ITEA Office
High Tech Campus 69 - 3
5656 AG Eindhoven
The Netherlands

T + 31 88 003 6136
E info@itea3.org
W www.itea3.org

ITEA 3 is a EUREKA strategic ICT cluster programme

Exploitable Results by Third Parties

17005 SCRATCh

Project details

Project leader:	Andries Stam, Almende
Email:	andries@almende.org
Website:	https://scratch-itea3.eu/

Name: DCMS Data Set Tool

Input(s):	Main feature(s)	Output(s):
▪ DCMS data	▪ Converting data into a local Data set for internal use and data manipulation	▪ Dataset ▪ Manipulation interface

Unique Selling Proposition(s):	▪ Free tool to obtain knowledge in the beginning of development on potential applicable standards and requirements.
Integration constraint(s):	▪ Some knowledge of Python script language
Intended user(s):	▪ Development Phase
Provider:	▪ https://github.com/SCRATCh-ITEA3/knowledge-base
Contact point:	▪ Franklin Selgert, AnyWi BV, franklin.selgert@anywi.com
Condition(s) for reuse:	▪ None

Latest update: 18-03-2022

Name: SCRATCh Knowledge Base

Input(s):	Main feature(s)	Output(s):
▪ Data scraped from website of standard and regulatory bodies, like ENISA, OWASP	▪ Large collection of data ▪ Simple web interface to access and export data for own use ▪ Tool to obtain security requirements at the start of a project	▪ Locally installed SQL database with interface and export options

Unique Selling Proposition(s):	▪ Useful tool to obtain security requirements at the start of a project
Integration constraint(s):	▪ Needs a local install of Maria DB and WAMP server or other local web server, or an install on a web server supporting Maria DB or SQL server and PHP version 7 or higher. ▪ Snapshot of data available in 2021. No update of data foreseen.
Intended user(s):	▪ Development
Provider:	▪ https://github.com/SCRATCh-ITEA3/KB
Contact point:	▪ Franklin Selgert, AnyWi BV, franklin.selgert@anywi.com
Condition(s) for reuse:	▪ None, free tool, uses publicly available information on the internet

Latest update: 18-03-2022

Name: OWASP Dependency Track Github Action

Input(s):	Main feature(s)	Output(s):
▪ Source code of any programming code hosted in Github. DT OWASP instance URL and API key	▪ It creates a Bill of Materials (BoM) of the source code of a project, uploads it to a OWASP Dependency Track Instance and provides the result within the CI/CD cycle	▪ It provides a risk score derived from the library versions used in the project

Unique Selling Proposition(s):	▪ This GitHub action enables the direct use of a Dependency Track OWASP instance to analyze the source code of our projects in a very convenient way, without requiring neither any human action nor additional service. ▪ When the code is uploaded or merged to a repository the action is triggered and the vulnerability analysis performed. ▪ The result is provided and can be used directly within the CD/CI process, for example to prevent users from pushing code with known vulnerabilities. Additionally it also checks the licenses of the added libraries.
Integration constraint(s):	▪ It is required an DT OWASP deployed accessible from Internet with valid certificates.
Intended user(s):	▪ Any developer
Provider:	▪ https://github.com/marketplace/actions/owasp-dependency-track-check
Contact point:	▪ Ivan Abalde, Quobis, Ivan.abalde@quobis.com
Condition(s) for reuse:	▪ Open Source project, public action in Github, MIT license

Latest update: 18-03-2022

Name: Irdeto Trusted Software

Input(s):	Main feature(s)	Output(s):
▪ Mobile application archive (iOS or Android) ▪ Required Security level	▪ Automatic Zero Touch Protection ▪ AI driven algorithms that automatically determine how to apply protection in the most efficient way	▪ Protected Mobile application archive (iOS or Android)

Unique Selling Proposition(s):	▪ Beyond State of the Art: Is the first (and currently only) obfuscation tool that makes use of machine learning to automatically apply code protection ▪ Requires no interaction or preparation of the to be protected code
Integration constraint(s):	▪ Applications should be for Android or iOS
Intended user(s):	▪ Mobile Application publishers and developers
Provider:	▪ Irdeto BV
Contact point:	▪ Werner Strydom, Irdeto BV, WStrydom@irdeto.com
Condition(s) for reuse:	▪ Commercial License to be negotiated ▪ Availability of a Trial license will be determined on a case-by-case basis

Latest update: 18-03-2022

Name: IoT security verification standard OWASP-ISVS

Input(s):	Main feature(s)	Output(s):
▪ Application Design documentation ▪ E2E product	▪ Open standard of security requirements for Internet of Things (IoT) applications.	▪ Security recommendations for IoT applications.

