Chapter

Methods for Detection and Prevention of Vulnerabilities in the IoT (Internet of Things) Systems

Vesna Antoska Knights and Zoran Gacovski

Abstract

In this chapter, the problem of detection and prevention systems for Internet of Things attacks is discussed. We start with the term Internet of Things (IoT) that defines the use of intelligently connected devices and systems for data collection *via* embedded sensors and actuators in physical devices. IoT is omnipresent today and is expected to expand globally in the years ahead. This type of progress will provide services that improve the quality of human life and the productivity of enterprises, while creating the possibility for the so-called "Connected Life." The goal is to achieve protection against intruders who break into IoT systems to obtain certain sensitive data, gain control, or commit any kind of abuse. Reliability, integrity, and availability represent three different aspects in the field of security that should be achieved in systems such as the Internet of Things. In this work, we present three major areas that can help to mitigate the security risks in IoT systems. Also—two methods for intrusion detection are elaborated—signature-based and anomaly-based models. In the last section of this chapter, we present a real-world example that has already been implemented in reality (Intrusion detection system based on Snort at eggs/poultry farm).

Keywords: Internet of Things, vulnerabilities detection, prevention, threats, signature-based IDS, system security

1. Introduction

Internet of Things is a widespread, intelligent network composed of smart devices that enables the implementation of advanced services in housing, manufacturing, transport, health, and other sectors, as well as enabling a new ecosystem for application development. Examples of widespread IoT systems include the following:

- Fixed devices (home appliances, surveillance, smart meters, smart grid, street lamps).

- Mobile devices (in-car monitoring, transport/logistics, mobile robots, etc.).

- Personal devices (remote health monitoring, assisted living wristband, pharma sensors).

IoT devices share the sensor data they collect by connecting to an IoT gateway or other edge device—from where the data is sent to the cloud to be stored and analyzed. The data can also be analyzed locally on edge devices—in real time.

Today, with more connected "things" than the population of the Earth, the issue of IoT security is a major challenge [1]. More billions of IoT devices increases the threat and opens up the possibility of numerous attacks on the devices themselves. To address these security challenges, it is essential to explore frameworks like the 'Security Framework for Internet of Things proposed by El-Gendy and Azer [2]. Hacked devices cause disruption of connectivity and can also serve as a starting point for attacks on other devices and systems. The issue of confidentiality, availability, and integrity of data is greater than ever; therefore, it is necessary to ensure the functionality of CIA (Confidentiality, Integrity, Availability) through encryption and other protection methods.

Many authors have researched the appearing attacks and risks of the IoT devices:

- An attack on medical devices and equipment that the attacker has "locked" with a malicious program and demands a ransom (ransomware) [3]. One of the insecure medical devices that is in direct contact with patients and provides them with "life" is the cardiac electrostimulation (or "pacemaker"), with the associated programming device, due to the lack of passwords or any authentication.

- An attacker takes full control of the vehicle while driving [4]. Although the automotive industry invests a lot in product safety, research and testing have revealed vulnerabilities in numerous sensors that are present in newer cars—such as brake activation, vehicle steering, and other controls—for example,. in Tesla model S.

- The oil industry, as one of the critical infrastructures on which many other industries depend, uses numerous IoT sensors, devices, and applications in its business processes for the purpose of monitoring and control [5]. Unsafe IoT sensors and devices are present in the operation of the pipeline that connects the oil and gas fields and the refineries. Critical infrastructure is also at risk and is a frequent target of attacks.

Many IoT vulnerabilities could be mitigated with recognized security best practices, but too many products today do not include even basic security measures. There are many factors that contribute to this lack of security. It is unclear who is responsible for security decisions in a situation where one company designs the device, another supplies the component software, a third manages the network in which the device is embedded, and a fourth uses the device. This challenge is compounded by the lack of comprehensive, widely adopted international regulations—norms and standards for IoT security. Addressing the growing concerns about IoT security, it is vital to consider existing security protocols as highlighted in Maamar et al.'s comprehensive survey of Internet of Things security protocols [6]. Moreover, exploring recent surveys, such as the work by Alaba et al. [7], can provide valuable insights into the overall landscape of Internet of Things security.

Given the numerous incidents in the past few years that exploited IoT devices and ecosystems, countries have begun to recognize and be aware of the problem. In order for the IoT to function in a secure environment in the future, they started to formally standardize and legally regulate the Internet of Things and adhere to the best security practices.

However, advancements in robotics, such as the integration of anthropometric robots, offer potential solutions to enhance IoT security. For example, the use of mobile anthropometric robots with their ability to interact with the IoT infrastructure can improve security measures by enabling monitoring, threat detection, and response capabilities in IoT environments [8].

In addition to security protocols and surveys, it is essential to recognize the role of intrusion detection systems (IDS) in safeguarding IoT environments. Gupta et al. conducted a survey focused on intrusion detection systems in wireless sensor networks [9], shedding light on their significance in enhancing security in IoT ecosystems.

In our research, we have implemented and tested an intrusion detection system (IDS) at an egg/poultry farm Vezeshari. Our IDS was based on Snort—open-source signature-based intrusion detection system. We have set up the system rules to detect four types of IoT attacks: dynamic login attempts, XML injection attacks, SQL injection attacks, and Firmware (command) injection attacks. All of these attacks utilized code injections that target the wireless layer of the IoT system. The wireless frames from different Wi-Fi components of the IoT system are prone to these attacks, so we tested injection attacks at these points. To test our IDS, we invited ethical hackers from multiple countries that conducted orchestrated attack attempts. In most of the cases (over 80%), our IDS was able to detect and alert on the attack attempts—and the results are presented in Section 5. Our IDS is signature-based and to overcome its limitations, we plan to follow Tacker's et al. approach [10] that implements an anomaly-based IDS based on machine learning, and it will be our future research.

