A Proactive Approach to Mitigate Cyber Risks in IoT Systems

Daniel SAVU, Electra MITAN
National Institute for Research and Development in Informatics - ICI Bucharest
daniel.savu@ici.ro, electra.mitan@ici.ro

Abstract: The rapid proliferation of Internet of Things (IoT) devices has revolutionized industry and everyday life, connecting billions of devices worldwide. However, this growth has also led to increased cybersecurity risks, as IoT systems are highly vulnerable to attack due to limited security measures, weak defaults, and poor patch management. Artificial Intelligence (AI) and Machine Learning (ML) models can help optimize and secure IoT ecosystems by efficiently managing the data generated and protecting it from cyber threats. ML algorithms can analyze network traffic patterns and identify malicious activity such as attacks or unauthorized access. ML technologies can adjust security measures based on emerging threats, providing a dynamic and adaptive defense. The paper presents aspects of the legal framework regulating IoT in the European Union, the key components of a proactive cybersecurity strategy, real-time monitoring and incident response, the use of AI and ML to deal with cybersecurity incidents, as well as information on conducting penetration tests in IoT ecosystems and the tools useful to assess their security.

Keywords: Cybersecurity, Internet of Things (IoT), Artificial Intelligence (AI), Machine Learning (ML), Penetration Testing.

INTRODUCTION

Over the last decade, technological advances, the development of high-speed communication networks, increased accessibility and prices reduction of hardware components have led to the large-scale adoption of IoT to improve management, transport, and urban infrastructure, reduce costs and automate a range of activities. The IoT environment is a very important factor in the digital development of society (Rădulescu et al., 2023). The application domains are very diverse, including critical infrastructure, industry 4.0, transport, smart cities, smart homes, agriculture, health and pollution control (Kumar et al., 2019). IoT systems have the capability to increase productivity, accountability, traceability, and efficiency, but instead, their potential weaknesses are numerous (Liu et al., 2019).

The expansion of networks and the massive interconnection of billions of IoT devices are creating major cybersecurity challenges (Lone et al., 2023). The devices are vulnerable

https://doi.org/10.54851/v6i2y202410

to cyberattacks because networks are often not designed with security as a priority. Their vulnerabilities can be exploited to access and compromise the entire IoT ecosystem, so the issue of securing them must be at the forefront. The main vulnerabilities that can occur are: weak / no authentication; lack of data encryption; large attack surface; lack of consistent security standards; inadequate updates and maintenance; poor integration between devices; neglected security updates and patches; large attack surface; limited security capabilities; and insecure default configurations. These vulnerabilities also have associated risks that impact critical infrastructure, businesses, and user trust in technology, which is becoming increasingly critical: unauthorized network access, DDoS and botnet attacks (Kumari & Jain, 2023), data interception and modification, manipulation of device operation, data breaches and compromise of critical infrastructure.

The main threats are: malware designed for IoT devices (Wang et al., 2021); phishing and social engineering (Kayarga & Pruthvi, 2021); use of unsecured / weakly secured protocols. The impact of a cyber-attack on an IoT ecosystem can be profound and widespread across many industries and critical infrastructures, but also in the personal lives of individuals, with serious consequences: data security and privacy may be compromised; serious malfunctions may occur, leading to disruptions in the provision of essential services; public health and safety may be jeopardized; direct and indirect economic and financial losses to businesses and users may occur; user confidence in connected technology may be undermined; operations may be disrupted, affecting production and the safety of employees and equipment; the resilience of IoT systems may be reduced.

The GDPR (Regulation (EU) 2016/679) regulates the protection of European Union (EU) citizens' personal data, setting strict standards for collecting, storing, processing and protecting personal data and giving citizens more control over their information. Its main objective is to strengthen safeguards for the protection of citizens' personal data in response to the privacy challenges posed by the development of digital technologies (Li et al., 2019). According to the GDPR, personal data must be processed respecting seven key principles: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability.

The NIS2 Directive (Directive (EU) 2022/2555, 2022) introduced strict cybersecurity rules for EU Member States, aimed at strengthening cooperation between them and creating a common working framework and culture of cybersecurity at the level of companies and organizations in the economy and society. Technical, operational and organizational measures are used to manage the risks that threaten the security of IT systems used for production and service operations. The NIS2 directive focuses on securing IoT systems as part of efforts to improve cybersecurity by requiring stakeholders to implement and manage measures to ensure the cybersecurity of all devices, as any compromised device can be a gateway for cyber-attacks.

The Cyber Resilience Act (CRA) (COM/2022/0454) is the legal framework that establishes a set of cybersecurity rules for EU, regulating products and services with digital elements. Through strict standards and responsibilities, the CRA aims to improve the cybersecurity of digital products and IoT devices and manage vulnerabilities to strengthen the international competitiveness of European companies on a global scale. Implementing security requirements for products (access protection, confidentiality, integrity, availability, and security of delivery) ensures higher standards of cybersecurity and significantly reduces potential risks.

Alignment with global IoT security frameworks is essential to ensure a secure, interoperable, and cyber-resilient IoT ecosystem. IoT cybersecurity measures must be robust solutions that protect data and minimize the risks associated with the interconnection of devices and critical infrastructure (Ahmed & Khan, 2023). These measures include: designing IoT devices with built-in security, including the use of strong authentication, data encryption, and intrusion

protection; updating IoT device software and releasing patches for discovered vulnerabilities; implementing robust authentication mechanisms (multi-factor authentication - MFA); segmenting IoT networks from other critical networks, so that a compromise in one IoT system does not affect other critical infrastructure components; encrypting communications between IoT devices and central platforms; continuously monitoring and detecting anomalies and possible cyber-attacks; implementing standards and certification programs for IoT devices to ensure compliance with security best practices.

