nccgroup
People powered tech-enabled cyber security

FOX IT
part of nccgroup

# NCC Group's 2024 Annual Research Report

**Ristin Rivera**
Research Program Administrator

**Andy Davis**
Global Research Director

# Contents



# Executive Summary: Research at NCC Group

The 2024 Research Report highlights a year of significant contributions to the cybersecurity community by NCC Group. Through pioneering research, innovative tools, and active engagement with industry and academia, NCC Group continues to lead in advancing cybersecurity practices and addressing evolving challenges.

This year, we published:

**48** Common Vulnerabilities and Exposures (CVEs), showcasing our commitment to identifying and addressing software and hardware vulnerabilities.

**52** Blog Posts, offering in-depth insights, technical guidance, and thought leadership across various domains of cybersecurity.

**10** Open-Source Tools, empowering the global cybersecurity community with resources to enhance security capabilities.

**17** Public Reports, reinforcing transparency and collaboration by sharing findings from critical assessments and research initiatives.

Our research this year covered a wide range of critical topics. In vulnerability research and exploitation techniques, we focused on identifying and addressing weaknesses in software and hardware systems to mitigate security risks. In network and system security, we developed advanced strategies for detection, mitigation, and protection against potential threats. Our work in malware and ransomware analysis provided valuable tools and methodologies to counter emerging and increasingly sophisticated threats.

In the field of cryptography, we explored innovative solutions for secure communications, particularly in preparing for the challenges posed by a post-quantum world. We also analyzed the integration of AI into cybersecurity, assessing both the risks and opportunities presented by these technologies.

Additionally, we addressed vulnerabilities in telecommunications infrastructure, emphasizing the importance of securing critical systems that underpin global communications.

Looking ahead to 2025, we remain committed to the exploration of cybersecurity. Together, with our partners and the global community, we aim to build a safer, more secure digital world.

Section 01

# 25 Years of Research at NCC Group

**Andy Davis,**
Global Research Director

The research we have published over the last 25 years highlights the significant role NCC Group has played in the cybersecurity world due to our coverage of a wide array of topics, deep technical insights, and practical applications.

As it constitutes an extensive body of knowledge, I enlisted the help of OpenAI's ChatGPT to help me summarise the content. Here's what we came up with as an overview of how our work has impacted cybersecurity since 1999:

### Addressing Current and Emerging Threats

We dive into detailed analysis and mitigation strategies for both current and emerging cybersecurity threats. This includes advanced persistent threats (APTs), exploitation of new and existing vulnerabilities in software and hardware, and the increasing concerns around IoT security. By focusing on real-world threats, we have helped organisations prepare and defend against sophisticated attacks.

### Enhancing Secure Development Practices

With multiple publications focusing on secure coding practices, secure development lifecycle, and specific programming guidance, our research has been instrumental in elevating the security standards of software development across industries. This has become ever more important as software is increasingly becoming integral to our everyday lives.

### Promoting Cryptographic Security

The exploration of cryptographic algorithms, quantum cryptography, and secure communications protocols is vital for secure digital transactions. As cyber threats evolve, maintaining robust cryptographic practices is key to ensuring the confidentiality and integrity of our sensitive information.

### Forensics and Incident Response

The detailed forensic analyses provided in our publications are essential for understanding how breaches occur and how to effectively respond to them. This knowledge is used by incident response teams to quickly mitigate damage and for ongoing efforts to enhance detection and response capabilities within organisations.

### Guidance on Compliance and Best Practices

Our research includes discussions on security compliance, regulations, and best practices which are essential for organisations to not only meet mandatory regulatory requirements but also to adopt industry-leading security practices. This helps in fostering a security-aware culture within organisations and in building robust security frameworks that protect against breaches and data theft.

### Educational Impact

By providing in-depth technical knowledge, case studies, and research insights, our publications serve as valuable educational resources for security professionals, researchers, and students. They contribute to the broader understanding of complex cybersecurity topics, which is important for training the next generation of cybersecurity professionals.



Overall, our contribution through these publications significantly impacts many aspects of cybersecurity by advancing knowledge, shaping industry standards, improving security practices, and driving technological and methodological innovations in the field. Hopefully, our work not only assists organisations in defending against dynamic and sophisticated cyber threats but also plays a crucial role in the academic and research-oriented advancements in cybersecurity, ultimately helping to build a more secure and resilient future.

Below is a timeline of notable NCC Group research publications over the last 25 years.

| | |
|---|---|
| 2001 | Windows 2000 Format String Vulnerabilities |
| 2002 | Oldest publication from still-serving NCC consultant |
| 2003 | Quantum Cryptography first discussed |
| 2004 | Blind Exploitation of Stack Overflow Vulnerabilities |
| 2005 | Improving the Exploitation Prevention Mechanisms on the Windows platform |
| 2006 | Implementing and Detecting a PCI Rootkit |
| 2007 | Attacking the Windows Kernel |
| 2008 | Developing secure Android mobile applications |
| 2009 | Microsoft SDL: Return-on-Investment |
| 2010 | Security Compliance as an Engineering Discipline |
| 2011 | USB: Undermining Security Barriers |
| 2012 | Abusing Privileged and Unprivileged Linux Containers |
| 2013 | Bypassing Windows AppLocker using a Time of Check Time of Use vulnerability |
| 2014 | An Implementer's Guide to Cyber-Security for Internet of Things Devices and Beyond |
| 2015 | Secure Device Manufacturing: Supply Chain Security Resilience |
| 2016 | Hardware Design: FPGA Security Risks |
| 2017 | First mention of AI in an NCC publication |
| 2018 | Ethics in Security Testing |
| 2019 | Connected Health: Security Landscape Review |
| 2020 | Exploring DeepFake Capabilities & Mitigation Strategies with UCL |
| 2021 | An Illustrated Guide to Elliptic Curve Cryptography Validation |
| 2022 | BLE Proximity Authentication Vulnerable to Relay Attacks |
| 2023 | Rustproofing Linux |
| 2024 | LTair: The LTE Air Interface Tool |

Section 02

# Cryptography Services

**Javed Samuel,**
Global Lead for Cryptography Services

NCC Group's Cryptography Services team continued to deliver leading research in 2024. The variety of their rich outputs reflects the ever dynamic and evolving nature of the field of cryptography. Key themes from our crypto research during this period were:

- **Post-Quantum Cryptography**: There was a greater emphasis on post-quantum cryptography with the standardization of post-quantum cryptography algorithms by NIST.
- **Security Vulnerabilities**: From erroneous computations to time-based side-channel attacks, we further explored vulnerabilities in cryptographic implementations and their implications.
- **Blockchain Platform Cryptography**: The Cryptography Services team delivered multiple public reports which focused on the relationship between cryptographic principles and various blockchain platforms.

In the post-quantum age, cryptography research is no longer just about securing information; it includes staying ahead of quantum threats, redefining trust in digital systems, and building a resilient future. Cryptography Services' research in the ever-changing cryptography landscape ensures that the team remains up to date to deliver the best value to customers.

## Papers

Multiple consultants worked on publications on a range of cryptography topics in 2024.

- In this paper Gerald Doussot explained how to implement the Secure Hash Algorithm3 (SHA-3) family of functions in Lean 4, a functional programming language and theorem prover.

**Read Here**

- Thomas Pornin published A Prime-Order Group with Complete Formulas from Even-Order Elliptic Curves.

**Read Here**

- Giacomo Pope has been working with the SQIsign team, who are working on both an optimized and portable reference C-implementation of the signature scheme for the second round of the PQ-DSA call for NIST.

**Read Here**

- Thomas Pornin and others worked on Efficient Proofs of Possession for Legacy Signatures to be presented at 2025 IEEE Symposium on Security and Privacy (SP).

**Read Here**

## Blog Posts

The Cryptography Services team continued work on Cryptopals videos, as well as contributions to Real World Cryptography.

- Eli Sohl had multiple new Cryptopals videos covering CTR mode, padding oracles and cryptography visualization.

**Read Here**

**Read Here**

**Read Here**



- Several members of the team attended Real World Cryptography (RWC) in Toronto.

**Read Here**

- Marie-Sarah Lacharite served as a reviewer and moderated the Zero Knowledge and Fully Homomorphic Encryption session.

## Published Code

Additionally, Cryptography Services consultants worked on multiple implementations of various post-quantum cryptography algorithms.

- Thomas Pornin completed Rust, C and Go implementations of Post Quantum Cryptography algorithm Falcon/FN-DSA, with same performance and features.

**Read Here**

**Read Here**

**Read Here**

- Eric Schorn completed Post Quantum Cryptography Implementation of recently published FIPS 203, 204 and 205.

