Active Security

2022-03-07

DE/NL
ITEA3, 17005
BMBF, 01IS18062(A-E)

Abstract

The main challenge in the SCRATCh project is to describe a work-flow that improves the overall security of IoT systems without inventing yet another methodology. This approach targets the functional outcome of a business process. It is a minimalistic approach to elevate overall security aspects of IoT development in any given sector. Basically, we describe in SCRATCh how to create a secure system, test its security aspects and keep it secure based on criteria/requirements. The method revolves around three main aspects that are mapped to the DevOps chain: Constrain, Comply and Control. Security entails all aspects of this chain to develop a system that has built-in counter measurements for active and passive types of attacks and recommendation how to keep the system secure by preprogramed adaptations or human interaction described in processes.

Table of Contents

1. Introduction

The terminology for active and passive security has its roots in military, one can image all kinds of different approaches in the terms active and passive, Introduction of AI in the security realm makes the distinction a bit less clear. Is a well-trained algorithm active or passive? To be complete the paper shortly addresses the term dynamic security introduced in the EU cordis program.

2. Active and passive cyber security

For defining active and passive security, let us imagine a battle situation: A city is under siege and wants to secure its citizens from outside attacks. Of course, there are several ways how to achieve this. A wall and a moat can prevent attackers from just walking in, whereas bowmen perform counterattacks on every opponent that dares to approach the city walls.

If we want to separate these defense measures into active and passive, it becomes obvious that walls and moats must be passive. They cannot perform any actions but still contribute to the city's security. Bowmen on the other hand actively try to defend the city by shooting arrows at their opponents. Of course, we would not consider that the wall and the moat had to be built before the battle, because the preparation is always something active. The security that we achieve by these measures can thus be defined as follows:

Active security *is security derived from defensive (counter-)actions during the attack. Therefore, active security is the opposite of passive security, where no actions are performed during the attack.*

In cyber security active defense measures can be anything that reacts on suspicious behavior. For these actions we need to measure and detect such suspicious behavior first. A simple example exists in the detection of repeated port scans from one certain IP address in order to block this address. Another example is a brute force prevention by blocking a certain user after several failed login attempts. the action being active is performed by a human, repetitive attacks can be converted to programming rules implemented by a human. In a formal sense according to the definition the rule implemented is passive, like a city wall

Differently put passive measures in a cyber security context are related to prevention of known attacks by closing static attack surfaces. Examples are port blocking, firewalls and some patches for known vulnerabilities.

Dynamic cyber security

When we look at our imaginary city siege again, the city general would most probably react on a strategy change of the attacker's army. That might mean, that our bowmen change their position. In every case the city's defense strategy dynamically adapts to the attacker's behavior. This requires more intelligence than having a wall of bowmen standing on the wall to attack every enemy in range (always performing the same action). In other words: We need intelligent reactions for dynamic security. Thus, we define dynamic security as follows:

Dynamic security is *security derived from an intelligent (counter-)strategy during the attack. An intelligent strategy changes (counter-)actions, if appropriate. Thus, dynamic security is always active security.*

3. Other definitions

The CNSS Glossary from 2015 (Committee on National Security Systems, 2015) defines the term active cyber defense as a 'synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. Meaning that in addition to passive cyber defense, where known threats are mitigated using passive measures (in reaction to attacks in the past) like firewalls, anti-malware and rule-based IDS, the active aspect describes the capability to constantly anticipate, monitor and learn about new attack methods using SIEM, anomaly detection and threat intelligence.

Another definition was proposed by Robert M Lee in his white paper "The Sliding Scale of Cyber, (Lee, 2015) Security", in which security measures are categorized in a scale from architecture over passive defense, active defense, intelligence to offense. In this framework active defense lies between passive defense and intelligence and is defined by 'the process of analysts monitoring for, responding to, learning from, and applying their knowledge to threats internal to the network.'