In the recent past, cyber incidents in IoT ecosystems have had a significant impact on critical infrastructure, industries and individual users. Here are a few examples:

- In 2016, the Mirai botnet attack (one of the largest DDoS attacks) (Antonakakis et al., 2017), (Andriu, 2019) infected thousands of IoT devices (surveillance cameras, routers, and other Internet-connected devices). The devices were compromised due to the use of weak default passwords and the lack of security updates. Once infected, the devices were used to launch DDoS attacks against major services and websites. This resulted in massive website outages (Twitter, Reddit, Spotify, The New York Times) affecting millions of users worldwide. The need for strong passwords and security updates for all IoT devices was demonstrated;
- In 2017, the US Food and Drug Administration (FDA) issued a warning about cyber vulnerabilities in some IoT medical devices, including defibrillators and insulin pumps (Kramer & Fu, 2017). Attackers could have remotely taken control of the devices and changed critical settings, putting patients' lives at risk. The attacks could have had a serious impact on patient health and safety. Security updates and new protection protocols were needed. Stringent cybersecurity standards for connected medical devices and the integration of safeguards at the product design stage proved necessary;
- In 2021, an attack on DNS routers used in IoT ecosystems. Attackers exploited vulnerabilities in routers to redirect Internet traffic. IoT routers were compromised by attacking unsecured firmware and default configurations. DNS settings were altered; users were redirected to phishing sites, affecting thousands of IoT devices and networks worldwide, compromising data and exposing users to financial and security risks.

Emerging technologies such as Artificial Intelligence (AI), Machine Learning (ML), advanced cryptography, 5G networks, blockchain, multi-factor authentication technologies, Zero Trust Architecture (ZTA), threat detection and response technologies provide the solutions to improve the security of IoT ecosystems that continue to grow in complexity and size. Deploying these proactive solutions helps protect devices and data, creating a more secure, resilient and reliable IoT environment.

AI (Trilles et al., 2024) and ML (Haji & Ameen, 2021) detect anomalous patterns of behavior in IoT networks with proactive threat detection capabilities by analyzing large volumes of data in real-time; algorithms identify sophisticated attacks and prevent security breaches; advanced cryptography (symmetric and asymmetric) - algorithms can secure data by protecting communications between IoT devices from unauthorized eavesdropping and tampering; quantum cryptography ensures the exchange of cryptographic keys in a way that cannot be cracked by conventional methods, providing impenetrable security against sophisticated cyber-attacks; multi-factor authentication (MFA) - technologies add an additional layer of verification to the traditional password and can include biometrics, physical tokens, location-based authentication.

5G technology enables better security management of simultaneously connected IoT devices, providing enhanced security measures (end-to-end encryption, network segmentation); ZTA assumes that no device, user or application is trusted by default, even within the network (Syed et al., 2022). Every access must

be continuously verified and authenticated, increasing the protection of IoT devices from unauthorized access; Extended Threat Detection and Response (XDR) technologies integrate and correlate security data from disparate sources, building a unified, clear picture of cyber threats and attacks (George et al., 2021).

As a newer technology, quantum computing can contribute to: the development of advanced cryptographic methods (quantum cryptography), providing high levels of security for IoT communications; streamlining network management, optimizing data routing, resource management, reducing energy consumption; rapid and complex analysis of data generated by IoT devices (patterns, more accurate predictions); simulation of the behavior of complex systems (transport networks, environmental interactions), supporting urban planning and sustainable development.

The paper structure is: Section 2 - Key components of a proactive cyber security strategy, Section 3 - Real-time monitoring and response to threats, Section 4 - AI and ML in mitigating the cyber risks of IoT ecosystems, Section 5 - Penetration tests in IoT ecosystems, Section 6 - Recommendations on securing IoT ecosystems, and finally Conclusions and Reference List.

KEY COMPONENTS OF A PROACTIVE CYBER SECURITY STRATEGY

A brief analysis of cyber threats evolution in IoT ecosystems shows that the exponential growth in the number of connected devices provides attackers with more entry points into networks. The diversity of devices is also a problem: many are designed without security in mind, making them vulnerable to exploitation; many devices are not regularly updated / have no automatic update mechanism, exposing them to known attacks. The complexity of IoT ecosystems also stems from interconnectivity and cloud dependency. Cyber threats can include DDoS attacks, intrusions and hacking, and data exfiltration (Perwej et al., 2021). Vulnerabilities also arise from a lack of standardization and regulatory compliance. An emerging trend is to approach security from the design phase of IoT devices, integrating security measures from the development stage. The use of automated security solutions can help monitor and protect IoT ecosystems through anomaly detection and rapid incident response. They play an important role in raising awareness of the associated cyber risks among developers to promote best practices in the use and development of IoT devices. The evolution of cyber threats is dynamic and complex. As technology advances, so do attackers' tactics. Implementing proactive security strategies can protect users' devices and data through innovative solutions and user education.

Proactive cybersecurity strategies for IoT ecosystems ensure the integrity, confidentiality, and availability of data and connected systems, as every device in the system has potential vulnerabilities.

Key components of such a strategy in IoT ecosystems:

- IoT-specific risk assessment (Kandasamy et al., 2020): vulnerability identification (the infrastructure is regularly assessed to identify specific weaknesses and vulnerabilities of IoT devices, including hardware, software, and communication protocols); impact analysis (the potential impact of cyber incidents on IoT systems is determined, considering the sensitive data managed and the impact on operations).
- Security policies and procedures: customized IoT policies (defining specific policies to address the unique risks and requirements of IoT devices, including relevant compliance regulations); incident response procedures (establishing clear procedures for handling cyber incidents involving IoT devices, including isolation of compromised devices).
- IoT security technologies: authentication and access control (robust authentication mechanisms are implemented to ensure that only authorized users and devices can access the network) (Ali et al., 2019); data encryption (all data transmitted between devices is encrypted to prevent interception and unauthorized access).

