Mini Project on Current Topics in Computer Security: Tips, Resources, Timeline

The 'mini project' requirement for EECS 3482 should be seen as a 4-fold opportunity:

1) To deepen your knowledge about a current and relevant topic in computer/information security that you are (also) interested and curious about.
2) To perform Internet-based journalism-style information gathering and reporting.
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/story that you are: 1) **passionate about**, and 2) **comfortable to discuss**.
- Take enough time to research the topic. *(Ideally a week or more for researching the topic, and another week for preparing the presentation.)*
- 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.)*

2) When preparing the presentation:

- Your presentation should address the following key questions pertaining to the selected topic:
  1) What exactly happened and why? *(background story)*;
  2) How it happened? *(technical aspects)*;
  3) What are the broader security and/or societal implications of this story?
- Where applicable, do your best to make a connection between the story you are covering and material taught in class.
- 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.)*

3) When delivering the presentation:

- **The presentation should be approx. 6 minutes long.** *(2 minutes per each presenter!)*
- http://www.wikihow.com/Do-a-Presentation-in-Class

TIMELINE

Before January 16.	**Teams of 3 students formed. Presentation dates determined.** Students are encouraged to form teams on their own, as well as to propose/choose their preferred 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 Monday, Jan 16: 1) **the exact names, student numbers, and email addresses of all team members**; 2) the preferred presentation date. Students that fail to form their own teams will be assigned to randomly-formed teams by the instructor, and will be allocated a randomly-selected presentation date.
At least a week before presentation date allocated to Team X.	**Team X informs the instructor about their selected topic.** Team X can select a presentation topic from the list of potential topics available in the last section of this document, or can come up with a topic of their own. (The topics from the provided list will also be allocated on the 'first-come first-served' basis.)
Friday/Sunday before presentation date allocated to Team X.	**Team X emails a preliminary copy of their presentation to the instructor.** Teams that present on a Monday will send a soft-copy of their presentation the preceding Friday, while teams that present on Wednesday will send a soft-copy of their presentation the preceding Sunday. The instructor will examine the presentation for quality, clarity and organization, and provide a feedback the following day.

EVALUATION

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

$$\textbf{BaseScore} = 0.3*\textbf{InstructorScore} + 0.7*\textbf{AverageStudentScore}$$

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, another 'bonus' weighting scheme will additionally be applied:

$$\textbf{ActualScore (Team presenting in slot(i))} = \textbf{BaseScore} * \left(1.25 - \frac{0.25}{17}(i-1)\right)$$

where, i = 1, 2, …, 18 are the days/slots of student presentations, starting January 18 (see course Web-site).

Reference Sites

Below is a list of assorted recommended reference sites that you may find useful when choosing and/or researching a particular cyber security topic and/or news story:

- http://www.infosecurity-magazine.com/
- http://securityintelligence.com/
- http://www.darkreading.com/
- http://www.securityweek.com/
- http://www.theregister.co.uk/security
- http://www.technewsworld.com/perl/section/cyber-security
- http://www.informationsecuritybuzz.com/
- http://www.homelandsecuritynewswire.com/topics/cybersecurity
- http://www.infosecnews.org/
- http://www.infosecurity-magazine.com/
- http://www.inforisktoday.eu/
- http://threatpost.com/
- http://www.trendmicro.com/vinfo/us/security/news/
- http://www.wired.com/security/

Potential Topics/Stories

1. ~~Security Trends of 2016~~ **Team 7 (M. Maithani, K. Patel, N. Modgil)**

http://www.welivesecurity.com/wp-content/uploads/2016/01/eset-trends-2016-insecurity-everywhere.pdf
https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf
https://www.proofpoint.com/sites/default/files/human-factor-report-2016.pdf

2. ~~Cybercrime as a Service~~ **Team 15 (Y. Zheng, P. Thayer, A. Chaudhry)**

https://www.rsa.com/content/dam/rsa/PDF/2016/05/2016-current-state-of-cybercrime.pdf
http://documents.trendmicro.com/assets/guides/executive-brief-exploits-as-a-service.pdf
http://documents.trendmicro.com/assets/resources/ransomware-as-a-service.pdf

3. ~~Ransomware Evolution and Current Landscape~~ **– Team 19 (A. Kim, E. Lin, Q. Chen)**

