UNITED STATES NAVAL ACADEMY
SY304: Human Factors in Cyber Operations
Spring Semester AY2020

Professor: LCDR Joseph M. Hatfield, Ph.D.
Office: Leahy Hall Rm. 101
Email: hatfield@usna.edu
Office Hours: Open-door policy, but students are encouraged to schedule an appointment (arrange by email)

Course Description:

This course will examine human factors in cyber operations. It is a reading and writing intensive course that focuses on human behavior and human choices as these relate to the success of operations in cyberspace—be they offensive, defensive, or inquisitive. The course includes interactive labs, including a lock picking lab, in-class group work, and two technical labs using the Social Engineering Toolkit (SET), an open source tool specifically designed to perform advanced attacks against the human element. The course is interdisciplinary in nature, drawing its content from scholarly work in technical fields (e.g. computer science, information technology, engineering) the social sciences (e.g. psychology, anthropology, political science, law) and the humanities (e.g. history, ethics, philosophy). Scholars and practitioners who limit their focus purely to technical factors have an incomplete understanding of the cyber domain, just as inadequate technical exposure leads to misunderstandings of the opposite kind.

Successful cyber operations require the integration of both technical and human factors. Technical factors include the theory and design of computers and network architectures, but also the practical employment and exploitation of programs, hardware, communication protocols, cryptographic techniques, firewalls, and so on. Human factors involve *people*—the choices people and groups make, the behaviors they habituate, which influence the success of cyber operations. Human decisions can render a technically secure network insecure, and, in fact, do so quite regularly. Humans can be tricked, manipulated, and influenced to an attacker's advantage. Similarly, they can be trained to recognize human-focused attacks and somewhat mitigate that risk through proper countermeasures. Management policies—another form of human decision making—can limit the scope of human choices within an organization, thereby bettering or worsening an organization's vulnerability to attack. Human behavior is also influenced by ethical, legal, and normative constraints which can be exploited by an attacker, buttressed by a defender, and discovered by inquisitive collectors.

In total, human factors are at least as relevant to the successful attack or defense of computer networks as technical factors. With the advent of powerful security tools—security-focused operating systems, end to end encryption, and anonymizing browsers—human factors have arguably become even more important to network security than technical factors. For this reason, some observers refer to human-focused cyber-attacks as "the highest form of hacking."

While other courses within the cyber operations major emphasize cyber-attacks against (and by) nation-states, SY304 takes banks, manufacturing companies, healthcare providers, local governments, and similar small to medium-sized organizations as its primary context. The vast majority of cyber-attacks are conducted by criminals seeking monetary enrichment targeting such medium-sized entities. Studying human factors first within this setting helps students learn the principles behind these techniques without having to simultaneously learn the principles and motivations that lie behind policy choices in the broader context of international politics.

As a student in this class, you will learn concepts and gain experience with techniques that could be used unethically or illegally. DO NOT use knowledge or experience gained for such purposes. You MAY NOT use tools and techniques learned in this class to violate USNA policy (or any other government restrictions) on information system use. Your conduct MAY NOT run counter to the Human Research Protection Program (HRPP) Procedure Manual: https://www.usna.edu/HRPP/proceduremanual.php.

Course Learning Outcomes:

1. Understanding the relationship between human and technical factors within the context of cyber operations.

2. Gain a comprehensive understanding of the techniques involved in targeting human beings (e.g. social engineering) as well as defending against such targeting in cyber operations.

3. Reasoning through the ethical, legal, and normative aspects of human-centered cyber operations.

4. Exposure to important academic research on human factors in cyber operations drawn from technical disciplines, the social sciences, and the humanities.

5. Demonstrate effective written and oral communication skills.

ABET Key Performance Indicators (KPI's) addressed by this course include verbal communication, written communication, the use of visuals, legal principles, ethical principles, make judgments, team dynamics, human security, environmental security, confidentiality, integrity, availability, risk, adversarial thinking, offensive cyber operations, and defensive cyber operations.

Course Materials:

There currently exists no academically rigorous English-language textbook on human factors in cyber operations. This is a shame since textbooks nicely summarize and make intelligible to undergraduate audiences peer-reviewed scholarly research. Absent such a text, courses on human factors must choose between two pedagogical strategies. The first approach makes non-academic material (e.g. magazine and newspaper articles, technical blogs, popular books) the basis of the course, with instructor lectures and expertise supplementing this content to add academic rigor. The second approach brings primary academic sources directly to the students, with instructor lectures and classroom activities helping to explain the significance of the research to students. Until a proper textbook is written, the department's Accreditation Board for Engineering and Technology (ABET) standing requires that we take the latter approach to ensure scholarly rigor.

Therefore, academic journal articles and conference proceedings comprise the core readings for this course. These articles have been chosen from a variety of journals in computer science, information technology, computer engineering, psychology, anthropology, political science, history, law, and philosophy. Selected articles act as representatives of a class of research on the topic they cover. They function as starting points for in-class discussions. In a number of cases, older but lucidly written articles were preferred over articles that were newer but less cogently expressed. These are all available online through your Nimitz Library login, through inter-library loan, or are available to the public generally. They are also available on the course Blackboard site.

In the course schedule below, readings are separated into two categories: "Required" and "Recommended." *Required* readings are those that students must read carefully (and be able to discuss in

detail) before coming to class. *Recommended* readings are supplemental in nature and students are not expected to have read these. However, those wishing to gain additional insight on a particular topic should consider doing so. Also, students writing papers on questions that align with primary readings should strongly consider reading these recommended sources and using their bibliographies.

Note: In the digital age, it has become alarmingly common for highly sensitive information to become widely available—through Wikileaks and other avenues—even as their content remains classified. Please note that this information does remain classified and shall be treated as such by all students possessing a security clearance. Such students are bound by signed non-disclosure agreements which prevent them from accessing or further disseminating leaked material.

Evaluation:

Grade Calculations:	Six Week	Twelve Week	Final Grade
6wk Exam	50%	25%	10%
12wk Exam	-	25%	10%
Final Exam	-	-	20%
Participation	10%	10%	10%
Pop-Quizzes	40%	40%	20%
Attack Plan	-	-	15%
Essay	-	-	15%
Total	100%	100%	100%*

***Normal grade rounding applies (e.g. 89.4% = B; 89.5% = A)**

Exams [40% of course grade]. There will be a six and twelve week exam, covering only the material specific to that teaching period, and a comprehensive final exam covering the entire course. These will each consist of multiple choice, fill in the blank, and essay questions.

