Master Course Description for EE-4XX (ABET sheet) New Course

Title: Network and Web Security

Credits: 4
Coordinator: Radha Poovendran, Professor, Electrical and Computer Engineering

Goals: To develop an understanding of the fundamental principles of network and communication security. This course is an introduction to the basic theory and practice of network security. This course will serve as an introduction to the vulnerabilities and defenses in network and communication systems. We will introduce state-of-the-art network and web security attacks along with hand-on activities to provide better understanding of the security vulnerabilities. The objective of this course is to enable students to understand the main challenges in designing security mechanisms and protocols for thwarting attacks on existing and emerging computer networks including network's communication protocols, domain name systems, wireless networks, web security.

Learning Objectives: At the end of this course, students will be able to:

1. *Study, implement and analyze* some of fundamental networks' protocol security attacks and defenses including TCP session Hijack attack, man-in-the-middle, heartbleed bug and attack
2. *Study, implement and analyze* the representative of fundamental web security attacks and defenses including DNS spoofing attack, denial of service attack
3. *Study, implement and analyze* some of fundamental domain name systems' attacks and defenses including Cross-site request forgery,Cross-site scripting attacks and SQL injection attack
4. *Study, and analyze* some of fundamental wireless security protocols and security vulnerabilities and defenses

Textbooks:

1. Wenliang Du, Computer & Internet Security: A Hands-on Approach, Second Edition

References:

2. Mike Speciner et al., Network Security: Private Communications in a Public World 2nd Edition, (also available in Kindle format)

Prerequisites by Topic:

1. EE 419 Introduction to Computer-Communication Networks [Recommended]
2. EE 418 Network Security and Cryptography [Required]
3. EE 241 Programming for Signal and Information Processing Applications or Familiarity with Python is essential [Required]

Topics:

Network Security [Week 1-4]:

1. Network background and attacks on TCP, DNS, DHCP, Packet sniffing and spoofing attack *[week 1]*
2. *SYN flooding attack [week 2]*
3. *TCP Session Hijack attack [week 2]*
4. Intro to network's attacks' types (Phishing, Botnet, DoS (Denial of Service), Routing Hijacking, HoneyNets, Privilege Escalation, Man-in-the-middle, etc), Network Mapping tools, Vulnerability Scanners *[week 3]*
5. Malice-in-the-middle attack *[week 3]*
6. Heartblead bug and Attack *[week 4]*
7. Blended Attacks *[week 4]*

DNS [Week 5-6]:

8. Review of DNS (DNS Domain Hierarchical, Zone,query process, etc) *[week 5]*
9. DNS Spoofing and defense *[week 5-6]*
10. DNS Rebinding Attack and Defense *[week 6]*

Web security in practice [Week 7-8]:

11. Firewalls and Firewall Rules, Virtual Private Network (VPN, TLS/SSL), how to setup VPN to bypass firewalls *[week 7]*
12. Cross-site request forgery *[week 7]*
13. Cross-site scripting attacks *[week 8]*
14. SQL injection attack *[week 8]*

Wireless network security [Week 9]:

15. System security in wireless network (Trusted platforms, Trust principles, technologies and methodologies for trusted platforms, trusted platform in practice (TPM))
16. Physical layer security (Shannon's Perfect secrecy, Wyner's wiretap channel, Wiretap code for achievable Secrecy using linear codes)

Grading: 35% Homework, 20% midterm, 15% Project, 25% final exam, 5% in-class quiz participation activity.

ABET Student Outcome Coverage: This course addresses the following outcomes:

H = high relevance, M = medium relevance, L = low relevance to course.

(1) *An ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics.* **(H)** The course uses networks tools. Students must implement the security attacks and defenses. Engineering judgment is developed through understanding the vulnerability of network protocols and advantages of security defenses. Throughout the course we emphasize the need to use sound design principles instead of relying on ad-hoc heuristics only. Towards this direction, network security protocols with design flaws are discussed. Assignments require students to analyze other network protocols with weaknesses. The homework involves solving engineering problems identified by the assignments and exemplified by class discussion. The exams and projects challenge the students to identify other network security issues and their solutions.

(2) *An ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors.* **(M)** The project challenges the students to develop, design and implement different security attacks.

