COINS RESEARCH SUMMER SCHOOL 2021 (ONLINE-ZOOM)

Final Report

COINS School Description

The COINS summer school is a one-week intensive course for Ph.D. students in computer and information security and in related fields. In 2021 the summer school is offered in cooperation with the UiA study centre in Metochi on Lesvos Island, Greece. But, due to COVID-19 the summer school sessions were conducted online via zoom.

Submitted By:

Sarang Shaikh
PhD Candidate
Department of Information Security and Communication Technology

Norwegian University of Science and Technology (NTNU), Gjøvik, Norway
Email: sarang.shaikh@ntnu.no
Profile:
https://www.ntnu.edu/employees/sarang.shaikh

Supervised By:

Sule Yildirim Yayilgan
Professor
Department of Information Security and Communication Technology

Norwegian University of Science and Technology (NTNU), Gjøvik, Norway
Email: sule.yildirim@ntnu.no
Profile:
https://www.ntnu.edu/employees/sule.yildirim

Day 1

The summer school started at 08:00 am with a very warm welcome from **Hanno Langweg**, COINS Scientific Director, NTNU and without wasting more time on other discussions he started the first session.

08:00 am – 12:00 pm → Session 1, 2: Risk assessment, threat modelling and cascading threats

The session was conducted by **Panayiotis Kotzanikolaou** (Associate Professor at the Department of Informatics, University of Piraeus, Greece, and Director Cybersecurity Research Lab). The overall content of the session was based on two major papers:

1. "Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., & Lopez, J. (2018). "A survey of IoT- enabled cyberattacks: Assessing attack paths to critical infrastructures and services". IEEE Communications Surveys & Tutorials, 20(4), 3453-3495."
2. "Stellios I., Kotzanikolaou P. and Grigoriadis C., "Assessing IoT enabled cyber-physical attack paths against critical systems". Elsevier Computers and Security, Vol.107, August 2021, 102316."

The focus of the session was to discuss critical infrastructures (CIs) and their security threats which have arises due to the introduction and use of internet-of-things (IoT) devices. The main category of CIs which involves the use of IoT devices is the "cyber-physical systems" which was the focused point throughout the session. Major examples of cyber-physical systems are smart grids, smart cars, smart traffic management, autonomous ships, remote patient management, etc. According to a study, 35.82 billion IoT devices will be installed worldwide by 2021 and 75.44 billion by 2025. The IoT devices can be used as attack enablers for cyber-physical systems. Mainly, we learned about how IoT enabled cyber-attacks can be carried out against cyber-physical systems. Overall, 50 recent attacks were discussed comprising of real incidents as well as proof-of-concept (PoC) attacks. Some of the under-discussion attacks are given in Table 1.

Attack Title	Attack Type	Real Damage	Potential Damage	Critical Level
Take control of a car remotely through the internet	PoC	The manufacturer was forced to patch 1400000 vehicles	Compromising people safety, disturbing traffic	High
Take control of traffic control lights	PoC	--	This attack may cause disturbing traffic lights to create traffic jams or cars accidents	High
Take control of in-hospital devices	Real	The fixing took couple of weeks as the devices needs to be replaced	Access to the medical records using infected medical systems	High
Ukraine's smart grid	Real	230000 peoples were affected	Harming the public confidence, economic loss	High

Table 1: IoT-Enabled Attack Types

From all of these attacks' analysis, following steps were suggested to avoid future IoT-enabled cyber-physical attacks.

- Avoid installing IoT near critical systems
- Consider all attack paths
- Control internet access to/from IoT
- Control physical access to IoT devices
- Authenticate network communications, etc

The question asked from my side relating to the PhD topic was:

Question: My PhD topic is related in the domain of smart border control technologies like e-gates, biometrics, fingerprints etc.; Do you have any idea how cyber-attacks are being handled in systems like these to preserve data privacy and protections?

Answer: We are mainly discussing security problems, but we have privacy problems as well. If these technologies are exploited that is very big problem. Side effects of these attacks:

1. Attackers attacked a hospital, get hacked the data privacy leaks.
2. Security and privacy are major concerns
3. Cyber physical attack path (fake voice record) for biometrics destroys the physical characteristic of the user. And these needs to be addressed for securing the systems.

