Cybersecurity Education for Enterprise Cloud Services

Casimer DeCusatis, Ph.D.
The New York State Cloud Computing & Analytics Center at Marist College
Poughkeepsie, NY  (casimer.decusatis@marist..edu  @Dr_Casimer)
Overview

• Why study cybersecurity?

• Proposed Marist cybersecurity concentration

• Education philosophy and next steps
Security is in demand for today’s qualified graduates

“Federal agencies to hire more cyber defenders in 2014”

Security is the only area of certified IT skills that has never had a negative quarter throughout this recession
74% Increase in Venture Funding for Security

Cybersecurity startups to bank $788 million

By Sara Ashley O'Brien @saraashleyo July 21, 2014: 10:38 AM ET

Small Business Resource Guide

Total early stage VC investment in cyber security

- $160 million in 2011
- $235 million in 2012
- $452 million in 2013
- $788 million in 2014

(Source: PrivCo)
**New York State Charges Ahead On Critical Infrastructure Cybersecurity Legislation**

Mondaq Business Briefing - Orrick United States - New York State Charges Ahead On Critical Infrastructure Cybersecurity Legislation

**Publication Date:** 03/18/2015  
**Source:** Mondaq Business Briefing  
By Mr Aravind Swaminathan and Shea Gordon Leitch

On Feb. 26, 2015, in an effort to make "New York State's computer infrastructure the most secure in the nation," the New York State Senate passed a suite of four cybersecurity-related bills focused on protecting critical infrastructure entities, such as providers of financial services, telecommunications, energy and health care. The bills mark an aggressive effort to toughen penalties on cybercriminals who attack critical infrastructure (S3404 and S3406), 1. to implement cybersecurity review processes and reporting by key state agencies (S3405), 2. and to establish a "baseline framework" and information-sharing protocols around cybersecurity risks (S3407).

Although the Senate bills put New York at the forefront of state critical infrastructure cybersecurity legislation, certain provisions should cause significant concern in corporate boardrooms and C suites because they effectively transform "voluntary" government guidelines into mandates without at least offering confidentiality protections sufficient to prevent use of that information against them.

"Consultative" Cybersecurity Risk-Reduction Framework
Traditional perimeter-based security control…
... are changing to security centered around applications and data
**Intro Cybersecurity**

- Vulnerability Assessment, Reconnaissance
- Windows security, authentication
- Packet capture, traffic analysis, cloud security
- DDoS, MITM, phishing, database injection attacks
- Encryption techniques
- Governance, Legal, & Ethical issues (with Marist School Criminal Justice)

**Hacking & Penetration Testing**

- Penetration Test Plans
- Exploits to compromise Windows & Linux with Metasploit
- Malware identification, fraud prevention, mitigation
- Incident response, intrusion detection systems
- WAN & wireless security
- Guest Lecture: U.S. Military Academy, West Point

**Mobile Device Security**

- Wireless LAN (WLAN), Wi-Fi, and mobile attacks
- Discovering, tracking, and fingerprinting mobile devices
- Auditing & Forensics tools
- BYOD Policies
- Android hacks & security measures
- Mobile security app development
- Guest Lecture, BlackPhone SquidWrench Maker Group
The great thing about frameworks is that there’s so many to choose from…

• **STRIDE**

<table>
<thead>
<tr>
<th>Function</th>
<th>Function</th>
<th>Category</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identify</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PR</td>
<td>Protect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DE</td>
<td>Detect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RS</td>
<td>Respond</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RC</td>
<td>Recover</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Confidentiality**
- **Availability**
- **Integrity**

**Security Objectives**
<table>
<thead>
<tr>
<th>Course</th>
<th>Identify</th>
<th>Protect</th>
<th>Detect</th>
<th>Respond</th>
<th>Recover</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW Dev II</td>
<td>x</td>
<td>xxx</td>
<td>xx</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intro. Cloud</td>
<td>xx</td>
<td>xx</td>
<td>xx</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Operating Systems</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ethical Hacking</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>xx</td>
<td>xx</td>
</tr>
<tr>
<td>Networking</td>
<td>xx</td>
<td>xxx</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Management</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database Systems</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Theory Languages</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Recommendations for new course:**

- Increased holistic approach (all five categories in one class)
- More content on Response/Recovery, including data governance (Criminal Justice)
- More content on hands-on exercises and topical issues (security issues in the news)
- Reinforce topics from existing courses (SQL injection, access control, hashing, encryption)
Disclaimer

• The security breach techniques demonstrated in this lecture should never be used on the Internet, or any public or private network. These examples are used for illustration purposes only. Your professor and Marist College do not assume any liability if you use these techniques outside of class, even if you claim to be “just practicing the course material”.

• In other words, don’t try this at home.
Intro to Cybersecurity Labs

- Lab 1 – Reconnaissance and Probing using common tools
- Lab 2 – Vulnerability Assessment
- Lab 3 – Windows Active Directory & User Access Controls
- Lab 4 – Change control: group policy objects and MS Baseline Security
- Lab 5 – Packet Capture & Traffic Analysis
- Lab 6 – Business Continuity Planning
- Lab 7 – Encryption
- Lab 8 – Web Site and Database Attacks
- Lab 9 – Layered Security
- Lab 10 – Implementing an IS Security Policy
Lab Tool Examples

- FileZilla (file transfer)
- NetWitness Investigator (packet analysis)
- Wireshark (packet capture)
- Open VAS (remote scan/audit of devices, applications, DBs, services)
- PuTTY (SSH/Telnet client for remote connection to Linux machines)
- Zenmap (IP subnet scan for firewalls, packet filters, OS, etc)
Industry Certification Mapping

