Privacy in the Internet of Things for Smart Healthcare

Daojing He, Ran Ye, Sammy Chan, Mohsen Guizani, and Yanping Xu

With the rapid development of wearable biosensors and wireless communication technologies, various smart healthcare systems are proposed to monitor the health of patients in real time. However, many security problems exist in these systems. After giving an overview of these security threats, the authors discuss the security vulnerabilities of password building and present a password strength evaluation method that takes into account users' personal information.

Abstract

With the rapid development of wearable biosensors and wireless communication technologies, various smart healthcare systems are proposed to monitor the health of patients in real time. However, many security problems exist in these systems. For example, a password guessing attack can compromise IoT devices, leading to invasion of health data privacy. After giving an overview of security threats of healthcare IoT, this article studies security vulnerabilities of password building and presents a password strength evaluation method that takes into account users' personal information.

Introduction

With the rapid development of wearable biosensors and wireless communication technologies, various smart healthcare systems such as wireless medical sensor networks (MSNs) are proposed to monitor the health of patients in real time [1]. In the smart healthcare environment, sensors are deployed in a variety of ways such as being installed at home, offices, and public facilities, or being attached to clothes or wearable accessories to sense the position, motion, and changes in vital signs of patients. The patients' health data are transferred to the medical database, which is shared and accessed by healthcare providers, researchers, government agencies, insurance companies, and patients. In this way, medical processes, such as clinical diagnosis and emergency medical response, will be developed, thereby greatly improving the efficiency of healthcare. This will revolutionize the healthcare services of family hospitals and medical institutions.

When transmitting and managing the data of the connected smart healthcare system, there are three main security problems:

1. The diversification of attackers: A smart healthcare system is often an important monitoring system, which attracts people from all sectors of society including attackers such as terrorists or even a malicious person who wants to retaliate.
2. The diversity of intrusion methods: A smart healthcare system often has a fixed topological form and data transmission mode, and relatively simple interaction requirements, but there are many kinds of sensor nodes. Thus, such a system may be attacked via various communication networks and field buses.
3. Specialization of attack methods: The attacks on the smart healthcare system in the past several years have occurred many times, and are specifically targeted for a certain feature or function of the system. This shows that these attacks have become more professional and devastating compared to traditional cyber-attacks [2–4].

This article focuses on security issues of the Internet of Things (IoT) for healthcare. It is structured as follows. The next section gives an overview of healthcare IoT and describes its security threats. Then security vulnerabilities of password building for identity authentication, password guessing attacks based on social engineering, and an overview of password strength evaluation methods are presented. Our proposed password strength meter based on users' personal information is presented. Subsequently, some future research directions are provided. Finally, we conclude this article.

Overview and Security Threat of the Smart Healthcare System

Overview of the Smart Healthcare System

There are many ways to deploy a smart healthcare system. In real-life applications, the deployment option depends on the particular requirements or conditions in practice, such as sensor network topology (local or remote), the number of potential users (one or more), and the available resources (high-performance PCs or small mobile devices). The smart healthcare system is often based on the client-server architecture. As shown in Fig. 1, the healthcare data acquisition unit deployed in the natural environment is referred to as the client, which is used to collect the healthcare data. Also, the data center deployed in the cloud is referred to as the server, which is used to store the data from the healthcare data acquisition units. The healthcare data are transmitted to the server from the clients through secure links [5].

The healthcare data acquisition unit comprises healthcare data sources and a field control unit. The healthcare data sources include, but are not limited to, the sensor nodes, which are used to collect healthcare data, such as blood pressure,

Digital Object Identifier:
10.1109/MCOM.2018.1700809

Daojing He and Ran Ye are with East China Normal University; Sammy Chan is with City University of Hong Kong; Mohsen Guizani is with the University of Idaho; Yanping Xu is with Hangzhou Dianzi University.

0163-6804/18/$25.00 © 2018 IEEE

heart rate, blood sugar, pulse rate, brain activity, temperature, and humidity. Analyzing the output data of such sensors allows the estimation of specific types of motion that the device undergoes such as translation, tilt, shake, rotation, and swing. These nodes are designed to be extensively mobile and operate in environments that may have limited computing infrastructure support. A field control unit can control and manage a plurality of healthcare data sources, integrate healthcare data, and make unified format conversion and preliminary data analysis according to the predefined format of the aggregate data. The way in which the healthcare data source transfers data to the field control unit includes wired and wireless modes. The wired mode refers to data transmission through the bus based on commonly used protocols such as controller area network (CAN) or highway addressable remote transducer (HART), while in wireless mode, data is transmitted through wireless sensor network technologies, such as Zigbee. After that, the field control unit is connected to the Internet by wired or wireless means (e.g., Bluetooth, WiFi, Zigbee, mobile communication network, or WiMAX), and the healthcare data is forwarded to the cloud data center.

