Performance Evaluation of an Authentication Scheme for IoT Networks

Chi Ho Lau
Department of Electrical Engineering
City University of Hong Kong
Hong Kong SAR, PRC
email: chihlau-c@my.cityu.edu.hk

Sammy Chan
Department of Electrical Engineering
City University of Hong Kong
Hong Kong SAR, PRC
email: eeschan@cityu.edu.hk

***Abstract*—With the wide application of Internet of Things (IoT), the security of IoT systems has attracted significant research interest. In particular, since many devices can be connected to an IoT network, they face an authentication issue, which may be exploited by attackers to break into them. Recently, we have proposed an authentication scheme based on the blockchain technology to authenticate IoT devices before they can join an IoT network. In this paper, we develop a stochastic model to evaluate the efficacy of the authentication scheme. Numerical results indicate that the proposed scheme significantly increases the probability that a device stays in a healthy state.**

***Index Terms*—IoT, blockchain, authentication.**

I. INTRODUCTION

The Internet of Things (IoT) has brought tremendous improvement to our quality of life. Machines, devices, sensors can connect and communicate with each other via networks. Together with existing Internet standards, IoT devices, such as wireless cameras and innumerable sensors, provide services for information transfer, analytics, and applications [1].

The security of IoT has already attracted the attention of many researchers [2]. It is not a trivial issue that may only affect an individual household or company. For example, the pitfall of the IoT network may be exploited by the attackers to break into the smart city infrastructure [3]. Among all security concerns of IoT, the authentication of IoT devices is a well-known issue. Since many IoT devices are welcomed to join the network, how to make sure all of them are legitimate is an important issue. A straightforward solution is to scrutinize all IoT devices. One may suggest a system like a vehicle registration system or mobile phone registration system to keep a registry of the owners of these IoT devices. However, the number of IoT devices is far more than the number of vehicles or mobile phones. This solution may cost tremendous administration overhead and discourage users to use IoT devices.

In [4], we proposed a solution to solve the problem of authenticating devices in IoT networks. This solution utilizes blockchain technology to store the identity information of authenticated devices. Based on its characteristics, blockchain is used to create the digital identification of IoT devices and authenticate IoT devices. A private blockchain is generated in each IoT network to isolate the network from outside access. It highly increases the security level of the IoT network and the integrity of information collected by IoT devices. This paper evaluates the performance of our proposed authentication scheme by considering a stochastic threat model. Numerical results indicate that the proposed scheme significantly increases the probability that a device stays in a healthy state.

II. OVERVIEW OF AUTHENTICATION SCHEME

The distributed property of blockchain makes malicious tampering or forgery difficult. Also, every transaction within the network is signed by a private key that provides strong protection against forgery. Therefore, blockchain technology is suitable to store identity information.

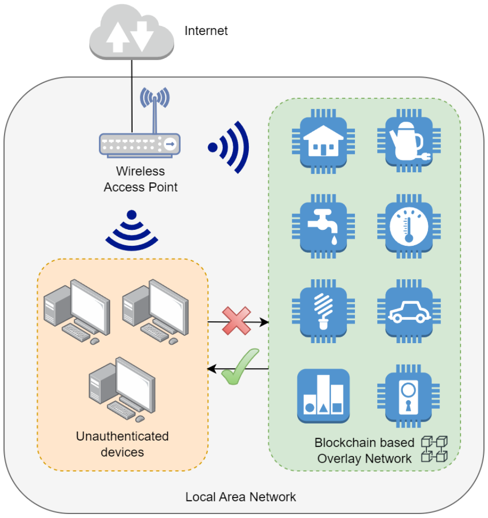

Fig. 1. Overview of the overlay network.

The final target of our scheme is to construct a secure overlay network that includes authenticated devices only. The overlay network separates authenticated devices and unauthenticated devices within the same Local Area Network (LAN). All authenticated devices discard traffic outside the overlay network, which protects them against internal and external attacks. Figure 1 shows the resulting overlay network after using our proposed scheme. More than one overlay network can be established within a LAN.

The authentication within the overlay network is supported by a coin-based blockchain system. The blockchain database stores transactions which can be used to determine the balance of an account characterized by an account number. The account number is a public key of an IoT device which also acts as the device identifier (Id). A device identifier will be used to encrypt the communication among the authenticated devices in the overlay networks. To join the overlay network, a device needs to be authenticated by a Hardware Authenticator (HA). HA is an offline device kept by the system administrator. This device has three functions, namely, generating genesis block, signing Authentication Transaction (AT), and generating new blocks.

