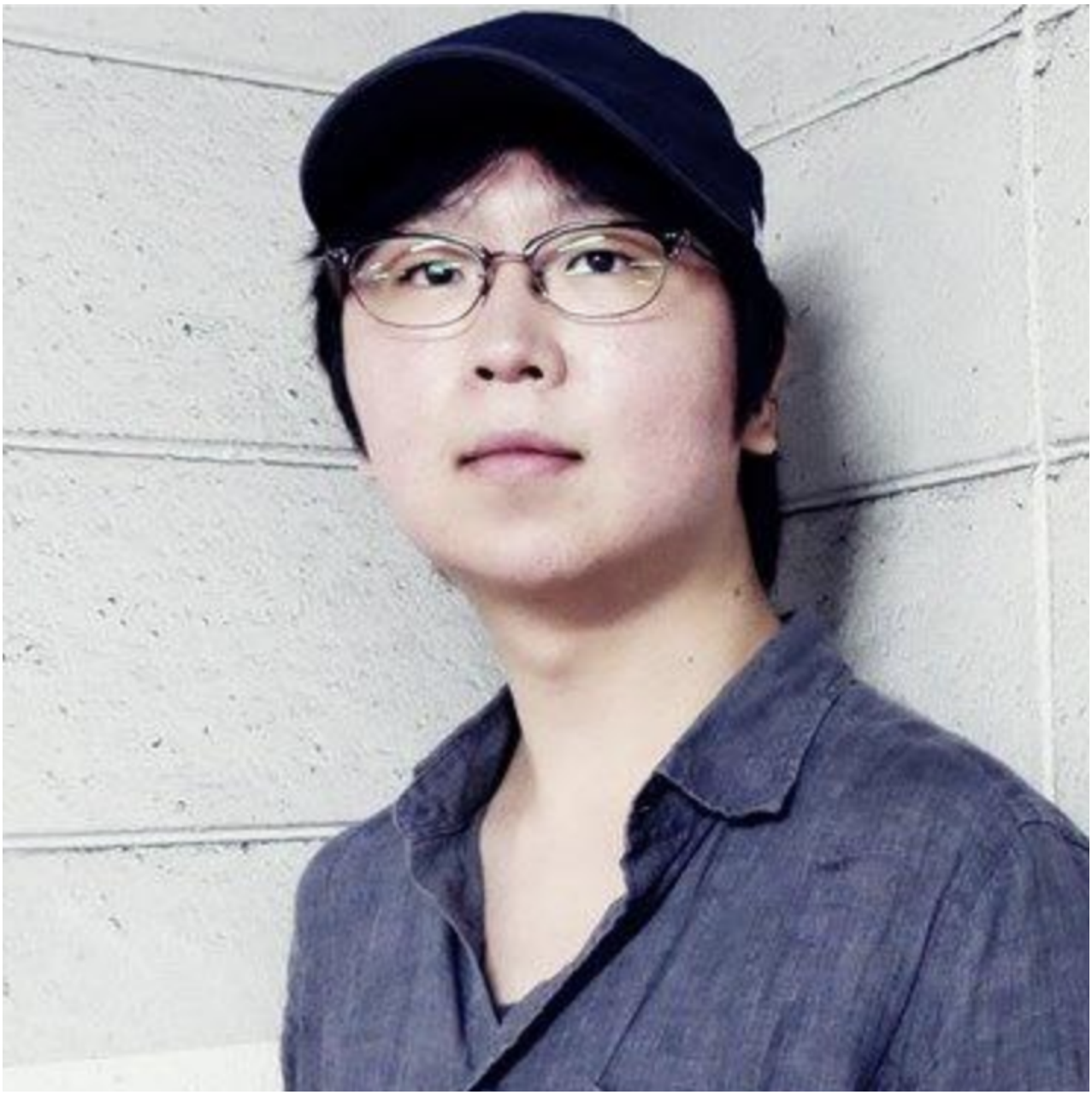
Speakers 2019

typhooncon.com/typhooncon-2019/speakers



SeungJin Lee
Louis Hur

Alexander Liskin

Altaf Shaik

Ben Sparkes

Boris Larin
Brandon Azad

James Lee

Jeremy Fetiveau

Ki Chan Ahn

Kirils Solovjovs

Paolo Stagno
Ravishankar Borgaonkar

Seunghun Han

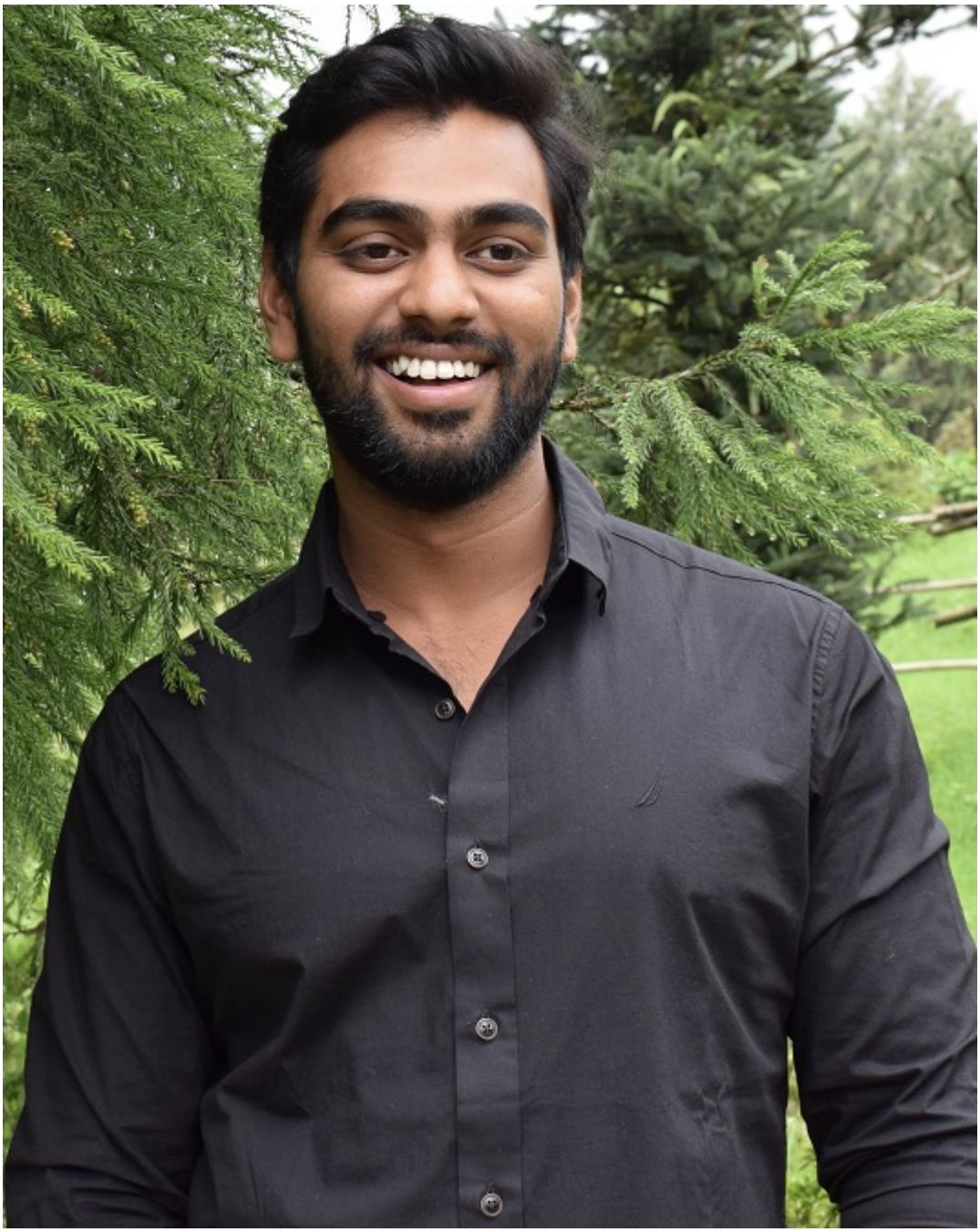
Siguza

Valentina Palacin

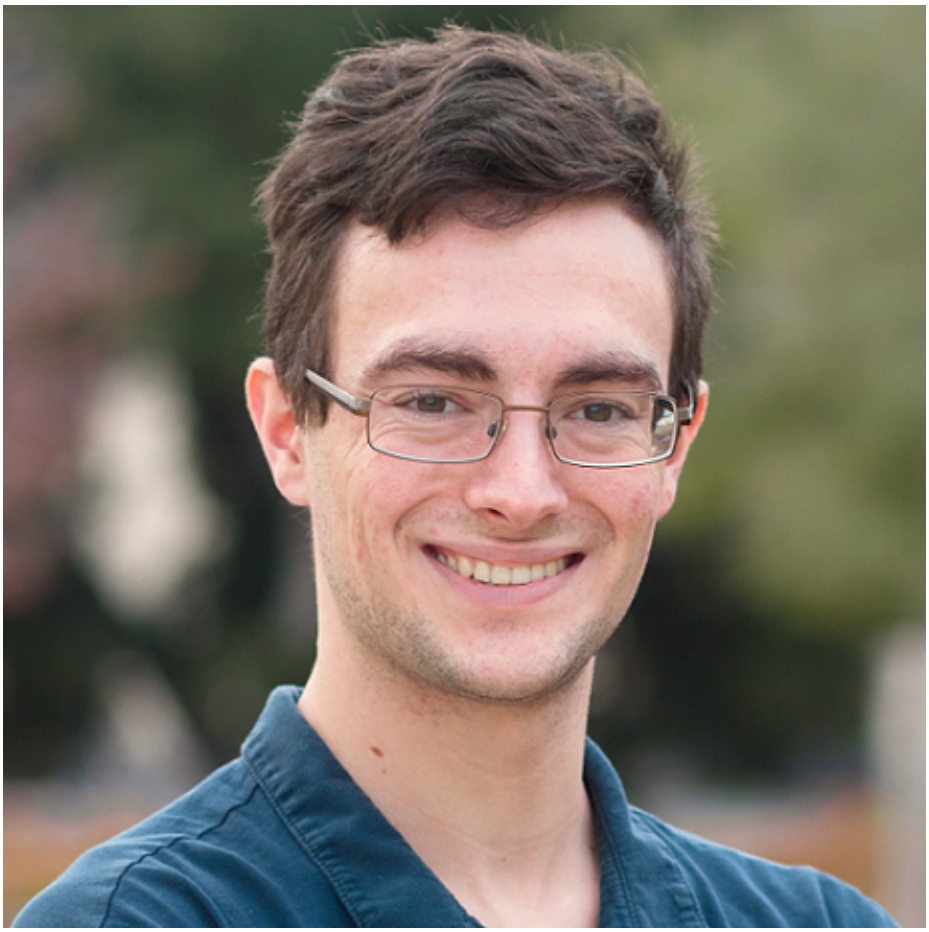
Yang Zhang

Yongtao Wang

Zhi Zhou




NEW YORK CITY
MANHATTAN
BRONX
BROOKLYN
QUEENS
STATEN ISLAND



Keynote Speakers

SeungJin Lee / @Beist

A journey from a geeky young hacker to an executive — Leading a security team at a big firm and how it can be better

Bio – Beist has been a member of the IT security field since 2000. His first company was Cyber Research based in Seoul, South Korea and first focused on pen-testing. He then got a Computer Engineering B.A. degree from Sejong University. He has won more than 10 CTF hacking contests in his country as well as passed DefCon quals 5 times. He has run numerous security conferences and hacking contests such as SECUINSIDE and CODEGATE in Korea. Also, he has given talks at BLACKHAT Las Vegas, SYSCAN, CANSECWEST, AVTOKYO, HITCON, SECUINSIDE, EDSC, and TROOPERS. Hunting bugs and exploiting them are his main interest. He was one of GRAYHASH company founders. Now, he's a lead of GRAYLAB security at LINE in Korea.