The main functions of the cloud data center are data storage, data management, and data security protection. Data storage mainly includes video data storage, image data storage, structured data storage, semi-structured data storage, and so on. Data management mainly implements data index, data fusion, data analysis, data display, and so on. Data security protection is mainly for sensitive data encryption, sensitive data isolation, access control, rights management, backup recovery, audit logs, and so on.

The architecture shown in Fig. 1 presents the integration of cloud computing and IoT for healthcare. This integration is expected to significantly improve healthcare services and provide a platform for continuous and systematic innovation. By facilitating effective cooperation among the different involved entities in the following way, it simplifies healthcare processes and enhances the quality of medical services. It collects patients' vital data and delivers the data to a cloud using IoT technologies. The cloud provides a flexible storage and processing infrastructure from which medical practitioners can make timely diagnoses based on both online and offline analyses of data [6].

Security Threats of Connected Smart Healthcare

Passive Attack: A passive attack is characterized by an adversary eavesdropping on a communication channel. In such an attack, the adversary does not attempt to break the system or alter the transmitted data (i.e., active attack). Instead, the adversary monitors the exchanged packets to gain information about the target (e.g., the users, the system, the communicating entities). Three examples of passive attack are side-channel attack, keylogging, and touchlogging [7, 8].

Active Attack: An active attack is characterized by an adversary attempting to intrude on the system. During an active attack, the adversary would inject false data into the system as well as potentially corrupt the data within the system.

Here, we consider a denial of service (DoS) attack as an example to illustrate active attacks.

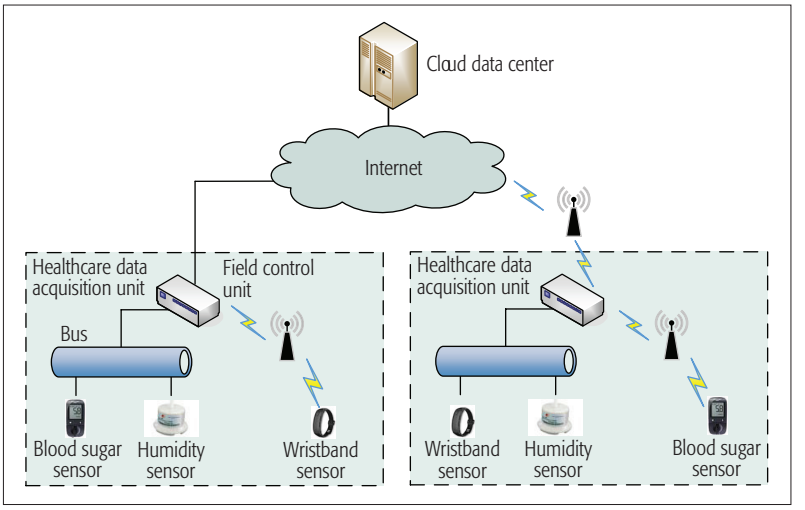

Figure 1. A typical structure of connected smart healthcare.

An adversary can compromise a device by password guessing and then use it to launch DoS attacks. For instance, *Mirai* is a brute force password guessing malware, exploiting the factory-default usernames/passwords such as root/admin, admin/admin, and root/123456 [9]. Recently, a DNS service provider was hit by a distributed DoS attack from millions of IoT devices that had been compromised with the Mirai botnet [9].

Password Security for Identity Authentication of a Healthcare System

Identity authentication is the basic means to protect information security of a healthcare system. As a text password is simple to use, low-cost, and easy to deploy, it has gradually become the most widely used authentication method to ensure the security of a healthcare system.

Security Vulnerabilities of Password Building

For convenience, a user password is hardly formed by random characters. Instead, it is usually relevant to the user's behavior of the intrinsic motivation and external environment. Therefore, users often choose weak passwords that are simple and easy to remember. As a result, such passwords can easily be attacked by violent crack and dictionary attacks. Moreover, because of the high intrinsic value of a password, it attracts adversaries to constantly study the preference in the process of password construction and then improve the password guessing algorithm. Currently, user password vulnerabilities are mainly concentrated in the following aspects.

Construct a Password with Preference: The analysis of a large number of leaked password datasets has demonstrated that a user prefers to choose words that are meaningful, or simply transform a word by satisfying the requirements of the password setting policy for the site. Most passwords are simply combinations of simple letters and numbers. Thus, they are highly susceptible to brute force and dictionary attacks.

