Cybersecurity Laboratory's Security Day

Venue: LT F, HKUST

Date: Nov 19, 2016

Session 1 (1:30PM-2PM).
Official opening of the lab, photo taking at the lab.
Opening remarks in LTF by **Prof. Yang Qiang**, CSE department head, **Prof. Tim Cheng**, Dean of engineering school and **Mr Charles Mok**, Member of Hong Kong Legislative Council.

Session 2 (2PM-2:40PM).
Introduction by cybersecurity lab researchers by **Prof. Ding Cunsheng, Prof. Wang Tao** and **Dr. Nicole Fern**, CSE Department.

Moderator: Prof. Charles Zhang, Director, Associate Professor, CSE Department

Title 1 (2:10PM-2:20PM): Hardware Security: Identifying Vulnerabilities in Unspecified Functionality

Abstract
Traditional verification methods and metrics attempt to answer the question: does my design correctly perform the intended functionality? This talk will look at hardware verification from a security perspective, which demands the verification effort answer an additional question: does my design perform malicious functionality in addition to the intended functionality? This talk will motivate through examples why malicious design modifications, known as Hardware Trojans, altering only unspecified design functionality are both powerful and stealthy and provide an overview of the techniques our group has developed to address this threat.

Speaker: Nicole Fern

Biography
Nicole Fern received her undergraduate degree in Electrical Engineering from The Cooper Union for the Advancement of Science and Art and her PhD degree in the ECE department at UC Santa Barbara under the advisement of Professor Tim Cheng. She is now a post-doc at UC Santa Barbara and a Visiting Scholar at Hong Kong University of Science and Technology. Her research interests include hardware verification and security.

Title 2 (2:20PM-2:30PM): Walkie-Talkie: An Efficient and Effective Website Fingerprinting Defense

Abstract
Website fingerprinting (WF) is a traffic analysis attack that allows an eavesdropper to determine the web activity of a client, even if the client is using privacy technologies such as proxies,

VPNs, or Tor. Recent work has highlighted the threat of website fingerprinting to privacy-sensitive web users. Many previously designed defenses against website fingerprinting have been broken by newer attacks that use better classifiers. In this talk we will discuss Walkie-Talkie, an effective and efficient website fingerprinting defense that cannot be defeated by any website fingerprinting attack. Walkie-Talkie modifies the browser to communicate in half-duplex mode rather than the usual full-duplex mode.

Speaker: Wang Tao

Biography
Tao Wang joined the Cybersecurity Lab at HKUST as an Assistant Professor in 2016. His research is in security and privacy, with a special focus on web privacy and anonymity networks. Tao Wang received his Ph.D. at the University of Waterloo, having been awarded the Ontario Graduate Scholarship for his research.

Title 3 (2:30PM-2:40PM): My Past and Current Research

Abstract
In this talk, I will introduce my past and current research interests briefly.

Speaker: Ding Cunsheng

Biography
Cunsheng Ding was educated at Shaanxi Normal University (China), The Northwestern Telecommunications Engineering Institute (China), The Karlsruhe Institute of Technology (Germany), and The University of Turku (Finland). His education has a background in physics, computer science and mathematics.

Dr. Ding was a lecturer of mathematics for four years at Xidian University, China; and an assistant professor of computer science for three years at The National University of Singapore, Singapore. Since 2000 he has been with the Computer Science and Engineering, The Hong Kong University of Science and Technology.

Session 2 (2:40PM-4:20PM)
Industrial talks, 20 mins each including Q&A.

Title 1 (2:40PM-3:10PM): Introduction to the HKUST Firebird CTF team, Capture The Flag (CTF) Game, Cyber Security and Research

Abstract
Other than learning from textbook about security or reading one's paper, we advance our skills via joining Capture The Flag games. There are numerous prominent CTF teams in this planet and we have played CTF since 2010.

In this talk, we will brief about CTF, how the game could be beneficial to the development of skills, cybersecurity and research area as well as impact on the world. We may walk through simple challenges so that you could realize the importance and fun behind.