Unique Selling Proposition(s):	▪ Requirements are applicable to a wide range of devises across many sectors; ▪ Requirements are actionable and workable, i.e. achievable in practice; ▪ Three levels of security are defined.
Integration constraint(s):	▪ Applicable to connected products that are part of a rich application ecosystem.
Intended user(s):	▪ Requirement Engineers, Analysists & Architects, Developers, Testers.
Provider:	▪ https://github.com/OWASP/IoT-Security-Verification-Standard-ISVS
Contact point:	▪ Cédric Bassem, NVISO, cbassem@nviso.eu
Condition(s) for reuse:	▪ CC-BY-SA-4.0 License

Latest update: 18-03-2022

Name: IOXY - Open-Source MQTT interception proxy

Input(s):	Main feature(s)	Output(s):
▪ MQTT communication channel ▪ Access to client and server	▪ MQTT intercepting proxy	▪ A clear overview of data communicated ▪ Provides features to alter data in transit, as well as replaying of recorded messages.

Unique Selling Proposition(s):	▪ Multi-protocol support ▪ Multi-broker support (broker agnostic implementation) ▪ GUI
Integration constraint(s):	▪ Supports: MQTT,MQTTS and MQTT over Web Sockets ▪ Credential and certificate-based authentication as well as TLS ALPN are supported.
Intended user(s):	▪ Developers, Testers
Provider:	▪ https://github.com/NVISOsecurity/IOXY
Contact point:	▪ Cédric Bassem, NVISO, cbassem@nviso.eu
Condition(s) for reuse:	▪ GPL-3.0 License
	Latest update: 18-03-2022

Name: FirmwareCheck tool to automate dynamic analyses of IoT-firmwares

Input(s):	Main feature(s)	Output(s):
▪ Emulates a buildroot-generated firmware that is supplied ▪ Alternatively runs standalone on any Linux system	▪ Various security checks are run, that roughly correspond to the OWASP IoT Top 10 such as checking for outdated components, default passwords, open ports, processes running as root etc.	▪ HTML-Report that describes findings ▪ Console-output for CI/terminal only view

Unique Selling Proposition(s):	▪ Enables automation of dynamic analyses on firmware images. This enables tests such as checking for running services and by which users these services are run. This goes beyond static analysis of firmwares.
Integration constraint(s):	▪ Firmware needs to be generated with buildroot and it must be a QEMU compatible firmware in order to run in a CI. As an alternative, the standalone version can be run on any Linux system, but then the firmware has to be deployed to the device first
Intended user(s):	▪ Firmware developers and DevOps, researchers testing IoT firmwares and devices
Provider:	▪ https://github.com/OTARIS/FirmwareCheck
Contact point:	▪ OTARIS, office@otaris.de
Condition(s) for reuse:	▪ Apache 2.0 License

Latest update: 18-03-2022

Name: OTAlyzer

Input(s):	Main feature(s)	Output(s):
▪ Network capture files such as .pcap(ng) files or files generated by mitmproxy ▪ Keyword- and Severity-files, describing the keywords to look for and their severity levels if found in the data	▪ Searches for occurrences of predefined keywords in the network capture file, by searching TCP, HTTP(S) and MQTT traffic ▪ Also detects hashed values or encoded values	▪ A report containing all findings and metadata for each finding, as well as a severity level for each finding

Unique Selling Proposition(s):	▪ The OTAlyzer automates work that is otherwise done manually in using tools such as wireshark or mitmproxy ▪ The OTAlyzer enables to take the network dimension into account in unit tests, helping a developer to ensure privacy of a software in a CI
Integration constraint(s):	▪ OTAlyzer runs cross-platform on Linux and Windows ▪ Traffic needs to be captured in one of the supported input formats
Intended user(s):	▪ Developers and researchers commonly dealing with network capture files
Provider:	▪ https://github.com/OTARIS/OTAlyzer
Contact point:	▪ OTARIS, office@otaris.de
Condition(s) for reuse:	▪ Apache 2.0 License

