SECURITY EXPLORATIONS

SECURITY EXPLORATIONS

FREQUENTLY ASKED QUESTION

How big is your company ?

It's a one man shop (it always has been).

Don't you think this is not sufficient to successfully complete large commercial assignments (evaluate security of large SW / HW) ?

Over the years, Security Explorations has shown that it was able to successfully complete such projects as proven by our non-commercial research available on the website. The company was able to find dozens of security vulnerabilities (20+ on average per vendor / project) missed by security teams of major software vendors, found instances of broken patches and even security issues in HW (such as in secure processors). All, by the means of a pure binary reverse engineering process, which is more difficult and time consuming than source code analysis.

We believe that it's not about the size of the company, but 20+ years long experience, quality and unique skills.

In 2012 / 2013, Security Explorations discovered over 40 security issues in Java SE from Oracle, which has caused significant havoc for the company. Years later, former SVP at Oracle disclosed that "the security issues in Java forced Oracle to move close to 50 engineers into a dedicated security group" [1].

The above speaks for itself and serves as a perfect summary of our capabilities.

Where does your funding come from ?

We are 100% self-funded (no VC / investor involved). Our operation is primarily funded through commercial security research and services provided to 3rd parties.

Does your company sell 0-days ?

We have a commercial service (Security Research Program - SRP) through which access to the results of our research (i.e. technical vulnerability details, Proof of Concept codes or tools) could be gained on a fee basis. In some cases, this may include 0-days as well.

We also have the offensive capabilities development service in our offering of which goal is to discover a previously unknown security vulnerability (0-day) in a given product and develop a reliable Proof of Concept code for it.

Does your company purchase vulnerabilities and exploits from a third party?

No. We do not rely on any 3rd party when it comes to security research. All of our R&D regarding vulnerabilities discovery and Proof of Concept codes development is conducted by our company.

What are your company's platforms of interest for vulnerabilities R&D (Microsoft Windows / Linux / Apple iOS / Google Android / OSX / Web applications and services / etc.) ?

We do not limit our R&D interests to specific platforms or technologies.

It is common for us to research a given target completely from scratch. We have proven many times that we can find many security vulnerabilities in a target that was not known by us prior to the engagement.

I don't understand your business model. What's the purpose of releasing research worth many dollars for free to the public ?

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.

Do you participate in Bug Bounty programs ?

We prefer to work on different terms and be compensated for the actual security evaluation / analysis work being done than per the number of bugs found as in bug bounty programs. Bugs are not equal with respect to the time / efforts required to spot them. Same when it comes to their severity, impact and exploitation.

In a Bug Bounty model, security analysis of a given code / software component yielding no vulnerabilities is the unpaid work, although it may still provide a valuable result to the customer (a given skilled party did analyze a given code and found it clean).

I would like to hire you for a gig in a specific geographical location ? Is that possible ?

In general, we conduct all of our security evaluation assignments remotely from our lab in Poznan, Poland. That said, we do not work in customer locations as this could unnecessarily expose our tools and know-how among others.

Our visits to on-site customer locations are limited to general meetings with management and engineering staff for technical, informational or business purposes.

Do you take all assignments ?

We do our best to assist all customers looking to evaluate security of their solutions. However, in some rare cases, we cannot accept a given assignment. This is usually due to our busy schedule or Non-Disclosure Agreements.

How do you choose your targets ?

There is no formula behind which product / vendor we put under the microscope. It's a combination of our interests, experience, intuition, general directions and conditions of information security market.

Over the years, we built a list of 20+ targets that we believe are worth having a deeper look from a security perspective. We always find it handy when selecting a topic for a new security research, though some entries need to be replaced with others from time to time.

How do you know that a given project will be successful ?

We never know that. This is the risk, which is an imminent part of our profession.

What's your policy regarding bug collisions ?

Occasionally, we do encounter bug collisions with other researchers or vendors. Our policy is to not publish any announcement regarding "lost vulnerabilities", which has not been reported to the vendor yet. Again, we treat this as the risk being part of our profession.

Why do you keep hacking Java related targets ?