- Monitoring and detection: security monitoring solutions (implementing monitoring solutions that detect unusual activities/anomalies in the behavior of IoT devices); intrusion prevention systems (deploying an IPS system that blocks cyber-attacks in real-time and protects the network).
- User training and awareness: employee training (specific training sessions will be organized for employees on security and best practices in the use of IoT devices); end-user awareness (end-users will be informed about the risks associated with IoT devices and how to protect personal data).
- Device lifecycle management: purchasing and implementation planning (assessing the security of IoT devices before purchase and establishing procedures for integrating them into the infrastructure); updates and patches (regularly scheduled software updates and application of security patches to IoT devices).
- Collaboration: working with device manufacturers (partnering with IoT device vendors to ensure products meet required security standards); participating in IoT security communities (seeking to participate in security forums and working groups to share information and learn from others' experiences).
- Incident management: specific response plan for IoT (a step-by-step incident response plan to be followed in the event of a cyber-attack on IoT devices is developed); plan testing (exercises and simulations are conducted to verify the effectiveness of the response plan and identify gaps).
- Continuous assessment and improvement: periodic review of policies (periodic review of security policies and procedures is planned to update them in line with changes in the threat landscape); feedback from the incident (feedback is collected following security incidents to improve existing measures and adapt the security strategy).
- Contingency planning: business continuity plans (plans are developed to ensure the continuity of critical operations in the event of a cyber-attack on the IoT system); data recovery (procedures are established for rapid data recovery in the event of security incidents).

Such a strategy integrates risk assessment, specific policies, advanced security technologies, training, and collaboration to ensure: the protection of devices, security of data, minimization of the impact of incidents, user confidence in technologies, and adaptability to a safe and reliable environment for users.

REAL-TIME MONITORING AND RESPONSE TO THREATS

Information technology manages data and communications, while operational technology manages physical operations and machines, incorporates hardware and software into the system, and monitors and manages physical processes (Pawar, 2024). The IoT ecosystem collects and shares data over the Internet. Security measures protect the connected devices and data.

Networks provide instant access to data and operations, which attracts cybercriminals and gives them the opportunity to exploit the wide range of vulnerabilities in IoT devices: weak passwords, insecure networks, insecure APIs, cloud or mobile interfaces, outdated or obsolete components, insecure data transfer and storage, poor device management, lack of confidentiality, insufficient physical security, inadequate authentication mechanisms.

IoT devices compromised by the above vulnerabilities can become tools for launching significant cyber-attacks (DDoS attacks, malware) that disrupt IoT network operations and services. This situation facilitates data theft, unauthorized access, and the spread of malware to other network assets. The examples of threats we present below are just some of the many risks that target IoT devices and networks: Trojan Attacks, Side Channel Attacks, Botnet, Spoofing Attacks, Eavesdropping, Relay Attacks, and OnPath Attacks.

Therefore, real-time monitoring and response to cyber threats is critical to maintaining security in IoT ecosystems. Constant monitoring and rapid response can prevent greater damage and reduce the exposure time to attacks. Real-time monitoring and response in IoT ecosystems can be achieved in the following ways:

- Time monitoring of the system: by implementing IDS - Intrusion Detection Systems (monitoring of network traffic and devices) and IPS - Intrusion Prevention Systems (threat detection and automatic blocking of attacks);
- Network traffic monitoring - by continuously analyzing the flow of data between devices and back-end servers and identifying anomalies; setting alarms for unusual activity;
- Monitoring the operational and security status of devices;
- Anomaly detection based on AI and ML using algorithms that identify unusual behavior.

Automate real-time response to threats by deploying a Security Orchestration, Automation and Response (SOAR) solution (Kinyua & Awuah, 2021) isolate compromised devices to prevent attacks from propagating; automatically apply security updates to IoT devices as vulnerabilities are discovered; provide real-time alerts to the security team. If a threat is not resolved in time, it is escalated to higher levels of management.

AI and ML can be used for IoT ecosystem monitoring which brings significant benefits given the increasing complexity and size of IoT systems. Devices are connected in distributed networks, generate large volumes of data, and are exposed to multiple threats. AI and ML can analyze data in real-time, detect abnormal behavior, optimize operations for increased performance, and provide improved security. Next, we will present an exhaustive overview of the activities that can be carried out using AI and ML.

1. Predictive analytics and proactive maintenance

Predictive analytics uses AI and ML models to anticipate problems in the ecosystem before they become critical. Predictive maintenance analyses historical data to identify patterns that indicate possible component failure/wear. This enables proactive maintenance, reduces downtime, and improves operational efficiency. In a smart factory, IoT sensors monitor production equipment. AI can analyze data from these sensors to predict when a machine needs maintenance, preventing unplanned production interruptions.

2. Real-time monitoring and anomaly detection

AI and ML models can detect anomalies in real-time because they can learn and recognize normal and abnormal behavior of IoT ecosystems. Data flows are monitored in real-time and unusual behavior/activity is flagged, indicating operational problems, cyber-attacks, and misuse of resources. AI models can continuously adapt based on incoming new data and learn from past behaviors to quickly identify emerging threats. In an IoT network in a smart home, AI can monitor energy flows and device behavior, detecting potential problems such as sudden spikes in energy consumption that could signal a malfunction or cyber-attack.

3. Response automation and performance optimization

AI and ML models enable the automation of monitoring and adjustments in IoT ecosystems, optimizing device performance and network efficiency without human intervention in response. In an IoT traffic management system, AI can detect increases in vehicle flow and adjust the timing of traffic lights to optimize traffic without the need for human operator intervention. An IoT energy management system in a smart building can adjust energy consumption based on data received from sensors about room occupancy and weather conditions.

