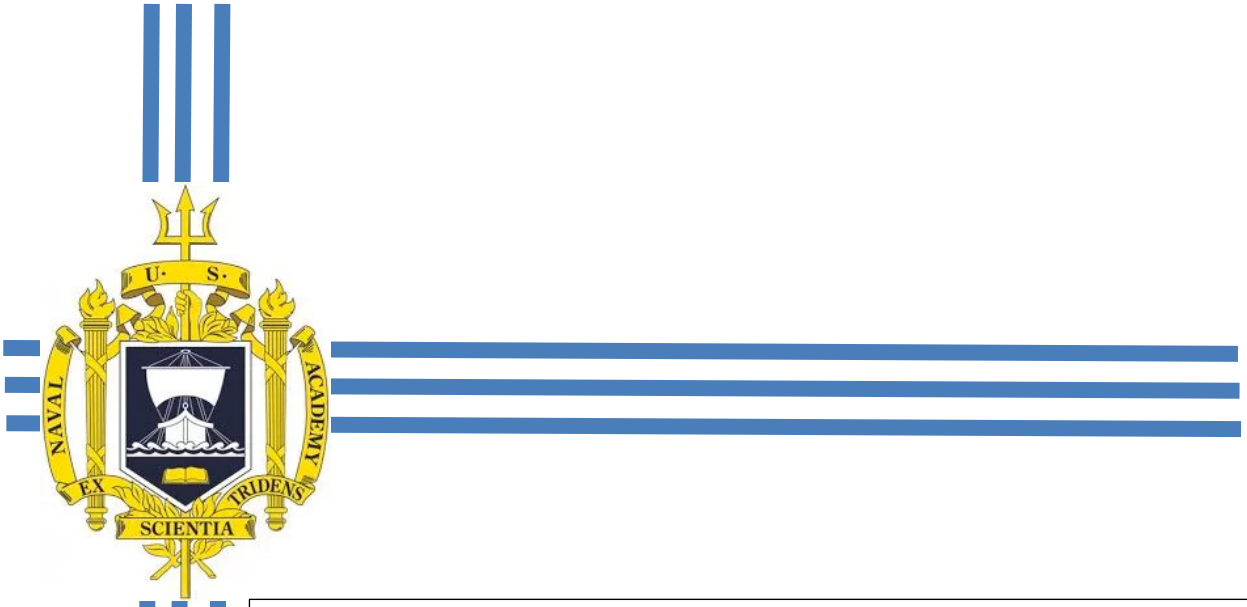

US Naval Academy
IT432 Advanced Computer And Network Security

Curriculum Summary

October 2019

OEHLER.MICHAEL.JOHN.1384223504

Digitally signed by OEHLER.MICHAEL.JOHN.1384223504
Date: 2019.10.10 12:44:46 -04'00'

Overview

Attached is the curriculum summary for the US Naval Academy's IT432 Advanced Computer And Network Security, as taught by the course coordinator, Dr. Michael Oehler, for the Fall 2019 semester; namely the USNA 2020 Academic Year (AY20):

	Description
Course	IT432
Title	Advanced Computer and Network Security
Credits	2-2-3 (2 hours lecture, 2 hours laboratory exercise, 3 credits overall)
Description	The course covers topics in secure system design, including: cryptography, data integrity, and authentication mechanisms for operating systems and computer networks. Where the IT430 course focuses primarily on securing an existing system, this course studies how to design a system to meet security goals. Students will design and implement components of a secure system.
Offered	Fall 2019, AY20
Requisites	IT430 Computer and Network Security