Abstract – I will share my career journey starting from a 16 years old hacker, voyaging through working for Korean Cyber-Command, being an entrepreneur and currently going on as an executive in a big corporate. This fantastic story will include my challenges and sufferings as a researcher of different levels and roles. It'll also include my experiences during creating and operating a startup company, funs and borings, and how we got to join LINE. Finally, I'd like to share what security teams are responsible for in big corporations, and what we have thought of to do an even better job.

Louis Hur / @Louishur

Bio – Louis Hur is the CEO and founder, for NSHC Inc, one of the top Korean Information Security Company. With more than 15 years of experience as an information security specialist in penetration testing, bug hunting, malware analysis, and cyber-espionage.

He is an author for both IOS Forensic Analysis and Security Guide book for CISO. Louis Hur is also involved as a team leader for 3.20 Korea Cyber Terror Response Team and had presented as a speaker in Black Hat, HTICON, ISEC, and CSS.4.

Speakers

Altaf Shaik, Ravishankar Borgaonkar / @raviborgaonkar

New attacks targeting 5G networks

Bio – Altaf Shaik is a principal security researcher at Kaitiaki Labs and currently pursuing PhD at the Technical University of Berlin. He is experienced in analyzing cellular network technologies from radio to networking protocol layers. His recent renowned research includes low-cost 4G IMSI catchers and security issues in several cellular baseband chipsets.

Bio – Dr. Ravishankar Borgaonkar works as a research scientist at Sintef Digital and undertakes research in securing next generation digital communication. His primary research themes are related to mobile telecommunication and involved security threats. This ranges from 2G/3G/4G/5G network security to end-user device security. After receiving his PhD in 'security in telecommunication' area from the technical university of Berlin, he was a security researcher at Deutsche Telekom's lab for 3 years. Since that time he has worked for Intel Collaborative Research Institute for Secure Computing at Aalto University, as well as for the University of

Oxford. He has found several protocol flaws in 3G/4G technologies. The demonstrated vulnerabilities affected billions of 3G/4G devices and resulted a change in the existing 3G/4G communication standards.

Abstract – 5G mobile networks are around the corner and boast with revised security features from 4G. After a practical investigation, we bring to light a new set of vulnerabilities in the 5G/4G protocols and their network operations. Using an inexpensive radio toolset we exploit these vulnerabilities that are found in millions of devices right from the mobile operator's infrastructure to the end-user devices such as mobile phones, IoT sensors, and laptops. Especially, we present automated cellular exploitation tools and also share the traces and data sets with the research community. Our tests are carried out in various continents and highlight vulnerable implementations inside 4G base stations around the world. We target a wide range of devices including the latest NB-IoT chipsets and demonstrate a new class of hijacking, bidding down and battery draining attacks in 4G/5G networks.

Boris Larin / @oct0xor & Alexander Liskin / @0x1fffffffffff

Momigari – Overview of the latest Windows OS kernel exploits found in the wild (Slides

)

Bio – Boris Larin is a Senior Malware Analyst in the Heuristic Detection and Vulnerability Research team at Kaspersky Lab. Boris is very passionate about reverse engineering and has been doing it for the last decade, performing vulnerability research on software for different CPU architectures and systems. In his current role, Boris is responsible for detecting exploits using modern antivirus technologies. Besides that, Boris is the author of educational materials for Kaspersky Academy, and his latest write-ups about zero-day exploits and the inner workings of commonly exploited software can be found on Securelist.com.

Bio – Alexander Liskin works for Kaspersky Lab for more than 10 years, now he is Head of Heuristic Detection and Vulnerability Research team. The group is responsible for heuristic and generic malware detection, development of effective malware detection methods, static and dynamic exploit detection, packed objects analysis, format parsers, vulnerability assessment and patch management. He graduated from Department of Mechanics and Mathematics of Moscow State University. In addition, Alexander leads SDL practices implementation within the department, and he is the owner of malware auto-processing infrastructure projects and KL's Sandbox.