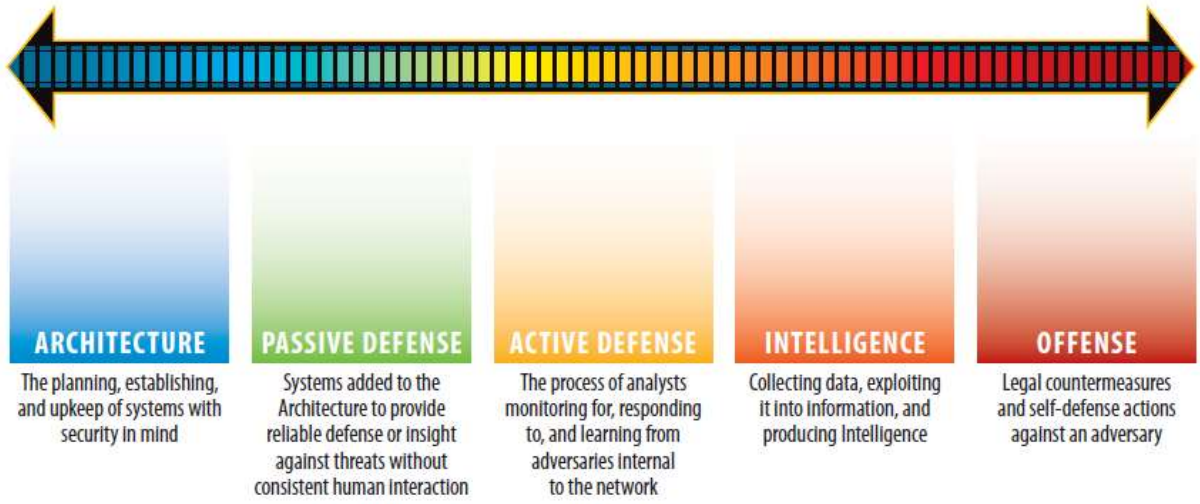

Fig X: Sliding Scale of Cyber Security [SANS, 2015]

While the previous definitions do not include hack-backs, the following definitions do include hack-backs in active cyber defense. Hack-backs describe the process of attempting to neutralize the threat actor's resources and infrastructure with counter cyber attacks.

In a research report from 2017 by Rober S. Dewar, (Lee, 2015), the term is similarly defined as "an approach to achieving cyber security predicated upon the deployment of measures to detect, analyze, identify and mitigate threats to and from communications systems and networks in real-time as well as the malicious actors involved. This requires that defenders have the capability and resources to take proactive or offensive action against threats as well as interact with malicious actors, both in the defended systems and in those malicious actors' home networks.'. Along with the

definition the following tools were given as examples: white-worms (“righteous malware”), hack-backs, address hopping and honeypots.

Dynamic cyber security (according to EU Cordis programme)

In development (constrain and comply): innovative, integrated and holistic approaches in order to minimize attack surfaces through appropriate configuration of system elements, trusted and verifiable computation systems and environments, secure runtime environments, as well as assurance, advanced verification tools and secure-by-design methods. This may entail a whole series of activities, including behavioral, social and human aspects in the engineering process until developed systems and processes address the planned security/privacy/accountability properties.

In operation (control): Innovative capabilities to dynamically support human operators (e.g. Incident Response professionals), in controlling response and recovery actions, including information visualization. The capabilities should include the assessment how attacks propagate in a particular infrastructure and/or across interconnected infrastructures (e.g. attack-defense graphs) and what the best measures are to withstand and recover from a threat/attack, including the convergence with measures beyond cyber that can be needed (e.g. security policies).

Given the basic discriminatory factor in the definitions as human interaction passive versus active, it follows that a security measurement built in the system as a result from security by design could be classified as passive in the Operational Phase and active in the development phase. And at the same time, it is Dynamic if innovative.

4. Guidance for this paper

Scratch in relation to Active security, taking the following definitions as starting point.

> ***Active security*** *is security derived from defensive (counter-)actions during the attack. Therefore, active security is the opposite of passive security, where no actions are performed during the attack.*
> ***Dynamic security is*** *security derived from an intelligent (counter-)strategy during the attack. An intelligent strategy changes (counter-)actions, if appropriate. Thus, dynamic security is always active security.*

The rule for this paper will be to define per phase the type of security taken based on the above definition

To build a secure system all kinds of measurements need to be implemented from start in SCRATCh terms from the constrain phase. It makes sense to review the term active security per phase. From a security perspective this will lead to reasonable secure systems. At start the system then has a certain amount of security measurements implemented. In the operational phase the "real" active security part has to solve the unknown or new threats by use of active security, being of an operational or AI type.

The term dynamic is used when from a SCRATCH perspective if a measurement can be seen as innovative. Example an AI agent that detects attacks and adapt the response.

