Mini Research Project on a Current Topic in Network Security: Tips, Resources, Timeline

The 'mini research project' requirement for EECS 4482 should be seen as a 4-fold opportunity:

1) To deepen your knowledge about one of the fundamental, well-known and current topics in network security, which is not covered in the regular lectures, and which you are interested and curious about.
2) To perform independent research on a technical topic using a range of on-line resources.
3) To practice you teamwork, leadership and critical-thinking skills.
4) To improve you presentation and public-speaking skills.

General Tips

1) When picking the topic:

- Pick a topic that you **are interested about** and/or **think is important**.

2) When researching the topic:

- Take enough time to research the topic (*ideally 3+ weeks*).
- Consult a number of different sources/references to obtain a range of different views and perspectives. *(The optimal number of references is 10 or more.)*
- Make sure to research (i.e., learn about) not only the fundamental theory but also the latest trends pertaining to the given topic.

3) When preparing the presentation:

- Take enough time to prepare and rehearse the presentation.
- Keep your slides simple. *(Text should be in bullet form, with not more than 2 lines per bullet, and no more than 5 bullets per slide. Slides with images should have less if any text.)*
- Apply *'a picture is worth a thousand words'* rule when putting your presentation together. *(If used properly, images can considerably simplify the job of explaining a complex concept, while magnifying the overall impact and effectiveness of your presentation.)*
- **Presentation should be concluded with 3 points (in questions + answers form) that the audience should remember.** *(Some of these questions will be included in the midterm and final examination.)*

2) When delivering the presentation:

- **The presentation should be approx. 8-10 minutes long.** *(3 min per each presenter!)*
- http://www.wikihow.com/Do-a-Presentation-in-Class

TIMELINE

Before Friday January 18.	**Teams of 3 students formed. Topic and resentation dates determined.** Students are encouraged to form 3-member teams on their own, as well as to choose their preferred topic and presentation date. The dates will be allocated on 'first-come first-served' basis. A representative of each team should email the instructor (vlajic@cse.yorku.ca) the following information by Friday, Jan 18: 1) **the exact names, student numbers, and email addresses of all team members**; 2) the preferred topic; 3) the preferred presentation date. Students that fail to form their own teams and/or pick their topic will be assigned to a randomly-formed team by the instructor, and will be allocated a randomly-selected topic as well as a randomly-selected presentation date. **For a list of possible presentation dates see the course Web-site!**
At least a week before presentation date allocated to Team X.	**Team X emails a preliminary copy of their presentation to the instructor.** At least a week before Team X's presentation date, the team will send a soft-copy of their presentation to the instructor. The instructor will examine the presentation for quality, clarity and organization, and provide a feedback within 1-2 days.

EVALUATION

The base score for each presentation will be obtained as a weighted sum:

$$\textbf{BaseScore} = 0.5 * \textbf{InstructorScore} + 0.5 * \textbf{AverageStudentScore}$$

Both the instructor and the audience-students will fill out a performance evaluation sheet and provide their individual scores for: a) the depth, and b) quality/clarity of the presentation.

To encourage early presentations, the 'bonus' weighting scheme will additionally be applied:

$$\textbf{ActualScore (Team presenting in slot(i))} = \textbf{BaseScore} * \left(1.25 - \frac{0.25}{9}(i-1)\right)$$

where, i = 1, 2, ..., 10 are the days/slots of student presentations, starting January 30 (see course Web-site).

Reference Sites

Below is a list of recommended reference sites that you may find useful when researching a particular network security topic:

- IEEE online library: http://ieeexplore.ieee.org.ezproxy.library.yorku.ca/Xplore/home.jsp
- ACM online library: http://dl.acm.org.ezproxy.library.yorku.ca/dl.cfm
- Elsevier online library: http://sciencedirect.com.ezproxy.library.yorku.ca

Available Topics

~~1. Bluetooth Security/Attacks~~ **Team 8 (A. D'Errico, M. Jafareih, A. Halawani)**