Password Reuse: A user often has multiple network or service accounts. In order to facilitate the memory and management of these accounts, the user is often accustomed to choosing the same or similar passwords for different types of accounts.

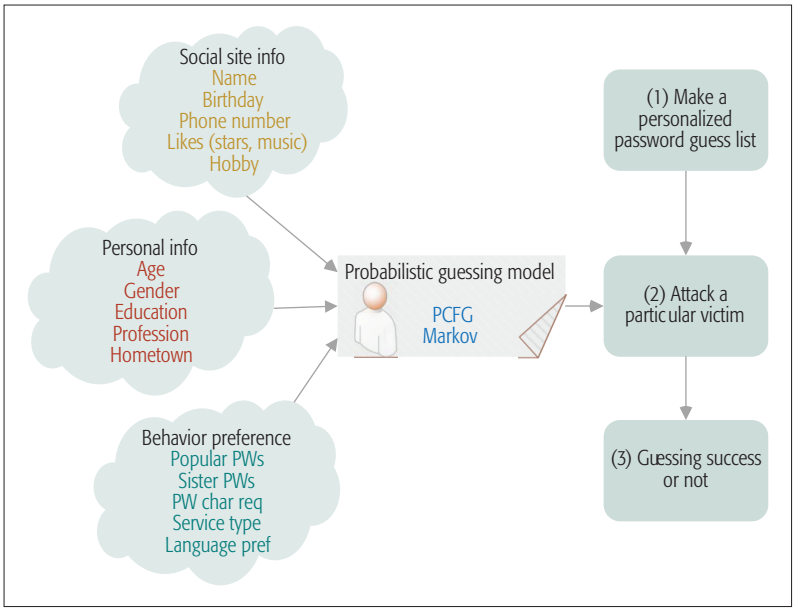

Figure 2. Password attack based on social engineering.

This approach not only provides an easy way for an adversary to break passwords, but also causes significant losses in his/her private health data.

Password Building Based on Personal Information: A user prefers to add personal information when building his/her passwords, such as his/her birthday, name, phone numbers, and identity IDs. This can help the user to memorize these passwords, but in the case of a password guessing attack, if this information is added, the success rate of password guessing can be significantly improved [10].

Password Attack Based on Social Engineering

As mentioned above, an adversary often uses social engineering methods to collect victims' relevant personal information, such as their names, birthdays, and hobbies, on social networking sites [11]. As shown in Fig. 2, subsequently, the adversary generates a target attack method with the mainstream probabilistic model, such as probabilistic context-free grammars (PCFG) and Markov chains (Markov), and it will greatly improve the success rate of guessing victims' passwords.

A number of password datasets have been exposed to the public in recent years, usually containing several thousands to millions of real passwords. As a result, there are several password measurement or password cracking studies based on analyzing those datasets. In this article, a dataset called 12306 is used to illustrate how personal information is involved in password building.

At the end of 2014, the dataset 12306 was leaked to the public anonymously. It is a dataset containing usernames/passwords from the official web site of the online railway ticket reservation system in China, www.12306.cn. Thus, it is named 12306. It is collected by trying usernames and passwords from other online leaked datasets, and has grown to more than 130,000 Chinese passwords. Compared to other leaked datasets available in the Internet, 12306 is considered to be of medium size. However, besides plaintext usernames/passwords, it also contains additional users' personal information, such as names and government-issued unique ID numbers.

After analyzing the passwords contained in 12306, we note that 28.3 percent of passwords involve birthdays, 25.7 percent involve account names, 20.5 percent involve names, 13.8 percent involve email addresses, 2.5 percent involve ID numbers, and 1.6 percent involve mobile phone numbers. This demonstrates that personal information is commonly involved in password creation.

Password Strength Evaluation

In order to provide timely feedback of the password strength results to the users, most information management systems use certain password strength meters (PSMs) to help users choose and improve the strength of passwords when they register for information services or modify the passwords [12]. At present, the PSM design of most information management systems such as mainstream web sites is based on heuristics. Their password strength measurements may be inconsistent or conflict with each other. This causes confusion, frustration, and misunderstanding in users. According to different underlying design ideas, these password strength evaluators can be divided into rule-based, pattern-based, and attack-based algorithms. Rule-based PSM methods are mainly based on the length and type of the contained characters. The typical representative is the National Institute of Standards and Technology PSM (NIST-PSM) [13], in which the computation does not involve any personal information. The main goal of the pattern-based PSM is to detect the construction patterns (e.g., keyboard order, first letter case, sequential character pattern) of each sub-segment of the password, and then assign the corresponding scores to the found patterns. The sum of the scores of all patterns gives the password intensity value. A typical representative of pattern-based PSM is Zxcvbn. PSM based on an attack algorithm determines the strength according to the degree of difficulty of attacking a given password using existing advanced password attack algorithms (e.g., the number of guesses and the time required for cracking). Typical representatives are PCFG-based PSM and Markov-based PSM.