Classroom Participation [10% of course grade]. Class participation is required to succeed in this course. Outstanding participants provide frequent, relevant, and informed commentary. Respectful debate is highly encouraged throughout the course. Students are expected to display proper classroom decorum, including paying attention, taking diligent notes, and staying awake at all times. Labs and group work factor into your classroom participation grade. *The use of laptops during class is prohibited except during labs (where they are required) or following instructor approval.* Why? A growing body of research evidence indicates that laptops distract from learning, both for users and for those around them, that students who use laptops tend to get poorer grades than those that do not, and that laptop lecture notes are generally less helpful than those taken by hand.[1]

Pop-Quizzes [20% of course grade]. You will be given short surprise quizzes throughout the course to test whether you have done the readings for the class period. If you have taken notes in a traditional notebook, you may use the notebook during the quiz. Access to other forms of notetaking (e.g. computer, margin of printed essay) will not be allowed during quizzes.

[1] Sana, Faria, Tina Weston, and Nicholas J. Cepeda. 2013. "Laptop Multitasking Hinders Classroom Learning for Both Users and Nearby Peers." *Computers & Education*, Vol. 62, pp. 24-31. Mueller, Pam A., and Daniel M. Oppenheimer. 2014. "The Pen is Mightier than the Keyboard: Advantages of Longhand over Laptop Note Taking." *Psychological Science* 25(6): 1-10. Carter, Susan Payne, Kyle Greenberg, and Michael S. Walker. 2017. "The Impact of Computer Usage on Academic Performance: Evidence from a Randomized Trial at the United States Military Academy." *Economics of Education Review*, Vol. 56, pp. 118-132.

Attack Plan [15% of course grade]. During the course you will be put into groups and asked to perform passive reconnaissance of a real cyber target (e.g. company, bank, government office, organization). Your team will then create an attack plan and justify each aspect of your plan using human factors-related research. ***Note:*** *SY304 students who are also enrolled in* ***SY306 Web & Databases for Cyber Operations*** *may use this plan as the basis for the technical exploits they will design in SY306 provided that this arrangement has been approved by SY306 instructors.*

Groups must first choose an identity (including a group name and a corresponding goal) and an appropriate target. For example, a bank might be an appropriate target for a student group pretending to be a profit-seeking criminal enterprise. A hacktivist group might choose to target a corporation whose products violate the group's moral principles, etc. Students will then conduct passive reconnaissance against a real cyber target (e.g. company, bank, government office, organization). Passive reconnaissance is legal physical or electronic surveillance that does not alert the target in any way nor leave a trace that is indicative of potential hostile future actions. Methods that fall into the grey area between passive and active reconnaissance (e.g. port-mapping, network scanning, injection attack exploration, pinging, and onsite impersonation to gain privileged physical access) shall not be undertaken. Reconnaissance should consider vulnerabilities in the target's website, social media profiles (including its employees), and even physical reconnaissance if the target is feasibly available (e.g. in Annapolis). Students are encouraged to use their imaginations to best reconnoiter their targets within the aforementioned guidelines. Following the reconnaissance stage, groups will create a plan of attack that specifies the non-technical and technical methods they propose to utilize to accomplish their goals. Each overall attack plan must include at least two technical and two social engineering-based attack methods. The attack plan will constitute 15% of students' overall course grade and a common grade will be assigned to each group member.

The attack plan culminates in two assignments and a complete grading rubric for the attack plan can be found at the end of this syllabus:

- **Oral presentation:** a 15 minute, visually interesting, verbal presentation will be provided as a group during class time. PowerPoint presentations are not strictly required but may be the best tool with which to convey your team's plan.

- **Written report:** the attack plan will be documented in a written report from each team. The report will be between 5 and 7 pages in length, use Times New Roman 11pt font, and will justify its decisions by citing human factors research using the same *Chicago Manual of Style* author-date in text citation method specified in the syllabus under the "Essay Guidance" section. All other formatting decisions remain up to the group and can take the form of a professional report, an academic paper, or some combination of the two.

Course Essay [15% of course grade]. Write a 2,500 word essay on one of the following questions.
1) What is social engineering and what human factors make people so vulnerable to it? Use examples of at least four social engineering attack types.

2) What role have human factors played in recent cyber operations? Discuss at least two cyber operations from recent history (last 25 years). Discuss offensive and defensive techniques as applicable.

3) Is training and evaluation (including pen-testing) the key to defending against human focused cyber-attacks? If not, why? If so, what kind of training and evaluation is useful and why? Use examples of at least three human focused cyberattacks.

Essay Guidance:

Writing is a fundamental skill that must be developed to be a successful Navy or Marine Corps officer. Your essays should constitute a (1) well-written (2) informed argument (3) with a clear structure that utilizes (4) a proper citation method and (5) one that demonstrates critical thinking. The grading rubric that will be used to evaluate your essays can be found below.

The essays will adhere to the following requirements: 11 point Times New Roman font, 1.5 line-spaced, 1 inch margins on all sides, and include name/section (e.g. MIDN Tom Jefferson/1001) as a header on the top right. Please do not include a cover page. The title of your essay shall be the question it attempts to answer. *Chicago Manual of Style* (in-text author-date system) format will be used and proper citations are required.

Guidance on word count requirements: the essay is to be no more than 2,500 words. A bibliography does not count towards the length requirement, nor does the title. However, the in-text citation does count. For example the sentence – Scholars have put forward sophisticated models of human vulnerabilities (Stajano 2011, 72). – would contribute twelve words to your word count. Anything less than 2,400 is considered short and points will be deducted. The question prompts have sufficient breadth to warrant 2,500 word treatment. At this stage in your academics you should be looking for areas you can cut in order to get down to the maximum, not stretching things artificially in order to get up to the desired word count.

A good essay clearly states its thesis early (even in the first sentence) and telegraphs to the reader the argument's main points which the author will make in order to justify the thesis. It then does what it says; it follows these steps, using academic sourcing to contextualize the author's argument against what others have said. Non-academic sources, such as websites, news articles, and so on, are used only to *supplement*—not replace—proper academic sourcing. Toward the end, typically, good essays will discuss counterarguments that can be made against the thesis, its main points, or any assumptions employed. Good essays don't necessarily have to provide an extensive rebuttal to these, and a simple "it is beyond the scope of this essay to address this objection" will often suffice. Good essays end by providing a summary of the paper's thesis and main points, as well as recommending new questions for further research, as appropriate. There is no cut and dry answer to the question of how many academic sources are required, since this will depend upon how sources are used, the scope of one's argument, and so on. In general, however, SY304 essays with less than six academic sources will be considered *prima facie* to be inadequate.

Please consult the *Chicago Manual of Style* (17th Edition) for the exact way you'll need to do your in-text citation according to the author-date system, bibliographical format, and any other stylistic question. It is available at this Nimitz Library link:
http://www.chicagomanualofstyle.org/book/ed17/frontmatter/toc.html

Assignments shall be submitted (printed copy) at the beginning of class on the due date as well as via email (electronic copy) NLT 1700 that day.