4. Improve security and detect cyber threats

Machine Learning models can improve the security of IoT ecosystems by detecting and preventing cyber-attacks faster and more accurately than traditional systems; they can

detect malicious traffic patterns or abnormal device behavior, alert administrators, and automatically block attacks. AI models can optimize authentication and encryption mechanisms by dynamically adapting to network conditions or threat levels. In an IoT network managing critical infrastructure, AI can detect unauthorized access attempts to sensitive systems and trigger automatic protection measures, such as blocking access or resetting devices.

5. Data Analysis and Decision Improvement

AI models can efficiently analyze data and extract useful information, facilitating informed decisions. In big data analysis, machine learning algorithms can detect patterns that may not be obvious at first glance, helping to understand system behavior and optimize overall performance. The analysis of historical and real-time data can lead to the prediction of possible failure points and the identification of preventative solutions. In a smart agriculture IoT ecosystem, AI can analyze data on soil moisture, weather conditions, and crop water requirements to optimize irrigation processes. An IoT system on a production line can use AI to predict machine problems before they occur, based on unusual vibrations or other signals, reducing downtime.

AI AND ML IN MITIGATING THE CYBER RISKS OF IOT ECOSYSTEMS

The normal functioning of IoT ecosystems requires the efficient and secure interaction of interconnected devices, platforms, and applications that collect, transmit, and analyze data to perform the tasks at hand. Optimal integration of physical devices with networking technologies and analytics platforms ensures high performance and protection against cyber threats. However, deviations from the normal/expected behavior of devices and data flows can occur. Anomalies can be early signals of technical problems, operational errors, or cyber-attacks. Their detection and management ensure the security and proper functioning of these systems.

Anomalies in IoT systems can vary in cause and impact and may relate to device behavior, traffic, access, resource consumption, timing, data quality, data volume, data reporting frequency/mode, location, latency in data delivery (minor deviations from the usual operating pattern that can be resolved by recalibration or configuration, signs of complex cyber-attacks - high volume of network requests or unusual device behavior, network failures). They can be caused by hardware failures, software errors, network problems, misconfigurations, and cyber-attacks. Here are the main attack methods specific to IoT ecosystems (Shafiq et al., 2022): Denial of Service (DoS) and Distributed Denial of Service (DDoS), Eavesdropping and Sniffing, Man-in-the-Middle (MitM), Firmware Tampering, Botnets, Side Channel, Software Exploits, Ransomware, Replay, Authentication and Authorization, Sybil and Sinkhole in IoT Networks, over Wireless and Sensor Networks, Firmware and Software Updates. Early detection helps maintain IoT ecosystems' integrity, security, and performance. Deploying solutions based on AI and ML (Shah, 2021) can help identify anomalies and respond quickly to potential threats.

Various techniques can be used to detect anomalies: ML-based (supervised, unsupervised, semi-supervised models), Statistical Methods (threshold-based detection, time series analysis, data distribution modeling), heuristic methods (rule-based detection), stream data anomaly detection, security anomaly detection (Intrusion Detection Systems - IDS), data packet analysis. Failure to detect anomalies in time can have a negative impact on IoT ecosystems: reduced performance, compromised security, and significantly high costs.

AI and ML methods and techniques for cyber threat detection are constantly evolving, enabling organizations to stay ahead of emerging threats and protect critical assets in an increasingly complex cybersecurity landscape. Their effective implementation requires a combination of advanced technology, quality data, and human expertise to ensure a rapid and tailored response to cyber threats.

Here are some of the AI and ML methods and techniques used for threat detection.

- Anomaly detection - ML models profile the normal behavior of users, applications, and networks. A deviation from normal behavior is detected as an anomaly, which may indicate a potential threat.
- Threat classification: Supervised learning models are trained on labeled datasets (data about known attacks and legitimate activity) and then classify new security events by identifying threats in real-time.
- Zero-day malware detection: The models analyze the behavior and characteristics of new files or processes and detect unknown malware; they identify behavior patterns and evasion techniques used by polymorphic or zero-day malware.
- Unsupervised learning to detect unknown threats: the models analyze unlabeled data to discover new threat patterns without requiring prior knowledge about existing attacks.
- Semi-supervised learning for enhanced detection: combines a small amount of labelled data with a large amount of unlabeled data to detect threats more efficiently, even when there is not enough predefined data.
- Reinforcement learning: Models can learn by continuously interacting with the environment, adjusting defensive strategies based on feedback to optimize incident response and adapt the system to emerging threats.
- Text analysis and Natural Language Processing (NLP) - Thematic Modelling, Sentiment Analysis: Models analyze and classify text (email) messages to detect threats such as phishing.
- Convolutional Neural Networks (CNNs) and Recursive Neural Networks (RNNs) - process surveillance image data/ analyze executable files and data sequences (logs), analyze network traffic and detect anomalies, and identify attack patterns.

Here are some examples of how algorithms are used to detect cyber threats:

- Identify unusual data access, unauthorized network connections, or unusually large data transfers. These can indicate insider attacks, malware activity, or account compromise. Algorithms: K-Means, Support Vector Machines (SVM), Neural Networks.
- Classify executable files as malware or legitimate software, identify phishing emails, or detect brute force attacks. Algorithms: SVM, Logistic Regression, Random Forest, Term Frequency - Inverse Document Frequency (TF-IDF), Word Embeddings (Word2Vec), Naive Bayes, Decision Trees, Neural Networks.
- A detection system that runs files in a sandbox environment and monitors their behavior to detect malicious activity, such as unauthorized access to the file system or unauthorized communication with command and control (C&C) servers. Algorithms: decision trees, SVM, neural networks, principal component analysis (PCA).
- Identifying an insider attack within an organization or discovering an unknown botnet spreading across the network without knowing the type of malware being used. Algorithms: clustering techniques, feature extraction techniques, autoencoder neural networks;
- Identify phishing or targeted attacks within an organization by combining historical data with new security intelligence. Algorithms: Self-training, co-training, neural networks, clustering;
- An AI system that learns to improve the effectiveness of firewalls or security policies by analyzing past attacks. Algorithms: Q-learning, Deep Q-Networks (DQN), Policy Gradient Methods, Proximal Policy Optimization (PPO), Trust Region Policy Optimization (TRPO).

