ROOTCON® Hacking Conference - ROOTCON 12 Archives

rootcon.org/html/archives/rc13

Talks

APAD: An EDR Grade Agent for Wi-Fi Access Points
by: Vivek Ramachandran
(PDF) (Video)
Wi-Fi is ubiquitous and the de facto way to connect to the Internet. With increasing Wi-Fi speeds and the gradual disappearance of the network port on our laptops, it might soon be the only way. Being entrusted with such an important responsibility, one would assume that Wi-Fi access points would have sufficient built-in security and attack detection. Unfortunately, this is farther away from the truth as it could be! Wi-Fi access points in the personal and SMB space have barely evolved over the past decade! This puts users at great risk - we routinely hear about attackers redirecting DNS and other traffic, attacking users behind an access point, etc. One would ask - why are the Access Point vendors not doing anything about this? Simple answer: hardware vendors typically don't care much about software. So, we've decided to take matters into our own hands :)

In this talk, we will be releasing - Access Point Attack Detector (APAD): an enterprise-grade access point monitoring agent built from the grounds up. APAD will have a kernel and user mode components which will continuously monitor your access point platform for attacks and intrusion

attempts! The tool should be easily portable to most Linux based access point platforms. For our demo - we will be using OpenWRT along with a hardware access point! Enough said - looking forward to seeing you at the talk!

Dissecting APT Malware against Taiwan in 2019
by: Bletchley Chen & Inndy Lin
(PDF) (Video)
Due to the special political situation in Taiwan, Taiwan receives many APT attacks every year, including different sectors from government, IT to financial. Up to the first-half year in 2019, we have already discovered several APT attacks, and investigating in several APTs, such as: Shadow Hammer, ASUS web storage. In this presentation, we will share tactics as well as detailed malware technique. In the tactic level, these APT attacks first compromise lower-security level, but trusted third party as the vector to reach the targets. Or utilize normal system administration tools, and cloud services to achieve their intent and avoid investigating. In the malware technique, the more sophisticated dropper and downloader are used. These malware are widely equipped with anti-analysis technique as well as file-less memory module. Meanwhile, the investigation and reversing tool and technique will also be included in this talk.

```
APT against Taiwan in 2019
    ASUS Shadow hammer
    ASUS WebStorage
APT Tactics
    Supply chain attacks
    Synthesis normal program for malicious intent
Malware Techniques
    Stealth method
    Multi-stage dropper
    File-less Memory Module
Investigating Procedure
    Threat Hunting System
    Threat Intellegence System
    Defeating common obfuscation technique by IDAPython
```

Behind LockerGoga – A walk through a ransomware attack worth 40m$
by: Magda Lilia Chelly, CISSP, PhD
(PDF) (Video)
At first, I'll give the audience a brief walkthrough of the history of input validations against SQL Injection. Then, some classic and practical evasions will be shown with the slide, and I'll explain why these evasions work and how validation functions handle afterward. Of course, those de facto well-known WAFs, like ModSecurity, and some common filters, like libinjection, will also be discussed at the end of the walkthrough.

As I finish the introduction of input validations above, I'll then introduce a novel way utilizing the concept of Polymorphism in order to bypass the limitations. The outline probably looks like following: Go through a brief introduction of the mutation technique, the differences among other evasion techniques, the scheme, the algorithm, and the potential risks it may raise in the future. Some new bypasses against ModSecurity and libinjection will be shown and evaluated at last. In conclusion, I'll talk about future works and possible improvements to the idea. I'll also discuss why there exist such developer UX/ergonomics problems that stop developers from using true

solutions such as parameterized queries, strict HTML templating, strong typing and/or taint-tracking systems, and therefore, might lead to the problem of lexical and syntactic equivalences in many input languages as well.

Farewell, WAF - Exploiting SQL Injection from Mutation to Polymorphism
by: Boik Su @qazbnm456
(PDF) (Video)
At first, I'll give the audience a brief walkthrough of the history of input validations against SQL Injection. Then, some classic and practical evasions will be shown with the slide, and I'll explain why these evasions work and how validation functions handle afterward. Of course, those de facto well-known WAFs, like ModSecurity, and some common filters, like libinjection, will also be discussed at the end of the walkthrough.