Late Policy: A full letter grade will be reduced for each calendar day an assignment is late. In the event that an assignment's grade falls on a borderline between letters (C/D for example), you should expect late assignments to end up on the lower side of that border. You are future Navy and Marine Corps officers; I have little patience for missed deadlines - unless circumstances are in the extreme (e.g. you're verified as in the hospital, emergency leave, and so on).

Academic Honesty and Plagiarism:
Students are expected to exhibit complete integrity in all of their activities. Academic dishonesty, including plagiarism of any type, may be cause for the initiation of an honor proceeding. Plagiarism is the act of presenting another's words, ideas, or work (or your own previous work)—whether accidentally or deliberately—as your own. This is a form of cheating and an honor violation; it will not be tolerated. You are encouraged to seek clarification if you have questions on citation requirements. *When in doubt, ask!* Students are encouraged to utilize the Nimitz Library resources: http://libguides.usna.edu/plagiarism.

Extra Instruction:
I am always available for extra-instruction – please make an appointment and come prepared. Seek EI early and often! You are also encouraged to seek assistance from your classmates. If you do need EI, please e-mail me to schedule a date/time.

Itinerary

Readings Key:
BB = Blackboard, **URL** = Public Website, **LAB** = Lab Notes (distributed by instructor), **InCl** = In Class discussion/viewing (students not required to read/view prior to class). Required material shall be reviewed by students before the class date listed below.

Class Date	Topic	Readings & Assignments*
9 **Jan**	Course Intro	Course introduction, syllabus review, and discussion about how to read academic research.
14	Introduction to the Study of Human Factors in Cyber Operations	***Required:*** **BB:** Grudin, Jonathan. 2005. "Three Faces of Human-Computer Interaction." *IEEE Annals of the History of Computing* 27(4): 46-62. **BB:** Furnell, S.M., A. Jusoh, and D. Katsabas. 2006. "The Challenges of Understanding and Using Security: A Survey of End-Users." *Computers & Security* 25(1): 27-35. ***Recommended:*** **BB:** Acquisti, Alessandro, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. 2017. "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online." *ACM Computing Surveys* 50(3): 1-41. **BB:** Kraemer, Sara, Pascale Carayon, and John Clem. 2009. "Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities." *Computers & Security* 28(7): 509-520. **BB:** Egelman, Serge, and Eyal Peer. 2015. "Predicting Privacy and Security Attitudes." *ACM SIGCAS Computers and Society* 45(1): 22-28.
16	Introduction to the Study of Human Factors in Cyber Operations (Part 2)	***Required:*** **BB:** Kline, Douglas M., Ling He, and Ulku Yaylacicegi. 2011. "User Perceptions of Security Technologies." *International Journal of Information Security and Privacy* 5(2): 1-12. **BB:** Ashenden, Debi. 2008. "Information Security Management: A Human Challenge?" *Information Security Technical Report* 13(4): 195-201. ***Recommended:*** **BB:** Kraemer, Sara, and Pascale Carayon. 2007. "Human Errors and Violations in Computer and Information Security: The Viewpoint of Network Administrators and

		Security Specialists." *Applied Ergonomics* 38(2): 143-154. **BB:** Komatsu, Ayako, Daisuke Takagi, and Toshihiko Takemura. 2013. "Human Aspects of Information Security: An Empirical Study of Intentional versus Actual Behavior." *Information Management & Computer Security* 21(1): 5-15. **BB:** Sommestad, Teodor, Mathias Ekstedt, Hannes Holm, and Muhammad Afzal. 2011. "Security Mistakes in Information System Deployment Projects." *Information Management & Computer Security* 19(2): 80-94. **BB:** Metalidou, Efthymia, Catherine Marinagi, Panagiotis Trivellas, Niclas Eberhagen, Georgios Giannakopoulos, and Christos Skourlas. 2014. "Human Factor and Information Security in Higher Education." *Journal of Systems and Information Technology* 16(3): 210-221.
21	Social Engineering: History and Definitions	***Required:*** **BB:** Hatfield, Joseph. 2018. "Social Engineering in Cybersecurity: The Evolution of a Concept." *Computers & Security*, Vol. 73, pp. 102-113. **InCl:** "The Secret History of Hacking." Discovery Channel Documentary. Watch in class 0:00-22:00 – pay particular attention to the human side of phone phreaking and how it influenced hacker culture. https://www.youtube.com/watch?v=PUf1d-GuK0Q&t=235s ***Recommended:*** **BB:** Heartfield, Ryan, and George Loukas. 2015. "A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks." *ACM Computing Surveys* 48(3): 1-39. **BB:** Krombholz, Katharina, Heidelinde Hobel, Markus Huber, and Edgar Weippl. 2015. "Social Engineering Attacks on the Knowledge Worker." *Journal of Information Security Applications*, Vol. 22, Issue C, pp. 113-122. **BB:** Kjaerland, Maria. 2006. "A Taxonomy and Comparison of Computer Security Incidents from the Commercial and Government Sectors." *Computers & Security* 25 pp. 522-538.
23	Social Engineering: Psychological Explanations and Pretexting	***Required:*** **BB:** Gragg, David. 2003. "A Multi-Level Defense Against Social Engineering." *SANS Institute InfoSec Reading Room*, pp. 1-21. **BB:** Stajano, Frank, and Paul Wilson. 2011. "Understanding Scam Victims: Seven Principles for Systems Security." *Communications of the ACM* 54(3): 70-75. ***Recommended:*** **BB:** Ormond, Dustin, and Merrill Warkentin. 2015. "Is This A Joke? The Impact of Message Manipulations on Risk Perceptions." *The Journal of Computer Information Systems* 55(2): 9-19. **BB:** Hadlington, Lee. 2017. "Human Factors in Cybersecurity; Examining the Link between Internet Addiction, Impulsivity, Attitudes towards Cybersecurity, and Risky Cybersecurity Behaviours." *Heliyon* 3(7): 1-18. **BB:** Neupane, Ajaya, Nitesh Saxena, Jose Omar Maximo, and Rajesh Kana. 2016. "Neural Markers of Cybersecurity: An fMRI Study of Phishing and Malware Warnings." *IEEE Transactions on Information Forensics and Security* 11(9): 1,970-1,983. **BB:** Fan, Wenjun, Kevin Lwakatare, and Rong Rong. 2017. "Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations." *International Journal of Computer Network and Information Security*, Vol. 2017, Issue 1, pp. 1-11. **BB:** Heartfield, Ryan, George Loukas, and Diane Gan. 2016. "You Are Probably