**Read Here**

**Read Here**

**Read Here**

## Presentations

Various members of the Cryptography Services team presented at cryptography conferences across a range of topics.

- Javed Samuel presented on Open Source Cryptography at International Cryptography Module Conference in September.

**Read Here**

- Paul Bottinelli presented  on Cryptography Vulnerabilities in the context of Modern Programming languages International Cryptography Module Conference in September.

**Read Here**

- Kevin Henry and Elena Bakos Lang presented on Lessons on secure deployment of cryptographic primitives at the University of Waterloo in July.

**Read Here**

## Public Reports

The team completed public reports for a range of customers across various cryptography areas. These public reports included:

- Kevin Henry, Marie-Sarah Lacharite, and Eli Sohl completed an assessment of libxmtp, which is a Rust implementation of the Extensible Message Transport Protocol (XMTP), built upon Messaging Layer Security (MLS) in a Web3 environment.

**Read Here**

- Gerald Doussot, Parnian Alimi, Marie-Sarah Lacharite, Thomas Pornin, Eli Sohl, and Javed Samuel completed a cryptography security assessment of selected aspects of the WhatsApp Identity Proof Linked Storage (IPLS) protocol implementation.

**Read Here**

- Kevin Henry, Parnian Alimi, and Elena Bakos Lang completed a cryptographic security assessment of keyfork, described as an opinionated and modular toolchain for generating and managing a wide range of cryptographic keys offline and on smartcards from a shared mnemonic phrase.

**Read Here**

- Paul Bottinelli, Kevin Henry, Elena Bakos Lang, and Eric Schorn reviewed the consensus mechanism implemented by snarkOS: a decentralized operating system for zero-knowledge applications that forms the backbone of Aleo network, which verifies transactions and stores the encrypted state applications in a publicly verifiable manner.

**Read Here**

Section 03

# Hardware and Embedded Systems

**Sultan Qasim Khan,**
Regional Practice Lead

The Hardware and Embedded Systems team continued to research a broad range of topics over 2024, ranging from wireless communication protocols to confidential computing to reverse engineering of binaries for uncommon architectures. The team published numerous blog posts, new and improved tooling, and multiple conference talks over the past year. Notable highlights include:

- **Reverse engineering and identifying vulnerabilities in the PowerG radio protocol:** James Chambers and Sultan Qasim Khan reverse engineered the proprietary PowerG radio protocol used by Johnson Controls alarm systems and identified exploitable weaknesses in the protocol and popular devices using it. Findings were presented at the Recon 2024 conference.

  **Read Here**

- **Over-the-air exploitation of Sonos devices:** Robert Herrera, together with Alex Plaskett of the Exploit Development Group (EDG), identified a vulnerability in the Wi-Fi stack of a Sonos device and developed an over-the-air exploit that enabled covert listening. This research was presented at Black Hat USA 2024. Details of this project are discussed further in this report among other projects by the EDG.

  **Read Here**

- **Development of tooling to reverse engineer binaries for the NanoMIPS ISA:** James Chambers and Robert Herrera developed and released the first public tooling for reverse engineering of binaries targeting the NanoMIPS ISA, which is gaining prominence for its use in MediaTek 5G basebands.

  **Read Here**

- **Public report analyzing the eBPF verifier:** Nathaniel Theis and Chris Anley conducted an in-depth security assessment of the eBPF verifier that validates the safety of eBPF programs for the Linux kernel. The assessment uncovered and led to the fixing of a significant bug, and the full assessment report has been made public.

  **Read Here**

- **Public report on Confidential Mode for Google Cloud Hyperdisk:** Catalin Visinescu conducted a security design analysis of Data Encryption Key (DEK) handling in the Confidential Mode of Google Cloud Hyperdisk. An overview of the analysis was made available in a public report.

  **Read Here**

- **Improvements to Sniffle:** Over the course of 2024, Sultan Qasim Khan implemented numerous enhancements to Sniffle, NCC Group's open-source Bluetooth Low Energy sniffer and testing tool. Highlights from Sniffle releases 1.8 to 1.10 include decoding of advertising data, improved support for extended advertising, support for additional hardware including low-cost Sonoff CC2652P dongles, support for receiving packets with invalid CRCs, and improved performance and reliability.

  **Read Here**

Section 04

# Security Research Team, Fox-IT

**Stefan de Reuver,**
Lead Security Analyst

## Edge Devices

Previously, in 2023, we saw an uptick in compromised edge devices, such as VPN gateways, firewalls, and routers. As predicted back then, this trend continued this year with even greater force. As these devices are still mostly a network's first line of defence, being able to properly investigate them after a breach is important for scope- and root-cause analysis. Building on previous years' experience, we improved our analysis and response capabilities for edge devices, enabling us to technically deep dive these systems just as well as other systems in a client's network!

Looking forward, we want to focus on creating more visibility by leveraging our current Network Detection and Response (NDR) and Security Information and Event Management (SIEM) monitoring capabilities to proactively monitor and alert our customers about threats that are specific to these edge devices.

## Leading Forensic Analysis Innovation

In 2022, we released our Digital Forensics & Incident Response (DFIR) framework, Dissect, to the public, enabling DFIR analysts across the globe to seamlessly analyze and collect data from any type of system. Currently, Dissect is widely adopted within the DFIR community and is even included in well-regarded training courses from institutes like SANS. We are continuously expanding and improving upon Dissect with the community, to provide the industry with bleeding edge innovations within the field of DFIR, such as hypervisor-based data acquisition and analysis.

Most of our innovations have mainly focused on host analysis and acquisition. We believe that memory analysis and acquisition is still a largely underexplored topic, and its analysis remains cumbersome within the industry.

Currently we are making advancements in this area, with the goal to make the analysis and acquisition of memory artefacts as seamless as host analysis and acquisition currently is with Dissect. Additionally, we are also increasing our operational technology (OT) analysis capabilities by adding support for OT specific systems.

## APT Tracking

Based on past incident response (IR) cases involving the advanced persistent threat (APT) group Lazarus, we started to track this threat actor together with our threat intelligence (TI) team. We discovered that the specific threat actor we were tracking is a Lazarus subgroup publicly known as AppleJeus, which targets the cryptocurrency and trading industry.

We managed to identify a new AppleJeus campaign in 2024 and warn several organizations proactively to help stop further compromise. We presented and shared our unique insights about this actor and malware at the FIRST 2024 conference.

We plan to keep tracking this additional subgroup with our current knowledge and share information with other organizations and law enforcement.

## Scanning the Internet

We are continuously scanning the Internet for malicious servers to feed into our security operations centre (SOC), DFIR and TI teams with curated indicators on these servers. This includes new signatures for tools and malware commonly used by threat actors or that we have identified during incident response cases. In 2024, we have heavily improved this pipeline.




Now, this same scanning pipeline is also used for vulnerability research. For example, we routinely identify and fingerprint edge devices on the Internet to provide statistics that can help estimate the impact a vulnerability could have and whether our customers are affected by it.

Looking forward to 2025, we plan to keep improving our internet scanning capabilities and the processing of scan results. We want to publish more of this scan data we automatically collect with this pipeline, allowing the industry to also leverage this data for a more secure digital future.

## Improving Threat Hunting

We worked on creating a readable and structured way to record indicators of compromise, allowing for programmatic parsing thereof. This idea stems from the need for recording indicators of compromise quickly and easily by forensic investigators, while also allowing these indicators to be ingested by other tools, e.g., detection platforms or internal tooling.

This helps in the overall picture as it allows us to more easily use such indicators in the various detection platforms we are currently using. The diversification of detection platforms requires a unified approach to performing searches of indicators. We plan to simplify and improve the process of threat hunting, in terms of processing indicators and performing threat hunts.

## Network Detection and Response

In recent years, endpoint detection and response (EDR) and extended detection and response (XDR) have taken a larger role in detecting threat actors at the SOC. We still believe that network detection is a vital part in catching these actors. This is also what we observe internally within our NDR customer base. Albeit the ever-increasing use of encryption, we remain able to effectively leverage our NDR capabilities to detect lateral movement in their internal network and notify our customers about threats. This is especially important for systems like edge devices, which gained the interest of threat actors as an initial point of entry. Combined with the fact that agent- and log-based monitoring brings about their own set of challenges, we believe NDR is especially effective here.

In addition to creating new detection signatures and improving existing ones, we also improved our detection signature accuracy by researching automated detection rule validation testing using internally developed tooling. Looking forward, we want to improve our OT network detection capabilities to broaden our NDR coverage.