Speaker: Anthony Lai (*VXRL, Affiliated Member*), Ping Fan KE (a.k.a. Zetta) (*VXRL, Affiliated Member),* Alan Ho (*Knownsec*)

Biography:
Anthony is with hybrid experience in application development, code security, penetration test and threat analysis areas for 13 years. He has done vulnerability assessment, penetration, IT audit and training for government and various corporates. He is now a lead consultant and guest threat advisory of several MNCs. He is currently a part time PhD student supervised by Dr. Jogesh Muppala, focus on threat and malware analysis and attack profiling. Anthony published research in Blackhat USA, DEFCON as well as Hack-In-Taiwan and has set up a security research group called VXRL (www.vxrl.org). He is the chairman of OWASP (HK Chapter) and is the mentor of SANS course including GREM and GXPN holder. He is passionate over Capture The Flag (CTF) games since 2011.

Zetta is a security researcher of Valkyrie-X Security Research Group (VXRL), a non-profit organization for information security research in Hong Kong. He has experience in web application security and cryptography. He also actively participates in worldwide Capture the Flag (CTF) game. He is currently a PhD student in the Department of ISOM at HKUST, and his research focus is on economics of security.

Alan Ho is passionate over Web hacking, Application security and various research. He is now working as a Web Application Security consultant. He got experience in development, penetration test, incident response, security operation planning and investigation. He is a certified as an OSCP, also a SANS GWAPT Holder and published the SANS Gold Paper - “Website Security For Mobile”. He is also the VXRL security researcher and CTF crew member.

Title 2 (3:10PM-3:30PM): Contemporary Issues in Penetration Testing

Abstract
In recent years, it is not difficult to find hacking events, security incidents, or security breaches etc. on daily news. The introduction of cybersecurity fortification initiative has been set out from Hong Kong Monetary Authority, which purpose is to give out a new testing framework for financial institutes to reduce cyber risks. Intelligence-led cyber attack simulation testing (iCAST) is one of major components as well as a new challenge to these financial institutes. Unlike traditional penetration testing, it merely focuses on individual systems or applications (technical assessment). iCAST is more like an all-in- one suite in which it covers story lines, test goals, and information from cyber threat intelligence. The way to satisfy the requirement from HKMA becomes an important issue to the institutes. In this talk, we are trying to answer this question as a point of view from a pentester.

Speaker: Timture Choi, *Security Consultant NTT Security*

Biography
Timture Choi has mastered several skill sets in information security and education sectors. He is now a security consultant at the one of the leading IT security companies. His major role is a pentester to carry out different type of assessments for his clients. Before that, he had been working in the one of leading universities in Asia (HKUST) for 10 years. He had been involved in teaching a number of PG/UG courses in computer security, computer programming, vulnerability assessment, risk management, penetration testing, forensic investigation, IS auditing and IT governance.

His research interests are wired/wireless IDS/IPS, ethical hacking techniques, information security auditing, prime number seeking, ICT in education, and educational psychology.

Title 3 (3:30PM-3:50PM): My Security Dairy: Case Study and Funny Sharing

Abstract
Doris will share the latest cyber security incidents happened in the Banking and Finance industry (with the sensitive information hidden of course!), and how the latest emerging threats and regulatory compliance requirement changes industry’s top of mind in Cyber Security.

Speaker: Ms Doris CHAN, *Consulting Engineer, CISCO Systems*

Biography
Doris Chan has been working at Cisco as 9 years and is currently a Consulting Engineer & Field Advisor for Cisco Hong Kong and Macau. She works with Cisco’s large and strategic clients in Banking and Finance in the region, designing network and security architectures.

As Field Advisor, she is also actively involved with Cisco’s product teams providing advice on the security strategy and product futures. Prior to joining Cisco, Doris has worked for SITA and Dimension Data as Solution Architect.

Title 4 (3:50PM-4:10PM): Game Security Exposed

Abstract
Reveal a Game Security workflow and technique its involves, talk about how can protect a virtual asset by our knowledge as a security researcher.

