



Research Symposium, July 11-12, 2007

Workshop Five: Trustworthy and Secure Information Systems and Computing

Thursday July 12, 2:00 – 4:30 p.m.

Skempton Building, Room 228, Imperial College London

Chair: Larry Rohrbough, UC Berkeley

Overview

The role and penetration of computing systems and networks in our societal infrastructure continues to grow, and their importance to societal safety and the security has never been greater. Beyond mere connection to the Internet and access to global resources, information systems are now used for controlling critical infrastructures for electricity, healthcare, finance, and medical networks. As society uses computers, systems, and networks in increasingly important ways, the underlying technology provided often does not meet the desired level of trust and many critical infrastructure control systems remain untrustworthy. Viruses and worms sweep the Internet and exhibit increasing virulence and rate of speed that is also directly proportional to their growing ease of deployment. Privacy and security remain poorly understood, poorly supported, and generally inadequate. Broader issues of software usability, reliability, and correctness remain challenging as does understanding how users interact with computers and ways in which computers and systems can be designed to influence users to behave in a more secure manner. Exacerbating the problem, industry stakeholders are unable to recruit new employees adequately trained in security-related technologies.

This workshop will explore ways to address the challenges to developing, deploying, using, and interacting with trustworthy systems. Speakers will discuss research into a number of areas designed to enhance system trustworthiness, security, and dependability. Their results and findings will provide ideas for both technology developers and end users to enable a more trustworthy and secure computing environment.

The Topology of Covert Conflict

Ross Anderson, University of Cambridge

Often an attacker tries to disconnect a network by destroying nodes or edges, while the defender counters using various resilience mechanisms. Examples include a music industry body attempting to close down a peer-to-peer file-sharing network; medics attempting to halt the spread of an infectious disease by selective vaccination; and a police agency trying to decapitate a terrorist organisation. Albert, Jeong and Barabási famously analysed the static case, and showed that vertex-order attacks are effective against scale-free networks. We extend this work to the dynamic case by developing a framework based on evolutionary game theory to explore the interaction of attack and defense strategies. We show, first, that naive defenses don't work against vertex-order attack; second, that defenses based on simple redundancy don't work much better, but that defenses based on cliques work well; third, that attacks based on centrality work better against clique defenses than vertex-order attacks do; and fourth, that defenses based on complex strategies such as delegation plus clique resist centrality attacks better than simple clique defenses. Our models thus build a bridge between network analysis and evolutionary game theory, and provide a framework for analysing defense and attack in networks where topology matters. They suggest definitions of efficiency of attack and defense, and may even explain the evolution of insurgent organisations from networks of cells to a more virtual leadership that facilitates operations rather than directing them. Finally, we draw some conclusions and present possible directions for future research.

What is the System? Challenges in Evaluating the Trustworthiness of Critical Infrastructures

Robin Bloomfield, City University, London

Abstract TBA

Detection of Attacks on Cognitive Channels

Annarita Giani, UC Berkeley

A lot of research has focused on trying to prevent very specific attacks, such as computer compromises, network port scanning, etc. Although this works well for providing a better security infrastructure, it does not tell us either the "big picture" or the ultimate attacker's intent. Furthermore, these approaches can generate a large number of alarms, much of them related, which can overwhelm security administrators.

Our work builds on this previous work by correlating different sources of alarms and presenting a unified view of the ultimate attacker's intent. A cognitive channel is the communication channel between a person and the information technology used. An attack on a cognitive channel exploits the vulnerabilities between the user, her perception of the information system, and the actual underlying technology. The sophistication of modern information systems and their growing presence in human activities has made these channels attractive targets and they are increasingly the weak links in an information system. This has created a significant gap between computer security technology and the threat space. Modern cognitive channel attacks are complex processes that can be detected and tracked. An effective approach to defending against cognitive channel attacks therefore involves accurate process modeling and the development of new attack models based on processes. We have identified and implemented several approaches based on the Process Query System paradigm (PQS). PQS is a new information retrieval technology in which user queries are expressed as process description. The goal of a PQS is to make multiple hypotheses using a data stream or database of events correlated with the processes' states. This talk outlines the main feature of PQSs and its application in the detection of the ultimate attacker's intent.

What are the Security Research Challenges Facing a Large Telco Today and in the Future?

Bryan Littlefair, BT

What does the future hold for security, what challenges are we going to face? The whole information security industry is constantly fighting fires and behind the game, releasing patches and updates to recently released software and hardware as new exploits and vulnerabilities come to the fore. This presentation outlines some of the challenges that BT is facing in the security domain. It will briefly touch on some of the public aspects of the security of the 21st Century network: BT's new 11 Billion pound network.

We will also look at the current research agenda within the security research centre: what is driving the programme from an internal and external perspective, what are the big issues and what do we class as priority challenges?