This chapter is organized as follows: in Section 2, we elaborate on the vulnerability risks of IoT systems; in Section 3, we present risk prevention and management for the IoT systems; in Section 4, we explain the usage of intrusion detection and prevention systems (IDS/IPS). In Section 5, a real-world use case (Vezeshari's IDS) is presented with methodology and key results, and then in Section 6, we give final conclusions.

2. Vulnerability risks for IoT systems

Anything that can disrupt the operation, integrity, and availability of an IoT device, or network of IoT devices is a threat. There are different types of threats. There are natural threats, such as floods, earthquakes, or storms. There are unintentional threats that result from accidents or mistakes. Finally, there are deliberate threats that result from ulterior motives. Each of these types of threats can be fatal to the IoT infrastructure.

The IoT risks are divided into four categories (**Figure 1**).

- Base risk—the possibility of device breach (data loss, physical harm, integrity risk).
- Harm to other stakeholders—including those not previously anticipated.
- Risk for future misuse cases.
- Future aggregation risks—network effect on other connected devices.

Therefore, the general security requirements for IoT systems (**Figure 2**) must include the following:

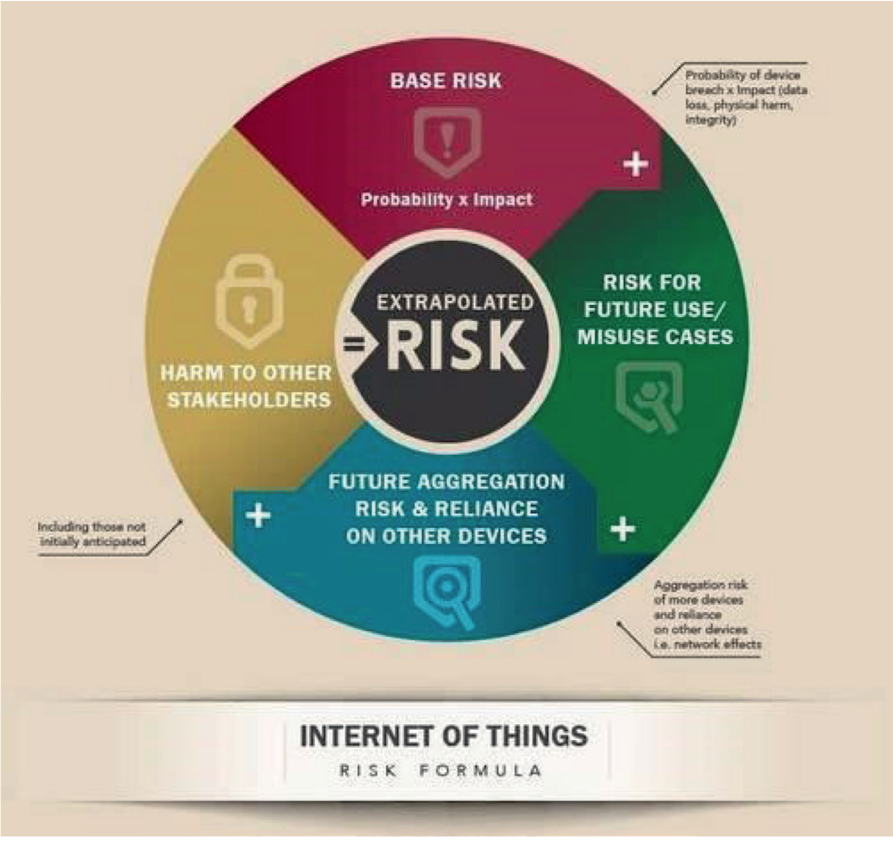

BASE RISK
Probability x Impact
Probability of device breach x Impact (data loss, physical harm, integrity)
+
RISK FOR FUTURE USE/ MISUSE CASES
EXTRAPOLATED
=RISK
HARM TO OTHER STAKEHOLDERS
Including those not initially anticipated
+
FUTURE AGGREGATION RISK & RELIANCE ON OTHER DEVICES
+
Aggregation risk of more devices and reliance on other devices i.e. network effects
INTERNET OF THINGS
RISK FORMULA

Figure 1.
IoT risks.