Latest update: 18-03-2022

Name: Fuzz-Against-The-Machine (FATM) - MQTT-Fuzzer

Input(s):	Main feature(s)	Output(s):
▪ A textfile with Strings which serve as values for the generation of the MQTT packets ▪ Log files	▪ Generation, mutation and delivery of MQTT control packets, which have the potential to reveal programming flaws in MQTT brokers ▪ Replay feature for log files that helps to analyze detected errors	▪ Log files containing the hexadecimal representation of every sent packet

Unique Selling Proposition(s):	▪ Fuzzing is a suitable testing technique to enhance the security of MQTT applications ▪ FATM was able to detect a Memory Leak inside Mosquitto MQTT Broker (CVE-2021-34431)
Integration constraint(s):	▪ FATM relies on the Python library Scapy for building MQTT packets ▪ FATM is easily deployed on Linux
Intended user(s):	▪ Developers and researchers working with MQTT applications
Provider:	▪ https://github.com/OTARIS/Fuzz-Against-The-Machine
Contact point:	▪ OTARIS, office@otaris.de
Condition(s) for reuse:	▪ GPLv2 License

Latest update: 18-03-2022

Name: SPTool

Input(s):	Main feature(s)	Output(s):
▪ Test cases ▪ Source Code	▪ Test Case Prioritization ▪ Tests Case Automatization ▪ Secure issue detection	▪ Priorized test cases ▪ Test Case report ▪ More secure source code

Unique Selling Proposition(s):	▪ Priorized test case execution. ▪ Improved security issue detection ▪ Testing cost reduction
Integration constraint(s):	▪ Requires Junit-XML, Test Suite JSON, Test history Json, Tet Runner (e.g, C++ test case executor)
Intended user(s):	▪ SW Developers ▪ SW Testers
Provider:	▪ ULMA Embedded Solutions
Contact point:	▪ Asier Larrucea, ULMA, alarrucea@ulmaembedded.com
Condition(s) for reuse:	▪ commercial licence to be negotiated ▪ free license can be provided for research purposes

Latest update: 18-03-2022

Name: Irdeto Keys & Credentials Service

Input(s):	Main feature(s)	Output(s):
▪ Production requests for device ranges ▪ Production code	▪ Security foundation rooted in hardware ▪ Trusted Integrity and identity ▪ Security Foundation for products ▪ Predictably, reliably, and safely for decades, in remote and hostile environments ▪ Secured Manufacturing ▪ HSM based ▪ 4 eye principle for key ceremonies	▪ Secured and trusted devices with trusted Identity ▪ Signed Production code

Unique Selling Proposition(s):	▪ Secure facilities, dedicated personnel, Hardware Security Modules ▪ 24/7 monitoring, incident and vulnerability management ▪ Full traceability between keys ↔ hardware and software supply chains ▪ Business continuity programs and external audits ▪ Integration into UNECE R.155 / ISO 21434 cybersecurity strategies ▪ IEC62443 Compliance ▪ Managed Code Signing ▪ Trust Authority, PKI and Key Management ▪ Cryptographic Expert Assessment ▪ Trusted Identities
Integration constraint(s):	▪ Code Signing requires minimal integration in Release Pipeline ▪ Highest Grade of Secured Devices requires some integration with SOC and/or device manufacturing
Intended user(s):	▪ Device manufacturers ▪ Various layers in a multi-vendor infrastructure requiring PKI security (e.g., EV charging)
Provider:	▪ Irdeto BV
Contact point:	▪ Werner Strydom, Irdeto BV, WStrydom@irdeto.com
Condition(s) for reuse:	▪ Commercial License to be negotiated ▪ Availability of a Trial license will be determined on a case-by-case basis
	Latest update: 18-03-2022

Name: Remote Device Connection

Input(s):	Main feature(s)	Output(s):
▪ Internet connection ▪ *nix device	▪ Enabling remote connection to devices behind NAT	▪ DynDNS connector to remote device

Unique Selling Proposition(s):	▪ IoT devices lack screens to display connectivity information ▪ They are often deployed behind a NAT shielded network making it difficult to access without additional user configuration ▪ Solution shows how to utilize OpenSource components nodeRed and LocalTunnel to remotely connect to IoT devices
Integration constraint(s):	▪ Central server for devices to connect toAuthentication not included, needs to be implemented on the devices
Intended user(s):	▪ Users requiring remote access to various IoT devices without
Provider:	▪ https://github.com/SCRATCh-ITEA3/IoTunnel
Contact point:	▪ Jannik Kramer, Consider it GmbH, hello@consider-it.de
Condition(s) for reuse:	▪ Open source / free of charge