The use of AI and ML in cyber threat detection brings scalability (real-time analysis of large volumes of data), adaptability (to emerging threats), proactive detection (anomalies and

unknown complex attacks), and threat response automation (faster response time and reduced damage from cyber-attacks).

PENETRATION TESTS IN IOT ECOSYSTEMS

Modern businesses are complex, technology-dependent and highly interconnected. Technologies evolve rapidly and create widespread opportunities for theft, fraud and other forms of exploitation by criminals both from outside and inside an organization. Criminals can exploit traditional vulnerabilities in a very short time; they can exploit newly reported vulnerabilities in the information systems that are now the backbone of every organization. In a strong networked environment, these crimes can be committed globally, from almost anywhere in the world, and can have a significant impact on the very existence of an organization/ community. Therefore, strong measures must be taken: defining and implementing a robust security architecture strategy, framework, and governance processes; developing a set of models that support standardized and repeatable security solutions developed according to security needs; measuring the maturity of the security architecture against generally accepted practices, specific policies, and partners for effective prioritization of activities.

By implementing appropriate policies and measures, cyber-attacks on IoT ecosystems can be prevented and risks minimized before they materialize. This approach anticipates threats, protects infrastructure, and preserves data integrity. The basic components of a timely cybersecurity strategy for IoT ecosystems include risk assessment, secure design of IoT devices, authentication, and access control, continuous monitoring and analysis, regular patching and updates, user education and awareness, development of security policies and plans with incident response procedures, partnering with security experts and organizations.

Penetration testing is useful in protecting infrastructure from cyber threats. The risk associated with an IoT ecosystem is given by its value, weighted by the probability of exploitation of its threats and vulnerabilities, and the potential impact of successful exploitation of a threat or vulnerability. Increasing any of these factors will increase the relevant risk; decreasing any of these factors will reduce the risk. Understanding all of this makes it possible to reliably assess risk.

Penetration testing assesses and quantifies the threats and vulnerabilities associated with an IoT ecosystem under test and attempts to exploit those vulnerabilities that have the potential to allow access to the system. By performing specific tests, an independent and objective security assessment of the system can be made, highlighting the specific risk of unauthorized access to the system from the outside and the inside. The true technical risks associated with IoT systems can be identified to facilitate the subsequent identification of the necessary controls to be implemented to address these risks.

A complete penetration test should ensure application security testing; network infrastructure security testing; and user security testing (Figure 1):

- Network security pen testing: identifies network-related vulnerabilities - routers, switches, network hosts - external and internal network penetration testing, wireless network penetration testing, perimeter network penetration testing, network segmentation testing, voice over IP penetration testing;
- Web application pen testing: evaluates overall security, identifies risks associated with code errors, injections, broken authentication - authentication and authorization testing, SQL injection and command injection vulnerability testing, Cross-Site Scripting (XSS) vulnerability testing, file inclusion vulnerability testing, Cross-Site Request Forgery (CSRF) vulnerability testing, session hijacking and

session sealing testing, input validation testing, exposed content and sensitive information testing, performance and availability testing (DoS);
- IoT security pen testing: determines the security of various IoT devices through hardware security testing, application testing;
- Cloud security pen tests: validate the accuracy of cloud configuration; identify cloud-related risks such as data breaches, and data loss;
- User (social engineering) pen tests: use of phishing techniques to determine how a network can defend, detect, and respond; spear phishing, whaling, pretexting, baiting attacks, tailgating and piggybacking attacks, password policy testing, voice phishing

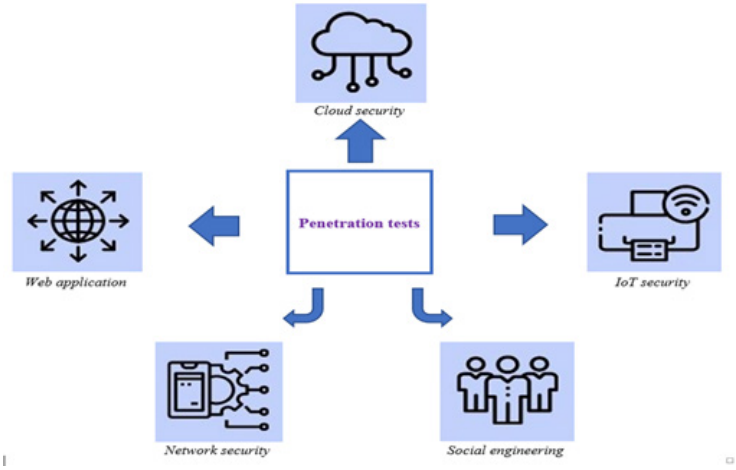

Figure 1. *Components security testing in an IoT system*

In IoT ecosystems, the penetration testing process involves several steps:
- planning - define the objectives of the penetration test (identify vulnerabilities, assess resilience to attack, test compliance with security standards); identify the IoT devices, software applications, and associated networks that will be subject to the penetration test;
- reconnaissance - gather information using reconstruction techniques to obtain data about devices, software applications, protocols used, and security configurations; scan the network to identify IP addresses, open ports, and active services associated with IoT devices;
- vulnerability assessment - test security configurations to identify bad/weak settings (passwords, insecure protocols); scan for vulnerabilities using automated tools; analyze source code of applications associated with IoT devices to identify security flaws;
- exploitation of identified vulnerabilities - conduct simulated attacks to determine if vulnerabilities can be effectively exploited (network attack/communication interception; software exploitation; physical security testing);
- impact assessment -assesses the potential impact of exploiting vulnerabilities on the privacy, integrity, and availability of the IoT ecosystem and risk assessment with categorization of vulnerabilities by type, threat type, impact severity, exposure, device type, lifecycle, purpose of exploitation;
- test report development - describes the vulnerabilities identified, how they were exploited, and their impact, and makes recommendations for remediation of the issues identified; presents the results to

the security team and decision makers for remediation prioritization;
- fixing vulnerabilities - supplementing security measures (patches, software updates, other security measures); reviewing and adjusting security policies and procedures to prevent similar problems in the future;
- retesting - verifying the effectiveness of implemented measures by conducting additional penetration tests; continually adjusting security strategies based on lessons learned and newly identified threats.