The communication within the overlay network is encrypted based on the identity information provided by the blockchain system. The encryption and decryption are carried out by a firewall module within the IoT device. All traffic will be encrypted automatically without any modification to the working programs. The firewall provides network-layer encryption. For details of the authentication mechanism, readers are referred to [4].

III. PERFORMANCE EVALUATION

It is assumed that an attacker targets an IoT network and is interested in salvaging all protected data on each device. These data are protected by the account management module of the OS. It is assumed that physical access to those IoT devices is not available for the attacker. The attacker is unauthenticated and is not in the same network as the IoT. It is also assumed that no internal attack from another device within the IoT network is possible. Therefore, the attacker can only attack IoT systems through the Internet. Exploits on software packages could sometimes expose protected data, such as the exploits on database software that could grant access to the protected folder. However, this access is limited to the workspace of the software package because a properly implemented OS contains an application within a sandbox. Unfortunately, the attacker can still inject malicious programs using these software exploits to perform privilege escalation and gain full control of the system.

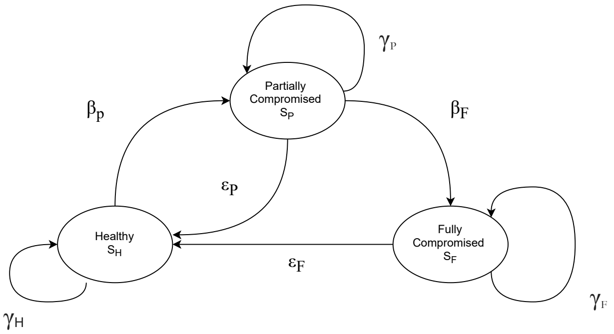

Fig. 2. Security model based on Markov chain.

Figure 2 describes our security model. Consider an IoT device is running at a healthy state (S_H) and is not compromised by any attackers. With probability γ_H, this device stays in this healthy state. The attacker keeps attacking this device which could change the state to others, including partially compromised (S_P) and fully compromised (S_F). The fully compromised state must be transitioned from the partially compromised state. Such a process cannot be reversed because it is irrational to turn a fully compromised system into a partially compromised one. Both compromised statuses can be recovered and return to a healthy state (e.g., by patching). A partially compromised state recovers with probability ε_P while the fully compromised state has probability ε_F. The probability for a healthy device to transition to a partially compromised state is β_P and to transition from partially compromised to fully compromised is β_F. However, both compromised states can remain in the same state. The partially compromised state has a probability γ_P to stay that way while a fully compromised state recovers probability γ_F. Assuming the state can only have a one-step transition, the transition probability matrix of the above Markov chain is:

$$P = \begin{bmatrix} \gamma_H & \beta_P & 0 \\ \varepsilon_P & \gamma_P & \beta_F \\ \varepsilon_F & 0 & \gamma_F \end{bmatrix}$$

If we put a Markov chain $\{X_n\}$ in the long run such that $n \to \infty$, the probability for each state j will converge to a limiting probability (π_j). These converged probabilities are considered as the steady-state probabilities. The limiting probabilities are not affected by the initial condition X_0. It can be shown that this model is a regular Markov chain when β_P , β_F and ε_F are > 0. To estimate the long-term behavior for the IoT device, we must assume the probability of being compromised > 0.

A set of system equations can be set to determine the limiting distribution (π_0, π_1, π_2):

$$\gamma_H \pi_0 + \varepsilon_P \pi_1 + \varepsilon_F \pi_2 = \pi_0 \tag{1}$$

$$\beta_p \pi_0 + \gamma_P \pi_1 = \pi_1 \tag{2}$$

$$\pi_0 + \pi_1 + \pi_2 = 1 \tag{3}$$

Equations (2) and (3) can be rewritten as:

$$\pi_1 = \frac{\beta_P \pi_0}{1 - \gamma_P}.$$

$$\pi_2 = 1 - \pi_0 - \frac{\beta_P \pi_0}{1 - \gamma_P}.$$

By substituting π_1, π_2 into Equation (1)

$$\pi_0 = \frac{\varepsilon_F (1 - \gamma_P)}{(1 - \gamma_P)(1 - \gamma_H + \varepsilon_F) - \beta_p (\varepsilon_P - \varepsilon_F)}$$

Since for each state $i \sum_{(j=0)}^{\infty} P_{ij} = 1$, therefore, $\beta_P = 1 - \gamma_H$. By solving equations (2) & (3):

$$\pi_0 = \frac{\varepsilon_F (1 - \gamma_P)}{\varepsilon_F (1 - \gamma_P) + \beta_p (\varepsilon_F + \beta_F)}$$

$$\pi_1 = \frac{\beta_P \varepsilon_F}{\varepsilon_F (1 - \gamma_P) + \beta_p (\varepsilon_F + \beta_F)}$$

$$\pi_2 = \frac{\beta_P \beta_F}{\varepsilon_F(1-\gamma_P)+\beta_p(\varepsilon_F+\beta_F)}$$

IV. NUMERICAL RESULTS

Kuhn *et al.* categorize computer vulnerabilities into 18 groups [5] based on the US National Vulnerability Database (NVD) [6]. To estimate the security enhancement of the proposed scheme, this paper further groups them into categories based on the potential impact on the system: partially compromise vulnerability (V_P) and fully compromise vulnerability (V_F). Table I shows these two groups of vulnerabilities.

