ECS Center for Cybersecurity (ECSCYBER): Preparing the Next Generation Cybersecurity Workforce

By Mikhail Gofman
ECS Center for Cybersecurity (ECSCYBER)

• Founded in 2015
• **Mission:** promote cybersecurity education, research, and outreach
Past Accomplishments (1)

• Developing Cybersecurity Curriculum:
  – New courses
  – Technical infrastructure for hands-on cybersecurity learning
  – Incorporating high-impact learning practices (hands-on hacking, exposure to research, etc)
Past Accomplishments (2)

- Publication of cybersecurity research at top conferences and journals
  - Biometrics
  - Access Control
  - Cloud Security
  - Hardware Security
Past Accomplishments (3)

• Supporting student groups in regional and national cybersecurity competitions

Offensive Cybersecurity Society (OSS) team won 2nd place in 2018 Collegiate Penetration Testing Competition
Current Mission

• Have CSUF recognized as Academic Excellence in Cyber Defense (CAE-CD) by the National Security Agency (NSA)

• “The goal of the [CAE-CD] program is to reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber defense and producing professionals with cyber defense expertise” –nsa.gov
CAE-CD Schools “Next Door”

• What is missing?
The Answer!
What it Takes to become CAE-CD?

- **Key:** An undergraduate cybersecurity concentration covering:

<table>
<thead>
<tr>
<th>Foundational Knowledge Units:</th>
<th>Optional Knowledge Units (Any 14/58 topics provided by NSA):</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Cybersecurity Foundations</td>
<td>• Advanced Cryptography</td>
</tr>
<tr>
<td>• Cybersecurity Principles</td>
<td>• Algorithms</td>
</tr>
<tr>
<td>• IT Systems Components</td>
<td>• Cloud Computing</td>
</tr>
<tr>
<td></td>
<td>• Cybersecurity Ethics</td>
</tr>
<tr>
<td></td>
<td>• Data Structures</td>
</tr>
<tr>
<td></td>
<td>• Databases</td>
</tr>
<tr>
<td></td>
<td>• Penetration Testing</td>
</tr>
<tr>
<td></td>
<td>• Privacy</td>
</tr>
<tr>
<td></td>
<td>• Web Security</td>
</tr>
<tr>
<td>Technical Core Knowledge Units</td>
<td>• Software Assurance</td>
</tr>
<tr>
<td>• Technical Core KUs</td>
<td>• Software Reverse Engineering</td>
</tr>
<tr>
<td>• Basic Cryptography</td>
<td>• .</td>
</tr>
<tr>
<td>• Basic Networking</td>
<td>• .</td>
</tr>
<tr>
<td>• Basic Scripting and</td>
<td>• .</td>
</tr>
<tr>
<td>Programming</td>
<td>• .</td>
</tr>
<tr>
<td>• Network Defense</td>
<td>• .</td>
</tr>
<tr>
<td>• Operating Systems Concepts</td>
<td>• .</td>
</tr>
</tbody>
</table>

---
Where We Are Now

• A cybersecurity concentration in Computer Science proposed in Spring 2019 (in the approval process)
  – Built on top of the existing computer science major:

<table>
<thead>
<tr>
<th>Required Courses:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Introduction to Cybersecurity</td>
</tr>
<tr>
<td>• Network Security</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Three Electives Chosen From</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Cryptography</td>
</tr>
<tr>
<td>• Cloud Computing and Security</td>
</tr>
<tr>
<td>• Malware Analysis</td>
</tr>
<tr>
<td>• Web Security</td>
</tr>
<tr>
<td>• Block Chain Technologies</td>
</tr>
</tbody>
</table>
Where We Are Now

• Reworking/extending current cybersecurity curriculum toward CAE-CD compliance:

Required Courses:
• Introduction to Cybersecurity
• Network Security

Three Electives Chosen From
• Cryptography
• Cloud Computing and Security
• Malware Analysis
• Web Security
• Block Chain Technologies

Recently added as required Computer Science core course
How Close are we to Meeting CAE-CD?

