SCIENCE CHINA
Information Sciences

• LETTER •

October 2018, Vol. 61 109303:1–109303:3
https://doi.org/10.1007/s11432-017-9428-6

A proactive defense mechanism for mobile communication user data

Caixia LIU[1*], Xinsheng JI[1], Jiangxing WU[1] & Xiao QIN[2]

[1]*The National Digital Switching System Engineering & Technological R&D Center, Zhengzhou* 450002*, China;*
[2]*Department of Computer Science and Software Engineering, Samuel Ginn College of Engineering, Auburn University, Auburn* AL36849-5347*, USA*

Received 5 December 2017/Revised 27 February 2018/Accepted 20 April 2018/Published online 16 August 2018

Citation Liu C X, Ji X S, Wu J X, et al. A proactive defense mechanism for mobile communication user data. Sci China Inf Sci, 2018, 61(10): 109303, https://doi.org/10.1007/s11432-017-9428-6

Dear editor,
Several studies have recently reported on major vulnerabilities in the Signaling System No.7 (SS7) used in mobile networks [1, 2]. The reported vulnerabilities and security issues would lead to the illegal acquisition and tampering of mobile communication user data, known as cellphone user data. The cellphone user data contain important information such as identity identification, location identification, security parameter-set. Due to these vulnerabilities, an increasing number of solutions have been presented to address the security issues [2–4]. Currently, almost all solutions deploy signaling firewalls or signaling monitors at the operators' network boundaries to filter or monitor the abnormal signaling from exterior networks. These solutions are passive protection mechanisms and can effectively prevent abnormal-signaling from external networks but cannot prevent abusive access using normal signaling. This study proposes a proactive defense mechanism known as DVM to address this issue. The DVM mechanism establishes a dynamic and virtual mapping between the cellphone user's identity identification and other data to conceal the real mapping relations. Thus attackers fail to access real user data. The DVM mechanism uses dynamic technique to manipulate user data.

Contributions. The main contributions of this study are summarized as follows.

(1) An attack model and an attack chain are developed that form the the basis for the entire study.

(2) The user's data mapping relation and their wide distribution could be the main reasons for user data disclosure. Based on this analysis, we eliminate the proactive defense thoughts to break or conceal user data's mapping relation in insecure SS7 networks.

Based on the DVM mechanism, these challenging issues are addressed: (a) manipulating data under the existing mobile communication mechanisms; (b) the conditions that must be met when a data item is manipulated; (c) implementing user data dynamic manipulation; (d) ensuring normal communication after user data are dynamically manipulated.

A theoretical analysis model is presented to evaluate the DVM's security efficiency. In addition, the effects of multiple parameters (e.g., time-interval, and occurrence probability of user data dynamic manipulation) on security improvement are studied.

Attack model and attack chain. In SS7 networks, attackers may attack user data via two abusive access modes: (1) sending normal signaling or normal commands to users' data storage entities to acquire or tamper with user data; (2) collecting signaling data on signaling pathways to extract user data that are carried in signaling data.

[*] Corresponding author (email: lcxtxr@163.com)

To meet the SS7 protocol specifications, attackers tend to acquire necessary conditions (known as necessary resources) such as target users' identity identifications and data storage entities' addresses, to attack user data.

The following assumptions based on the aforementioned analysis:

(1) Only attackers who have acquired the necessary resources, R, can complete an attack process. R represents a set of necessary resources. Thus, $R = \{R_1, R_2, \dots, R_n\}$.

(2) Attack processes are serial and mutually restricted. A follow-up process relies on the previous process. If a process is not completed, the corresponding follow-up processes cannot be performed.

(3) Let p_i $(i = 1, 2, \dots, n)$ be the probability of attackers successfully acquiring the necessary resources R_i $(i = 1, 2, \dots, n)$.

(4) p_e denotes the successful probability of attacking user data after attackers have acquired the necessary resources R.

State transfer graph is used to delineate the process of attacking user data. In the attack chain, S_0 denotes the initial state of an attack process. S_{end} denotes the successful-completion state of the attack.

