Tutorials on Select Topics in Information Security

in conjunction with

18th International Conference on Information Systems Security

December 16 – 20, IIT Tirupati, Andhra Pradesh, India.

♦♦♦

Techniques of Malware Design and Deployment

By Saurabh Sharma, Kaspersky Lab

Duration: 11 hours (hands-on)

MITRE ATT&CK Framework: An Introduction

By Harshal Tupsamudre, Qualys

Duration: 3 hours (hands-on)

Encrypted Traffic Analysis: An Overview

By Debapriyay Mukhopadhyay, Vehere

Duration: 3 hours (hands-on)

Secure Digital Transformation Leveraging the Aadhaar

By Vijayakumar Manjunatha, eMudhra

Duration: 3 hours

Registration can be done at https://icissconf.org

Students: Rs. 4,000 • Academia: Rs. 8,000 • Others: Rs. 12,000

Techniques of Malware Design and Deployment

Saurabh Sharma, Sr. Researcher, Global Research & Analysis Team, Kaspersky Lab

Abstract: Malware (short for malicious software) refers to any program that is deliberately created to perform an unauthorized, often harmful, action. Malware is used in most cyberattacks happening nowadays, be it cybercrime or nation-state cyber warfare. As an example, in a nation-state cyber-attack, a trojan can be used to provide backdoor access to steal sensitive information from a government’s network or disrupt services at national critical infrastructure. Ransomware is another example of destructive malware used to encrypt files on the computer systems of an organization to demand money in return for the decryption of the files. As the political and financial stakes become higher, the sophistication and robustness of both the cyber defence mechanisms and the malware technologies with the respective operation models have also increased therefore it is extremely important to study the techniques behind malware development and deployment in order to better understand cyberattacks and develop effective countermeasures. As the cyber security industry evolved, the malware authors upped their game to remain under the radar by introducing innovative techniques. On the other hand, fundamental development blocks of malware remained unchanged and can be broadly classified into the below categories. The tutorial will be a mix of theory and a live demo of design and deployment techniques observed in real-world attack scenarios.

Modules:
Covert Malware Launching
Data Encoding
Anti-Reverse Engineering
Spear Phishing Attachment
The exploitation of Remote Services
Supply chain attack
Watering hole attack

Prerequisites:
Basic knowledge of C/C++ programming language
Basic familiarity with Intel Assembly language
Knowledge of programming fundamentals for Windows OS
Laptop with Virtualbox running Windows7/Windows 10
Free IDA Pro version https://hex-rays.com/ida-free/

About the Resource Person: Saurabh Sharma is a senior security researcher at the Global Research and Analysis Team (GReAT) in Kaspersky. He contributes to the GReAT team’s mission by helping to investigate the most active and advanced threat actors, targeted attacks, attacker tools, and more. Saurabh’s professional passions include reverse engineering malware, as well as uncovering, tracking, and analyzing APT campaigns, and providing technical reports. Saurabh has previously spoken at various international infosec conferences in India and abroad.

MITRE ATT&CK Framework: An Introduction

Harshal Tupsamudre, Sr. Research Engineer, Threat Group, Qualys

Abstract: MITRE ATT&CK framework is an open source and constantly evolving knowledge base of adversary tactics, techniques, and procedures (TTP) that is based on real-world observations. Many cybersecurity product companies operating in Endpoint Protection (EPP) and Endpoint Detection & Response (EDR) space rely on the information contained within ATT&CK to prevent, mitigate, and detect attacks. Security analysts use ATT&CK data to track techniques of specific advanced persistent threat (APT) groups and malware that are known to target a specific country or sector or platform. Various adversary emulation frameworks have been developed around the ATT&CK framework. ATT&CK provides a common language for both offensive and defensive security researchers. There are four primary use cases of ATT&CK: a) threat intelligence, b) detection and analytics, c) adversary emulation, and d) assessment and engineering. In this tutorial, we will delve into each use case in detail. Along the way, we will learn to map adversary and malware activities to ATT&CK TTP and use different ATT&CK tools that allow us to interact and work with ATT&CK data (e.g., ATT&CK Navigator, STIX API, and Python utilities). We will also run Atomic Red Team, an open-source adversary emulation tool for select ATT&CK techniques on Windows, and detect the emulated techniques using Sysmon, a device driver which can be used on Windows to monitor system activity. We will show that ATT&CK data can be modelled as a graph and we can use graph queries to draw interesting insights about APT groups and malware families. Finally, we will discuss issues encountered while using ATT&CK (e.g., Infrequent Updates, False Positives) and different possible ways to circumvent them.

