC), and Ken Perano (Sandia National Laboratories).
- **Privacy Graphs: A conceptual model for understanding privacy**
Jodie P. Boyer (UIUC)
- **Towards Efficient Detection of Stepping Stone Attacks With Spread-Spectrum Watermarks**
Amir Houmansadr, Negar Kiyavash, and Nikita Borisov (UIUC)
- **Data Sandboxing: A Technique for Enforcing Confidentiality Policies**
Tejas Khatiwala Raj Swaminathan V.N. Venkatakrisnan (UIC)
- **Do As I SaY! Programmatic Access Control with Explicit Identities**
Andrew Cirillo, Radha Jagadeesan, Corin Pitcher and James Riely (DePaul)

3:50pm to 4:20pm

Break (LWSN Commons Area)

4:20pm to 6:00pm

Session 3: Policies (LWSN 1142)

- **An Automated Framework for Validating Firewall Policy Enforcement**
Adel El-Atawy, Taghrid Samak, Zein Wali, Ehab Al-Shaer (DePaul), Sheng Li, Frank Lin, and Christopher Pham (Cisco)
- **SayAnything: A New Security Architecture for Authentication**
Jon Solworth (UIC)
- **EXAM -- a Comprehensive Environment for the Analysis of Access Control Policies**
Dan Lin (Purdue), Prathima Rao (Purdue), Elisa Bertino (Purdue), and Jorge Lobo (IBM Research)
- **Consistent Security Policy Enforcement in a Changing Environment**
Alan M. Carroll and Susan Hinrichs (Network Geographies and UIUC)
- **Towards High-level Firewall Policy Language for Multi-domain Networks**
Bin Zhang, Ehab Al-Shaer, Radha Jagadeesan, James Riely, Corin Pitcher (DePaul)

Appendix B: QUT Workshop Responses

Workshop Questions

2nd EU-US Workshop on Dependability and Security – April 26-27, 2007 -- Monticello, IL

Pre-Workshop Request from Participants

The breakout sessions will be run as a collective brainstorming exercise aiming to identify the key technical issues you see emerging in the respective theme areas. The objective is to identify the technical issues and also to prioritize the co-operation themes across the EU-US and participants from Australia and Japan. Given the above, in order to assist the Chairs in the smooth running of the breakout sessions, we would **request a brief contribution** (1-2 pages), **by April 20**, to Ms. Molly Tracy (mollyt@iti.uiuc.edu) and Ms. Shirley Olson (sla@iti.uiuc.edu) covering the following aspects, taking into account the **Criteria for International Collaborative Research on Security and Dependability** as set out in the accompanying document:

Theme 1: The interconnection across diverse computing and communication entities that would result in future pervasive networked information and communications technology (ICT) systems is already a reality while clearly the requisite security and dependability (S&D) elements to support trustworthy usage are still evolving. In order to systematically address the long term S&D issues in such polymorphic, mixed-mode and continually evolving networked environments, a clear characterization of the system and services model needs to be established where such S&D issues could meaningfully be scoped.

Please answer the questions labeled (a), (b) and (c) with the following guidelines in mind:

- "Prioritized Technical Issues to Address over the Next 3 years": Please articulate 2-3 specific technical answers for each question below that you see as key problems in the technical topics addressed by the Theme

- "Suggested Mechanisms to Establish EU-US Co-operation": Answers should take into account the mutual necessity and benefits of global co-operation that would justify and motivate the practicalities in establishing the co-operations.

(a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

(b) What do you foresee as the key technical issues/challenges in characterizing and scoping the development of architectures, protocols and overall system/service environments for S&D to be meaningful?

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above architectures, protocols and overall system/service environments for S&D?

Theme 2: The second thrust is on development of **attributes** and **mechanisms** needed to provide & enhance (on demand and at run-time), the desired security and dependability within the MME & across multiple domains, whether fixed or mobile. In addition to securing the “system,” there is a need to look at securing the applications and services which operate across these future polymorphic networked systems.

Please answer the questions labeled (a), (b) and (c) with the following guidelines in mind:

- "Prioritized Technical Issues to Address over the Next 3 years": Please articulate 2-3 specific technical answers for each question below that you see as key problems in the technical topics addressed by the Theme

- "Suggested Mechanisms to Establish EU-US Co-operation": Answers should take into account the mutual necessity and benefits of global co-operation that would justify and motivate the practicalities in establishing the co-operations.

(a) What are the key **Attributes** required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate **Trust Models, Security Models, Resilience and Dependability Models, Privacy Models** and **Trust/Security/Privacy Policies** within these future polymorphic networked systems?

(b) What are the associated **Mechanisms** needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay / Infrastructure solutions, large and small scale security, long term security, middleware solutions?

(c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

QUT Responses

Queensland University of Technology response to workshop questions.