The probability of an attacker shifting from the initial state to successfully completing the attack process (i.e., p_{succ}) is expressed as follows:

$$p_{\text{succ}} = p_1 \times p_2 \times \cdots \times p_n \times p_e. \tag{1}$$

From the attack model and attack chain, we infer that once the network access permissions or necessary resources are obtained by the attackers, they are likely to be effective for a long period of time; therefore, breaking or disrupting the attack chain can effectively address the issues of abusive access to user data.

Basic idea of DVM. In mobile networks, different data items that belong to the same users are usually mapped when they are stored, transmitted and interchanged. Thus, once a data item are known, attackers can easily access the other data items that are mapped with the known data item belonging to the same user. Besides, due to cellphone users' mobility characteristics, user data are normally transmitted frequently from one network entity to another and are normally widely stored in different entities, including different operator networks. From the attack model, we infer that the users' data mapping relation and the wide data distribution may be the main characteristics that are exploited to illegally access user data. As a result, we eliminate proactive defense thoughts to break or conceal users' data mapping relation in the insecure SS7 networks.

Further, based on human behaviors, attackers usually target specific persons, groups, or networks; thus, the targets' identity identification used in the networks should be considered as information given a priori. We believe that protecting user data involves securing a rich set of data items that have mapping relations with users' identity identifications. Therefore, the DVM mechanism is presented to establish a dynamic and virtual mapping between users' identity identification and other datasets to conceal the mapping relation between users' real identities and other data items.

Let ID be user's identity identification (e.g., cellphone number). Let S_{ID} denote the dataset that has a mapping relation with ID; thus, $S_{\text{ID}} = \{d_1, d_2, d_3, \dots, d_k\}$, where d_i denotes the ith data-item in set S_{ID}, and k denotes the number of data items.

The basic idea of the DVM mechanism is to establish a dynamic and virtual mapping between ID and S_{ID}. If a user intends to protect a subset of S_{ID}, then our strategy is to establish a dynamic and virtual mapping between ID and the subsets of S_{ID}.

We design two ways to establish the dynamic and virtual mappings between ID and S_{ID}. First, S_{ID} in hidden by dynamically manipulating a user's data set or subset. Second, ID is hidden by dynamically manipulating a user's identity identification. Figure 1(a) and (b) depict these two approaches.

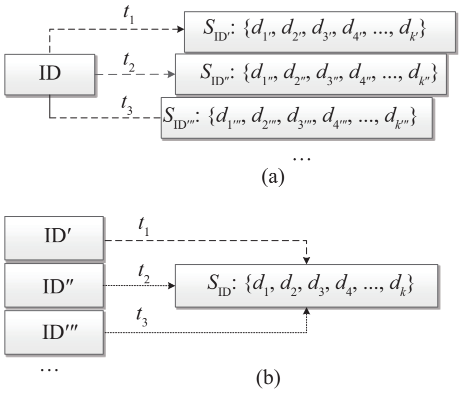
t_1
$S_{\text{ID}'}$: $\{d_{1'}, d_{2'}, d_{3'}, d_{4'}, \dots, d_{k'}\}$
ID
t_2
$S_{\text{ID}''}$: $\{d_{1''}, d_{2''}, d_{3''}, d_{4''}, \dots, d_{k''}\}$
t_3
$S_{\text{ID}'''}$: $\{d_{1'''}, d_{2'''}, d_{3'''}, d_{4'''}, \dots, d_{k'''}\}$
…
(a)
ID′
t_1
ID″
t_2
S_{ID}: $\{d_1, d_2, d_3, d_4, \dots, d_k\}$
ID‴
t_3
…
(b)

Figure 1 Two approaches to implement user data dynamic and virtual mappings. (a) Dynamically manipulating user dataset; (b) dynamically manipulating user Identity identification.

Using the mapping techniques, two challenging issues can be mitigated: whether user data can be manipulated under the existing mobile communication mechanisms and the required conditions for manipulation a data item. The two challenges are addressed by analyzing the attributes of user data as well as spatiotemporal and spatiotemporal mapping characteristics (detailed information is included in Appendix A).