		Not the Weakest Link: Towards Practical Prediction of Susceptibility to Semantic Social Engineering Attacks." *IEEE Access Journal*, Vol. 4, pp. 6,910-6,928. **BB:** Iuga, Cristian, Jason R. C. Nurse, and Arnau Erola. 2016. "Baiting the Hook: Factors Impacting Susceptibility to Phishing Attacks." *Human-centric Computing and Information Sciences* 6(1): 1-20.
28	Social Engineering: Theoretical Models	***Required:*** **BB:** Mouton, Francois, Louise Leenen, and H. S. Venter. 2016. "Social Engineering Attack Examples, Templates, and Scenarios." *Computers & Security*, Vol. 59, pp. 186-209. ***Recommended:*** **BB:** Indrajit, Richardus Eko. 2017. "Social Engineering Framework: Understanding the Deception Approach to the Human Element of Security." *International Journal of Computer Science Issues*, 14(2): 8-16. **BB:** Sarriegi, Jose M., and Jose J. Gonzalez. 2008. "Conceptualising Social Engineering Attacks through System Archetypes." *International Journal of System of Systems Engineering* 1(1/2): 111-127. **BB:** Workman, Michael. 2007. "Gaining Access with Social Engineering: An Empirical Study of the Threat." *Information Systems Security* 16(6): 315-331. **BB:** Mouton, Francois, Mercia M. Malan, Louise Leenen, and H.S. Venter. 2014. "Social Engineering Attack Framework." *Information Security for South Africa*, pp. 1-9.
30	Social Engineering: Automated Techniques	***Required:*** **BB:** Kaul, Priya, and Deepak Sharma. 2013. "Study of Automated Social Engineering, its Vulnerabilities, Threats and Suggested Countermeasures." *International Journal of Computer Applications* 67(7): 13-16. **BB:** Jhaveri, Hardik, Harshit Jhaveri, and Dhaval Sanghavi. 2014. "Sybil Attack and its Proposed Solution." *International Journal of Computer Applications* 105(3): 17-19. ***Recommended:*** **BB:** Lauinger, Tobias, Veikko Pankakoski, Davide Balzarotti, and Engin Kirda. 2010. "Honeybot, Your Man in the Middle for Automated Social Engineering." *Proceedings of USENIX Symposium on Networked Systems Design and Implementation*, April 2010. **BB:** Bringer, Matthew, Christopher Chelmecki, Hiroshi Fujinoki. 2012. "A Survey: Recent Advances and Future Trends in Honeypot Research." *International Journal of Computer Network and Information Security*, 4(10): 63-75. **BB:** Huber, Markus, Martin Mulazzani, Edgar Weippl, Gerhard Kitzler, and Sigrun Goluch. 2010. "Exploiting Social Networking Sites for Spam." *Proceedings of the 17th ACM Conference on Computer and Communications Security*. Oct. 2010, pp. 693-695. **BB:** Huber, Markus, Martin Mulazzani, Sebastian Schrittwieser, and Edgar Weippl. 2010. "Cheap and Automated Socio-Technical Atacks based on Social Networking Sites." *Proceedings of the 3rd ACM Workshop on Artificial Intelligence and Security*. Oct. 2010, pp. 61-64. **BB:** Asuncion, Arthur, and Michael T. Goodrich. 2010. "Turning Privacy Leaks into Floods: Surreptitious Discovery of Social Network Friendships and Other Sensitive Binary Attribute Vectors." *Proceedings of the 9th annual ACM workshop on Privacy in the electronic society*. Oct. 2010, pp. 21-30. **BB:** Li, Shujun, S. Amier Haider Shah, M. Asad Usman Khan, Syed Ali Khayam, Ahmad-Reza Sadeghi, and Roland Schmitz. 2010. *Proceedings of the 26th Annual*

		Computer Security Applications Conference, pp. 171-180. **BB:** Tsvetkova, Milena, Ruth Garcia-Gavilanes, Luciano Floridi, and Taha Yasseri. 2017. "Even Good Bots Fight: The Case of Wikipedia." *Public Library of Science (PLoS) One* 12(2): 1-13. **BB:** Samuel, Justin S. and B. Dhivya. 2015. "An Efficient Technique to Detect and Prevent Sybil Attacks in Social Network Applications." *IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, March, pp. 1-3.
4 **Feb**	Lab 1	**LAB:** This lab teaches students the importance of, and techniques for, **lockpicking**.
6	Reverse Social Engineering	***Required:*** **BB:** Irani D., Balduzzi M., Balzarotti D., Kirda E., Pu C. 2011. "Reverse Social Engineering Attacks in Online Social Networks." In: Holz T., Bos H. (eds) *Detection of Intrusions and Malware, and Vulnerability Assessment*. DIMVA 2011. Lecture Notes in Computer Science, vol. 6739. Springer, Berlin, Heidelberg. pp. 55-74. **BB:** Abu-Nimeh, Saeed, and Saku Nair. 2008. "Bypassing Security Toolbars and Phishing Filters via DNS Poisoning." *IEEE Global Telecommunications Conference* (2008), pp. 1-6. ***Recommended:*** **BB:** Meligy, Ali, Hani M. Ibrahim, and Mohamed F. Torky. 2017. "Identity Verification Mechanism for Detecting Fake Profiles in Online Social Networks." *International Journal of Computer Network and Information Security*, 9(1): 31-39. **BB:** Jabee, Roshan, and M. Afshar Alam. 2016. "Issues and Challenges of Cyber Security for Social Networking Sites (Facebook)." *International Journal of Computer Applications* 144(3): 36-40.
11	6 week exam	Six week exam will take place during class and will consist of multiple choice, fill in the blank, short answer, and essay questions. Notebooks are not allowed.
13	Social Engineering: Phishing	***Required:*** **BB:** Aleroud, Ahmed, and Lina Zhou. 2017. "Phishing environments, techniques, and countermeasures: A survey." *Computers & Security*, Vol. 68, pp. 168-196. **BB:** Pattinson, Malcolm, Cate Jerram, Kathryn Parsons, Agata McCormac, and Marcus Butavicius. 2012. "Why Do Some People Manage Phishing E-mails Better Than Others?" *Information Management & Computer Security*, 20(1): 18-28. ***Recommended:*** **BB:** Flores, Waldo Rocha, Hannes Holm, Marcus Nohlberg, and Mathias Ekstedt. 2015. "Investigating Personal Determinants of Phishing and the Effect of National Culture." *Information & Computer Security* 23(2): 178-199. **BB:** Foozy, Cik Feresa Mohd, Rabiah Ahmad, and Mohd Faizal Abdollah. 2013. "Phishing Detection Taxonomy for Mobile Device." *International Journal of Computer Science Issues*, 10(1): 338-344. **BB:** Lötter, André, and Lynn Futcher. 2015. "A Framework to Assist Email Users in the Identification of Phishing Attacks." *Information & Computer Security* 23(4): 370-381. **BB:** Purkait, Swapan. 2012. "Phishing Counter Measures and their Effectivness – A Literature Review." *Information Management & Computer Security* 20(5): 382-420. **BB:** Flores, Waldo Rocha, Hannes Holm, and Gustav Svensson. 2014. "Using Phishing Experiments and Scenario-based Surveys to Understand Security Behaviours in Practice." *Information Management & Computer Security* 22(4): 393-406. **BB:** Parsons, Kathryn, Dragana Calic, Malcolm Pattinson, Marcus Butavicius, Agata