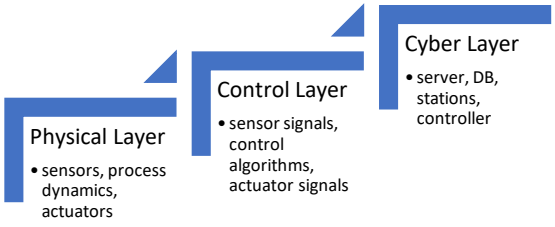
Here this calls for the lunch break from 12:00 pm to 4:00 pm. The lunch break was consisted of our own personal lunch and zoom screen was set to some delicious food screens. Also, we did the virtual sight-seeing of Limonos monastery via YouTube links.

16:00 pm – 18:00 pm → Session 3: ICS/OT/IIoT/IoT security

The session was conducted by **Marina Krotofil** (Cyber Security Product Owner, IoT platform: Connected Vessels, Terminals and Warehouses, A.P. Moller, Maersk). The session focused on the introduction to different types of cyber-physical system (CPS) including:

1) Industrial Control System (ICS)
2) Operational Technology (OT)
3) Industrial Internet-of-Things (IIoT)
4) Internet-of-Things (IoT)

Moreover, the session discussed main concepts of CPS and its application areas including chemical sector, logistics, agriculture, smart cities, autonomous vehicles, smart phones, etc. The ICS/OT/IIoT systems are not directly connected to the internet. However, IoT systems are directly connected to the internet. The discussion continued with the introduction to the different layers of CPS consisting of:



The major takeaway before going into the dinner break was to understand that in CPS "Attack Design != Attack Success". For making a successful attack you need to understand the domain and structure of the targeted CPS and design attack based on the weakest part of the CPS where attack can carry the maximum damage.

Here this calls for the dinner break from 18:00 pm to 19:00 pm.

19:00 pm – 21:00 pm → After Dinner Session: Analysis and visualization of raw network data (hands-on exercise)

The session was conducted by **Jessica Steinberger** (Universität der Bundeswehr München – Unveiling the truth). The session focused on the hands-on exercise on analysis and visualization of raw network data. In other terms, it was related to the field network forensics. Network forensics is the sub field of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection. The major tools covered in this hands-on were: R language, Wireshark, R Studio, Gephi, Cyberchef, WinHex and Network Miner. We were provided with a prebuilt virtual machine (VM) containing all these tools. The focus of this session was based on learning some basics of R language using R studio including:

- Defining different datatypes and variables in R
- Reading large files using R
- Performing arithmetic operations in R
- Performing different visualizations like bar chart, pie chart, histograms, bubble chart, etc in R

Day 2

08:00 am – 12:00 pm → Session 4, 5: The science of (fighting) fake news

The session was conducted by **Giancarlo Ruffo** (Associate Professor of Computer Science, Dipartimento di Informatica, Università degli Studi di Torino). The main agenda of the session was **"Using network science to model, analyze, and mitigate misinformation diffusion in social media".** There were two major parts of the session. 1) Fake news and its terminologies, 2) Network science and how it could be used for detecting fake news. The session started with the explanation of different terminologies and types of fake news including misinformation, malformation, conspiracy theories, spam, hate speech, rumors, etc. Next, the impact of fake news on individuals and possible ways of creating awareness among individuals regarding fake news was discussed.

Without wasting the time, the speaker shifted to towards explaining "Network Science" and specifically the "Complex Networks". Basically, complex networks are built on graph based approaches. A graph (or a network) is made of nodes and links. The speaker discussed basic definitions of the graph like nodes (vertices), links (edges), directed, undirected, weighted, unweighted graphs, etc. Some other relevant concepts like degree, adjacency matrix,

centrality measures, closeness, betweenness, centrality distributions, robustness, community structures, partitions, etc. were also discussed.

The question asked from my side relating to the PhD topic was:

Question: What do you think regarding supervised learning or dictionary-based methods for detecting fake news?

Answer: Include, community feature into the supervised learning for detecting fake news. Use of graph neural networks.