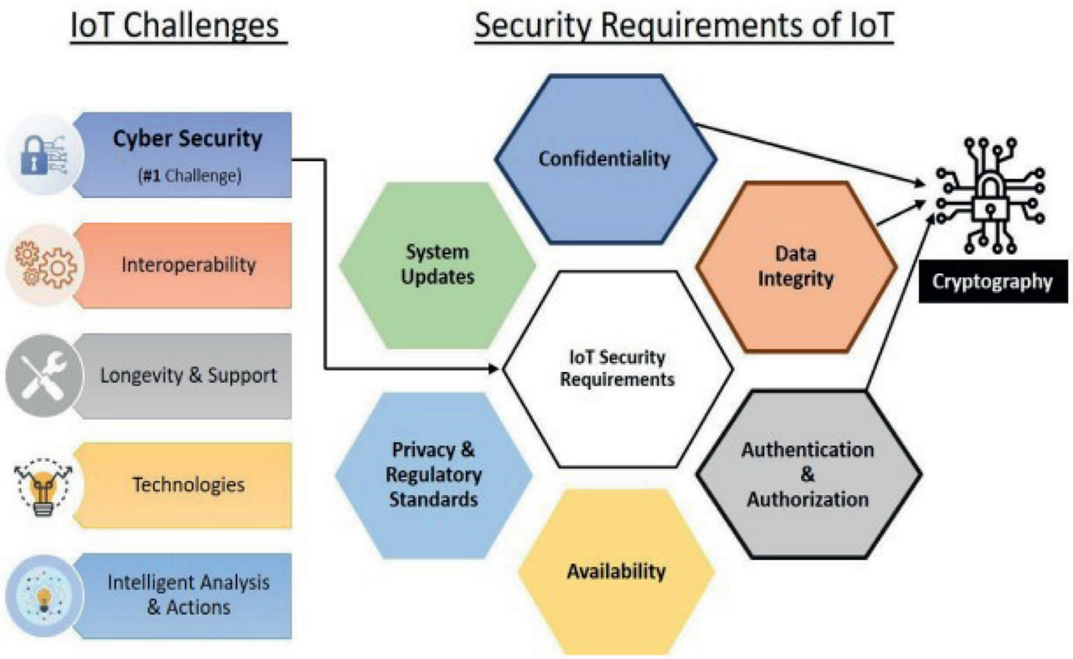


Figure 2.
IoT security challenges and requirements.

- Availability—the assurance that the services and resources (IoT devices) will be available and usable when requested by the user.

- Authentication—only authorized users have access to devices and services based on the following controls: authorization (granting and revoking of access rights), delegation (transfer of part of the rights of one entity to another), and authentication of users (identity check).

- Confidentiality—protects the existence of the connection, the flow of traffic, and the content of the information from disclosure to unauthorized users [11].

- Restoration—assurance that information and IoT devices will survive an attack and that availability can continue after the attack.

IoT vulnerability is an integral weakness of the design, configuration, or implementation of the IoT system that weakens protection. Most vulnerabilities can be found in one of these sources:

- *Bad design*: Hardware and software systems that contain design holes that can be misused. Basically, IoT systems are created with security holes. An example of this is the malware mail attack that leads to gaining access to IoT devices. These vulnerabilities (holes) can occur in any environment—Windows, Linux, Android, which may be resolved with a service pack, etc.

- *Poor implementation*: IoT systems that are incorrectly configured are susceptible to attack. This type of vulnerability usually results from inexperience, insufficient training, or irresponsible work. An example of this type of vulnerability would be a system that has no privileges for restricted access to critical devices and thus allows access to the devices.

- *Poor management*: Inadequate procedures and insufficient checks. Security measures cannot operate in a vacuum; they must be documented and monitored. Even the simplest things like daily system backup must be verified. There is a need to allocate responsibility for IoT devices and share responsibility for others. For this issue, the IoT provider should ensure that procedures are followed and that no person has total control over the system.

Although there are only three types of vulnerabilities, they can manifest in many ways. The first security rule is the physical protection of devices and networks. Central hosts and servers should be stored in separate rooms that can only be accessed by authorized personnel (owners). Routers, communications equipment, and portable media (disks, smartcards) should also be stored in secure locations with limited access. As part of this process, individuals and companies must consider the physical and natural environment in which IoT operates. The possibility of earthquakes, fires, floods, and other unforeseen accidents should be considered and properly planned. Accordingly, owners must ensure the security of all media (disks, tapes, smartcards) that contain vital information and make regular data backups.

Communication is the transmission of information through a medium. As such, it is inevitably vulnerable to interception, monitoring, burglary, etc. Owners should also take care of other forms of communication interception (Wi-Fi, antennas, etc.). Network and packet eavesdroppers are common tools that can read network flow.

It is important to note that every network and IoT system has vulnerabilities. Human mistakes, carelessness, laziness, greed, and rage pose the greatest threat to infrastructure with possible high damage. Moreover, human vulnerability and the risks associated with them are the most difficult to defend.

3. Risk prevention and management for the IoT systems

The IoT risk sources can be classified into four categories, as displayed in the following table (**Table 1**).

IoT risks can be treated (mitigated) *via*:

- Avoidance—means avoiding the risk by eliminating the risky process or resources by modifying the process.

- Mitigation—means mitigating risk by implementing measures to reduce risk, for example by improving existing security measures and controls.

Domain	Risk source
Sensor layer	• Physical characteristics—small dimensions require even smaller components with limited (security) capabilities. • Device price—cheaper device price means cheap components without security features embedded. • Power consumption—the long interval of usage requires energy-efficient components that do not possess security capabilities. • Wireless communication—this enables interception of the signal, and if the data is not encrypted, it is subject to intrusion, theft, and misuse. • Heterogeneity—a lot of different standards makes it difficult to provide good security.
Access layer	• Wireless technology—wireless data transmission opens up the possibility of unauthorized interception and analysis of traffic. • Traffic convergence between multiple devices/users in one node—connection of a large number of devices in one point (switch/hub) can be misused in a large number of attacks (traffic eavesdropping, MitM, DoS, etc.)
Network layer	• Traffic routing—OSPF, BGP, and other traffic routing algorithms have flaws that can be exploited to compromise security. • Public routers—they can be subject to attacks like DDoS.
Application layer	• A large number of penetrations—one cloud server manages the data of a large number of private and business users, which raises the issue of data segmentation, privacy, confidentiality, and the like. • Immature technology—the rapid development of services based on cloud computing raises the level of risk due to the insufficient research on security flaws and protection methods. • Enrolling many users in one physical server—identified security flaws in virtualization, the exploitation of which can cause harm to a large number of users at the same time.

