INSE 6120: Cryptographic Protocols and Network Security

1 General Information

- Course name: INSE 6120 Cryptographic Protocols and Network Security (4 credits)
- Lecture time & location
  - Section FF: Tuesdays, 17:45-20:15, FG-B060
  - Section DD: Mondays, 17:45-20:15, FG-C070
- Instructor: Mohammad Mannan, Concordia Institute for Information Systems Engineering, ENCS.
- Office: EV6.221 (EV building, 6th floor)
- Email: m.mannan@concordia.ca
- Office hours: Tuesdays from 11:45-13:15
- Course website (general info): http://www.encs.concordia.ca/~mmannan/teaching/inse6120-fall2013.html
- Course materials: **accessible only on Moodle (via MyConcordia.ca)**
- Communication: Last minute changes, announcements and useful hyperlinks will be made available on Moodle or via email (must access the email registered at MyConcordia.ca)

2 Course Description

- The course introduces concepts, methodologies, techniques, tools and research problems in network security. Methods used in the design and analysis of security protocols, as well as an introduction to prominent cryptographic protocols will be presented. We will address the issue of network security policies, authentication and authorization services. In addition, we will address issues such as botnets, darknets and network security monitoring.
- A selected subset of the following topics will be covered: Cryptographic protocols, authentication protocols, key distributions protocols, e-commerce security protocols, security protocol properties: authentication, secrecy, integrity, availability, non-repudiation, atomicity, certified delivery, crypto-protocol attacks, security protocols design, implementation and analysis. OSI security architecture, models and architectures for network security, authentication using Kerberos and X.509, email security (PGP, S/MIME), IP security, IPv6, web security, SSL/TLS, virtual private networks, firewalls (screening routers, packet filtering, firewall architecture and theory, implementations and maintenance, proxy servers), content filtering, denial of service attacks, wireless networks security, network security policies, intrusion detection, host-based IDS, network based IDS, misuse detection methods, anomaly detection methods, intrusion detection in distributed systems, intrusion detection in wireless ad hoc networks.
- Prerequisite: INSE6110 Foundations of Cryptography or equivalent. Basic understanding of cryptographic techniques and networking is required.

3 Learning Outcomes

By the end of the course, the students will learn about:

1. Cryptographic protocols: taxonomy, design and analysis
2. Protocol properties and flaws
3. Network security policies
4. Authentication and authorization services
5. IP security and virtual private networks
6. Public key infrastructure
7. Intrusion detection and prevention
8. Network security monitoring

In addition, we will tentatively organize labs where the students will be exposed to the main practices of network security on Cisco networking infrastructure. More precisely, they will be exposed to:

1. Basic routing and switching commands on Cisco devices
2. AAA security, NAT, control lists and threat mitigation
3. Configuration of firewall and intrusion prevention systems
4. Configuration of virtual private networks using IKE and IPSec
5. Setup of a network topology, securing it and attack mitigation

4 Tentative Schedule

The following set of slides, available from the Moodle course site, will be covered in (order may vary).

1. Cryptographic Protocols: Definitions, Properties, Types
2. Cryptographic Protocols: Taxonomy of Attacks and Analysis
3. Design Principles of Engineering Security Protocols
4. Analysis of Security Protocols
5. Analysis of SSL
6. Worms: Propagation and Detection Techniques
7. Distributed Denial of Service (DDoS) Attacks
8. Online Dictionary Attacks and Defences
9. Botnet Detection and Defences
10. Internet Censorship

Notes:

- The aforementioned schedule, content and order may be subject to modification by the instructor when judged academically appropriate without prior notice.
- The midterm will be held close to mid-October. Exact time for the midterm, the project presentations/report submission and the final exam will be announced in class. The final exam will be scheduled by the University examination office during the final exam period.

5 Course Materials

1. Lecture slides and papers as made available via the course Moodle site
2. Optional Textbook: Protocols for Authentication and Key Establishment
   - Authors: Colin Boyd, Anish Mathuria
   - Publisher: Springer, ISBN-10: 3540431071
   - Parts of the book can be accessed through Google eBook books.google.ca
   - Few copies of the book are available in the Concordia book store
3. Optional Textbook: Network Security: Private Communications in a Public World, 2nd edition
   - Authors: Charlie Kaufman, Radia Perlman, Mike Speciner
   - Publisher: Prentice Hall, ISBN-10: 0130460192
4. Optional Textbook: Handbook of Applied Cryptography
   - Authors: Alfred Menezes, Paul Van Oorschot, Scott Vanstone
   - Publisher: CRC press, ISBN: 0-8493-8523-7
   - Free copy of the book is available online www.cacr.math.uwaterloo.ca/hac
5. Optional Textbook: Cryptography and Network Security: Principles and Practice, fifth edition
   - Authors: William Stallings
   - Publisher: Prentice Hall, ISBN: 978-0-13-609704-4
   - Older editions (e.g., 3e) are fine

6 Marks Distribution

1. **25%**: Assignments/Projects (may include programming, report writing and presentations)
2. **25%**: Midterm exam
3. **50%**: Final exam

Late Assignments: All assignments/projects will be due in class (unless otherwise specified). Late assignments suffer a penalty rate of 20% per day, up to 5 days (weekends count).

Midterm Makeup: There will be NO makeup for the midterm. In the case of a serious illness or emergency, the weight of the midterm will be moved towards the final exam. Be prepared to provide written documentation (e.g., a medical excuse from your doctor) to verify the emergency and its seriousness.

7 Academic Code of Conduct

Any form of cheating, plagiarism, impersonation, falsification of a document as well as any other form of dishonest behaviour by a student is an academic offence under the Academic Code of Conduct and may lead to severe academic penalties up to and including suspension and expulsion. As examples only, you are not permitted to:

- Copy from anywhere without indicating where it came from
- Let another student copy your work and then submit it as his/her own
- Hand in the same assignment in more than one class

- Have unauthorized material or devices in an exam. Note that you do not have to be caught using them just having them is an offence
- Copy from someone's else exam
- Communicate with another student during an exam
- Add or remove pages from an examination booklet or take the booklet out of an exam room
- Acquire exam or assignment answers or questions
- Write an exam for someone else or have someone write an exam for you
- Submit false documents such as medical notes or student records
- Falsify data or research results

For details of the Academic Code of Conduct, see: provost.concordia.ca/academicintegrity/

8 Students' Responsibilities

1. Students are expected to attend every class. Some material may only be covered in class and not made available on the course website. Students are expected to read the assigned material and to actively participate in class discussions.
2. Students are expected to be respectful of other people's opinions and to express their own views in a calm and reasonable way. Disruptive behaviour will not be tolerated. Students are expected to be familiar with the Code of Rights and Responsibilities: http://rights.concordia.ca
3. If you cannot attend class for any reason, unforeseen or not, you are to come and talk or write to me as soon as possible.

9 Student Services

1. Concordia Counselling and Development offers career services, psychological services, student learning services, etc. http://cdev.concordia.ca
2. The Concordia Library Citation and Cycle Guides: http://library.concordia.ca/help/howto/citations.html
3. Advocacy and Support Services: http://supportservices.concordia.ca
4. Student Transition Centre: http://stc.concordia.ca
5. New Student Program: http://newstudent.concordia.ca
6. Office for Students with Disabilities: http://supportservices.concordia.ca/disabilities/
7. The Academic Integrity Website: http://provost.concordia.ca/academicintegrity/

10 Disclaimer

In the event of extraordinary circumstances beyond the University's control, the content and/or evaluation scheme in this course is subject to change.