Cybersecurity and National Security

ECE 595

Professor: **Dr. Christopher Lamb**
Phone: **505-228-8090**
Email: **cclamb@unm.edu**

Course Description

This course will cover the importance of cybersecurity to national policy today. Specifically, we're going to discuss the history of cybersecurity as a strategic weapon, how long it's been recognized as such and why, and recent campaigns where cybersecurity (or the lack thereof) has been used as a weapon.

Recent developments over the past ten years have highlighted the transformational nature of cybersecurity in national policy and with regard to national security. We've seen (alleged) attacks against utilities, manufacturing, and corporations, all with links to nation-aligned groups. We're going to cover how cybersecurity as a national property of strategic importance was first recognized in the United States, and how we've evolved over the years with respect to how it is addressed. We'll also cover studies of recent campaigns conducted by suspected nation-state aligned groups to understand how these kinds of attacks have evolve and how they're executed today.

At the end of the course, the students will write a research paper on a cybersecurity topic they select, and give a presentation over that topic to the class.

Course Objectives and Methodology

The class will be structured collaboratively, with shared readings and discussion over those readings. At the end of the course, my goal is for all the involved students to have a clear understanding of how cybersecurity has evolved as an area of national importance, why it's more important than ever today, and how nation-states seem engage in this kind of activity. When we finish, you'll know why cybersecurity is important as a national policy area and how malware campaigns are structured and executed.

Learning Objectives

- Understand the history and importance of cybersecurity as a policy area.
- Analyze recent campaigns to understand how these kinds of attacks are executed today.
- Study how today's campaigns are structured and executed, and how they have evolved over the past thirty years.

Course Delivery

This course will be delivered on line (distance learning) giving the students flexibility and ability to complete their academic work solely on line. Course materials, such as reading assignments, powerpoint presentations, assignments and projects will be available online. Students are required to read the

materials and to discuss with other students and the instructor the materials including research that the students have undertaken as part of the requirements.

Evaluation Procedures

1. **Assignments/Discussions/Deliverables that coincide with the parts of the course:** Students will be asked to engage in a discussion with other students and the faculty on a number of questions based on the reading assignment and the link between the materials and security. Some of the questions posed for discussion may require the students to engage on additional research beyond their course's reading assignment. These discussions are part of the overall grade of the course. These assignments will account for 50% of students' overall grade. The assignments will be graded based on the depth of the arguments presented by the discussion.
2. **Research Project**: Students will be required to work on a 15-page research project, on a topic previously approved by your instructor. In the interest of providing more benefits to every student (from their work but also from attending presentations by other students), the instructors will approve on a first-come first-serve basis a different technology area for each student. This way, a student will work on one technology area but listen to final presentation and engage in discussions on multiple areas.

This research project will account for the remaining 50% of the student's final grade. The paper is due on the last week of class and will be presented by the student at the end of the course during the face-to-face meetings..

Project Description: A critical success factor continues to be the ability to write clearly, concisely, and creatively. The goal of this joint research project is to examine the impact of cybersecurity and the lack thereof on global security. Each student will work on a different technology area in cybersecurity, and examine it in a national security context. How does this technology area affect the future, how well are we doing and what are the major policy and strategic recommendations that you have for the US to do better in this area? Your project should also consider likely global scenario changes in the next 20-25 years as much as possible.

1. **Research Paper Guidelines**: Roman/Helvetica/Fourier 12 point font, double spaced, references should follow IEEE guidelines. These fonts and reference formatting should be supported in all major word processors or typesetting programs (e.g. Latex, MS Word).
2. **Grading Procedure**: Grading procedure will be based on the following criteria: a) Does the weekly discussion and the research upon which it is based have a clear, and creative core argument? b) Is that core argument well supported? c) Is it well written? And d) Can we draw policy implications from it?
3. **Grading Scale**: Your final grade will be a combination of the points assigned to the assignments (50 points) and your research paper project (50 points)

The scale used is as follows:

A+ (95 -100 points average);

A (90-94 points average);

B+ (85-89 points average);

B (80-84 points average);

C+ (75-79 points average);

C (70-74 points average);

D (69-60 points average).