Table 1.
IoT risk sources.

- Transfer—means the transfer of the consequences of the harmful effect of the risk to other natural or legal persons. For example, by purchasing an insurance policy against a harmful event or by agreeing on the compensation that the service provider would be obliged to pay for certain harmful events in the case of outsourcing the process.

- Acceptance—implies acceptance of the potential consequences of the harmful effect of the risk. The organization is aware of the risk, but the conclusion is that the costs of procurement and annual maintenance of the security system are greater than the potential lost income and losses caused by a damaged reputation, and it has decided to accept the risk without implementing additional measures.

The best practices for IoT security are defined by the IEEE—the world's largest professional organization for technology advancement. In February 2017,—IEEE issued the document "Internet of Things (IoT) Security Best Practices" [12]. The document is divided into three areas, with recommendations for each area:

- Device protection with prescribed measures and recommendations:
    - Make the hardware resistant to unauthorized use.
    - Provide regular firmware updates and upgrades.
    - Conduct dynamic testing.
    - Prescribe procedures for data protection on device disposal.
- Network protection with the following recommendations:
    - Use strong authentication.
    - Use strong encryption and security protocols [13].
    - Minimize device throughput.
    - Segment the network.
- Protection of the entire IoT system with the following recommendations:
    - Protect sensitive data.
    - Promote and conduct ethical hacking.
    - Standardization of devices and certification of personnel and organizations.

The conclusion is that the mentioned recommendations and measures should be used by manufacturers who produce IoT devices, by programmers and engineers who come up with the design of devices and systems, by researchers and testers to evaluate IoT systems, and by legislators when creating security and other acts that cover the IoT area.

4. Intrusion, detection, and prevention systems

The main goal of the intrusion detection and prevention system is to prevent situations that are not categorized as normal, but as suspicious (caused by the misuse of information), and to detect attacks and achieve security when such modes occur [14–16]. It also includes documentation of existing threats and serves as a controller of the IoT system security design. Intrusion Detection System (IDS) provides attack information, advanced diagnosis, systems recovery, and various investigations that allow ongoing events to be performed, including stopping the attack, terminating the network connection or user session, blocking the availability of the attack target, and changing the appropriate security.

The IDS [16], upon detection of an intrusion into the IoT system, raises an audio or video alarm, or sends a warning in the form of an e-mail message or text message to a smartphone. An improvement of this technology is the System (IPS), which can detect an intrusion and, furthermore, prevent that intrusion from Intrusion Prevention being successful through an appropriate active response.

The components of the IDS include (**Figure 3**) the following:

- Sensor (agent)—the agent is the module that collects event data and analyzes system activities. In the case of using an IDS, the agent is called a "sensor".

- Management server—it is responsible for analyzing information received from ongoing activities and deciding whether there is an attack in progress. This server also uses information from other elements, e.g. signatures and profiles, to complete the analysis.

- Management interface (console)—serves as an interface between the IDS and the administrator. The console is used to monitor system events received by the IDS. Some consoles are also used to configure agents and perform software upgrades.

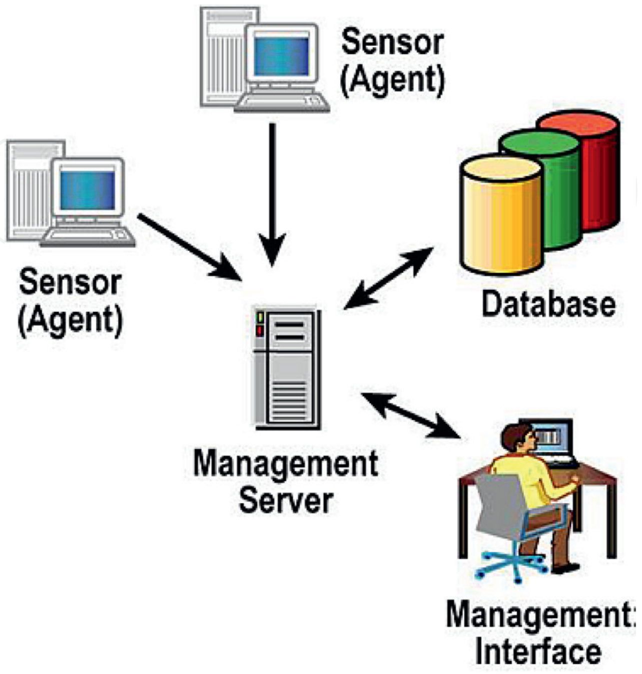


Figure 3.
Components of the IDS system.

- Database—the database server is used to store the information received from the agents and the management server. The management server also uses the database server to complete the analysis.

There are two major methods for intrusion detection—a signature-based model and an anomaly-based detection model.

Signature-based detection model—this method works by comparing current events with certain known signatures. Below are some examples of signatures:

- An attempt to log into the system as an administrator (root), which violates the system's security policy.

- Email messages with the subject "Free Screensavers" and containing an attachment in the message "screensaver.exe", which refers to spam messages.

- The operational system log for entering the system with code 645, which refers to the server is disabled and should be audited.