As mentioned before, the analysis of the existing leaked password datasets reveals that users often build passwords based on personal preference (e.g., name, birthday, and other factors). If an adversary knows the users' behavior and then launches the password guessing attack based on the users' personal information, it will greatly increase the attack success rate. However, the existing password strength evaluators cannot provide an accurate evaluation result for this situation.

Our Proposed Password Strength Evaluation Method

Design

Here, we propose a PSM to overcome the shortcomings of the existing methods and to evaluate the strength of the password based on the personal identification information. The method includes the personal information classification

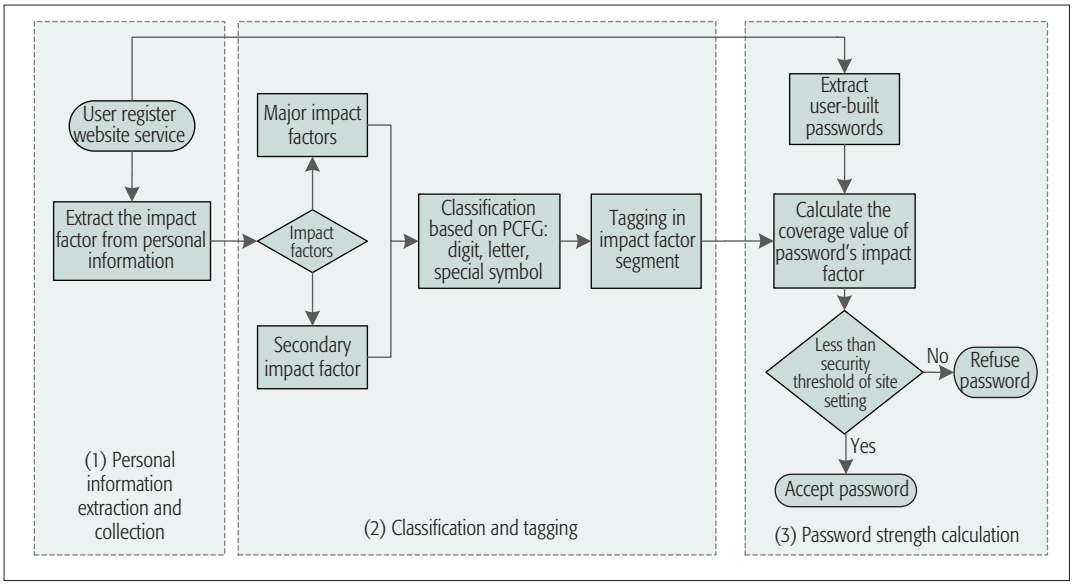

Figure 3. Proposed password strength evaluation method.

There are various personal identification items of users. Some of these personal information items can be used in the construction of the password directly, such as name or birthday; but some personal information is not used for password construction directly, such as gender and education level.

and label processing based on the context-free grammar, which can easily and accurately detect the personal information contained in the password and various forms of hidden variations. The personal identification information not only comes from the user's input, but also through the site crawler, cross-site information utilization, disclosed datasets, and other ways. It would provide strong defense against targeted password attack and also can be combined with the traditional rule-based and heuristic-based PSMs to help users choose a more secure password.

As shown in Fig. 3, our method based on personal information is divided into three stages:

- **Personal information collection stage:** When a user registers a website service, it extracts the impact factor fields from user-filled personal information that may be used to build the user's password.
- **Classification and tagging stage:** Classify the impact factor fields of the extracted password construction separately, and tag the impact factor field based on the user's common usage form in the building password process.
- **Password strength value calculation stage:** When a password is entered, it extracts the impact factor from the user information to calculate the coverage value of the impact factor in the user's password; then the coverage value can be combined with a heuristic detection method and a pattern detection method to calculate the password strength value. The maximum threshold value is chosen as a measure of the user's password strength.

The detailed description of each stage is provided as follows.