Section 05

# Security Research Services

**Jon Renshaw,**
Security Research Services Director

2024 has been an interesting and varied year, highlighting the overlap of cybersecurity with public life, and raising awareness of how attackers might impinge upon our freedoms as citizens and businesses. Some of the key themes of the year and their relationship to cybersecurity research services at NCC Group include:

**The threat from disinformation:** With such a bumper year for elections, disinformation and deepfakes were near the top of the list of potential threats likely to impact on civil society and democracy in 2024. While instances of deepfakes were observed during many of the national elections, it transpired that the quantity and impact of such disinformation was probably less than many expected (noting this is very hard to objectively measure). Perhaps the bigger impacts have been on fraud, with high-profile attacks on enterprises and increasing evidence of deepfakes being used in celebrity investment scams and romance scams.

Efforts to develop technologies to detect deepfakes continues with both the UK[1] and US[2] governments investing in research into emerging technology capabilities. NCC Group also joined the Coalition for Content Provenance and Authenticity (C2PA)[3] in 2024, providing cybersecurity insights into this developing approach aimed at embedding provenance metadata into digital content.

**The safety and security of Artificial Intelligence:** Generative AI continued to develop at pace in 2024, prompting global efforts to establish regulations and organisations capable of managing emerging risks. This includes understanding AI's capabilities to, either autonomously or as an aide to a human in the loop, provide an uplift in cyber attackers' ability to effectively or efficiently compromise targets.

Our own previous research has shown that whilst there is a potential uplift in vulnerability research, it really requires an expert to parse, understand, and explore the outputs of AI model analysis of code. While model developers and deployers continue to innovate, governments have acted. The EU has passed the AI Act, with key implementation dates throughout 2025, 2026 and 2027, and various governments have created organisations tasked with understanding, monitoring, and developing mitigations for the risks posed by AI.

This year, NCC Group carried out research on behalf of Google into how the risks to AI models change when models are deployed on edge and personal computing devices.[4] Our research concluded that whilst moving capability to the edge can result in performance and privacy improvements, it also creates a complex new attack surface with potential for hardware and side-channel vulnerabilities in GPUs and malware embedded in GPU programs.

**Security of Connected Devices:** Two significant pieces of legislation became law in the UK and the EU in 2024. The Product Security and Telecommunications Infrastructure (PSTI) Act mandates some basic controls for smart devices sold to consumers in the UK, including no default passwords and transparency around vulnerability reporting and security support. The Cyber Resilience Act goes even further, including requirements for secure-by-design for connected devices sold into the EU.

Over many years, NCC Group has researched the security of connected consumer and enterprise devices, often finding poor security hygiene and a lack of maturity in processes, including vulnerability disclosure and patch management. Looking forward, future research will hopefully reveal a step change in attitudes towards developing devices with security built in, as this legislation



encourages investment in improved cybersecurity capabilities at manufacturers.

**Telecommunications and Internet Security:** It has been a turbulent year in telecommunications security; for one, we saw a key implementation date of the UK Telecommunications Security Act (TSA) pass for tier 1 providers in March. But before that notable date, we saw a novel Denial of Service (DoS) attack against Orange España in January, using compromised credentials to reconfigure the Resource Public Key Infrastructure (RPKI), a technology deployed for Border Gateway Protocol (BGP) route validation.

NCC Group's research into the security of 5G Testbeds and Trials (5GTT) in the UK was published by the Department of Science, Innovation and Technology (DSIT)[5] and showed the value of integrating cybersecurity expertise into research programmes to identify gaps and help remove roadblocks to developing technology beneficial to all.

During the Olympics in France, we saw network outages as a result of physical attacks on fibre optic infrastructure, highlighting that physical security is still an important element of risk management and cyber resilience in highly distributed systems such as telecommunications networks.

In September, the White House released a "Roadmap to Enhance Internet Routing Security", advocating for wider adoption of RPKI as a "mature, ready-to-implement approach to mitigate vulnerabilities in BGP". However, in December, they announced that eight US telecommunications providers had been the victims of a China-backed hacking and espionage campaign targeting top political figures, with work ongoing to ensure the hackers had been removed from the compromised environments.

**Quantum Computing & Post-Quantum Cryptography:** NIST finalized the first standards from the Post-Quantum Cryptography (PQC) competition, providing a foundation for organisations to begin to migrate away from the current generation of quantum insecure algorithms. The migration has already begun in the internet ecosystem with Chrome leading the way on adoption of the hybrid scheme X25519Kyber768Draft00[6] but enterprise support will lag behind as organisations need to update their configurations and supporting cryptographic infrastructure. NCC Group continues to collaborate with industry partners on the security of quantum computing through the quantum datacentre of the future project, looking at both quantum use cases in cybersecurity, and the security of quantum computers and their supporting infrastructure.

**Privacy Enhancing Technologies:** NCC Group is assuring TikTok's implementations of cutting-edge Privacy Enhancing Technologies (PETs) as part of Project Clover, a high-profile and complex programme that aims to give users in the European Economic Area, Switzerland, and the United Kingdom assurance and confidence that their data is being kept safe and secure.

Differential privacy is one of the controls being used to secure aggregated user statistics (alongside other controls such as encryption and redaction for individual data) to protect users' privacy and provides strong theoretical guarantees of privacy for individuals represented by an aggregate dataset. Our researchers and testers are rigorously assuring the TikTok design and implementation of PETs, that are being implemented at scale, to protect over 175 million European users.

Section 06

# Future Research

**Ristin Rivera,**
Research Program Administrator

The future of security research is ambitious, focusing on emerging technologies, evolving threats, and more proactive defence mechanisms. At the same time, addressing data protection fatigue will require a paradigm shift in how security is delivered—making it simpler, seamless, and less reliant on user action. By marrying cutting-edge research with human-centered design, the industry can tackle both challenges head-on, ensuring a safer and more user-friendly digital landscape.

Individuals are constantly bombarded with privacy notifications, security warnings, and breach alerts. Whether it's endless cookie consent pop-ups, multi-step authentication processes, or navigating complex privacy settings, the sheer volume of decisions users must make often leaves them feeling overwhelmed and exhausted. This overload can lead to disengagement, where users either ignore warnings or make suboptimal security choices because they feel powerless to control their data effectively. The frustration of keeping up with constantly evolving threats while relying on tools that demand significant time and effort only exacerbates this fatigue.

As many grow weary of managing their data security and finding trust in corporations, stricter guidelines on how organizations handle data are requested more and more.

Laws such as the GDPR and CCPA pushed companies to take on greater responsibility for securing user information and providing transparency, and ISO standards give idealized guidelines. Future legislation will likely follow. Security researchers and developers will play a critical role in helping businesses comply with these laws, creating tools and frameworks to detect potential violations and ensure adherence to evolving regulatory standards.

Building trust through transparency will be crucial.

Section 07

# Our Research in 2024

## Vulnerability Research and Exploitation Techniques

### 4 Dec 23

### Shooting Yourself in the .flags – Jailbreaking the Sonos Era 100

*Alex Plaskett*

The research highlights critical security weaknesses in the Sonos Era 100's bootloader that could be exploited to achieve full device compromise. The security vulnerabilities found are on weaknesses within its bootloader. These vulnerabilities could allow attackers to gain unauthorized root or kernel-level code execution, leading to a complete compromise of the device. By updating their devices with the latest firmware released by Sonos, users can protect themselves from these vulnerabilities.

### 2 Jan 24

### Technical Advisory – Multiple Vulnerabilities in PandoraFMS Enterprise

*Oliver Brooks*

This TA highlights 18 critical vulnerabilities in PandoraFMS Enterprise v7.0NG.767, including unauthenticated admin account takeover, remote code execution, XSS, SQL injection, and more. Users are advised to update to the latest version and implement recommended security measures to protect their systems.

### 19 Dec 23

### Retro Gaming Vulnerability Research: Warcraft 2

*Caleb Watt*

This article explores the reverse engineering of the classic game Warcraft 2 to identify potential security vulnerabilities. Due to its age and the lack of modern security features like anti-cheat mechanisms, Warcraft 2 provides an accessible platform for learning basic game hacking techniques.

The author outlines a methodology that includes defining clear goals, such as uncovering bugs that could be exploited during multiplayer sessions, and reviewing existing research to build upon prior findings. The analysis also involves assessing the game's attack surface, particularly its peer-to-peer networking model, and using tools to examine the code and behavior for exploitable flaws.

### 25 Jan 24

### Memory Scanning for the Masses

*Axel Boesenach and Erik Schamper*

Memory scanning involves examining the memory of running processes to identify specific patterns, which is essential for tasks like credential access, malware detection, and data recovery. However, conducting comprehensive memory scans can be time-consuming, especially when dealing with large memory spaces.