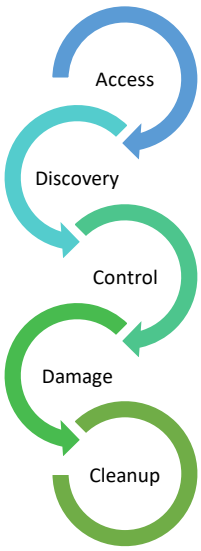
Question: How this network science / CN are adaptable to changes in community detection/structure over time? if community evolves or characteristics of the community changes?

Answer: The structure of the network is unstable and we have various snapshots of the networks. We need to understand the changes in the network, degrees, emerging, etc. Subfield of CN, evolution of time over communities, split between AI and machine learning. Evolution of networks → temporal networks, snapshots of two networks, Networks are adaptable.

Here this calls for the lunch break from 12:00 pm to 4:00 pm. The lunch break was consisted of our own personal lunch and zoom screen was set to some delicious food screens. Also, we did the virtual sight-seeing of Lesvos Geopark via YouTube links.

16:00 pm – 18:00 pm → Session 6: ICS/OT/IIoT/IoT security

The session was conducted by **Marina Krotofil** (Cyber Security Product Owner, IoT platform: Connected Vessels, Terminals and Warehouses, A.P. Moller, Maersk) and continued with the discussion done on the first day of the school. The discussion started with the development life cycle of the attacks in cyber-physcial systems (CPS). The major stages in these attacks are:



The speaker further continued with the explanation of one of the attach that she carried out for her PhD thesis.

Here this calls for the dinner break from 18:00 pm to 19:00 pm.

19:00 pm – 21:00 pm → After Dinner Session: Analysis and visualization of raw network data (hands-on exercise)

The session was conducted by **Jessica Steinberger** (Universität der Bundeswehr München – Unveiling the truth) and continued with the session conducted on Day 1 including how to load large network data (PCAP) files in R. Furthermore, some of the discussions are listed below:

- Use wireshark to export PCAP packet files into csv
- Use glimpse() and summary() packages to understand the overall summary of the data
- Use melt() to perform data transformation
- Finally, visualize network data to see most frequent ip addresses, sources, etc.

Day 3

08:00 am – 08:20 am → Information Meeting

The information meeting consisted of virtual visit to the Metochi Island via zoom. The care takers of the island showed us various classrooms and dining areas in the island including rooms as well.

08:20 am – 10:00 am → Session 7: Introduction to Usable Security

The session was conducted by Dr. Luigi Lo Iacono (Professor, Institute for Cyber Security & Privacy, Computer Science, University of Applied Sciences Bonn-Rhein-Sieg). The topic of the discussion was "Usable Security". According to a report from Verizon Data Breach Investigations in 2016, users are the weakest link in the security because 63% of the data breaches involved weak, default or stolen passwords. Usable security is all about understanding the security of a system from users' perspective. Therefore, throughout the session we tried to answer the very important question "Are users the enemy"? The major themes on which the session focused regarding usable security were user authentication, email security, phishing, mobile security and privacy, administrator, and developers. After discussing the various aspects in a case study related to "Usable Email Security" it was concluded that it is the developers who are the weakest links and not the users. There are total 11.65M (52%) full-time, 6.35M (28%) part-time and 4.30M (19%) non-professional developers worldwide. The major takeaway from the session was to make a balance between security and usability while developing any application which involves any security aspect.

The question asked from my side relating to the PhD topic was:

Question: usable security in smart-border control techs?

Answer: There is a new role, and new application domain. Obstacles in acceptance technologies, lower down those obstacles. Common approach in usable security is to make transparence in technologies and understanding the user's fear what makes him not to trust or trust the technologies, so focus on those and make those things aware to the users.

10:00 am – 12:00 pm → Session 8: The science of (fighting) fake news

The session was conducted by **Giancarlo Ruffo** (Associate Professor of Computer Science, Dipartimento di Informatica, Università degli Studi di Torino) and continued with the discussion from Day 2 of the summer school. The case study of analyzing citation network using complex networks are discussed. The citation network was based on the scientific articles in the fake news domain. The speaker and his team built a fake news search engine based on this citation network case study. This citation analysis allows us to identify relevant papers according to different complex networks things like in-degree, betweenness, authority score, etc. Other concepts under discussion were creating networks from twitter like retweet network or mention/reply network.