By using the previous number of vulnerabilities, the possible values of β_P and β_F can be estimated. Assume the average exploitation rate for V_p and V_F be E_P and E_F, respectively. Therefore, β_P= E_p V_P and $\beta_F = E_F V_F$.The limiting distribution is computed using the above information. π_j consists of four parameters: β_P, β_F, γ_P, ε_F.

$$p[n] = 0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 0.99$$

Let $p[n]$ be a series of probabilities that are used to substitute into the model as the above parameters respectively to determine the possible outcome of π_j. To compute the value of π_j, we substitute $p[n]$ to one of the parameters one a time while setting the other three parameters as 0.5. The last element (0.99) is added to demonstrate the behavior when the parameters are approaching the limits.

The proposed scheme can use the software firewall to filter unauthenticated communication. However, some of the vulnerabilities cannot be resolved because the proposed scheme relies on them. Three partially compromise vulnerabilities including configuration, cryptographic issues, authentication issues, and all fully compromise vulnerabilities cannot be stopped by the proposed scheme.

Misconfiguration can still paralyze the proposed scheme because the privileged user can deactivate the software or avoid starting it at the beginning. The proposed scheme relies on cryptography to authenticate and secure communication. If the problem resides in cryptographic issues, the proposed scheme will not work properly. Authentication is the key to the proposed scheme; it will fail if it cannot do authentication properly. The proposed scheme would use a different V_P based on this property. Table II shows the values of V_P for the cases of using and without using the proposed scheme, respectively.

The calculation of the probability for the proposed scheme will be using the new V_P. Therefore, the model should produce a higher value for π_0, which is the probability for a healthy state while reducing the probability for a partially and fully compromised state.

Figure 3 shows the probability of a healthy state at the steady-state of the Markov process without applying the proposed scheme. All parameters are displaying a decaying behavior when $p[n]$ increases except ε_F. γ_P has the fastest decaying rate which is polynomial decay. β_P and β_F are linear decay. The range of π_0 when replacing β_P with $p[n]$ is larger than β_F, which also decays faster. This phenomenon indicates that the healthy state is more sensitive to the probability of partially compromise vulnerability than fully compromise vulnerability. Parameters including β_P, β_F, ε_F yield 0.28 to 0.83 and 0.51 on average. The overall average probability for staying in a healthy state without using the proposed scheme is 0.48.

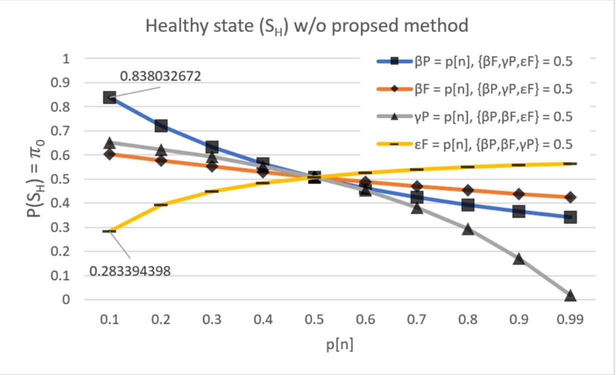

Fig. 3. Estimated probability of healthy state (S_H) without the proposed scheme.

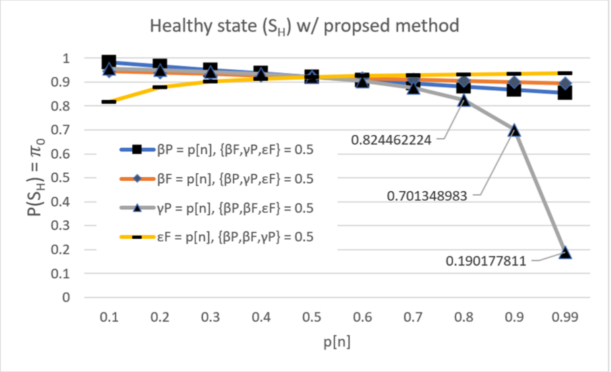

Fig. 4. Estimated probability of healthy state (S_H) with the proposed scheme.