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf
http://integranetworks.com/wp-content/uploads/2016/07/Integra-Networks-Ransomware-White-Paper.pdf
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/iSight-Ransomware-Threat-Landscape-Overview.pdf
https://www.sans.org/reading-room/whitepapers/incident/enterprise-survival-guide-ransomware-attacks-36962

4. ~~Locky Ransomware~~ **Team 16 (J. Cardona, A. Mule, M. Sawicki)**

https://nakedsecurity.sophos.com/2016/02/17/locky-ransomware-what-you-need-to-know/
https://www.infrascale.com/wp-content/uploads/pdf/Infrascale-Un-Locky-for-Business-eBook.pdf
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf

https://www.proofpoint.com/us/threat-insight/post/Locky-Ransomware-Cybercriminals-Introduce-New-RockLoader-Malware

5. ~~DDoS Trends~~ Team 3 (R. Truong, M. Mierzwa, S. J. Bae)

http://www.digitalattackmap.com/
https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q3-2016-state-of-the-internet-security-executive-summary.pdf
https://securelist.com/analysis/quarterly-malware-reports/76464/kaspersky-ddos-intelligence-report-for-q3-2016/
https://www.verisign.com/en_GB/security-services/ddos-protection/ddos-report/index.xhtml?loc=en_GB

6. ~~IoT Security~~ Team 17 (Z. Matthews, M. El Masri, N. Jaramillo)

https://www.verizon.com/about/sites/default/files/state-of-the-internet-of-things-market-report-2016.pdf
https://www.pubnub.com/blog/2015-05-04-10-challenges-securing-iot-communications-iot-security/
https://www.capgemini-consulting.com/resource-file-access/resource/pdf/securing_the_internet_of_things.pdf
https://www.w3.org/Talks/2016/0614-iot-security.pdf

7. ~~Mirai IoT Botnet~~ Team 20 (I. Manjra, M. Farhad, V. Milovanovic)

https://www.malwaretech.com/2016/10/mapping-mirai-a-botnet-case-study.html
http://heavy.com/tech/2016/10/mirai-iot-botnet-internet-of-things-ddos-attacks-internet-outage-blackout-why-is-internet-down/
https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html
https://www.us-cert.gov/ncas/alerts/TA16-288A

8. ~~ATM Skimming~~ Team 8 (Y. Huang, J. Hou, C. Wang)

https://usa.visa.com/content/dam/VCOM/download/merchants/final-skimming-webinar-041316.pdf
https://krebsonsecurity.com/2016/11/atm-insert-skimmers-a-closer-look/
http://www.securetransportassociation.org/files/resources/ATM_Skimming_Detection_and_Deterrence_Guide.pdf

9. ~~Fraud in Digital Advertising~~ Team 2 (S. Azari, S. Kalantari, O. Amini)

https://www.comscore.com/ger/content/download/35195/1931455/version/1/file/JAR-+JUN2016+Fraud+in+Digital+Advertising.pdf
http://cdn2.hubspot.net/hubfs/418991/Digital_Ad_Fraud.pdf?t=1436331135031
http://www.wfanet.org/pdf/WFA_Compendium_Of_Ad_Fraud_Knowledge.pdf
https://techcrunch.com/2016/01/06/the-8-2-billion-adtech-fraud-problem-that-everyone-is-ignoring/

10. ~~DNSChanger Attack (and Its Use of Steganography)~~ Team 14 (E. Lamb, H. Trivedi, D. Bickram)

http://arstechnica.com/security/2016/12/home-routers-under-attack-in-ongoing-malvertisement-blitz/
https://www.proofpoint.com/us/threat-insight/post/home-routers-under-attack-malvertising-windows-android-devices
http://thehackernews.com/2016/12/dnschanger-router-malware.html
https://www.bleepingcomputer.com/news/security/steganography-is-very-popular-with-exploit-kits-all-of-a-sudden/

11. ~~KillDisk (and Its Use in Hacks on Ukrainian Power Grid)~~ Team 12 (A. Shahrami, R. Abou-Nassar, M. Morsi)

https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
http://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/
http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

