CAPTCHA-based DDoS Defense System of Call Centers against Zombie Smart-Phone

Seung Wook Jung

Soongsil University
seungwookj@ssu.ac.kr

Abstract

Recently, some researchers alarm the security community that the smart-phone which is interoperable between telecom networks and Internet, is dangerous conduits for Internet security threats to reach the telecom network such as DDoS attacks to the emergency call center. But the detailed DDoS defense scheme for the emergency call center against DDoS attack by zombie smart-phones is not presented yet.

This paper presents a DDoS defense system, called cushion system, against zombie smart-phones to protect the emergency call center such as 911. The cushion system, a private branch exchange(PBX) extension, differentiates the legitimate human users and zombie smart-phones using CAPTCHA test which can be solved by only human users. This paper analyzes the negative impacts on the emergency call center by the DDoS attack. Also, this paper shows how much stronger the emergency call center becomes, when the emergency call center adopts the cushion system.

Keywords: *DDoS, Smart-Phone, and Call Center*

1. Introduction

Smart-phones have recently become increasingly popular because they provide rich applications and services to smart-phone users. For such rich applications and services, smart-phones are capable of running third-party software application. However, the openness of running third-party software also leaves the smart-phones open to malicious malware. In fact, hundreds of smart-phone malwares have emerged in the past few years [1]. This means the expansion of the Internet security threats into telecom networks by using smart-phones that are endpoints to both networks. One of the most serious threats to the telecom networks by compromised smart-phones might be DDoS attacks against emergency call centers such as 911, resulting in national crises [2].

To defend the emergency call centers against such DDoS attacks, [2] introduced very rough telecom side detection mechanism and protection mechanisms of DDoS attacks to call centers. In summary, if a call center experiences unexpected flash crowd and client behaviors are abnormal (such as connected call without voice traffic), then the call center may be sure to be attacked, and the telecom network can perform rate limiting, call filtering or put the zombie smart-phone IDs into a black list. However, [2] did not propose any detailed scheme about which smart-phone IDs should be put into the black list. To our best knowledge, there is no scheme for differentiating between innocent wireless calls and DDoS wireless calls to the call center. Note that the call admission control on the telecom network drops also innocent calls because the call admission control does not include a feature that differentiates between innocent calls and DDoS calls.

However, in Internet, DDoS traffic can be differentiated from innocent traffic in general, because DDoS traffics have different patterns with the innocent traffics. Therefore, in Internet, there are a lot of works to protect web servers from DDoS attack.

This paper proposes CAPTCHA [3]-based DDoS defense system, named cushion system, to protect emergency call centers from DDoS attacks by zombie smart-phones. The cushion system can be implemented as a PBX extension which is a part of CTI(Computer Telephony Integration). In our proposed system, after an emergency call center utility reaches a certain limit, for example 60%, caused by flash crowd or DDoS attack, in the case of wireless calls, the cushion system sends MMS message including CAPTCHA test back to the caller. CAPTCHA test cannot be solved by automatically by malicious software. Thereby, the cushion system differentiates between innocent wireless calls and DDoS wireless calls. Thus, the emergency call center accepts the wireless calls from only cellular phone that solved CAPTCHA test.

This paper examines negative impacts on the emergency call center by DDoS attack. As a result, small DDoS arrival rate such as about 18 DDoS calls per minute can make the regional small emergency call center service unavailable practically. Moreover, this paper show a formula which expresses how many DDoS calls makes the regional emergency call center service with the cushion system unavailable. As a result, this paper shows that the emergency call center with the cushion system is much robust than the emergency call center without the cushion system. Therefore, adopting the cushion system into the emergency call center is valuable.

The organization of this paper is as follows: The details of our proposed DDoS defense system of emergency call centers are provided in the section II. We analyze the proposed system in the section III. The section IV concludes the paper.

2. Proposed System

2.1. Threat Model

We assume the attacker may control the large number of smart-phones in order to conduct DDoS attack to the emergency call center such as 911. Also, the attacker can sniff, modify and delete inbound/outbound messages in the smart-phone. However, the attacker cannot access physically or logically the links that carry calls.

2.2. The Design of Cushion System against DDoS Attack

2.2.1. Authentication: During the periods of flash crowd, DDoS defense system of the emergency call center, called cushion system, authenticates the cellular phone, both of the smart phone and the feature phone. The emergency call center is in either of two states, NORMAL or SUSPECTED_ATTACK. When the call center perceives lines depletion beyond an acceptable limit, k1, it shifts to SUSPECTED_ATTACK state from NORMAL state. In SUSPECTED_ATTACK state, every new call from cellular phone has to solve CAPTCHA test in given duration such as 4 minutes before servicing. Note that the feature phone and smart-phone cannot be differentiated by the phone number. Therefore, both of the feature phone and smart phone have to solve CAPTCHA test to be served. The call center continues to operate in the SUSPECTED_ATTACK state until the load goes down to a particular threshold $k2 < k1$. In the NORMAL state, every call is accepted without any authentication.

