CYBERSECURITY CENTRE of EXCELLENCE
A joint initiative of DSCI & Government of Telangana

Den Haag

DSCI PROMOTING DATA PROTECTION
A NASSCOM® Initiative

Kingdom of the Netherlands

INDO-DUTCH CYBER SECURITY SCHOOL 2022

Programme 2022

Oct 28 - Nov 25, 2022

Online Action Learning

Updated!

INDO-DUTCH CYBER SECURITY SCHOOL 2022

SPONSORS

The Hague Centre for Strategic Studies

Den Haag

Kingdom of the Netherlands

Embassy of India
The Hague, The Netherlands

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

CYBERSECURITY CENTRE of EXCELLENCE
A joint initiative of DSCI & Government of Telangana

CONTENTS

Please note this programme is subject to updates!

AGENDA

Friday Oct 28

Launch Event - 18:00 IST / 14:30 CET

Week 1: Mon 31 -Fri 04

Lecture: Information manipulation & subversion of democracy - Mon 31, 16:45 IST / 12:15 CET

Lecture: Privacy - Mon 31, 18:10 IST / 13:40 CET

Lecture: Security - Tue 01, 17:00 IST / 12:30 CET

Lecture: Automated Vulnerability Research - Tue 01, 19:15 IST / 14:45 CET

Lecture: DSCI - Wed 02, 18:15 IST / 14:45 CET

Lecture: The Darkening Web - Wed 02, 20:30 IST / 16.00 CET

Lecture: Security - Thurs 03, 17:00 IST / 12:30 CET

Lecture: National Cyber Resilience Game - Thurs 03, 20:30 IST / 16:00 CET

Explanation of Week 2 challenges - Fri 04, 17:00 IST / 12:30 CET

Lecture: Career in Forensics - Fri 04, 18:15 IST / 13:45 CET

AGENDA

Week 2: Mon 07 - Fri 11

Lecture: HCSS - Mon 07, 17:00 IST / 13:30 CET

Lecture: Automotive Security - Mon 07, 18:15 IST / 13:45 CET

Lecture: Ransomware - Mon 07, 21:00 IST / 16:30 CET

Lecture: IAM - Tue 08, 17:00 IST / 12:30 CET

Lecture: Cyber Forensics - Tue 08, 17:15 IST / 14:45 CET

Lecture: Accountability - Wed 09, 17:00 IST / 13:30 CET

Lecture: Cryptography - Thurs 10, 17:00 IST / 13:30 CET

Lecture: DSCI - Thurs 10, 18:15 IST / 14:45 CET

Lecture: Threat Intel - Fri 11, 17:00 IST / 12.30 CET

Week 3: Mon 14 - Fri 18

Challenge consultation 1 - Wed 16, 17:00 IST / 13:30 CET

Challenge consultation 2 - Wed 16, 18:15 IST / 14:45 CET

Challenge consultation 3 - Wed 16, 19:30 IST / 16:00 CET

Challenge consultation 4 - Wed 16, 20:45 IST / 17:15 CET

Feedback on Cyber resilience Game - Thurs 17, 17:00 IST / 13:30 CET

AGENDA

Week 4: Mon 21 - Fri 25

All Challenge Providers: Judging the Solutions of the Challenges - Tue 22, 20:45 IST / 17:15 CET

All Challenge Providers: Judging the Solutions of the Challenges - Wed 23, 20:45 IST / 17:15 CET

Winning students prep their pitches/presentations - Thurs 24, 17:00 IST / 13:30 CET

Presentations and judging - Fri 25, 17:00 IST / 13:30 CET

Presentations and judging - Fri 25, 18:15 IST / 14:45 CET

Closing Ceremony - Fri 25, 19:30 IST / 16:00 CET

Note

Our students will receive a full list of Microsoft Teams links to every lecture and event during the IDCSS22, 24 hours before the Kick-Off Ceremony. In addition, the final schedule of each day will be sent out to all of our students after the end of lectures the previous day.

SPEAKERS

Topic: Ransomware

CHRISTOPHER PAINTER

Christopher Painter is the President of The Global Forum on Cyber Expertise Foundation and a former top US Cyber Diplomat. He also serves as a Board Member for the Center for Internet Security and as a Commissioner for the Global Commission on the Stability of Cyberspace.