To address this inefficiency, a user-friendly Python library designed to expedite the memory scanning process was explored and developed. By filtering memory regions based on their attributes—similar to file permissions—such as read, write, and execute permissions, the library narrows down the areas that need to be scanned.

This targeted approach significantly reduces the time required for scanning by focusing only on memory regions relevant to the search criteria.

### 5 Feb 24

### Ivanti Zero Day – Threat Actors observed leveraging CVE-2021-42278 and CVE-2021-42287 for quick privilege escalation to Domain Admin

*David Brown and Mungomba Mulenga*

David Brown and Mungomba Mulenga discuss the exploitation of specific vulnerabilities in Active Directory by threat actors, following the compromise of Ivanti Secure Connect VPN appliances. Threat actors have been observed exploiting two critical vulnerabilities in Active Directory:

CVE-2021-42278: This vulnerability allows unauthorized modification of the sAMAccountName attribute of computer accounts, enabling attackers to impersonate other accounts, including domain administrators.

CVE-2021-42287: This flaw permits attackers to forge Kerberos Ticket Granting Tickets (TGTs), facilitating unauthorized access to services by impersonating privileged users.

By combining these vulnerabilities, an attacker can escalate privileges from a regular user to a domain administrator within a short time frame. Threat actors exploit Active Directory vulnerabilities CVE-2021-42278 and CVE-2021-42287 to achieve rapid privilege escalation to domain administrator status, particularly following the compromise of Ivanti Secure Connect VPN appliances. Organizations are advised to apply relevant patches, monitor for suspicious activities, and enforce strict access controls to mitigate these threats.

## 9 Feb 24

### Puckungfu 2: Another NETGEAR WAN Command Injection

*McCaulay Hudson*

McCaulay Hudson details a command injection vulnerability in certain Netgear routers, identified during preparations for Pwn2Own Toronto 2022. The vulnerability resides in the /bin/pucfu binary, which executes during the router's boot process. This binary performs multiple HTTPS requests to specific domains.

By manipulating the router's DNS settings via a controlled DHCP server, an attacker can redirect these HTTPS requests to a malicious server. Due to improper certificate validation, the router accepts responses from this server, allowing the attacker to send specially crafted JSON responses that trigger a command injection in the /bin/pufwUpgrade component, executed by a cron job.

## 11 Jun 24

### Pumping Iron on the Musl Heap – Real World CVE-2022-24834 Exploitation on an Alpine mallocng Heap

*Aaron Adams*

CVE-2022-24834 in Redis servers running on Alpine Linux, highlighting the complexities introduced by the musl libc and its mallocng allocator. It details the necessary adjustments to traditional exploitation methods to accommodate the unique memory management of musl libc, providing insights into effective strategies for leveraging this vulnerability in such environments.

## 24 Sept 24

### Technical Advisory: Xiaomi 13 Pro Code Execution via GetApps DOM Cross-Site Scripting (XSS)

*Ken Gannon*

A critical vulnerability in the GetApps Android application (com.xiaomi.mipicks) versions 30.4.1.0 and below. This vulnerability is a DOM-based Cross-Site Scripting (XSS) issue within a privileged WebView, allowing attackers to execute arbitrary shell commands on affected devices. Exploiting this flaw could enable the installation and execution of malicious applications without user consent.



## 5 Nov 24

### Treat your points as cash

*Frank Gifford*

This research highlights the security risks associated with the management of customer loyalty points, particularly focusing on the potential for unauthorized point grants due to inadequate validation and authorization controls. To mitigate this vulnerability: implementing robust validation and authorization mechanisms within the system.

This includes ensuring that only authorized personnel can grant points and that the system properly handles and validates input to prevent unauthorized modifications. Additionally, employing secure coding practices and conducting regular security assessments can help identify and address potential weaknesses in the system.

# Network and System Security

## 10 Jun 24

### Enumerating System Management Interrupts

*Carles Pey*

Security risks posed by System Management Interrupts (SMIs), which can be exploited for malicious activities due to their privileged nature and independent operation from the operating system. The solution is to implement auditing mechanisms that track and enumerate SMIs on systems to prevent unauthorized firmware modifications. This proactive approach helps mitigate the risks of malware insertion and other supply chain attacks targeting the system's firmware.

## 7 Nov 24

### Defending Your Directory: An Expert Guide to Securing Active Directory Against DCSync Attacks

*Rafael Alfaro March & Rodrigo Munoz*

## 5 Nov 24

### Auditing K3s Clusters

*Andrew Wade*

The unique security auditing challenges associated with K3s clusters. K3s, a lightweight Kubernetes distribution, offers advantages like reduced size and simplified authentication options. However, these features necessitate a tailored approach to security auditing to effectively gather and analyze the necessary information from the cluster. By focusing on configuration manifests, control plane components, certificate-based authentication, and the cluster state store, organizations can better identify and mitigate potential security risks in K3s environments.

## 12 Nov 24

### Defending Your Directory: An Expert Guide to Fortifying Active Directory Certificate Services (ADCS) Against Exploitation

*Rafael Alfaro March & Rodrigo Munoz*

## 14 Nov 24

### Defending Your Directory: An Expert Guide to Fortifying Active Directory Against LDAP Injection Threats

*Rafael Alfaro March & Rodrigo Munoz*

## 20 Nov 24

### Defending Your Directory: An Expert Guide to Mitigating Pass-the-Hash Attacks in Active Directory

*Rafael Alfaro March & Rodrigo Munoz*

These four articles collectively provide a comprehensive framework for securing Active Directory (AD), addressing specific vulnerabilities and attack vectors, while emphasizing the importance of proactive defense in enterprise environments. Each article focuses on a distinct yet interconnected aspect of AD security, illustrating how weaknesses in one area can cascade into broader risks if not addressed.

The first article explores the threat posed by DCSync attacks, a technique where attackers exploit misconfigured or overly permissive replication privileges to exfiltrate credentials from AD. The proposed solutions include tightly restricting replication privileges, monitoring changes to replication permissions, and implementing robust detection mechanisms to identify malicious replication requests. This sets the foundation for understanding the critical importance of maintaining strict privilege controls and oversight in AD environments.

Building on this, the second article examines Active Directory Certificate Services (ADCS) and its susceptibility to exploitation, particularly through misconfigurations that attackers can leverage to escalate privileges. The discussion emphasizes securing certificate templates, auditing ADCS configurations, and limiting certificate issuance to trusted entities. This reinforces the importance of securing auxiliary systems tied to AD, as they often serve as critical infrastructure that can be weaponized in sophisticated attacks.

The third article shifts focus to LDAP injection threats, where adversaries exploit vulnerabilities in LDAP queries to gain unauthorized access or manipulate AD data. The mitigation strategies emphasize the need for secure coding practices, input validation, and the principle of least privilege to prevent attackers from leveraging these queries as an entry point. This highlights how application-layer vulnerabilities can intersect with AD security, necessitating a holistic approach.

Finally, the fourth article addresses the infamous pass-the-hash (PtH) attack, a technique that exploits stolen hash values to authenticate as legitimate users without needing plaintext credentials. The proposed defenses include enforcing strong authentication protocols such as Kerberos, restricting administrative privileges, and implementing Privileged Access Management (PAM) solutions to compartmentalize access. This brings the focus back to credential security, tying together the overarching theme of protecting the mechanisms that underpin AD operations.

Together, these articles reveal a layered and interconnected security ecosystem within Active Directory. They demonstrate that addressing individual vulnerabilities is insufficient without a comprehensive strategy that considers privilege management, secure configurations, and robust monitoring. The main issue tying these articles is the multifaceted nature of AD security: its complexity and integral role in enterprise environments make it a high-value target for attackers, requiring defenders to adopt a holistic and proactive approach to safeguard their directories.

## 23 Dec 24

### PMKID Attacks: Debunking the 802.11r Myth

*Óscar Alfonso Díaz*

PMKID-based attacks are not exclusive to networks with 802.11r enabled. The vulnerability stems from how access points handle PMKID requests during the RSN handshake, making any improperly configured network susceptible. By understanding the mechanics of these attacks and implementing appropriate security measures, such as updating firmware, using strong passwords, monitoring network activity, and considering an upgrade to WPA3, network administrators can better protect their Wi-Fi networks from potential breaches.

