|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ITU Logo | INTERNATIONAL TELECOMMUNICATION UNION  **TELECOMMUNICATION STANDARDIZATION SECTOR**  STUDY PERIOD 2017-2020 | | FG-AI4H-D-015 | |
| **ITU-T Focus Group on AI for Health** | |
| **Original: English** | |
| **WG(s):** | | N/A | Shanghai, 02-05 April 2019 | |
| **DOCUMENT** | | | | |
| **Source:** | | China Academy of Information and Communications Technology (CAICT) | | |
| **Title:** | | AI-Based Mining and Testing Tool for Smart Health Device Vulnerability | | |
| **Purpose:** | | Discussion | | |
| **Contact:** | | Kai Fu CAICT China | | Tel: +86 18310871563 Email: fukai@caict.ac.cn |
| **Contact:** | | Ziyi Yang CAICT China | | Tel: +86 18611172600 Email: yangziyi@caict.ac.cn |
| **Contact:** | | Chunxia Hu CAICT China | | Tel: +86 13810685625 Email: huchunxia@caict.ac.cn |

|  |  |
| --- | --- |
| **Abstract:** | With the popularity of smart health devices, security issues such as data tampering and information leakage are becoming more and more serious. Currently, lacking mining and testing tools for vulnerability, which are directly applied to health device, making the situation worse. In order to deal with the situation, detecting and fixing the vulnerability in advance become more essential. Our research aim at using AI to establish a set of vulnerability mining and testing tools through three stages: firstly, establish device vulnerability libraries; secondly, build algorithmic models for specific device and protocols, then develop vulnerability mining and testing tools; thirdly, extend targeted models to general models to help with various kinds of health devices. |

**Overview**

Sharp increasing in health demand of aging population and worldwide medical resources shortage, provides a great market opportunity for the development of smart health equipment. The widespread use of smart health devices will generate a large amount of health data for more professional and effective analysis, further promoting the advancement of the health field. However, with the application of smart health equipment worldwide, its security issues have become increasingly prominent. At present, major organizations and enterprises pay close attention to applications and ignore security issues.

In addition, there are no effective means to discover and fix vulnerabilities, which may affect the widespread application of smart health devices. The development of AI, such as machine learning, provides the necessary conditions for solving the security problems of smart health devices. In this way, using AI to establish a set of vulnerability mining and testing tools can effectively solve the security problems of smart health device to promote its development worldwide.

# Impact

With the development of Internet health care, the safety of smart health devices has become increasingly prominent. Incidents of hacking and information disclosure of smart health devices have emerged in an endless stream. Relevant survey data show that about 10% of health devices are detected with hacking tools. There are two main problems caused by smart health device vulnerabilities.

**Firstly, tampering with device data using health device security vulnerabilities.** In 2017, White Scope Security Inc. found that four well-known vendors had security issues with their home security systems, implanted devices, pacemaker programmers, and patient support networks. The third-party libraries used by the four pacemaker programmers has more than 8,000 vulnerabilities. An attacker can use a pacemaker vulnerability to write and run code remotely, causing the heartbeat frequency to be modified or even stopped, threatening the patient's illness.

**Secondly, causing patient data to leak by smart health device security vulnerabilities.** The smart health devices have become a key entry point for attackers to invade medical networks. According to TrapX's research report, the number of attacks on more than 500 patient data has increased by nearly 50% from 2015 to 2016. The cyber attacker obtains the patient's medical record as well as personally identifiable information, then resell the information and get a financial return.

Although hospitals usually install firewalls and deploy anti-virus/anti-intrusion tools on the internal network, these protections cannot be directly applied to smart health devices. It is important and urgent to detect and fix vulnerabilities in advance to reduce the likelihood of smart health devices being attacked.

# Existing Work

Founded in 1957, the China Academy of Information and Communications Technology (hereinafter referred to as “CAICT”) is a scientific research institute directly under the Ministry of Industry and Information Technology (MIIT) of China. While sticking to the positioning of “a specialized think-tank for the government, and an innovation and development platform for the industry” and cherishing the cultural philosophy of “boosting prosperity with virtues and expertise” for years, CAICT provides strong support for the industry’s major strategies, plans, policies, standards, testing and certification, thus proving itself an important facilitator in the leapfrog development and innovation of China’s information and communications industry.

In recent years, with a view to adapting to the new eco-social backdrop and requirements and under the new national strategy of building China into a “strong cyber and manufacturing power”, CAICT has strengthened its efforts in making innovations to achieve wider and deeper research landscape while reinforcing its advantages in telecommunication and Internet. In-depth study and foresighted planning have been conducted in the fields of 4G/5G, industrial Internet, smart manufacturing, mobile Internet, Internet of Things (IoT), Internet of Vehicles (IoV), cloud computing, big data, blockchain, artificial intelligence, future network, virtual reality/augmented reality (VR/AR), intelligent hardware, and cyber and information security. CAICT has played an important role in research on strategies and policies related to the integration between industrialization and ICT and IT application, technological innovation, industrial development, and security assurance, which have strongly supported the strategy and policy making, such as Internet+, China Manufacturing 2025 and Broadband China, as well as the implementation of key tasks concerning various sectors.

# Feasibility

Based on the disclosed embedded device vulnerabilities and health device vulnerability information, this project uses AI to analyse the causes of vulnerabilities, summarize the characteristics of vulnerabilities, establish a health device vulnerability mining algorithm model, and develop a corresponding vulnerability mining and testing tool. It is used for smart health device vulnerability mining and testing to better reduce the risk of attack in the health industry. For example, based on existing embedded device vulnerability information, establishing a vulnerability mining algorithm model for cardiac pacemakers, and developing corresponding tools to effectively evaluate the safety of existing pacemakers. It is of great feasibility to have great contribution to the development, testing and safety of pacemakers

# Data Availability

Our lab has around 2,000 network device vulnerabilities, including remote command execution, denial of service, and authentication bypass. In addition, we can also obtain device vulnerability information from CVE, NVD, CNVD, CNNVD and other public vulnerability libraries.

The designed algorithm summarizes the existing vulnerability information and extracts the vulnerability characteristics. In this way, we can mine the vulnerability of smart health devices and verify the effectiveness of the algorithm by the vulnerability detection rate.

# Benchmarking

The benchmarking process is divided into three stages

* The first stage: Establish a “known vulnerability database” by collecting health device vulnerabilities, summarizing and extracting common features.
* The second stage: Establish an algorithmic model, focusing on specific devices and protocols, for targeted vulnerability mining and testing.
* The third stage: Expand the model to build a general mining algorithm model for various health devices’ vulnerability, as well as develop the corresponding tools.

There are three sub-phases in the last two stages:

* Phase 1: vulnerability information collection and model developing
* Phase 2: Expected verification and usage feedback
* Phase 3: Continuous improvement of models and tools

**Expected results are as follows:**

Establish a “known vulnerability database” of health devices; establish an algorithm model for specific devices and protocols; expand to build a general mining algorithm model for various health devices’ vulnerability, as well as develop corresponding tools.

# Organizer Details

Please describe why your organization is interested in this project, and if you have run similar projects / benchmarks / challenges before.

|  |  |
| --- | --- |
| **Organization Name** | China Academy of Information and Communications Technology |
| **Contact Name** | Kai Fu |
| **Contact Email Address** | fukai@caict.ac.cn |
| **Contact Phone Number** | +86 18310871563 |
| **Project Title** |  |