Cyberattacks Crime and Defenses

Schema, Dates, Literature

Year 2020, version 1.0

The video lectures of last year are available at https://intranet.tue.nl/onderwijs/videocollege-tue/ (look for 2IMS20), or via the direct link: https://videocollege.tue.nl/Mediasite/Showcase/e67b8e0ccb0b42b5b737321255bb30cf44/Channel/4c3464c80f1341be98c185d4b596cf744d

This year, due to the COVID restrictions, we need to refer partly to the lectures given last year. We have set up an MS TEAMS group. Check CANVAS notification for the code to join the group. Also, we have two kind of lectures.

- UNCHANGED: each of the "unchanged" lectures is identical to one of the lectures given last year (the one reported in the list). Students are supposed to watch the corresponding video lecture on videocollege.tue.nl *before* the lecture slot. The lecture slot will be used for Q&A sessions with the lecturer, which will be held using MS TEAMS. You

- NEW: these lectures have new slides and a presentation is going to be through MS TEAMS. This presentation will be recorded.

- The exception is the first lecture: which will be a combination of NEW (the announcements) and an UNCHANGED lecture.

Questions will be answered during the TEAMS meetings and **not** via email unless there are particularly good reasons for doing so.

TENTATIVE CALENDAR. NOTE: Tuesday lectures – the ones with an uneven number – are from 13:30 till 15:45; Thursday lectures are from 8:45 till 10:45

1. 10/11 [SANDRO] **please join this lecture on MS teams, because we are going to explain how things will work this year, and make some announcements. The rest of the lecture is UNCHANGED wrt last year, namely:** Quick Recap of web application security (part 1). HTTP weaknesses, sessions, cookies. [UNCHANGED: video lecture 2019/2020: Lecture 1a and 1b]

    a. Vide lectures (from 2019/2020) 1a and 1 b (referring to the year 2019/2020)

    b. Slides: CCD20_Etalle01_webapps_and_attack_principles.pptx (exactly)

2. 12/11 [SANDRO] Recap of Web Attack techniques and Structure of a Targeted attack (part 1) [UNCHANGED: video lecture 2019/2020: Lecture 2a and 2b]

    a. Recap of Web attack techniques: XSS, SQL injections, Path traversals, DDOS, Browser exploitation Frameworks.

        i. slides CCD20_Etalle02a_SQLINJ_XSS_etc.pptx

    b. Structure of a targeted attack. Intelligence gathering, drive-by-exploit, watering hole, phishing, kill chain, living-off-the-lands.

i. slides CCD20_Etalle02b_targeted_attacks.pptx (till page 29)

3. 17/11 [SANDRO] Case study disruptive targeted attacks (1): Stuxnet, Ukraine 2015 and 2016. [UNCHANGED: video lecture 2019/2020: Lecture 3a and 3b]

    a. slides

        i. CCD20_Etalle02b_targeted_attacks.pptx (from page 29 till the end at minute 25 of lecture 03a)

        ii. CCD20_Etalle03_advanced_attacks_critical_infrastructure.pptx (till slide 34)

    b. The Real Story of Stuxnet, Posted 26 Feb 2013, by DAVID KUSHNER https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

    c. W32.Stuxnet Dossier. By Symantec. Read only: Executive Summary, https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

    d. T. Conway, R. M. Lee, M. J. Assante. Analysis of the cyber attack on the Ukrainian power grid. SANS ICS, 2016. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

4. 19/11 [SANDRO] Cases study IT attacks (2). Equifax, Target breach, the Hacking Team, booters; recent evolution of non-targeted attacks, ransomware, supply chain attacks.] [UNCHANGED: Video lectures 4a and 4b (from 2019/2020)]

    a. slides

        i. CCD20_Etalle03_advanced_attacks_critical_infrastructure.pptx (, finishing the lecture before, from slide 34)

        ii. CCD20_Etalle04a_case_study_IT_attacks.pptx (lecture a till slide 13 -- finished with lecture B)

    b. Background material

        i. Bruce Schneier on the Equifax Hack https://www.schneier.com/crypto-gram/archives/2017/1115.html

        ii. https://www.csoonline.com/article/3212260/ransomware/the-5-biggest-ransomware-attacks-of-the-last-5-years.html

        iii. https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know- now.html

        iv. http://pastebin.com/raw/0SNSvyjJ (The Hacking Team Hack)

        v. Stress Testing the Booters: Understanding and Undermining the Business of DDoS Services, by Mohammad Karami, Youngsam Park, Damon McCoy, 2015 https://arxiv.org/pdf/1508.03410v1.pdf

