SECURITY EXPLORATIONS

FREQUENTLY ASKED QUESTION

How big is your company ?

For various reasons, we don't reveal the actual number of people working for Security Explorations. It's sufficient to say that we are a small security outfit.

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 don't sell 0-days.

In the past, we had a commercial service (Security Research Program - SRP) through which early access to the results of our research (i.e. technical vulnerability details and Proof of Concept codes) could be gained on a fee basis, but this program has been suspended and we do not provide any similar service at the moment.

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).

We can offer you a Research Grant of $3k USD to take a quick look at our solution. Would you be interested ?

Unfortunately, the grant amount does neither corresponds to the pricing for commercial services published in our services section (price list), nor it reflects the usual Research Grant amounts (typically starting from $50k-$100k).

This offer manifests a typical misunderstanding of our operation. The fact that we do a lot of non-commercial research does not mean that we do commercial work for peanuts or for free.

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 for such a cooperation. At this moment we are not aware of any such a ground with respect to Oracle.

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

We once received a vague proposal from one vendor that sounded like this.

The proposal was not considered by us as 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 research 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. Some carefully worded statements about the harm / damage of a planned disclosure to a given company / ecosystem do happen.

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

We are always very cautious upon such contacts. In particular, we don't take part in any informal meetings with representatives of foreign / domestic governments, agencies or their affiliates.

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).

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,
- 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.

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.

There is no company twitter account for Security Explorations. Any chance of creating one in the future ?

We are indeed not present on Twitter. If anything changes in that matter in the future, we'll make a proper announcement on our website.