2.2.2. Architecture: Figure 1 illustrates the key components of cushion system in the call center, which is briefly described below. A system in the dotted line is a cushion system. The components outside of the dotted line and the controller represent general PBX(Private Branch eXchange) structure which would be used for CTI(Computer Telephony Integration).

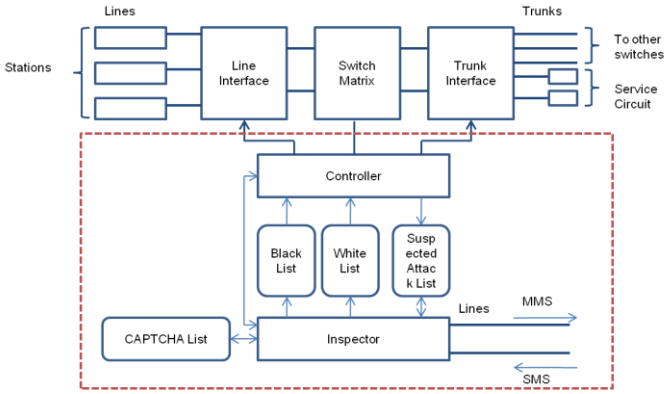

Figure 1. Cushion System Architecture

(a) **Controller :** controls the operation of PBX. We modify the controller for the cushion system. In the NORMAL state, the controller works as the controller of usual PBX system. In the SUSPECTED_ATTACK state, when a new call is arriving to the link interface, the controller searches the caller's cellular phone number (CPN) in the white list and black list which are shown in Fig.2. If the CPN in the white list, and the gap between CREATION_TIME in the white list and call arrival time is not longer than the certain limit k3, for example 30 minutes, then the controller connects the call to the station through switch matrix. If the gap is longer than k3, then the controller deletes the row of the CPN in the white list and puts the CPN to the suspected list with SEND_COUNTER as 0. If the CPN is in the black list, and the gap between CREATION_TIME in the black list and call arrival time is not longer than the certain limits k4, for example 1 hour, the controller drops the call. If the gap is longer than k4, then the row of CPN in the black list is deleted and the CPN is put in the suspected list with SEND_COUNTER as 0. If not in the white list, the black list, and the suspected attack list, the controller puts CPN with SEND_COUNTER as 0 in the suspected attack list and notifies the inspector that the new CPN is registered in the suspected attack list. Then the inspector goes to the process 1 below. If not in the white list and the black list, but in the suspected list, the controller notifies the inspector that the CPN is called. Then the Inspector goes to the process 1 below.

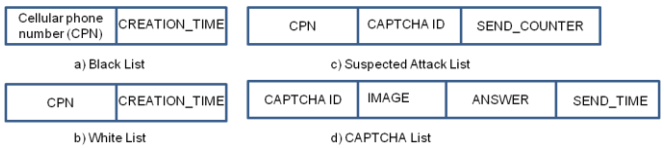

Figure 2. Structure of Lists

(b) **Inspector :** is the head of the cushion system and the inspector has different phone number from the call center.

1. The inspector reads the cellular phone numbers (CPNs) in the suspected attack list shown in Figure 2.
2. If SEND_COUNTER+1 of the certain CPN exceeds certain limit k5, for example 5, the inspector writes the CPN with the CREATION_TIME on the black list. Also, the inspector deletes the rows of CPN in the suspected list and the inspector ends the process.
3. If not exceed k5, the inspector sends the MMS message and adds 1 to SEND_COUNTER in the suspected attack list. Also, the inspector writes CAPTCHA_ID on the suspected attack list and writes SEND_TIME on the CAPTCHA list.
4. If the owner of CPN sends SMS to the inspector as the answer of the CAPTCHA test, the inspector reads CAPTCHA_ID with CPN in the suspected list.
5. The inspector reads the ANSWER and SEND_TIME of the given CAPTCHA_ID.
6. If the gap between SEND_TIME in CAPTCHA list and the SMS arrival time is longer than k6, such as 4 minutes, then the inspector adds 1 to SEND_COUNTER of CPN in the suspected attack list and goes to the process 2.
7. If not longer than 4 minutes, then the inspector compares the ANSWER of the given CAPTCHA_ID in the CAPTCHA list with the answer.
8. If the answer is right, then the inspector puts the CPN with CREATION_TIME in the white list and deletes the rows of CPN in the suspected list.
9. If the answer is wrong, then the inspector adds 1 to SEND_COUNTER of CPN in the suspected attack list and goes to process 2.

Controller can notify the inspector that the new CPN is registered in the suspected attack list. Then, the inspector goes to the process 1.

MMS message including CAPTCHA test sent by cushion system has two purposes. One is giving CAPTCHA test in order to differentiate zombie smart-phone from human user. The other one is letting the smart-phone owner know about that the smart-phone is compromised if the owner didn't call to the call center.

2.2.3. Characteristic

(a) **One Test Per One Call :** The cushion system gives one test per call. It means it is useless that the attacker solves a single test and distributes the answer to zombie smart-phones.