5. 24/11 [GUEST LECTURE BY Elisa Costante, FORESCOUT (ex SECURITYMATTERS)] [UNCHANGED: video lecture 2019/2020: Lecture 9a, which lasts 1h30] Lecture on Building Automation Security

6. 26/11 [SANDRO #5] [**NEW**]

    a. [**NEW**] Evolution of attacks

        i. slides **IN PROGRESS** CCD20_Etalle04b_attacks_evolution.pptx,

        ii. [literature: see the slides]

7. 1/12 [Part a is **NEW**, part b is UNCHANGED]

    a. [GUEST LECTURE BY SECURA] PROTECTING CROWN JEWELS: RED TEAMING IN OT [**NEW**]

    b. [UNCHANGED] IoT and Detection Part 1

        i. video lecture 2019/2020: Lecture 5b

        ii. slides: CCD20_Etalle05_CCD_iot_detection_v03.pptx (this lecture goes until slide 23, the rest is handled in the next one)

8. 3/12 [SANDRO #6] [UNCHANGED: video lecture 2019/2020: Lecture 8a and 8b]

    a. IoT and Detection: Finished the slides of last time

    b. Monitorability (Video lecture Lecture 8a (end) and 8b (first 30 minutes, more or less))

        i. Slides: CCD20_Etalle06_monitorability_v01.pptx

        ii. Paper: From Intrusion Detection to Software Design. (by S. Etalle) https://www.win.tue.nl/~setalle/2017_etalle_esorics_supervisable.pdf

9. 8/12 [SANDRO]. Defensive Policies - What works and what doesn't. [UNCHANGED: Video lecture 10a **only from minute 16 on** (the first 16 minutes are the explanation of last year exercise), Video lecture 10b: all]

    a. Slides: CCD20_Etalle07_Defensive_Policies_v03.pptx (until slide 44)

    b. Study material

        i. **Encryption in ICS networks: a blessing or a curse?** https://research.tue.nl/en/publications/encryption-in-ics-networks-a-blessing-or-a-curse

        ii. **So Long, And No Thanks for the Externalities**: The Rational Rejection of Security Advice by Users, by Cormac Herley. https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/SoLongAndNoThanks.pdf

iii. **Where Do All The Attacks Go?** By Dinei Florencio and Cormac Herley. Not the mathematics, only the principles. Available at: http://www.econinfosec.org/archive/weis2011/papers/Where%20Do%20All%20the%20Attacks%20Go.pdf]

10. 10/12 [GUEST LECTURE BY YURI BOBBERT][NEW]

    a. Paper: Yuri Bobbert& Jeroen Scheerder: On the Design and Engineering of a Zero Trust Security Artefact. To appear. Available in the slides directory.

11. 15/12 [LUCA, MARTIN, MICHELE] [NEW: LABORATORY]

12. 17/12 [LUCA] [UNCHANGED video lecture 2019/2020: Lecture 6a and 6b]

    a. Cybercrime markets: the ecosystem

        i. (this is only background, does not have to be studied). Europol. Drugs and the darknet. Perspectives for enforcement, reserach, and policy. 2017. Available at: http://www.emcdda.europa.eu/system/files/publications/6585/TD0417834ENN.pdf

    b. Cybercrime markets: malware and exploit commoditization

        i. Van Wegberg, Rolf, et al. "Plug and prey? measuring the commoditization of cybercrime via online anonymous markets." *27th {USENIX} Security Symposium ({USENIX} Security 18)*. USENIX} Association}, 2018.

13. 5/1 Invited lecture on cybercrime from Rutger Leukfeldt (NSCR). [UNCHANGED: Video Lecture 11a and 11b of the year 2019/2020]

    a. Leukfeldt, Eric Rutger, and Majid Yar. "Applying routine activity theory to cybercrime: A theoretical and empirical analysis." Deviant Behavior 37.3 (2016): 263-280.

    b. Leukfeldt, Rutger, Edward Kleemans, and Wouter Stol. "The Use of Online Crime Markets by Cybercriminal Networks: A View From Within." American Behavioral Scientist 61.11 (2017): 1387-1402.

14. 71 [LUCA] Advanced social engineering [NEW]

15. 12/1 [GUEST LECTURE BY SECURA] PEOPLE ARE NOT THE WEAKEST LINK. OUR UNDERSTANDING OF PEOPLE IS [NEW]

16. 7/1 [LUCA] A brief history of malware evolution. [UNCHANGED: video lecture 12a and 12b of 2019/2020. THIS IS THE LAST LECTURE AND WILL BE USED ALSO FOR A “BROADER” Q&A]

    a. Slides

    b. Grier, Chris, et al. "Manufacturing compromise: the emergence of exploit-as-a-service." *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 2012.

c. Hutchings, Alice, and Richard Clayton. "Exploring the provision of online booter services." *Deviant Behavior* 37.10 (2016): 1163-1178.

