Security in Emerging Computing and Networking Systems (Fall 2022)

CPSC 8580

Instructor Info

Mert D. Pesé

Office Hours: Mon & Wed 1-2p

215 McAdams Hall

http://www.mpese.com

mpese@umich.edu

Course Info

Prereq: Bachelor degree in Computer Science or equivalent

Mon & Wed

3.35p-4.50p

134 Lehotsky Hall

TA Info

Simeon Babatunde

Office Hours: Thu 1-3p

https://clemson.zoom.us/j/3473660703?pwd=V1VubFd5ZXBucGZtVlQ4VXErSG5udz09

sbabatu@clemson.edu

Course Description

A computing and networking system is considered emerging if it recently started getting deployed in the real-world, or is deemed promising for a wide-scale deployment in the near future. The security issues surrounding such emerging systems, however, may prevent end users from utilizing their full potential, or, even worse, may rule out the chances of their deployment in the future. Currently, these emerging systems range from Cyber-Physical Systems (CPS) such as autonomous vehicles to Internet of Things (IoT) such as connected smart home devices.

In this course, we will study security challenges in these emerging systems and discuss potential solutions. The course will start with an introductory section covering general security concepts, followed by lectures on three security topics in emerging computing and networking systems, namely automotive security, adversarial machine learning and IoT security. Lectures will be accompanied by research seminars where recent papers from leading conferences will be presented by students. A certain number of papers will also be read and reviewed by the students before class time to increase active participation in the discussion of all presentations. In addition, there will be a semester-long class project. Students can work in teams of 2-3 members. Each group is expected to write a conference-style paper describing their work. Furthermore, there will also be three homework problem sets.

(Tentative) Grading Scheme

20% — Paper Review: Write a short critical response for 17 (out of 40) papers that are presented in class. The papers for each due date are listed in the course schedule below. Papers marked with a star are required to be read and reviewed by everyone. For other papers, students can choose one paper per lecture to review. Responses are due at the beginning of class as a submission to Canvas. Check the guidelines below for more information on how to write a paper review.

10% — Paper Presentation: Choose one of the topics from the reading list, read both the required and recommended papers, and prepare a 20 minute presentation. 15 minutes of your presentation should discuss details of the required paper, as well as your review of it. The remaining 5 minutes are reserved for Q&A with the audience. Since some students will have reviewed the paper in advance, we can expect some active discussion. You will receive a Google Sheet after the first class that will let you choose a paper on a first-come-first-serve basis.

15% — Homework: For a better understanding of the security lectures taught in the first few weeks of the class, there will be three sets of homework problems. They can consist of a written and coding portion.

10% — Participation: Research can only flourish when there is an active exchange of great ideas. We want to keep the class interactive and after every presentation, there will be a brief Q&A session. Feel free to add your own critique of a paper and/or to discuss the presenter's review with the audience.

45% — Course Project: A semester-long project in this course has two goals. The first goal is to help you learn more about doing research in general. The second goal is to give you the opportunity to study particular areas of security in greater detail. Therefore, you are expected to perform a substantial research project; this involves selecting an open problem, reading the related work, designing, implementing, and evaluating a solution, and presenting your results. The main deliverables will be a project presentation, as well as a project report. Presentation grades will be based on: 1) the depth in presentation (i.e., how in-depth the paper is understood, correctness of responses to questions from the audience); and 2) slides preparation (slides need to be informative with technical depth). Class project grades will be assigned based on the novelty of the design, completeness of the system implementation, and clarity in the report.

Required Materials

There is no official textbook for the class. Slides will be provided and reading materials for each topic will be assigned from research papers that are listed in the reading section below.

Paper Review Guidelines

Write a ∼400 word critical response to each required paper.

A In the first paragraph:
   1. State the problem that the paper tries to solve; and
   2. Summarize the main contributions.

B In one or more additional paragraphs:
   1. Evaluate the paper's strengths and weaknesses;
   2. Discuss something you would have done differently if you had written the paper; and
   3. Suggest one or more interesting open problems on related topics.

Your most important task is to demonstrate that you've read the paper and thought carefully about the topic.

