INCS 775

Data Center Security

Zhida Li, Ph.D.
College of Engineering and Computing Sciences
NEW YORK INSTITUTE OF TECHNOLOGY

Today's - Objectives

- 1st part
  - Getting to know each other
  - Introduction to the course
  - Requirements, labs/assignments, quiz, project, exams
  - Overview of topics to be covered
- 2nd part
  - Fundamentals to data center

About the Instructor

- Received the B.E. and M.Eng.Sc. degrees in electrical engineering and microelectronic design from the University College Cork, Ireland
- Received the Ph.D. degree in engineering science from Simon Fraser University (SFU), Canada (advisor: Prof. Ljiljana Trajković)
- Research assistant at Tyndall National Institute, Ireland (2011-2014); Research Assistant in the Communication Networks Laboratory at SFU (2015-2022).
- Postdoctoral fellow working on cybersecurity
  - development of fast machine learning (ML) algorithms
  - real-time system for detecting network anomalies
- Assistant Professor
  - College of Engineering and Computing Sciences, NYIT

About the Instructor

- Zhida Li, Assistant Professor, New York Teck–Vancouver, Room 1842, Suite 180.
- Office hours: By appointment (zli74@nyit.edu)
- NYIT WWW: https://www.nyit.edu/bio/zli74 | Personal WWW: https://zhidali.me/
- LinkedIn: https://www.linkedin.com/in/zhidali/
- Google Scholar: https://scholar.google.com/citations?hl=en&user=t_hlHwQAAAAJ

Zhida Li

FOLLOW

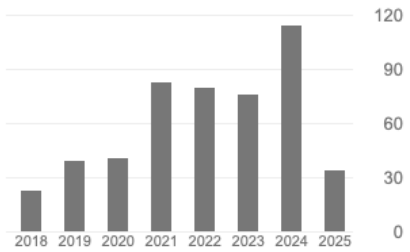
New York Institute of Technology - Vancouver
Verified email at nyit.edu - Homepage

Communication networks cybersecurity machine learning intrusion detection systems

TITLE	CITED BY	YEAR
Machine learning techniques for classifying network anomalies and intrusions Z Li, ALG Rios, G Xu, L Trajković 2019 IEEE international symposium on circuits and systems (ISCAS), 1-5	97	2019
Detecting BGP anomalies using machine learning techniques Q Ding, Z Li, P Batta, L Trajković 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC …	58	2016
Machine learning for detecting anomalies and intrusions in communication networks Z Li, ALG Rios, L Trajković IEEE Journal on Selected Areas in Communications 39 (7), 2254-2264	48	2021

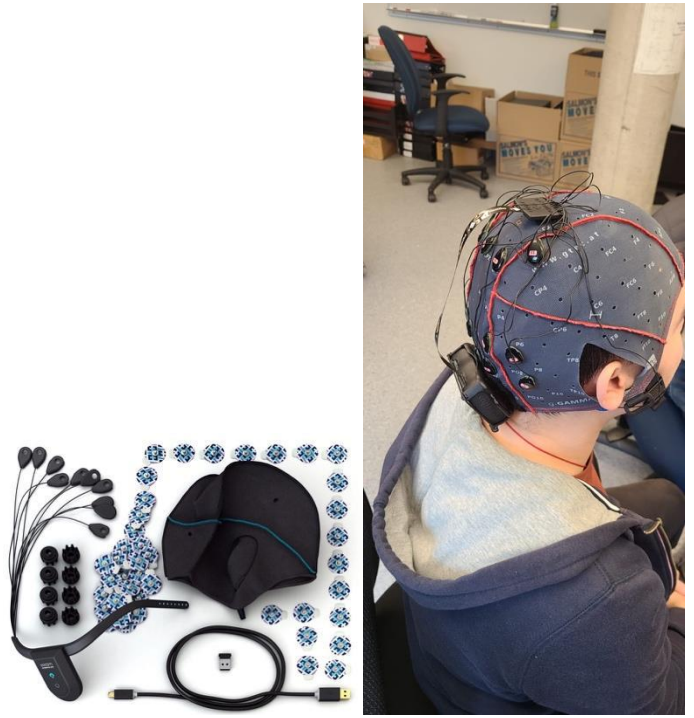
Cited by VIEW ALL

	All	Since 2020
Citations	503	428
h-index	12	11
i10-index	14	11



About the Instructor (cont.)