This type of IDS/IPS is very effective due to its low complexity in the implementation and detection process. It simply compares the current activity with the stored signatures to find any pattern in order to detect the attack. In addition, this model produces very specific attack reports compared to the anomaly-based model that is described below. A disadvantage of the signature-based detection and prevention model is its inability to detect new unknown attacks because the system has no signatures to enter the system for new attacks.

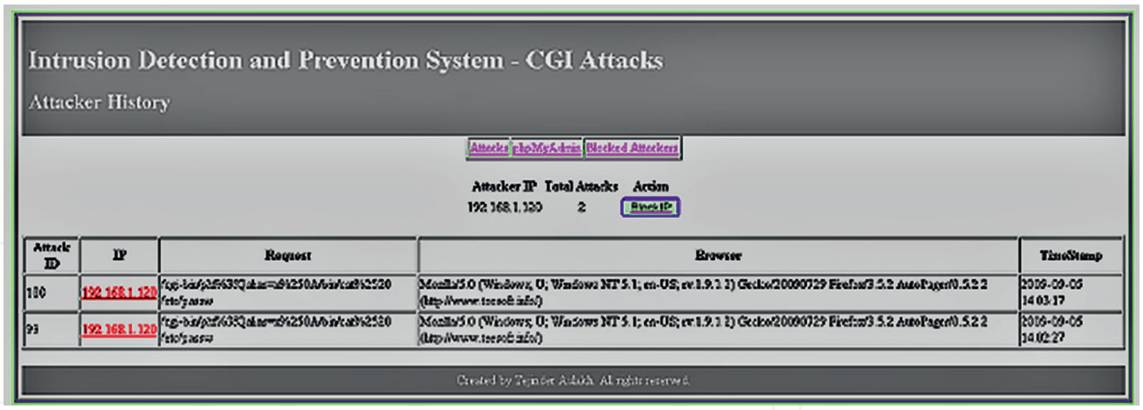
Anomaly-based detection model—this model detects attacks based on profiles. Profiles contain the pattern or normal behavior mode in which the system is used. Profiles are derived based on specific users, networks, or applications. They are created by monitoring system usage over a period of time, known as the evaluation period (**Figure 4**). This model compares current activities with profiles in order to detect abnormal activity, which in most cases indicates a seizure.

Since system and network usage are not static and always contain some variation over time, the profile must also adjust accordingly over time. Therefore, after creating profiles during the evaluation period, the detection and prevention system changes the profiles over time. Below are examples of profiles:

- User profile contains 5% email activity. When the detection and prevention system using the anomaly-based model detects that the email activity in the system is more than 5%, it will consider it as an attack.

- Over the course of a few weeks, the average user opens, reads, and writes to the file system 2% of the time. When the detection and prevention system detects a sudden increase in file system activity, it will consider it an attack.

The advantage of the anomaly-based model is that it can detect even unknown attacks by comparing current abnormal events with events considered normal. Furthermore, this model can also be more efficient than a signature-based model, since there are a large number of signatures to compare when using the same model. On the other hand, the incidents detected by the anomaly-based model are not very specific and therefore require additional effort on the part of the administrator to determine the root point of the attack. In addition, this model is subject to the



Intrusion Detection and Prevention System - CGI Attacks

Attacker History

Attacker IP	Total Attacks	Action
192.168.1.120	2	Block IP

Attack ID	IP	Request	Browser	TimeStamp
100	192.168.1.120	/cgi-bin/phf%63Qalias=x%250A/bin/cat%2520/etc/passwd	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.2) Gecko/20090729 Firefox/3.5.2 AutoPager/0.5.2.2 (http://www.teesoft.info/)	2009-09-05 14:03:17
93	192.168.1.120	/cgi-bin/phf%63Qalias=x%250A/bin/cat%2520/etc/passwd	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.2) Gecko/20090729 Firefox/3.5.2 AutoPager/0.5.2.2 (http://www.teesoft.info/)	2009-09-05 14:02:27

Created by Tejinder Aulakh. All rights reserved.

Figure 4.
Attacks registered by an IDS/IPS.

so-called "slow attack". In this type of attack, the attacker first learns the threshold between normal and abnormal activity in the system. The attacker will then slowly attack the system to ensure that the activities during the attack do not reach a threshold that will result in the detection of the attack by the anomaly-based model.

5. Real-world use case: methodology and results

Vezeshari is a poultry and eggs farm from Zhelino, North Macedonia. They have chosen Xively (software by LogMeIn) for their needs and working processes, as well as their Xively IoT platform. By these, they can monitor the internal air temperature, air humidity, CO_2 amount, and water nutrient level, and also –get a history of security alerts (**Figure 5**). Security, scalability, and expertise are important deciding factors, and by choosing an IoT solution, Vezeshari can now handle the entire network of connections. They also have overview and support for different scenarios, while getting the best guidance and advice from professionals (Xively).

By getting secure, reliable, and fast access, Vezeshari maintenance team can now excel in other areas of the farm and overall business:

- Access to real-time data allows Vezeshari to quickly diagnose problems and take immediate action to resolve them. When working with livestock, real-time information on climate conditions is essential, as the environment needs to be optimal at all times.

- Vezeshari customers can gain insight into the current state of their farm to ensure the process is running smoothly. This reduces the total time the farmer needs to work on the farm.

- The developed Vezeshari analyzer provides better insight into how people use their products and how they would like the products to be used. This helps Vezeshari refine and optimize its products to meet all user needs.