Figure 4 shows the probability of a healthy state at the steady-state of the Markov process by applying the proposed scheme. Compared to Figure 3, the probability of staying in a healthy state is greatly increased. Parameters including β_P, β_F, ε_F yield 0.81 to 0.95 and 0.91 on average in the result. The decaying behavior is similar except γ_P. Between 0.9 and 0.99, the decay is greater than the previous data point. This further indicates the healthy state is more sensitive to the probability of partially compromise vulnerability than fully compromise vulnerability. The proposed scheme increased the overall probability of staying in a healthy state from 0.48 to 0.89, which is an 85% improvement.

A similar analysis can be carried out for the partially compromised state and fully compromised state. Here, we summarize the results in Table III, which shows the comparison of the average probability for a healthy state, partially compromised, and fully compromised state for an IoT system

TABLE I
VULNERABILITY COUNTS AND CATEGORIES FROM 2008-2016

Type of vulnerability	Count	Percentage	Level	Possible attack
Format String Vulnerability	110	0.294709	V_F	- Execute arbitrary code
Configuration	195	0.522438	V_P/V_F	- Exposure of config file - Execute arbitrary code
OS Command Injections	208	0.557267	V_F	- Execute arbitrary code
Race Conditions	377	1.010047	V_F	- Privilege escalation
Link Following	389	1.042197	V_F	- Privilege escalation
Credentials Management	589	1.578031	V_F	- Privilege escalation
Cryptographic Issues	779	2.087073	V_P / V_F	- Information leakage - Password leakage
Authentication Issues	920	2.464836	V_P / V_F	- Information leakage - Privilege escalation
Cross-Site Request Forgery (CSRF)	1161	3.110516	V_P	- Information leakage
Numeric Errors	1199	3.212324	V_F	- Privilege escalation
Code Injection	1545	4.139317	V_F	- Execute arbitrary code
Path Traversal	1686	4.51708	V_P	- Information leakage
Information Leak / Disclosure	2939	7.874079	V_P	- Information leakage
Input Validation	3763	10.08171	V_P / V_F	- Information leakage - Execute arbitrary code
SQL Injection	3828	10.25586	V_P / V_F	- Information leakage - Execute arbitrary code
Permissions, Privileges, and Access	4661	12.48761	V_F	- Privilege escalation
Cross-Site Scripting (XSS)	6220	16.66443	V_P	- Information leakage
Buffer Errors	6756	18.10047	V_F	- Privilege escalation
Total	37325	100	V_P = 57.57 V_F = 67.83	

TABLE II
COMPARISON OF V_P.

	Without proposed scheme	With proposed scheme
V_P	0.5757	0.0507
	Average improvement	80.43%

with and without our proposed authentication scheme. The proposed scheme increases the probability of a healthy state for the IoT device to 0.89. The probability of being partially compromised or fully compromised is reduced to 0.10.

TABLE III
COMPARISON OF STATE PROBABILITIES.

	Without proposed scheme	With proposed scheme	Difference
Average π_0 (Healthy state)	0.4852	0.8911	+83.66%
Average π_1 (Partially compromised state)	0.2989	0.0625	-79.09%
Average π_2 (Fully compromised state)	0.2158	0.0463	-78.53%
	Average	improvement	80.43%

V. CONCLUSION

In this paper, we have developed a stochastic threat model for IoT systems, which is used to evaluate the efficacy of our earlier developed authentication scheme. Numerical results have demonstrated that when the authentication scheme is deployed, the security level of IoT systems is significantly increased.

REFERENCES

[1] "Smart networked objects and internet of things," Association Instituts Carnot, Tech. Rep., 2011.

[2] R. Giuliano, F. Mazzenga, A. Neri, and A. M. Vegni, "Security access protocols in IoT capillary networks," IEEE Internet of Things Journal, vol. 4, no. 3, pp. 645657, June 2017.

[3] A. Greenberg. (2015) Hackers remotely kill a jeep on the highway with me in it. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway

[4] C. H. Lau, K. Y. Yeung, and F. Yan, "Blockchain-Based Authentication in IoT Networks," 2018 IEEE Conference on Dependable and Secure Computing (DSC), 10-13 Dec, 2018, Kaohsiung, Taiwan, pp. 1-8.

[5] R. Kuhn, M. Raunak, and R. Kacker, "It Doesnt Have to Be Like This: Cybersecurity Vulnerability Trends," IT Professional, vol. 19, no. 6, pp. 66-70, 2017.

[6] National Vulnerability Database, http://nvd.nist.gov 2017