Course Topics

Topics	**Security Services Studied**
Classic Security Models	**Design Principles**
The classic security models: Confidentiality Integrity and Availability (CIA), APAIN, Defense in Depth (DiD), and Technology People Procedures (TPP) are covered. The foundational security services are taught as a premise for "How do I secure my system?"	
Current Cyber Models	**Design Principles**
A current security model, known as Protect Detect Response (PDR), is discussed. An implementation of the PDR model is then shown within National Institute for Standards and Technology (NIST) Cyber Security Framework. The framework discusses how systems should be secured in 2019.	
Secure Design	**Design Principles**
The security matrix is presented a means to "secure the system." The security matrix associates security services, security controls, and security implementations. The matrix provides a structured approach to design a secure system. A parallel is then drawn between NIST's Special Publication 800-53, and its comprehensive list of security services and security controls. Security controls are discussed to include: discretionary access control, data at rest protection, system audit, 3rd party escrow, etc.	
Threat Driven Defense	**Threat**
Threat Driven Defense is a concept that mitigates known threats. Instead of selecting security services, network defenders choose those defensive measures to thwart known threats. Threat reporting, (cyber) information sharing, and "know the threat" are emphasized.	
Break the Attack Lifecycle	**Threat**
Threat Driven Defense is predicated on understanding the attacker's lifecycle. Namely, attackers take specific steps to compromise into our systems. Thus, defenders must know these steps and implement mitigation strategies to "secure their system." The steps are predicated on Lockheed Martin's "Kill Chain" and breaking the adversarial lifecycle. Mitre's ATT&CK and NSA's adversarial obstruction are introduced.	
Common Vulnerabilities Exposures (CVE)	**Threat**
Sharing cyber security information, Indicators of Compromise (IOCs), and vulnerability sharing is discussed. An emphasis is placed on Mitre's CVE database and NIST's National Vulnerability Database (NVD). Students are shown how vulnerabilities are measured. Students exercise the Common Vulnerability Scoring System (CVSS) calculator to rate a provided vulnerability.	
Salted Passwords & Rainbow Tables	**Authentication**
Credential theft is the foremost threat to our systems. (Classical) salt is introduced as a means to protect credentials stored to disk. Adversarial use of rainbow tables is also discussed. Students use bash commands to locate a given salt in a provided rainbow and crack a password. Students are instructed never to crack operational password files	

The Digest Authentication Protocol	**Authentication**
	Students are introduced to an authentication protocol; the Internet Engineering Task Force (IETF) Request For Comment (RFC) 2617, Digest Authentication. Digest Authentication is a cryptographic protocol that uses cryptographic hash functions, a nonce for currency, and the formation of two message digests. Students recognize the difference between Digest Authentication and that of plain text protocols.
Hash Message Authentication Code (HMAC)	**Data Integrity**
	A data integrity mechanism is presented. Namely, the Hashed Message Authentication Code (HMAC) and as defined by IETF RFC-2104. Students study the specification and perform an exercise to validate the integrity of a message given a shared secret, a cryptographic hash function, and an implement of HMAC.
Digital Signatures	**Authentication/Data Integrity**
	A classic digital signature system using symmetric keys and a trusted arbitrator is discussed. The concept of a Key Distribution Center (KDC), arbitrator, and the driving requirements of a digital signature are discussed. The system is used as a premise to introduce the design requirements for a digital signature system using public key cryptography and cryptographic hash functions.
Application Whitelisting (AWL)	**Protect & Mitigate**
	The use of Application Whitelisting (AWL) is a fundamental mitigation strategy commonly recommended by the US Government. Three types of AWL are discussed: Hash Based, Digital Signature Based, and Location Based. The pros and cons of each are discussed. Even though AWL is built into today's operating systems, few organizations deploy AWL. The reasons for non-deployment are discussed.
Anti-Exploitation Measures	**Protect & Mitigate**
	Malware commonly exploits the instruction pointer to gain control of a system. To mitigate exploitation, software is built with anti-exploitation measures. Three anti-exploitation measures are discussed: Data Execution Prevention (DEP) also known as the "No Execute bit (NX)", Address Space Layout Randomization (ASLR), and Structured Exception Handling Overwrite (SEHOP) are introduced. The current state of deployment within Microsoft's Windows operating system is discussed.
DoD Public Key Infrastructure	**Authentication**
	The Public Key Infrastructure (PKI) is a system used to authenticate public keys. The system is implemented as a hierarchy of digital signatures that reside at a trusted root. The PKI's "chain of trust", certificates, certificate authorities, and the root certificate store is discussed.
Kerberos Authentication Protocol	**Authentication**
	Kerberos is a trusted 3rd party (network) authentication protocol that uses symmetric key cryptography. Kerberos is used for Single Sign On (SSO) and is used by many operating systems. Kerberos is used for network authentication and access control across distributed systems.
NT LAN Manager (NTLM) Authentication Protocol	**Authentication**
	NT LAN Manager (NTLM) is a Challenge and Response (C&R) protocol still used by the Windows operating system. The details of the protocol are discussed. Students are made aware that attackers have access to tools to extract the hash, and thus the password. Mimikatz is the most common tool to do this.
Malvertising	**Threat**
	A new threat is discussed, malicious web advertising (Malvertising) and how attackers are attempting to compromise our systems. The discussion re-emphasizes the need to "Known the Threat".
Air Gapped Networks & Data Guards	**Protect**
	Governments use air gapped networks to separate and isolate their most sensitive information. Air gapped systems are then connected to the Internet via data guards and Cross Domain Solutions (CDS). The technical design of good and bad CDS systems are discussed.
Security Technical Implementation Guide	**Protect**
	DoD Security Technical Implementation Guide (STIGs) describe the system and network settings that are permitted. Students are shown the STIG viewer and various settings. The expectation of commanding officers to "STIG a system" and which category of settings must be met, are discussed.
Homomorphic Encryption	**Confidentiality**
	Homomorphic encryption is a cryptographic system in which one operation in the ciphertext domain is reflected by another in the plaintext domain. The use of the Paillier public-key encryption system is demonstrated. The concept of Private Information Retrieval (PIR) is introduced.