Topic: Automated Vulnerability Research

KOEN GIJSBERS

Koen Gijsbers is the Program Director Automated Vulnerability Research at dcypher - Netherlands Enterprise Agency. He also serves as a Non-Executive Director at Angoka and as an Advisory Board Member for the NATO Cooperative Cyber Defence Centre of Excellence.

Topic: Information Manipulation & Subversion of Democracy

ARTHUR LAUDRAIN

Arthur Laudrain is a strategic analyst at The Hague Centre for Strategic Studies, a DPhil candidate in Cybersecurity at the University of Oxford, a Fellow at the European Cyber Conflict Research Initiative and at the Open Diplomacy Institute. Laudrain is an expert on emerging technologies and international affairs, foreign interference in democratic processes, information manipulation and cyber strategies.

SPEAKERS

Topic: The Darkening Web

ALEXANDER KLIMBURG

Dr. Alexander Klimburg is Senior Fellow at HCSS and senior Associate at the Center for Strategic and International Studies. He currently serves as the Head of the Centre for Cybersecurity at the World Economic Forum. Dr. Klimburg has researched and advised on numerous policy topics within the wider field of international cybersecurity since 2007.

Topic: Cyber Forensics

HANS HENSELER

Dr J. Henseler has served part-time as the professor of Digital Forensics & E-Discovery at University of Applied Sciences Leiden since 16 August 2016. He is also a senior adviser in the Digital and Biometrical Traces division at the Netherlands Forensic Institute, a board member at the Netherlands Register of Court Experts and chair of the board of directors at DFRWS.

Topic: Cryptography

MARC STEVENS

Marc Stevens is a tenured researcher at the Cryptology Group at Centrum Wiskunde & Informatica in Amsterdam. He obtained his PhD in 2012 from the Mathematical Institute, Leiden University, He is an expert in cryptanalysis, with emphasis on practical attacks on MD5 and SHA-1.

SPEAKERS

INSTITUTE FOR ACCOUNTABILITY IN THE DIGITAL AGE

Topic: Accountability

FRITS BUSSEMAKER

Frits Bussemaker is the chairman of the Institute for Accountability in the Digital Age' (I4ADA), in the Hague. Mr Bussemaker also works an independent Business Community Builder for I-Partnerschap Rijk-Hoger Onderwijs, under the Dutch government. Mr Bussemaker's work links Information Technology, Innovation and Impact.

Please note this is a preliminary programme and is subject to updates!

CHALLENGES

Challenge 1:

Memory Acquisition from various platform:

Memory forensic plays a significant role in identifying various artefacts that may not be found in the hard disk including evidence of fileless malware and rootkits. Windows 11 has made it compulsory to have TPM which may affect the process of memory acquisition. Moreover, it has a feature of Virtualization Based Security (VBS) which will further divide User Space and Kernel Space in Isolated User Mode and Secure Kernel respectively. Most of the tools for memory acquisition load the device driver into the kernel and read the physical memory. Sometimes it was noticed that when tool attempts to acquire memory, it identifies it as a malicious and causes Blue Screen of Death (BSOD). Which wipes out all the data from RAM.

Normally to acquire memory from various platform, different tools are used and to acquire memory from Linux is bit difficult task and new feature of MAC OS (M1 and M2 chip) does not allow tool to acquire RAM from the system.

Tasks:

1. Develop a comprehensive tool which can acquire RAM from most of the platform (Windows, Linux, and MAC)
2. How to determine whether the system has Virtualization Based Security (VBS) is enabled or not and if yes, acquire memory from user space as well as kernel space including components of secure kernel.

CHALLENGES

Challenge 2:

Guarding Organizations from Browser based Attacks:

According to a recent study, approximately 45% of people surfing the Internet are not utilizing the most secure version of their web browser like other software, without the appropriate security patches applied, web browsers are vulnerable to attack or exploit. A fully patched web browser can still be vulnerable to attack or exploit if the browser plug-ins are not fully patched. Traditionally, browser-based attacks originated from bad websites. However, due to poor security coding of web applications or vulnerabilities in the software supporting web sites, attackers have recently been successful in compromising large numbers of trusted web sites to deliver malicious payloads to unsuspecting visitors. A newly discovered spyware effort attacked users through 32 million downloads of extensions to Google's market-leading Chrome web browser, researchers at Awake Security told Reuters, highlighting the tech industry's failure to protect browsers as they are used more for email, payroll, and other sensitive functions. Google said it removed more than 70% of the malicious add-ons from its official Chrome Web Store after being alerted by the researchers last month.