Modules:
Introduction to MITRE ATT&CK framework
Use cases of MITRE ATT&CK framework
Installation and Usage of Atomic Red Team
Graph-based view of ATT&CK data
Challenges in EDR/EPP

Prerequisites:
Knowledge of common security terminologies
Elementary working of malware
APT (Advanced Persistent Threats) groups

About the Resource Person: Harshal is a Sr. Research Engineer at Threat Research Group of Qualys. He has around 20 research publications and 7 patents. He holds the best thesis award for his MTech thesis at IIT Kharagpur. He regularly contributes to the MITRE ATT&CK framework.

Encrypted Traffic Analysis: An Overview

Debapriyay Mukhopadhyay, Security Consultant, Vehere Technologies

Abstract: This tutorial is aimed to cover a broad area of Cyber Security called Encrypted Traffic Analysis (ETA). But, without understanding SSL/TLS, it is very difficult to proceed with the deep details of ETA. In this tutorial, I propose to cover both in two modules – the first module talks about details of SSL/TLS and the second module shows how that can be used to gain potential visibility information for Network Forensics and Cyber Security.

Modules:
SSL/TLS protocol internals
SSL/TLS traffic analysis using open-source tools

Prerequisites:
Basics of cryptography (symmetric & asymmetric)
Wireshark
TCP/IP basics

About the Resource Person: Debapriyay Mukhopadhyay is currently associated with Vehere Technologies Pvt Ltd as a Security Consultant. He received M.Sc. in Pure Mathematics from the University of Kalyani, India in 1997. He received an M.Tech degree in HRDM from IIT, Kharagpur in 2000, followed by an M. Tech degree in Computer Science from ISI, Kolkata in 2002. He has 19 years of Industry experience working mostly in Network Security, Cryptography and SSL/TLS.

Secure Digital Transformation Leveraging the Aadhaar

Vijayakumar Manjunatha, Chief Technology Officer, eMudhra

Abstract: Aadhaar has become a universal reference as a successful, large-scale, cardless Digital Identity implementation. The scale of the implementation is enormous, not only in the enrolment of a large population but also putting it to use in transforming the country's digital framework and enabling the people in a secure & seamless way to transact with government, businesses, and in their daily life. This tutorial aims at covering certain dimensions of it, its security aspects, as well as how it makes the ecosystem more secure.

Modules:
The first part will introduce the participants to an overview structure of the Aadhaar Ecosystem, including its broader security aspects on how the system is structured to work with state-of-the-art security. This being a sensitive area, the references would be more from the information available in the public domain. It will also cover references to the alternative approaches and the challenges faced by other countries. And also on how other countries are approaching the Aadhaar kind of secure Digital Identity system.

The second part throws detailed insights into how the system enables the ecosystem as a whole in order to bring Digital Transformation to the country. The successful modelling of the ecosystem stack towards paperless (digital signature framework), cashless (Payments framework), and presence-less (Authentication / KYC framework) layers.

The Third part covers more details about Digital Signatures and the importance of Cryptography in effective paperless transformation. It goes deeper into how challenging it is for several countries even with smaller populations, and how India has become successful in paperless layer enablement using the Aadhaar Authentication framework.

The fourth part covers the role of cryptography in digitization, and how various industry transactions leverage cryptographic means to secure transactions like Aadhaar Authentication, Banking, e-payments / UPI, and Tendering / Procurement systems.

The final part is an interactive discussion to benefit students and researchers from both academics and industries, in order to address the open area of thought around the subject.

Prerequisites: None

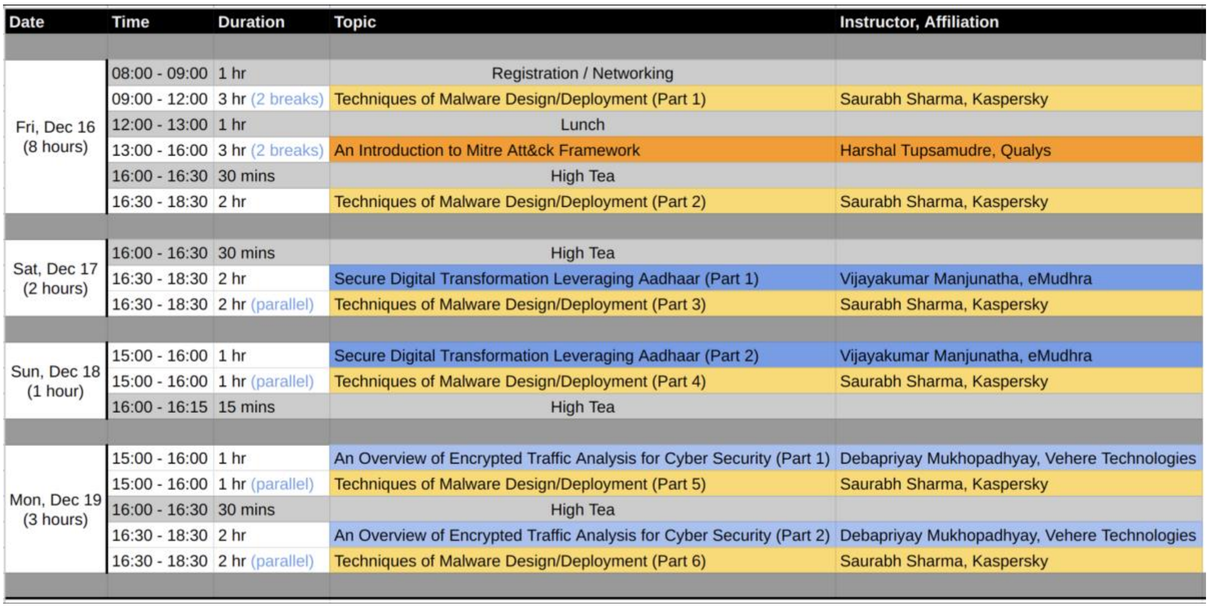
About the Resource Person: Vijayakumar Manjunatha is the Senior Vice President & Head of Technology (CTO) at eMudhra, and with responsibility for Technological Advancements, Engineering & Product Innovations. Vijay is also involved in various advisories & consultations and is an industry expert in the areas of Digital Signatures / Electronic Signatures. With his knowledge & experience in various aspects of technology & business, He fulfils the techno-functional quotient for various national and international projects. He has been part of several white papers and standards document reviews and publications around this space.