Honor Code: UNM formally recognizes the responsibility of our students and professors to behave in an ethical manner.

Netiquette

- *"In following with the UNM Student Handbook, all students will show respect to their fellow students and instructor when interacting in this course. Take Netiquette suggestions seriously. Flaming is considered a serious violation and will be dealt with promptly. Postings that do not reflect respect will be taken down immediately." (Rebecca Adams, OLIT 535)*
- *"This course encourages different perspectives related to such factors as gender, race, nationality, ethnicity, sexual orientation, religion, and other relevant cultural identities. The course seeks to foster understanding and inclusiveness related to such diverse perspectives and ways of communicating."*
- *Link to Netiquette document: http://online.unm.edu/help/learn/students/pdf/discussion-netiquette.pdf*

Copyright Issues

All materials in this course fall under copyright laws and should not be downloaded, distributed, or used by students for any purpose outside this course.

Accessibility

The American with Disabilities Act (ADA) is a federal anti-discrimination statute that provides comprehensive civil rights protection for persons with disabilities. Among other things, this legislation requires that all students with disabilities be guaranteed a learning environment that provides for reasonable accommodations of their disabilities. If you have a disability requiring accommodation, please contact the UNM Accessibility Resource Center in 2021 Mesa Vista Hall at 277-3506 or http://as2.unm.edu/index.html. Information about your disability is confidential.

- Blackboard's Accessibility statement: http://www.blackboard.com/accessibility.aspx
- Include links to accessibility statements for all other technologies included in the course.

Academic Misconduct

You should be familiar with UNM's Policy on Academic Dishonesty and the Student Code of Conduct (http://pathfinder.unm.edu/campus-policies/other-campus-policies.html) which outline academic misconduct defined as plagiarism, cheating, fabrication, or facilitating any such act.

Example Drop Policy

UNM Policies: This course falls under all UNM policies for last day to drop courses, etc. Please see http://www.unm.edu/studentinfo.html or the UNM Course Catalog for information on UNM services and policies. Please see the UNM academic calendar for course dates, the last day to drop courses without penalty, and for financial disenrollment dates.

Technical Skills

In order to participate and succeed in this class, you will need to be able to perform the following basic technical tasks:

- Use UNM Learn (help documentation located in "How to Use Learn" link on left course menu, and also at http://online.unm.edu/help/learn/students/)
- Use email – including attaching files, opening files, downloading attachments
- Copy and paste within applications including Microsoft Office
- Open a hyperlink (click on a hyperlink to get to a website or online resource)
- Use Microsoft Office applications
    - Create, download, update, save and upload MS Word documents
    - Create, download, update, save and upload MS PowerPoint presentations
    - Create, download, update, save and upload MS Excel spreadsheets
    - Download, annotate, save and upload PDF files
- Use the in-course web conferencing tool (Collaborate Web Conferencing software)
- Download and install an application or plug in – required for participating in web conferencing sessions

Technical Requirements

Computing

- A high speed Internet connection is highly recommended.
- Supported browsers include: Internet Explorer, Firefox, and Safari. Detailed Supported Browsers and Operating Systems: http://online.unm.edu/help/learn/students/
- Any computer capable of running a recently updated web browser should be sufficient to access your online course. However, bear in mind that processor speed, amount of RAM and Internet connection speed can greatly affect performance. Many locations offer free high-speed Internet access including UNM's Computer Pods.
- For using the Kaltura Media Tools inside Learn, be sure you have downloaded and installed the latest version of Java, Flash, and Mozilla Firefox. They may not come preloaded.
- Microsoft Office products are available free for all UNM students (more information on the UNM IT Software Distribution and Downloads page: http://it.unm.edu/software/index.html)

For UNM Learn Technical Support: (505) 277-0857 (24/7) or use the "Create a Support Ticket" link in your course.