Managing Human Factors in Security Systems

Angela Sasse, University College London

The presentation will summarise the relevant insights from a White Paper on "Human Vulnerabilities in Security Systems". The paper was funded by the U.K. Department of Trade and Industry and authored by a cross-disciplinary Working Group that brought

together security experts from industry and academic researchers in computer science and behavioural sciences. Key drivers for malicious behaviour are: dwindling loyalty and trust between organisations and staff, boredom, revenge, and a sense of entitlement, especially among executives. Key enablers are: the complexity of current systems, security models (command and control) that do not fit modern, global organisations, and failure to use human intelligence in the detection of malicious acts. Key recommendations include business process-centred security models, explicit definitions of roles and responsibilities, improved security awareness, awareness, education and training programs, and the inclusion of security goals in psychological contracts and reward schemes.

Secure Sensor Networks

Shankar Sastry, University of California, Berkeley

Ad hoc sensor networks have become popular over the past few years and the domain of their application has increased widely and continues to grow. However, the security of these networks poses a great challenge due to multiple unique aspects of the sensor networks. First, sensor networks consist of tiny wireless devices which have limited hardware and energy resources. In addition, these networks are generally deployed and then left unattended. These facts coupled together make it impractical to directly apply the traditional security mechanisms to the sensor network paradigm. As a result, there is a need to analyze and better understand the security requirements of sensor networks. This talk provides a comprehensive taxonomy of security attacks on sensor networks, and gives solutions for each set of attacks. More importantly, it points out the research directions that need to be investigated in the future.

Workshop speakers

Ross Anderson: Professor of Security Engineering, Computer Laboratory, University of Cambridge

Ross Anderson is a researcher, writer, and industry consultant in security engineering. In cryptography, he co-designed the BEAR, LION and Tiger cryptographic primitives, the block cipher Serpent (with Biham and Lars Knudsen), and the stream cipher Pike. He has also discovered weaknesses in many algorithms (FISH) and security systems.



Robin Bloomfield: Professor of System and Software Dependability, City University, London

Robin Bloomfield is currently director of the Centre for Software Reliability at the City University, London. His research is in the dependability (reliability, safety, security) of computer-based systems. His work in safety in the past 20 years has combined policy formulation, technical consulting and underpinning research. He is involved in a wide range of projects and is currently the project Director for the EPSRC funded £2M Interdisciplinary Design and Evaluation of Dependability (INDEED) project and a partner in the EU funded IRRIS – Integrated Risk Reduction of Information-based Infrastructure Systems project



Annarita Giani: Postdoctoral Fellow, University of California, Berkeley

Annarita Giani received her Laurea Degree in Applied Mathematics from the State University of Pisa, Italy, and her Ph.D. in 2006 from Dartmouth College. Her research was instrumental in the development of the Process Query System. Since the inception of the PQS project in 2003, she has been involved in investigating hidden discrete event systems models for process detection and estimation. Her current research includes investigation of techniques to assure robustness and reliability of wireless sensor networks for healthcare systems.



Bryan Littlefair: Global Head of Security Research and Development, BT

Bryan Littlefair is the Global Head of security research and development at BT's research centres in the UK, Malaysia and China. He is responsible for the global security pipeline of the UK's incumbent telecom supplier and for delivering security solutions internally. His achievements include designing some of the bespoke security solutions for BT's 21CN, which is the dramatic overhaul and upgrade of the BT network to meet the future needs of their customers. The team is also heavily involved in security standards and actively participate in standards bodies.



Angela Sasse: Professor of Human-Centred Technology, University College London

Angela Sasse holds an M.Sc. in Occupational Psychology from Sheffield University and a Ph.D. in Computer Science from the University of Birmingham. She worked as a human factors specialist for Philips Corporate Industrial Design and started as lecturer in the Department of Computer Science at UCL in 1990. Her research interests involve anything to do with people, technology and communication.



Larry Rohrbough: Executive Director, Team for Research in Ubiquitous Secure Technology (TRUST), University of California, Berkeley

Larry Rohrbough has over 15 years of experience in software engineering, technology consulting, program management, and business development. He has domain expertise in embedded systems, wireless sensor networks, large-scale operations support systems, and complex, software-intensive systems. Prior to joining UC Berkeley, he was the Chief Technology Officer of the ESCHER Research Institute, a non-profit organization focused on transitioning government-sponsored R&D from the research community to commercial and government end users. He holds a B.S. in Systems Analysis from Miami University and an M.S. in Software Systems Engineering from George Mason University.



S. Shankar Sastry: Director, CITRIS and TRUST, and Professor of Bioengineering, Mechanical Engineering and Electrical Engineering and Computer Sciences, University of California, Berkeley

TRUST and CITRIS **Director Shankar Sastry** received his Ph.D. in 1981 from the University of California, Berkeley. He was on the faculty of M.I.T. as assistant professor from 1980 to 1982 and at Harvard University as a chaired Gordon Mc Kay professor in 1994. Prof. Sastry is also the Director of the Richard C. Blum Center for Developing Economies at UC Berkeley.