# Malware, Ransomware and Digital Forensics

## 14 Dec 23

### Reverse, Reveal, Recover: Windows Defender Quarantine Forensics

*Max Groot and Erik Schamper*

The forensic challenges associated with analyzing files that have been quarantined by Windows Defender; once quarantined, these files are typically encrypted and moved to a secure location, making it difficult for forensic analysts to inspect their contents. This lack of visibility creates a barrier for incident responders and security professionals attempting to gather evidence, analyze malicious behavior, or confirm false positives. This article details a method to reverse-engineer Windows Defender's quarantine system, enabling forensic professionals to decrypt and recover quarantined files. By studying the encryption mechanisms and the file handling processes of Windows Defender, the researchers developed techniques to extract and decrypt quarantined files for analysis. This process allows analysts to inspect the original content of quarantined items, providing valuable insights into the nature of the threats and aiding in comprehensive forensic investigations.

## 22 Feb 24

### Unmasking Lorenz Ransomware: A Dive into Recent Tactics, Techniques and Procedures

*Global Threat Intelligence*

Lorenz ransomware group has been targeting small to medium-sized businesses globally since early 2021. Lorenz employs double-extortion tactics, exfiltrating sensitive data before encrypting systems and threatening to sell or publicly release it unless a ransom is paid. Recent investigations have revealed significant changes in their Tactics, Techniques, and Procedures (TTPs), including:

- Transition from '.sz40' to '.sz41', indicating a shift in their encryption methods.
- Use of random strings for file and scheduled task names to evade detection.
- Deployment of binaries to create local admin accounts, ensuring continued access.

## 13 Mar 24

### The Development of a Telco Attack Testing Tool

*Mark Tedman*

Mark Tedman goes into the necessity of robust security testing in telecommunications networks and introduces an in-house developed tool designed to facilitate such testing. Telecommunications networks face several security challenges. Many networks still operate on outdated equipment and protocols, which were not designed with modern security threats in mind.

The swift evolution of technologies like 5G and the Internet of Things (IoT) often prioritizes functionality and speed over security considerations. The intricate web of interconnected components and service providers can create security gaps, as not all stakeholders may implement robust security measures. The regulatory environment for telecom security varies across countries and is often inadequate to address emerging threats, leaving networks exposed. Global manufacturing of telecom equipment introduces potential risks, as malicious components could be introduced into the network infrastructure.

## 28 Mar 24

### Android Malware Vultur Expands Its Wingspan

*Joshua Kamp*

Vultur's evolution underscores the necessity for continuous vigilance and proactive security measures to protect Android devices from increasingly sophisticated threats. Vultur has introduced several new features to increase its control over infected devices: the malware can download, upload, delete, and locate files on the device. Vultur can perform actions such as scrolling, swiping, clicking, and muting or unmuting audio. It can prevent specific applications from running and display custom notifications in the status bar. Vultur can disable the device's Keyguard, effectively bypassing lock screen security measures.

## 25 Apr 24

### Sifting through the spines: identifying (potential) Cactus ransomware victims

*DFIR, Willem Zeeman and Yun Zheng Hu*

The Cactus ransomware group's exploitation of vulnerabilities in Qlik Sense servers to gain unauthorized access to organizations' networks. The Cactus ransomware group has been actively targeting vulnerable Qlik Sense servers since November 2023. These attacks involve exploiting specific vulnerabilities in the Qlik Sense data visualization and business intelligence platform, which organizations use for data analysis. By compromising these servers, the attackers can infiltrate networks, leading to potential data breaches and operational disruptions. The critical need for organizations to secure their Qlik Sense servers against exploitation by the Cactus ransomware group. Implementing robust cybersecurity measures and maintaining vigilance are essential to protect sensitive data and maintain operational integrity.

## 4 Oct 24

### Forensic Readiness in Container Environments

*Rafael Alfaro March*

When maintaining forensic readiness within containerized environments, Containers, due to their ephemeral and dynamic nature, can complicate traditional forensic investigations.

By implementing comprehensive logging, establishing clear data retention policies, utilizing centralized logging solutions, regularly testing forensic capabilities, and integrating forensic practices into DevOps pipelines, organizations can enhance their ability to respond to and investigate security incidents effectively.

## 8 Nov 24

### Nameless and shameless: Ransomware Encryption via BitLocker

*DIFR*

Ransomware groups are leveraging BitLocker, a legitimate Windows feature designed for disk encryption, to encrypt victims' data during attacks. Unlike traditional ransomware methods that use custom encryption algorithms, this approach exploits BitLocker's built-in capabilities to lock access to drives, making detection and mitigation more difficult.

The use of a trusted system tool adds a layer of complexity for defenders, as the activity might blend into normal operations or administrative tasks.



# Telecommunications Security

## 14 Mar 24

### LTair: The LTE Air Interface Tool

*Eva Esteban Molina*

Telecommunications networks, especially those utilizing LTE technology, are susceptible to various security threats. These threats can compromise the integrity and confidentiality of communications, potentially leading to unauthorized access, data breaches, and service disruptions.

To address these vulnerabilities, NCC Group's Eva Estaban Molina developed LTair, an open-source tool based on the SRSran framework. LTair enables the emulation of a complete LTE network, including a rogue LTE base station (eNodeB), a full core network, and user equipment (e.g., mobile phones). This capability allows for the simulation of various attack scenarios to evaluate the security posture of LTE networks.

# Software Development and AI in Security

## 9 Jan 24

### Rust for Security and Correctness in the embedded world

*Chris Bury*

Rust's suitability for embedded systems, emphasizing its ability to provide memory and concurrency safety, performance efficiency, and adaptability to low-level programming requirements. By adopting Rust, developers can create more secure and reliable embedded applications, mitigating risks associated with traditional languages like C.

## 7 Feb 24

### Analyzing AI Application Threat Models

*David Brauchler*

Here, David Brauchler examines the security implications of integrating machine learning (ML), particularly Large Language Models (LLMs), into application architectures. It introduces the Models-As-Threat-Actors (MATA) methodology to identify and assess new threat vectors associated with AI/ML components. The integration of AI/ML models into applications necessitates a revaluation of traditional threat models. By recognizing AI models as potential threat actors and employing methodologies like MATA, organizations can better identify, assess, and mitigate security risks associated with AI-enhanced applications.

## 8 Apr 24

### Technical Advisory – Ollama DNS Rebinding Attack (CVE-2024-28224)

*Gérald Doussot*

A critical vulnerability in Ollama, an open-source system for managing large language models (LLMs). This vulnerability allows attackers to remotely access Ollama's API without authorization, potentially leading to unauthorized activities such as exfiltrating sensitive file data, interacting with LLM models, deleting models, and causing denial-of-service attacks through resource exhaustion. The issue was addressed in release v0.1.29, and users are advised to update to this version or later. The vulnerability arises from a DNS rebinding flaw in Ollama, enabling attackers to bypass the browser's same-origin policy and gain unauthorized access to the API. This access can lead to various malicious activities, including data exfiltration and service disruption.

## 12 Apr 24

### Non-Deterministic Nature of Prompt Injection

*Jose Selvi*

Jose Selvi (AI Services) highlights challenges in detecting prompt injection vulnerabilities in large language models (LLMs) due to their non-deterministic behaviour. Unlike deterministic systems like SQL databases, LLMs exhibit non-deterministic behaviour, meaning they can produce different outputs for the same input. This variability complicates the detection of prompt injection vulnerabilities, as responses may not consistently reveal the presence of such vulnerabilities.



## 31 May 24

### Why AI Will Not Fully Replace Humans for Web Penetration Testing

*Steven van der Baan*

While AI can automate tasks like data processing and pattern recognition, it lacks the contextual understanding that human penetration testers bring. Web applications are complex and operate within specific business contexts, requiring human insight to identify vulnerabilities. Additionally, AI may struggle to adapt to novel attack vectors or zero-day exploits. The solution is a hybrid approach where AI can enhance the efficiency of penetration testing but cannot fully replace human expertise. Human testers provide creativity, intuition, and an understanding of business logic that AI cannot replicate. AI tools can be used to augment human capabilities, but human oversight is still required for accurate and reliable results, especially in identifying logical flaws or business logic errors.

## 5 Jun 24

### Cross-Execute Your Linux Binaries, Don't Cross-Compile Them

*Domen Puncer Kugler*

There is a challenge of running software on devices with different architectures. Traditionally, this involves cross-compiling, where you adapt code to work on a different architecture. However, cross-compiling can be complex and time-consuming, especially when dealing with complex software dependencies. Instead of cross-compiling, the solution proposed is to cross-execute Linux binaries using emulation. This approach involves creating a chroot environment on the target device, allowing you to execute binaries compiled for a different architecture without having to modify the code. Tools like QEMU can be used to emulate the target architecture, simplifying the deployment process.