As I finish the introduction of input validations above, I'll then introduce a novel way utilizing the concept of Polymorphism in order to bypass the limitations. The outline probably looks like following: Go through a brief introduction of the mutation technique, the differences among other evasion techniques, the scheme, the algorithm, and the potential risks it may raise in the future. Some new bypasses against ModSecurity and libinjection will be shown and evaluated at last. In conclusion, I'll talk about future works and possible improvements to the idea. I'll also discuss why there exist such developer UX/ergonomics problems that stop developers from using true solutions such as parameterized queries, strict HTML templating, strong typing and/or taint-tracking systems, and therefore, might lead to the problem of lexical and syntactic equivalences in many input languages as well.

Hacking ICS devices/PLC's for Fun - ICS and IOT Hacking
by: Arun Mane
(PDF) (Video)
New generation malware and attacks have been targeting ICS and systems causing huge monetary and human life losses. ICS system still vulnerable in nature because it’s poorly understood. As ICS industries is old and functioning from a long time, there is no considering of security aspect since they started. Apart from PLC, RTU, DCS and SCADA system, there are third party vendors devices available in the market which can talk or convert one protocol to another, sometimes they called serial servers or couplers. These devices still in a vulnerable state as per their HMI, Protocols and hardware point of view. In this talk, we will demonstrate about these devices vulnerability as well as some well-known plc vulnerabilities.

Hunting Threats with Wireshark Plugins
by: Nishant Sharma, Jeswin Mathai, & Shivam Bathla
(PDF) (Video)
Network traffic dumps can be very valuable when processed with proper tools. There are various open source and paid tools to analyse the traffic but most of them either have predefined functionality or scalability issues or one of dozen other problems. But, what if we can convert our favourite traffic analysis tool Wireshark, to an extensible, free platform independent threat/signature/attack hunter tool? In this presentation, we will talk about developing wireshark plugins to do security analysis of live and stored packets. We will use examples of older and newer protocols (including non-standard ones) to explain the plugin workflow and development.

Identity crisis: war stories from authentication failures
by: Vishal Chauhan
(PDF) (Video)
Your online identity has become one of your most valuable assets. Identity vulnerabilities can let attackers completely masquerade as you online: access your personal information, your social media, online banking, and more.

In this talk, we will explore some of the vulnerabilities that Microsoft has observed related to online identity compromise and the approaches we've taken to address these issues. These examples will demonstrate how you might approach searching for other vulnerabilities in the identity space and the bug bounty programs that exist to support these efforts.

Making Anomaly Detection system(ADS) for Vehicles (Automotive Hacking)
by: by: Arun Mane & Nikhil Bogam
(PDF) (Video)
Today all vehicles are connected through V2X technologies. All manufacturers are coming with new technologies which can be added technologies for Vehicle industries like Fleet management systems, diagnosis toolset etc. These systems are from third-party vendors which are still in a vulnerable state. So addressing their weakness requires specific skillset in cybersecurity as well as attack mitigation of vehicle industries. Mitigation part (Making ADS) requires huge and niche expertise in vehicle industries. No one show, how to mitigate these vehicle attacks through ADS systems in any conference. In this talk will show you how to mke ADS (Anomaly detection system) to mitigate vehicle cybersecurity attacks.

```
CANBus attacks

- Introduction and protocol Overview

- Firehose attack

- Replay Attacks

- Right-After and Right-Before Attacks

- Denial of Service
```

Making an ADS (Anomaly Detection system)

- To mitigate Firehose attack:- The expected CAN message reception frequency is checked with actual. If it is not in range, then the message is discarded and will not be processed. If expected CAN message is not received with expected frequency the system transit to a safe/secure state. (CAN message frequency checking)

- To mitigate Replay Attacks: - Transmitter ECU sends an encrypted message, which includes monotonic counter and data and at the receiver end, after decryption receiver checks received monotonic counter is equal to last received counter plus the incremental value of the monotonic counter. In case of mismatch, receiver discard the message, which in turn prevents replay attack.

- To Mitigate Right-After and Right-Before Attack: - The receiver ECU CAN message circular buffer shall check if buffer is filled. So if Last in First out circular buffer is implemented and Right - After attack is executed then checking of buffer full will prevent the over-riding of malicious CAN message on intended CAN message. Similarly, if First in First out circular buffer is implemented and Right-Before attack is executed then checking of buffer full will prevent the over-riding of malicious CAN message on intended CAN message

- To mitigate Denial of Service:- All expected CAN message is filtered and unexpected messages are discarded. In case of DOS attack is executed, then the filter will not have allowed processing this unexpected messages. Frequency Checker of CAN frame

The Man-In-The-Middle attack against a certain password manager
by: Soya Aoyama
(PDF) (Video)
How many sites do you use? Is the password long enough and secure? Do not tell me you reused it. Unfortunately, we have not a memory good enough to remember so many passwords long and secure. For this reason, there are several companies providing password management applications. However, are they really secure?