Phase /Type	Passive	Active	**Dynamic**
Constraints	DMCS Data Set Tool Knowledge Base Trusted Software Cloakware Software Protection MCUXpresso IDE	OWASP Dependency Track GitHub Action Denuvo Anti-Tamper	
Comply	OWASP-ISVS Irdeto Keys & Credentials Key Provisioning Tools	IOXY OTAlyzer Firmware Update System Remote MCU Firmware Update	FirmwareCheck SPTool
Control	Secure Storage	Anomaly Detection Toolkit	Deception Toolkit

TABLE 1 ACTIVE/PASSIVE/DYNAMIC SECURITY MATRIX

Fig to highlight the scratch tools in relation to the terminology active passive dynamic

5. Example of SCRATCh tool and what type of security they provide

Deception toolkit (Daniel)

The framework provided by the deception toolkit allows for various active and dynamic security strategies, depending on which kind of fake entity is presented to the attacker. Cyber deception aims to hide real information from attackers (Dissimulation) and present false information (Simulation). This is particularly effective in the reconnaissance phase (see Lockheed Martin Cyber Killchain), where the attacker is seeking information about the target, such as IT-infrastructure, employed software services and personnel. An active security approach incorporating deception could be lures in a web application such as randomly returning HTTP 200 Status codes for non-existing resources to sabotage a directory brute force. The dynamic approach would adapt the invented, false information to the information the attacker is seeking. Is the attacker probing for a specific vulnerability in e.g. a WordPress plugin, than the deception strategy could not only be to simulate the existence of this specific plugin, but also start a honeypot with this specific vulnerability present.

6. Examples of active and passive security in Demonstrators

Use Case Police

This use case focuses around defending a mobile surveillance application that runs as a wearable device on a police agent as by definition is deployed in inherently insecure deployments (e.g., when the police agent is monitoring a demonstration and checking for known persons of interest such as participants in past incidents. The summary of the security use cases was given in SCRATCh deliverable D4.1:

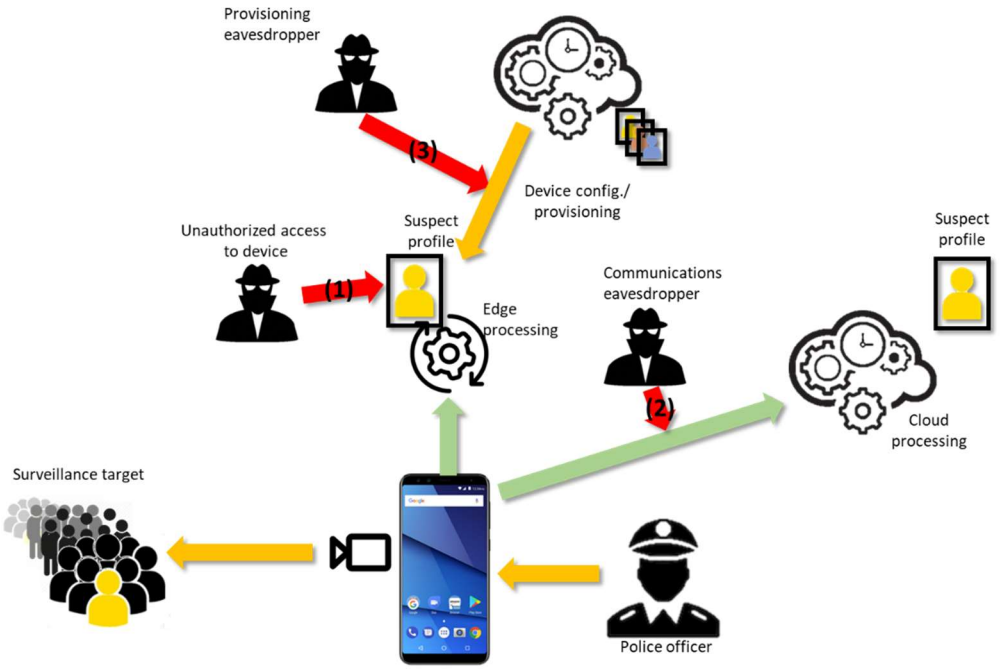

FIGURE 1 POLICE USE CASE SECURITY USE CASES

We can see the three main security use cases identified by the red arrows and index numbers 1 to 3. They correspond to the following simplified scenarios:

1. The device is lost or stolen and its contents are analyzed by a malicious user.
2. Critical data (typically, facial profiles of suspects) is intercepted during the provisioning of the device.
3. Wireless data communications with the server are intercepted over the air by a malicious user.