Abstract – Momigari (red leaf hunting) is the Japanese tradition of searching for the most beautiful leaves in autumn.

In the space of just one month in the autumn of 2018, we found a number of zero-day exploits in the wild for the Microsoft Windows operating system. Two of them were for the newest and fully updated Windows 10 RS4, which until then had no known memory corruption exploits.

We also uncovered exploits for vulnerabilities that had been unintentionally fixed with security updates, but which had been unpatched zero-days for a long time leading up to that. These findings shows that exploit writers continue to find new ways to reliably exploit unstable vulnerabilities and bypass modern mitigation techniques for the most secure operating system.

[expand title="Read more"]The most interesting thing is that many of these exploits are related. This suggests that the masterminds behind them are not afraid of wasting a number of zero-days at a time because their armory is full.

In this presentation, we will look at multiple local privilege escalation exploits actively used in the wild and tied into a single framework that was not previously known.

This advanced framework shows signs of maturity: the highest standards of code development and a deep technical knowledge of Windows OS inner workings, observed from the shellcodes that are used in the exploits.

In this presentation, we will share the following:

- An in-depth analysis of the framework that was used for the zero-day exploit development
- An in-depth analysis of vulnerabilities used by attackers
- The interesting techniques that were used to bypass exploit mitigation mechanisms[/expand]

Ben Sparkes / / @PsychoTea

Totally Not Spyware Jailbreak (Slides

)

Bio – Ben Sparkes (@iBSparkes / @PsychoTea) is an independent security researcher mainly focused on iOS/macOS and XNU exploitation. He works as part of the Jailbreak community and has released and worked on public Jailbreaks in the past (Meridian, Totally Not Spyware).

Abstract – On the 2nd September 2018, jailbreak team “Jake Blair” (@iBSparkes, @littlelailo, @s1guza, @stek29) quietly released the “Totally Not Spyware” jailbreak. The jailbreak is a browser-based exploit chain targeting iOS devices, using bugs in the WebKit engine and the XNU kernel to perform privilege escalation and jailbreak the device. The jailbreak focused iOS versions 10.0 through 10.3.3, however the techniques used are applicable to any iOS version, including the latest versions of iOS 12. In this talk we’ll look at how the jailbreak works, including details of the WebKit exploit, breaking out of the browser sandbox, running shellcode, exploiting the kernel, and some detail on the kppless post-exploitation methodology.

Brandon Azad / @_bazad

Voucher Swap (Slides

)

Bio – Brandon Azad is a security researcher at Google Project Zero specializing in macOS and iOS.

Abstract – Among the vulnerabilities fixed in iOS 12.1.3 was CVE-2019-6225, a(nother) serious MIG reference counting issue in Apple's kernel. Independently discovered by both me and Qixun Zhao (@S0rryMybad), this vulnerability was quite serious because it was reachable from within any sandbox and could be exploited very reliably. In this talk we'll look at how this vulnerability was discovered and how to exploit it to achieve arbitrary kernel read/write on iOS 12.1.2.

James Lee / @**Windowsrcer**

One API to rule them all: Receive 10+ CVEs with bugs which broke SOP in All Major Browsers

Bio – Founder of S2SWWW, Security Vulnerability researcher.

Abstract – The Same Origin Policy (SOP) is one of the most important Web browser mitigation which prevent attackers from stealing sensitive information such like cookies from cross-origin websites.

In this talk, I'll talk about SOP bypass Vulnerabilities which worked in 5 major browsers: Chrome, Firefox, Edge, IE and Safari.

Jeremy Fetiveau / @__x86

Attacking TurboFan (Slides

)

Bio – Jeremy Fetiveau (@__x86) is an independent security researcher interested in browser exploitation. He contributes to the blog doar-e (@doar_e).