The answer is simple - we love to break Java based products. Due to Java ubiquity and widespread use, Java hacks are often prerequisites to successful completion of various interesting research projects (i.e. SAT TV set-top-boxes, database, cloud).

Can you disclose what you are currently working on ?

As a rule, we don't reveal the targets of our not yet published research projects. Disclosing the topic of our current / upcoming research might easily lead to the project failure.

Can you share any perspectives you might have, trends you see, predictions for the future ?

For similar reasons outlined above, we cannot do that as trends and prediction often overlap with our own research interests and projects.

What are the main obstacles you encounter in your work ?

Occasionally we experience difficulties when it comes to an access to a given technology or software for security evaluation purposes (non-commercial security research).

Most notable cases:

- In Apr 2013, we asked Juniper for access to Junos SDK and Junos Space SDK in order to evaluate the capabilities of its devices and the SDK itself. Both were supposed to be available to all registered developers per information on Juniper pages, but in reality this was not the case. We exchanged several mails with Juniper people on the topic and finally gave up as it didn't look promising. We concluded that they would not give us access to their SDKs as we experienced similar difficulties / questioning before with another company (successfully hacked regardless of the obstacles experienced).

- In Oct 2015 we informed Oracle that we were interested to evaluate the security of Oracle M7 SPARC chip and its Silicon Secured Memory feature in particular. We told the company that we could conduct the whole analysis for free as long Oracle provided us with the necessary hardware and the results of the analysis could be made available to the public. Oracle didn't express any interest in our offer.

Are you treating Oracle as an enemy ?

We are not enemies of Oracle or any other company. We are enemies of incompetence, negligence and false / misleading statements when it comes to software security.

We do our best to treat all vendors the same. Our GAE for Java (SE-2014-02) research project (awarded $100k by Google) serves as the best example of that:

- Google was not provided with an advanced copy of our project report prior to its publication (we never do that),
- the company was subject to the same criticism due as in case of other vendors from the Java ecosystem,
- unpatched vulnerabilities' disclosure was triggered by the same events as for other vendors (silent fixes, no status information / vulnerability confirmation).

Have you ever been engaged by Oracle to improve Java security ?

Over the recent years there were several attempts from both sides aimed to evaluate the feasibility of a cooperation between the two companies. All of them failed. That said, we have never been cooperating with Oracle on a commercial basis.

Any chances to see you finally cooperating with Oracle ?

We are always open to work with Oracle or anyone else provided that there is a proper ground and will for such a cooperation. At this moment we are not aware of any with respect to Oracle.

Have you ever received a prospect of a business relationship in exchange for a limited vulnerability disclosure ?

In 2012, we received a vague proposal from STMicroelectronics that sounded like this. The company stated that it is ready to allocate financial resources to build with us a cooperation which will be publicly acknowledged.

At the same time, the company representative hinted that we should consider limited disclosure of the details pertaining to the vulnerabilities found in their set-top-box chipsets.

ST proposal was not considered by us. We prefer to work with companies that come to us because they want to use our skills to improve security of their products, not to achieve a limited vulnerability disclosure of our own, non-commercial projects.

Have you ever received a legal threat from any company ?

Not in a direct or legally formalized way as this would be immediately published by us in a "Legal Threats" section of our website.

It's however worth to mention that STMicroelectronics did send us a message a few days prior to our planned Hack In The Box Security Conference talk in which among other things and in a very careful wording the company indicated that publication or disclosure on the process we followed to extract control word from ST devices will damage ST and other vendors in the ecosystem.

ST message was ignored on our side and we proceeded with full disclosure of the issues in company products during our talk.

Have you ever profited from your discovery of ST vulnerabilities and an illegal sharing of a protected TV content / SAT TV signal / CWs in particular ?

No. Suggesting that this might have been the case is highly improper. It manifests a common perception of security researchers investigating security of a SAT TV ecosystem in terms of TV pirates.

Security Explorations neither promotes, nor encourages the acts of a digital satellite TV piracy.

How do you deal with representatives of foreign governments or companies having closed ties with secret agencies ?