There are various personal identification items of users. Some are composed of letters, such as names and hobbies; some are composed of numbers, such as birthdays and mobile phone numbers; and some are composed of a combination of letters, numbers, and special characters such as usernames. Some of these personal information items can be used in the construction of the password directly, such as name or birthday; but some personal information is not used for password construction directly, such as gender and education level. In the personal information collection stage, the user's registration information could be analyzed and extracted with reference to leaked related datasets. To some extent, it can resist the guessing attack based on cross-station reuse.

In the classification and tagging stage, the extended PCFG algorithm [14] is used to classify the collected personal information into the letter segment *L*, the digit segment *D*, and the special character segment *S*. According to their influence degrees, the personal information is divided into the major influence factor and the secondary influence factor. For example, the user's name and birthday are the major influence factor in letter segment and digit segment, respectively. Through analyzing the changes of users' passwords in practice, we fully consider different variations in each field and representation by tagging.

For example, impact factor classification of a user's name "Li Lei" corresponds to the letter segment *L*, and the labels are *N*1–*N*6, where *N*1 represents the full spelling of the user's name (e.g., lilei or leili), *N*2 represents the user's initials (e.g., ll), *N*3 represents the user's surname, *N*4 represents the user's given name, *N*5 represents the combination of user's surname and initial of given name (e.g., lil), and *N*6 represents the combination of user's given name and initial of surname (e.g., llei or leil). The impact factor classification of the user's birthday (say, 1985.8.25) corresponds to the digit segment *D*, and the labels are *B*1–*B*10, where *B*1 represents the *Y.M.D* combined format of birthday (e.g., 19950825), *B*2 represents the *M.D.Y* combined format of birthday (e.g., 08251995), and *B*3 represents the *D.M.Y* combined format of the birthday (e.g., 25081995), *B*4 represents the day (*D*) portion of the birthday, *B*5 represents the month (*M*) portion of the birthday, and *B*6 represents the combined month and day (*M.D*) data of the birthday (e.g., 0825). *B*7 represents the combined year and month (*Y.M*) data of the birthday (e.g., 199508), and *B*8 represents the last two digits of the year in the birthday plus

Password	Markov	NIST	Our method
lilei1995	12.5	23.1	5.6
ll1995	11.8	17.1	5.8
lilei950825	20.3	39.6	8.7
lilei0825	13.7	20.8	7.4
llei95	9.5	15.9	3.4

Table 1. Comparison of different password strength meters.

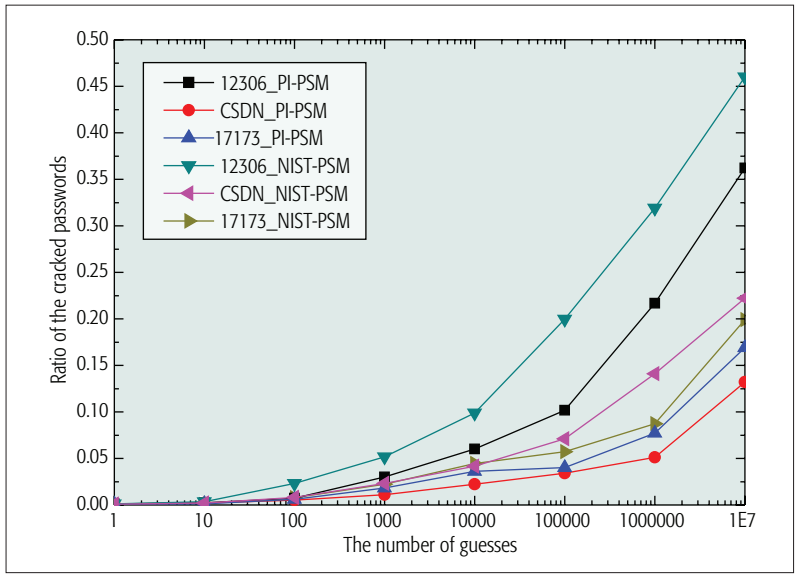

Figure 4. Ratio of cracked passwords for the PI-PSM and NIST-PSM methods.

the month and the day ($Y_{1/2}.M.D$, i.e., 950825). $B9$ represents the month and day of the birthday plus the last two digits of the year ($M.D.Y_{1/2}$, i.e., 082595). $B10$ represents the month and year of the birthday ($M.Y$, i.e., 081995). This classification method not only takes into account the length of each label value, but also varying forms of the influence factor.

In the password strength value calculation phase, we first consider detecting the actual variation of one of the impact factor label values in each field category. If any label value is detected, it continues to consider the impact factor's coverage length value based on the sliding window. As a result, the greater coverage value indicates that the greater impact factor of the personal information, the weaker the strength of the password.

The evaluation of the password strength can be a combination of the above personal information coverage value and other traditional heuristic methods based on the length, character composition, keyboard mode, and commonly used weak password tables.

