SECURITY EXPLORATIONS IN A NUTSHELL

BASIC INFORMATION

Security Explorations (http://www.security-explorations.com) is a security company from Poland, providing various services in the area of security and vulnerability research. The company 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 is the company's founder and CEO. He 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 involved in hacking various Java based products for the last 8 years. 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.

One of the missions of our company is to increase general awareness of users and vendors in the area of computer and Internet security. Pro Bono security research is the essential part of that mission.

CUTTING-EDGE SECURITY RESEARCH

We are 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),

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.

INFLUENCIAL SECURITY RESEARCH

Although we are a small security outfit, our research sometimes influences the decisions and actions of the biggest players in the industry. This further often implicates 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.

Finally, 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".

REWARDED SECURITY RESEARCH

Our research and its thoroughness was recognized by Google. In 2015, the company issued a total of 100 000 USD in rewards to Security Explorations for a security research project targeting Google App Engine.

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).

INDEPENDENT SECURITY RESEARCH

Our ambition is to conduct quality, unbiased, vendor-free and independent security and vulnerability research. We are immune to various games tried by vendors and aimed at influencing the disclosure process and/or a content of our publications.

This is the primary reason for applying the following informal rules during our contacts with vendors (real cases for our Pro Bono research outlined below):

- we never formalize any business relationships with vendors of affected technologies prior to the release of the fixes / prior to the release of the content of our publication,
- we never sign any NDA that would impact the disclosure process,
- we never provide a vendor with an advanced copy of our publications ("preview copy of a presentation", etc.),
- we never limit the disclosure of vulnerabilities details in exchange for prospects of a business cooperation.

Our non-commercial security research is 100% self-founded and the choice of its targets is not influenced by any 3rd party.

NO EXPLOIT SALES / NO NATION STATE INVOLVED

For our non-commercial security research, only original vendors responsible for the fixing of the reported issues are provided with their technical details. We neither sell, nor provide 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.

SHOWING THE REAL STATE OF SOFTWARE SECURITY

Over the recent years, we were one of key players that exposed vendor's incompetence and negligence regarding security of software:

- We showed that security issues discovered in IBM, Google and Oracle products violated Oracle's "Secure Coding Guidelines for the Java Programming Language",
- We exposed questionable software quality assurance processes of IBM and Oracle by discovering multiple instances of improperly patched security vulnerabilities we reported to both companies,
- We revealed that both Google and Oracle were hosting user applications on outdated (1+ years old) and insecure versions of Java Runtime in their cloud environments,
- We showed that new security features introduced to Oracle code were not thoroughly reviewed. We demonstrated that Click2Play security feature introduced by Oracle to Java in order to protect against malicious Java content was not providing any protection to users,
- We proved that Oracle was not delivering true statements regarding the impact of security vulnerabilities patched. The company claimed that Java security vulnerabilities were limited to the web browser only. We proved that these vulnerabilities could be remotely exploited on servers. We also demonstrated that these vulnerabilities affected Oracle's own Java cloud service offering and that they were instrumental to break security of "unbreakable" Oracle Database,
- We showed that contrary to Oracle statements, patching Java SE bugs could be done within hours, not months,
- Finally, we showed that Oracle was not delivering database patches to all clients at the same time. As a result the company was exposing its customers at the risk of being hacked.