Vijay is also the convener and member of the Panel for Digital Signature at the Bureau of Indian Standards (BIS). He is an active member in the cryptographic & PKI domain and works with Asia PKI Consortium, India PKI Forum, CA Browser Forum, and ETSI (ESI). He also engages with several global organizations including FIDO alliance, Microsoft, Google, Mozilla, Apple, and Adobe in these areas. He is also the Chair of the Technology and Standards working group of the Asia PKI Consortium.

Vijay is an expert member of the United Nations UN/CEFACT. In this capacity, he works on several white papers and recommendations for trade facilitation and electronic business (e-Governance Domain).

As an International Expert in the domain, he has delivered talks, tutorials, and lectures at various International Conferences, Research Institutes, and Private/Public Forums. Vijay is instrumental in setting up electronic signature technology (Digital India program). He was closely involved in the Technical Architecture of eSign, with the Information Technology Ministry (MEITY), where eMudhra was the first eSign Service Provider launched in the country with more than 330 million users in a short span of time.

PROGRAM SCHEDULE



Date	Time	Duration	Topic	Instructor, Affiliation
Fri, Dec 16 (8 hours)	08:00 - 09:00	1 hr	Registration / Networking	
	09:00 - 12:00	3 hr (2 breaks)	Techniques of Malware Design/Deployment (Part 1)	Saurabh Sharma, Kaspersky
	12:00 - 13:00	1 hr	Lunch	
	13:00 - 16:00	3 hr (2 breaks)	An Introduction to Mitre Att&ck Framework	Harshal Tupsamudre, Qualys
	16:00 - 16:30	30 mins	High Tea	
	16:30 - 18:30	2 hr	Techniques of Malware Design/Deployment (Part 2)	Saurabh Sharma, Kaspersky
Sat, Dec 17 (2 hours)	16:00 - 16:30	30 mins	High Tea	
	16:30 - 18:30	2 hr	Secure Digital Transformation Leveraging Aadhaar (Part 1)	Vijayakumar Manjunatha, eMudhra
	16:30 - 18:30	2 hr (parallel)	Techniques of Malware Design/Deployment (Part 3)	Saurabh Sharma, Kaspersky
Sun, Dec 18 (1 hour)	15:00 - 16:00	1 hr	Secure Digital Transformation Leveraging Aadhaar (Part 2)	Vijayakumar Manjunatha, eMudhra
	15:00 - 16:00	1 hr (parallel)	Techniques of Malware Design/Deployment (Part 4)	Saurabh Sharma, Kaspersky
	16:00 - 16:15	15 mins	High Tea	
Mon, Dec 19 (3 hours)	15:00 - 16:00	1 hr	An Overview of Encrypted Traffic Analysis for Cyber Security (Part 1)	Debapriyay Mukhopadhyay, Vehere Technologies
	15:00 - 16:00	1 hr (parallel)	Techniques of Malware Design/Deployment (Part 5)	Saurabh Sharma, Kaspersky
	16:00 - 16:30	30 mins	High Tea	
	16:30 - 18:30	2 hr	An Overview of Encrypted Traffic Analysis for Cyber Security (Part 2)	Debapriyay Mukhopadhyay, Vehere Technologies
	16:30 - 18:30	2 hr (parallel)	Techniques of Malware Design/Deployment (Part 6)	Saurabh Sharma, Kaspersky

--
With Best Regards from
The Tutorial & PhD Forum Co-chairs of the ICISS 2022
Shachee Mishra, IBM Research
Vishwas Patil, IIT Bombay
Jayanarayan Tudu, IIT Tirupati.