Human Centered Cybersecurity

Wednesdays [Every day is like Sunday…]
Dr. Filipo Sharevski fsharevs@cdm.depaul.edu
Discord Channel https://discord.gg/uZvw3ab

Application of behavioral theories in cybersecurity context. Topics include economic theories of decision making, heuristics, biases, and bounded rationality, signal detection theory, mental models, social engineering, game theory, information search, and cognitive engineering. Students work on an individual project applying one of these theories to a practical cybersecurity scenario of their choice. There are no required textbooks for this course. Although, I am happy to recommend many interesting texts outside of the assignments. All the readings are uploaded in D2L.

Assignments

This is the tentative schedule for the class:

W	Module	Assignment
1	Economic theories in cybersecurity decision making	Homework 1 / Simulation 1
2	Heuristics and biases in cybersecurity decision making	Homework 2
3	Bounded rationality in cybersecurity decision making	Homework 3
4	Signal detection theory in cybersecurity settings	Homework 4 / Simulation 2
5	User mental models of cybersecurity threats	Homework 5
6	Social engineering	Homework 6
7	Game theory and exploitation	Homework 7 / Simulation 3
8	Information search in cybersecurity settings	Homework 8
9	Cognitive engineering	Homework 9
10	Project presentations	

The weights of each assignment for contributing to the final average are as follows:

Assignment	Weight in final grade
Homework / Simulation	(8 + 8 + 10) 26%
Only Homework	24%
Discussion Participation	10%
Project	40%

Assignments are due a week after each is assigned at 11:59 PM. NO late assignments will be accepted. Bargaining for grades is not allowed and is considered academic dishonesty.

Grading

Grading is based on a percentage basis, which is then convert to a letter as:

Percentage	Grade	Percentage	Grade	Percentage	Grade
100-92	A	91-90	A-		
87-82	B	81-80	B-	89-98	B+
77-72	C	71-70	C-	79-78	C+
67-62	D	61-60	D-	69-68	D+
				59-0	F

Project/Presentation

Mid quarter, you have to choose a topic of interest and conduct a substantive resaerch that shall result into a final paper and presentation. In the week of finals, you will present your paper. Make a presentaion and voice over it. Or any type of recorded presentation will do. For your paper to be graded and included in your final grade, you HAVE to deleiver a presentaiton.

Week-by-week schedule

Week 1: Economic theories of cybersecurity decision making

This module provides the foundation for later exploration of decisions in cybersecurity, including a survey of decision theory, a summary of relevant economic concepts, and a review of cybersecurity concepts. It also introduces a list of who the people are in human-centered cybersecurity.

Readings:

- Bauer, J.M., & van Eeten, M.J.G. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy 33, 706-719.*
- Anderson, R., & Moore, T. (2006). The economics of information security. *Science 314,* 610-613. DOI: 10.1126/science.1130992

Week 2: Heuristics and biases in cybersecurity decision making

This module is an overview of systematic violations of rationality in human decision making, specifically based on heuristic reasoning. The heuristics and biases framework explain these systematic violations of rational decision- making based on the limited resources available to human decision-makers.

Readings:

- Pfleeger, S.L., & Caputo, D. (2012). Leveraging behavioral science to mitigate cyber security risk. Computers & Security 31, 597-611. doi:10.1016/j.cose.2011.12.010
- Rosoff, H., Cui, J., & John, R.S. (2013). Heuristics and biases in cyber security dilemmas. Environment Systems and Decisions 33(4), 517-529.

Week 3: Bounded rationality in cybersecurity decision making

This module is a general overview of bounded rationality, which is the notion that humans adapt both to their external environment and to their internal information processing limits. The module proposes several mechanisms for this adaptation and applies those mechanisms to specific situations in cybersecurity.

Readings:

- Gigerenzer, G., & Goldstein, D.G. (1996). Reasoning the fast and frugal way: Models of bounded rationality. Psychological Review 103(4), 650-669.
- Pieters, Wolter. 2019. "On Security Singularities." In Proceedings of the 2018 Workshop on New Security Paradigms.

Week 4: Signal detection theory in cybersecurity settings

Signal detection theory describes the tradeoffs in trying to detect particular signals in noisy environments – what causes people or systems to "cry wolf" or to under-report violations.

Readings:

- Werlinger, R., Muldner, K., Hawkey, K., & Beznosov, K. (2010). Preparation, detection, and analysis: The diagnostic work of IT security incident response. Information Management & Computer Security 18(1), 26-42. DOI 10.1108/09685221011035241
- Sawyer, B.D., Finomore, V.S., Funke, G.J., Mancuso, V.F., Funke, M.E., Matthews, G., & Warm, J.S. (2014). Cyber vigilance: Effects of signal probability and event rate. Proceedings of the Human Factors and Ergonomics Society 58th Annual Meeting, 1771-1775.