Penetration testing uses tools to identify and exploit vulnerabilities in systems, networks, and applications, test security and make recommendations to improve cyber protection. There is a variety of tools that can be categorized according to their specific purpose:

- for information gathering and OSINT (Open Source Intelligence): visualizing relationships between people, companies, and domains; searching for devices connected to the Internet, and servers; gathering information related to domains, IP addresses - Maltego, Shodan, Recon-ng;
- for vulnerability scanning: identification of configuration issues, software vulnerabilities, vulnerability scanning and security testing of systems and applications; device discovery, identification of open ports and analysis of services running on them: Nessus, OpenVAS, Nmap;
- for vulnerability exploitation: penetration testing and simulation of cyber-attacks; exploitation of vulnerabilities in web browsers, simulation of attacks based on the exploitation of web pages; detection and exploitation of SQL injection vulnerabilities, penetration of applications using databases: Metasploit, BeFF, SQLmap;
- for testing the security of web applications: intercepting HTTP/S traffic, processing it, and identifying vulnerabilities in applications; detecting vulnerabilities such as SQL injection, Cross-Site Scripting, and poor configuration: Burp Suite, Wapiti, Acunetix;
- for testing the security of wireless networks: monitoring, eavesdropping, and password cracking for Wi-Fi networks; packet analysis, network and access point discovery, WPS protocol PIN code cracking: Aircrack-ng, Kismet, IoT Inspector, Reaver;
- for forensics and post-attack analysis: open source forensic analysis to investigate and gather evidence after attacks; RAM memory analysis to analyze the details of a compromised system and collect samples; network packet analysis to monitor network traffic and identify suspicious activity: Autopsy, Volatility, Wireshark;
- for password management and authentication: testing the security of passwords, cracking passwords that support numerous hash types (MD5, SHA, bcrypt); cracking passwords, checking their reliability using dictionaries or brute force attacks; testing authentication on various protocols (HTTP, FTP, SSH): Hashcat, John the Ripper, Hydra;
- for social engineering and phishing: simulation of social engineering attacks (phishing, vishing, spear-phishing); simulation of phishing campaigns, fake emails and web pages for user testing: Social-Engineer Toolkit, Gophish.

Some useful tools for penetration testing are briefly mentioned below: Nmap, Metasploit, Burp Suite, IoT Inspector, Wireshark.

Nmap (Network Mapper) (Kaur, G. & Kaur, N., 2017) is a network scanning and analysis tool used to identify devices connected to a network, check their status, and identify potential vulnerabilities. It can be used to scan open ports in a system, perform TCP and UDP scans; detect devices connected to a network (operating system type, version, installed software products), identify specific details about network devices; detect known or

specific vulnerabilities in the network; perform advanced scans (stealth, SYN). Nmap is used for security auditing; identification of active network devices and services; penetration testing; and network monitoring.

Metasploit (Raj & Walia, 2020) is a tool that can identify connected devices, exploit vulnerabilities by having a large number of exploit modules that can target various vulnerabilities specific to IoT devices (buffer overflow vulnerabilities, SQL injection, or authentication issues), and search for exploits that target certain services or applications used by IoT devices. Metasploit allows the use of custom payloads to gain access or execute commands on IoT devices, selecting different payload types depending on the operating system and device architecture. After gaining access to an IoT device, post-exploits modules can be used to extract information or perform additional actions. Metasploit has modules for simulating DoS attacks, which is useful for assessing the resilience of IoT devices to saturation attacks. It can be integrated with other security testing tools, such as Nmap for scanning and Burp Suite for web application analysis, to extend its IoT security testing capabilities.

Burp Suite (Kore et al., 2022) is a tool used to test the security of web applications with a wide range of functionalities, with a specific role in evaluating and identifying web application vulnerabilities. It can also be used for security testing of IoT devices, although some specific aspects of this domain may require different approaches than testing traditional web applications. The following shows how this tool can be used in the context of IoT, with a customized approach and understanding of the specifics of IoT communications. The Proxy Burp component can be configured to intercept traffic between IoT devices and their servers. This can include setting up a proxy on mobile devices or computers that interact with IoT devices. For IoT devices communicating over HTTP/S, Burp can capture requests and responses for analysis and modification. For vulnerability scanning, the Scanner component can scan APIs and web services associated with IoT devices for vulnerabilities such as SQL injection or XSS. Access to relevant device APIs is important. For API testing, many IoT devices communicate via RESTful or SOAP APIs, and Burp Suite can analyze these interfaces to uncover security issues. The Intruder function can be used to fuzz API parameters or configuration interfaces of IoT devices, testing different payloads to evaluate application behavior. The Repeater function modifies and resends requests to IoT devices to test the response to invalid or unusual data. When IoT devices use specific encoding formats for transmitted data, the Decoder feature is used to analyze and understand the communication. Comparing responses from IoT device APIs identifies variations that could indicate misbehavior or potential vulnerabilities. Many IoT devices use protocols such as MQTT, CoAP, or WebSocket, which may require additional tools or custom configurations to test effectively.