NetFlow (Data Logging & Analysis)	Audit
NetFlow is a form of data logging in which network connections are summarized. The concept of a data tuple to summarize a network connection is presented. Commands from Carnegie Mellon's SiLK RW suit are introduced. Students are taught to perform network traffic analysis on NetFlow data.	
Yara Rules (Rules to Identify Malware)	**Detection**
YARA rules are a way of identifying malware (or other files) by creating rules that look for certain characteristics. The construction of YARA rules is discussed and the need for cyber security information sharing is discussed again.	
Industrial Control Systems (ICS)	**Threat**
Industrial Control Systems (ICSs) are introduced. ICS risks are discussed. Specific cyber security threats to ICS systems is discussed.	
Supervisory Control and Data Acquisition (SCADA)	
Supervisory Control and Data Acquisition (SCADA) systems are introduced. SCADA risks are discussed. Specific cyber security threats to SCADA systems are discussed. Course ends with a recognition that SCADA systems are highly susceptible to attack. Few have any of the security controls built-in.	

Laboratory Assignments

Weekly lab assignments are designed to correspond with class room discussions, are hands on, and demonstrate classroom theories. All lab assignments are submitted as a formal writeup, intended to be delivered to an external customer. Lab reports are expected to be polished and well written. Most labs use a codebase written for the class, consisting of 10,000 lines of Python, and mimics a launch system:

Lab Title	Course Topics Emphasized
Basic Authentication	**Design Principles, Authentication, Security Protocols**
Students identify why Basic Authentication (RFC 2617) is weak, capture relevant packets, and discover a plaintext password is sent. Student's use the course's (mock) launch control system.	
Vulnerability Discovery	**Threat Driven Defense**
Given an artificial threat report. Students use the information to locate, identify, and mitigate a back door in the course's launch control system. Student "know the threat" and break the attacker's lifecycle.	
Salted Passwords	**Design Principles**
Students construct salted passwords and integrate their design into the course's launch control system.	
Digest Authentication	**Threat**
Students write code to implement the Digest Authentication protocol and integrate their design into the course's launch control system. Students recognize that Digest Authentication is better than the Basic Authentication protocol.	
Hashed Message Authentication Code (HMAC)	**Data Integrity**
Students write code to implement HMAC and integrate their design into the course's launch control system. Students recognize that data integrity over the "launch commands" is very important.	
Digital Signatures	**Data Integrity**
Students write code to sign and validate digital signatures they have placed on the source code.	
PKI & Certificate Chains	**Authentication**
Students use openssl(1) to convert, display, and valid certificates taken from the DoD's Public Key Infrastructure (PKI) and from their browser root certificate store.	
Homomorphic Encryption	**Confidentiality**
Students implement the Paillier cryptographic algorithm. Discover the homomorphic nature of this public key cryptosystem.	
NetFlow (Data Logging & Analysis)	**Data Integrity**
Students build the SiLK toolset from source. Use SiLK tools to discover malicious activity in a NetFlow dataset.	
YARA (Rules to Identify Malware)	**Authentication/Integrity**
Students learn how to write YARA rules and developed regular expressions (regex) within those rules.	
SCADA Systems	**Protect & Mitigate**
Many SCADA systems rely on a protocol called MODBUS. Students learn how to write a disruptive packet to disable a traffic-light (demonstrative purposes only). Students learn that SCADA system are not secure.	

Reading Assignments

Each week students are given a reading assignment and asked whether the security article, government security report, or academic paper had any impact. Asked to discuss whether the material is meaningful. This is an important skill, versus writing a summary.