SECURITY EXPLORATIONS IN A NUTSHELL

Dec 2025

BASIC INFORMATION

Security Explorations (https://security-explorations.com) is a security research laboratory of AG Security Research company (https://agsecurityresearch.com). The lab came to life in 2008 as a result of a true passion of its founder for breaking security of things and analyzing software for security defects.

The founder

Adam Gowdiak received M.Sc. degree in Computer Science from the Poznan University of Technology. Prior to founding Security Explorations, he worked for the Poznan Supercomputing and Networking Center and Sun Microsystems Laboratories. For over 8 years, he was also an active member of a notable Polish security research group called The Last Stage of Delirium, or LSD.

Adam is an experienced Java Virtual Machine hacker, with over 100 security issues uncovered in the Java technology over the recent years. He is also the Argus Hacking Contest co-winner and the man who has put Microsoft Windows to its knees (the original discoverer of MS03-026 / MS Blaster worm bug).

PRO BONO SECURITY RESEARCH

Security Explorations has been always involved in hacking various Java based products. Over that time, we conducted several non-commercial (Pro Bono) security research projects that resulted in a discovery of dozens of highly critical security issues.

- In 2012, we showed that digital satellite TV set-top-boxes used by a major Polish satellite TV platform could be infected with malware just in the same way as PC systems are these days,
- In 2012 and 2013 we demonstrated that security of Java SE technology used by nearly a billion of users around the globe was far below the standard,
- In 2013 we broke security of Oracle Java cloud service and showed that user applications and data were not properly safeguarded in Oracle cloud environment,

- In 2014, we broke security of Oracle Database that according to Oracle CEO "hasn't been broken into for a couple of decades by anybody" and that is "so secure, there are people that complain",
- In 2014 and 2015, we discovered multiple vulnerabilities in Java security sandbox used in Google Cloud environment
- In 2019 we discovered over 30+ security vulnerabilities in a reference implementation of Java Card technology from Oracle used in financial, government, transportation and telecommunication sectors among others. Contrary to one of the major SIM card vendors' claims, we proved that Java Card vulnerabilities do matter. We showed that they can be instrumental for a discovery of far more serious issues such as a remote, over-the-air Gemalto SIM card applet loading vulnerability.
- In 2022 we conducted security analysis of Microsoft Play Ready content protection technology in the environment of CANAL+ SAT TV operator. As a result, a significant PlayReady limitation and a fault at CANAL+ end were discovered and access to over 18k+ movie assets available in CANAL+ VOD library was demonstrated (massive piracy).
- In 2023, we discovered multiple security vulnerabilities in Telit Cinterion IoT modem gateways targeting automotive, medical, energy and telecom industries. The end result was a complete device compromise (code execution at ARM Supervisor level) from a remote network location (triggered through SMS message, only phone number of a target device would need to be known for a remote attack)

One of the missions of Security Explorations is to increase general awareness of users and vendors in the area of computer and Internet security. Pro Bono security research has been always the essential part of that mission.

CUTTING-EDGE SECURITY RESEARCH

We were the original discoverers of a key deficiency of Java SE security model (Reflection API weaknesses and RMI attack vector, both reported to the vendor in 2005), that has been plaguing the technology for the last decade and has manifested itself in a form of dozens of security vulnerabilities affecting software and online services coming from Apple, Google, IBM and Oracle.

We were the first to break security of:

- Java for mobile phones (J2ME) with MIDP 2.0 security features aimed at protecting users and devices from malicious software,
- Nokia Series 40 Platform devices,
- digital satellite TV set-top-boxes running Java MHP middleware from Advanced Digital Broadcast,
- secure cryptographic processors from STMicroelectronics used to secure HDTV content broadcasted by various SAT TV operators around the world (STi710x and STi7111 DVB chipsets),
- Java based cloud hosting environments coming from Oracle and Google (Oracle Java Cloud Service and Google App Engine for Java),
- EAL4 certified Kigen eUICC (eSIM) card with GSMA consumer certificates installed into it

We were also the first to:

- discover and implement an attack against a mobile 3G phone allowing for a remote deployment and execution of a malicious Java application (i.e., a backdoor, malware or virus),
- demonstrate novel techniques for both a setup and exploitation of type confusion vulnerabilities in Java environments,
- demonstrate novel techniques for a security compromise of Oracle Database with the use of Java security vulnerabilities,
- demonstrate GSMA certificate theft and abuse for plaintext eSIM profile download and SIM (subscriber) spoofing.

INFLUENCIAL SECURITY RESEARCH

Although we are a one-man shop, our research sometimes influenced the decisions and actions of the biggest players in the industry. This further often implicated the software experience of millions of users around the world.

Our Java SE security research has been in particular very influential and was followed by an enormous set of events. Just to mention the following:

- Apple, Google, Microsoft and Mozilla blocked Java in their web browsers,
- US Department of Homeland Security warned users about Java security risks,
- Certain financial institutions decided to move away from client-side Java (Applets),
- Federal Trade Commission started investigation against Oracle over deceptive Java security updates,

Our Oracle Database security research has forced Oracle to start providing regular security updates to the embedded Database Java VM.

Our digital satellite TV research has again raised a question whether a secret implementation embedded in a silicon can be trusted. It also questioned the worthiness of security certifications awarded to such "closed" solutions by "renown security evaluation laboratories".

As a result of our eSIM security research, GSMA organization decided to shut down all test (TS.48) profiles. GSMA also published Application Note to provide guidance for the industry in order to avoid the misuse of Remote Application Management (RAM) keys to install, within Profiles, a malicious Java Card Applications in an eUICC supporting Java Card technology.

RESEARCH WITH A REAL CONTRIBUTION TO THE FIELD

The results of our researches have been used or been a subject of interest[1] to both the industry and academia. This includes, but is not limited to the following:

- major software and hardware vendors,
- security companies such as firewall vendors and antivirus companies,
- world's top universities[2],
- world's top research laboratories and think-tanks,
- world's top financial institutions,

[1] as indicated by IP addresses recorded in our web server logs in a time period of Feb 2018-Jun 2019.
[2] 10 of the top 20 universities from Academic Ranking of World Universities (Shanghai Ranking 2018).

- renown international organizations,
- cyber threat analysis companies and organizations,
- major cable and SAT TV operators,
- government institutions,
- military and intelligence agencies.

REWARDED SECURITY RESEARCH

Our research and its thoroughness were recognized by some vendors. In 2015, Google issued a total of 100 000 USD in rewards to Security Explorations for a security research project targeting Google App Engine. In 2025, Kigen issued 30 000 USD reward for the detailed work we have performed to identify the vulnerability affecting company's eUICC card.

RESEARCH FEATURED IN THE MEDIA

Our research was featured over 200 times in various digital and printed media publications. This includes renown media outlets such as Reuters, Forbes, Bloomberg, CNN or NBC News and international technical news portals (Computerworld, Ars Technica, The Register, Dark Reading, Security Week, SC Magazine, PC World, ZDNet, InfoQ and Softpedia among others).

NO EXPLOIT SALES / NO NATION STATE INVOLVED

For nearly 18 years of our activity, only original vendors responsible for the fixing of the reported issues were provided with their technical details. We neither sold, nor provided any vulnerability information or Proof of Concept codes to anyone else prior to their publication. This in particular concerns, but is not limited to:

- various nation states or defense contractors acting on their behalf,
- security vulnerability brokers.