(3) *An ability to communicate effectively with a range of audiences.* **(M)** Students are required to write up their simulations in an engineering format. The ability to communicate effectively in writing is a portion of the grade received on homework and projects. Students are required to give a short presentation on their projects defined on security attacks and defenses.

(4) *An ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts.* **(H)** The course covers security vulnerabilities in systems and their defense implications,

enabling the students to analyze and identify the vulnerabilities of network protocols. Impact of good network security protocols is emphasized. We discuss the impact of design and implementation of insecure protocols and the way they can be exploited. Case studies of designing protocols that are resilient to common security threats such as man-in-the-middle and denial of service attacks will be discussed.

(5) *An ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives.* **(H)** The course project is conducted in teams of three to four members and constitutes 15% of their grade.

(7) *An ability to acquire and apply new knowledge as needed, using appropriate learning strategies.* **(H)** The course emphasizes the need for evolving current secure system designs as new threats emerge and security assumptions are weakened. Further, pointers to security websites and articles will be provided in order to enhance knowledge in this emerging area.

Master Course Description for EE-468 (ABET sheet)

Title: Software and Embedded Systems Security
Credits: 4
Coordinator: Radha Poovendran, Professor, Electrical and Computer Engineering

Goal: This course in general is about exploiting the basic building blocks of security bugs—assembler, source code, the stack, the heap, and so on and help the students to explore, and understand the systems they are running and how to better protect them. This course covers the critical topic of discovering, exploiting, and preventing system security flaws by integrating and applying the techniques and methodologies; also discusses the strengths and weaknesses of these techniques and methodologies, and when each should be used. In particular, the course will teach binary reverse engineering, vulnerability analysis, exploit development, patching vulnerabilities, bug hunting, etc. through ten-weeks of hands-on labs with examples. During this course students will learn how to use GDB debugger which demonstrates what is going in a program while it executes or what another program was doing at the moment it crashed.

Learning Objectives: At the end of this course, students will be able to:

1. Using GDB debugger to analyze binary codes
2. Writing shell codes and exploit the vulnerabilities in the shell environment
3. Investigating the basic building blocks of security bugs—assembler, source code, the stack, the heap
4. How to exploit the vulnerabilities of system using binary codes and analyzing defenses proposed to address these vulnerabilities
5. Plan and execute a cyber penetration test, and utilize various vulnerability vectors that can be used to achieve an attacker's goals.

Prerequisites by Topic:

1. EE 469 Computer Architecture I (5) [Recommended]
2. EE 472 Real-Time and Embedded Operating Systems [Highly Recommended]

3. EE 241 Programming for Signal and Information Processing Applications or Familiarity with Python is essential [Required]

Textbooks:

1. Chris Anley et al., The Shellcoder's Handbook: Discovering and Exploiting Security Holes, 2nd Edition 2nd Edition

References:

2. Wenliang Du, Computer & Internet Security: A Hands-on Approach, Second Edition
3. Peter Kim, *The Hacker Playbook 3: Practical Guide to Penetration Testing*, McGraw-Hill, 2018.
4. Matt Monte, *Network Attacks and Exploitation: A Framework* (1st edition), 2015.

Topics:

1. Intro to reverse engineering (e.g., Binary analysis, Exploit writing, Patching vulnerabilities) *[Week 1]*
2. Environment variable and attack *[Week 2]*
3. Writing shellcode, shellcode tricks, shellshock attack *[Week 3]*
4. Frame-pointer attack and buffer overflow attack *[Week 4]*
5. Return to libc and ROP attack *[Week 5]*
6. Format string vulnerability *[Week 6]*
7. ShadowStack, CFI, and other defenses *[Week 7]*
8. Meltdown attack and Spectre attack *[Week 8]*
9. Hardware Trojans and techniques for hardware Trojan threat mitigation *[Week 9]*

Grading: 20% Homework, 40% projects, 10% midterm, 20% final exam, 5% in-class activity, 5% for filling the end of the course evaluation forms.

ABET Student Outcome Coverage: This course addresses the following outcomes:

H = high relevance, M = medium relevance, L = low relevance to course.

(1) *An ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics.* **(H)** The course uses binary debugger tools e.g. GDB. Students must implement the security attacks and defenses. Engineering judgment is developed through understanding the vulnerability of systems security defenses. Throughout the course we emphasize the need to learn how to write customized tools to protect your systems, not just how to use ready-made ones. Towards this direction, security defenses designed to address the flaws are discussed. Assignments require students to analyze other defenses with weaknesses. The homework involves solving engineering problems identified by the assignments and exemplified by class discussion. The students develop the state-of-the-art system security attacks and their defenses.