Consider again the example user Li Lei, born on 1995.8.25, who has passwords such as lilei1995, ll1995, llei95, lilei950825, and lilei0825. Compared to traditional password strength meters, our method takes full account of personal information. As shown in Table 1, the existing evaluation tools such as Markov and NIST produce strength values that are much higher than our method. This clearly reflects the actual situation.

Experiment Evaluation

In order to verify the efficacy of our proposed password strength meter (named PI-PSM), we select three leaked real password datasets, and then adopt a method based on password guessing attacks, which simulates the password cracking process in real life, to compare the performance of PI-PSM and NIST-PSM. The selected leaked real password datasets arise from typical application scenarios, including an online booking website, a technical forum, and online game services. The datasets contain user's name, ID number, clear text password, mobile phone number, email, and other rich user information.

We first obtain the strength values of the passwords in each dataset. Then the passwords are sorted according to their strengths in decreasing order. The first 10,000 passwords are taken to form a test set. Thus, two test sets are obtained from each dataset. Subsequently, we used the Personal-PCFG target attack algorithm proposed by Li *et al.* [15] to carry out the password guessing for each test set. We recorded the proportion of the cracked passwords under a certain guessing number and plot the results in Fig. 4.

As can be seen in Fig. 4, the ratio of the cracked passwords for the test sets generated by PI-PSM are significantly less than the corresponding test sets generated by NIST-PSM. Thus, the set of password strength sequences calculated by PI-PSM is significantly better than that by NIST-PSM. In other words, it means that with regard to resisting the password guess attack, PI-PSM is better than NIST-PSM.

Also, from Fig. 4, it can be seen that the performance difference between PI-PSM and NIST-PSM for dataset 12306 is more significant than that of the two other datasets. This is because dataset 12306 contains more personal information, and thus the password strength evaluation is more accurate.

Future Directions

Social Engineering on Healthcare IoT

Security and privacy protection are certainly very important issues of IoT applications, particular healthcare IoT. This is because healthcare IoT tends to use location, personal, and context information of users in order to provide its services. This brings major security and privacy problems that require totally new solution approaches. The problems are further complicated when social engineering is involved. Generally, security threats can be categorized as either technical hacking or social engineering. An example is a malicious action based on the use of telephone numbers and names collected from websites. Social engineering is a dangerous form of security attack because it exploits the basic qualities of human nature such as trust. It is impossible to defend against by just using hardware or software.

The followings are some typical social engineering attacks on healthcare IoT:

1. Shoulder-surfing: A very simple technique where an adversary tries to monitor the physical activity of the victim or its device in close proximity. For example, the adversary could capture sensitive information such as a password by monitoring the screen and keyboard.

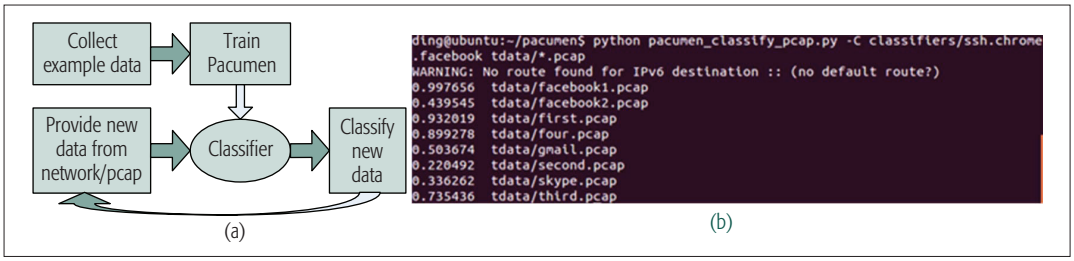

Figure 5. Architecture and test process of Pacumen: a) architecture of Pacumen; b) a glimpse of the test process.

2. Phishing: Commonly, this attack is associated with fake emails and websites. However, in healthcare IoT, it may include fake services. For example, when a device needs to connect to an access point, it might select the fake one that offers the best signal strength. Subsequently, when the device transmits data to the faked access point, the adversary could access the sensitive information contained in the data.

Today, researchers of IoT security are focusing their efforts on the technical side of information security, but there are only a few studies on the social engineering part of security and privacy protection. Thus, future work should focus on developing some efficient security mechanisms to prevent healthcare IoT from social engineering attacks.

Traffic Analysis on Encrypted Channels Based on Machine Learning

An effective way to ensure Internet security is employing SSH tunnel and Socks proxy jointly. With this combination, an encrypted tunnel can be created. All the data communicated is encrypted. In addition, the process of encryption and decryption can only be controlled and monitored by the user.