Abstract – In the area of browser exploitation, the current trend is to attack JavaScript engines, and more specifically the optimizing compiler. TurboFan is the one being used by the chrome browser and is part of the v8 engine.It has been affected by many interesting bugs, many of which allow very reliable exploitation.The objective of this talk is to discuss the engine's internals and some reductions made on the sea of nodes before shifting the focus on security. In particular, this presentation will examine what kind of bugs have been recently affecting the optimizing compiler, how to reliably exploit those incorrect behaviors and what changes have been made to prevent this.

Ki Chan Ahn / @externalist

The journey on exploiting the Magellan bug on Chrome (Slides

)

Bio – Ki Chan Ahn (@externalist) is a security researcher working at Exodus Intelligence. His general field of interest is bughunting & exploitation in various operating systems, browsers, and hypervisors. In the past, he has been doing Pentesting and Web/Mobile Application auditing in the Financial Sector.

Abstract – This talk focuses on exploiting the Magellan bug found by the Tencent Blade team in Google Chrome Desktop. Nowadays, browser research is heavily focused on exploiting the JIT engine. This bug was a good example to test how resistant Chrome was to classic memory corruption bugs that occur outside the Javascript engine, and demonstrate the feasibility of exploiting such bugs. The presentation will discuss how the exploit was designed from scratch by constructing primitives built around WebSQL, and present various ideas to overcome exploitation hurdles to finally build a full exploit that runs arbitrary code in the Chrome renderer process.

Kirils Solovjovs / @**KirilsSolovjovs**

RouterOS vulnerabilities and malware campaigns (Slides

)

Bio – Mg. sc. comp. Kirils Solovjovs is Lead Researcher at Possible Security, bug bounty hunter, IT policy activist, and the most visible white-hat hacker in Latvia having discovered and responsibly disclosed or reported multiple security vulnerabilities in information systems of both national and international significance. Kirils has developed the jailbreak tool for Mikrotik RouterOS. He has extensive experience in social engineering, penetration testing, network flow analysis, reverse engineering, and the legal dimension.

Abstract – We've seen a variety of MikroTik vulnerabilities being used in the wild to distribute malware or hijack routers. In an updated version of author's legendary talk on MikroTik, he describes the modus operandi of 2018 malware campaigns on MikroTik routers and explores all relevant vulnerabilities.

Author believes that the recent malware campaigns are a direct consequence of the wide availability of RouterOS jailbreaking tools and security research.

In this talk we talk about all currently known relevant vulnerabilities in RouterOS systems on a technical level, featuring such recent exploits as chimay_red, winbox, samba and licupgr.

Author will also be giving an update on what new developments have happened in MikroTik world since the release of RouterOS 6.41.

Paolo Stagno / @**Void_Sec**

A Drone Tale, All Your Drones Are Belong To Us (Slides

)

Bio – Paolo Stagno (aka VoidSec) has worked as a consultant for a wide range of clients across top tier international banks, major tech companies and various Fortune 1000 industries. At ZeroDayLab, he was responsible for discovering and exploiting new unknown vulnerabilities in web applications, network infrastructure components, IoT devices, new protocols and technologies. He is now a freelance security researcher and a penetration tester focused on offensive application security. He enjoys understanding the digital world we live in, disassembling, reverse engineering and exploiting complex products and code.

Abstract – In 2013, DJI Drones quickly gained the reputation as the most stable platform for use in aerial photography and other fields. Since then Drones have increased their field of application and are actively used across various industries (law enforcement and first responders, utility companies, governments and universities) to perform critical operations on daily basis. As a result of that, Drones security has also become a hot topic in the industry.

This talk will provide a comprehensive overview of the security model and security issues affecting the underlying technologies, including existing vulnerabilities in the radio signals, Wi-Fi, Chipset, FPV system, GPS, App and SDK. As part of the presentation, we will discuss the

architecture of one of the most famous and popular consumer drone product: the DJI Phantom 3. This model will be used to demonstrate each aspect of discovered security vulnerabilities, together with recommendations and mitigations.

