One Week GIAN Course on

Incident Handling and Forensics

(December 11-15, 2017)

1.0 Overview

The pervasive interconnectivity of systems (e.g. cloud computing and Internet of Things) used in our Internet-connected society can potentially be, and have been, exploited by actors with malicious intents, ranging from cyber criminals acting alone to organized groups of financially-, criminally- and issue/ideologically-motivated crime groups to state-sponsored actors. It is not surprising that information security incidents are increasing in both number and the level of sophistication. For example, Symantec Corporation reported that more than 430 million new types of malware were discovered, the number of spear-phishing attacks targeting employees increased 55 percent, and crypto-style ransomware grew 35 percent in the fiscal year 2015. Of note, the report highlighted that security incidents moved to new targets such as smart phones, Mac and Linux systems, and cloud computing environments.

The increasing trend of organizations moving sensitive data to cloud infrastructure has resulted in an urgent need to ensure that security and privacy safeguards are in place, as cloud services are potential criminal targets due to the amount of sensitive organizational data stored in the cloud. As surveyed by the Cloud Security Alliance in 2016, industry experts identified 12 critical issues to cloud security with data breaches, poor credential management, and insecure application programming interfaces (APIs) being the top three. A proactive incident handling strategy is one key approach to mitigating risks to the confidentiality, integrity and availability (CIA) of assets, as well as minimizing loss (e.g. financial, reputational and legal) in a dynamic cloud environment.

Existing information security incident handling strategies, however, may not be adequate as cloud data would generally be virtualized, geographically distributed and ephemeral, presenting both technical and jurisdictional challenges. This is consistent with CSA's report entitled 'Security Guidance for Critical Areas of Focus in Cloud Computing', which highlights three critical focus areas, namely Incident Response, Notification and Remediation (Cloud Security Alliance 2011).

In investigating and responding to computer security incidents, digital forensics can play a crucial role. Forensic tools and techniques are not only useful for criminal prosecution in a court of law, but also for various other tasks within an organization, such as event reconstruction (i.e. who, what, when, where, how, and why an incident took place), data or system recovery, and system operation troubleshooting. Similarly, incident handling is not only for responding to incidents, but more importantly, identifying the root causes to prevent similar breaches from reoccurring. Therefore, incorporating forensically sound practices in an incident handling strategy would support cloud service users to be better prepared, more proactive, and forensically ready when analyzing an incident.

For more details, please visit GIAN cell at http://mnit.ac.in.

2.0 Dates/Deadlines

Course Duration: Dec. 11-15, 2017

Last Date for Registration: Dec. 4, 2017

3.0 Objectives

The primary objectives of this course are as follows:

i) Introduce participants to the cyber threat landscape and situational awareness
ii) Introduce participants to the fundamentals of incident response and handling practices,
iii) Introduce participants to the fundamentals of forensic investigation practices
iv) Enhance the capability of the participants to identify, control and remove asset management-related problems in engineering system.

4.0 Who can attend

- Executives, engineers and researchers from manufacturing, service and government organizations including R&D laboratories.
- Scientists/Security professionals from government organizations including R&D laboratories.
- Faculty from reputed academic institutions and technical institutions.
- Students at all levels (BTech/MSc/MTech/PhD)

5.0 Lectures/Modules

- Definitions and types of cyberthreats, Cyberthreat actors and motivations, Potential attack vector, and potential targets, particularly in under-explored sectors that can have cascading effects due to interdependencies between (the critical infrastructure) sectors
- What are the security risks of popular consumer technologies to organizations? Risk management, and Incident response and evidence collection
- Cloud Security: DDoS attack solution space
- Risk management, and Incident response and evidence collection
- Digital forensics fundamentals
- Digital forensics challenges (e.g. contemporary technologies such as cloud and mobile)
- Secure Deletion on Solid State Drives
- Digital forensics
- Volume and partition analysis
- VM Appliance Security and Vulnerability removal
- Volume and partition analysis
- Mobile App Analysis: A Case Study Tutorial
- File system analysis: FAT and NTFS
- File deletion and recovery
- KKRC Signature and hash analysis
- File deletion and recovery, and Signature and hash analysis