Theme 1:

a) What do you foresee as the key challenges in specifying S&D in such unstructured and unbounded future ICT environments?

- The selection of an appropriate level of abstraction (or abstractions) for such specifications, would appear to be a significant challenge.

b) What do you foresee as the key technical issues / challenges in characterizing and scoping the development of architectures, protocols and overall system/service environments for S&D to be meaningful?

- Significant challenges associated with run-time security versus designing security in. Presumably, the components (or a subset of components) within polymorphic MME's will be required to exhibit

certain security and dependability properties. How will the minimum number of trustworthy components required to construct a trustworthy service be determined. How will the service user (or provider) detect when the number of components required falls below a minimum threshold and how will they react?

- Deciding where service intelligence lies (in the network or in the end points) and how this intelligence might migrate between the two, depending on context. Quality of service and denial of service resistance would seem to require intelligence in the infrastructure. Resilience and fault tolerance, intelligence in the end hosts. But in emerging MMEs, limited assumptions can be made as to the capability of end hosts, as they may be disposable, lightweight devices.

- Determining how intelligence should migrate between the edge and the core and the instantiation of this (virtualization??) will require advances in trusted systems technologies. Gaining assurance that such approaches can not be used against the system (via denial of service attacks for example) may be problematic.

c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above architectures, protocols and overall system / service environments for S&D?

On the assumption that some subset of components in future polymorphic networks must exhibit predictable properties, how can assurance of such properties be obtained? The scale of the systems involved would make current approaches to evaluation infeasible. Furthermore, the timeframes for evaluations are far too long to remain relevant to the dynamic nature of these emerging, unbounded infrastructures.

The dynamic nature of service provision, and the extensive use of proprietary underlying technology suggests a need for improved techniques for evaluating and assessing, in a blackbox fashion, the runtime behaviours of components, systems, and services. Such challenges would seem to be present not only in future networks, but emerging areas such as dynamically composed web services.

Assuming future networks are an order of magnitude greater in scale and contain highly heterogeneous components and technologies, efficient techniques will need to be developed for the evaluation of large, and most likely highly distributed, data sources. How can these data sets be efficiently distributed / accessed?

How will access to such data sets be secured to ensure that the information contained within them cannot be used to undermine the S&D of the infrastructure.

Theme 2:

a) What are the key Attributes required to enhance the dependability, security, and more broadly, trust features, and needed to define appropriate Trust Models, Security Models, Resilience and Dependability Models, Privacy Models and Trust/Security/Privacy Policies within these future polymorphic networked systems?

Identity is an important conceptual attribute in emerging MMEs. More particularly, layer appropriate concepts of identity will be required if there is to be any expectation that meaningful tradeoffs

between security and privacy are to be made. Determining the requirement for identity at the application, network and device layers is not yet fully understood, or specified, and the identity of individuals can be used inappropriately.

Other key attributes include the trustworthiness of devices (both hardware and software), assurance of compliant behaviours or the ability to assess (and possibly enforce) compliant behaviours.

b) What are the associated Mechanisms needed to improve S&D such as monitoring schema, adaptation mechanisms, overlays, protocols, crypto, CIP / Overlay / Infrastructure solutions, large and small scale security, long term security, middleware solutions?

Where trust in the hardware and software used by devices in a highly interconnected MME cannot be assured, mechanisms that permit the monitoring and evaluation of behaviour of such devices must be possible to ensure that these behaviours conform to expectations.

One specific area where this is a requirement already is the area of compliant cryptologic protocols. In compliant cryptologic protocols, two mutually mistrusting entities are able to ensure that the protocol they engage in conforms to specific requirements, requiring them only to trust in the design of the security system, not the other entity. In this way compliant cryptologic protocols act as a broker between the mistrusting entities.

Balancing the need for lightweight devices to leverage sufficient security (constrained by their computational and storage resources) and the provision of supporting infrastructure of a scale suitable for use in networks orders of magnitude larger than current networks is challenging.

While the use of virtualisation to address current problems is intuitively appealing, significant issues of trust, when virtualised instances of processes migrate between platforms for example, remain to be addressed.

The traceability of actions, in an environment where services are dynamically composed, and the preservation / accessibility of forensic evidence in polymorphic networks and MMEs will be far more difficult. Identifying the correct balance between security and privacy concerns of evermore pervasive systems remains an open problem.

c) What sort of test beds, data sets, and models for evaluation and validation would need to be put in place for assessing the above attributes and mechanisms for proof of concept and validation of the enhancement of S&D within these future polymorphic networked systems?

Fundamental problems in provable security suggest that current formal models of (cryptographic) security are unlikely to be able to deal with the complexity associated with analysing the protocols adopted by large scale MMEs, unless advances are made in the composability and reusability of proofs.