I have executed a man-in-the-middle attack against a certain password management application. Surprisingly, the password was exchanged in plain text between .exe and .dll, and it was very easy to steal it. The program I created is generic and, under certain conditions, can steal information between all .exe and .dll in Windows. In this talk, I will demonstrate the actual attack, and provide technical explanations to enable this attack. And finally, I suggest ways to protect other apps from this attack.

Navigating the Shift from Opportunistic to Targeted Ransomware
by: Christopher Elisan
(PDF) (Video)
CryptoLocker, WannaCry, and the hundreds of other ransomware families that indiscriminately infected businesses and government agencies worldwide have been studied and in some cases neutralized by researchers who figured out how to decrypt data locked down by the respective malware.

Nimble threat actors, however, have lately focused on a much more targeted approach to potential profits. While still largely relying on commodity exploits for known vulnerabilities or configuration weaknesses to gain access to a network, rather than dropping malware on certain machines, attackers have been hitting organizations hard by flooding ransomware onto endpoints and network shares and demanding drastically high ransoms in return for decrypted data.

This is an abrupt turn from what had been the norm for more than two years. Already, state and local government operations have suffered major incursions, with one of the biggest being the attack against the city of Atlanta one year ago. Victims in other industries, notably financial services, telecommunications, and health care, have also felt the brunt of these new targeted ransomware attacks.

Pilot Study on Semi-Automated Patch Diffing by Applying Machine-Learning Techniques
by: Asuka Nakajima
(PDF) (Video)
When developing a 1-day exploit code, patch diffing (binary diffing) is one of the major techniques to identify the part that security fixes are applied. This technique is well-known since long ago among reverse engineers, and thus to support the diffing, various tools such as BinDiff, TurboDiff, and Diaphora have been developed. However, although those fantastic tools greatly support the analysis, patch diffing is still a difficult task because it requires deep knowledge and experience. In order to address this issue, we conducted a pilot study with the goal to achieve a semi-automated patch diffing by applying machine-learning techniques. Based on the hypothesis that "similar types of vulnerabilities will be fixed in a similar manner," we have applied the unsupervised machine learning technique to extract those patterns and considered the way to achieve semi-automated patch diffing. In the talk, we will show the details of our pilot study and share the insights that we have gained it. We believe that our insights will help other researchers who will conduct similar research in the future.

z3r0 to h3r0 - Targeting Crown Jewels over the Internet
by: Viral Maniar
(PDF) (Video)
It is very common nowadays to hear about company X been pwned by a hacker. But, have you ever wondered how hackers can get into these companies' network? Are they really utilising precious 0–days to get inside these networks? Even after installing and managing all the latest flashy "cyber" products which detects and blocks unknown threats - why are we still vulnerable?

As a penetration tester, I perform plenty of external penetration tests which includes open source intelligence (OSINT) gathering techniques such as subdomain enumeration, Email addresses dictionary creation and password spraying. Information gathered through such techniques are very crucial for a targeted attacker to perform preliminary reconnaissance on the company and its employees. The presentation will also cover how malicious actors use the exposed information and correlate these in a short span of time to obtain access to the internal host. Once an attacker gains the initial foothold, it is a matter of time to perform a privilege escalation and gain complete access over the domain. In short, this talk will demonstrate a number of techniques hacker uses to profile a company and gain access to the crown jewels aka from z3r0 to H3r0. Attendees will leave with detailed information on how they can better protect their infrastructure.

Speakers

Asuka Nakajima
Asuka Nakajima is a researcher at the NTT Secure Platform Laboratories. She studied at the Faculty of Environment and Information Studies at the Keio University. Her research interests include reverse engineering, vulnerability discovery, and IoT security. Since 2014, she has been a member of the executive committee of SECCON (SECurity CONtest, the largest CTF organizer in Japan). She is also a founder of "CTF for GIRLS", the first security community for women in Japan.