IoT Inspector (Huang et al., 2020) is an IoT device security monitoring and assessment tool that analyzes and identifies vulnerabilities in IoT networks to understand the connected devices' behavior. For traffic analysis, it captures and analyzes data packets sent by IoT devices to visualize communications and identify potential security issues; it can monitor traffic in real-time to detect unusual behavior or suspicious activity. Vulnerability identification includes scanning capabilities to identify known vulnerabilities in the software and protocols used by IoT devices; it uses vulnerability databases to check whether devices are exposed to known risks. An intuitive interface provides a quick visualization of the security status of connected devices. Analyzes IoT device behavior to understand usage patterns and detect anomalies. Enables identification of device types and software in use, providing visibility into the IoT ecosystem.

Wireshark (Iqbal & Naaz, 2019) is a tool that can identify vulnerabilities and security risks in IoT networks and assess how devices and applications handle data: Can monitor communications (data packets transmitted between IoT devices and associated servers - traffic from sensors, actuators, and other

connected devices); decode and analyze specific protocols - MQTT, CoAP, Zigbee - and analyze transmitted messages; identify vulnerabilities (exposing sensitive data; detecting misconfigurations - open ports, unauthorized communications between devices); can verify authentication between devices and servers and examine data transmission between devices to detect breaches in security protocols; analyze communications in MitM attacks; analyze DdoS attacks; identify abnormal network behavior; identify packets that should not be on the network; indicate possible security breaches / unauthorized activities); can be integrated with other security tools such as Nmap, Metasploit or Burp Suite for a more comprehensive security assessment of IoT ecosystems.

RECOMMENDATIONS ON SECURING IOT ECOSYSTEMS

A proactive approach to mitigating cyber risks in IoT systems involves implementing advanced security measures, rigorous monitoring procedures, and managing vulnerabilities before they are exploited. The IoT ecosystem is complex, with multiple connected devices exchanging data over the network; under these conditions, cyber risks are diverse. Therefore, a preventive strategy is needed to ensure the protection of the system. In this context, the following are considered:

- secure design and implementation of security protocols for hardware and software components; secure communication protocols; automatic firmware updates;
- authentication and access control through complex and unique passwords, multi-factor and certification-based authentication; strict limitation of access to basic functions for users and devices as needed; centralized identity management;
- network segmentation by separating the IoT network from the rest of the IT infrastructure; continuous network monitoring to detect intrusions, detect unusual activity, block attacks, observe anomalies, and regularly audit device configurations and access;
- vulnerability management through scanning tools and regular patching with updates to address security issues, bugs, and vulnerabilities; precise protocols for emergency updates for critical vulnerabilities that are discovered;
- end-to-end data encryption of transmitted and stored metadata, logs, and other auxiliary data; privacy protection by limiting and monitoring access to personal and critical data;
- periodic attack simulation (penetration testing) to assess the level of network security and continuous security evaluation; simulation of an IoT environment in a cyber-range to test the security of infrastructure and incident response practice; attack-defense / "red team - blue team" exercises to test the effectiveness of security measures;
- developing an incident response and recovery plan that includes: a detailed incident response protocol with assigned responsibilities; a business continuity and disaster recovery plan with regularly tested backup and recovery procedures; regular simulations and staff training to minimize human error.

Adopting a proactive prevention and protection approach to IoT security is an ongoing process that involves continuous monitoring, rigorous updates, and testing to protect IoT systems from attack and ensure data availability and integrity.

CONCLUSIONS

The proactive approach to mitigate cyber threats helps secure the complex and interconnected framework of the IoT environment. Anticipating threats, deploying robust defenses, and educating users reduce risk and ensure the overall security of IoT ecosystems. By focusing on the essential elements of a proactive cybersecurity approach, organizations can establish a baseline of

protection that anticipates and addresses vulnerabilities before they are exploited. Continuous threat monitoring and response enhances IoT security reducing the risk of damage and data breaches.

AI and ML technologies serve as the main resources for reducing IoT cyber threats by enhancing the system's ability to recognize patterns, detect anomalies, and adapt to changing threats in real-time. Penetration testing contributes to a proactive approach to IoT security, providing insight into potential vulnerabilities and facilitating timely remediation. Security assessment software tools facilitate continuous evaluation and provide a holistic view of the IoT infrastructure, ensuring compliance with security standards and improving system integrity. In this framework, organizations can efficiently secure their IoT environments while promoting safe and sustainable IoT development. This approach and use of cutting-edge technologies can create a robust defense system adapted to the ever-evolving cyber threat environment, ensuring that IoT devices operate securely, and reliably in a trusted environment for users. In this manner, a strong cybersecurity culture, so necessary in the digital age is built.

REFERENCE LIST

Ahmed, S. & Khan, M. (2023). Securing the Internet of Things (IoT): A Comprehensive Study on the Intersection of Cybersecurity, Privacy, and Connectivity in the IoT Ecosystem. *AI, IoT and the Fourth Industrial Revolution Review.* 13(9), 1-17.

Ali, I., Sabir, S. & Ullah, Z. (2019). Internet of Things Security, Device Authentication and Access Control: A Review. To be published in *Cryptography and Security*. [Preprint] https://arxiv.org/abs/1901.07309 [Accesed 24th July 2024].

Andriu, A.V. (2019). DoS and DDos Attacks on IoT Devices. *Romanian Cyber Security Journal.* 1(2), 85-88.

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J. & Zhou, Y. (2017). Understanding the Mirai Botnet. In the *Proceedings of the 26th USENIX security symposium (USENIX Security 17), 16-18 August 2017, Vancouver, BC, Canada.* 1093-1110.

COM/2022/0454 - European Parliament legislative resolution of 12 March 2024 on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive). *Official Journal of the European Union*, L333, 27.12.2022, 80–152. http://data.europa.eu/eli/dir/2022/2555/oj [Accessed 25th September 2024].