These scenarios were analyzed and mapped to the proposed SCRATCh tools and methodologies. Visualized on the matrix proposed in section 4, the end results is as follows:

Phase /Type	Passive	Active	**Dynamic**
Constraints	Knowledge Base *DMCS Data Set Tool*		
Comply	OWASP-ISVS Secure Storage Code Obfuscation	*IOXY* **OTAlyzer** *Manual testing* *Pen testing*	
Control	*Intrusion detection*	***Process to react on security alerts from the system***	*Secure Storage wipe on active threat*

TABLE 2 SECURITY MATRIX FOR USE CASE POLICE

In the table, we use the following convention: text in **bold** refers to implemented solutions in the Police UC during SCRATCh. Text in *italics* refers to solutions that have been designed but not fully implemented (due to lack of resources).

In Constraints we only use Passive elements, such as complying and checking on build to the essential security requirements in the Knowledge Base. This applies to all security scenarios (1), (2) and (3). We could have focused on the DMCS Data Set Tool but it wasn't done due to lack of time in the project.

In the Comply phase for Passive we use a Secure Storage approach in which the device stores its more critical data (facial profiles, etc.) in a secure storage facility implemented in hardware (using ARM TrustZone). We also obfuscate code that is interpreted by the system (Python code) so that it is not immediately readable. Finally, we used OWASP-ISVS to check our compliance with the list of general requirements expressed there. All these three Passive actions safeguard against the security scenario (1) happening. We use Otalyzer in this phase to ensure that communications are secure, providing Dynamic Security for security scenario (2). In terms of Active security, we could potentially have implemented Penetration Testing measures and other tests to solve particularly issues in security scenarios (2) and (3).

Finally, in the Control phase no measures were implemented but several were considered. For Passive security, a simple intrusion detection scheme for the network would provide security in scenarios (3) and mostly (2). For Active security, a monitor to detect active security events or to detect the 'security health' of the system could be useful for all security scenarios. For Dynamic security, when the security event was triggered, a complete deletion of the Secure Storage could have been provided, erasing critical data (facial profiles, encryption keys, security credentials) from the device so it would not have been accessible after device capture in security scenario (1).

Use Case Connected Retail

In the use case connected things in retail stores, continuous secure and reliable integration of connected things, we address the new security challenges that arise from the IoT in retail. The future retail stores will have more smart devices integrated into its infrastructure. In order to integrate these devices securely, various tools developed or identified in the SCRATCh project have been applied to this use case. A detailed description can be found in D4.2.

In the Constrain phase used services are checked for known CVES based on the OWASP dependency track. Also the source code is being checked for vulnerabilities using static code analysis, dynamic code analysis and symbolic execution.

In the Comply phase tools and services are integrated to ensure identity based on a secure provisioning and the use of Secure Elements in the IoT Devices. A firmware update system developed in the SCRATCh project is implemented and shows mitigation of potential threats through all layers of a firmware update beginning with a code change and ending with the actual installation of a new firmware version.

In the Control phase each integrated device runs a secure boot mechanism which ensures the integrity of running software. Sensitive parts of these mechanisms are done with a secure element. Deception and anomaly detection toolkits are used to detect potential attacks on the IoT devices and help to minimize risk if actual attacks are taking place.

Phase /Type	Passive	Active	**Dynamic**
Constraints		OWASP Dependency Track GitHub Action Code Analysis (static and dynamic code analysis, symbolic execution)	
Comply	Identity and security provisioning tools Binary signing	Firmware Update System	
Control	Secure boot with secure element	Deception Toolkit (Obfuscation and Decoys)	Anomaly Detection Toolkit

7. Conclusion

Categorisation is method to give some insights in a complex issue, for security the categorization into active and passive has its drawbacks. As Active has “good” sound and Passive a “lesser” sound to it, the contrary is true. Passive as in no human involved, is actually a better method as it operates 24x7 against cyber-attacks. In the battle against cyber-attacks it should be goals nr 1 to transform a mitigation from active to passive. The Focus of SCRATCh was targeted towards this type of automation enhancing the passive security. The EU approach of coining dynamic security seems a better way of approaching the complex field of cyber security.

8. Bibliography

Committee on National Security Systems, C. N. (2015, April 06). *glossary-2015-cnss.pdf.* Retrieved from https://cryptosmith.files.wordpress.com/: https://cryptosmith.files.wordpress.com/2015/08/glossary-2015-cnss.pdf

Dewar, R. (2017). *Active Cyber Defense.* https://www.researchgate.net/publication/321057804_Active_Cyber_Defense.

Lee, R. M. (2015, September 01). *The Sliding Scale of Cyber Security.* Retrieved from https://www.sans.org: https://www.sans.org/white-papers/36240/