		McCormac, and Tara Zwaans. 2017. "The Human Apsects of Information Security Questionnaire (HAIS-Q): Two further Validation Studies." *Computers & Security* 66: 40-51.
18	Social Engineering: Impersonation & Tailgating	***Required:*** **InCl:** "Tiger Team: Car Dealer Takedown." YouTube Channel episode. https://www.youtube.com/watch?time_continue=5&v=MdQas_We_kI, watch in class. **BB:** AlliedBarton, "Security Tailgating: Best Practices in Access Control" *White Paper*. ***Recommended:*** **BB:** Oberle, Alexander, Pedro Larbig, Ronald Marx, Frank G. Weber, Dirk Scheuermann, Daniel Fages, Fabien Thomas, and Arkoon Netasq. 2016. "Preventing Pass-the-Hash and Similar Impersonation Attacks in Enterprise Infrastructures." *2016 IEEE 30th International Conference on Advanced Information Networking and Applications*, pp. 800-807. **BB:** Bustard, John D., John N. Carter, Mark S. Nixon, and Abdenour Hadid. 2014. "Measuring and Mitigating Targeted Biometric Impersonation." *IET Biometrics* 3(2): 55-61.
20	Social Engineering: Phone Spoofing, Shoulder-surfing & Dumpster Diving	***Required:*** **InCl:** "Voice Solicitation." Fusion: Real Future, episode on Social Engineering. https://www.youtube.com/watch?v=lc7scxvKQOo, watch in class. **InCl:** "Third Party Authorization." CNN Money, episode on Social Engineering. https://www.youtube.com/watch?v=PWVN3Rq4gzw, watch in class. **URL:** Fried, Robert B. "Dumpster Diving." Social-Engineer.org. https://www.social-engineer.org/wiki/archives/DumpsterDiving/CrimeandClues_dumpster_diving.htm **BB:** Rao, Kameswara, and Sushma Yalamanchili. 2012. "Novel Shoulder-Surfing Resistant Authentication Schemes using Text-Graphical Passwords." *International Journal of Information and Network Security*, 1(3): 163-170. ***Recommended:*** **BB:** Li, Mengyuan, Yan Meng, Junyi Liu, Haojin Zhu, Xiaohui Liang, Yao Liu, and Na Ruan. 2016. "When CSI Meets Public WiFi: Inferring Your Mobile Phone Password via WiFi Signals." *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1,068-1,079. **BB:** Applegate, Scott D. 2009. "Social Engineering: Hacking the Wetware!" *Information Security Journal: A Global Perspective*, 18(1): 40–46. **BB:** Helms, Marilyn M., Lawrence P. Ettkin, and Daniel J. Morris. 2000. "Shielding Your Company against Information Compromise." *Information Management & Computer Security*, 8(3): 117-130.
25	Data Destruction & Deletion Security Policy	***Required:*** **BB:** Reardon, Joel, David Basin, and Srdjan Capkun. 2014. "On Secure Data Deletion." *IEEE Security & Privacy* 12(3): 37-44. ***Recommended:*** **BB:** Keele, Benjamin J. 2009. "Privacy by Deletion: The Need for a Global Data Deletion Principle." *Indiana Journal of Global Legal Studies* 16(1):363-384. **BB:** Cachin, Christian, Kristiyan Haralambiev, Hsu-Chun Hsiao, and Alessandro Sorniotti. 2013. "Policy-based Secure Deletion." *Proceedings of the 2013 ACM SIGSAC conference on computer & communications security*, Nov., pp. 259-270. **BB:** Shu, Junliang, Yuanyuan Zhang, Juanru Li, Bodong Li, and Dawu Gu. 2017.

		"Why Data Deletion Fails? A Study on Deletion Flaws and Data Remanence in Android Systems." *ACM Transactions on Embedded Computing Systems* 16(2): 1-22. **BB:** D'Orazio, Christian, Aswami Ariffin, and Kim-Kwang Raymond Choo. 2014. "iOS Anti-Forensics: How Can We Securely Conceal, Delete and Insert Data?" *47th Hawaii International Conference on System Science*, *IEEE* pp. 4,838-4,847. **BB:** Liu, Simon, and Rick Kuhn. 2010. "Data Loss Prevention." *IT Professional* 12(2): 10-13.
27	Cyber Physical System Security	***Required:*** **InCl:** Tech Insider: Break into a Power Plant. https://www.youtube.com/watch?v=pL9q2lOZ1Fw, watch in class. **BB:** Brenner, Joel F. 2013. "Eyes Wide Shut: The Growing Threat of Cyber Attacks on Industrial Control Systems." *Bulletin of the Atomic Scientists* 69(5): 15-20. ***Recommended:*** **BB:** Guri, Mordechai, Matan Monitz, and Yuval Elovici. 2017. "Bridging the Air Gap beween Isolated Networks and Mobile Phones in a Practical Cyber-Attack." *ACM Transactions on Intelligent Systems and Technology* 8(4): 1-25. **BB:** Adepu, Sridhar, and Aditya Mathur. 2016. "An Investigation into the Response of a Water Treatment System to Cyber Attacks." *2016 IEEE 17th International Symposium on High Assurance Systems Engineering*, pp. 141-148. **BB:** Banerjee, Ayan, and Tridib Mukherjee. 2012. "Ensuring Safety, Security, and Sustainability of Mission-Critical Cyber–Physical Systems." *Proceedings of the IEEE* 100(1): 283-299. **BB:** Berning, Tony. 2015. "Protecting Critical Infrastructure from Threats." *Database and Network Journal* 45(2): 13-15.
3 **Mar**	Lab 2	**LAB:** Kali Linux, Social Engineering Toolkit (SET) lab on phishing e-mails & credential harvesting
5	Attack Planning	Students will use class time to meet with their teams and begin their attack planning.
Spring Break		
17	Malware	***Required:*** **BB:** Ovelgönne, Michael, Tudor Dumitras, B. Aditya Prakash, V.S. Subrahmanian, and Benjamin Wang. 2017. "Understanding the Relationship between Human Behavior and Susceptibility to Cyber Attacks: A Data-Driven Approach." *ACM Transactions on Intelligent Systems and Technology* 8(4): 1-25. ***Recommended:*** **BB:** Lévesque, Fanny Lalonde, Jude Nsiempba, José M. Fernandez, Sonia Chiasson, and Anil Somayaji. 2013. "A Clinical Study of Risk Factors Related to Malware Infections." *Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications Security*, pp. 97-108. **BB:** Shrestha, Babbins, Di Ma, Yan Zhu, Haoyu Li, and Nitesh Saxena. 2015. "Tap-Wave-Rub: Lightweight Human Interaction Approach to Curb Emerging Smartphone Malware." *IEEE Transactions on Information Forensics and Security* 10(11): 2,270-2,283. **BB:** Holland, Benjamin, Tom Deering, Suresh Kothari, Jon Mathews, and Nikhil Ranade. 2015. "Security Toolbox for Detecting Novel and Sophisticated Android Malware." *IEEE/ACM 37th IEEE International Conference on Software Engineering*, pp. 733-736.