Literature that would be nice to discuss.

NEW STUFF TO BE LOOKED AT

- Blocki, Jeremiah, Ben Harsha, and Samson Zhou. "On the economics of offline password cracking." *IEEE Secur. Priv.(2018, to appear)* (2018).
- Europol. Drugs and the darknet. Perspectives for enforcement, reserach, and policy. 2017. Available at: http://www.emcdda.europa.eu/system/files/publications/6585/TD0417834ENN.pdf
- Van Wegberg, Rolf, et al. "Plug and prey? measuring the commoditization of cybercrime via online anonymous markets." *27th {USENIX} Security Symposium ({USENIX} Security 18)*. USENIX} Association}, 2018.
- Hutchings, Alice, and Richard Clayton. "Exploring the provision of online booter services." *Deviant Behavior* 37.10 (2016): 1163-1178.
- Pastrana, Sergio, et al. "Characterizing Eve: Analysing Cybercrime Actors in a Large Underground Forum." *International Symposium on Research in Attacks, Intrusions, and Defenses*. Springer, Cham, 2018.
- Le Blond, Stevens, et al. "A Look at Targeted Attacks Through the Lense of an NGO." *USENIX Security Symposium*. 2014.
- Sheng, Steve, et al. "Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions." *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2010.
- Leukfeldt, Eric Rutger, and Majid Yar. "Applying routine activity theory to cybercrime: A theoretical and empirical analysis." Deviant Behavior 37.3 (2016): 263-280.
- Leukfeldt, Rutger, Edward Kleemans, and Wouter Stol. "The Use of Online Crime Markets by Cybercriminal Networks: A View From Within." American Behavioral Scientist 61.11 (2017): 1387-1402.
- Zero Days, Thousands of Nights - rand.org, by Lillian Ablon, Andy Bogart. RAND corporation, 2017. Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1751/RAND_RR1751.pdf
- Markets for Cybercrime Tools and Stolen Data, by Lillian Ablon, Martin C. Libicki, Andrea A. Golay. RAND Corporation, 2014. Availabe at www.rand.org
- Framing Dependencies Introduced by Underground Commoditization, by Kurt Thomas, Danny Huang, David Wang, Elie Bursztein, Chris Grier, Thomas J. Holt, Christopher Kruegel, Damon McCoy, Stefan Savage, Giovanni Vigna. Available at https://research.google.com/pubs/pub43798.html

- Branch, Federal Network Resilience Cybersecurity Assurance. Unintentional Insider Threats: Social Engineering. (2014). Only the sections: 3, 5, 6.1, 6.2, 6.3 Available at https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_77459.pdf

- Luca Allodi, Marco Corradin, Fabio Massacci. Then and Now: On the Maturity of the Cybercrime Markets. The lesson black-hat marketeers learned. IEEE Transactions on Emerging Topics in Computing, 4(1):35-46, Jan 2016. https://www.win.tue.nl/~lallodi/allodi-tetcs-15.pdf

- M. Karami, Y. Park, D. McCoy Stress Testing the Booters: Understanding and Undermining the Business of DDoS Services, WWW '16 Proceedings of the 25th International Conference on World Wide Web. Pages 1033-1043 (for the assignments)

- Michel van Eeten Katsunari Yoshioka Daisuke Makita Carlos Hernandez Gañan Maciej Korczyński Arman Noroozian. Who Gets the Boot? Analyzing Victimization by DDoS-as-a-Service. Proceedings RAID 2016. (for the assignments) available at http://mkorczynski.com/RAID16Noroozian.pdf

- Who is Anna-Senpai, the Mirai Worm Author. Blog Krebs on Security. https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/comment-page-5/#comments

Perhaps

- Workman, Michael. Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. Journal of the Association for Information Science and Technology 59.4 (2008): 662-674. Available at https://www.semanticscholar.org/paper/Wisecrackers-A-theory-grounded-investigation-of-ph-Workman/6b4dcbc51e891aa7a79b054dcf518d3f5f293572 or https://pdfs.semanticscholar.org/6b4d/cbc51e891aa7a79b054dcf518d3f5f293572.pdf (or similar address, look for it on the internet, possibly from the TU/e network).

- Investigation Report for the September 2014 Equation malware detection incident in the US, available at https://securelist.com/investigation-report-for-the-september-2014-equation-malware-detection-incident-in-the-us/83210/

- https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/: article that describes a safety-related automotive attack on a Jeep by Miller and Valasek

- https://www.escrypt.com/sites/default/files/documents/Ransomware-against-cars.pdf: article that describes ransoomware that is targeting in-vehicle environments by Escrypt