Learning Objectives

- Explain common software and network vulnerabilities and attacks, defense mechanisms against network attacks, and cryptographic protection mechanisms
- Describe the cost and tradeoffs associated with designing security into a product
- Analyze cutting-edge research in automotive and IoT security, as well as adversarial machine learning
- Learn to critically review a paper and summarize it, as well as review and provide helpful criticism to your peers' work
- Design a research project and learn how to write a research paper

Grading Policies

All assignments should be submitted through the course website (Canvas), unless stated otherwise. Homework and Projects are due at 11:59 PM on the due date described in the assignments. Late submissions are highly discouraged. Late policy is as follows: An immediate deduction of 50% will be applied to submissions after the deadline but before 24 hours past the deadline; submissions made 24 hours or more past the deadline will not be accepted. If you feel that an error has been made in grading an assignment or an exam, you must submit a written re-grade petition within one week after the assignment or exam has been returned to you. Verbal appeals are not acceptable and grades will not be changed after the one-week period.

Letter grades are assigned according to the standard 10-point scale: The final score will be rounded up, e.g., if you receive

A	90-100
B	80-89
C	70-79
D	60-69
F	0-59

a 89.5, it will be rounded up to 90 and you will still receive an A. There will be no extra credit opportunities throughout the semester. Curving is at the discretion of the professor.

Time to Wait

Students are expected to wait for 15 minutes after the beginning of a lecture before leaving if the instructor is late and no announcement has been posted on Canvas.

Absences

As per Clemson academic policy, course instructors may use reasonable academic penalties which reflect the importance of work missed due to unexcused absences, since absence from class is detrimental to the learning process. Course instructors who penalize students for unexcused absences must state attendance requirements as related to the grading, on the course syllabus and keep accurate attendance records. See the Academic Regulations section of the current Undergraduate catalog or the Policies and Procedures of the Graduate catalog, both located at the Course Catalog home page.

If you are sick, please stay home. Let the professor know in advance via e-mail that you are not attending that day's class and you are fine. If there are other reasons (e.g., family-related, etc.) that you cannot attend, please let the professor know as well.

Academic Integrity

As members of the Clemson University community, we have inherited Thomas Green Clemson's vision of this institution as a "high seminary of learning." Fundamental to this vision is a mutual commitment to truthfulness, honor, and responsibility, without which we cannot earn the trust and respect of others. Furthermore, we recognize that academic dishonesty detracts from the value of a Clemson degree. Therefore, we shall not tolerate lying, cheating, or stealing in any form.

See the Undergraduate Academic Integrity Policy website for additional information and the current catalogue for the policy. For graduate students, see the current Graduate School Handbook for all policies and procedures.

Accessibility

Clemson University values the diversity of our student body as a strength and a critical component of our dynamic community. Students with disabilities or temporary injuries/conditions may require accommodations due to barriers in the structure of facilities, course design, technology used for curricular purposes, or other campus resources. Students who experience a barrier to full access to this class should let the instructor know and make an appointment to meet with a staff member in Student Accessibility Services as soon as possible. You can make an appointment by calling 864-656-6848, by emailing studentaccess@lists.clemson.edu, or by visiting Suite 239 in the Academic Success Center building. Appointments are strongly encouraged – drop-ins will be seen, if at all possible, but there could be a significant wait due to scheduled appointments. Students who have accommodations are strongly encouraged to request, obtain and send these to their instructors through the AIM portal as early in the semester as possible so that accommodations can be made in a timely manner. It is the student's responsibility to follow this process each semester.

You can access further information at the Student Accessibility website. Other information is at the university's Accessibility Portal.

The Clemson University Title IX Statement Regarding Non-Discrimination

The Clemson University Title IX statement: Clemson University is committed to a policy of equal opportunity for all persons and does not discriminate on the basis of race, color, religion, sex, sexual orientation, gender, pregnancy, national origin, age, disability, veteran's status, genetic information or protected activity in employment, educational programs and activities, admissions and financial aid. This includes a prohibition against sexual harassment and sexual violence as mandated by Title IX of the Education Amendments of 1972. This Title IX policy is located on the Campus Life website. Ms. Alesia Smith is the Clemson University Title IX

Clemson University aspires to create a diverse community that welcomes people of different races, cultures, ages, genders, sexual orientation, religions, socioeconomic levels, political perspectives, abilities, opinions, values and experiences.

Emergency Preparation

Emergency procedures have been posted in all buildings and on all elevators. Students should be reminded to review these procedures for their own safety. All students and employees should be familiar with guidelines from the Clemson University Police Department. Visit here for information about safety.

Clemson University is committed to providing a safe campus environment for students, faculty, staff, and visitors. As members of the community, we encourage you to take the following actions to be better prepared in case of an emergency:

1. Ensure you are signed up for emergency alerts
2. Download the Rave Guardian app to your phone
3. Learn what you can do to prepare yourself in the event of an active threat

Changes to Syllabus

Lecture topics and assignments are subject to change. The course syllabus is a general plan for the course; deviations to the class may be necessary and will be announced to class by the instructor.