		BB: Neupane, Ajaya, Md. Lutfor Rahman, Nitesh Saxena, and Leanne Hirshfield. 2015. "A Multi-Modal Neuro-Physiological Study of Phishing Detection and Malware Warnings." *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 479-491.
19	Password Security Policy	***Required:*** **BB:** Tam, L., M. Glassman, and M. Vandenwauver. 2010. "The Psychology of Password Management: A Tradeoff between Security and Convenience." *Behaviour & Information Technology* 29(3): 233-244. ***Recommended:*** **BB:** Shay, Richard, Saranga Komanduri, Adam L. Durity, Phillip Huh, Michelle L. Mazurek, Sean M. Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor. 2016. "Designing Password Policies for Strength and Usability." *ACM Transactions on Information and System Security* 18(4): 1-34. **BB:** Schweitzer, Dino, Jeff Boleng, Colin Hughes, and Louis Murphy. 2011. "Visualizing Keyboard Pattern Passwords." *Information Visualization* 10: 127-133. **BB:** Butler, Rika, and Martin Butler. 2015. "The Password Practices Applied by South African Online Consumers: Perception versus Reality." *South African Journal of Information Management* 17(1): 1-11. **BB:** Pilar, Denise Ranghetti, Antonio Jaeger, Carlos F. A. Gomes, and Lilian Milnitsky Stein. 2012. "Passwords Usage and Human Memory Limitations: A Survey across Age and Educational Background." *PloS One* 7(12): 1-7. **BB:** Halevi, Tzipora, and Nitesh Saxena. 2015. "Keyboard Acoustic Side Channel Attacks: Exploring Realistic and Security-Sensitive Scenarios." *International Journal of Information Security* 14, pp. 443-456. **BB:** Brainard, John, Ari Juels, Ronald L. Rivest, Michael Szydlo, and Moti Yung. "Fourth-Factor Authentication: Somebody You Know." 2006. *Proceedings of the 13th ACM conference on computer and communications security*.
24	Human Security in Social Networks	***Required:*** **BB:** Fire, Michael, Roy Goldschmidt, and Yuval Elovici. 2014. "Online Social Networks: Threats and Solutions." *IEEE Communication Surveys & Tutorials* 16(4): 2,019-2,036. ***Recommended:*** **BB:** Ruan, Xin, Zhenyu Wu, Haining Wang, and Sushil Jajodia. 2016. "Profiling Online Social Behaviors for Compromised Account Detection." *IEEE Transactions on Information Forensics and Security* 11(1): 176-187. **BB:** Najaflou, Yashar, Behrouz Jedari, Feng Xia, Laurence T. Yang, and Mohammad S. Obaidat. 2015. "Safety Challenges and Solutions in Mobile Social Networks." *IEEE Systems Journal* 9(3): 834-854. **BB:** Yu, Haifeng, Michael Kaminsky, Phillip B. Gibbons, and Abraham D. Flaxman. 2008. "SybilGuard: Defending against Sybil Attacks via Social Networks." *IEEE/ACM Transactions on Networking* 16(3): 576-589. **BB:** Post, Gerald V., and Suzanne B. Walchli. 2014. "Social Network Privacy: Trusting Friends." *Journal of Information Privacy and Security* 10(3): 113-137. **BB:** Cao, Jian, Qiang Li, Yuede Ji, Yukun He, and Dong Guo. 2016. "Detection of Forwarding-Based Malicious URLs in Online Social Networks." *International Journal of Parallel Programming* 44(1): 163-180. **BB:** Laleh, Naeimeh, Barbara Carminati, and Elena Ferrari. 2014. "Risk Assessment in Social Networks based on User Anomalous Behaviours." *IEEE Dependable and Secure Computing* 13(20): 1-13.

26	Firewalls and Intrusion-Detection Systems (IDS)	***Required:*** **BB:** Raja, Fahimeh, Kirstie Hawkey, Pooya Jaferian, Konstantin Beznosov, and Kellogg S. Booth. 2010. "It's Too Complicated, So I Turned It Off! Expectations, Perceptions, and Misconceptions of Personal Firewalls." *Proceedings of the 3rd ACM Workshop on Assurable and Usable Security Configuration* (Oct. 2010): pp. 53-62. ***Recommended:*** **BB:** Chen, Song, and Vendana P. Janeja. 2014. "Human Perspective to Anomaly Detection for Cybersecurity." *Journal of Intelligent Information Systems* 42(1): 133-153. **BB:** Ullrich, Johanna, Jordan Cropper, Peter Frühwirt, and Edgar Weippl. 2016. "The Role and Security of Firewalls in Cyber-Physical Cloud Computing." *EURASIP Journal on Information Security*, Vol. 16, pp. 1-20. **BB:** Hu, Hongxin, and Gail-Joon Ahn. 2012. "Detecting and Resolving Firewall Policy Anomalies." *IEEE Transactions on Dependable and Secure Computing* 9(3): 318-331. **BB:** Ogut, Hulisi, Huseyin Cavusoglu, and Srinivasan Raghunathan. 2008. "Intrusion-Detection Policies for IT Security Breaches." *INFORMS Journal on Computing* 20(1): 112-123.
31	12 week exam	Six week exam will take place during class and will consist of multiple choice, fill in the blank, short answer, and essay questions. Notebooks are not allowed.
2 **Apr**	Browsing Habits	***Required:*** **BB:** Kelley, Timothy, and Bennett I. Bertenthal. 2016. "Attention and Past Behavior, Not Security Knowledge, Modulate Users' Decisions to Login to Insecure Websites." *Information and Computer Security* 24(2): 164-176. ***Recommended:*** **BB:** Sanchez-Franco, Manuel J. 2006. "Exploring the Influence of Gender on Web Usage via Partial Least Squares." *Behaviour & Information Technology* 25(1): 19-36. **BB:** Herzberg, Amir. 2009. "Why Johnny Can't Surf (Safely)? Attacks and Defenses for Web Users." *Computers & Security* 28(1-2): 63-71. **BB:** Anderson, Bonnie Brinton, Anthony Vance, C. Brock Kirwan, David Eargle, and Jeffrey L. Jenkins. 2016. "How Users Perceive and Respond to Security Messages: A NeuroIS Research Agenda and Empirical Study." *European Journal of Information Systems* 25(4):364-390. **BB:** Knijnenburg, Bart P., and Alfred Kobsa. 2013. "Making Decisions about Privacy: Information Disclosure in Context-Aware Recommender Systems." *ACM Transactions on Interactive Intelligent Systems* 3(3): 1-23. **BB:** Neria, Michal Ben, Nancy-Sarah Yacovzada, and Irad Ben-Gal. 2017. "A Risk-Scoring Feedback Model for Webpages and Web Users Based on Browsing Behavior." *ACM Transactions on Intelligent Systems and Technology* 8(4): 1-21. **BB:** Beatty, Patricia, Ian Reay, Scott Dick, and James Miller. 2011. "Consumer Trust in E-Commerce Web Sites: A Meta-Study." *ACM Computing Surveys* 43(3): 1-46. **BB:** Jang, Young-Min, Rammohan Mallipeddi, and Minho Lee. 2014. "Identification of Human Implicit Visual Search Intention based on Eye Movement and Pupillary Analysis." *User Modeling and User-Adapted Interaction* 24(4): 314-344.
7	The Research Process	This class period will be dedicated to discussing research steps and paper writing