[expand title="Read more"]

A special focus will be on the recent changes and countermeasures DJI has applied to the firmware of its products in order to harden the security, following the recent accusations and the US Army ban. While the topic of hacking drones by faking GPS signals has been shared before at major security conferences in the past, this talk will extend these aspects to include geo-fencing and no fly zones abuses.

[/expand]

Seunghun Han / @kkamagui1

Betrayal of Reputation: Trusting the Untrustable Hardware and Software with Reputation (Slides

)

Bio – Seunghun Han is a hypervisor and an operating system security researcher at National Security Research Institute of South Korea and before that was a firmware engineer at Samsung Electronics. He is an expert in the hypervisor and had his own hypervisor, Shadow-box. He also had several CVEs on Linux kernel and BIOS/UEFI firmware, and he contributed patches to

various system and security software. He was a speaker and an author at USENIX Security, Black Hat Asia, HITBSecConf, beVX, and KIMCHICON. He was also a member of the Influencer Program at Black Hat Asia 2019 and authored the books, “64-bit multi-core OS principles and structure, volume 1 (ISBN-13: 978-8979148367) and volume 2 (ISBN-13: 978-8979148374)”.

Abstract – Reputation is based on trust, and people normally believe the products produced by global companies like Intel, HP, Dell, Lenovo, GIGABYTE, and ASUS because of their reputation. Their products are built with some kinds of hardware and software that are made by them or confirmed by them. Global companies have spent their efforts making and managing high-quality products for profit and reputation. So, trust based on reputation works properly.
Despite their efforts, the complexity of hardware and software has been increasing. Because of it, it is hard to check the correctness and completeness of specifications and implementations related to their products.
[expand title=”Read more”]
In this talk, I introduce the case that hardware and software, especially BIOS/UEFI firmware, Intel Trusted Execution Technology (TXT), and Trusted Platform Module (TPM), betrays your trust. Reputable companies defined specifications and implemented them, and TPM with UEFI/BIOS firmware and Intel TXT has been widely used and responsible for the root of trust.
I found two vulnerabilities, CVE-2017-16837 and CVE-2018-6622, related to the sleep process. Unlike previous researches, the vulnerabilities can subvert the TPM without physical access. To mitigate the vulnerabilities, I also introduce countermeasures and a tool, Napper, to check the vulnerabilities. Sleep process is a vital part of the vulnerabilities, so Napper makes your system take a nap and check them. [/expand]

Siguza / @**s1guza**Evolution of iOS mitigations (Slides

)

Bio – Siguza is a Computer Science student, have been an enthusiast programmer for many years, and have become an iOS kernel hacker/jailbreaker since late 2016. He has talked before at Zer0con 2018 and 0x41con 2019.

Abstract – As Apple continues to harden their products against exploitation, they are introducing new mitigations not only in their software, but also their hardware. The iPhone system architecture has long deviated from the original ARM specification, with important proprietary changes that have gone mostly or entirely undocumented. This talk fills the gaps between what little information we get from Apple's open source components, and what you can learn from basic trial-and-error. It explores in depth the new challenges an attacker has to face on iOS 12, with a special focus on the latest additions brought by the A12 SoC.

Valentina Palacin / @**fierytermite**

Once Upon a Time in the West – A story on DNS Attacks (Slides

)

Bio – Valentina is one of Deloitte Threat Intelligence Analyst, and she have specialized in tracking APTs worldwide using ATT&CK Framework to analyze their tools, tactics and techniques. IShe is a self-taught developer with a degree in Translation and Interpretation from Universidad de Málaga (UMA), and a Cyber Security Diploma from the Universidad Tecnológica Nacional (UTN).

Abstract – Just like in Old West movies, we are going through a land riddle with well-known gunmen: OceanLotus, DNSpionage and OilRig, who roam at ease, while the security cowboys sleep. This presentation will uncover the toolset and techniques used by these gunmen, taking a closer look at their big guns and their behavioral patterns. We will explore the attacks involving DNS that took place during the last decade to examine the latest discovered techniques in order to improve detections to dodge the bullets they are firing in our direction.

