Project Synopsis

Proposed by: TÜBİTAK BILGEM, Sabancı University, Arçelik

CS01: Secure and resilient digital infrastructures and interconnected systems

Call: HORIZON-CL3-2022-CS-01-01: Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures

Tentative Title: Monitoring and Responding to Advanced Threats Using Customizable Hardware-supported IoT Honeypot System

Honeypots are one of the most important technologies which are used to detect the attacker's behaviors. A honeypot can be thought of as a trap which is set to detect or understand attacks towards particular online and internal devices. Honeypots are a type of security product that is created on purpose to be probed, attacked, and compromised. This way honeypots allow cyber security experts to understand and categorize the attacks better. Groups of honeypots are generally deployed as a network of instances called honeynets. Current honeynets have various issues related to customizability and luring sophisticated attackers. Once a honeypot is identified, attackers create signatures to avoid them in future. This causes poorly-designed and deployed honeypots to be avoided by sophisticated attackers. Such honeypots fail to deliver their promise to gather high quality attack data to the security analyst.

Honeypots can be categorized by levels of interaction of attackers with decoy services:

Low Interaction Honeypots only provide an imitation of specified services. There is no real operating system. Honeypot of this type is relatively easy and quick to be applied and easy to be detected by attacker.

High Interaction Honeypots provide a full system to interact. It provides real services and systems like an actual system. Therefore, the attacker can perform a full system control on honeypot. It provides more information about attacker's tools, tactics, and motives.

In this project, we are aiming to develop a customizable and hardware-supported high interaction honeynet that can emulate various devices in a realistic manner. Such a honeynet will be capable of providing a realistic interface and response to the sophisticated attackers. The attackers can be categorized by different levels of users. First of them, the most basic users accessing a honeypot is average computer users, a Level 1 user. They might come upon the honeypot by happenstance or have malicious desires, but not much technical knowledge. The next type of attacker is a motivated and educated attacker, a Level 2 user. They might look a bit deeper into a honeypot to examine properties of systems for fingerprinting and exploit them for malicious activities. Finally, Level 3 users are automated web crawlers that search for IoT devices on the internet. These tools, such as Shodan, run different tests and scripts against public facing Internet devices in a manner similar to Nmap. Therefore, Nmap scans may be done against the actual device or honeypot system, and compared to test the ability of the honeypots to appear as an actual IoT device placed on the public internet. In this project, the system responses to all levels of attackers and it is able to detect attacks to vulnerabilities of communication protocols (e.g.,

Heartbleed), database attacks such as SQL injection, operating system targeted attacks (e.g., Shellshock), memory based buffer overflow attacks, Web/Application based attacks (XSS, CSRF, SSRF etc.).

In our approach, we will use single board computers (such as Raspberry Pi and/or Arduino) and/or reprogrammable FPGA devices. These devices will be customizable to emulate IoT devices with Linux-based firmware or other devices with operating system supported by ARM architecture. So that an organization can be able to reflect its own infrastructure as a honeynet. Moreover, the deployment will be in a realistic environment, rather than easy identifiable cloud services.

The architecture of the system is distributed on sites at different locations. Management and monitoring are done centrally on the cloud.

Furthermore, the honeynet system will have smart attack categorization algorithms to identify sophisticated attack types. Using AI and ML algorithms, attack types can be easily classified.

In addition, the same algorithms can be improved to create signatures for existing offensive and protection tools. Offensive tools such as Burp Suite, Metasploit and Nmap can use these signatures to assess for misconfigurations and vulnerabilities. Meanwhile, protection tools such as Snort and Suricata can use these signatures to protect networks against latest attacks. Lastly, attack data collected from honeynet systems will be shared to national CERTs/CSIRTs, Google safe browsing and responsible hosting provider to facilitate crime prevention and remediation process. In order to achieve this, an API will be created to share abuse data and IOCs. hosting providers that did not use our API point will be informed via email-based notification to facilitate cleanup.

TUBITAK BILGEM:

TÜBİTAK Informatics and Information Security Advanced Technologies Research Center (BİLGEM) is the national R&D center that produces innovative and national solutions for the needs of our country with its studies in the fields of informatics, information security and advanced electronics. Being the most competent R&D center in Turkey, BİLGEM carries out technological R&D studies that ensure the security, integrity, safe transmission and storage of military and civilian information in order to ensure technological independence in the field of information security and informatics in Turkey.
Consisting of more than 1600 staff , more than 80% of whom are R&D staff , TÜBİTAK BİLGEM operates on information technology, information security and advanced electronics. Based upon its experience exceeding 40 years, the center is now one of the most competent R&D centers of Turkey. The main activities of BİLGEM are Research and Development, Testing and Evaluation, Prototype Production and Training. Our center has institutes that have signed hundreds of successful projects in the fields of advanced electronics, information technologies, cryptology, cyber security, software technologies, information security, electronic warfare and telecommunication.These institutions are namely the National Research Institute of Electronics and Cryptology (UEKAE), the Information Technologies Institute (BTE), The Advanced Technologies Research Institute (İLTAREN), The Cyber Security Institute (SGE) and The Software Technologies Research Institute (YTE). Thanks to the projects of the

aforementioned institutes, Turkey has become one of the few countries declaring its technological independence in the fields of information security and informatics.
Products and solutions developed by BİLGEM have gone beyond the country's border, being used by many European and Asian countries and NATO as well. In other words, Turkey is no more a country which only imports informatics and information security; but also competes with the world's leading countries in this regard.