• Intro to Cybersecurity course
  – Based on NIST Risk Management Framework, Labs cover ISC² certification
  – Covers all topics requires for U.S. Government courseware certification NSTISSI 4011: National Training Standard for Information Systems Security (INFOSEC) Professionals
  – Publisher provides a mapping to requirements from the following organizations:
    • National Centers of Academic Excellence (CAE)/Cyber Defense Education Program NSA/DHS sponsored program through CISSE http://www.cissee.info/
      and the DHS National Initiative for Cybersecurity Careers and Studies (NICSS) http://niccs.us-cert.gov/
    • Department of Defense Cybersecurity Workforce Strategy (DCWS) and Workforce Development Framework (CWDF) including DoDD 8570.01 Information Assurance Training, Certification and Workforce Management (emerging)
<table>
<thead>
<tr>
<th>Goal/ Objective</th>
<th>CAE Program</th>
<th>NICE Workforce Framework</th>
<th>DoD CWF</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Audience</strong></td>
<td>Promotes higher education and research; and produces professionals with information assurance (IA) expertise in various disciplines</td>
<td>Describes and categorizes cybersecurity work and identifies sample job titles, tasks and KSAs</td>
<td>Provides the foundation for identifying education, training, and certification requirements to support cybersecurity personnel qualification</td>
</tr>
</tbody>
</table>
| **Mapping Components** | 2-year, 4-year and graduate-level institutions in the U.S. seeking CAE designation  
• students, employers, and hiring managers | colleges  
• training vendors  
• students  
• employers/employees  
• policymakers | military, civilian, and contractor cybersecurity personnel  
• training vendors, certification bodies, colleges, and continuing education providers |
| **2Y Core Knowledge Units** | 7 Categories  
• 31 Specialty Areas  
• Task/KSA level  
• Job Titles | 7 Categories  
• 31 Specialty Areas  
• Task/KSA level  
• Job Titles | DoD work roles, tasks, functions and baseline KSAs  
• Under Development |
| **Integration** | The NICE Framework informed development of the CAE Knowledge Units (KUs); thus, many CAE Core KUs are core across the NICE Framework Specialty Areas. NICE Framework will also inform development and implementation of the DoD CWF. |
Case Study

- An attack case study reviews an actual attack (successful or otherwise). It includes the threat agent, risk management, and mitigation techniques. The required elements of a case study are:

- Attack Overview
- Threat Agent Profile and Motivation
- Attack Scenario
  - Goals, Resources required (skills, equipment, timing)
  - How the attack took place (detailed description)
  - Collateral results
  - Mitigation (map to first principles such as defense in depth, kill chains, etc)
- Risk Management Framework (NIST RMF)
  - Categorize the information system (FIPS, SP, CIA mapping, 4 point impact scale)
  - Existing and recommended security controls (attack matrix, risk matrix)
  - Implementation requirements (5 properties, Chapter 1)
  - Assessment of controls
  - Authorization and deployment
  - Monitoring
- References (primary references preferred)
Case Study Project

• Project 1
  – Introduce the case study framework and requirements (chapter 1, 2)
  – Provide a list of potential topics
  – Students select a topic (or propose their own) subject to instructor approval
  – Turn-in: topic with at least one primary reference

• Project 2
  – Attack Scenario
  – Research and include at least three primary references
  – Turn-in: address all attack scenario required elements (2 page minimum, no maximum)

• Project 3
  – Risk Management Framework elements 1-3
  – Include mapping to first principles
  – Turn-in: address RMF requirements & update attack scenario (2 page minimum, no maximum)

• Project 4
  – Submit completed case study for instructor and peer review
  – Turn-in: address all case study requirements, updating prior sections per class discussions
Hacking & Penetration Testing Labs

• Introduction & Ethical Hacking
• Cryptographic Concepts
• Footprinting & Social Engineering
• Port & Vulnerability Scanning
• Web & Database Attacks
• Network Sniffing, Session Hijacking, and Denial of Service
• Firewalls, IDS, IPS
• Incident Response, Basic Forensics
Cloud Security Vulnerability Scan
How about an example?

If user input is inserted without modification into an SQL query, then the application becomes vulnerable to SQL injection as in the following example:

```php
$unsafe_variable = $_POST['user_input'];
mysql_query("INSERT INTO `table` (`column`) VALUES ('$unsafe_variable')");
```

That's because the user can input something like

```
value'); DROP TABLE table;--
```

and the query becomes:

```
INSERT INTO `table` (`column`) VALUES('value'); DROP TABLE table;--
```

Structured, analytical, repeatable

Security Intelligence

Real-time Processing
- Real-time data correlation
- Anomaly detection
- Event and flow normalization
- Security context & enrichment
- Distributed architecture

Security Operations
- Pre-defined rules and reports
- Offense scoring & prioritization
- Activity and event graphing
  - Compliance reporting
  - Workflow management

Big Data

Big Data Warehouse
- Long-term, multi storage
- Unstructured and structured
- Distributed infrastructure
- Preservation of raw data
- Hadoop-based backend

Analytics and Forensics
- Advanced visuals and interaction
- Predictive & decision modeling
- Ad hoc queries
- Spreadsheet UI for analysts
- Collaborative sharing tools
- Pluggable UI

Creative, exploratory, intuitive

Security Intelligence with Big Data
QUESTIONS?

Follow @Dr_Casimer or http://www.ofcconference.org/en-us/home/about/ofc-blog/