Seungpyo Hong

Offensive Security Researcher · Career Statement

newbiepwner@kakao.com Seoul, South Korea phantomn.github.io phantomn ph4nt0m

Summary

Offensive Security Researcher with 24+ delivered projects spanning financial-sector Web/App penetration testing, OT/ICS (IEC 62443), IoT and medical-device (FDA) security, and cyber-defence exercise development. Achilles Communication Certificate Level 2 for an LS ELECTRIC automation device; NATO CCDCOE Locked Shields 2025 overall 6th of 17 and DFIR track 1st; 16 Linux kernel CVEs, 5 IoT CVEs, 3 LLM inference-engine CVEs, and 4 FVEs.

Core Competencies

- Financial and public electronic-finance Web/App penetration testing — 12 sites across savings banks, capital, securities, insurance, and manufacturing (A3 Security)
- OT/ICS security — IEC 62443-4-2 threat modeling and penetration testing; Achilles Communication Certificate Level 2 for an LS ELECTRIC device
- IoT vulnerability analysis and security tooling — smart-building IoT detection, IoT/CCTV incident-response tooling, and 16 CVEs from a Linux kernel filesystem fuzzer
- Medical-device security — FDA eSTAR consulting, Web/App and device penetration testing, and Cybersecurity Controls certification support
- Cyber-defence exercise development and operation — KEPCO ELECCON, NATO CCDCOE Locked Shields 2025 (overall 6th of 17, DFIR 1st), APEX 2025/2026 Green Team, DFIR challenge development

Experience

CoreSecurity, Associate Researcher, ICS Security Research Team — Seoul
June 2021 – present
5 years 4 months

- OT/ICS security — IEC 62443-4-2 threat modeling and penetration testing, Achilles Level 2 certification, and automated assessment tooling
- IoT security — smart-building IoT vulnerability-detection technology and its field validation; IoT/CCTV incident-response tooling
- Medical-device security — FDA eSTAR consulting and Web/App and device penetration testing
- Cyber-defence exercises — KEPCO ELECCON operation and challenge development; Locked Shields 2025 (overall 6th of 17, DFIR 1st); APEX 2025/2026 Green Team, DFIR challenge development

A3 Security, Staff, Security Technology Team — Seoul
June 2020 – June 2021
1 year 1 month

- Penetration testing of 12 financial and public electronic-finance sites — 1–2 high-severity findings per site on average
- Security review of non-standard systems — KT GiGA Genie AI speaker, NongHyup RPA, DB Insurance claim-call
- ISMS / ISO 27001 certification support consulting (Coway)

OT/ICS Security (IEC 62443)

Achilles Communication Certificate Level 2 for an LS ELECTRIC automation device — 2024.07 – 2025.03 · Contribution 100%

Pre-assessment, testing, and remediation to obtain the international communication-robustness certification (Achilles Level 2) for the LS ELECTRIC PLC line, which must keep control functions running under DoS, storm, and malformed-traffic conditions.

- Communication-robustness testing of the PLC line across all Achilles Communication Certificate Level 2 test items
- Storm/fuzzing/malformed-packet resilience testing and defect reproduction against communication stacks such as the XGT Protocol
- [Result] Achilles Level 2 certification obtained for the LS ELECTRIC PLC line; communication-robustness defects fixed in firmware
- Tools: Achilles Test Platform · XGT Protocol · PLC · Wireshark · Python

IEC 62443-4-2 automated-assessment tooling for LS ELECTRIC 2025.03 – 2025.11 · Contribution 90%

During IEC 62443-4-2 certification prep for the PLC line, component-security requirement (CR) checks were mostly manual. Built tooling to automate the communication-checkable requirements and cut repeated-assessment cost.

- Selected and tooled the IEC 62443-4-2 SL1 requirements that can be automated over the network
- Automated checks across FR2 (use control), FR3 (system integrity), FR4 (data confidentiality), and FR7 (resource availability)
- Built a web UI for target/result management and a result-storage pipeline
- [Result] Automated communication-based IEC 62443-4-2 assessment tool for the PLC line, cutting assessment time versus manual work
- Tools: Python · FastAPI · TypeScript · React · TailwindCSS · SQLite3

LS ELECTRIC automation-device threat-modeling consulting 2023.03 – 2023.11 · Contribution 40%

Systematic threat modeling and validating penetration testing for the IEC 62443-4-2 certification of an automation device (XGI-CPUZ).

- System Definition → Function Point Definition → Data Flow Analysis, with DFDs produced
- STRIDE + DREAD threat and risk assessment
- Threat validation via penetration testing based on the national critical-infrastructure vulnerability-assessment methodology
- [Result] XGI-CPUZ threat-modeling and penetration-testing reports delivered
- Tools: STRIDE · DREAD · DFD · IEC 62443-4-2

Smart-ship infrastructure vulnerability-analysis tooling and security technology 2024.07 – 2024.11 · Contribution 25%

A smart ship's internal CBS mixes Windows/Linux PCs with embedded IoT/IIoT, so ordinary scans cannot reliably identify assets and vulnerabilities. Built an assessment tool based on the national critical-infrastructure guide.