To address the challenges with respect to (1) the dynamic manipulation of user data and (2) to ensure normal communication after some data items are dynamically manipulated, we developed a DVM principle prototype based on existing mobile communication networks. In the principle prototype, the dynamic manipulation is separately verified with location, routing and identity identifications (i.e., MSISDN number) in different scenarios. The MSISDN number for dynamic manipulation mechanism was reported previously [5].

Security efficiency evaluation. Based on the attack state transfer diagram (refer to Appendix B), we analyzed the security improvement offered by the DVM mechanism and suggested methods to achieve good security efficiency.

Let p_{ij} denote the probability that the state is transformed from S_i to S_j ($i > j$; $i = 1, 2, \ldots, n$; $j = 0, 1, 2, \ldots, n-1$). According to the attack model as well as the attack chain, we concluded that the attackers' attack state at time t only depends on the state at time $t-1$ and is independent of any state prior to time $t-1$. Thus, we model the attack chain as a Markov chain.

Let p_{si} ($i = 1, 2, \ldots, n$) and p_{se} respectively represent the steady-state probability of the attackers' attack state being in S_i and S_{end}. Then, the probability for the attackers' successful attacks (i.e., p'_{succ}) is expressed as

$$p'_{\mathrm{succ}} = p_{se} = p_{sn} \times p'_e. \tag{2}$$

In (2), p'_e is the probability that the state is transferred from S_n to S_{end}.

We introduce γ, which is the attack-difficulty increment, to quantify security improvement offered by the proposed DVM mechanism. γ is expressed as

$$\gamma = \frac{p_{\mathrm{succ}} - p'_{\mathrm{succ}}}{p'_{\mathrm{succ}}} = \frac{p_{\mathrm{succ}}}{p'_{\mathrm{succ}}} - 1. \tag{3}$$

In (3), p_{succ} and p'_{succ} are derived from (1) and (2).

Three conclusions are presented from the analysis results. First, the DVM mechanism substantially improves the overall system security by increasing attack difficulty. Second, the dynamic-manipulation time interval and the dynamic manipulation probabilities significantly affect the attack-success probability and attack difficulty. Last, defense efficiency can be improved by dynamically manipulating the necessary resources that must be acquired earlier in the attack chain.

Conclusion. To address the issue of user data disclosure in SS7 networks, a proactive defense mechanism known as DVM was proposed. We first built the attack model and attack chain and then analyzed the main factor that leads to user data disclosure in SS7 networks. This motivated us to eliminate proactive thoughts concerning defense against such attacks. In addition, we addressed four challenging issues of the DVM mechanism. Finally, we analyzed the DVM'S security efficiency. We believe that the DVM mechanism is a theoretical foundation that will adapt to a wide range of application scenarios to improve data security.

Acknowledgements This work was supported in part by National Natural Science Foundation Innovation Research Group Project of China (Grant No. 61521003) and in part by Visiting Scholar Program of China (Grant No. 201407820028). Xiao QIN's study was supported by U.S. National Science Foundation (Grant Nos. CCF-0845257, CNS-0917137, CNS-0757778, CCF-0742187, NS-0831502, CNS-0855251).

Supporting information Appendixes A and B. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Positive Technologies. Signaling system 7 (SS7) security report. 2014. https://www.ptsecurity.com/

2 SANS Institute. The fall of SS7-How can the critical security controls help? 2015. https://www.sans.org/

3 AdaptiveMobile. AdaptiveMobile SS7 protection: securing the network against privacy & fraud attacks. 2015. https://www.adaptivemobile.com/

4 NetNumber. NetNumber Signaling Firewall Protects SS7 International Mobile Roaming Traffic for Major Global Mobile Operator Group. 2017. https://www.netnumber.com/

5 Liu C X, Ji X S, Wu J X. A mimic defense mechanism for mobile communication user data based on MSISDN virtualization. Chin J Comput, 2018, 41: 275–287