TÜBİTAK BİLGEM aims to make our country a reference point with the technologies it has developed, the solutions it offers to universities, the military, the public and private sectors, and the infrastructure works that enable these researches and numerous national and international achievements. In addition, BİLGEM aims to be an R&D center that shapes the future and to direct the science and technology of the future.

TÜBİTAK BİLGEM Cyber Security Institute is a national institute working in various areas of cyber security. SGE provides guidance and special support for several public and private sector organizations including ministry of national defence.

In Cyber Security Institute, there are three main areas: Cyber Security Education and Guidance, Testing and Evaluation and Advanced Cyber Security Technology Development. For technology development, researches have been made in several areas including IOT security, critical

infrastructures, cloud security, honeypot systems, simulation technologies. Also institute has projects in Data Security, Digital Forensics and Endpoint and Information Security.

As a natural partner of NATO and CCDCOE (Cooperative Cyber Defence Centre of Excellence), SGE has trained several military organizations in developing countries like Azerbaijan, Tunisa and Jordan under NATO SPS (Science for Peace and Security) program. SGE joins operational and strategic courses, executive cyber seminars and cyber security exercises like Cross-Sword, prepared by CCDCOE.

SABANCI UNIVERSITY:

Sabancı University has numerous future-shaping applied strategic projects since 1996, continuing in its vision of becoming a leading research university. We have made 7100+ publications and obtained 250+ patents to date. As Sabancı University we get 40+ EU projects with an 8 M€ budget in 2021. In the listings of the world's best universities in the Times Higher Education list (THE) and QS, Sabancı University holds its lead in the rankings among universities from Turkey. Sabancı University is ranked 68th in THE 2021 Best Universities in Asia rankings, in the 81-90 band in the 2021 QS Universities Under 50, and 21st in QS Emerging Europe and Central Asian Countries.
Sabancı University is the pioneering university of Turkey in the areas of cybersecurity and cryptography. Cryptography and Information Security (CISEC) Group of Sabancı University have a wide range of research and development expertise in cryptographic security and cyber security areas. The group has conducted and been involved in several privately and publicly funded projects and co-authored publications in the areas of applied cryptography, IoT and Wireless System

Security, cryptographic engineering, privacy-enhanced technologies, cyber incident detection and remediation, security in networked-systems.
Prof. Albert Levi and Dr. Orcun Cetin are an expert in security and privacy in networked-systems, especially in security and privacy in IoT, IIoT, and using machine learning for boosting security in these areas, in addition to providing security and privacy via statistical and cryptographic ways.
Prof. Cemal Yılmaz is an expert in software security. His works have been focusing on data-driven dynamic analysis of systems to detect (i.e., whether there is an attack), isolate (if so, who is attacking), and prevent attacks at runtime by using statistical and artificial intelligence-based (AI-based) analysis approaches with a special focus on the applicability of the proposed approaches in practice.

ARCELIK A.S:

Arçelik is a multinational household appliances manufacturer, owned by Koç Holding which is one of the largest groups in Turkey and Europe, and the only Turkish company in Fortune Global 500.
Arçelik is pioneer of innovation, working towards the goal of leading the technology in home appliances sector. We dedicate 1.5% of our total annual turnover to research and development (R&D) and employ over 2000 researchers in our central and operational R&D departments. Our high level of expertise in Internet of Things (IoT) cyber security is reflected in our 2018 award of IoT Security Champion from the IoT Security Foundation (IoTSF).
As Arçelik we are following IoT Cyber Security standards very closely. We also applied to the IASME IoT Security assured scheme in its first year of inception and having successfully certified our first product - the connected refrigerator. We also got one of first Common Criteria approval(in EAL2 level) for one of our connected appliance. We think that built-in security should be in center of design and every IoT device should satisfy the minimum recommended requirements. We believe we are one of great examples of a connected device manufacturer that is committed to demonstrate our security compliance to our customers.
In R&D Cyber Security Technology Team, we are dealing with cyber security design infrastructure of millions of Arçelik's connected IoT products, iOS&Android mobile applications, and aws based cloud services for both individually in all respective domains and also e2e relationship in between. We are also responsible from DevSecOps processes, SAST and DAST tools for our S-SDLC processes, creating SBOM for all domains.