Here this calls for the lunch break from 12:00 pm to 4:00 pm. The lunch break was consisted of our own personal lunch and zoom screen was set to some delicious food screens. Also, we did the virtual sight-seeing of the museum and olive oil industries via YouTube links.

16:00 pm – 18:00 pm → Session 9: Analysis of cryptographic algorithm implementations during CC Evaluation

The session was conducted by **Thomas Hesselmann**. The main focus of the session was to discuss two major cryptographic algorithms. 1) Elliptic Curve Digital Algorithm (ECDA), 2) Elliptic Curve Digital Signature Algorithm (ECDSA). The speaker focused on the evaluation and analysis of these algorithms while running on different cloud computing (CC) platforms. The major discussions done by the speaker were on the analysis made on development as well as production level like analysis of functional requirements, implementations, product configurations, firewalls, protocols, etc. Vulnerability analysis was the focused point in this analysis.

Day 4

08:00 am – 10:00 am → Session 10: Risk Based Authentication

The session was conducted by Dr. Luigi Lo Iacono (Professor, Institute for Cyber Security & Privacy, Computer Science, University of Applied Sciences Bonn-Rhein-Sieg). The topic of the discussion was "An Introduction to Risk Based Authentication". The main motivation behind studying this topic was to understand weakness in password-based authentications, intelligent password guessing, phishing, etc. Although, 2FA is widely used approach to solve above problems but still it is not so much popular among the peoples. Risk based authentication is relatively a new approach to increase account security without compromising user interaction. The approach suggests to calculate risks based on different

other factors while users log in like frequency of same ip address, same operating system, etc. if there is something new or unusual while login from ip address or operating system it calculates a risk score in order to identify if to allow or not the login. The various risk-based authentication methods used by famous IT companies are given below.

Service	Used features and weightings
Amazon	IP address
GOG.com	IP address
Google	IP address, Time parameters, User agent string
LinkedIn	IP address, User agent string, Language, Time parameters

Additionally, the major authentication ways by famous IT companies are given below.

Service	Used features and weightings
Amazon	Verification code (email, text)
Facebook	Approve login on computer, verification code (email, text), asking friends for help, identify photos of the friend
GOG.com	Verification code (email, text)
Google	Most frequent sign-in location, verification code (email, text), confirmation button on second device)
LinkedIn	Verification code (email)

Now, coming towards the discussion of how much of these risk-based authentication methods are acceptable by the peoples. So there are two major factors which affects the acceptance of these methods. 1) trust in online service, 2) device involved. The speaker and his team conducted a suvery study in order to understand the acceptability of the risk-based authentication methods. The survey is available as:

"Wiefling, S., Iacono, L. L., & Dürmuth, M. (2019, June). Is this really you? An empirical study on risk-based authentication applied in the wild. In IFIP International Conference on ICT Systems Security and Privacy Protection (pp. 134-148). Springer, Cham."

The question asked from my side relating to the PhD topic was:

Question → Did you considered the affect and role of demographic and education or previous background knowledge on RBA methods on overall acceptance of different RBA methods?

Answer → We did not worked on this. This could be done in future and open issues, limitations. But this has much impact on the responses for RBA in our study.

10:00 am – 12:00 pm → Session 11: The science of (fighting) fake news

The session was conducted by **Giancarlo Ruffo** (Associate Professor of Computer Science, Dipartimento di Informatica, Università degli Studi di Torino) and continued with the discussion from Day 3 of the summer school. Here another case study was discussed based on modelling epidemics on networks. The considered epidemic was "The Black Death", which spread in whole Europe between 1346 and 1353 and killed almost 30-60% of Europe's population. Another case study discussed by the speaker was modelling the spread of

misinformation where the network was built upon the nodes of susceptible, believer and fact checker.

Here this calls for the lunch break from 12:00 pm to 4:00 pm. The lunch break was consisted of our own personal lunch and zoom screen was set to some delicious food screens. Also, we did the virtual sight-seeing of the Molyvos Castle via YouTube links.

16:00 pm – 18:00 pm → Session 12: Cyber Risk and Resilience Analytics (Theory)

The session was conducted by **Sachin Shetty** (Professor, Department of Computational, Modeling and Simulation Engineering, Old Dominion University). The main agenda of the session was to discuss overview of the cyber risk and resilience analytics and modelling attacker opportunity. The main motivation behind studying this topic was to understand the cyber risks in critical infrastructures (CIs) and their early-stage identifications of threats including their rapid response to minimize the damage. The speaker gave talks on multiple topics related to these areas.