5.2 Registration Fees: **GIAN Portal registration fee: Rs 500 (mandatory for all participants).**

Registration to the GIAN portal is one time affair. Once registered in the portal, an applicant will be able to apply for any number of GIAN courses as and when necessary. One time Non---refundable fee of Rs.500/- is to be charged for this service. Please also note that mere registration to the portal will not ensure participation in the courses. The course coordinator has the final say on the selection of participants. This is NOT course participation fee. The candidate has to pay course participation fee as per directive from the course coordinator/host Institute to the local Institute only. You are required to apply online using the following steps:

1. Create login and password at http://www.gian.iitkgp.ac.in/GREGN/index
2. Login and complete the Registration Form and select Course(s)
3. Confirm application and pay Rs.500/--- (non---refundable) through online payment gateway.
4. Download “pdf file” of the application form and email it to the Course Coordinator (gaurms@mnit.ac.in and gaurav@curaj.ac.in).

Course participation fee

• Participants from abroad	:	US $100
• Industry/Research Organizations/PSU	:	Rs. 5000/-
• Faculty members from Academic Institutios	:	Rs. 4000/-
• Research Scholars/Students from Academic Instititions*	:	Rs 2000/-
• Faculty/Students from IIIT Kota*	:	Rs 2000/-
• Faculty/Research Scholars/PG students (MNIT)	:	NIL
• Undergraduate students (in final year) (MNIT)	:	NIL

* The above fee includes all instructional materials, computer use for tutorials and lab sessions, free Internet facility in lecture hall and lab space. The participants will be provided with accommodation, if available, on payment basis.

5.2 Fees Payment

1. Fees may be paid via Demand Draft in favor of “REGISTRAR (SPONSORED RESEARCH) MNIT Jaipur” payable at Jaipur.

OR

Fees can be paid through National Electronic Funds Transfer (NEFT) Account No. : 676801700388 In name of “REGISTRAR (SPONSORED RESEARCH) MNIT Jaipur” , Bank : ICICI Bank, Branch MNIT Jaipur IFSC Code: ICIC0006768. **Preferred mode of registration is Demand Draft.**

2. Email filled in “Registration Form”, scan copy of “Demand Draft/ NEFT Transaction Receipt” and pdf file (downloaded from GIAN Portal Registration) to gaurms@mnit.ac.in and gaurav@curaj.ac.in. **Please mention “GIAN (Incident Handling and Forensics) in Subject and email on/before December 4, 2017.**

6.0 The Faculty

6.1 Prof. Kim-Kwang Raymond Choo:

Prof. Kim-Kwang Raymond Choo holds a Ph.D. in information technology from Queensland University of Technology, Australia, and a Graduate Diploma in Business Administration from The University of Queensland, Australia. Prior to starting his Cloud Technology Endowed Professorship at UTSA, Professor Choo spent five years working for the University of South Australia, and five years working for the Australian Government Australian Institute of Criminology. He was a visiting scholar at INTERPOL Global Complex for Innovation (October’15 to February’16), and a visiting Fulbright scholar at Rutgers University School of Criminal Justice and Palo Alto Research Center (formerly Xerox PARC) in 2009.

Prof. Choo’s areas of research include cyber security and digital forensics. He has co-edited six books entitled “Cloud Security Ecosystem” (published by Syngress: An Imprint of Elsevier, 2015), “Mobile Security and Privacy” (published by Syngress: An Imprint of Elsevier, 2017), “Contemporary Digital Forensic Investigations of Cloud and Mobile Applications” (published by Syngress: An Imprint of Elsevier, 2017), “Green, Pervasive, and Cloud Computing” (published in Springer’s Lecture Notes in Computer Science book series, 2017), “Algorithms and Architectures for Parallel Processing” (published in Springer’s Lecture Notes in Computer Science book series, 2017), and “Advanced Multimedia and Ubiquitous Engineering” (published in Springer’s Lecture Notes in Electrical Engineering book series, 2017). He has co-authored a number of publications in the areas of cyber security, and digital forensics including a book published in Springer’s “Advances in Information Security” book series, a book published by Syngress/Elsevier (Forewords written by Australia’s Chief Defence Scientist and Chair of the Electronic Evidence Specialist Advisory Group, Senior Managers of Australian and New Zealand Forensic Laboratories), seven Australian Government refereed monographs, 30 refereed book chapters, 251 refereed journal articles, 100 refereed conference articles and six parliamentary submissions.

