Detection of attacks on the Internet of Things based on intelligent analysis of devices functioning indicators

Tigran Ovasapyan
Dmitry Moskvin
Artem Tsvetkov
The number of IoT devices in the world is growing every year. This is also reflected in the growth in the number of attacks.

Growth in the number of malware samples for "smart" devices according to Kaspersky Lab data.
How IoT Networks Work

The modern concept of the Internet of Things implies an interconnected, interconnected network of devices, sensors, embedded systems, mobile devices, etc. that collect, process and exchange various kinds of information.

**IoT networks are used in the following areas:**
- transport;
- housing and communal services;
- medicine;
- safety;
- the quality of life;
- banking;
- agriculture / animal husbandry.

**Important features of IoT networks:**
- distribution of network;
- processing of confidential data;
- do not interact with a person directly;
- to fully investigate attacks, it is required to emulate devices.
## Comparative analysis of IoT platforms

<table>
<thead>
<tr>
<th></th>
<th>Contiki</th>
<th>Android Things</th>
<th>Riot</th>
<th>Apache Mynewt</th>
<th>Zephyr</th>
<th>TinyOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux kernel based</td>
<td>–</td>
<td>+</td>
<td>–</td>
<td>–</td>
<td>+</td>
<td>–</td>
</tr>
<tr>
<td>Support for multitasking and multithreading</td>
<td>+/-</td>
<td>+</td>
<td>+/-</td>
<td>+/-</td>
<td>+</td>
<td>–</td>
</tr>
<tr>
<td>Own development tools</td>
<td>–</td>
<td>+</td>
<td>–</td>
<td>+/-</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Centralized update capability</td>
<td>–</td>
<td>+/-</td>
<td>–</td>
<td>+/-</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Can be used for complex tasks</td>
<td>–</td>
<td>+</td>
<td>–</td>
<td>–</td>
<td>+</td>
<td>–</td>
</tr>
</tbody>
</table>
## Threats to IoT networks

<table>
<thead>
<tr>
<th>Physical</th>
<th>Network</th>
<th>Software</th>
<th>Cryptographic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interference with nodes</td>
<td>Traffic analysis</td>
<td>Viruses and worms</td>
<td>Side channel attacks</td>
</tr>
<tr>
<td>RFID radio attack</td>
<td>RFID spoofing</td>
<td>Spyware and adware</td>
<td>Cryptanalysis</td>
</tr>
<tr>
<td>Interfering with wireless sensor networks</td>
<td>RFID cloning</td>
<td>Trojan horses</td>
<td></td>
</tr>
<tr>
<td>Injection of malicious nodes</td>
<td>Unauthorized RFID Access</td>
<td>Malicious scripts</td>
<td></td>
</tr>
<tr>
<td>Physical Damage</td>
<td>Sinkhole attack</td>
<td></td>
<td>Man in the middle attack</td>
</tr>
<tr>
<td>Social engineering</td>
<td>Man in the middle attack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resource depletion attack</td>
<td>Denial of service attack</td>
<td>Denial of service attack</td>
<td></td>
</tr>
<tr>
<td>Injection of malicious code into a site</td>
<td>Attack on routing mechanisms</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sibyl Attack</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Basic methods of securing IoT devices

<table>
<thead>
<tr>
<th>Static</th>
<th>Dynamic</th>
</tr>
</thead>
<tbody>
<tr>
<td>– signature analysis</td>
<td>– profiling</td>
</tr>
<tr>
<td>– analysis of application components</td>
<td>– tracking abnormal behavior</td>
</tr>
<tr>
<td>– bytecode analysis</td>
<td>– analysis of virtual environment behavior</td>
</tr>
</tbody>
</table>

**Disadvantage:** when a new infection or attack method appears, the method may not respond to malware until it is detected and signatures for a specific vulnerability are generated

**Disadvantage:** the possibility of false positives, as well as the existing need for preliminary collection of data on the legitimate state of the system and further tuning of algorithms

**Solution for IoT devices:** Leverage dynamic analysis techniques from remote IoT device data
Android Things OS is built on Android mobile OS
You can use an Android mobile device emulator to test and experiment on various attacks

Routing attacks
Features:
- difficult to detect by standard methods
- can disable an entire network

Resource depletion attack
Features:
- difficult to detect by standard methods
- causes great harm to devices and users

Link Noise Attack
Features:
- allows you to disrupt the entire network on which the infected host is located
- allows you to turn your device into a bot
General scheme of implementation of the method for detecting attacks in IoT networks

- **Emulator**
- **Emulated device metrics data files**
- **"Raw" data that needs to be converted to a single format**
- **Combining all data in one table and normalizing indicators**
- **Data processing and preparation**
- **Using machine learning methods**

Implementation of attacks using software
Collecting device metrics data to implement a method for detecting attacks in IoT networks

An example of data obtained during the emulation of attacks:

For each attack emulation experiment, we managed to obtain the following data from the device:
- total processor load (in percent)
- total use of RAM
- the amount of RAM available in the system
- the amount of free RAM;
- cache

Received parameters for network interfaces:
- package send interface
- packet receiving interface
- Sending IP address
- port of dispatch
- Recipient IP address
- recipient port
- package size
Three algorithms were chosen as classifiers for building models and testing:

- k-Nearest Neighbors (k-NN)
- Support Vector Machine (SVM)
- Random Forest (RF)

During the training, the following parameters were selected:

- For kNN:
  number of neighbors k ranging from 2 to 20
- For SVM:
  regularization parameter C from the set \([10^{-5}, 10^4, \ldots, 10^5, 10^6}\]
- For RF:
  the number of trees n ranges from 2 to 100

**Sample size:** 69481 records
The data is shuffled and broken up in the ratio:

- 75% of data used for training
- 25% for tests
Testing models and comparing learning outcomes

Results of classification by the kNN method with the number of neighbors $k = 10$:

<table>
<thead>
<tr>
<th>Accuracy (%)</th>
<th>Recall (%)</th>
<th>Precision (%)</th>
<th>F-score (%)</th>
</tr>
</thead>
</table>

Results of classification by the SVM method with the linear kernel parameter $C = 10^{-2}$:

<table>
<thead>
<tr>
<th>Accuracy (%)</th>
<th>Recall (%)</th>
<th>Precision (%)</th>
<th>F-score (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>97.2366</td>
<td>97.2603</td>
<td>97.4790</td>
<td>97.2233</td>
</tr>
</tbody>
</table>

RF classification results with number of trees $n = 42$:

<table>
<thead>
<tr>
<th>Accuracy (%)</th>
<th>Recall (%)</th>
<th>Precision (%)</th>
<th>F-score (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>97.4093</td>
<td>97.5220</td>
<td>97.6611</td>
<td>97.4696</td>
</tr>
</tbody>
</table>
1. A study of the principles of functioning of networks of the Internet of Things and a comparative analysis of existing emulation platforms was carried out. A platform for software emulation was identified within the framework of the study.

2. Typical threats have been analyzed and actual attacks exposed to IoT networks have been identified.

3. Existing methods of detecting attacks on IoT devices are considered, their advantages and disadvantages are determined.

4. A method for detecting attacks on the Internet of Things networks using the analysis of device indicators has been developed and its effectiveness has been experimentally evaluated. The best result is achieved when using the k nearest neighbors (kNN) algorithm with the parameter $k = 10$. 