The SSH technique provides a function called dynamic forwarding. With this function, the SSH server can provide a Socks proxy service. Thus, the actual data transmission is carried out by the SSH server. The SSH protocol only permits the person who is able to link to the SSH server to send data. The user hence can keep its privacy and secrecy. For example, even its Internet service provider cannot identify which website or which web service it is using, as its web traffic is encrypted by the SSH protocol.

However, although data packets are encrypted and can only be decrypted by the SSH server, some useful information may still be extracted from the side information of encrypted packets such as the packet length and the inter-arrival time of a series of packets.

We refer to the act of extracting information from encrypted channels as *traffic analysis*. Specifically, it is possible to identify which website (e.g., Facebook, Linkedin) or which web service (e.g., Skype) a user is using. This means that even the use of encrypted tunnel to ensure privacy may be weak.

Pacumen is claimed to be the first open source software to identify encrypted channels using a machine learning approach. The details of this project can be found online at https://github.com/bniemczyk/pacumen. With this tool, we can make experiments to see if it is possible to identify the traffic under encrypted tunnels.

From the functional perspective of machine learning, Pacumen consists of five modules, as illustrated in Fig. 5a. As usual, we need to collect example data (i.e., historical data or so-called training data) to train a classifier. After that, new data from the network is fed into the classifier to produce results. The curve at the bottom means that the performance (i.e., accuracy) of the classifier can be optimized.

Pacumen provides several classifiers trained by a decision tree classification algorithm including websites like Gmail, Facebook, and Linkedin using either Chrome or Firefox, as well as web services like Skype. Figure 5b illustrates an example of the experiment. Here we attempt to see if the tested. pcap file contains behavior of surfing Facebook using Chrome. It shows that one of the two Facebook files is recognized with 99.7656 percent confidence and the other file only with 43.9545 percent confidence. On the other hand, some files without such behavior bring high confidence. This may be because the test data we prepared contains too much impurity, and the feature of those behaviors with high confidence may be similar to surfing Facebook in Chrome.

The above result illustrates that Pacumen does well in some scenarios. Thus, the attempt to use encrypted tunnel to protect security and privacy may not be reliable. A possible countermeasure is to improve the SSH protocol so that for data of any size, the lengths of encrypted packets are the same. However, this may sacrifice efficiency. Thus, future research work should consider how to balance the efficiency and security.

Conclusion

IoT devices in smart healthcare are attractive targets for cybercriminals as IoT devices often employ weak security measures, and their compromise can lead to privacy breaches and safety threats in the real world. In this article, we have focused on password guessing attacks. We have proposed a password strength meter that takes into account users' personal information. It helps users to select passwords with a higher degree of security.

An effective way to ensure Internet security is employing SSH tunnel and Socks proxy jointly. With this combination, an encrypted tunnel can be created. All the data communicated is encrypted. In addition, the process of encryption and decryption can only be controlled and monitored by the user.

Acknowledgment

This research is supported by the National Science Foundation of China (Grants 51477056 and U1636216), the National Key R&D Program of China (2017YFB0801701, 2017YFB0802805, and 2017YFB0802302), the Shanghai Rising-Star Program (No. 15QA1401700), a special project of the Shanghai Science and Technology Commission on Technical Standards (No. 16DZ0503000), a research grant from the Science and Technolo-

The attempt to use encrypted tunnel to protect security and privacy may not be reliable. A possible countermeasure is to improve the SSH protocol, so that for data of any size, the lengths of encrypted packets are the same. However, this may sacrifice efficiency. Thus, future research work should consider how to balance the efficiency and security.

gy on Communication Security Laboratory (No. 6142103030304), and the State Grid Corporation Science and Technology Project "The pilot application on network access security for patrol data captured by unmanned planes and robots and intelligent recognition based on big data platform" (Grant No. SGSDDK000KJJS1600065). This work is also supported by a strategic research grant from City University of Hong Kong (No. 7004615). Daojing He is the corresponding author of this article.