He is the co-inventor of two PCT and one provisional patent applications on digital forensics and mobile app security filed in 2015. Since 2011, Professor Choo has supervised to completion 15 Ph.D. and 13 masters theses. In 2016, he was named Cybersecurity Educator of the Year APAC. In 2015, he and his team won the Digital Forensics Research Challenge organized by Germany’s University of Erlangen-Nuremberg. He is also recipient of a number of awards, such as ESORICS 2015 Best Research Paper Award. In April 2017 he was appointed an Honorary Commander, 502nd Air Base Wing, Joint Base San Antonio-Fort Sam Houston, USA. He is also a Fellow of the Australian Computer Society and a Senior Member of IEEE.

6.2 Prof. MS Gaur (Course Coordinator)

Dr. Manoj Singh Gaur assumed charge of Director, Indian Institute of Technology, in June, 2017. Prior to joining IIT Jammu he was a Professor and Head of the Department of Computer Science and Engineering at Malaviya National Institute of Technology Jaipur, India. Additionally, he was Professor In Charge (Coordinator) of IIIT Kota, which is currently mentored by MNIT Jaipur. He has been Dean (Students) and Head, Central Computer Centre at MNIT Jaipur as well. He also served as Chairman, Senate UG Board at MNIT Jaipur. He completed his Master's degree in Computer Science and Engineering from Indian Institute of Science Bangalore and PhD from University of Southampton.

In his teaching and research career, he has been Investigator of a number of funded research projects in the area of Information Security and Networks on Chip. He has been part of core group of Project ISEA which is a major multi Institutional project in the domain of Information Security. His current research areas include Computer and Network Security (Network Attack Models and Countermeasures), Mobile Platform Security, Cloud Security, Malware Analysis, Networks-on-Chip, and SDN. He has published more than 170+ papers in reputed journals and conferences. He has also contributed a number of contributed book chapters.

He has a number of funded international collaborations with many countries. He has supervised sixteen PhDs till date and currently twelve research scholars are working in his research group. He has served technical program committees of many IEEE/ACM conferences and is a contributing reviewer of a number of ACM/IEEE/Elsevier/IET/Springer journals.

6.3 Gaurav Somani (Course Coordinator)

Gaurav Somani is an Assistant Professor at Department of Computer Science and Engineering, Central University of Rajasthan, India. His research interests include Distributed Systems and Security Engineering. He has published number of papers in various conferences and journals of international repute and reviewer of many top journals. Some of his top papers are published in highly reputed journals such as Computer Networks, Annals of Telecommunications, IEEE Cloud Computing, Computers and Electrical Engineering, FGCS and IEEE Cloud. He has written a book on “Scheduling and Isolation in Virtualization" which is published by VDM Verlag Dr. Muller Publishers, Germany. This book is used as a text/reference book in some graduate level programs across the globe. He has also co-authored another book on “Research Advances in Cloud Computing” published by Springer, Singapore which will be available in the market by April-May 2017. He has been a reviewer of many top journals in security and distributed systems. He is also a part of multiple international conferences across the globe where he has played a role of TCP member, sessions chair and the speaker. He was the keynote and the tutorial chair at the ICISS 2016. He is a member of IEEE and ACM.

Course Coordinators

1. Prof. Manoj Singh Gaur (Coordinator)
   Professor, Department of Computer Science and Engineering
   Malaviya National Institute of Technology
   JLN Marg, Jaipur – 302017, India.
   Tel: +91 0141 2713227 (O)
   Email: gaurms@mnit.ac.in

2. Gaurav Somani
   Assistant Professor
   Computer Science and Engineering
   Central University, Rajasthan
   Email: gaurav@curaj.ac.in