9	Attack Plan Presentations	Each group has 15 min to present their attack plan
14	Use of Mobile Devices	***Required:*** **BB:** Barn, Balbir S., Ravinder Barn, and Jo-Pei Tan. 2013. "Smart Phone Activity: Risk-Taking Behaviours and Perceptions on Data Security among Young People in England." *International Journal of Social and Organizational Dynamics in IT* 3(4): 43-58. ***Recommended:*** **BB:** Jeske, Debora, Pam Briggs, and Lynne Coventry. 2016. "Exploring the Relationship between Impulsivity and Decision-Making on Mobile Devices." *Personal and Ubiquitous Computing* 20(4): 545-557. **BB:** Raguram, Rahul, Andrew M. White, Yi Xu, Jan-Michael Frahm, Pierre George, and Fabian Monrose. 2013. "On the Privacy Risks of Virtual Keyboards: Automatic Reconstruction of Typed Input from Compromising Reflections." *IEEE Transactions on Dependable and Secure Computing* 10(3): 154-167. **BB:** Palaghias, Niklas, Seyed Amir Hoseinitabatabaei, and Michele Nati. 2016. "A Survey on Mobile Social Signal Processing." *ACM Computing Surveys* 48(4): Article 57, pp. 1-52. **BB:** Riedl, Peter, Rene Mayrhofer, Andraes Möller, Matthias Kranz, Florian Lettner, Clemens Holzmann, and Marion Koelle. 2015. "Only Play in Your Comfort Zone: Interaction Methods for Improving Security Awareness on Mobile Devices." *Personal and Ubiquitous Computing* 19(5): 941-954. **BB:** Glisson, William Bradley, Tim Storer, Gavin Mayall, Iain Moug, and George Grispos. 2011. "Electronic Retention: What Does Your Mobile Phone Reveal about You?" *International Journal of Information Security* 10(6): 337-349.
16	Legal & Ethical Constraints on Human Behavior in Cyberspace	***Required:*** **BB:** Hatfield, Joseph M. 2019. "Virtuous Human Hacking: The Ethics of Social Engineering in Penetration-Testing." *Computers & Security* 83: 354-366. . ***Recommended:*** **Law** **BB:** Workman, Michael. 2009. "How Perceptions of Justice Affect Security Attitudes: Suggestions for Practitioners and Researchers." *Information Management & Computer Security* 17(4): 341-353. **BB:** Mittal, Sandeep, and Priyanka Sharma. 2017. "A Review of International Legal Framework to Combat Cybercrime." *International Journal of Advanced Research in Computer Science* 8(5): 1,372-1,374. **BB:** Espino, Meredith Mays. 2017. "A Tale of Two Phones: A Discussion of Law Enforcement's Use of the All Writs Act to Force Apple to Open Private iPhones." *Rutgers Computer & Technology Law Journal* 43(1): 97-109. **BB:** Kumar, Manish, G.S. Baluja, and Dinesh Sahu. 2016. "Analysing Net Neutrality with Indian Netizens' Perspective." *Compusoft: An International Journal of Advanced Computer Technology* 5(8): 2,204-2,210. **BB:** Pelker, C. Alden. 2016. "Permission to Come Aboard (An Adversary's Network)? Ensuring Legality of Enhanced Network Security Measures through a Multilayer Permission Acquisition Scheme." *American Criminal Law Review* 53(2): 437-477. **BB:** Shackelford, Scott J., and Zachery Bohm. 2016. "Securing North American Critical Infrastructure: A Comparative Case Study in Cybersecurity Regulation."

		Canada-United States Law Journal 40(1): 61-70. **BB:** Strawbridge, Jamie. 2016. "The Big Bluff: Obama, Cyber Economic Espionage, and the Threat of WTO Litigation." *Georgetown Journal of International Law* 47(2): 833-865. **BB:** Rubinstein, Ira S., and Woodrow Hartzog. 2016. "Anonymization and Risk." *Washington Law Review* 91(2): 703-731. **BB:** Trope, Roland L., and Lixian Loong Hantover. 2016. "Hacking Away at Trust." *Business Lawyer* 72(1): 195-203. **BB:** Giles, Courtney. 2015. "Balancing the Breach: Data Privacy Laws in the Wake of the NSA Revelations." *Houston Journal of International Law* 37(2): 543-579. **URL:** Council of Europe Convention on Cybercrime. Specifically see the Budapest Convention https://www.coe.int/en/web/cybercrime/the-budapest-convention **URL:** National Institute of Standards and Technology (NIST) Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations." http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf **URL:** International Organization for Standardization - ISO 27001 Information Security Management Systems, https://www.iso.org/isoiec-27001-information-security.html **URL:** Payment Card Industry Data Security Standard (PCIDSD) https://www.pcisecuritystandards.org/pci_security/ **URL:** Gramm-Leach-Bliley Act (GLBA), https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act **URL:** Federal Trade Commission Red Flags Rule, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/red-flags-rule **URL:** International Traffic in Arms Regulations (ITAR), https://www.pmddtc.state.gov/regulations_laws/itar.html **URL:** Foreign Corrupt Practices Act (FCPA), https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act **URL:** Family Educational Rights and Privacy Act (FERPA), https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html **Ethics** **BB:** McMahon, Joan M., and Ronnie Cohen. 2009. "Lost in Cyberspace: Ethical Decision Making in the Online Environment." *Ethics and Information Technology* 11(1): 1-17. **BB:** Myyry, Liisa, Mikko Siponen, Seppo Pahnila, Tero Vartiainen, and Anthony Vance. 2009. "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study." *European Journal of Information Systems* 18(2): 126-139. **BB:** Levy, Yair, Michelle M. Ramim, and Raymond A. Hackney. 2013. "Assessing Ethical Severity of e-Learning Systems Security Attacks." *The Journal of Computer Information Systems* 53(3): 75-84. **BB:** Milson, Andrew J., and Beong-Wan Chu. 2002. "Character Education for Cyberspace: Developing Good Netizens." *The Social Studies* 93(3): 117-120. **BB:** Elovici, Yuval, Michael Fire, Amir Herzberg, and Haya Shulman. 2014. "Ethical Considerations when Employing Fake Identities in Online Social Networks for Research." *Science and Engineering Ethics* 20(4): 1,027-1,043.