Yongtao Wang / @by_sanr, Yang Zhang / @izykw

NTLM Relay Risk Is Coming: A New Exploit Technique Makes It Reborn

(Slides 

)

Bio – Yongtao Wang(Sanr) is the leader of Red Team at BCM Social Corp.
He has profound experience in wireless security and penetration testing, and his research focuses on malware analysis, vulnerability exploitation. He shares research achievements at China Internet Security Conference (ISC), Blackhat, Codeblue, POC, CanSecWest, HackInTheBox etc.

Leader of Red Team at BCM Social Corp.
He has profound experience in wireless security and penetration testing, and his research focuses on malware analysis, vulnerability exploitation.
He shares research achievements at China Internet Security Conference (ISC), Blackhat, Codeblue, POC, CanSecWest, HackInTheBox etc.

Bio – Yang Zhang(izy) is an independent security researcher with rich experience in web security research and penetration testing, core member of XDSEC. He has received several acknowledgments from famous companies for his security reports. Currently focusing on the security research of web application security, cloud security, blockchain security.

Abstract – NTLM relay attacks have been around for more than a decade. The oldest method is SMB Relay, which can be traced back to a security tool released by Sir Dystic in 2001, it needs to be emphasized that it's independent of application layer protocol (such as SMB). In fact, there is a security issue in the NT-LAN-Manager authentication protocol. As we all know, there are two

ways to implement NTLN relay attack.
1. Relay credential to the victim machine (Credential Reflection), Microsoft released MS08-068 patch for this vulnerability.
2. Relay credential to another host (Credential Relay), that is a currently widely-used attack method because Credential Reflection has been fixed by Microsoft. Unfortunately, there are a lot of restrictions to implement Credential Relay in some attack scenarios.
[expand title="Read more"]
We propose a new attack technology that can successfully implement the Credential Reflection attack and bypass all Microsoft defense strategies, which will directly lead to RCE. In this talk, we will first review the history of NTLM relay attacks. After that, we will introduce a new attack technique for Credential Reflection, that can bypass the Microsoft defense strategies(MS-08068) and implement the credential reflection attack by relaying The Net-NTLM hash to the machine itself, effect of RCE（Remote Command Execution) can be achieved. In addition, we will describe it in real-world attack scenarios and release a automated exploit tool for this vulnerability.
[/expand]

Zhi Zhou / @CodeColoristI Want to Break Free: Unusual Logic Safari Sandbox Escape

Bio – Zhi Zhou (@CodeColorist) is a senior security engineer currently working at AntFinancial LightYear Security Labs, who mainly focuses on product security across different platforms and also passionate to real world pwn games. He has been acknowledged by Microsoft, Apple, Adobe and VMWare for reporting security issues. His previous research including one of the earliest research on practical SQLite (WebSQL) exploits that affects most popular browsers and mobile devices, and inspired the recent Magellan exploit for Chrome. He's also the author of open source iOS app pentesting tool Passionfruit, which now has over 1k stars on GitHub.

Abstract – Sandbox escape plays an important role in a full chain browser exploit. Through the recent pwnage competitions like Pwn2Own and TianfuCup, the most seen approach was through memory corruption. But there were also successfully exploited logic bugs by phoenix team. Inspired by them, I found some userspace IPC logic issues that are reliably exploitable, to break out the sandbox and pop us a Calculator.

In this session, I'll discuss the idea and steps on how to audit inconspicuous logic issues and turn them into exploit primitives. For example, CVE-2018-4310 is a logic bug that can launch apps (like Calculator) inside WebKit sandbox on both iOS and macOS. While having limitation on loading custom payload for full chain exploit, it has an unexpected effect on iOS that you can build an unstoppable background app process. Another bug without CVE in cfprefsd that it failed to check sandbox state, which survived so many rounds of Pwn2Own, can break sandbox and even persistent after reboot, as a one-liner. I'll explain the exploitation details on how to trigger instant escape with it. It was demonstrated as part of a sandbox to kernel logic exploit chain on XPWN 2018.