- Through the mobile Connect App, farmers can set parameters for optimal growing conditions and receive notifications and alerts related to parameters in the farm. Trusted software provides a better customer experience and enables instant problem resolution.

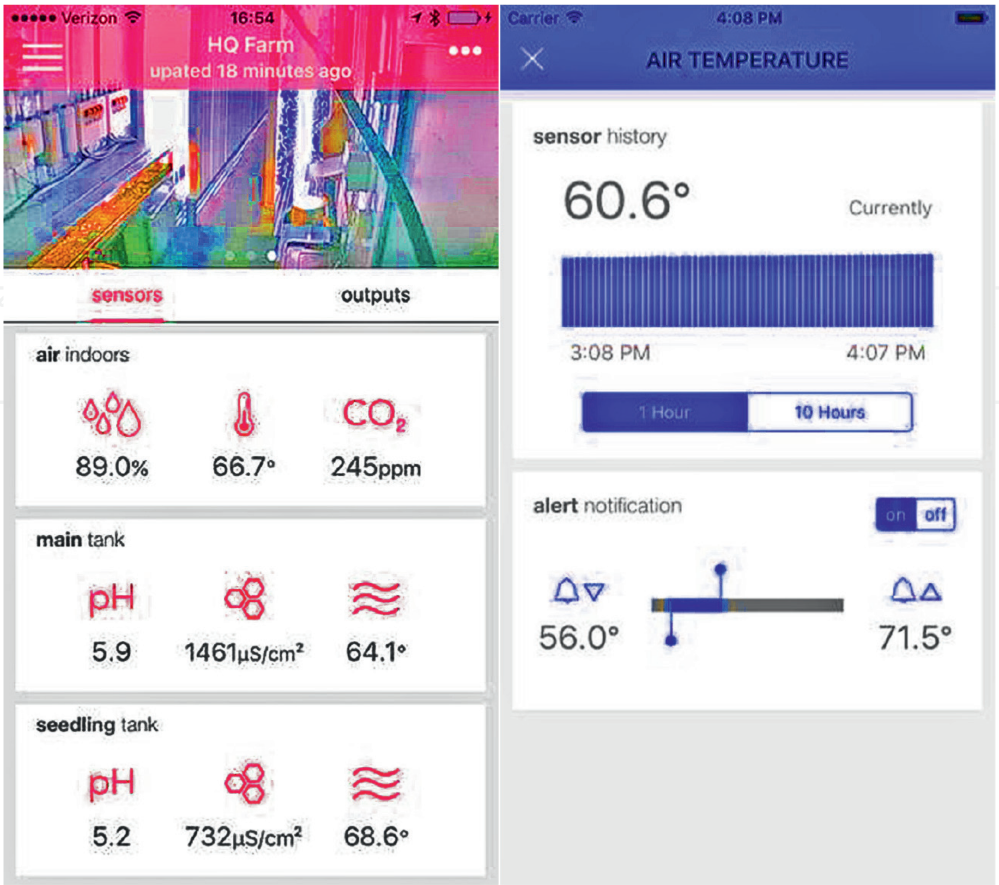


Figure 5.
Chicken farm application—allows monitoring of internal air temperature, air humidity, CO$_2$ amount, water nutrient level, as well as a history of alerts (presented graphically).

- Vezeshari employees have insight into day-to-day farm activities that gives them the ability to proactively meet customer needs, while also growing their business by selling consumables that are needed quickly based on farm usage.

Today, the entire Vezeshari working process is supported by state-of-the-art systems for detection and prevention of attacks that are updated and optimized daily. Thus, they achieve protection that is reliable even against the biggest threats and attacks in the system. Attack detection and prevention systems are composed of various antivirus and antispyware software, as well as the latest versions of firewalls for protection. Other methods using an increased level of security and data encryption, such as protection of the smartphone and tablet applications themselves through various types of generated passwords, are used in order to enable the detection and prevention systems to successfully recognize and prevent attacks in the systems.

To test the resilience of Vezeshari's network, we have implemented signature-based IDS (intrusion detection system). We used Snort—open-source signature-based IDS—and we have set up its rules to detect the following types of attacks:

- Dynamic login attempts.
- XML injection attacks.

- SQL injection attacks.

- Firmware (command) injection attacks.

To test our IDS, we invited ethical hackers from several countries (Hungary, Israel, France, USA, Netherlands) *via* forums and mailing lists (total of 56 participants). The attackers utilized code injections that targeted the wireless layer of the IoT system. The wireless frames from different Wi-Fi components of the IoT system are prone to these attacks—so we tested injection attacks at these points. To test our IDS, the ethical hackers conducted orchestrated attack attempts from multiple locations.

We've installed and configured Snort software in accordance with [17]. We opened the extracted folder *snortrules* then navigated to the *etc* folder and copied the snort. conf file then pasted it in *C:Snortetc* folder. Next we moved the folders so_rules, preproc_rules to the *C:Snort* directory path.

We entered and enabled the rules set before launching Snort, that is, we enabled ICMP rules so that Snort can detect any ping probes to the system while running. For example, a rule to detect a suspicious TCP intrusion (access rule) is in the form:

alert tcp any any -> any any (msg:"Suspicious User-Agent detected"; flow:to_server,established; content:"User-Agent|3a| "; nocase; content:"curl|2f|";nocase; sid:1000002; rev:1;)

The Snort software was operating in real time and results of the intrusion detection testing are presented in the following table (**Table 2**).