Latest update: 18-03-2022

Name: Firmware Update System

Input(s):	Main feature(s)	Output(s):
▪ Use Case Traits ▪ Hardware Limits	▪ Set up a Secure DFU Pipeline ▪ End Device Monitoring	▪ Manifest Design ▪ Status Updates

Unique Selling Proposition(s):	▪ Holistic approach for setups with multiple devices & vendors ▪ Thorough security profiling based on modern knowledge
Integration constraint(s):	▪ Cryptography (including Decrypt on End Devices)
Intended user(s):	▪ IoT End Device Vendors / Maintainers
Provider:	▪ https://github.com/SCRATCh-ITEA3/firmware-update-system
Contact point:	▪ Merijn van Tooren, Almende BV, merijn@almende.org
Condition(s) for reuse:	▪ CC-By

Latest update: 18-03-2022

Name: Remote MCU Firmware update via Git Server

Input(s):	Main feature(s)	Output(s):
▪ NXP MCU ▪ GIT Repository ▪ Network connection	▪ Updated end devices without the need for special infrastruture	▪ FW update procedure

Unique Selling Proposition(s):	▪ Remote update of devices in the field ▪ Utilization of publicly and free-of-charge infrastructureBasic security setup
Integration constraint(s):	▪ Network connection to target repositories ▪ NXP MCU based devices
Intended user(s):	▪ Demonstrators, Beta environments
Provider:	▪ NXP Semiconductors Germany GmbH
Contact point:	▪ Till Witt, NXP, till.witt@nxp.com
Condition(s) for reuse:	▪ Non-disclosure agreements ▪ Details to be defined

Latest update: 18-03-2022

Name: Deception Toolkit

Input(s):	Main feature(s)	Output(s):
▪ HTTP or SSH Service to Proxy	▪ Inject lures into application traffic ▪ Conceal critical information	▪ Alerts in dashboard ▪ High detection rate

Unique Selling Proposition(s):	▪ Can be installed without modification of proxied host ▪ Fine-grained control over deception strategies ▪ Easy deployment and configuration with containers and dashboard
Integration constraint(s):	▪ Need to set the firewall to only accept messages from the proxy ▪ Need to direct incoming requests through the proxy, e.g., by pointing the DNS domain to the proxies IP ▪ The SSH proxy needs the SSH keys or credentials for the SSH service that is being proxied
Intended user(s):	▪ SMEs with HTTP or SSH service to protect
Provider:	▪ https://github.com/SCRATCh-ITEA3/SCRATCh-Tools-Repo/tree/master/C3_Control/07_Operate/Deception_Toolkit
Contact point:	▪ Daniel Reti, DFKI, Daniel.reti@dfki.de
Condition(s) for reuse:	▪ None

Latest update: 18-03-2022

Name: Secure Storage		
Input(s):	Main feature(s)	Output(s):
▪ Any data that requires to be stored safely (immune to device interception)	▪ Secure storage enables devices running on top of an ARM architecture implementing ARM TrustZone to store critical data of limited size (e.g., encryption keys) in a secure manner that can't easily be accessed even if the device is physically compromised. The TrustZone enables a safe execution environment with separate CPU and RAM.	▪ Any secure data previously stored in the Secure Storage

Unique Selling Proposition(s):	▪ Having a storage for data that is secure but does not require the use of dedicated hardware (Secure Elements, etc.) and that can be implemented using the widely available ARM TrustZone extension.
Integration constraint(s):	▪ The implementation is very dependent on the details of the Use Case. No SCRATCh general implementation is provided, only a proof-of-concept.
Intended user(s):	▪ Any application that requires data to be stored securely even if a malicious user logs into the device.
Provider:	▪ HI Iberia Ingeniería y Proyectos ▪ Further info at https://github.com/SCRATCh-ITEA3/SCRATCh-Tools-Repo/tree/master/C3_Control/07_Operate/Secure_Storage
Contact point:	▪ Raúl Santos de la Cámara, HI Iberia, rsantos@hi-iberia.es
Condition(s) for reuse:	▪ Since there is no general implementation, there is no general reuse case or conditions. Contact HIB for consultancy on the topic.
	Latest update: 18-03-2022