Web Conferencing

Web conferencing will be used in this course during the following times and dates: For the online sessions, you will need:

- A USB headset with microphone. Headsets are widely available at stores that sell electronics, at the UNM Bookstore or online.
- A high-speed internet connection is highly recommended for these sessions. A wireless Internet connection may be used if successfully tested for audio quality prior to web conferencing.

For UNM Web Conference Technical Help: (505) 277-0857

Tracking Course Activity

UNM Learn automatically records all students' activities including: your first and last access to the course, the pages you have accessed, the number of discussion messages you have read and sent, web conferencing, discussion text, and posted discussion topics. This data can be accessed by the instructor to evaluate class participation and to identify students having difficulty.

Course Content

Content for the course will come from a variety of sources, including freely available technical reports which you'll read and we'll discuss.

I'm going to give you references to the required reading covering these campaigns, and these reports will give you insight into how the campaigns were prosecuted and discovered. I strongly encourage you to supplement your reading with additional material. Find areas that you resonate with in the readings, and explore them!

One quick note - you may be tempted to download and discuss the NSA ANT catalog released by Edward Snowden. Please be aware that this material is still classified, and marked as such. If you have a security clearance, and you download this material, you will have highly classified material on your personally owned devices, and due to your clearance, you may be held responsible for that. Also, because of this, I can't discuss any of this material - sorry about that.

I intend to break the course into eight week-long modules. Some of the reports are fairly technical - as you know, this isn't a technical course, but I would like you to look these over so you understand them at a superficial level. It's important to understand how we do attribution and how malware is delivered, and some technical content is unavoidable in these areas. Look over the code to get some idea of what's going on; read to understand how the code is packaged and how it communicates with command and control elements. And ask me questions! That's what I'm here for.

Week 1

Technical Reports (Stuxnet):

http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet/

https://www.symantec.com/connect/blogs/exploring-stuxnet-s-plc-infection-process

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Week 2

Technical Reports (Flame, Duqu):

https://www.crysys.hu/skywiper/skywiper.pdf

https://www.wired.com/2012/06/flame-tied-to-stuxnet/

https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

Week 3

Technical Reports (Duqu 2):

http://www.crysys.hu/duqu2/duqu2.pdf (This requires registration)

https://securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf

Week 4

Submit Final Report Topic

Technical Reports (BlackEnergy):

http://get.cyberx-labs.com/blackenergy-report

https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf

https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Week 5

Technical Reports (Goldeneye):

https://blog.kaspersky.com/ransomware-for-dummies/13592/

https://blog.malwarebytes.com/threat-analysis/2016/04/petya-ransomware/

https://blog.malwarebytes.com/threat-analysis/2016/05/petya-and-mischa-ransomware-duet-p1/

https://blog.malwarebytes.com/threat-analysis/2016/07/third-time-unlucky-improved-petya-is-out/

https://blog.malwarebytes.com/threat-analysis/2016/12/goldeneye-ransomware-the-petyamischa-combo-rebranded/

Week 6

Technical Reports (RIG Exploit Kit):

https://www.trustwave.com/Resources/SpiderLabs-Blog/RIG-Exploit-Kit-%E2%80%93-Diving-Deeper-into-the-Infrastructure/

http://blog.talosintel.com/2016/01/rigging-compromise.html

https://blog.malwarebytes.com/threat-analysis/exploits-threat-analysis/2016/07/a-look-into-some-rig-exploit-kit-campaigns/

Week 7

Submit Final Report, Presentation Material

Technical Reports (APT28):

https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

http://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf

https://www.root9b.com/sites/default/files/whitepapers/root9b_follow_up_report_apt28.pdf

Week 8

Submit Final Report, Presentation Material

Technical Reports (CrashOverride, Hatman):

https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

https://dragos.com/blog/trisis/TRISIS-01.pdf

https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

(Optional - Source Code; also has links to above reports and more)
https://github.com/ICSrepo/TRISIS-TRITON-HATMAN

Workshop with Introduction to Directed Energy

Final Presentations