

The Malicious Exploitation of Information Systems: Preventing the Rise of the Insider Threat

6th – 7th November 2008
University College London

Day 1 - Conference

- 9:30 **Welcome**
Chairs: *Angela Sasse (University College London), Nigel Jones (Cyber Security KTN)*
- 9:40 **Overview of a Multidisciplinary Exploration of Insider Threats**
Shari Lawrence Pfleeger (The RAND Corporation)
- What is the problem? A taxonomy of insiders and their unwelcome actions
 - Addressing the problem: Research blending technology with an understanding of the environment in which insiders operate
 - Sensible responses: Marrying the taxonomy with appropriate proactive and reactive strategies
- 10:10 **An Empirical Approach to Identify Information Misuse by Insiders**
Deanna Caputo (MITRE)
- In this on-going research effort, we examine the similarities and differences in information gathering behaviour between malicious and benign users
 - We designed and executed a human experiment protocol for enumerating these similarities/differences
 - We plan to use experiment data to validate ELICIT detectors, identify new differentiating patterns and include other human attributes when considering malicious behavior
- 10:40 **Tea & Coffee break**
- 11:00 **Insider Threat: Defining Behavioural & Organisational Vulnerabilities**
Speaker from CPNI
- Discussion of interim results of CPNI's ongoing research into the Insider Threat
 - Overview of the individual and organisational vulnerabilities that can lead to Insider activity
 - Outline of behavioural indicators of the Insider Threat
- 11:30 **Risk Managing Insider Threats**
Laurence Mulley (SOCA)
- Managing recruitment through pre-employment screening
 - Monitoring the threat through management processes
 - Management controls to counter the threat
- 12:00 **My Experiences of Committing Fraud**
Convicted fraudster, interviewed by Martin Gill (Perpetuity Research and Consultancy International)
- How he exploited weaknesses in company procedures
 - The approaches he used to successfully bribe staff
 - The process of avoiding capture, for a while!

12:30 **Lunch**

13:30 **Risk Mitigation Models: Lessons Learned from Actual Insider Attacks**

Dawn Cappelli (CERT)

- The Software Engineering Institute CERT Programme has collected several hundred case files for actual insider cyber crimes that occurred between 1996 and 2007, including theft of confidential or sensitive information, IT sabotage, fraud, and threats to critical infrastructures.
- We focus on technical, behavioural, and organisational aspects of actual compromises.
- The presentation will highlight our empirically-based MERIT model of insider IT sabotage, as well as our recent findings regarding 100 cases in which current or former employees or contractors stole personally identifiable information, proprietary customer information, or trade secrets.

14:00 **Is there a Business Case for Employee Monitoring?**

Robert Coles (Merrill Lynch)

- What employee bad behaviour causes concern
- What monitoring can we do today
- What monitoring could we do tomorrow and what is the value

14:30 **Managing Risk by Monitoring Employees**

Kate Legg (Higgs & Sons)

- The legal framework
- Striking the right balance and proportionality
- How far can you legally go

15:00 **Tea & Coffee break**

15:30 **Issues in the Technologies of Digital Investigation**

Peter Sommer (London School of Economics & Open University)

- How to conduct Forensic Investigations of the Insider Threat
- How to establish a Corporate Forensic Readiness Programme
- Effective use of post-incident analysis: drawing the lessons/closing the loop with prevention

16:00 **Closing Panel**

Day 2 – Masterclasses

MORNING SESSION

1. **Modelling Organisations to Identify Points of Weakness Which Insiders Exploit**
Clive Blackwell (Information Security Group, Royal Holloway, University of London)
Author of the forthcoming book, “The Insider Threat to Organisations”
 - Provide a practical three-layer security architecture incorporating the social, logical and physical aspects to represent organisations and the threats they face at all layers
 - Illustrate the model’s effectiveness to systematically examine the typical insider threats of fraud, sabotage and breach of confidentiality along with possible defensive measures
 - Show how the model may be executed from business plans and diagrams made using software such as Microsoft Visio™ to automate the discovery of system weaknesses and provide advice on their remediation

OR

2. **Pro-active Detection of Malicious Insiders Through Information-Use Patterns**
Mark Maloof (MITRE)
 - Insiders who misuse their privileges to steal sensitive information can be identified by examining their patterns of information
 - Leveraging context about the user and the information with which they interact helps differentiate legitimate from benign patterns
 - We have developed and successfully tested these concepts, building a system called ELICIT (Exploit Latent Information To Counter Insider Threats)

AFTERNOON SESSION

3. **Designing Out Crime**
Paul Ekblom (Design Against Crime Research Centre, Central Saint Martins College of Art & Design)
 - Clear definition of what we mean by dishonesty
 - Process for identifying and tackling problems – using participants’ own examples
 1. Identifying scope of problem – e.g. cash till, back office
 2. Within that scope, identifying specific dishonesty problems faced, analysing the causal conditions that let them happen in terms of a) design of existing procedures and technology, and b) wider context
 3. Prioritising which to tackle in terms of a) harm and b) likely capability to do something about it
 4. Capture of wider design requirements of the system (low error rate, ease of learning procedures, customer-friendliness etc.)
 5. Design of solution(s) which are simultaneously user-friendly whilst abuser-unfriendly, using ingenuity to maximise benefit and minimise negative side-effects; and future-proofing – thinking ahead to offenders’ possible countermoves
 6. Testing – importance of iteration
 7. Maintenance – monitoring and maintaining effectiveness
 8. Preparing for the next crime – anticipation or reaction? Monitoring, deciding when to scrap system, pipelining
 - Running the arms race – importance of variety, adaptability etc.

OR

- 4. Effective Communication & Persuasion for Behaviour Change**
Peter Trim (Birkbeck College) & Angela Sasse (University College London)