Ethics and Law

To defend a system, you need to be able to think like an attacker, and that includes understanding techniques that can be used to compromise security. However, using those techniques in the real world may violate the law or the university's rules, and it may be unethical. Under some circumstances, even probing for weaknesses may result in severe penalties, up to and including expulsion, civil fines, and jail time. Our policy in this course is that you must respect the privacy and property rights of others at all times, or else you will fail the course.

Acting lawfully and ethically is your responsibility. Carefully read the Computer Fraud and Abuse Act (CFAA), a federal statute that broadly criminalizes computer intrusion. This is one of several laws that govern "hacking." Understand what the law prohibits. The EFF provides helpful advice on vulnerability reporting and other legal matters.

Reading List

Automotive Security (AS)

1. Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H. and Savage, S., 2010, May. Experimental security analysis of a modern automobile. In 2010 IEEE symposium on security and privacy (pp. 447-462). IEEE.
2. Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F. and Kohno, T., 2011. Comprehensive experimental analyses of automotive attack surfaces. In 20th USENIX security symposium (USENIX Security 11).
3. Song, H.M., Kim, H.R. and Kim, H.K., 2016, January. Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network. In 2016 international conference on information networking (ICOIN) (pp. 63-68). IEEE.
4. Cho, K.T. and Shin, K.G., 2016. Fingerprinting electronic control units for vehicle intrusion detection. In 25th USENIX Security Symposium (USENIX Security 16) (pp. 911-927).
5. Cho, K.T. and Shin, K.G., 2017, October. Viden: Attacker identification on in-vehicle networks. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 1109-1123).
6. Pesé, M.D., Stacer, T., Campos, C.A., Newberry, E., Chen, D. and Shin, K.G., 2019, November. LibreCAN: Automated CAN message translator. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (pp. 2283-2300).
7. Serag, K., Bhatia, R., Kumar, V., Celik, Z.B. and Xu, D., 2021. Exposing New Vulnerabilities of Error Handling Mechanism in CAN. In 30th USENIX Security Symposium (USENIX Security 21) (pp. 4241-4258).
8. Kulandaivel, S., Jain, S., Guajardo, J. and Sekar, V., 2021, May. Cannon: Reliable and stealthy remote shutdown attacks via unaltered automotive microcontrollers. In 2021 IEEE Symposium on Security and Privacy (SP) (pp. 195-210). IEEE.
9. Chen, Q.A., Yin, Y., Feng, Y., Mao, Z.M. and Liu, H.X., 2018, February. Exposing Congestion Attack on Emerging Connected Vehicle based Traffic Signal Control. In NDSS.
10. Wan, Z., Shen, J., Chuang, J., Xia, X., Garcia, J., Ma, J. and Chen, Q.A., 2022. Too Afraid to Drive: Systematic Discovery of Semantic DoS Vulnerability in Autonomous Driving Planning under Physical-World Attacks. arXiv preprint arXiv:2201.04610.
11. Wen, H., Chen, Q.A. and Lin, Z., 2020. Plug-N-Pwned: Comprehensive Vulnerability Analysis of OBD-II Dongles as A New Over-the-Air Attack Surface in Automotive IoT. In 29th USENIX Security Symposium (USENIX Security 20) (pp. 949-965).
12. Francillon, A., Danev, B. and Capkun, S., 2011. Relay attacks on passive keyless entry and start systems in modern cars. In Proceedings of the Network and Distributed System Security Symposium (NDSS). Eidgenössische Technische Hochschule Zürich, Department of Computer Science.
13. Garcia, F.D., Oswald, D., Kasper, T. and Pavlidès, P., 2016. Lock It and Still Lose It—on the (In) Security of Automotive Remote Keyless Entry Systems. In 25th USENIX security symposium (USENIX Security 16).

Adversarial Machine Learning (AML)