		BB: Stahl, Bernd Carsten, Neil F. Doherty, Mark Shaw, and Helge Janicke. 2014. "Critical Theory as an Approach to the Ethics of Information Security." *Science and Engineering Ethics* 20(3): 675-699. **BB:** Shilton, Katie. 2015. "Anticipatory Ethics for a Future Internet: Analyzing Values during the Design of an Internet Infrastructure." *Science and Engineering Ethics* 21(1): 1-18. **BB:** Sharma, Seemu, Hitashi Lomash, and Seema Bawa. 2015. "Who Regulates Ethics in the Virtual World?" *Science and Engineering Ethics* 21(1): 19-28. **BB:** Mouton, Francois, M. M. Malan, H. S. Venter. 2013. "Social Engineering from a Normative Ethics Perspective." Information Security for South Africa (ISSA), pp. 1-8. **BB:** Hurwitz, Roger. 2014. "The Play of States: Norms and Security in Cyberspace." *American Foreign Policy Interests* 36(5): 322-331.
21	Lab 3	**LAB:** Kali Linux, Browser Exploitation Framework (BeEF) lab
23	Human Privacy Practices: Human Error, Onion-Routing, Encryption, Virtual Private Networks, Cryptocurrency and the Dark Web	***Required:*** **URL:** https://www.wired.com/2015/04/SILK-ROAD-1/ **URL:** https://www.wired.com/2015/05/silk-road-2/ ***Recommended:*** **BB:** Koch, Robert, Mario Golling, and Gabi Dreo Rodosek. 2016. "How Anonymous Is the Tor Network? A Long-Term Black-Box Investigation." *Computer* 49(3): 42-49. **BB:** Kshetri, Nir. 2017. "Can Blockchain Strengthen the Internet of Things?" *IT Professional* 19(4): 68-72. **BB:** Victors, Jesse, Ming Li, and Xinwen Fu. 2017. "The Onion Name System: Tor-powered Decentralized DNS for Tor Onion Services." *Proceedings on Privacy Enhancing Technologies*, Vol. 2017, Issue 1, pp. 21-41. **BB:** Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." *Anonymously published online in October 2008.* https://bitcoin.org/bitcoin.pdf **BB:** Damopoulos, D., G. Kambourakis, M. Anagnostopoulos, S. Gritzalis, and J. H. Park. 2013. "User Privacy and Modern Mobile Services: Are They on the Same Path?" *Personal and Ubiquitous Computing* 17(7): 1,437-1,448. **BB:** Schneier, Bruce. 2017. "IoT Security: What's Plan B?" *IEEE Security & Privacy* 15(5): 1. **BB:** Lin, Jie, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao. 2017. "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications." *IEEE Internet of Things Journal* 4(5): 1,125-1,142.
28 Essay Due	Last Day of Class	Course wrap-up & Student Opinion Forms (SOFs)
TBD	Final Exam	Date, Time, and Location TBD

Attack Plan Grading Rubric

Group members:

Basic Expectations (5 pts each):

Selected target is appropriate for the assignment (e.g. corporation, bank, government office, or organization – but not USNA!)	
Reconnaissance is *passive* and includes no *active* techniques (borderline cases are subject to instructor approval)	
Each member of the group took an active role in the overall project	

Research Expectations (25 pts):

Decisions in the attack plan are strongly tied to research discussed in the class. Both the presentation and paper make clear which studies inform which attack plan decisions.	

Presentation Expectations (5 pts each):

Presentation is no more than 15 min in length	
Each group member participates in giving the presentation	
Visually interesting; time and care was taken to visually inform the audience.	
Presentation makes clear *why* the target was chosen and what the team planned to gain from attacking the target (i.e. the goal).	
Presentation discusses which passive techniques were used during reconnaissance	
Presentation clearly defines which social engineering techniques the team plans to use (technical exploits may be taken up in SY306)	

Written Report Expectations (5 pts):

Length is appropriate (5-7 pages)	
Choice of format is professional and/or scholarly (report should include a bibliography in either case)	
Report makes clear *why* the target was chosen and what the team planned to gain from attacking the target (i.e. the goal).	
Report discusses which passive techniques were used during reconnaissance	
Report clearly defines which social engineering techniques the team plans to use (technical exploits may be taken up in SY306)	
Report is reasonably free from grammatical mistakes (occasional slip ups OK)	

Overall Grade:

Comments:

Research Paper Grading Rubric

Name:

Basic Expectations (5 pts each):

Word length near limit (neither exceeded nor significantly short)	
Bibliography is sufficient for argument of this kind/length	

Format Expectations (2 pts each):

Font (11 point Times New Roman, 1.5" spaced)	
Margins (1-inch uniform), Name/Section at top right	
Title of essay is the question it attempts to answer (no cover page)	
Bibliography correctly uses Chicago style	
Citation correctly uses Chicago author-date standard in body	

Paper Structure (0-5 pts):

(0-1) Completely unacceptable; (2) Unacceptable (Below Standards); (3) Acceptable (Meets Standards); (4) Very Good (Occasionally Exceeds): (5) Excellent (Exceeds Standards)

Introduction: Spurs reader's interest; clear picture of where paper is headed	0 1 2 3 4 5
Thesis: Expresses a viewpoint with clarity	0 1 2 3 4 5
Thesis: Provides an answer to the question asked	0 1 2 3 4 5
Citation content: Discusses important works relevant to the topic	0 1 2 3 4 5
Argument: Provides sub-arguments supporting thesis	0 1 2 3 4 5
Argument: Signposts each step of the argument for the reader (logical clarity)	0 1 2 3 4 5
Argument: Overall quality and sophistication of the argument (rigor)	0 1 2 3 4 5
Counterargument: Addresses counterarguments adequately	0 1 2 3 4 5
Conclusion: Restates argument in light of the reasons/support provided	0 1 2 3 4 5
Conclusion: Recommends new questions for further research OR uses conclusion to reinforce the limits of the paper's conclusion.	0 1 2 3 4 5

Writing Style (10 pts):

Reasonably free from grammatical mistakes (occasional slip ups OK)	
Free from overstatements and unsubstantiated claims	
Paper gives an argument and is not purely descriptive or informative	

Overall Grade:

Comments:

Syllabus Review:

J. M. HATFIELD
LCDR USN

CAPT James Caroland
Chair, Cyber Science Department