

# 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 your teamwork, leadership and critical-thinking skills.
- 4) To improve your 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

<p><b>Before Wednesday September 18.</b></p>	<p><b>Teams of 3 students formed. Topic and presentation dates determined.</b></p> <p>Students are encouraged to <u>form 3-member teams on their own</u>, as well as to choose their preferred <u>topic</u> and <u>presentation date</u>. The dates will be allocated on ‘first-come first-served’ basis.</p> <p>A representative of each team should email the instructor (<a href="mailto:vlajic@cse.yorku.ca">vlajic@cse.yorku.ca</a>) the following information by Wednesday, Sep 18:</p> <ol style="list-style-type: none"> <li>1) the exact <u>names</u>, <u>student numbers</u>, and <u>email addresses</u> of all team members;</li> <li>2) the <u>preferred topic</u>;</li> <li>3) the preferred <u>presentation date</u>.</li> </ol> <p>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 one of the left-over topic as well as a left-over presentation date.</p> <p><b>For a list of possible presentation dates see the course Web-site!</b></p>
<p><b>At least a week before presentation date allocated to Team X.</b></p>	<p><b>Team X emails 2 documents to the instructor:</b></p> <ol style="list-style-type: none"> <li>1) a preliminary copy of their presentation;</li> <li>2) a breakdown of each team-member’s contribution to the project/presentation.</li> </ol> <p>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. Besides their presentation, team X will also send another separate document clearly describing the contributions of each team member to the project’s background research as well as the preparation of presentation slides.</p>

## EVALUATION

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

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

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:

$$\text{ActualScore (Team presenting in slot(i))} = \text{BaseScore} * (1.25 - \frac{0.25}{8} (i - 1))$$

where, i = 1, 2, ..., 9 are the days/slots of student presentations, starting September 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: S. Doyle, A. Marjia, S. Attalla)**

NIST Guide to Bluetooth Security

[https://www.niatec.iri.isu.edu/\(S\(5pvzas455hrdzsrxbwh1ndqb\)\)/GetFile.aspx?pid=505](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 12: P. Sison, J. Laya, S. Usman)**

Issues in DNS Security

[https://cdn.ttgtmedia.com/rms/pdf/DNS%20Security\\_Ch%202.pdf](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](https://conference.apnic.net/data/39/dnssec-final_1425360815.pdf)

Domain Name System Security

[https://acsc.gov.au/publications/protect/dns\\_security.pdf](https://acsc.gov.au/publications/protect/dns_security.pdf)

DNS Security

[https://www.f5.com/pdf/agility2018/dns\\_security.pdf](https://www.f5.com/pdf/agility2018/dns_security.pdf)

### **3. BGP Security/Attacks**

BGP Security Best Practices

[https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC\\_III\\_WG4\\_Report\\_March\\_%202013.pdf](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](https://www.researchgate.net/publication/272485008_Security_in_Border_Gateway_Protocol_BGP)

#### **4. IPv6 Security/Attacks (Team 10: N. Anjum, A. Maywapersaud, ??)**

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](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/](https://www.theregister.co.uk/2018/03/03/ipv6_ddos/)

#### **5. VoIP Security/Attacks (Team 3: Z. Gu, J. Sun, Z. Cao)**

Introduction to VoIP Security

[https://www.owasp.org/images/b/b6/VOIP\\_Security\\_basics.pdf](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-dbf12bd0c567183709648093997d459.r57.cf1.rackcdn.com/assets/networking-wp-intrusion-prevention-the-future-of-voip-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: Z. Israr, L. Sterner, A. Tang)**

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](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**

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](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. IoT Security (Team 2: J. Park, L. Cho, R. Malatombee)**

Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

<https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf>

Smart IoT Devices in the Home: Security and Privacy Implications

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8371556>

An Overview of Wireless IoT Protocol Security in the Smart Home Domain

<https://arxiv.org/pdf/1801.07090.pdf>

A Survey of Protocols and Standards for Internet of Things

<https://arxiv.org/ftp/arxiv/papers/1903/1903.11549.pdf>

#### **9. Content Delivery Networks: Attacks and Defences (Team 1: S. Bhardway, J. Galati, S. Amininiaki)**

What Is a CDN?

<https://www.cloudflare.com/learning/cdn/what-is-a-cdn/>

CDN SSL/TLS / CDN Security

<https://www.cloudflare.com/learning/cdn/cdn-ssl-tls-security/>

End-User Get Maneuvered: Empirical Analysis of Redirection Hijacking in Content Delivery Networks

<https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-hao.pdf>

Forwarding-Loop Attacks in Content Delivery Networks

<https://www.jianjunchen.com/papers/cdn-loops.NDSS16.pdf>

#### **10. Botnet Communications and Protocols (Team 6: V. Vavan, E. G. Dos Santos, J. Hoang)**

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](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>

#### **11. Latest Trends in DDoS Attacks (Team 5: T. Alvear, A. El Shafie, A. Sharma)**

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](https://www.nexusguard.com/hubfs/Threat%20Report%20Q2%202018/Nexusguard_DDoS_Threat_Report_Q2_2018_EN.pdf)

## **12. Anonymous Networks (Team 9: L. Farhan, S. Johal, Z. Liu)**

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/InSITE14p103-120Grahm0483.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](https://homes.cs.washington.edu/~yoshi/papers/Tor/PETS2008_37.pdf)

## **13. Wi-Fi Tracking and MAC Address Randomization (Team 4: R. Dhamija, W. Safdar, A. Abu-Mahfouz)**

Wi-Fi Internet connectivity and privacy: hiding your tracks on the wireless Internet

[https://ora.ox.ac.uk/objects/uuid:dfa1a8fc-c97a-4ede-88dd-8d97d5693e92/download\\_file?file\\_format=pdf&safe\\_filename=Wi-Fi%2BInternet%2Bconnectivity%2Band%2Bprivacy%253B%2Bhiding%2Byour%2Btracks%2Bon%2Bthe%2Bwireless%2BInternet.pdf&type\\_of\\_work=Conference](https://ora.ox.ac.uk/objects/uuid:dfa1a8fc-c97a-4ede-88dd-8d97d5693e92/download_file?file_format=pdf&safe_filename=Wi-Fi%2BInternet%2Bconnectivity%2Band%2Bprivacy%253B%2Bhiding%2Byour%2Btracks%2Bon%2Bthe%2Bwireless%2BInternet.pdf&type_of_work=Conference)

On Wi-Fi Tracking and the Pitfalls of MAC Address Randomization

<https://ido2016.sciencesconf.org/122873/document>

A Study of MAC Address Randomization in Mobile Devices and When it Fails

[https://www.researchgate.net/publication/314361145\\_A\\_Study\\_of\\_MAC\\_Address\\_Randomization\\_in\\_Mobile\\_Devices\\_and\\_When\\_it\\_Fails](https://www.researchgate.net/publication/314361145_A_Study_of_MAC_Address_Randomization_in_Mobile_Devices_and_When_it_Fails)