1. Papernot, N., McDaniel, P., Jha, S., Fredrikson, M., Celik, Z.B. and Swami, A., 2016, March. The limitations of deep learning in adversarial settings. In 2016 IEEE European symposium on security and privacy (EuroS&P) (pp. 372-387). IEEE.
2. Papernot, N., McDaniel, P., Goodfellow, I., Jha, S., Celik, Z.B. and Swami, A., 2017, April. Practical black-box attacks against machine learning. In Proceedings of the 2017 ACM on Asia conference on computer and communications security (pp. 506-519).
3. Zhao, Y., Zhu, H., Liang, R., Shen, Q., Zhang, S. and Chen, K., 2019, November. Seeing isn't believing: Towards more robust adversarial attack against real world object detectors. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (pp. 1989-2004).
4. Cao, Y., Xiao, C., Cyr, B., Zhou, Y., Park, W., Rampazzi, S., Chen, Q.A., Fu, K. and Mao, Z.M., 2019, November. Adversarial sensor attack on lidar-based perception in autonomous driving. In Proceedings of the 2019 ACM SIGSAC conference on computer and communications security (pp. 2267-2281).
5. Sun, J., Cao, Y., Chen, Q.A. and Mao, Z.M., 2020. Towards robust LiDAR-based perception in autonomous driving: General black-box adversarial sensor attack and countermeasures. In 29th USENIX Security Symposium (USENIX Security 20) (pp. 877-894).
6. Zhu, Y., Miao, C., Zheng, T., Hajiaghajani, F., Su, L. and Qiao, C., 2021, November. Can we use arbitrary objects to attack lidar perception in autonomous driving?. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (pp. 1945-1960).
7. Shen, J., Won, J.Y., Chen, Z. and Chen, Q.A., 2020. Drift with Devil: Security of Multi-Sensor Fusion based Localization in High-Level Autonomous Driving under GPS Spoofing. In 29th USENIX Security Symposium (USENIX Security 20) (pp. 931-948).
8. Cao, Y., Wang, N., Xiao, C., Yang, D., Fang, J., Yang, R., Chen, Q.A., Liu, M. and Li, B., 2021, May. Invisible for both camera and lidar: Security of multi-sensor fusion based perception in autonomous driving under physical-world attacks. In

2021 IEEE Symposium on Security and Privacy (SP) (pp. 176-194). IEEE.
9. Jing, P., Tang, Q., Du, Y., Xue, L., Luo, X., Wang, T., Nie, S. and Wu, S., 2021. Too good to be safe: Tricking lane detection in autonomous driving with crafted perturbations. In 30th USENIX Security Symposium (USENIX Security 21) (pp. 3237-3254).
10. Sato, T., Shen, J., Wang, N., Jia, Y., Lin, X. and Chen, Q.A., 2021. Dirty road can attack: Security of deep learning based automated lane centering under Physical-World attack. In 30th USENIX Security Symposium (USENIX Security 21) (pp. 3309-3326).
11. Zhang, Q., Hu, S., Sun, J., Chen, Q.A. and Mao, Z.M., 2022. On adversarial robustness of trajectory prediction for autonomous vehicles. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 15159-15168).
12. Yang, K., Tsai, T., Yu, H., Panoff, M., Ho, T.Y. and Jin, Y., 2021, May. Robust Roadside Physical Adversarial Attack Against Deep Learning in Lidar Perception Modules. In Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security (pp. 349-362).
13. Ji, X., Cheng, Y., Zhang, Y., Wang, K., Yan, C., Xu, W. and Fu, K., 2021, May. Poltergeist: Acoustic adversarial machine learning against cameras and computer vision. In 2021 IEEE Symposium on Security and Privacy (SP) (pp. 160-175). IEEE.

IoT Security (IOTS)

