

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”

CAL POLY POMONA



- *What is missing?*

The Answer!



What it Takes to become CAE-CD?

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

Foundational Knowledge Units:

- Cybersecurity Foundations
- Cybersecurity Principles
- IT Systems 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
- Cloud Computing
- Cybersecurity Ethics
- Data Structures
- Databases
- Penetration Testing
- Privacy
- Web Security
- Software Assurance
- Software Reverse Engineering
- .
- .
- .

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:

Required Courses:

- Introduction to Cybersecurity
- Network Security

Three Electives Chosen From

- Cryptography
- Cloud Computing and Security
- Malware Analysis
- Web Security
- Block Chain Technologies

Where We Are Now

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

Required Courses:

- Introduction to Cybersecurity **REVISED**
- Network Security

Recently added as
required Computer
Science core course

Three Electives Chosen From

- Cryptography **REVISED**
- Cloud Computing and Security
- Malware Analysis **NEW!**
- Web Security **NEW!**
- Block Chain Technologies **NEW!**

How Close are we to Meeting CAE-CD?

Foundational Knowledge Units:

- Cybersecurity Foundations
- Cybersecurity Principles
- IT Systems 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

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...
 - **Network Protocol Security:** Vulnerabilities in web, email, routing, and server systems
 - **Control Hijacking:** Buffer overflow and attacks that take control of network applications
 - **Sandboxing and Confinement:** Isolating suspicious/vulnerable applications in secure environments
 - **Network Security Architecture:** Firewalls, Intrusion Detection/Prevention Systems, Perimeter Security, Virtualization Security Techniques....
 - **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?