- Windows/Linux assessment checklists based on the national critical-infrastructure vulnerability-analysis guide
- SSDP-discovery-based IoT/IIoT sensing to collect OS, host, and device information
- Mapped NVD/MITRE CVE/CWE to the CBS by CPE and validated command/code-execution flaws with PoC code
- [Result] Shell/PowerShell automation modules and a five-entity vulnerability DB, with CSV and other export formats
- Tools: Python · SSDP · CVE/CWE · CPE · SQLite · Shell/PowerShell

IoT Vulnerability & Tooling

IoT/CCTV incident-response tooling 2022.08 – 2022.12 · Contribution 45%

IoT devices such as CCTV have no standardized evidence-collection procedure or tooling for incidents. Built an automated investigation tool that quickly secures firmware configuration files and logs.

- Designed and built an automated incident-evidence-collection tool for 40 domestic and foreign CCTV models
- UART access, flash dumping, and binwalk-based firmware extraction with full collection of configuration files and logs
- [Result] Field validation at a public agency — collected and analyzed compromise artifacts across 40 device models
- Tools: Python · C/C++ · UART · binwalk · Firmware Dump · Linux

Smart-building IoT vulnerability-detection technology and field validation (Year 1) 2021.08 – 2021.12 · Contribution 40%
Smart-building IoT devices run embedded Linux with a mix of protocols, so ordinary scanning struggles. Needed automated scanning-to-mapping detection technology and a validation testbed.

- Validated IoT scanning via wired (BACnet, KNXnet, Modbus) and wireless (Wi-Fi, BLE) protocol discovery
- Mapped collected data (OS, protocol, firmware, model) to NVD CVE/CWE and developed PoC validation scenarios
- [Result] Built a functional smart-building testbed and validated the detection tool
- Tools: BACnet · KNXnet · Modbus · BLE · CVE/CWE · SQLite

Smart-building IoT vulnerability-detection technology and field validation (Year 2) 2022.01 – 2022.10 · Contribution 40%
Applied Year 1 detection technology to an operating smart building to validate and improve detection accuracy.

- Field validation against a real smart building — collected device/sensor/protocol data and detected vulnerabilities
- Identified true/false/missed positives, derived detection rates, and updated the vulnerability DB
- [Result] Derived accuracy-improvement actions from the field validation
- Tools: IoT Scanning · CVE/CWE · PoC Validation · CSV/Excel Report

KT GiGA Genie AI speaker device penetration testing 2020.10 · Contribution 100%

- Analyzed the UART debug interface of the GiGA Genie AI speaker device
- Assessed the attack surface via Bluetooth communication and Android APK analysis
- Tools: UART · Bluetooth · APK · Android

Medical Device Security (FDA/eSTAR)

Medical-device FDA security consulting 2024.03 – 2024.12 · Contribution 30%
Infrastructure threat modeling through device and integrated-system penetration testing, plus eSTAR submission documentation, to meet the cybersecurity requirements of a medical-device maker preparing FDA premarket clearance.

- Threat modeling of the FDA-certification infrastructure and derivation of threats and mitigations
- Vulnerability validation via penetration testing of the device and its integrated Web/App
- eSTAR submission documentation consulting based on FDA Premarket Cybersecurity requirements
- Tools: FDA Premarket Cybersecurity · eSTAR · Threat Modeling

Medical-device security certification consulting (Cybersecurity Controls) 2024.06 – 2025.03 · Contribution 45%
Design and documentation of cybersecurity controls across device, base station, mobile app, and server for a digital therapeutic (a transcutaneous electrical nerve stimulator for ADHD) pursuing security certification.

- Analyzed communication paths and data flows across device-app (BLE), app-server (LTE/5G), web (HTTPS), and base station (Wi-Fi)
- Designed and validated controls: JWT (HS256)/RTR, OTP signup authentication, password policy, and dashboard RBAC
- [Result] Authored Cybersecurity Controls submission documents covering concurrent-connection limits, session management, and role separation
- Tools: BLE · JWT/HS256 · OTP · RBAC · HTTPS

Federated-learning drug-discovery acceleration project (K-MELLODDY) 2024.07 – 2024.12 · Contribution 30%

A federated drug-discovery (FDD) platform handles multi-institution data and models, so it needs security built into the whole development lifecycle plus real threat controls.

- Analyzed and defined an NIST SSDF-based secure development process for the FDD platform (reviewing IEC 62443, FDA, ISO 27001, EU CRA)
- Identified real threats via FDD threat modeling and applied source-level security controls (API security)
- Established a supply-chain security scheme (SBOM + VEX + EoS) and ran two production-environment penetration tests
- Tools: NIST SSDF · Threat Modeling · SBOM/VEX · IEC 62443 · FDA Cybersecurity

Cyber Range & CTF Development

NATO CCDCOE Locked Shields 2025 — Korea-Canada joint DFIR blue team 2025.01 – 2025.04 · Contribution 45%

Competed in Locked Shields, the world's largest international cyber-defence exercise, on the Korea-Canada joint DFIR blue team. Analyzed compromise artifacts and reported response under live attack.