Tasks:

1. Develop a browser artifact collector and mention why it is unique from other tools which are available in the market?
2. What are the artifacts that you will collect for the analysis?
3. What is your approach for doing browser forensics?
4. How to secure our web browser and what are the steps that are necessary to take to prevent attacks?

CHALLENGES

Challenge 3:

Guarding organizations from Ransomware attacks:

Ransomware has been a persistent threat for organizations across industries for many years now. As more businesses embrace digital transformation, the likelihood of being targeted in a ransomware attack has grown considerably. This is because the methods cybercriminals employ to carry out attacks are becoming more difficult to identify and manage. One of the most successful families of ransomware has returned once again, with a new email spam campaign designed to infect victims with the file-encrypting malware. Locky was one of the first major forms of ransomware to become globally successful and at one point was one of the most common forms of malware in its own right. Locky was released in 2016 and is spread primarily through emails containing an infected Microsoft Word document. When a user opens the document, they will see unintelligible data and the phrase "Enable macro if data encoding is incorrect." If they enable macros, then the ransomware will be downloaded and begin encrypting files. After the encryption is complete, victims receive a message on how to pay the ransom and get their files back.

Tasks:

1. Develop a mechanism or tool on how you will stop ransomware without encrypting the files?
2. How will you determine the attack pattern of the ransomware?
3. What are the artifacts that will you collect for analysis?
4. Is there any possibility to stop ransomware using YARA signatures? If yes, what is your approach?

CHALLENGES

Challenge 4: Deepfakes:

The use of videos and audios as definitive evidence of events has begun to be challenged by high-quality fake videos and audios made by AI-algorithms (the deep fakes). Deep neural networks (DNNs) provide a new spin on the perplexing subject of online deception. Although digital image and video modification is not new, the rapid development of DNNs in recent years has made the process increasingly faster and seamless. Deep Fake videos that are well-crafted can generate illusions of a person's presence and actions that do not exist and can result in severe political, social, financial, and legal consequences.

Tasks:

1. Identify the current deepfake detection methods/techniques.
2. Identify what are the current limitations and come up with new ideas that can counter them

CHALLENGES

Challenge 5:

21st Century Instruments for Accountability:

In this era of the Global Digital Revolution, digital technologies provide the world with a wealth of positive accomplishments. Societies and individuals can benefit in all manner of ways through access to knowledge, people and organizations on a local and global level. More than that, digital has become a must-have, for people, society and the economy. Indeed, digital technology fosters innovation. Online platforms, e commerce, social media, artificial intelligence, data analytics, robotics and the internet of things (IoT) are further expediting this process by hyper-connecting individuals, organizations, communities, societies and data, with tens of billions of objects and entities. Unfortunately, the Internet is not immune to evil. Breaches of norms and values are also occurring in the online and cyber worlds, ranging from fraud, identity theft, bullying and other forms of personal harassment or exploitation through to malign social engineering, phishing and hacking attacks which can threaten key networks and even entire nations. A number of prerequisites have to be met to maintain democratic principles i.e. privacy, security, transparency, safety, wellbeing, and accountability. I4ADA will focus on developing instruments for accountability in the Digital Age. Instruments can be traditional, such as new international legislation or international government lead institutes. Or instruments can be more modern such as the creation of an Accountability Index or other digital instruments to measure, track, and/or manage accountability variables. Develop a framework of both measures/indicators as well as metrics for the assessment of accountability on country and/or organization level and provide sources for open and free to use sources that provide the data that are required to make it executable.

Questions that might guide your thinking:
Are there standards, frameworks or metrics in other domains like in physical security, health environment or safety that might guide us? Do you know of initiatives that could be used as a kernel to further develop this framework? Sources for inspiration and guidance:
Questions that might guide your thinking:
Are there standards, frameworks or metrics in other domains like in physical security, health environment or safety that might guide us? Do you know of initiatives that could be used as a kernel to further develop this framework?

Sources for inspiration and guidance:
https://i4ada.org/#charter
https://accesstomedicinefoundation.org/access-to-medicine-index
https://www.weforum.org/projects/partnering-for-cyber-resilience
https://hcss.nl/report/assessing-cyber-security
http://dwh.hcss.nl/apps/gfce_cyber_monitor/
https://stratbase.hcss.nl/apps/cyber_dashboard