As we can see from the table, our IDS was able to successfully detect and alert on the attack attempts in most of the cases (over 80%). The most successful our system was for the firmware command injection attacks (95.3%), and the least successful in case of XML injection attacks. The rate of success varies for different attacks, because of the different capability to hide the harmful code within the legitimate IP packets. (The Snort rules can easily detect a harmful code within the firmware commands, rather than within XML code.)

The results indicate that our IDS for detection and prevention of attacks should be updated and optimized weekly, in order to achieve reliable and robust protection even against the most current threats and attacks, especially for this new IoT technology.

Of course our approach (usage of signature-based detection and Snort) has potential limitations, such as the following:

- Potential false positives (false negatives) reported by the IDS. If we applied the default Snort configuration, it would report a lot of false alarms.

- Interfaces that have overlapping IP addresses as matching criteria in Access rules might not be detected by Snort rules as intended.

Attack type	Signature	Total attempts	Detection/alert rate
Dynamic login attempts	20,790,001	348	311 (89%)
XML injection attacks	20,810,001	1250	1009 (80.7%)
SQL injection attacks	1,220,002	282	240 (85.1%)
Firmware (command) injection	1,310,001	455	434 (95.3%)

Table 2.
Detection rate of four different types of attacks.

- Services based on the payload of connections, such as network applications, URL categories, or URL list applications, can hardly be implemented as traffic Access rules for Snort inspection.

- Snort inspection is not supported for Virtual engines (WAN access).

To overcome these limitations we plan to extend our IDS by implementing an anomaly-based detection as the one elaborated in [10] by Tacker et al., and we are discussing this possibility in the last section of this paper (future work).

6. Conclusion and future work

The Internet of Things, which is also called the fourth industrial revolution, truly deserves that name. The tendency of IoT is to connect all disconnected devices. Today, life without the Internet of Things is unimaginable. Numerous devices from households, (air conditioners, lighting, video surveillance) to numerous devices in practically all industries (agriculture, healthcare, finance, energy, the automotive industry etc.), in order to improve the quality of life and increase economic growth, are interconnected, integrated and share data in real-time with the help of networks of all networks, the Internet.

But there is also a real danger that these devices will be exposed to cyber-attacks and that the confidentiality, integrity, and availability of data will come into question. IoT devices generate a large amount of data; therefore the question of the security of these devices and the entire IoT ecosystem arises, as well as the question of privacy.

Of course, as for everything else, it is necessary to carry out a risk assessment, from the identification of the resource, the vulnerability of the resource itself, possible threats that can exploit the vulnerability, and in the case of an attack, to determine the consequences that the attack could cause. The practice has shown the vulnerability of IoT devices due to several reasons, from the very physical characteristics of the devices, which are small in size, mostly untested for safety before use, low price, and low energy consumption. It is this sensor layer that is most at risk, in contrast to the access, network and application layers, where the risk is mostly assessed as low to medium.

Also, IoT technologies are not followed by legislation either, only in the last two to three years have societies recognized the problem and become aware of the risks and started the process of establishing a legislative and standardization framework that will regulate the IoT area.

The only way to stop attacks is to know the techniques used to attack. Therefore, organizations' security systems will need to adopt the most robust model or mechanism that provides the strongest protection against threats to ensure that the system remains secure. The attack detection and prevention system (IDS/IPS) ensures that attacks are detected and prevented using multiple approaches. Active attack detection and prevention systems aim to limit the damage that attackers can cause by building a local network that is resistant to the appropriate attack or threat.

In the last section of the paper, we presented a real-world use case (a poultry farm) that has acquired an IoT solution (Xively) and is now able to monitor the internal air temperature, air humidity, CO2 amount, water nutrient level, and get a history of security alerts that now can be controlled. At Vezeshari, we have implemented an open-source IDS in Snort to detect four types of IoT attacks: dynamic login attempts, XML injection attacks, SQL injection attacks, and Firmware (command) injection attacks. All of these attacks utilize code injections that target the wireless layer of the IoT system. The wireless frames from different Wi-Fi components of the IoT system are prone to these attacks so we tested injection attacks at these points.

To test our IDS we invited ethical hackers from multiple countries that conducted orchestrated attack attempts. In most of the cases (over 80%) our IDS was able to detect and alert on the attack attempts, and the results are presented in Section 5. The rate of success varies for different attacks, because of the different capabilities to hide the harmful code within the legitimate IP packets. Therefore, our system for detection and prevention of attacks should be updated and optimized weekly, to achieve reliable and robust protection even against the biggest threats and attacks in the system, especially in a new branch of technology such as the Internet of Things.

In future work, we plan to extend our IDS by implementing anomaly-based detection, i.e. by utilizing machine learning techniques. Anomaly-based IDS-s require larger processing resources, but they are superior in the detection of new, previously unknown threats. They are also adaptive and dynamic, as they can learn from the network behavior and update the baseline accordingly. There are eight methods for detecting traffic anomalies in real-time data, namely: projection-based methods, regression-based methods, support vector machines, decision tree–based methods, density-based methods, clustering, distance-based, and time series–based methods.

We plan to apply support vector machines [18] and decision trees [19]. Both of these machine learning methods are based on training the detector (IDS system), which will learn and be able to detect the real anomalies (intrusions). In the testing phase, a new data set will be used to develop the system's capacity to generalize to previously unseen intrusions. Support Vector Machine (SVM) method is a classification approach where support vectors form the boundaries of a class. In detecting anomalies, a single-class SVM will be used to define a normal class, and points that are outside the class boundaries can be defined as anomalies. Tree-based methods create a tree structure from data, where the tree will be updated with new data, but if new data causes significant changes in the tree structure, the model needs to be re-trained.