References

[1] R. Gravina *et al.*, "Multi-Sensor Fusion in Body Sensor Networks: State-of-the-Art and Research Challenges," *Information Fusion*, vol. 35, May 2017, pp. 68–80.
[2] H. Javdani and H. Kashanian, "Internet of Things in Medical Applications with A Service-Oriented and Security Approach: A Survey," *Health and Technology*, Feb. 2017, pp. 1–12.
[3] S. Moosavi *et al.*, "End-to-End Security Scheme for Mobility Enabled Healthcare Internet of Things," *Future Generation Computer Systems*, vol. 64, Nov. 2016, pp. 108–24.
[4] Z. Zhou *et al.*, "Energy-Efficient Event Determination in Underwater WSNs Leveraging Practical Data Prediction," *IEEE Trans. Industrial Informatics*, vol. 13, no. 3, June 2017, pp. 1238–48.
[5] A. Rahman, M. Daud, and M. Mohamad, "Securing Sensor to Cloud Ecosystem Using Internet of Things (IoT) Security Framework," *Proc. Int'l. Conf. Internet of Things and Cloud Computing*, no. 79, Cambridge, U.K., 22–23 Mar. 2016, pp. 1–5.
[6] A. Botta *et al.*, "Integration of Cloud Computing and Internet of Things: A Survey," *Future Generation Computer Systems*, vol. 56, Mar. 2016, pp. 684–700.
[7] H. Kim *et al.*, "STBC: Side Channel Attack Tolerant Balanced Circuit with Reduced Propagation Delay," *Proc. IEEE Computer Society Annual Symp. VLSI*, Bochum, Germany, 3–5 July 2017, pp. 74–79.
[8] H. Gross, S. Mangard, and T. Korak, "An Efficient Side-Channel Protected AES Implementation with Arbitrary Protection Order," *Proc. CT-RSA*, vol. 10159 of LNCS, Springer, Jan. 2017, pp. 95–112.
[9] M. Murphy, "The Internet of Things and the Threat It Poses to DNS," *Network Security*, vol. 2017, no. 7, July 2017, pp. 17–19.
[10] C. Castelluccia, M. Durmuth, and D. Perito, "Adaptive Password-Strength Meters from Markov Models," *Proc. 19th Annual Network & Distributed System Security Symp.* , San Diego, CA, 5–8 Feb. 2012, pp. 1–14.
[11] K. Krombholz *et al.*, "Advanced Social Engineering Attacks," *J. Info. Security and Applications*, vol. 22, June 2015, pp. 113–22.
[12] X. Carnavalet and M. Mannan, "A Large-Scale Evaluation of High-Impact Password Strength Meters," *ACM Trans. Info. Sys. Secur*, vol. 18, no. 1, June 2015, pp. 1–32.
[13] https://pages.nist.gov/800-63-3/, accessed Jan 5, 2018.
[14] M. Weir *et al.*, "Password Cracking Using Probabilistic Context-Free Grammars," *Proc. IEEE Symp. Security and Privacy*, Berkeley, CA, 17–20 May 2009, pp. 391–405,.
[15] Y. Li, H. Wang, and K. Sun, "A Study of Personal Information in Human-Chosen Passwords and Its Security Implications," *Proc. IEEE INFOCOM*, San Francisco, CA, 10–14 Apr. 2016, pp. 1242–54.

Biographies

Daojing He [S'07, M'13] (djhe@sei.ecnu.edu.cn) received his B.Eng.(2007) and M. Eng. (2009) degrees from Harbin Institute of Technology, China, and his Ph.D. degree (2012) from Zhejiang University, China, all in computer science. He is currently a professor in the School of Computer Science and Software Engineering, East China Normal University, P.R. China. He is on the Editorial Boards of eight international journals such as *IEEE Communications Magazine*.

Ran Ye is currently a Master's candidate in the School of Computer Science and Software Engineering, East China Normal University.

Sammy Chan [S'87, M'89] (eeschan@cityu.edu.hk) received his B.E. and M.Eng.Sc. degrees in electrical engineering from the University of Melbourne, Australia, in 1988 and 1990, respectively, and his Ph.D. degree in communication engineering from the Royal Melbourne Institute of Technology, Australia, in 1995. Since December 1994 he has been with the Department of Electronic Engineering, City University of Hong Kong, where he is currently an associate professor.

Mohsen Guizani [S'85, M'89, SM'99, F'09] (mguizani@ieee.org) received his B.S. (with distinction) and M.S. degrees in electrical engineering, and his M.S. and Ph.D. degrees in computer engineering from Syracuse University, New York, in 1984, 1986, 1987, and 1990, respectively. He is currently a professor and Chair of the Electrical and Computer Engineering Department at the University of Idaho. He is a Senior Member of ACM.

Yanping Xu (xuyanping@hdu.edu.cn) received her B.Eng. degree (2010) from Chongqing University of Posts and Telecommunications and M. Eng. (2013) and Ph.D. (2017) degrees in computer science from Beijing University of Posts and Telecommunications, China. She is currently a lecturer at Hangzhou Dianzi University.