12. ~~USB Drop & USB Kill Attack~~ Team 3 (P. Y. Ng, J. Y. Ou, W. Yao)

http://www.pcmag.com/news/346755/hey-dummy-drop-that-usb-drive
https://zakird.com/papers/usb.pdf
http://www.computerworld.com/article/3118344/computer-hardware/this-usb-thumb-drive-will-fry-your-unsecured-computer.html
http://www.techworm.net/2016/09/usb-kill-2-0-sale-destroys-device-plugged.html#prettyPhoto

13. ~~Security and Privacy of Wearable Devices~~ Team 11 (J. Loja, S. S. Virk, S. W. Chow)

http://aircconline.com/ijnsa/V8N3/8316ijnsa02.pdf
https://www.priv.gc.ca/media/1799/wc_201401_e.pdf
http://www.uknow.com/wp-content/uploads/2014/03/Location-Services_White_Paper.pdf
https://www.symantec.com/content/dam/symantec/docs/white-papers/how-safe-is-your-quantified-self-en.pdf
https://www.democraticmedia.org/sites/default/files/field/public/2016/aucdd_wearablesreport_final121516.pdf

14. ~~Deep and Dark Web~~ Team 4 (A. Aolaritei, D. Nowak, R. Agyapong)

https://www.sans.org/reading-room/whitepapers/covert/ocean-internet-deep-web-37012
https://media.scmagazine.com/documents/224/deeplight_(1)_55856.pdf
https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf
http://www.batblue.com/the-darknet/

15. ~~Bitcoin: Who Invented It and How It Works~~ Team 1 (M. Tsymbal, M. Abuasab, C. Reyes)

http://www.sciencealert.com/bitcoin-was-the-best-performing-currency-of-2016
https://bitcoin.org/bitcoin.pdf
http://scitechconnect.elsevier.com/wp-content/uploads/2016/07/Introduction-to-Bitcoin.pdf
http://bravenewcoin.com/assets/Reference-Papers/A-Gentle-Introduction/A-Gentle-Introduction-To-Bitcoin-WEB.pdf
http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf

16. ~~Social Media Security and Privacy~~ Team 10 (D. N. Xuan, H. Singh, M. Asad)

https://www.russharvey.bc.ca/resources/socialmedia.html
http://www.sciencedirect.com/science/article/pii/S1877050916000211
https://www.bluecoat.com/en-gb/company/press-releases/blue-coat-social-media-security-report-2016
http://cacm.acm.org/magazines/2016/7/204021-the-rise-of-social-bots/fulltext

17. ~~Medical Devices Security~~ Team 6 (Y. Koren, M. Mujahid, M. K. Chowdhury)

https://ww2.kqed.org/futureofyou/2016/01/25/hacked-medical-devices-still-a-big-threat-in-2016/
http://delivery.acm.org/10.1145/2900000/2890488/p66-burns.pdf?ip=99.227.164.242&id=2890488&acc=OPEN&key=4D4702B0C3E38B35%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35%2E6D218144511F3437&CFID=884641113&CFTOKEN=58922946&__acm__=1483501139_cc2804430678fec4572c9b2d4a5d6c22

http://www.wise-intern.org/journal/2016/documents/Jen_Madary_Paper.pdf
https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/co-hc-5-the-time-to-address-medical-device-cybersecurity-is-now.pdf

18. ~~Automotive Cybersecurity~~ Team 13 (J. L. Tran, P. Jiang, T. Mahmood)

http://www.mcafee.com/ca/resources/white-papers/wp-automotive-security.pdf
http://www.gao.gov/assets/680/676064.pdf
http://www.pcmag.com/news/346795/car-hackers-return-to-black-hat-with-new-attacks-to-drive-yo

19. ~~Mobile Device Security~~ Team 9 (A. Martinenco, M. Averbach, N. Ahmed)

http://www.crowdresearchpartners.com/wp-content/uploads/2016/03/BYOD-and-Mobile-Security-Report-2016.pdf
http://resources.alcatel-lucent.com/asset/200492
http://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2016.pdf

20. ~~Cloud Security~~ Team 18 (D. Fan, W. Li, Y. Huang)

https://media.scmagazine.com/documents/114/cloud-security-spotlight-repor_28381.pdf
https://thesai.org/Downloads/Volume7No4/Paper_64-Data_Security_Privacy_Availability_and_Integrity.pdf
https://www.ipc.on.ca/wp-content/uploads/2016/08/Thinking-About-Clouds-1.pdf