Foundational Knowledge Units:
- Cybersecurity Foundations
- Cybersecurity Principles
- IT System Components

Technical Core Knowledge Units
- Technical Core KUs
- Basic Cryptography
- Basic Networking
- Basic Scripting and Programming
- Network Defense
- Operating Systems Concepts

Optional Knowledge Units (Any 14/58 topics provided by NSA):
- Advanced Cryptography
- Algorithms
- Data Structures
- Software Assurance
- Cybersecurity Ethics
- Databases
- Cloud Computing
- Web Security
- Software Reverse Engineering

- Privacy
- Penetration Testing
- Wireless Sensor Networks
- Network Forensics
- Linux System Administration

More work needed
What do these Courses Entail?

- **Introduction to Security**: Cybersecurity Overview
  - **Cybersecurity Principles**: Confidentiality, Integrity, Availability, Privacy, Threats...
  - **Cybersecurity Fundamentals**: Separation of duties, Trust Relationships, Isolation...
  - **Access Controls**: Access Control Models
  - **Security task automation**: Scripting for Windows and Linux
  - **IT Security**: Vulnerability Patching, Physical Security, Social Engineering
  - **Security Compliance and Standards**: Compliance with policy, standards or laws
  - **Network Security**: Firewalls, enterprise networks, penetration testing...
  - **Cryptography Basics**: protection of at rest and in-transit data...
What do these Courses Entail?

- **Network Security: Fundamentals of Network Security**
  - *Network Vulnerabilities*: complexity, legacy protocols, new technologies
  - *Attackers and Malware*: Pay-Per-Install Networks, Hacktivists, Advanced Persistent Threats...
  - *Control Hijacking*: Buffer overflow and attacks that take control of network applications
  - *Sandboxing and Confinement*: Isolating suspicious/vulnerable applications in secure environments
  - *IT Security Practices*: Policies, Regulations, Baselines...
What do these Courses Entail?

- **Cryptography: Data Security Through Encryption**
  - Data Encryption
  - Digital Signatures
  - Data Integrity Verification
  - Authentication Protocols
  - Cryptography in web, email, and mobile security
  - Onion and DarkWeb
  - Introduction to Blockchain
What do these Courses Entail?

• **Malware Analysis: Unmasking the mind of malware**
  
  – TONS of hands-on exercises in reverse engineering of real-world viruses, worms, ransomware...
  
  – Malware Types
  
  – Machine Code
  
  – Reverse Engineering Malware
  
  – Inferring Malware Function Through Code Inspection
  
  – Inferring Malware Function Through Behavioural Analysis
  
  – Defeating Malware’s Anti-Analysis Techniques
  
  – Developing Anti-Virus Detection Signatures
What do these Courses Entail?

• Cloud Computing & Security: Cutting-Edge Cloud Computing Principles and Practices
  
  – Hands-on building of large-scale cloud computing applications
  
  – Cloud computing service frameworks
  
  – Resource virtualization (computing, storage, and network)
  
  – Cloud Computing architecture and industry frameworks (e.g., Hadoop)
  
  – Monitoring, management, and security protection of cloud computing
  
  – Software networking and risk mitigation methodology for cloud computing.
  
  – Vulnerabilities and risks of cloud computing
  
  – Data classification and protection in cloud
  
  – User identification and access control in cloud computing
What do these Courses Entail?

• **Blockchain Security: Blockchain Technologies and Security Applications**
  
  – Blockchain technologies, security applications, cryptocurrency, cryptographic techniques, etc
What is Coming Up?

• Courses in:
  – **Penetration Testing**: finding and exploiting system vulnerabilities
  – **Network Forensics**: extracting digital evidence, analysing cybercrimes, etc
  – **Optimizing the proposed concentration**: ensure that all students meet the optional KU requirements

• **Tentative Timeline for CAE-CD: Submit Application by 2025**
The Team

- Dr. David Falconer
- Dr. Yun Tian
- Dr. Wenlin Han
- Dr. Paul Inventado
- CS Department Chair Dr. Christopher Ryu
- ECS Dean Dr. Susan Barua
- ECS Associate Dean Dr. Sang June Oh
- Talisa Terrell (MITRE)
Thank You! Questions?