Funded by the European Commission
Seventh Framework Programme

Cyber ROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. **607642**

Vulnerability Assessment

Author(s): John Rodriguez (INOV)

CC RG-40 - Component and System level penetration testing procedures during development and integration of complex systems
CC RG-44 - Assess vulnerabilities and risks of integrating ICT components in physical/embedded systems or field devices
CC RG-49 - Attack simulations
CC RG-50 - Component level penetration testing
CT RG-51 - Component level penetration testing
CC RG-87 and CT RG-84 - Assessment tools for specific vulnerabilities of data exchange nodes

ABSTRACT

The level and diversity of cyber threats that citizens, companies, public authorities and society in general is currently facing is unprecedented and all forecasts indicate that it will tend to get worse, due to multiple factors.

Of particular concern is the fact that mobile platforms for personal and professional usage, like smartphones and tablets are increasingly present in today's society. Companies are slowly adopting BYOD (bring-your-own-device) policies, integrating user's devices into their infrastructure and using new professional applications in their daily activities. Although major platforms like Android and iOS try to establish some security in their architecture, the proliferation of malware in the official application distribution channels, as well as speculation about pre-installed malware at factory level, has demonstrated that current security levels are insufficient and current vulnerability assessment methods are inappropriate for the current level of threats.

Threats to cyber-physical systems, e.g. to disrupt cyber components, impacting operational capabilities and performance of cyber/physical assets, as well as cyber-attacks applied to entire company systems are now common place, and in many cases they seem to be "state-sponsored" to some extent. Malware attacks against industrial systems, as well as specifically targeted malware (using software and hardware components) are now a real threat to the multitude of critical infrastructure operators that support the core functions of modern society.

To address and mitigate the above mentioned threats, it is essential to be able to clearly assess the level of cyber vulnerability existing in each component, model, system, procedure and entity (company, etc.), which are interconnected and can produce cascading effects beyond the obvious. Only in this way it can be possible to fully understand, in a continuous way, what needs to be corrected and the level of resources that will eventually be needed. To achieve this objective, a new type of vulnerability assessment tools and procedures is needed, that can go beyond currently used penetration testing and equivalent procedures.

Vulnerability assessment tools and procedures

DISTANCE TO THE MARKET: **TRL 5-7**
COST OF THE TOPIC: **2 STREPs + 1 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **5**
TIME SPAN FOR ADDRESSING THE ACTION: **48 months**
ACTORS: **national cybersecurity centres, law enforcement agencies, IT security industry, high-tech SMEs, research/academia, critical infrastructure operators, public authorities, electronics and semiconductor industry**

Penetration testing as a technique to validate system security has been around for several decades, but only in the last 15 years it has grown into a full blown industry. The technique involves active analysis of target systems for potential software vulnerabilities, operational weaknesses, including people and the processes the system is part of. It is done so, by simulating an attack to the system employing automated tools or manual actions, or both, in order to violate some security properties of the system or process.

Different methodologies have been defined providing completeness and effectiveness of the performed tests and a wide range of certifications for security testers (CPT, CPTE, CompTIA, CSTA, GPEN, OSCP, CEH, CEPT, etc.) has been developed giving customers some assurance about the contracted services.

Independently from the chosen method, penetration testing depends on a good characterization of the target infrastructure. One of the first steps after identifying the target (differently represented in each methodology) is to understand the security assumptions, the threats and identify the goals of the test. This can typically be achieved by building some kind of attack tree that will guide the tests to be conducted. Tools are used to assist in fields such as: vulnerability assessment, fuzzing, brute forcing, SQL injection, exploitation frameworks, protocol analysis, reverse engineering, etc.

Other tools try to minimize the security analyst's work by performing dynamic application security testing simulating an attacker. Nevertheless, fully automated broad spectrum security testing is always of limited utility and manual tuning is required for trustable results.

What is now envisioned is a new level of vulnerability assessment tools and procedures, that can go beyond currently used penetration testing and equivalent procedures. These should include, among other innovative features: advanced risk analysis and modelling, security testing at all points of data exchange and component level penetration testing.

The minimum expected outcome from the proposed action should include, but not be limited to, the following deliverables:

- Component and system level penetration testing procedures used during development and integration of complex systems.
- Assess vulnerabilities and risks of integrating ICT components in physical/embedded systems or field devices.
- Attack simulations.
- Component level penetration testing.
- Assessment tools for specific vulnerabilities of data exchange nodes.