Week 5: User mental models of cybersecurity threats

End users and professionals have internal ideas of what the main threats to cybersecurity are that they should protect against. For instance, users who think of a computer network as analogous to an organism may think to protect against contagious threats that come in from outside but may not think to protect against data exfiltration from inside.

Readings:

- Volkamer, M., & Renaud, K. (2013). Mental models: General introduction and review of their application to human-centred security. Number Theory and Cryptography: Lecture Notes in Computer Science 8260, 255-280.

- Padamos, Arne. 2019. “Against Mindset.” In Proceedings of the 2018 Workshop on New Security Paradigms (forthcoming).

Week 6: Social engineering

A large proportion of successful attacks on networks involve some degree of compromise of human systems rather than technological systems. This type of attack may include anything from a flash drive left in a parking lot to the creation of a fake help line for technical support.

Readings:

- Yang, W., Xiong, A., Chen, J., Proctor, R.W., Li, N. (2017, April). Use of phishing training to improve security warning compliance: Evidence from a field experiment. HoTSoS 2017, April 4-5, 2017, Hanover, MD, USA. doi: 10.1145/3055305.3055310
- Levine, Timothy R. 2014. “Truth-Default Theory (TDT): A Theory of Human Deception and Deception Detection.” Journal of Language and Social Psychology 33 (4): 378–92. doi:10.1177/0261927X14535916.

Week 7: Game theory and exploitation

The interplay of attack and defense can be considered using a game theoretic framework in which malicious actors and network defenders are playing against each other for particular gains and to avoid particular losses.

Readings:

- Maqbool, Z., Makhijani, N., Pammi, V. C., & Dutt, V. (2017). Effects of motivation: rewarding hackers for undetected attacks cause analysts to perform poorly. Human factors, 59(3), 420-431.
- Sinha, A., Fang, F., An, B., Kiekintveld, C., & Tambe, M. (2018). Stackelberg Security Games: Looking Beyond a Decade of Success. In IJCAI (pp. 5494-5501).

Week 8: Information search in cybersecurity settings

Analysts in cybersecurity must search for information within logs and documentation. In this module, we will look at theories of information search and how optimizing information search can be applied in cybersecurity analysis.

Readings:

- Pirolli, P., & Card, S. (1995). Information foraging in information access environments. CHI '95, 51-58.
- Dalton, A, B Dorr, L Liang, and K Hollingshead. 2017. “Improving Cyber-Attack Predictions through Information Foraging.” In 2017 IEEE International Conference on Big Data (Big Data), 4642–47. doi:10.1109/BigData.2017.8258509.

Week 9: Cognitive Engineering

Cybersecurity professionals are an invaluable part of cybersecurity protection systems. Optimizing their performance is a necessary part of securing a network. This module covers some of the ways that software can support or not support cybersecurity performance.

Readings:

- Paul, C.L., & Whitley, K. (2013). A taxonomy of cyber awareness questions for the user- centered design of cyber situation awareness. In L. Marinos and I. Askoxylakis (Eds.): HAS/HCII 2013, LNCS 8030, 145-154. Heidelberg: Springer-Verlag.
- Dutt, V., Ahn, Y.S., & Gonzalez, C. (2013). Cyber situation awareness: Modeling detection of cyberattacks with instance-based learning theory. Human Factors 55(3), 605-618. DOI: 10.1177/0018720812464045

Week 10: Final Project presentation

Students will present their final projects and solicit peer review comments, critiques, and suggestions.

Other Important Information

Attendance: I expect you will attend (watch the recording of) every class.

Class Cancelation: Unless DePaul closes because of weather, we will have class.

Academic Integrity: I expect that you have read and understood DePaul's Academic Integrity policy: http://academicintegrity.depaul.edu/ .

Changes to Syllabus: I reserve the right to change the syllabus and you will be timely informed of such changes. I don't expect significant deviations of the course agenda.

Academic Policies:
http://www.cdm.depaul.edu/Current%20Students/Pages/PoliciesandProcedures.aspx

Students with disabilities: Contact the instructor or the Center for Students with Disabilities (CSD) at: csd@depaul.edu prior to the class start.

Preferred Name & Gender Pronouns: I will gladly honor your request to address you by an alternate name or gender pronoun: http://policies.depaul.edu/policy/policy.aspx?pid=332

Online Teaching Evaluation (OTE): Please evaluate the course in CampusConnect when you receive a notification towards the end of the quarter.