The field of IoT security is a contemporary and dynamic field of research. The broader significance of our research is that we implemented a cost-effective IDS in a real poultry farm. Our findings presented in this paper illustrate an IDS that is affordable and easy to implement in many small and medium businesses. We proved that the IoT system should not be put in function without providing its security. Our system is able to detect multiple threats, including DoS (denial of service) and malware (virus attacks). Our ultimate goal will be to develop an autonomous IDS and apply state-of-the-art techniques of machine learning and deep learning that can learn from the big IoT data. In addition, such future IoT IDS would have features such as self-configuration, self-optimization, self-protection, and self-healing.

Author details

Vesna Antoska Knights[1]* and Zoran Gacovski[2]

1 Faculty of Technology and Technical Science—Veles, University "St Kliment Ohridski"—Bitola, Bitola, Republic of North Macedonia

2 Faculty or Faculty of Technical Sciences, Mother Teresa University—Skopje, Skopje, Republic of North Macedonia

*Address all correspondence to: vesna.knights@uklo.edu.mk

References

[1] Ashoor AS, Gore S. Importance of intrusion detection system (IDS). International Journal of Scientific and Engineering Research. 2011;**2**(1):75-78. ISSN: 2229-5518

[2] El-Gendy S, Azer MA. Security framework for internet of things (IoT). In: 2020 15th International Conference on Computer Engineering and Systems (ICCES). Piscataway, USA: IEEE; 2020. pp. 1-6. DOI: 10.1109/ICCES51560.2020.9334589

[3] Newman LH. A new pacemaker hacks put malware directly on the device. 2018. Available from: https://www.wired.com/story/pacemaker-hack-malware-black-hat/

[4] Mahaffey K. Hacking a Tesla Model S: What we found and what we learned? 2015. Available from: https://blog.lookout.com/hacking-a-tesla

[5] Hanes D, Salgueiro G, Grossete P, Barton R, Hanes J. IoT Fundamentals: Networking, Technologies, Protocols and Use Cases for the Internet of Things. San Jose, USA: Cisco Press; 2017

[6] Maamar Z, Yahyaoui H, Mosbah M, Hemery J. Security for Internet of Things: A survey of existing protocols. In: Proceedings of the International Conference on Internet of Things and Big Data. New York, USA: ACM; 2018

[7] Alaba F, Othman M, Hashem IAT, Alotaibi F. Internet of things security: A survey. Journal of Network and Computer Applications. 2017;**88**:10-28

[8] Antoska V, Jovanović K, Petrović VM, Baščarević N, Stankovski M. Balance analysis of the Mobile Anthropomimetic robot under disturbances – ZMP approach. International Journal of Advanced Robotic Systems. 2013;**10**(4):1-10. DOI: 10.5772/56238

[9] Gupta BB, Nayyar A, Rautaray SS. A survey of intrusion detection systems in wireless sensor network. Journal of Network and Computer Applications. 2016;**60**:19-31

[10] Tucker J, Coughlan M, Nelson T, Klimkowski B. Implementing an anomaly-based intrusion detection system: Focus on internal threat – Masquerade attacks. American International Journal of Contemporary Research. 2016;**6**(4):1-11

[11] Abomhara M, Koien G. Security and privacy in the internet of things: Current status and open issues. In: PRISMS 2014 - International Conference on Privacy and Security in Mobile Systems (PRISMS 2014). Aalborg, Denmark, USA: IEEE; May 2014

[12] IEEE – Institute of Electrical and Electronics Engineers. Internet of Things (IoT) Security Best Practices. 2017. Available from: https://standards.ieee.org/wp-content/uploads/import/documents/other/whitepaper-internet-of-things-2017-dh-v1.pdf

[13] Thakor VA, Razzaque MA, Khandaker MRA. Light weight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. IEEE Access. 2021;**9**:28177-28193

[14] Bilgin D, Gacovski Z, Pivovarov V, Goracinova L. System for detection of network threats based on classifiers. TEM Journal. 2014;**3**(2):120-126

[15] Sandhu UA, Haider S, Naseer S, Ateeb OU. A survey of intrusion

detection & prevention techniques. In: International Conference on Information Communication and Management IPCSIT. Singapore: IACSIT Press; 2011

[16] Rudner M. Cyber-threats to critical national infrastructure: An intelligence challenge. International Journal of Intelligence Counter-Intelligence. 2013;**26**(3):453-481

[17] Wasielewski C, Sam Nivethan VJ. Securium Solutions – Snort Setup for IDS. Feb 2023. Available from: https://securiumsolutions.com/setting-up-snort-ids-basic-configuration/

[18] Chitrakar R, Chuanhe H. Anomaly detection using support vector machine classification with k-medoids clustering. In: 2012 Third Asian Himalayas International Conference on Internet. USA: IEEE; 2012. pp. 1-5. DOI: 10.1109/AHICI.2012.6408446

[19] Reif M, Goldstein M, Stahl A, Breuel TM. Anomaly detection by combining decision trees and parametric densities. In: 2008 19th International Conference on Pattern Recognition. USA: IEEE; 2008. pp. 1-4. DOI: 10.1109/ICPR.2008.4761796