DSI Industrial & Policy Recommendations (IPR) Series
Vulnerabilities in IT-Security Products

In October 2016, the Digital Society Institute hosted a workshop dedicated to the topic of vulnerabilities at large and in particular of vulnerabilities in security products. The workshop included talks from Thomas Dullien (former Google Project Zero), Matthias Luft (ERNW), Dr. Christoph Peylo (T-Labs) and a comment from Michael Kranawetter, (Head of Information Security Microsoft Germany).

The state of vulnerabilities in IT-security products

As the workshop participants identified, IT-security products commonly suffer from security issues. Even though their basic paradigms haven't evolved significantly from signature-based detection, they have to do a lot of parsing, perform many different tasks on different processes, in turn generating a high internal complexity and a high number of vulnerabilities in code and processes. Defect rates can be much higher than in other software products and persistent, as the IT-sec industry is still dominated by SMEs, who are not able to invest into expensive procedures for software quality assurance or verification.

Most security products also lack basic security features in themselves, examples including ASLR (Address Space Layout Randomization) or sandboxing, and run in privileged mode with high levels of access across the systems they are supposed to protect. Many of these issues are well known throughout the industry, but not tackled as solutions are deemed too costly and as the uninformed market doesn't demand them. Sadly, the market rather rewards fancy slideshows and interfaces, so money is put into marketing rather than quality assurance. Much of the actual innovation effort is devoted to keeping pace with the race of innovations in the underlying systems to be protected, so the security products can deliver their functions in a constantly changing environment.

Given the high defect rates, the bad coding and quality assurance practices and the lack of basic security features while running on high privileges in the system, IT-security products are attractive and willing targets for attackers. The workshop group deemed it likely that any system expecting mid-level or targeted attacks will suffer a net loss in security, if IT-security products are implemented.

Creating transparency for the security of IT-security products is a demanding task. Objective, scientifically valid methods to assess the security quality of the products do not exist, nor is there an entity conducting such assessments. Pen testing usually doesn't include a test of the security environment as an attack surface, and reverse engineering IT-security products is mostly illegal as it violates the EULA and is not easy for security testers as higher-end security products are very expensive. In addition, there is no tolerance in the IT-security market for an open discourse about the weaknesses and vulnerabilities of IT-security products. Publications of tests are usually met with law suits and immediate demands to

withdraw all publicized material, as has just happened in the case of the FireEye-hack "Playing with Fire".

Certifying security products could be an option, but certification processes are much too slow to warrant competitive advantage through certification. These highly bureaucratic processes take around two years, despite the group deemed it entirely possible to conduct the necessary assessments within three weeks. In this speed, products are outdated when they are finally certified.

Conclusion

Ironically, implementing IT-security products can be dangerous and create a net loss in security, as many of the products are highly vulnerable and open critical attack vectors into the systems they are supposed to protect. This would not have to be the case. Many basic security measures could be applied. But the relevance of security in security is not a topic yet and the according characteristics are not transparent or measurable, so the market does not demand security in security yet.

In order to improve this situation, both short-term and long-term, the workshop members and the DSI have developed a set of recommendations.

Industrial recommendations

Demand security characteristics: Before striking a contract with a security firm, demand to see everything that is being done to secure the product itself. Ask for defect rates, quality assurance processes, penetration tests, technical security quality features such as ASLR or sandboxes, practices in reporting and disclosure, security policies and for the amount and quality of personnel solely assigned to assuring security in security products. A guide to such questions can be found in the DSI study on "Cyberreadiness for Small and Medium Enterprises".

Establish more neutral and critical expertise: Neutral and critical experts are often not included in critical decision-making processes on security and are frequently not invited to larger industrial or political conferences to avoid confrontation. But critical confrontation must be included, not excluded, to improve security.

Create third party bug bounty programs: Industrial IT-users should offer bug bounties for vulnerabilities and security issues in IT-security products. To enable this activity, they should request permissions for white box testing of IT-security products when contracting such a product. A procedure will have to be defined to warrant the confidential treatment of source code for third parties. Industrial IT-users should consider sponsoring IT-security products to small hacking companies for testing.

Demand cooperation in vulnerability management: IT-security customers must demand by contract proper vulnerability and patching management processes from IT-security companies

and assistance in vulnerability management, in patching and during incidents related to the IT-security product.

Create information and information sharing on security of IT-security: Industrial IT-users should generate information on security issues in security products. Systematic tests could be designed and conducted by a joint center for testing. Academic institutions or industrial initiatives could conduct such testing, similar to Google's Project Zero, but any testing would have to follow a rigid methodology and involve high talent to be effective. Test results could be published. In addition, industrial IT-users should create larger peers groups to exchange knowledge about vulnerabilities in IT-security products and form regimes to generate more pressure on IT-security companies to improve the security quality of their products.

Policy recommendations

Basic security measures must be mandatory: Wherever regulators require a specific level of IT-security, they must define and demand basic security functionalities within security products, levels of code quality and tolerance levels for code defect rates. Sandboxing is an example of a comparatively inexpensive technology with significant impact on product security. If security-wise critical design choices are being made such as the software running on high privileges, functional reasons and risk assessments must be provided.

Security of security must be transparent: Security quality must be tested and rendered comparative, so the market can develop along objective characteristics. Security measures and policies, vulnerabilities and any management processes affecting software quality, vulnerability and patch management must be publicized. Claims to security must be tested methodologically to be verified. Results must be published. IT security agencies should use their rights to testing IT product with an emphasis on security products.

EULAs must enable reverse engineering: Independent tests of the security of IT-security, whether academic or by IT-users, must be legal. To legalize such tests, EULAs should not forbid reverse engineering, but enable and describe a cooperative process of responsible reverse engineering. Contradictory copyright regulation should be modified.

Legal protection for responsible disclosure procedures: As many IT-security companies still react aggressively upon the disclosure of their weaknesses, such disclosure, if responsible, must be protected by law. If the disclosure of a weakness is in the public interest, the researcher and publisher should not be liable.

Review IT certification processes: The certification process for good IT-security products must be reformed. It must be possible to certify a product, if necessary preliminarily, within one month. Otherwise, certification will be ever less relevant for actual market dynamics.