Cybersecurity at CSU CI

http://www.msoltys.com/cybersecurity
Michael Soltys michael.soltys@csuci.edu, @MichaelMSoltys
Updated: November 2, 2018

Introduction: Hardly a week passes by without new reports of data breaches; for example:

- the 2017 Equifax data breach exposed the sensitive personal info of 143M Americans;
- the 2015 OPM data breach where sensitive information, including SSNs of 21.5 million individuals, was stolen from the background investigation databases;
- the 2013 Target data breach that affected more than 41 million of the company's customer payment card accounts and where Target paid a multi-state settlement of over $18M.

What can we do? Cybersecurity protects information, systems and assets, while delivering business value through risk assessment and mitigation strategies. Think of it as follows: *you invest capital in developing intellectual property; Cybersecurity ensures that you profit from it*.

What is Cybersecurity: Cybersecurity, also called Information Security, is a burgeoning field of Computer Science (CS). It focuses on protecting computers, networks, programs, and data from unintended or unauthorized access, change, or destruction. It is an interdisciplinary field which is traditionally housed under Computer Science, but borrows from Engineering, Mathematics, Management, Psychology, Social Sciences and Law.

At CSUCI we are working to become a hub of expertise in Cybersecurity. We offer:
Minor in Cybersecurity: Known as *Security Systems Engineering* (http://bit.ly/CSUCISSE), built around COMP 424 (Cybersecurity) and MATH 482 (Cryptography). As the minor is traditionally taken by CS majors, most students also take COMP350 (Software Engineering) and COMP 429 (Networks), which are important components of Cybersecurity.

Graduate (Masters level) offering in Cybersecurity: We offer a graduate CS course in Cybersecurity, COMP 524 (fall 2018), which is intended for an advanced audience (and covers much more than CompTIA Security+). See syllabus outline on the back. Permission to enroll can be given to interested students who are not matriculated in the Masters program. We also offer COMP 529 (Cloud Computing) in conjunction with Amazon Web Services, which offers certification as an AWS Cloud Computing Architect, with strong emphasis on security in the cloud.

Relationships: We have a relationship with the local Navy, Point Mugu and Port Hueneme. For example, Navy personnel are taking COMP 524 this fall, to fulfill their Cybersecurity training. We also have a close collaboration with the SoCal High Technology Task force (HTTF). In the summer of 2017 the COMP 524 students designed a tool in digital forensics for HTTF. We are also members of CyberWatch West, with the mission to to increase the quantity and quality of the cybersecurity workforce throughout the western United States. Michael Soltys is on the Assemblymember Jacqui Irwin Cybersecurity Advisory Board.

Syllabus Outline for COMP 524 Cybersecurity at CSUCI

1. Cryptography: basic definitions ("what does it mean for a cryptosystem to be secure?") fundamental theorem, tenet and assumption of cryptography.
2. Caesar and Mono-Alphabetic Ciphers. Symmetric Ciphers: substitutions, permutations and XOR. Assignment 1: break a MAC cipher.
3. Ciphers: DES, IDEA, AES. htpasswd and two Case Studies: Breaking Crypt, and Breaking Pseudo-Random number generator RC4 and WEP.
4. Blocks and Hashes. We look at several common block cipher schemes: ECB, CBC, CFB, OFB and CTR. Hashing: one-way and collision resistant. Birthday Paradox. Hashes: MD5. Breaking Crypt. Case Study: DRM (Digital Rights Management) and Rsync.
5. Public Key Cryptography: hardness of discrete log and factoring: Diffie-Hellman, ElGamal, RSA.
6. What is a protocol? Authentication: Needham-Schroeder protocol, and Kerberos.
7. Tools 1: OpenSSL and GnuPG: both are free tools, and if they are not included in your OS, they can be downloaded, for example, from:
    a. https://www.openssl.org
    b. https://gpgtools.org
8. Tools 2: hashcat and John the Ripper: both also free from
    a. https://github.com/hashcat/hashcat
    b. https://www.openwall.com/john
9. Tools 3: Kali Linux, Palo Alto Firewalls and Wireshark; Malware and Virus Total: we will start by reading the classical paper by Ken Thompson, Reflections on Trusting Trust, from 1984. We will then examine some typical malware in more detail. Assignment 2: implementation of protocol in Python.
10. CompTIA Security+: We will cover the material in the CompTIA Security+ certification. However, at this point in the course, we will have seen several fundamental concepts, and so we will be able to cover the material quickly:
    a. Understanding identity and access management
    b. Exploring network technologies and tools
    c. Securing your network; Securing hosts and data
    d. Comparing threats, vulnerabilities and common attacks
    e. Protecting against advanced attacks
    f. Using risk management tools
    g. Implementing controls to protect assets
    h. Implementing policies to mitigate risks
11. Presentations by students from a pool of about 50 articles in advanced aspects of Cybersecurity. It is important to have strong communication tools, as the work-place requires presenting and writing.