Day 5

08:00 am – 12:00 pm → Session 13, 14: Reading Security Protocol Specifications is Difficult and Error Prone

The session was conducted by **Dieter Gollmann** (TU Hamburg-Harburg). The main agenda of the session was all about the security protocols, their specifications, understanding, development, deployment and complexities. To get an overview of how much reading or designing security protocols are difficult and error prone the discussion started with discussing one of the famous protocol “OAuth 2.0”. The use case used for this protocol was from the popular social networking site “Facebook”. The speaker explained the complete flow of OAuth 2.0 where an authorization request is sent by the protocol. Once the permission is granted, it asks for access token. Finally, after providing the access token the required resource/information is sent back. Now, this flow seems perfectly ok on overview but inside this protocol there are a lot of specification that needs to be analyzed while working on it. The speaker further explained the different vulnerabilities in this protocol like attacking via redirect_URI, exploitation using access token, hacking path separators, stealing access token via redict_URI, etc.

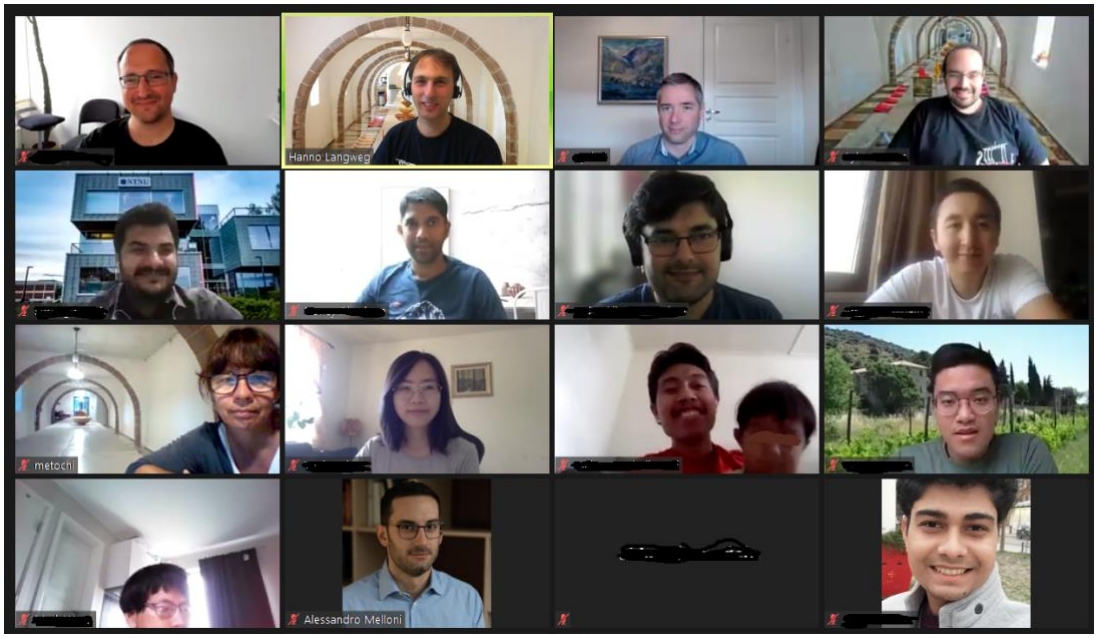
Here this calls for the lunch break from 12:00 pm to 4:00 pm. The lunch break was consisted of our own personal lunch and zoom screen was set to some delicious food screens.

16:00 pm – 18:00 pm → Session 15: Cyber Risk and Resilience Analytics (exercise with virtualized software environment)

The session was conducted by **Sachin Shetty** (Professor, Department of Computational, Modeling and Simulation Engineering, Old Dominion University). The main focused points of this hands-on exercise were:

- Hands on exercise in virtualized environment
- Learn to generate and analyze attack graphs
- Computer cyber risk and resilience metrics

Finally, this calls for the ending of the summer school and we switched off the zoom.



Thankyou So Much,