We require that any contacts with such entities take place on a formal / official / commercial ground and are conducted directly (not through cover-up / proxy companies or individuals). We in particular require the following:

- for meetings:
  - a brief reason for the request to meet, brief agenda for the meeting along with information about its participants needs to be provided,
  - a copy of any NDA document required prior to the meeting needs to be provided,
  - an initial meeting needs to take place in a given government / agency location (HQ, Embassy or Consular office),
- for communication:
  - all communication needs to take place with the use of official e-mail / postal addresses,
  - any messages exchanged cannot be anonymous (full name of a person behind each message received needs to be known),
  - all sensitive information needs to be encrypted with the use of asymmetric cryptography (PGP, GPG, etc.).
- for accounting:
  - all services provided are invoiced in accordance with Polish laws,
  - all payments need to be done via wire transfer.

Why are you so careful about contacts with representatives of foreign governments ?

There are two primary reasons for it:

- when providing services to foreign governments we need to make sure that everything is done in accordance with Polish laws / international laws Poland is a signature of,
- we have reasons to believe that not all governments operate within the rules of law (i.e. some express an interest in "cloud / web applications capabilities", but do not provide any clarification regarding legal basis such capabilities could be arranged for them).

Would you come to give a talk at my security event / conference ?

In the beginning of our activity, we did publish the results of our research by the means of conference presentations. As a rule, we never did any talk twice to make sure that an audience was always provided with both novel and never published before content.

Over the recent years, we moved towards a publication model through our website. That said, our public appearances are currently limited to invitation only talks.

Due to the fact that some event organizers do not understand the obligations / good practices associated with a term *invitation*, we currently require that an inviting party covers in full both our hotel stay and air trip costs to the event.

Additionally, for commercial events we require that an organizer provides a honorarium equal to 2 weeks of our work (the average time it takes us to prepare a conference presentation).

Would you be interested to join our security team ?

We are not considering any career changes at the moment as we love what we do at Security Explorations. We also want to live and work in Poland.

That said, the only viable option to have us work exclusively for other company is to acquire Security Explorations and turn it into its Polish, Poznan city office.

Do you support full disclosure of security vulnerabilities ?

We support publication of vulnerability information. Such information dissemination usually allows to improve the overall state of the art of the whole security field.

Why do you notify the public about the existence of the issues found at the same time they get reported to vendors ?

After dealing with various vendors for over 20+ years, we believe that such a transparency allows to either avoid or immediately expose many problems during vulnerability handling. This in particular includes denial of a reported vulnerability, silent fixes or long time to patch.

We don't give vendors any deadline with respect to the fixing of reported issues. We understand that some issues (especially architecture ones) may take more time to fix than others. The only obligation vendors have is to confirm or deny reported issues to us and provide status reports regarding the fixing process.

The public can monitor vendor's progress from a time of a bug report to its patch. They can make own judgments regarding vendor's handling / evaluation of security vulnerabilities and if necessary

can inquire or press vendors to act faster. On the other hand, vendors have a great opportunity to prove they do take security issues seriously and can deliver fixes faster than anticipated.

Why are you releasing Proof of Concept codes ?

Proof of Concept codes are the only way to show the real impact of security vulnerabilities. One needs to remember that bug discoverers like to overrate their findings in order to gain publicity, while vendors tend to downplay bugs importance to calm down their customers. Proof of Concept codes usually allow to verify claims of both parties. They also allow to verify the presence of vulnerabilities in a target software. Not to mention that they are very handy to verify the operation of patches and protection measures.

Can you keep information deemed as confidential that way ?

We are the subject to various strict Non-Disclosure Agreements (NDAs) and have a very good understanding of confidentiality. It is our uttermost priority to make sure that everything confidential and subject to NDA stays so.

We require mutual NDAs from all parties willing to start any serious business talks with us. Parties that either ignore / do not want to sign mutual NDA at some stage of our talks are deemed as unprofessional and we do not perceive them as potential business partners.

How do you make sure that your research material is not leaked to the public ?

Our research materials are always stored in encrypted form on a system that is never connected to any network. Similarly, all of our PGP keys are also stored in a physically isolated system. No sensitive material is stored by us on any of our Internet connected systems.

REFERENCES

[1] How many software engineers does Oracle have working on Java?
https://www.quora.com/How-many-software-engineers-does-Oracle-have-working-on-Java