This work has been submitted to NECTAR, the

**Northampton Electronic Collection of Theses and Research.**

http://nectar.northampton.ac.uk/4240/

**Creator(s):** Al-Sherbaz, A., Minai, A., Dravid, R. and Xue, J.

**Title:** An embedded pedagogic model for computer forensics within an undergraduate programme

**Date:** 10 November 2011

**Originally presented to:** 7th Annual Teaching Computer Forensics Workshop

**Conference URL:**
http://www.ics.heacademy.ac.uk/events/displayevent.php?id=264


**Version of item:** Presented version
An Embedded Pedagogic Model for Computer Forensics within an Undergraduate Programme

Proposed by the Computing Division, University of Northampton
The 7th Annual Teaching Computer Forensics Workshop
University of Sunderland – 10th Nov 2011

Presented by Ali Al-Sherbaz
Authors: Amir Minai, James Xue, Rashmi Dravid, The University of Northampton
Overview:

- **Facts - Cybercrimes**
  - The Evolution of Privacy
- **Dale’s Cone** of Experience in learning
- **The Proposed Model:** present an embedded computer forensics/cyber security materials within an undergraduate Programme
- **Conclusion**
Facts

- Computer forensics / Cyber-Security which has a strong multi-disciplinary background derives from the computing subjects in networking, programming, security and mathematics.
- Cyber crimes are on the rise, however, Cyber security professionals are in depressingly low numbers.
- Reflecting the technological fluctuations, it is seen as essential for students to be continuously updated.
- The evolution of privacy on Social Networking is changing
The Evolution of Privacy on Facebook
Learning From Experience Model

- **Least effective learning results from**
  - listening to spoken words

- **Most effective methods**
  - Hands-on lab activities based on real, everyday life experiences

- **Best learning methods use perceptual styles**
  - Perceptual learning styles are sensory based

- **Action-learning techniques result in up to 90% retention**

- **More real-life experiences.**

- **A tool to help instructors make decisions about designing Learning Activities and Resources**
Dale’s Cone of Experience

People Generally Remember:

- 10% of what they Read
- 20% of what they Hear
- 30% of what they See
- 50% of what they hear and see
- 70% of what they say and write
- 90% of what they do

People Are Able To: (Learning Outcomes)

Read
- Define List
- Describe Explain

Hear
- View Images
- Watch Video
- Demonstrate Apply Practice

See
- Attend Exhibit/Sites

Watch a Demonstration
- Analyze Design Create Evaluate

Participate in Hands-On Workshop
- Design Collaborative Lessons

Design or Model a Real Experience
- Simulate or Model a Real Experience

Design/Perform a Presentation - Do The Real Thing
The Proposed Model

- The depth of knowledge required for learning such topics as forensic and cyber security should be offered from the underlying principles to their abstraction.

- Increasing awareness of cybersecurity and emphasising the need for a common vision among students addresses the challenges.

- Some of the modules already cover part of computer forensics implicitly.
The Proposed Model

- Focuses on the delivery and assessment of certain computing modules, with an evaluation of its efficiency on the use of time and effort in order to satisfy the minimum requirements of the curriculum.

- Embed the computer forensics materials within the undergraduate modules to extend students’ knowledge and skills in a practical context.

- Highlighting these topics to the students and making them more visible as computer forensics is one of the main objectives.

- Enhance the existing computing modules by dedicating certain amount of lecture time on computer forensic related concepts.
The Proposed Module

- Forensics and Cyber-Security
- Security
- Network
- Database
- Programming
# Internet & Computer Security Module

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Awareness</td>
<td>Cryptographic systems</td>
<td>Pki</td>
<td>Firewalls</td>
<td>Internet</td>
</tr>
<tr>
<td>Security technology in context</td>
<td>Crypto Algorithms</td>
<td>SSL</td>
<td>IDS &amp; IPS</td>
<td>Database</td>
</tr>
<tr>
<td>Security Vulnerabilities</td>
<td>Crypto analysis</td>
<td>IPSec</td>
<td></td>
<td>Enterprise</td>
</tr>
<tr>
<td>Security (Hardware &amp; Software)</td>
<td></td>
<td>VPNs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Management</td>
<td></td>
<td>Kerberos</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Internet
- Database
- Enterprise
Internet & Computer Security Module (Practical)

- Footprinting the network (Pen test)
  - Security Analysis
  - Network threat testing

- Cryptography
  - Encryption basics
  - Encryption software
  - PKI exercise

- GNUPG
  - Email security

- Network Security tools
  - Firewall
  - SNORT
Network Module

Logging
- Cisco devices
- Windows hosts
- Syslog
- SNMP traps
- Enterprise Log and Search Archive (ELSA)

Monitoring
- Wireshark for packet capture and analysis of security threats

Capturing and Analyses
- Track packets and bytes at flow level
- Nmap and OpenVAS for port scans
- Ping sweeps

Action
- Routers and Switches
- Network Address Translations
- Access Control Lists
- Stateful packet Inspection.
- Intrusion detection/Prevention (IDS) Systems
DataBase Module

Ensure the right privileges are granted.
- During SQL DDL lecture/practical session
- Lower system and database privileges.

Firewall the database (GreenSQL)
- Prevent malicious attach (SQL Injection)
- Install and test how it works

Apply Best Practices
- Physical location, Antivirus, Regularly apply software patches.
- Rename root to a new name.
- Disable LOCAL INFILE in MySQL.
- Remove anonymous accounts.
- Remove test database.
Internet Programming Module

- Invalidated Input
- Broken Access Control
- Broken Authentication
- Cross Site Scripting (XSS) Flaws
- Buffer Overflows
- Injection Flaws
- Improper Error Handling
- Insecure Storage
- Denial of Service (DoS)
- Insecure Configuration Management
- Session Management
- Malware Attack
Conclusion

- To raise Cyber-Crime awareness it is imperative that computing courses within universities increase the level of student knowledge and skills by providing professional education.

- The teaching and learning of computer forensics and cyber-security can be integrated within a modular scheme without the need to add to an existing over loaded module pool.

- The proposed embedded model is founded on learning methods that reinforce learning through activities within technically related fields.

- The model can be adopted by Universities when considering to develop integrated modules.
Thanks

Any Question?

Looking for Feedback