Spring 2020

CS 646-102: Network Protocols Security (Revised for Remote Learning)

Roberto D. Rubino

Spring 2020
CS 646-102 : Network Protocols Security
Meeting Schedule: Tuesday 6:00pm – 8:50pm
Room: Faculty Memorial Hall 110

Instructor: Roberto D. Rubino
Email: rr8@njit.edu
Course website: https://canvas.njit.edu/
Webex meeting room: https://njit.webex.com/meet/rr8

Beginning with the March 24th class, instruction will move exclusively to a virtual setting. Real-time lectures will be provided via the professor's Webex personal meeting room at the standard class time and Webex address listed above. Lectures will be recorded and posted to the course website within 48-hours.

Office hours: Prior to class and by appointment (in-person & via Webex)

Prerequisites:
CS 656 or ECE 637: "Internet and Higher Layer Protocols".
Also, students should be able to program in C/C++ for the programming component of the mini-projects.

Textbook:
Due to the dynamic and evolving nature of the network security field, the course will feature a mixture of material based on the recommended textbook, on instructor notes, and on scientific articles in order to reflect recent developments in this area.

There is no required textbook.
The following textbook is recommended to help navigate the course material:
"Network Security: Private Communication in a Public World (2nd edition)",
by C. Kaufman, R. Perlman, M. Speciner,
Prentice Hall 2002 (ISBN 0130460192).

Description:
This course covers the security of network protocols currently used on the Internet. It seeks to familiarize students with common threats and network attacks, and provides an in-depth study of methods used to secure network communication. The course includes an applied component, which will help students gain practical experience in attacking and defending networked systems. Topics include authentication systems, secure communication at data link, network, transport and application layers, vulnerabilities of Internet protocols, domain name system and routing security, firewalls, intrusion detection, honeypots, wireless networks security, malware propagation and detection, and web security.

A tentative list of topics includes:

- Introduction (overview of network security issues, cryptographic algorithms, authentication techniques)
- Layer 2/3 security
- Authentication systems, Key establishment protocols, Kerberos
- Secure communication at the data link and network layers (IPSEC and IKE)
- Secure communication at the transport and application layers (SSL/TLS, email security, PGP)
- Vulnerabilities of Internet protocols
- Denial of service (DoS) attacks and defenses
- Firewalls, IP spoofing prevention
- Routing protocols security and router security
- Domain name server (DNS) security
- Traffic monitoring, Intrusion detection, Honeypots
- Wireless networks security
- Spam, Phishing, and Pharming
- Malware propagation and containment, Botnets
- Anonymity and privacy on the Web

Grading:

Three Projects:	45%
Midterm exam:	25%
Final exam:	30%

Extra credit will be given for active participation in discussions during the class (up to 10%). The exams are closed book unless specified otherwise.

Learning Outcomes:

After completing the course, students will be able to:

- Identify the appropriate security primitives that should be used to achieve specific security goals for communication over insecure networks.
- Analyze the security of the main mechanisms used on the Internet to secure communication between computer systems at various network layers, including physical, network, transport, and application layers.
- Describe common attacks against wired and wireless network protocols using standard terminology, allowing them to communicate effectively with other security professionals.
- Assess whether a given communication protocol achieves the desired security goals.
- Design a new communication protocol that achieves one or more specific security goals.
- Gain a deep understanding of attacks against web applications and of design principles for effective defenses.
- Critically analyze a scientific article that focuses on the security of network protocols.

Honor Code:
The NJIT Honor Code will be upheld, and any violations will be brought to the immediate attention of the Dean of Students. Note in particular that copying lab assignments or exam papers, in full or in part is forbidden.

Modifications to Syllabus:
The syllabus may be modified at the discretion of the instructor or in the event of extenuating circumstances. Students will be notified in class of any changes to the syllabus.