Speaker: Kelvin Chan, *Security Researcher, Tencent*

Biography
Kelvin Chan, former Windows kernel & Games security researcher. and I am currently working in department of Game Security Research and Development in Tencent. for seven years, also as guest speaker in VXCON, and joined a VXRL as a member. I also engaged in Online Games

Security (i.e. Direct-X, kernel, and CPU architecture) for both making and defensing game cheats. Also, I began researching on Intel Virtualization Technology extension for security purposes since 2014. And also has a open-source nested-virtual machine monitor project which is available on github now.

4:10PM-4:30PM. tea break.

Session 3 (4:30PM-5:50PM)
Industrial talks, 20 mins each including Q&A.

Title 1(4:30PM-4:50PM): Internet of Threat (IOT)

Abstract: The way that smart devices are getting more popular has potentially exposed users to much more cyber threats than before. Hackers can easily initiate DDOS attacks with IOT botnet and create huge amount of traffic to overload hosting servers. These recent cyberattack cases, its influence and preventive measures will be covered.

Speaker: Mr. Eric FAN, *Convener of Information Security & Councillor, Hong Kong Information Technology Federation*

Biography
Mr. Eric Fan graduated from the Staffordshire University major in Information System and is currently working in UDomain Web Hosting Company Limited as the Head of Technical Department. He has more than ten years' experience in the Information and Technology industry and leading the change of UDomain to become one of the market leaders in the web hosting industry. He is also the director of New Sky Internet Ltd and leading the company awarded the Fast Growing Company in Hong Kong Network and Top System Engineer in 2010 Award by Juniper Network. He has participated the leading edge information technologies and architectures which include information security, network monitoring and management, storage, virtualization, Internet architecture and network solutions for Enterprises and Service Providers. Currently, Eric is holding a number of public offices, including Vice Chairman in External Affairs of Professional Information Security Association (PISA), Convenor of Mobile and NGN Security Specialist Group, a member of the executive committee of Hong Kong Wireless Technology Industry Association (HKWTIA), and a member of Radio Spectrum and Technical Standards Advisory Committee (SSAC) under the Hong Kong government. He strives to promote wireless security and to protect SMEs in Hong Kong from being hacked.

Title 2 (4:50PM-5:10PM): Security Audit as a Profession

Abstract
In this age of rampant cyber crimes, security auditors today have a lot of expectations placed upon them. With technologies and new economies enabled people to conduct businesses in ways previously unthought of, so did auditors' scope and depth of review keep breaking new grounds.

As a result, demands for auditors with strong IT infrastructure and/or system development backgrounds are greater than ever. How then, should IT practitioners prepare themselves to enter the profession?

This talk will answer that question by presenting a broad overview of industrial best practices for the delivery of professional security audit services, as well as the knowledges, skills, abilities and qualifications required for professional competence.

Speaker: Alan Chung, *TransPerfect Legal Services*

Biography
Alan Chung has over 12 years hands-on experience in IT Security in wide range of roles from advisory manager in a Big 4, to in-house IT Risk Auditor in an investment bank, to Professional Service Consultant in a top-tier security product vendor and consultancy firm. His areas of expertise lie in Network Security, IT Audit, Ethical Hacking, Penetration Test, Incident Response, Computer Forensic, as well as Firewall Configuration & Review.

Alan is a defense infrastructure expert, an insatiable seeker of knowledge that insists on rooting out the deepest technical secrets of all things. Armed with across-the-board insights on commercial solutions, Alan was responsible for the original infrastructure build-out for a great many multi-million-dollar big-name companies.

He has presented at PacSec Tokyo 2013 Conference a talk on “Bypassing DDoS Mitigation”, DEF CON 20 a talk on “DDoS black and White Kungfu Revealed”, and at the 6th Annual HTCIA Asia-Pacific Conference a workshop titled “Network Attack Investigation”. Alan also contributed to research projects presented in DEF CON 21 and Black Hat USA 2013.

Alan is holder of CFE, CISA, GNFA and GREM. He received two masters degrees from The Hong Kong University of Science and Technology, namely MSc in Telecommunications and MSc in Engineering Enterprise Management. He is a member of HTCIA, ACFE and IEEE.