She has presented at various security conferences and events including BlackHatUSA 2019, PHDays VI, AsiaCCS 2019, and AIS3(Advanced Information Security Summer School in Taiwan). Asuka also serves as a Review Board member for Black Hat Asia 2018/2019, and BlueHat

Shanghai 2019. She is also an author of the best seller book called "Cyber Attack" in Japan. (Bluebacks, 2018)

Arun Mane
Arun is a Founder and Director of Amynasec labs company which is specialized in Vehicle/Iot/ICS and he also Hardware, IOT and ICS Security Researcher. His areas of interest are Hardware Security, SCADA, Automotive security, Fault Injection, RF protocols and Firmware Reverse Engineering. He also has experience in performing Security Audits for both Government and private clients. He has presented a talk at the nullcon 2016,2017,2018 Goa, GNUnify 2017, Defcamp 2017, 2018 Romania, BsidesDelhi 2017, c0c0n x 2017, EFY 2018, x33fcon2018, BlackHat USA 2018, Defcon USA 2018, OWASP Seasides 2019 Goa. Also Trainer for Practical Industrial Control Systems (ICS) hacking training, delivered in x33fcon2018,2019, HIP 2018 and also delivered training for IoT hacking in HITB 2017, HIP 2017, BlackHat Asia 2018 and private clients in London, Australia, Sweden, Netherlands etc. He is an active member of null open community.

Bletchley Chen
Bletchley Chen is currently a senior researcher in Cycraft. His research focuses on network attack and defense, machine learning, software vulnerability, malware and program analysis. He earned his PHD degree of Computer Science and Engineering from National Chiao-Tung University (NCTU). He also dedicates to security education. Founding of NCTU hacker research clubs, he trains students to participate world-class security contests, and has experience of participating DEFCON CTF. Besides, he has presented technical presentations in non-academic technique conferences, such as HITCON and VXCON. As an active member in Taiwan security community, he is in the review committee of HITCON conference (Vice Chief in 2019 HITCON CMT), and member of CHROOT - the top private hacker group in Taiwan. He organized BambooFox Team to join some bug bounty projects and discover CVEs in COTS software and several vulnerabilities in campus websites.

Boik Su
Syue-Siang Su (Boik Su) has four-year experience in Web Security and actively using OSS to create or manage tools for his research in the field. He has not only devoted himself to research but also received some awards from CTFs, been the speaker at AVTokyo 2017 and 2018, Taiwan Modern Web 2017, OSCON 2018, and the lecturer at HITCON Training and National Center for Cyber Security Technology in Taiwan.

Christopher Elisan
Christopher Elisan, Director of Intelligence at Flashpoint, is a seasoned Reverse Engineer, Malware Researcher and published Author. He speaks at conferences around the world and frequently provides expert opinion about malware, botnets and advance persistent threats for leading industry and mainstream publications. Elisan’s published works include Hacking Exposed: Malware and Rootkits, 2 ed.

Inndy Lin
Inndy Lin is a researcher in Cycraft, mainly focuses on malware reversing and supporting advanced malware research. He is also an active member in Taiwan student community, who

delivered many technique talks in HITCON, SITCON and TDOH. As a leader of Security Club in National Taiwan University of Science and Technology, He also acted as TA in AIS3, which is the largest student infused training project.

Jeswin Mathai
Jeswin Mathai is a Researcher at Pentester Academy and Attack Defense. He has presented/published his work at DEF CON China, Blackhat Arsenal and Demo labs (DEFCON). He has a Bachelor's degree from IIIT Bhubaneswar. He was the team lead at InfoSec Society IIIT Bhubaneswar in association with CDAC and ISEA, which performed security auditing of government portals, conducted awareness workshops for government institutions. He was also the part of team Pied Piper who won Smart India Hackathon 2017, a national level competition organized by GoI. His area of interest includes Malware Analysis and Reverse Engineering, Cryptography, WiFi security and Web Application Security.

Nikhil Bogam
Nikhil is an Automotive expert in Safety and Security. His areas of interest are ECU security, CAN, LIN Network Security. He also has experience in Security Design, Implementation in Automotive products. He has 13 years of experience in Automotive product development. In his tenure, he worked with Hella, Tata Elxsi, Continental for many Car manufacturer BMW, Honda, VW. Currently, He is working with Lear Corporation. He also delivered a workshop at OWASP Seasides 2019 Goa on CAR Hacking.

Nishant Sharma
Nishant Sharma is a R&D Manager at Pentester Academy and Attack Defense. He is also the Architect at Hacker Arsenal where he leads the development of multiple gadgets for WiFi pentesting such as WiMonitor, WiNX and WiMini. He also handles technical content creation and moderation for Pentester Academy TV. He has 6+ years of experience in information security field including 4+ years in WiFi security research and development. He has presented/published his work at Blackhat USA/Asia, DEF CON China, Wireless Village, IoT village and Demo labs (DEFCON USA). Prior to joining Pentester Academy, he worked as a firmware developer at Mojo Networks where he contributed in developing new features for the enterprise-grade WiFi APs and maintaining the state of art WiFi Intrusion Prevention System (WIPS). He has a Master's degree in Information Security from IIIT Delhi. He has also published peer-reviewed academic research on HMAC security. His areas of interest include WiFi and IoT security, AD security, Forensics and Cryptography.