NIST Guide to Bluetooth Security
https://www.niatec.iri.isu.edu/(S(5pvzas455hrdzsrxbwh1ndqb))/GetFile.aspx?pid=505
Bluetooth Security: Treats and Solutions A Survey
https://pdfs.semanticscholar.org/8872/521819c79505ac20e5da8dd14f8c41eb3f07.pdf
Security Vulnerabilities in Bluetooth Technology as Used in IoT
https://www.mdpi.com/2224-2708/7/3/28/pdf
Security threats in Bluetooth technology
https://www.sciencedirect.com/science/article/pii/S0167404817300615
Bluetooth Security (Presentation)
https://ece.umd.edu/class/ents650/BluetoothSecurity.pdf

~~2. DNS Security/Attacks (DNSSEC)~~ **Team 3 (A. Klif, N. Ahmad, A. Al-Gailani)**

Issues in DNS Security
https://cdn.ttgtmedia.com/rms/pdf/DNS%20Security_Ch%202.pdf
Security vulnerabilities in DNS and DNSSEC
http://web.mit.edu/6.033/www/papers/dnssec.pdf
Understanding and Deploying DNSSEC
https://conference.apnic.net/data/39/dnssec-final_1425360815.pdf
Domain Name System Security
https://acsc.gov.au/publications/protect/dns_security.pdf
DNS Security
https://www.f5.com/pdf/agility2018/dns_security.pdf

~~3. BGP Security/Attacks~~ **Team 10 (A. Solovey, Y. Bai, H. Ahmad)**

BGP Security Best Practices
https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf
Securing BGP — A Literature Survey
https://ieeexplore-ieee-org.ezproxy.library.yorku.ca/stamp/stamp.jsp?tp=&arnumber=5473881
Securing the Border Gateway Protocol
https://www.cs.purdue.edu/truselab/readings/ripe45-eof-stephen.pdf
The State of BGP Security
https://www.blackhat.com/docs/us-15/materials/us-15-Remes-Internet-Plumbing-For-Security-Professionals-The-State-Of-BGP-Security.pdf
Security in Border Gateway Protocol (BGP)
https://www.researchgate.net/publication/272485008_Security_in_Border_Gateway_Protocol_BGP

~~4. IPv6 Security/Attacks~~ **Team 2 (H. Sharma, S. Saad, S. Ahmed)**

The security implications of IPv6
https://www.sciencedirect.com/science/article/pii/S1353485813700680
IPv6 Security Vulnerabilities
http://dergipark.gov.tr/download/article-file/147978
IPv6 Security: Attacks and Countermeasures in a Nutshell
https://www.sba-research.org/wp-content/uploads/publications/Johanna%20IPv6.pdf
IPv6 Security
https://www.first.org/resources/papers/conf2018/Herberg-Frank_FIRST_20180624.pdf
It's begun: 'First' IPv6 denial-of-service attack puts IT bods on notice
https://www.theregister.co.uk/2018/03/03/ipv6_ddos/

~~5. VoIP Security/Attacks~~ **Team 6 (K. Irizawa, R. Wan, E. R. Aguero)**

Introduction to VoIP Security
https://www.owasp.org/images/b/b6/VOIP_Security_basics.pdf
VoIP Security and Best Practices
https://www.sangoma.com/wp-content/uploads/2018/06/voip-security-best-practices.pdf
Intrusion prevention: The future of VoIP security
http://691d3755c7515ca23f7b-dbfc12bd0c5671837096480939977d459.r57.cf1.rackcdn.com/assets/networking-wp-intrusion-prevention-the-future-of-volp-security-wp-4aa3-0863enw.pdf
A Survey on VoIP Security Attacks and Their Proposed Solutions
http://ijaiem.org/Volume2Issue3/IJAIEM-2013-03-15-032.pdf
VoIP Hacking Techniques
https://hakin9.org/voip-hacking-techniques/
VoIP's Big Security Problem? It's SIP
https://www.pcmag.com/article/365251/voips-big-security-problem-its-sip