Topic 3 (5:10PM-5:30PM): The Business of Cyber Crime Investigations

Abstract
The art and science of crime fighting have remained elusive to ordinary people. Specific examination methods and tools such as computer forensics and e-discovery are fairly commonly available, but they are merely means to achieve specific tasks in an investigation, which is a much broader discipline that includes many different elements, each requiring different tools and techniques to tackle.

This talk given by a veteran cyber crime fighter Albert Hui, a modern-day Sherlock Holmes, will shed light on how such elusive practice is offered at a professional level, the best practice methodologies adopted by multinational investigation firms and consultant investigators alike.

Speaker: Albert Hui, *Security Ronin*

Biography
Albert Hui is a security expert with over twenty years of experience in the industry. Having spent years breaking and protecting IT systems for investment banks, government and national critical infrastructures, he is most adept in securing sensitive mission-critical systems. As a testament to his versatility and ability to present technical risks in business terms, he has served in a technical advisory capacity at the group level during the RBS-ABN AMRO merger, as well as managed Asia-Pacific cyber threat response at Morgan Stanley.

Ever a thought leader, Albert has spoken at Black Hat, ACFE Fraud Conference, HTCIA Forensics Conference, GIR Live Hong Kong and Economist Corporate Network. He takes great pride in having co-designed the original cyber forensics curriculum for the Hong Kong Police Force. Having conducted numerous forensic examinations and fraud investigations on both civil and criminal matters over the years, Albert is a cyber forensics expert witness recognized by courts of law in multiple jurisdictions.

Albert is an advisory board member of the SANS GIAC Program, and executive committee member of IEEE Computer Society Hong Kong Chapter. On top of professional qualifications GREM, GCIH, GCIA, GNFA, GCFA, GCFE, GPEN, GXPN, GAWN, GSNA, GSEC, CISA, CISM, and CRISC, Albert holds a Master of Philosophy in Computer Science from the Hong Kong University of Science and Technology, where he is a former lecturer and now a convocation standing committee member.

Topic 4 (5:30PM-5:50PM): Finding software defects and vulnerabilities with Pinpoint

Abstract
Software quality assurance and security auditing is often a labor intensive work even for skilled persons. Our passion is using algorithms to find and explain software defects and vulnerabilities fully automatically. We are building a tool Pinpoint at Sourcebrella Inc, a startup that focuses on building automatic tools for verifying correctness of industry size software systems. In this talk, I will show how Pinpoint can help industry practitioners and briefly introduce the key designs of Pinpoint.

Speaker: Xiao Xiao

Biography
Xiao Xiao obtained his PhD from Hong Kong University of Science and Technology in 2016. His research focuses on developing efficient and scalable analysis methodologies to uncover code properties for industry-scale software. Particularly, he did five years of study on pointer analysis theory, algorithms, applications, and published papers on all major PL&SE top venues. From Oct. 2014, he launched the Pinpoint project to develop next-generation program verification tool that emphasizes the verification of pointer intensive programs. Later, he co-founded Sourcebrella Inc. to commercialize Pinpoint.

Session 4 (5:50PM-6:30PM)
Discussion about Security Industry
Moderator: Ricci IEONG, Adjunct Assistant Professor, CSE Department

Topic 1 (5:50PM-6:10PM): UST alumni in Security Industry

Abstract

HKUST is the nest of security experts. Many of our HKUST alumni are working in the security industry. So Ricci arranged a forum discussion with a number of UST alumni who participated in Hong Kong Security Industry to discuss on the following topics:

How they started to participate in the industry? What are the hot topics in the security industry? What is/are missing from current Hong Kong security market? What university in Hong Kong can help Hong Kong security industry?

Topic 2 (6:10PM-6:30PM): How to switch from fresh grad to security specialist

Abstract

As the nest of security experts for over 20 years, many of HKUST alumni not only participated but also drive the security industry in Hong Kong. However, as industry practitioner, Ricci found that university fresh graduate may not be able to fit well into the Security Industry. So Ricci invited a number of HKUST alumni who graduated from different year to discuss together to explore how current fresh graduate can better fit into the Security industry:

How our alumni started to go into Security Industry? Why they wish to work in this industry? What they think they need to prepare themselves for this security work? What is the "one thing" they consider students should do before they can find a security work?