## 21 Oct 24

### Comparing AI Against Traditional Static Analysis Tools to Highlight Buffer Overflows

*Mark Tedman*

Mark Tedman investigates the effectiveness of Large Language Models (LLMs) in identifying buffer overflow vulnerabilities in binary code, comparing them to traditional static analysis tools. Buffer overflows are critical security flaws that can lead to unauthorized code execution and system compromise. Traditional static analysis tools have limitations in detecting such vulnerabilities, especially in complex or obfuscated code. Leveraging LLMs accessed through the Ollama platform to analyze unknown binaries for buffer overflows, Ollama facilitates the deployment and usage of multiple LLMs on local machines, ensuring data privacy by processing information locally. The analysis is conducted on a sample 'C' source code implementing a simple UDP server, which contains a buffer overflow vulnerability. The findings are then compared with results from CWE_Checker, a static analysis tool for ELF binaries.

## 4 Dec 24

### Analyzing Secure AI Design Principles

*David Brauchler*

Integrating LLMs into applications requires more than just content filtering to ensure security. By adopting secure design principles such as 'Secure by Design,' the principle of least privilege, defense in depth, and conducting regular security assessments, organizations can mitigate the risks associated with AI integration. These measures help prevent severe vulnerabilities and ensure that AI-enhanced applications are robust against potential threats.

# Malware+H2:H53, Ransomware and Digital Forensics

## 16 Sept 24

### The Dark Side: How Threat Actors Leverage AnyDesk for Malicious Activities

*Lauren Eynon*

Lauren Eynon highlights the dual-use nature of AnyDesk, emphasizing that while it serves legitimate purposes, it can also be exploited by cybercriminals to gain unauthorized access to systems. By employing social engineering tactics, attackers can deceive users into installing AnyDesk, leading to potential security breaches. The article underscores the importance of user education, strict access controls, continuous monitoring, and robust endpoint security to prevent such malicious activities.

## 6 Dec 24

### Phish Supper: An Incident Responder's Bread and Butter

*DFIR*

NCC Group's Digital Forensics and Incident Response (DFIR) team details a BEC incident where attackers used phishing emails to compromise Microsoft 365 accounts. They maintained access by registering new authenticator apps and creating inbox rules to hide their activities. The attackers then sent further phishing emails from compromised accounts to harvest more credentials. Implementing MFA, disabling unnecessary features, enforcing conditional access policies, conducting regular security reviews are crucial steps to mitigate such threats.



# Collaboration with Industry & Academia

**Public Reports:**

1. Zcash Zebra Security Assessment
   **Read Here**
2. Penumbra Labs R1CS Implementation Review
   **Read Here**
3. Entropy/Rust Cryptography Review
   **Read Here**
4. Caliptra Security Assessment
   **Read Here**
5. Zcash FROST Security Assessment
   **Read Here**
6. WhatsApp Auditable Key Directory (AKD) Implementation Review
   **Read Here**
7. Aleo snarkVM Implementation Review
   **Read Here**
8. Security Review of RSA Blind Signatures with Public Metadata
   **Read Here**
9. Aleo snarkOS Implementation and Consensus Mechanism Review
   **Read Here**
10. AWS Nitro System API & Security Claims German
    **Read Here**
11. AWS Nitro System API & Security Claims Spanish
    **Read Here**
12. AWS Nitro System API & Security Claims French
    **Read Here**
13. AWS Nitro System API & Security Claims Italian
    **Read Here**
14. Google Privacy Sandbox Aggregation Service and Coordinator
    **Read Here**
15. Confidential Mode for Hyperdisk – DEK Protection Analysis
    **Read Here**
16. Keyfork Implementation Review
    **Read Here**

# Tools

**Skrapa** - *Axel Boesenach and Erik Schamper*
Skrapa is an open-source tool developed to assist forensic analysts in collecting and parsing memory dumps for identifying malicious PowerShell activity. It automates the process of extracting relevant PowerShell artifacts, such as scripts, commands, and modules, from memory dumps, making it an effective resource for incident response and post-compromise investigations. Skrapa is particularly useful when traditional logging is unavailable or incomplete, as it allows analysts to recover evidence of PowerShell usage directly from memory.

**Read Here**

**Android Demystification Toolbox** - *Nicolas Guigo*
The Android Demystification Toolbox (ADT) is an open-source suite of tools designed to assist in the analysis and reverse engineering of Android applications (APKs). It provides a set of utilities for extracting and decompiling APK files, making it easier for security analysts, reverse engineers, and researchers to understand the inner workings of Android apps.

**Read Here**

**Ghidra nanoMIPS** - *James Chambers*
Prior to this development, there was no publicly available, reliable tool for analyzing nanoMIPS firmware within Ghidra. This gap hindered efficient reverse engineering of devices utilizing this architecture. James Chambers introduces a module developed to enhance Ghidra's capabilities in analyzing nanoMIPS architecture, commonly used in MediaTek 5G baseband firmware.

**Read Here**

**Cranim**
*James Chambers*

**Read Here**

**Cranim** - *Eli Sohl*
Cryptographic concepts can be abstract and challenging to grasp. Traditional textual explanations often fall short in conveying the dynamic nature of cryptographic operations. There was a need for a tool that could visually represent these processes to facilitate better comprehension. Cranim addresses this need by providing a framework for creating visual representations of cryptographic operations. It utilizes Manim's capabilities to produce both animations and static images, making it easier to illustrate and understand cryptographic mechanisms. The toolkit is accessible for public use, with installation and usage guidelines available on its GitHub repository.

**Read Here**

**ScoutSuite** - *Luis Toro Puig*
We welcomed the addition of DigitalOcean support to ScoutSuite, an open-source multi-cloud auditing tool. This integration enables users to assess the security posture of their DigitalOcean environments by identifying misconfigurations and potential vulnerabilities.

The integration of DigitalOcean into ScoutSuite introduces new rules for various DigitalOcean services, including managed databases, droplets, networking devices like load balancers, firewalls, and DNS entries, as well as Space Objects (buckets) and managed Kubernetes clusters.




This addition allows users to conduct comprehensive security assessments across multiple cloud providers, enhancing their ability to evaluate and improve their cloud security posture more robustly.

**Read Here**

**Stepping Stones** - *Stephen Tomkinson*
"Stepping Stones" is an open-source tool developed by NCC Group's Stephen Tomkinson to enhance the efficiency and accuracy of red team activity logging. By providing a centralized platform for documenting actions, integrating with tools like Cobalt Strike, and offering features such as credentials management, it streamlines the documentation process, aiding in post-engagement analysis and reporting. This tool is available for the wider red teaming community to utilize and contribute to.

**Read Here**

# Cryptopals 1-18

Cryptopals challenges are a set of cryptography-related programming exercises designed to teach the principles and practice of cryptography through hands-on problem-solving. These challenges are freely available on the Cryptopals website.

What are Cryptopals challenges?

Cryptopals challenges were created by a team at Matasano Security, known for their expertise in cryptography and security. This team later became part of NCC Group, a global cybersecurity consultancy. These challenges started off as six sets of progressively more difficult problems. Each set focuses on specific cryptographic concepts and techniques. At the end of 2024, we had 18 challenges for you to try. Cryptopals challenges address the problem of:

1. **Lack of practical cryptography skills:** Many developers and security professionals lack hands-on experience in implementing, analyzing, and breaking cryptographic systems, which can lead to insecure applications.
2. **Understanding cryptographic vulnerabilities:** The challenges demonstrate how cryptographic systems can fail when implemented incorrectly, emphasizing the importance of secure design.
3. **Bridging the gap between theory and practice:** They provide a structured way to learn cryptography by doing, rather than just reading about concepts.

Cryptographic education is critical for improving the security of systems and applications. A solid understanding of cryptographic principles and vulnerabilities enables developers to identify and address potential weaknesses in implementation. Knowledge of real-world attack techniques, such as those demonstrated in challenges like Cryptopals, equips practitioners to anticipate and mitigate exploitation scenarios effectively.

If you're interested in cryptography, Cryptopals is a fantastic, practical resource to build expertise and confidence in this critical area of cybersecurity.

## 24 May 24

### Tutorial/Study Guide Announcing the Cryptopals Guided Tour Video 17: Padding Oracles!

*Eli Sohl*

The guided tour of Cryptopals Challenge Video 17, specifically focusing on Padding Oracles. Padding oracles are a type of vulnerability that can be exploited in certain cryptographic systems, particularly in block ciphers using modes like CBC (Cipher Block Chaining). Learn how padding oracles work, and get a hands-on demonstration to help you understand the theory and practical aspects of this type of vulnerability, particularly in the context of the Cryptopals Crypto Challenges.



## 5 Nov 24

### Announcing the Cryptopals Guided Tour Video 18: Implement CTR

*Eli Sohl*

Cryptopals Challenge Video 18, which focuses on implementing CTR (Counter) mode encryption. The concept of CTR mode is explained and demonstrated in the context of the Cryptopals Crypto Challenges.