(2) *An ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors.* **(M)** The project challenges the students to develop, design and implement different system security attacks.

(3) *An ability to communicate effectively with a range of audiences.* **(M)** Students are required to write up their simulations in an engineering format. The ability to communicate effectively in writing is a portion of the grade received on homework and projects. Students are required to give a short presentation on their projects defined on system security attacks and defenses.

(4) *An ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts.* **(H)** The course covers system security vulnerabilities and their defense implications, enabling the students to recognize the vulnerabilities of softwares and systems. Impact of good system security and the need to learn how to write customized tools to protect your systems is emphasized. We discuss the impact of design of insecure systems and the way they can be exploited. Focus here will be to show how to design systems that are resilient to common security threats such as buffer overflow attacks.

(5) *An ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives.* **(H)** The course project is conducted in teams of up to three to four members and constitutes 15% of their grade.

(7) *An ability to acquire and apply new knowledge as needed, using appropriate learning strategies.* **(H)** The course emphasizes the need for evolving current secure

system designs as new threats emerge and security assumptions are weakened. Further, pointers to security websites and articles are provided in order to enhance personal knowledge in this developing area.

Master Course Description for EE-4XX (ABET sheet) New Course

Title: Machine Learning for Cyber Security

Credits: 4

UW Course Catalog Description

Coordinator: Radha Poovendran, Professor, Electrical and Computer Engineering

Goals: This course will study the use of machine learning for cybersecurity applications. There are many security applications which have large amounts of data related to the system as well as adversarial actions. Our ability to identify the type of machine learning algorithms that are useful for specific security applications can help us to improve the defense against attacks and also anticipate the potential attack variants that may arise in the future. Even in the case when one does not know the type of attack, if the machine learning algorithms can identify any anomaly, then the next level of security checks can be performed by other means or experts.

But nothing comes in life for free and this holds for machine learning in the context of cyber too! Another point to remember is "Beware of what you add to your tool bag! You may have an adversary manipulating your machine learning itself." This leads to adversarial machine learning where the machine learning could be tricked to fail the detection! Attacks on Google Video, Toxic Comments, and Google Vision are some of the fun examples where simple modifications make the machine learning algorithms fail!

We will start with setups where the machine learning will be useful for the cybersecurity. As indicated in the title of the course, it will be hands-on course on applying machine learning for cybersecurity applications. Machine learning algorithms will be introduced as needed.

Learning Objectives: At the end of this course, students will be able to:

1. Use machine learning algorithms to implement cybersecurity concepts
2. Implement machine learning algorithms such as clustering, k-means, regression and ensemble methods for anomaly/intrusion detection

3. Use Python libraries - NumPy, and Scikit-learn to build and evaluate AI models

4. Understand how to combat malware, detect spam, and cyber anomalies

5. Use the state-of-the-art python libraries e.g. TensorFlow to develop complex models in the cybersecurity domain and implement real-world examples

Textbook: Hands-On Machine Learning for Cybersecurity by Soma Halder and Sinan Ozdemir; Packt Publisher.

Reference Texts:

1. AI for CyberSecurity by Alessandro Parisi; Packt Publishers
2. Machine Learning for Cybersecurity by Chiheb Chebbi; Packt Publishers
3. Machine Learning for Penetration Testing by Emmanuel Tsukerman; Packt Publishers
4. Adversarial Machine Learning by Vorobeychik and Kantarcioglu; Morgan and Claypool Publishers

Prerequisites by Topic:

1. Math 208 Matrix Algebra with Applications [Required]

2. Stat 390 Statistical Methods in Engineering and Science or IND E 315 Probability and Statistics for Engineers [Required]

3. EE 241 Programming for Signal and Information Processing Applications or Familiarity with Python is essential [Required]

4. EE 445 Fundamentals of Optimization and Machine Learning [Recommended]

Topics:

1. Introduction to Machine Learning for Cyber Security and Python Basics Review [Week 1]

2. Supervised Learning Techniques for Detecting Spam Emails [Week 2]

3. Machine Learning for Solving Automated Public Turing test to tell Computers and Humans Apart (CAPTCHAs) [Week 3]

4. Data Dimensionality Reduction in Cyber Attack Data [Week 4]

5. Network Anomaly Detection Using Clustering Techniques [Week 5]

6. Credit Card Fraud and Malicious Event Detection Using Decision Trees [Week 6]

7. Ensemble Learning for Online Ad blocking, Program Binary Analysis, and Credit Card Fraud Detection [Week 7]

8. Natural Language Processing Techniques for Instruction Set Architecture Identification of Program Binaries [Week 8]

9. Introduction to Adversarial Machine Learning and Backdoor Attacks (Trojan Horses) in Deep Learning [Week 9]

Course Structure: The class meets for two lectures a week, each consisting of 2 hours. There is (bi-)weekly homework due that includes small computer projects in Python. One team-oriented project is planned in this course with Python. Course includes one midterm and one final exam. In-class activities include daily quizzes.

Computer Resources: The course uses Python for homework exercises and course projects. Students are expected to use their personal laptops, but they may use the ECE department computers if available.

Grading: 45% Homework, 50% Project, 5% in-class quiz participation activity.

ABET Student Outcome Coverage: This course addresses the following outcomes:

H = high relevance, M = medium relevance, L = low relevance to course.

(1) *An ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics.* **(H)** The course uses mathematical tools. Students must identify and design suitable machine learning algorithms. Engineering judgment is developed through the understanding the limitations and advantages of a given data pre-processing techniques and/or machine learning algorithms. Throughout the course we emphasize the need to use sound design principles instead of relying on ad-hoc heuristics only. Towards this direction, machine learning algorithms that were mathematically correct but had design flaws are discussed. Assignments require students to analyze other machine learning algorithms with weaknesses. The homework involves solving engineering problems identified by the assignments and exemplified by class discussion. The homework and

project challenge the students to identify the issues and formulate their individual solutions.

(2) *An ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors.* **(M)** The project challenges the students to develop, design and implement different machine learning algorithms. In most cases, this is implemented in Python.

(3) *An ability to communicate effectively with a range of audiences.* **(M)** Students are required to write up their simulations in an engineering format. The ability to communicate effectively in writing is a portion of the grade received on homework and projects. Students are required to give a short presentation on a selected security topic to the class (depending on the instructor).

(4) *An ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts.* **(H)** The course covers security vulnerabilities in systems and their societal implications, enabling the students to recognize the ethical dilemmas that they may face in their professions. Impact of good network security protocols is emphasized. We discuss the impact of design and implementation of insecure machine learning algorithms and the way they can be exploited. Focus here will be to show how to design machine learning algorithms that are resilient to common security threats such as spams, toxic comments, and malicious URLs.

(5) *An ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives.* **(H)** The course project is conducted in teams of up to three to four members and constitute 45% of their grade.

(7) *An ability to acquire and apply new knowledge as needed, using appropriate learning strategies.* **(H)** The course emphasizes the need for evolving current secure system designs as new threats emerge and security assumptions are weakened. Further, pointers to security websites and articles are provided in order to enhance personal knowledge in this developing area.

Prepared By: Radha Poovendran

Last revised: 04/20/2022

Master Course Description for EE-418 (ABET sheet) New Name

Title: Network Security and Cryptography → **Applied Cryptography**

Credits: 4

UW Course Catalog Description

Coordinator: Radha Poovendran, Professor, Electrical and Computer Engineering

Goals: To develop an understanding of the fundamental principles of cryptography and its application to network and communication security. This course will serve as an introduction to the fundamental tools in cryptography and the protocols that enable its application to network and communication security. This course is an introduction to the basic theory and practice of cryptographic techniques used in computer security. We will cover topics including encryption (secret-key and public-key), digital signatures, secure authentication, key management, cryptographic hashing, public key infrastructure, and ethics and challenges associated with the use of computer security in vulnerable world.

Learning Objectives: At the end of this course, students will be able to:

1. *Describe* the basic cryptographic primitives, authentication protocols and why they work, what are the common design errors.
2. *Design, implement and analyze* some of basic algorithms to be covered in class using Python (or other languages such as MATLAB, Mathematica).
3. *Design* algorithms using block ciphers and relate it to the modern symmetric key encryption standards.
4. *Design and analyze* Hash functions for checking message integrity under transmission.
5. *Design and* analyze Message Authentication Codes (MAC)
6. *Analyze* the strength of a given crypto system using classical and modern cryptanalysis tools to be presented in class.