- Network anomaly detection:
  - develop new algorithms (echo state networks, graph neural networks , and transformers) to enhance the model robustness for time series data
  - enhance CyberDefense
  - extract additional features based on network topology
- Blockchain:
  - Ethereum phishing detection based on transaction records and labels collected from Etherscan (https://etherscan.io)
- Brain-computer interface:
  - analyze electroencephalogram (EEG) benchmarks
  - develop new algorithms and approaches to analyze data from the non-invasive collection of brain signals
- BCI & Neurotechnology, Virtual BR41N.IO Hackathon
  - https://www.br41n.io/Spring-School-2025
- BCI & NeuroTech Masterclass: Unicorn Brain Interface
  - https://www.gtec.at/event/masterclass-unicorn-2025/



About the Instructor (cont.)

- Publications related to Data Centers:
  - H. B. Yedder, Q. Ding, U. Zakia, **Z. Li**, S. Haeri, and Lj. Trajković, "Comparison of virtualization algorithms and topologies for data center networks," in *Proc. 26th Int. Conf. Comput. Commun. Netw., 2nd Workshop Netw. Security. Analytics Autom.*, Vancouver, Canada, Aug. 2017.

  - S. Haeri, Q. Ding, **Z. Li**, and Lj. Trajković, "Global resource capacity algorithm with path splitting for virtual network embedding," in *Proc. IEEE Int. Symp. Circuits Syst.*, Montreal, Canada, May 2016, pp. 666-669.

About the Instructor: External Service

- Secretary, Membership Development Committee, IEEE Canada
  https://www.ieee.ca/en/
- Secretary, IEEE Vancouver Section
  https://vancouver.ieee.ca/
- Chair, IEEE Circuits and Systems Society joint Chapter of the Vancouver/Victoria Sections
  https://vancouver.ieee.ca/cas/
- Counselor, IEEE NYIT-Vancouver Student Branch
  https://ieeenyit.org/
- Lead Guest Editor, MDPI Electronics
  https://www.mdpi.com/journal/electronics/special_issues/9NW7ZZGK91

About You

- Have you heard about Data Centers? What about Cloud-based Systems?
- Have you worked on any data center-related projects? What were they about?
- Do you know security issues with data centers and related topics?
- Have you ever tried to secure a network or data center?

What is this course all about?

INCS 775-VA2 (1387): Monday, 9:00 AM - 12:00 PM (PT) & Friday, 1:00 PM - 4:00 PM (PT) in Room 1812, Suite 180, 2985 Virtual Way, BTC (in-person)

Computer architectures and systems that provide critical computing infrastructure.

This infrastructure includes hardware devices like computers, firewalls, routers, and switches, as well as software applications such as email systems, web servers, and computer desktop operating systems.

Focus on implementing and managing organization-wide secure computing capabilities, with examples of critical systems including intranet, extranet, and Internet systems.

Course-Level Learning Outcomes

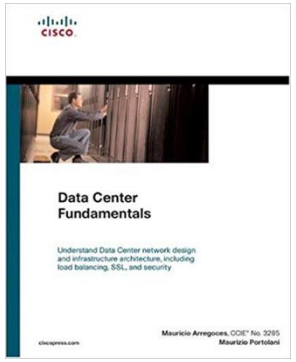
1. Identify and classify specific threats to which the data center is subject
2. Classify and describe network appliances used to secure a data center
3. Analyze a given data center network topology and define and document its security hierarchy
4. Implement defense-in-depth in data center designs
5. Outline security techniques available to minimize the security threats in the data center network
6. Prioritize security events and implement appropriate measures to mitigate future events in the data center network
7. Implement and document hardware and software security measures in a given Virtual Data Center Design.
8. Function effectively as a member of a team
9. Apply machine learning (ML) techniques to detect network suspicious records/flows/connections in data center