1. Fernandes, E., Jung, J. and Prakash, A., 2016, May. Security analysis of emerging smart home applications. In 2016 IEEE symposium on security and privacy (SP) (pp. 636-654). IEEE.
2. Mohajeri Moghaddam, H., Acar, G., Burgess, B., Mathur, A., Huang, D.Y., Feamster, N., Felten, E.W., Mittal, P. and Narayanan, A., 2019, November. Watching you watch: The tracking ecosystem of over-the-top tv streaming devices. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (pp. 131-147).
3. Kumar, D., Shen, K., Case, B., Garg, D., Alperovich, G., Kuznetsov, D., Gupta, R. and Durumeric, Z., 2019. All Things Considered: An Analysis of IoT Devices on Home Networks. In 28th USENIX security symposium (USENIX Security 19) (pp. 1169-1185).
4. Huang, D.Y., Apthorpe, N., Li, F., Acar, G. and Feamster, N., 2020. Iot inspector: Crowdsourcing labeled network traffic from smart home devices at scale. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 4(2), pp.1-21.
5. Sugawara, T., Cyr, B., Rampazzi, S., Genkin, D. and Fu, K., 2020. Light Commands:Laser-Based Audio Injection Attacks on Voice-Controllable Systems. In 29th USENIX Security Symposium (USENIX Security 20) (pp. 2631-2648).
6. Zhang, G., Yan, C., Ji, X., Zhang, T., Zhang, T. and Xu, W., 2017, October. Dolphinattack: Inaudible voice commands. In Proceedings of the 2017 ACM SIGSAC conference on computer and communications security (pp. 103-117).
7. Feng, H., Fawaz, K. and Shin, K.G., 2017, October. Continuous authentication for voice assistants. In Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking (pp. 343-355).
8. Soltan, S., Mittal, P. and Poor, H.V., 2018. BlackIoT:IoT Botnet of High Wattage Devices Can Disrupt the Power Grid. In 27th USENIX Security Symposium (USENIX Security 18) (pp. 15-32).
9. Scaife, N., Peeters, C. and Traynor, P., 2018. Fear the reaper: Characterization and fast detection of card skimmers. In 27th USENIX Security Symposium (USENIX Security 18) (pp. 1-14).
10. Urbina, D.I., Giraldo, J.A., Cardenas, A.A., Tippenhauer, N.O., Valente, J., Faisal, M., Ruths, J., Candell, R. and Sandberg, H., 2016, October. Limiting the impact of stealthy attacks on industrial control systems. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security (pp. 1092-1105).
11. Reardon, J., Feal, Á., Wijesekera, P., On, A.E.B., Vallina-Rodriguez, N. and Egelman, S., 2019. 50 ways to leak your data: An exploration of apps' circumvention of the android permissions system. In 28th USENIX Security Symposium (USENIX Security 19) (pp. 603-620).
12. Antonioli, D., Tippenhauer, N.O. and Rasmussen, K., 2020, May. BIAS: bluetooth impersonation attacks. In 2020 IEEE Symposium on Security and Privacy (SP) (pp. 549-562). IEEE.
13. Antonioli, D., Tippenhauer, N.O. and Rasmussen, K.B., 2019. The KNOB is Broken: Exploiting Low Entropy in the Encryption Key Negotiation Of Bluetooth BR/EDR. In 28th USENIX Security Symposium (USENIX Security 19) (pp. 1047-1061).
14. Wu, J., Wu, R., Antonioli, D., Payer, M., Tippenhauer, N.O., Xu, D., Tian, D.J. and Bianchi, A., 2021. LIGHTBLUE: Automatic Profile-Aware Debloating of Bluetooth Stacks. In 30th USENIX Security Symposium (USENIX Security 21) (pp. 339-356).

Course Schedule

Date	Topic	Readings Due & Other Notes
08/24 (W)	Course Introduction	N/A
08/29 (M)	Lecture 1: Fundamental Concepts	N/A
08/31 (W)	Lecture 2: Cryptography (Part I) Course Project Introduction	N/A
09/05 (M)	Lecture 2: Cryptography (Part II)	AS1*, AS2* HW1 released
09/07 (W)	Lecture 3: Network Security (Part I)	AML1*
09/12 (M)	Lecture 3: Network Security (Part II)	AML2*
09/14 (W)	Lecture 4: Software Security	IOTS1* HW1 due
09/19 (M)	Project Proposal Presentation	HW2 released
09/21 (W)	Lecture 5: Automotive Security	N/A
09/26 (M)	Lecture 6: Adversarial Machine Learning	N/A
09/28 (W)	Lecture 7: IoT Security	HW2 due
10/03 (M)	Paper Presentations	AS3, AML3, IOTS2 HW3 released
10/05 (W)	Paper Presentations	AS4, AS5, IOTS3
10/10 (M)	Paper Presentations	AML4, AML5, AML6
10/12 (W)	Paper Presentations	AS6, IOTS4, IOTS5 HW3 due
10/17 (M)	Paper Presentations	IOTS6, IOTS7, IOTS8
10/19 (W)	Paper Presentations	AS7, AS8, IOTS9
10/24 (M)	Paper Presentations	AML7, AML8, IOTS10
10/26 (M)	Paper Presentations	AS9, AS10, AML9
10/31 (M)	Midterm Project Presentations (Part I)	N/A
11/02 (W)	Midterm Project Presentations (Part II)	N/A
11/07 (M)	Fall Break (No Class)	N/A
11/09 (W)	Paper Presentations	AML10, AML11, IOTS11

11/14 (M)	Paper Presentations	AS11, AS12, AS13
11/16 (W)	Paper Presentations	AML12, AML13, IOTS12
11/21 (M)	Paper Presentations	IOTS13, IOTS14
11/23 (W)	Thanksgiving Break (No Class)	N/A
11/28 (M)	Final Project Presentations (Part I)	N/A
11/30 (W)	Final Project Presentations (Part II)	N/A
12/05 (M)	Final Project Presentations (Part III)	N/A
12/07 (W)	Final Project Presentations (Part IV)	Final Report Due