~~6. DHCP Security/Attacks~~ **Team 7 (D. Geller, M. Arndt, K. Sarbinowski)**

DHCP Security Features Technology White Paper
http://download.h3c.com/download.do?id=320314
DHCP exploitation guide
https://www.whitewinterwolf.com/posts/2017/10/30/dhcp-exploitation-guide/
A closer look into DHCP starvation attack in wireless networks
https://www.sciencedirect.com/science/article/pii/S0167404816301262
Solutions for LAN Protection
https://www.alliedtelesis.com/sites/default/files/documents/solutions-guides/lan_protection_solution_reva.pdf
Complete Guide to DHCP Snooping
http://www.firewall.cx/cisco-technical-knowledgebase/cisco-switches/1215-understanding-dhcp-snooping-concepts-and-how-it-works.html

~~7. 6LoWPAN Security/Attacks~~ **Team 9 (D. Li, D. Torres Fleites, M. Ahmad)**

Communication security and privacy support in 6LoWPAN
https://www.sciencedirect.com/science/article/abs/pii/S221421261630117X
Analytical study of security aspects in 6LoWPAN networks
https://www.researchgate.net/publication/261160546_Analytical_study_of_security_aspects_in_6LoWPAN_networks
Security Protocols and Privacy Issues into 6LowPAN Stack: A Synthesis
https://ieeexplore.ieee.org/document/6905706
6LoWPAN Fragmentation Attacks and Mitigation Mechanisms

https://www.comsys.rwth-aachen.de/fileadmin/papers/2013/2013-hummen-6lowpan.pdf
6LoWPAN
http://home.deib.polimi.it/cesana/teaching/IoT/como/classes/5-6LowPAN.pdf

~~**8. Botnet Communications and Protocols**~~ **Team 1 (V. Martintsov, A. Winkler, M. Chowdhury)**

A Taxonomy of Botnet Behavior, Detection, and Defences
https://ieeexplore-ieee-org.ezproxy.library.yorku.ca/stamp/stamp.jsp?tp=&arnumber=6616686
Botnet Communication Patterns
https://ieeexplore-ieee-org.ezproxy.library.yorku.ca/stamp/stamp.jsp?tp=&arnumber=8026031
A Survey on Botnet Architectures, Detection and Defences
https://pdfs.semanticscholar.org/bfae/82b6ff8044ac7d20c8c2556b62088af4a415.pdf
Botnets: Lifecycle and Taxonomy
https://www.researchgate.net/publication/252012673_Botnets_Lifecycle_and_Taxonomy
Botnets in DDoS Attacks: Trends and Challenges
http://www.cs.uccs.edu/~jkalita/papers/2015/HoqueNazrulEEETutorials&Surveys2015.pdf

~~**9. Latest Trends in DDoS Attacks**~~ **Team 5 (P. Bhardway, T. Gumbs, S. Wirk)**

Delving into Internet DDoS Attacks by Botnets: Characterization and Analysis
https://ieeexplore-ieee-org.ezproxy.library.yorku.ca/stamp/stamp.jsp?tp=&arnumber=8528549
DDoS attacks and rise of IoT botnets
https://ripe75.ripe.net/presentations/53-RIPE75-DDoS-and-Rise-of-IOT-botnets.pdf
Half Year 2018 DDoS Trends Report
http://info.corero.com/rs/258-JCF-941/images/H1-2018-Corero-Trends-Report-Final.pdf
Threat Report: Distributed Denial of Service (DDoS)
https://www.nexusguard.com/hubfs/Threat%20Report%20Q2%202018/Nexusguard_DDoS_Threat_Report_Q2_2018_EN.pdf

~~**10. Anonymous Networks**~~ **Team 4 (A. Wakif, B. Booth, E. Dao)**

How to Find Hidden Users: A Survey of Attacks on Anonymity Networks
https://ieeexplore-ieee-org.ezproxy.library.yorku.ca/stamp/stamp.jsp?tp=&arnumber=7152825
Anonymous Communication on the Internet
http://proceedings.informingscience.org/InSITE2014/InSITE14p103-120Grahn0483.pdf
A Survey on Routing in Anonymous Communication Protocols
https://arxiv.org/pdf/1608.05538.pdf
Recent Attacks on TOR
http://www.cse.hut.fi/en/publications/B/11/papers/salo.pdf
Shining Light in Dark Places: Understanding the Tor Network
https://homes.cs.washington.edu/~yoshi/papers/Tor/PETS2008_37.pdf