CTR mode is a symmetric key block cipher mode that turns a block cipher into a stream cipher. It uses a counter value that is encrypted and then XOR'd with the plaintext to produce the ciphertext. This mode is highly parallelizable and is commonly used in practice for secure encryption. The video walks through how to implement CTR mode step by step, giving viewers a deeper understanding of how this encryption technique works and how it can be exploited or used in real-world scenarios.

This is part of the Cryptopals Guided Tour, where the focus is on teaching cryptographic concepts and practical skills by walking through real challenges.

# Exploit Development Group (EDG)

In 2024 NCC's exploit development group presented at multiple different conferences, released whitepapers, blog posts, slides, competed at hacking competitions, and performed exploit related training. These fell into three major security research areas: Automotive, IoT/Hardware Security and Advanced Exploitation.

One major highlight of the year was competing at Pwn2Own Automotive 2024 in Tokyo; this resulted in a compromise of two in vehicle entertainment systems (IVIs) and one electric vehicle charger, winning NCC Group a total of $90,000.

# Automotive

This also led to research being published in the automotive space around Alpine IVI and the Phoenix Contact EV charger as follows:

**Revving Up: The Journey to Pwn2Own Automotive 2024**

On the 28th of September 2024, Alex Plaskett and McCaulay Hudson presented this talk at ROMHack, Italy.

Throughout this presentation we described our process with a deep dive into in-vehicle entertainment systems and an electric vehicle (EV) charger controller (Phoenix Contact CHARX SEC-3100).

**Read Here** **Watch here**

**Charging Ahead: Exploiting an EV Charger Controller at Pwn2Own Automotive 2024**

On the 18th of September 2024, McCaulay Hudson and Alex Plaskett presented this talk at 44CON, London. The talk was focused on the security of a specific EV charger component, the Phoenix Contact CHAR SEC-3100 and the vulnerabilities identified and exploited by the team.

**Read Here**

# IoT / Hardware Security

In the internet of things / hardware security domain, Alex and Robert researched a remote kernel exploit against Sonos one devices. This led to development of a covert wiretap implant which could be used to spy on conversations within the room.

**Listen-Up: Sonos Over-The-Air Remote Kernel Exploitation and Covert Wiretap**

On the 8th of August 2024, Alex Plaskett and Robert Herrera presented this talk at BlackHat 2024 in Las Vegas, USA.

This led to the publication of a 40-page whitepaper and slides from the event:

**Read Here** **Read Here**

We also presented multiple video demonstration of this to show the impact:

**Watch here**

# Advanced Exploitation

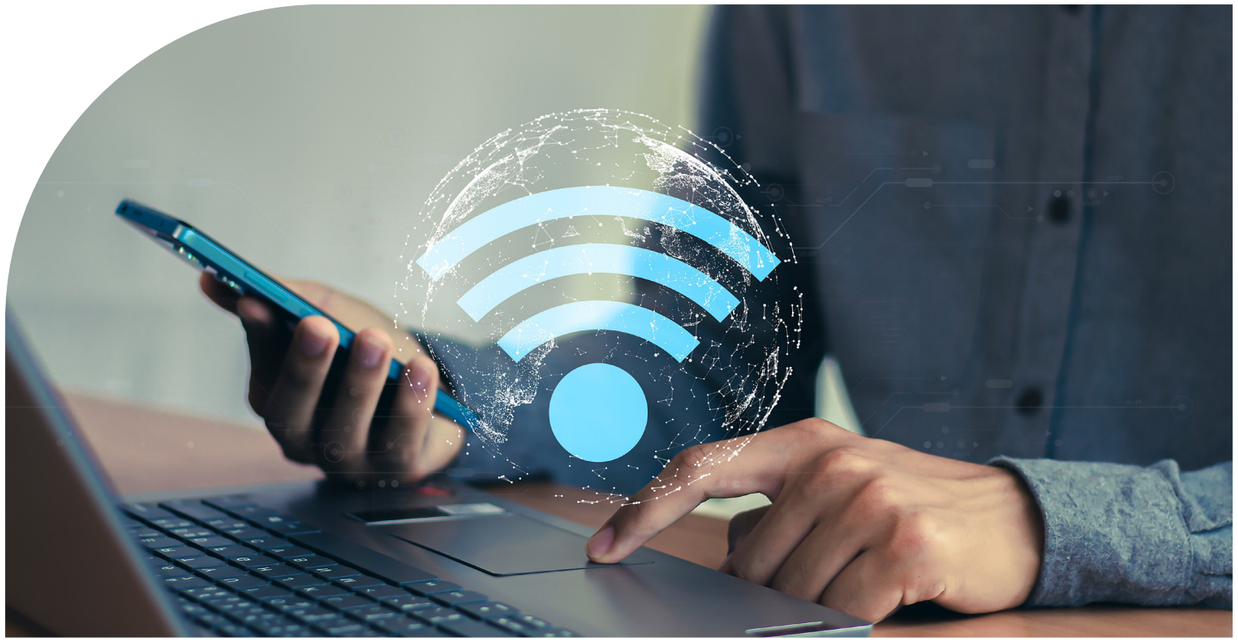
Over in the Advanced Exploitation corner, Aaron Adams produced a blog write-up of exploitation of an issue which a colleague at NCC was wanting to exploit on a security engagement. Having no public exploit working for this vulnerability within Redis in an Alpine container environment, Aaron developed one and wrote about the technical challenges faced.

**Pumping Iron on the Musl Heap – Real World CVE-2022-24834 Exploitation on an Alpine mallocng Heap**

This led to the publication of the following blog post:

**Read Here**





**Puckungfu 2: Another NETGEAR WAN Command Injection**

This blog post by McCaulay Hudson describes an issue which was found prior to Pwn2Own 2022 on NETGEAR RAX30 home router devices. With SoHo router device exploitation being topical throughout the year, NCC EDG's research examined a number of these devices previously.

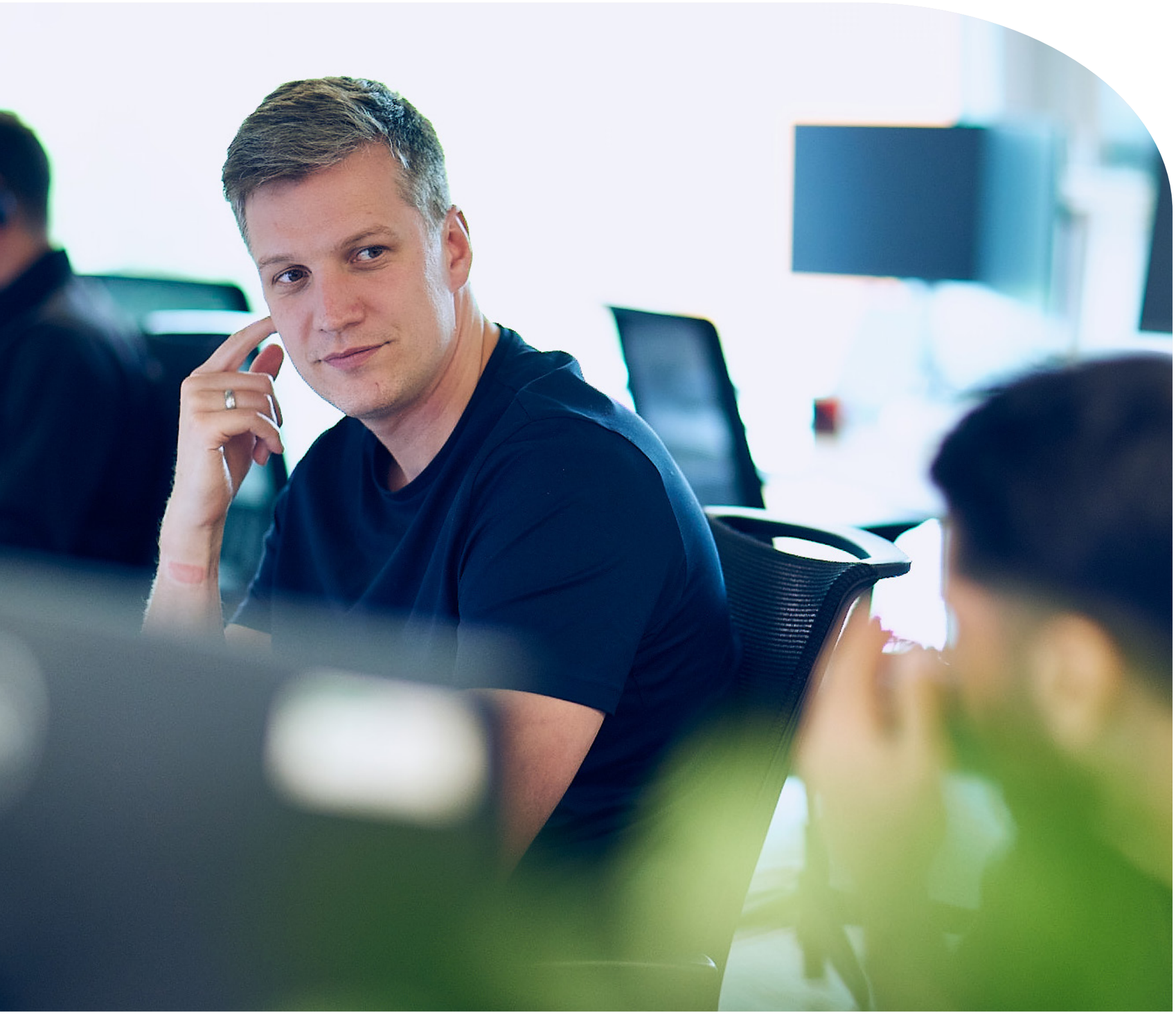
This led to the following blog post being published on the NETGEAR during 2024:

**Read Here**

# Exploitation Training

Cedric Halbronn presented training at OffensiveCon around Windows Exploitation foundations during 2024. The details on the course were as follows:

**Read Here**



Section 08

# Acknowledgements

We extend our deepest gratitude to the dedicated researchers, engineers, and collaborators whose hard work and innovation have made this year's achievements possible. Your expertise, creativity, and unwavering commitment to advancing cybersecurity continue to drive meaningful change.

Finally, we recognize the broader cybersecurity community for fostering an environment of knowledge sharing and collective action. Together, we are building a safer, more secure digital future. Thank you for being an essential part of this journey.

Section 09

# About Research at NCC Group

NCC Group employs some of the most talented security consultants and researchers on the planet, serving 15,000 clients worldwide and uncovering countless vulnerabilities per year through both client work and independent vulnerability research. With hundreds of specialized consultants, our technical security research areas extend into almost every area of security, as well as global standards bodies including CIS Benchmarks. We perform offensive and defensive research across a vast range of targets including blackbox and whitebox testing of previously unanalyzed emerging technologies and computational architectures.

We publish research in a variety of subfields including applied cryptography, hardware and embedded systems, secure coding and programming languages, browser and client-side security, cyber-physical systems, operating systems and their internals, mobile security and privacy, application security, privacy enhancing technologies, distributed systems, network and protocol security, cloud, containerization, and virtualization, and both offensive attacks on – and defensive uses of – machine learning and AI systems.

You can find samples of some of our recent public-facing work, including blog posts, whitepapers, conference talk listings, and technical advisories on our Research Blog, alongside our technical Twitter (X) account and our public GitHub which hosts over 300 open-source tools and datasets authored by NCC Group researchers. We also have deep academic research partnerships with several leading universities, as evidenced across several of our research publications. NCC Group also regularly conducts publicly reported security audits across a range of high impact and security-critical technologies.

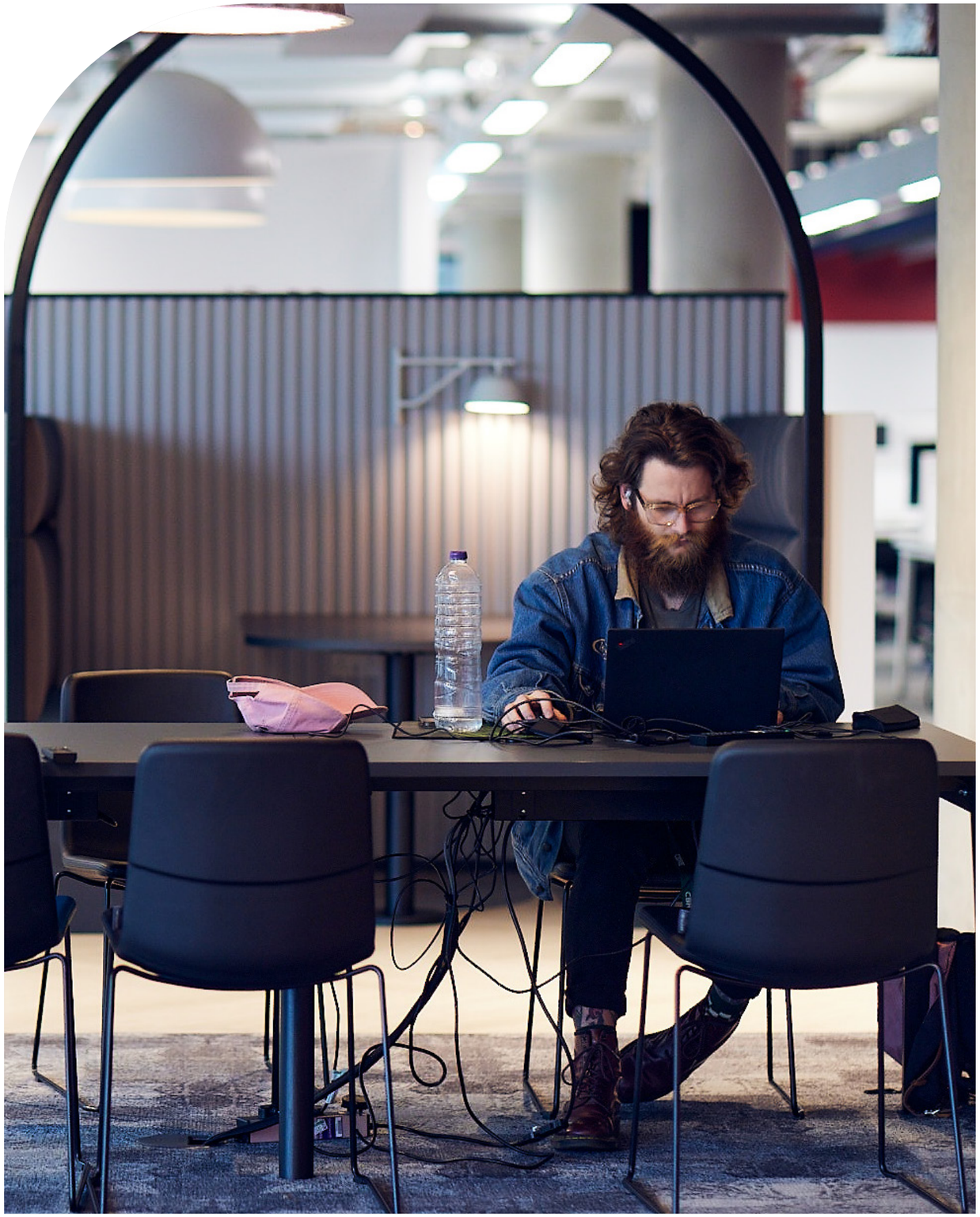
Our technical capabilities extend beyond our public-facing work, to include our internal-only groups and resources, including our world-class Exploit Development Group (EDG), Threat Intelligence Team and Full Spectrum Attack Simulation (FSAS) group, as well as several technical specialty practices and hundreds of pieces of unpublished proprietary tooling.

Our research program delivers thousands of research days annually, by researchers at all levels from across our global business. We support our researchers through a full-time technical research leadership team, mentorship and coaching, incentives and awards, and collaboration within and across several internal research groups. We regularly present our work in top research venues including Black Hat USA, Shmoocon, Hardwear.io, REcon, Appsec USA, Toorcon, BSidesLV, Chaos Communication Congress, Microsoft BlueHat, HITB Amsterdam, RSA Conference, CanSecWest, OffensiveCon, DEF CON, and countless others.

Our research is regularly covered by publications including Wired, Forbes, The New York Times, Politico, DarkReading, Techcrunch, Fast Company, the Wall Street Journal, The Register, SC Magazine, and The Hacker News, Bleeping Computer, Trend Micro, and Security Week, alongside other mainstream and trade publications globally.

**Read Here**

@nccgroupinfosec



# People powered, tech-enabled, cyber security

NCC Group is a global cyber business, operating across multiple sectors and geographies.

We're a research-led organisation, recognised for our technical depth and breadth; combining insight, innovation, and intelligence to create maximum value for our customers. As society's dependence on connectivity and the associated technologies increases, we help organisations to assess, develop and manage their cyber resilience posture to confidently take advantage of the opportunities that sustain their business growth.


## Contact Us:
**+44 (0) 161 209 5200**

**XYZ Building, 2 Hardman Boulevard**
**Spinningfields, Manchester**

**www.nccgroup.com**