B. Serdeniuk, Master student
N. Lobanchikova, PhD in Engr., As. Prof., research advisor
I. Bilyak, Lecturer, language advisor
Zhytomyr State Technological University

RESEARCH OF INFORMATION SECURITY PROCESSES IN IOT

In June 2018, the Juniper Research company in their IoT market research predicted doubling of the number of IoT devices by 2022. If analysts now estimate that the number of active IoT devices is 21 billion, then in four years their number will exceed 50 billion. Experts in the field of information security are worried about the progress of IoT-technologies. In their opinion the huge number of badly protected Internet devices gives new opportunities to cybercriminals who have already managed to break a number of IoT-systems.

The well-known cyber attack happened in October 2016 when a number of popular resources, services and social networks were found to be inaccessible: Amazon, Pinterest, Twitter, Soundcloud, Spotify, Reddit, GitHub, Starbucks, CNN, The New York Time, etc. Because of the attacks, the owners of the sites that run on the servers of the Dyn company suffered heavy losses. Today, it is known that the attackers used the Mirai programme, which can detect unprotected Internet devices such as routers, surveillance cameras, digital video recorders, etc. According to the Dyn, more than 100,000 unprotected connected devices were integrated into the botnet because they worked without password protection. The work of attacked sites was restored only after 14 hours.

The topicality of the problem is highlighted by incidents, capital losses of which are measured in billions of dollars. Industroyer, BrickerBot, Mirai - and this is just the visible tip of the iceberg.

The HP research data was not aimed at discovering certain dangerous internet devices and expose their developers, but to denfine the problems of IS-risks in the world of IoT as a whole, pay attention to problem both of device owners and problems which developers should solve. So, at the very beginning of the exploitation, a user must necessarily change the default factory password, because the factory passwords are the same on all devices and do not differ in reliability. Since not all devices have built-in IS protection, owners should also install external protection intended for home use so that their Internet devices do not become open gateways to the home network or direct harm tools.

In the course of the HP research, it was found that approximately 70% of the analyzed devices do not encrypt wireless traffic. Web interfaces of 60% of the devices are considered by HP experts as to have a defective access organization and a high risk of cross-site scripting. Most devices have passwords that are insecure. Approximately 90% of devices collect personal information about the owner without their knowledge.

In total, the HP specialists counted about 25 different vulnerabilities in each of the examined devices and their mobile and cloud components.

The HP experts’ conclusion is disappointing: there is no single IoT secure system today. A special danger for IoT is hidden in the context of the spread of targeted attacks. If hackers show interest to anyone, our helpers from the world of IoT will turn into traitors and give full access to the world of their owners.

Such weak points of IoT were distinguished:

- passing to IPv6;
- power supply of sensors;
- standardization of architecture and protocols, certification of devices;
- informational security;
- standard accounts from the manufacturer, weak authentication;
- lack of support from the manufacturer for the elimination of vulnerabilities;
- it is difficult or impossible to update the software and OS;
- use of text protocols and useless open ports;
- use the weakness of one gadget, hacker can easily get into the entire network;
- use of unprotected mobile technologies;
- use of unprotected cloud infrastructure;
- use of dangerous software.

Because the issue is extremely acute, tech-design companies, communications devices, network devices, software, and cyber-security companies are busy with the search of solution in information security for IoT devices. One of the leading security companies in IOT is Cisco Systems, which has played a leading role in developing the IOT model at the IoT World Forum (IWF), has developed the IoT security framework, which has become a useful addition to the reference model. Figure 1 illustrates the security environment from an IoT perspective.

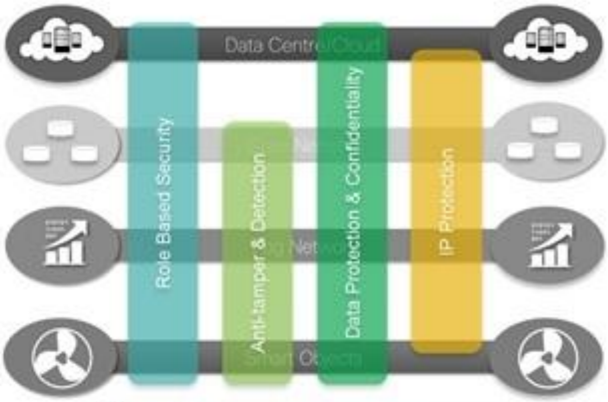

Figure 1 - Security environment from

The Cisco IoT model is a simplified version of the IoT model from the IWF. It consists of the following levels:

1. "Smart" objects and embedded systems: this part of IoT is most vulnerable.
2. Fog or peripheral network: this level includes wired and wireless connections of IoT devices. A key issue is the high variability of network technologies and protocols used by different IoT devices and the necessity to develop and implement a single security policy.
3. Core network: the core network provides paths for data transmission between platforms in the center of the network and IoT devices. Here the security problems are the same as in traditional networks. However, the huge number of end nodes with which the core interacts creates a significant security issue.
4. Data center and cloud services: this level includes platforms for applications, data storage and network management. IoT does not add any new security issues to this level, except for the need to deal with a huge number of individual end nodes.

With this four-level architecture, the Cisco model defines four general security solutions that cover several levels:

1. Role-based security: role-based access control systems assign role permissions rather than individual users. Users are given different roles, either statically or dynamically, according to their responsibilities.
2. Protection against interventions and detection of interventions: this solution is especially important at the devices level and the foggy network level, but also extends to the core network level. All these levels can use components that are physically located in the area of free access to them by anyone.
3. Data protection and confidentiality: this function covers all levels of architecture.
4. Protection of Internet protocols: data protection from listening and interception is important for all levels.

The Cisco document also proposes an IoT security concept that defines security features for IoT that covers all levels:

1. Authentication: this component covers the elements that initiate access, and primarily identifies IoT devices. Unlike typical corporate network devices, IoT end devices should be equipped with authentication methods that do not require human interaction. These methods include radio-frequency identification (RFID) tags, X.509 certificates or MAC addresses of end-users.
2. Authorization: authorization controls access to devices through the network. This element includes access control. Along with the level of authentication, it generates the necessary parameters to allow the exchange of information between devices and application platforms, thereby providing the work of IoT services
3. Network Enforced Policy: this layer encompasses all elements that route and transport endpoint traffic securely over the infrastructure, whether control, management or actual data traffic.
4. Secure Analytics: this component includes all the features necessary for centralized management of IoT devices. On the basis of visibility, there is the ability to control, including configuration, patches and updates, as well as countermeasures to terminate threats.
5. Visibility and Control: this secure analytics layer defines the services by which all elements (end nodes and network infrastructure, inclusive of data centers) may participate to provide telemetry for the purpose of gaining visibility and eventually controlling the IoT ecosystem. Further, it includes all elements that aggregate and correlate the information, including telemetry, to provide reconnaissance and threat detection. Threat mitigation could vary from automatically shutting down the attacker from accessing further resources to running specialized scripts to initiate proper remedy.

In the process of the research, a set of measures and tools for improving the safety of IoT is being developed. Many companies today have introduced their own information security models that they are constantly trying to standardize, correlate and implement. The research of technologies and security tools in IoT, the search for optimal security models at all levels: the hardware level, the software, the user level is the most important task today. The task with which the world's IT giants can not cope.