EUROSMART
The Voice of the Digital Security Industry

Added-value of high level security evaluation methodology versus Push-button testing

Executive summary

This white paper deals with current practices used in high level security evaluation methodology concerning vulnerability assessment, penetration testing and attack rating. It is compared to the trend in Common Criteria to use push-button testing usually applied in low level security evaluation methodology.

It does not argue against automated testing but clarifies what both approaches can provide as assurance and what are the limitations.

Methodology using Push-button security testing

A new very profitable business has been created with push-button security testing. Tool vendors would like to convince their potential customers that it is the most practical way to see every step in the attack vector and to understand the hacker's view.

The current practice is to create an automated test suite based on OWASP Top 10 application Security Risks [OWASP] or CVE - Common Vulnerabilities and Exposures [CVE]. It is convenient because test suites are created with no knowledge of implementation in a black box model.

Therefore, it is currently a trend in Common Criteria to consider that push-button is the preferable way for mutual recognition agreement to perform penetration testing for any type of TOE or expected level of confidence.

Key arguments for such practice

The key arguments are: consistent execution, repeatability, minimized human factor.

Additional arguments are: less skilled resource required to write and to run test, convenient, efficient to detect regression between 2 versions, easier control of cost and time, easy to deliver and to report.

For some vendors, the key interest of such practice is the ability to perform an internal pre-test campaign, increasing the confidence level of passing the penetration test campaign performed by the lab.

Limitations and Potential issues

Automatic testing means to run existing written test using predefined interfaces in a given purpose. It allows to identify known vulnerabilities through non-expected behaviors. It means that an expert has already identified a generic issue in advance that fits with a given scenario. It is not often the case.

When an abnormal behaviour is observed, usually existing pre-defined scenarios will not work, and testers have no clue if the breach is really exploitable due to missing access to sensitive resources such as source code.

But most of the time, no abnormal behaviour is observed with a given set of parameters and a specific context. So it only gives a little extended confidence of absence of vulnerability.

It is possible to use this approach for well-defined protocol or security features with limited configurations or numbers of parameters. Indeed, it is not easy to automate a task with a great number of parameters or a huge set of values to consider as depicted in the following example.

When you would like to determine sensitivity to light perturbation of execution flow for a given IC, you have at least to consider the following deterministic parameters as: instruction set, potential effect of laser, and parameters with plenty of possible values as for a laser test, physical location, spot size, wavelength, level of energy, shot duration form, temporal location... It seems that expertise and experience in testing is mandatory to reduce the variance of parameters to avoid combinatorial explosion.

Moreover, such a checklist-automated test approach leads to an issue concerning **how to model the behavior of a hacker**. In the situation of a certified product with identified test suites, the hacker will try to know which test suites have been already executed during the evaluation and then know what kind of tests are not worth to try. The attacker will consequently spend all resources on the parts that have not been consistently tested. It could be seen as saving of attack time.

As this approach does not rely on a source code-based vulnerability assessment, it can only be applied for lower evaluation assurance level up to EAL2 with AVA_VAN.2 enhanced-basic.

Extended use of Push-button security testing applicable to white box approach

If the standard use of push-button security testing is to implement security test suites using predefined interfaces identifying known vulnerabilities through non-expected behaviors as usually in a black box approach, there is another way to consider automated test execution.

It concerns automation of one or several steps of a given attack path from a defined attack scenario to quicken the execution of a test. Such practice is used in a white box approach as we described in the next chapter.

If some tries on a given parameter are automated, we usually separate the parameters prior to combine them to avoid combinatorial explosion and perform combination of results according to tester experience.

High level security evaluation methodology

In such methodology, there is a clear separation between vulnerability assessment, penetration testing and attack ranking as defined in [AAP].

Vulnerability Assessment (VA) relates to the process of analysing a given item (system/application/platform/IC) to find flaws or exploitable weaknesses by different means due to extensive access to all resources as specification, architecture, design, source code and already performed test in a white box approach. Such activity includes a theoretical attack assessment to identify if attack paths are realistic or not.

This analysis task is performed by the accredited experts such as laboratory and then usually backed up by identifying what and how these gaps or holes could lead to success for an attacker respectively compromising the system. Finally, a ranking and rating on severity is created based on study of realistic attack paths. Such tasks cannot (yet) be automated and require tailoring for the respective evaluation tasks.

Such task is very useful and efficient because it allows to focus the scope of penetration testing to the potential attack paths exploitable by an attacker.

Indeed, there is very few interest to run a full testing campaign if a quick review of design or source code gives enough assurance that a given attack path has no chance of success.

Penetration Testing (PT) is done consecutively to the vulnerability assessment using its outcome based on but limited to the standard attacks with real chance of success. PT assessment aims at finding and confirming case-by-case specific exploitable gaps with actual measurement or performance of attack path scenarios as taken from the standard attack catalogue (or new ones).

Note that practical verification may be speed-up case by case by using automated tool as described in case (2).

Attack Rating (AR) is performed when time allocated to test campaign is consumed. ITSEF prepares a quotation of attack paths based on results of test campaign. It allows to determine which attack paths seems to be achievable for a given attacker potential and to list the remaining potential vulnerabilities.

It is often misconceived that a full Vulnerability Assessment involves mandatory Penetration Testing which is a wrong assumption. If a Vulnerability Assessment proofs by argumentation that no weakness is observed for a given attack path, a Penetration Test can be omitted

Conclusion

Despite push button testing is more and more used for low level security evaluation methodology, this way to proceed is not sufficient for high level security evaluation methodology.

As we would like to obtain confidence of product robustness versus attacker possessing Moderate up to High attack potential, it seems not appropriate and efficient to use push button approach. Even if some tasks can be partially automated and some others complemented with Artificial Intelligence (AI) approach (using case (2) approach), nothing currently cannot replace experience and expertise of evaluator for vulnerability assessment and efficient penetration testing with attacker possessing high attack potential profile.

References

[OWASP] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
[CVE] https://cve.mitre.org/
[AAP] Application of Attack Potential to Smartcards,
http://www.sogisportal.com/documents/cc/domains/sc/JIL-Application-of-Attack-Potential-to-Smartcards-v2-9.pdf

About us

Eurosmart, the Voice of the Digital Security Industry, is an **international non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

Our members

Members are manufacturers of secure element, semiconductors, smart cards, secure software, High Security Hardware and terminals, biometric technology providers, system integrators, application developers and issuers.

EUROSMART members are companies (**BCA**, **Fingerprint Cards**, **Gemalto**, **Giesecke+Devrient**, **GS TAG**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **Inside Secure**, **Internet of Trust**, **Linxens**, **Nedcard**, **NXP Semiconductors**, **+ID**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **STMicroelectronics**, **Toshiba**, **Trusted Objects**, **WISekey**, **Winbond**), testing, inspection and certification (TIC) companies (**SGS**), laboratories (**CEA-LETI**, **Keolabs**, **SERMA**), research organisations (**Fraunhofer AISEC**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **Mobismart**, **Danish Biometrics**).

EUROSMART and its members are also active in many other security initiatives and umbrella organisations on EU-level, like CEN, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com   @Eurosmart_EU   @Eurosmart

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 36 35 | mail eurosmart@eurosmart.com