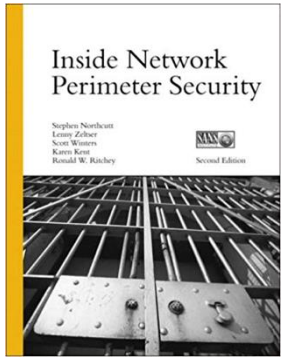
References

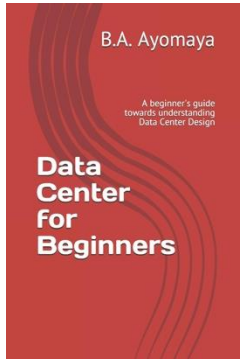
- Mauricio Arregoces and Maurizio Portolani, *Data Center Fundamentals*, 1st edition, Cisco Press, 2003.
  ISBN-13: 978-1587050237.
- Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent, and Ronald W. Ritchey, *Inside Network Perimeter Security*, 2nd edition, Sams Publishing, 2005.
  ISBN-13: 978-0672327377.
- B. A. Ayomaya, *Data Center for Beginners: A beginner's guide towards understanding Data Center Design*, 2020.
  ISBN-13: 978-1520527079.
- Curtis Franklin Jr. and Brian Chee, *Securing the Cloud: Security Strategies for the Ubiquitous Data Center*, 1st edition, CRC Press, 2019.
  ISBN-13: 978-1466569201.

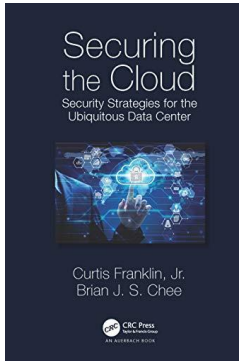
References (cont.)

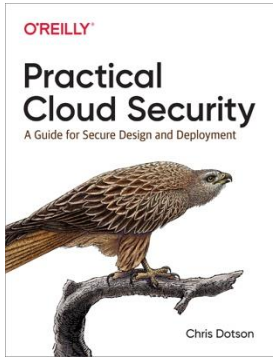
- Chris Dotson, *Practical Cloud Security: A Guide for Secure Design and Deployment*, 1st edition, O'Reilly Media, 2019. ISBN-13: 978-1492037514.
- Bhavani Thuraisingham, *Developing and Securing the Cloud*, 1st edition, Auerbach Publications, 2013.
  ISBN-13: 978-1439862919.
- James F. Kurose and Keith W. Ross, *Computer Networking: A Top-Down Approach*, 8th edition, Pearson, 2020.
  ISBN-13: 9780135928615.

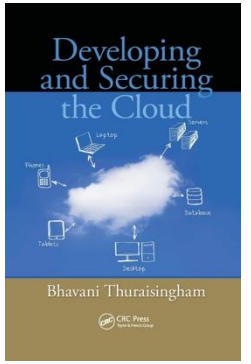


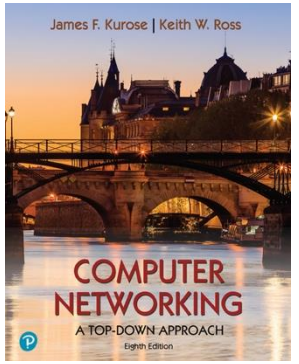












Other References

- William Stallings, *Data and Computer Communications*, 10th edition, Pearson, 2014. ISBN-13: 9780137561704.
- K. P. Murphy, *Probabilistic Machine Learning: An Introduction*. Cambridge, MA, USA: The MIT Press, 2022.
  ISBN-13: 978-0262046824.
  https://probml.github.io/pml-book/book1.html

Other References (cont.)

Journals:

- IEEE Communications Surveys & Tutorials
- IEEE Network - The Magazine of Global Internetworking
- IEEE Communications Magazine
- ACM Computer Communication Review
- IEEE Journal on Selected Areas in Communications
- IEEE/ACM Transactions on Networking

…

Note:
Papers from ACM: https://libguides.nyit.edu/az.php?s=16453&a=a&p=1, select “ACM Digital Library”, then log in.
Papers from IEEE Explore: https://libguides.nyit.edu/az.php?s=16453&a=i&p=1, select “IEEE Xplore”, then log in.