7. *Describe and analyze* authenticated session establishment protocols used in Internet Communication

8. *Describe* the ethical issues related to the misuse of computer security.

Textbook: D. Stinson, *Cryptography Theory and Practice*, 4th edition, Chapman & Hall/CRC, 2019.

Reference Texts:

1. C. Kaufman, R. Perlman, M. Speciner, *Network Security (Private Communication in a Public World),* Prentice Hall, 2002.

2. A. Menezes, P. Van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 2001.

Prerequisites by Topic:

1. Math 208 Matrix Algebra with Applications [Required]

2. Stat 390 Statistical Methods in Engineering and Science or IND E 315 Probability and Statistics for Engineers [Required]

3. EE 241 Programming for Signal and Information Processing Applications or Familiarity with Python is essential [Required]

Topics:

1. Introduction to classical cryptography and cryptanalysis (Stinson Chapter 1) [Week 1-2]

2. Block Ciphers and the Advanced Encryption Standard (Stinson Chapter 3) [Week 2]

3. Public key encryption based on RSA and Integer Factorization (Stinson Chapter 5) [Week 3]

4. Public key encryption based on El-Gamal and Discrete Logarithm Problem (Stinson Chapter 6) [Week 4]

5. Hash Functions for Message Integrity Verification (Stinson Chapter 4) [Week 5-6]

6. Digital signatures (RSA, El-Gamal, DSA) (Stinson Chapter 7) [Week 6-7]

7. Key Management Schemes, Authenticated Key Agreement Schemes (Stinson Chapter 10) [Week 8]

8. Public Key Infrastructure and the PKI Standard [Week 9]

9. Technology, Ethical Challenges, IEEE Code of Ethics related to Security Engineering in a vulnerable world [Week 9]

Course Structure: The class meets for two lectures a week, each consisting of 2 hours. There is (bi-)weekly homework due that includes small computer projects in Python. One team-oriented project is planned in this course with Python. Course includes one midterm and one final exam. In-class activities include daily quizzes.

Computer Resources: The course uses Python for homework exercises and course projects. Students are expected to use their personal laptops, but they may use the ECE department computers if available.

Grading: 35% Homework, 20% midterm, 15% Project, 25% final exam, 5% in-class quiz participation activity.

ABET Student Outcome Coverage: This course addresses the following outcomes:

H = high relevance, M = medium relevance, L = low relevance to course.

(1) *An ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics.* **(H)** The course uses mathematical tools. Students must identify and design suitable algorithms. Engineering judgment is developed through the understanding the limitations and advantages of a given cryptographic algorithm or network security protocol. Throughout the course we emphasize the need to use sound design principles instead of relying on ad-hoc heuristics only. Towards this direction, security protocols that were mathematically correct but had design flaws are discussed. Assignments require students to analyze other protocols with weaknesses. The homework involves solving engineering problems identified by the assignments and exemplified by class discussion. The exams and projects challenge the students to identify the issues and formulate their individual solutions. The students develop an implementation for stream cipher-based encryption of speech.

(2) *An ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors.* **(M)** The project challenges the

students to develop, design and implement different cryptographic algorithms. In most cases, this is implemented in Python.

(3) *An ability to communicate effectively with a range of audiences.* **(M)** Students are required to write up their simulations in an engineering format. The ability to communicate effectively in writing is a portion of the grade received on homework and projects. Students are required to give a short presentation on a selected security topic to the class (depending on the instructor).

(4) *An ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts.* **(H)** The course covers security vulnerabilities in systems and their societal implications, enabling the students to recognize the ethical dilemmas that they may face in their professions. Impact of good network security protocols is emphasized. We discuss the impact of design and implementation of insecure protocols and the way they can be exploited. Focus here will be to show how to design protocols that are resilient to common security threats such as user collusion.

(5) *An ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives.* **(H)** The course project is conducted in teams of up to three to four members and constitutes 15% of their grade.

(7) *An ability to acquire and apply new knowledge as needed, using appropriate learning strategies.* **(H)** The course emphasizes the need for evolving current secure system designs as new threats emerge and security assumptions are weakened. Further, pointers to security websites and articles are provided in order to enhance personal knowledge in this developing area.

Prepared By: Radha Poovendran

Last revised: 04/20/2022