George, D. A. S., George, A. H., Baskar, T. & Pandey, D. (2021). XDR: The Evolution of Endpoint Security Solutions-Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future. I*nternational Journal of Advanced Research in Science, Communication and Technology (IJARSCT).* 8(1), 493-501.

Haji, S. H. & Ameen, S. Y. (2021). Attack and anomaly detection in IoT networks using machine learning techniques: A review. *Asian Journal Research Computer Science.* 9(2), 30-46. doi:10.9734/ajrcos/2021/v9i230218.

Huang, D. Y., Apthorpe, N., Li, F., Acar, G. & Feamster, N. (2020). IoT Inspector: Crowdsourcing Labeled Network Traffic from Smart Home Devices at Scale. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies.* 4(2), 1-21. doi:10.1145/3397333.

Iqbal, H. & Naaz, S. (2019). Wireshark as a tool for detection of various LAN attacks. *International Journal of Computer Sciences and Engineering.* 7(5), 833-837. doi:10.26438/ijcse/v7i5.833837.

Kandasamy, K., Srinivas, S., Achuthan, K. & Rangan, V. P. (2020). IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security.* 8, 1-18. doi:10.1186/s13635-020-00111-0.

Kayarga, T. & Pruthvi, PR. (2021). A Review Article on Impact of Social Engineering Attacks against Security of IoT. *Turkish Online Journal of Qualitative Inquiry.* 12(7).

Kaur, G. & Kaur, N. (2017). Penetration testing–reconnaissance with NMAP tool. *International Journal of Advanced Research in Computer Science.* 8(3), 844-846.

Kinyua, J. & Awuah, L. (2021). AI/ML in Security Orchestration, Automation and Response: Future Research Directions. *Intelligent Automation & Soft Computing.* 28(2), 527-545. doi:10.32604/iasc.2021.016240.

Kore, A., Hinduja, T., Sawant, A., Indorkar, S., Wagh, S. & Rankhambe, S. (2022). Burp Suite Extension for Script based Attacks for Web Applications. In *2022 6th International Conference on Electronics, Communication and Aerospace Technology,* IEEE, 651-657.

Kumar, S., Tiwari, P. & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. *Journal of Big Data.* 6 (111), 1-21. doi:10.1186/s40537-019-0268-2.

Kumari, P. & Jain, A. K. (2023). A comprehensive study of DDoS attacks over IoT network and their countermeasures. *Computers & Security.* 127(C), 103096. doi:10.1016/j.cose.2023.103096.

Kramer, D. B. & Fu, K. (2017). Cybersecurity Concerns and Medical Devices: Lessons from a Pacemaker Advisory. *Jama.* 318(21), 2077-2078. doi:10.1001/jama.2017.15692.

Li, H., Yu, L. & He, W. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management.* 22(1), 1-6. doi:10.1080/1097198X.2019.1569186.

Liu, X., Qian, C., Hatcher, W. G., Xu, H., Liao, W. & Yu, W. (2019). Secure Internet of Things (IoT)-based smart-world critical infrastructures: Survey, Case Study and Research Opportunities. *IEEE Access.* 7, 79523-79544. doi:10.1109/ACCESS.2019.2920763.

Lone, A. N., Mustajab, S., & Alam, M. (2023). A comprehensive study on cybersecurity challenges and opportunities in the IoT world. *Security and Privacy.* 6(6), e318. doi:10.1002/spy2.318.

Pawar, S. (2024). *The Rise of IoT Attacks: Endpoint Protection Via Trending Technologies.* https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/the-rise-of-iot-attacks-endpoint-protection -via-trending-technologies [Accessed 24th September 2024].

Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N. & Jaiswal, A. K. (2021). A Systematic Literature Review on the Cyber Security. *International Journal of Scientific Research and Management.* 9(12), 669-710. doi:10.18535/ijsrm/v9i12.ec04.

Raj, S. & Walia, N. K. (2020). A Study on Metasploit Framework: A Pen-Testing Tool. In *2020 International Conference on Computational Performance Evaluation (ComPE), Shillong, India, 2020, IEEE,* 296-302. doi:10.1109/ComPE49325.2020.9200028.

Rădulescu, C. Z., Boncea, R. & Vevera, A. V. (2023). A Multi-criteria Weighting Approach with Application to Internet of Things. *Studies in Informatics and Control.* 32(4), 5-16. doi.org/10.24846/v32i4y202301.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*, L119, 04.05.2026, 1-88. http://data.europa.eu/eli/reg/2016/679/oj [Accessed 18th September 2024]

Shafiq, M., Gu, Z., Cheikhrouhou, O., Alhakami, W. & Hamam, H. (2022). The Rise of "Internet of Things": Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks. *Wireless Communications and Mobile Computing.* 2022(1), 8669348. doi:10.1155/2022/8669348.

Shah, V. (2021). Machine learning algorithms for cybersecurity: Detecting and preventing threats. *Revista Espanola de Documentacion Cientifica.* 15(4), 42-66.

Shah, V. (2021). Machine learning algorithms for cybersecurity: Detecting and preventing threats. *Revista Espanola de Documentacion Cientifica.* 15(4), 42-66.

Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z. & Doss, A.R. (2022). Zero Trust Architecture (ZTA): A comprehensive survey. *IEEE Access.* 10, 57143-57179.

Trilles, S., Hammad, S. S. & Iskandaryan, D. (2024). Anomaly Detection Based on Artificial Intelligence of Things: A Systematic Literature Mapping. *Internet of Things.* 25, 101063. doi:10.1016/j.iot.2024.101063.

Wang, H., Zhang, W., He, H., Liu, P., Luo, D. X., Liu, Y., Jiang, J., Li, Y., Zhang, X., Liu, W., Zhang, R. & Lan, X. (2021). An Evolutionary Study of IoT Malware. *IEEE Internet of Things Journal.* 8(20), 15422-15440. doi:10.1109/JIOT.2021.3063840.