Grading Guidelines

- Evaluation will be based on labs/assignments (in groups of up to 3), one group term project (in groups of up to 3), one in-class quiz, one in-class midterm exam, and one in-class final exam.

Item	Contribution to Total Grade
Labs/Assignments (Group)	20 %
Term Project (Group)	20 %
Quiz	5 %
Midterm Exam	25 %
Final Exam	30 %
TOTAL	100 %

Labs/Assignments (Group)

- Done in groups of a maximum of 3 students. Let me know if you want to work in a team but have no teammate.
- Tasks can be done during class time or submitted before the deadline to avoid a late penalty.
- There will be 1 submission from a group on Canvas.

Term Project (Group)
Option 1: *Research Writing* & Presentation

- Done in groups of a maximum of 3 students.
- We may choose a topic related to Data Centers, Data Center Security, or any subject connected to topics covered in class. Our goal is to learn and summarize research ideas and proposed systems/models/algorithms/architectures as well as the results from the state-of-the-art. Once you define the topic, confirmation from the instructor is required.
- Create a 5-page summary of the papers.
  IEEE paper format (two columns, single-spaced). The entire paper report should be no more than 8 pages and greater than or equal to 5 pages, including text, figures, equations, tables, and references. The Reference Section can be arranged on a separate page. (Minimum: 4 page content + 1 page reference)
  Figures and tables should be limited to a combined total of 6. Similarity Score <=30%.

Details will be presented on Canvas.

Term Project (Group)
Option 2: *Project Demo* & Presentation

- Done in groups of a maximum of 3 students.
- We may choose a topic related to Data Centers, Data Center Security, or any subject connected to topics covered in class. Once the student defines the topic, confirmation from the instructor is required.
- Create a 2-page report of your implementations.
  IEEE paper format (two columns, single-spaced).
- Note: Option 2 Projects that demonstrate high quality and depth of research, potentially comparable to conference publications, may receive bonus points.

Details will be presented on Canvas.

Term Project (Group)
Options 1 and 2: *Presentation*

- We will give a presentation in Week 7.2 and Week 8.1. Each group will have 20 minutes (15 minutes of presentation + 5 minutes of Q&A).

- Research writing reports (and code if applicable) and Slides should be submitted on Canvas.

Quiz, Midterm, and Final Exam

- Quiz: LockDown Browser, closed-book, in-person
- Midterm and Final Exam: Paper-based, closed-book, in-person
- True/false + multiple choice; Essay questions (provided descriptions / explanations / calculations / diagrams).

Grading Guidelines (cont.)

- Evaluation will be based on labs/assignments (in groups of up to 3), one group term project (in groups of up to 3), one in-class quiz, one in-class midterm exam, and one in-class final exam.

Item	Contribution to Total Grade
Labs/Assignments (Group)	20 %
Term Project (Group)	20 %
Quiz	5 %
Midterm Exam	25 %
Final Exam	30 %
TOTAL	100 %

Lower Limit (%)	Grade
90	A
85	A-
80	B+
75	B
70	B-
65	C+
60	C
0	F

Explanation to Grade

Grade	Description	Quality Points	Used in GPA Calculation
A	Excellent quality and full mastery of the course material, extraordinary distinction	4.0	Yes
A-	Excellent quality and full mastery of the course material	3.7	Yes
B+	Good to excellent comprehension of the course material and the skills necessary to work with course material	3.3	Yes
B	Good comprehension of the course material and the skills necessary to work with course material	3.0	Yes
B-	Reasonably good comprehension of the course material and the skills necessary to work with course material	2.7	Yes
C+	Adequate and slightly above satisfactory comprehension of the course material and met the basic course requirements	2.3	Yes
C	Adequate and satisfactory comprehension of the course material and met the basic course requirements	2.0	Yes
F	Failure	0	Yes

Schedule

- Syllabus on Canvas (subject to change).
- Updates from announcements.

Before We Start

Any questions?

Do you think this will be a hard class?