Magda Lilia Chelly
Magda Lilia Chelly is a CISO On Demand. She reviews technical architectures, cloud migrations, and digital transformations. She has a PhD and a CISSP. Magda is known for hacking passion in her spare time. With her expertise, and technical background provides a 360 degrees cyber security support for companies; from governance to incident management, she coordinates and builds resilient businesses. Magda' latest two projects covered the roles of an ISO Lead Implementer for a Fortune 500 and a business information security officer role for a MAS regulated Fortune 500 company covering 13 countries in Asia Pacific.

Shivam Bathla
Shivam Bathla is a Security Researcher at Pentester Academy and Attack Defense. He has a Bachelor's degree from NIT Delhi. He secured 5th rank in GCCS Peace-a-thon Contest. His area

of interest includes Malware Analysis and Reverse Engineering, Cryptography, WiFi security, Forensics and Web Application Security. He also has experience in Linux Kernel Exploitation.

Soya Aoyama
Soya Aoyama is a security researcher at Fujitsu System Integration Laboratories Limited. Soya has been working for Fujitsu for more than 20 years as a Windows software developer, and had been developing NDIS drivers, Bluetooth profiles, Winsock applications, and more. About four years ago, soya started security research, and has gave presentation in BSidesLV, GrrCON, ToorCon, DerbyCon and HackMiami in the past. Soya is also the organizer of BSides Tokyo.

Viral Maniar
Viral is a dedicated Principal Security Consultant and a Penetration Tester at Threat Intelligence Pty Ltd in Australia with over 7 years of experience in information security and management. Prior to joining Threat Intelligence, he held senior positions at KPMG and Ernst & Young. He has provided security consulting services including infrastructure (internal - external), application penetration testing, vulnerability assessments, wireless penetration testing, social engineering, red team engagements, API testing, Thick & Thin client testing and cloud architecture security reviews to numerous clients across various industries in the APAC region. He was involved with the RISC (RMIT Information Security Collective) Club while at University and worked as a developer for firewall security at Biarri Networks where he developed a visualisation algorithm to solve the issue of firewall rules management. He has participated in number of bug bounty programs and won awards for responsible disclosure of security vulnerabilities in web and mobile applications from companies such as Adobe, Apple, Google Chromium, IBM, C2FO, Blinksale, Appfog, TEDmed and many more. In his leisure time, he enjoys developing security tools and maintains number of projects on the Github. He has achieved industry certifications such as Offensive Security Certified Professional (OSCP) and SANS GPEN - Network Penetration Testing.

Vishal Chauhan
Vishal Chauhan is a Security Engineering Lead in the Microsoft Security Response Center (MSRC) team. All his time at Microsoft, he has delved into everything security from Systems to Web and anything in between. Lately he has been exploring various facets of cloud and web security.

Vivek Ramachandran
Vishal Chauhan is a Security Engineering Lead in the Microsoft Security Response Center (MSRC) team. All his time at Microsoft, he has delved into everything security from Systems to Web and anything in between. Lately he has been exploring various facets of cloud and web security.

Contest Winners
Receives the Black Badge entitled them for free entrance for next years conference.

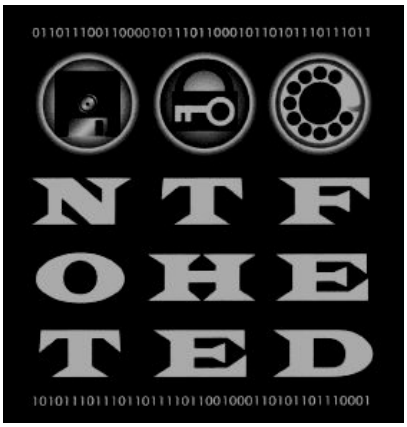
Capture The Flag
Team Harambae with 2050 points

Hacker Jeopardy
Team Girls (Bugcrowd, Microsoft)

Sponsors

Community Partners

Pics
ROOTCON 13 Pics


NTF
OHE
TED


black hat
ASIA 2019
MARCH 26-29, 2019
MARINA BAY SANDS / SINGAPORE

Arts