- Incident forensic analysis and timeline reconstruction under live attack scenarios
- DFIR CTF tasks — artifact analysis and malware triage
- [Result] Locked Shields 2025 overall 6th of 17 · DFIR track 1st
- [Result] Locked Shields 2026 overall 9th of 16
- [Participated] Locked Shields 2026 Korea-Hungary joint Special System blue team
- Tools: DFIR · Volatility · Wireshark · Sysmon · YARA

APEX CTF 2025 — DFIR network-forensics challenge development 2025.06 – 2025.09 · Contribution 45%

- Developed DFIR network-forensics challenges — forensic scenarios based on real incidents
- [Participated] APEX 2025, 2026 Green Team, DFIR challenge development
- Tools: DFIR · Network Forensics · Wireshark

KEPCO practical cyber-security training system enhancement (ELECCON) 2023.06 – 2023.12 · Contribution 30%

- Developed ELECCON qualifier CTF challenges
- Designed and built the finals attack/defence scenario on a power-grid (OT/ICS) environment
- Tools: OT/ICS · SCADA · CTF

Practical cyber-security training system advancement 2022.07 – 2022.09 · Contribution 40%

- Developed practical attack/defence qualifier challenges
- Built the finals attack/defence scenario on a power-grid (OT/ICS) environment
- Tools: OT/ICS · SCADA · CTF

Practical cyber-security training system enhancement (2024) 2024.09 – 2025.02 · Contribution 30%

- Built the finals attack/defence scenario on a power-grid (OT/ICS) environment
- Tools: OT/ICS · SCADA

2024 practical cyber-range course operation (smart-ship port) 2024.07 – 2024.12 · Contribution 20%

- Developed cyber-training content for a smart-ship environment

Hacking-scenario-based hacking-experience operation 2024.11 · Contribution 45%

- Ran a hacking-experience booth targeting IoT devices

C2021 event (ELECCON competition operation) 2021.05 – 2021.12 · Contribution 30%

- Assisted operation of the ELECCON attack/defence competition

Financial/Public Web/App Pentesting

Financial and public electronic-finance penetration testing (12 sites, A3 Security) 2020.06 – 2021.06

Multiple Web/App penetration tests and vulnerability assessments of financial and public electronic-finance infrastructure while at A3 Security. Checked for information leakage and follow-on attack paths and proposed remediations.

- Electronic-finance vulnerability assessment — Web/App penetration testing across financial sites (Cham Savings Bank, Acuon Capital, KOFIA, and others)
- Security review of financial/insurance/manufacturing systems — SBI Savings Bank (open banking, digital branch), Hyundai Motor HKMC, DB Insurance claim-call
- NongHyup RPA source-code review; penetration testing of Daekyo integrated-education platform, Autohands, UNTAC, and others
- [Result] 12 sites tested, 1–2 high-severity findings per site on average, with remediations proposed
- Tools: Burp Suite · OWASP Top 10 · Web/App Pentest · Source Code Review

Security Consulting & Certification

INFINITT DPS medical-imaging platform penetration testing 2024.07 – 2024.09 · Contribution 70%

Checklist-based vulnerability assessment and penetration testing of the Web and mobile (Android/iOS) services of a medical-imaging platform (DPS), checking for information leakage and follow-on attack paths.

- Manual Web/Mobile assessment based on the national critical-infrastructure guide and OWASP Top 10 2021
- Checked authentication, access-control, and input-validation flaws with Burp Suite, Wireshark, and APKTool
- [Result] 14 findings identified (3 medium, 11 low), all remediated on re-test; lead author of the English report
- Tools: Burp Suite · Wireshark · APKTool · OWASP Top 10 · Android/iOS

Coway certification support consulting (ISMS, ISO 27001) 2020.11 · Contribution 40%

- Delivered ISMS and ISO 27001 certification-support consulting

Information-security consulting engagement 2024.10 – 2025.01 · Contribution 25%

- Delivered an information-security consulting engagement

Vulnerability Research

16 OS kernel CVEs — Best of the Best 8th: Designed and built a custom filesystem fuzzer that surfaced 16 Linux kernel CVEs (including 0-days). Presented at CodeBlue 2019 (Tokyo) and Hack In The Box 2019 (Amsterdam).

5 IoT CVEs — independent research: Embedded/IoT device vulnerability analysis. CVE-2024-33788/33789/33791/33792/33793 (up to CVSS 9.8 CRITICAL).

3 LLM CVEs — independent research: llama.cpp inference-engine vulnerability analysis. CVE-2026-52130/52131/52132 (two remote unauthenticated DoS at CVSS 7.5; one abort on loading a malicious GGUF model).

4 FVEs — Findthegap bug bounty: Four web-vulnerability reports against a bug-bounty platform (details undisclosed).

Certifications & Education

- Linux Master Level 2 (KAIT, 2021.07)
- Network Administrator Level 2 (KAIT, 2024.07)
- B.S. in Computer Science, Kongju National University (2012.02 – 2020.02)
- Cheonan Commercial High School, Information Processing (2009.03 – 2012.02)