(b**) Drop Messages With CAPTCHA By An Attacker:** An attacker can fully control zombie smart-phones. Therefore, the attacker can drop MMS messages and calls continuously. To protect from this attack, we use k5, so the number of calls reaches k5, then the CPN is put in the black list. However, one problem is that the owner of the zombie smart-phone cannot see the messages, so the owner cannot be notified that the smart-phone is infected by malicious software.

(c) **Reduce Negative Impact On The Service By Continuous Calls:** An authentication mechanism that relies on CAPTCHAs has a disadvantage. That is the attacker can force the system to continuously send CAPTCHA tests, imposing an unnecessary overhead on the system. To deal with this issue, we separate the controller who serves the call and the inspector who sends callers CAPTCHA tests and checks answers. Also, after several trials without answers, calls from the zombie smart-phone will be blocked.

(d) **Differentiations Human User From Zombies Smart-phone:** The zombie has two options; either (1) imitate human users who cannot solve the test and leave the system after a few trials, in which case the attack has been subverted, or (2) keep calling though they cannot solve the test. However, by continuing calling without solving the test, the zombies become distinguishable from human users.

3. Security Analysis

3.1. Modeling of 911 Service

To investigate how smart-phone DDoS attack adversely affects the performance of a emergency call center such as 911, at first the modeling of 911 service is required. The network model of 911 service for such purpose is developed and described in detail by [4]. Therefore, we would like to refer [4] and summarize the network model of 911 service in [4] to clarify the impact of smart-phone DDoS attack to the call center.

In reality, a call center handles wireline calls, wireless calls, and VOIP calls, and taking time to handle a call depends on the type of these calls. Therefore, [4] developed an open multi-class queuing network model[5] to quantify DDoS attack's impact. In this queuing network model, there are multiple classes of customers C1, C2, ... CK. In this model, there are M stations, namely call center operators, denoted by S1, S2, ..., SM. The service demand of class Ci by the station Sj, where $1 < i < K$ and $1 < j < M$, is denoted by Di,j. The overall utility of a operator j and its utility due to class i customers are denoted by Uj and Ui,j, respectively. Also, we define Ri,j as the average residence time, including both service time and waiting time, of customers of class Ci at station Sj. Let Ri be the average residence time of class Ci customers in the network. Assuming that the arrival rate of class Ci customers is λ_i, we have the following solution :

$$U_{i,j} = \lambda_i \times D_{i,j}, U_j = \sum_{i=1}^{K} U_{i,j}, R_{i,j} = \frac{D_{i,j}}{1-U_j}, R_i = \sum_{j=1}^{M} R_{i,j} \quad (1)$$

In this model, wireline calls, wireless calls, and VOIP calls are treated as a customer class, respectively. [6] showed that between 25% and 70% calls are unintentional calls due to misdialing. Such unintentional calls require short time to handle while the real emergency call takes longer time. In this paper, we assume that 20% of calls are unintentional calls, because we need heavy loads for analyzing DDoS impacts. VOIP calls are still rare compared with wireline and wireless calls. Thus, we do not further break down VOIP calls. Therefore, we have five customer classes : wireline emergency calls, wireline unintentional call, wireless emergency calls, wireless unintentional calls, VOIP calls.

According to PSN(Public Safety Network)[7], the average call volume per hour for a regional 911 call center is between 20-70 calls. To analyze DDoS impacts, we assume more hourly call volume and 90 calls per hour. To derive the arrival rate of each class, we use the incoming call statistics in 2011[8]: wireline 24%, wireless 75%, VOIP 1%. Thus, for wireline emergency calls, wireline unintentional calls, wireless emergency calls, wireless unintentional

calls, and VOIP calls, their proportions are 19%, 5%, 60%, 15%, and 1%. Therefore, the arrival rate of each class of customers are 0.28, 0.07, 0.9, 0.22 and 0.015 calls per minute, respectively.

Due to the lack of exact statistics data for the service demand(duration) of each call, this paper assumes as Table 1. Also, due to lack of exact number of 911 operators in one call center, we assume 25 operators in one call center as [4].

Table 1. Summary of Arrival Rate and Service Duration of Classes

Class	Service duration	Arrival rate	Comments
Wireline emergency call	5min	0.28	Operations have to call back and cooperate with other assistants
Wireline unintentional call	1min	0.07	Operators decide the false alarm shortly
Wireless emergency call	5min	0.9	As wireline emergency call, Successful DDoS traffic classified in this class
Wireless unintentional call	1min	0.22	As wireline unintentional call
VoIP calls	2min	0.015	Rare and use average duration

3.2. Threat Analysis:

We classify DDoS calls from zombie smart-phones as wireless unintentional calls which take 1 minute in our assumption. A successful DDoS attack against 911 services means the utility of 911 resource is 1(100%), which leads to a long waiting time of real emergency calls. Using open multi-class queuing network model, this paper explores how the increasing call arrival rate of DDoS calls adversely affects the quality of the 911 service.

If there are 25 call operators in a call center and no DDoS attacks to the call center just as normal state, the utility of the call center is 24.9% according to the equation (1). When DDoS traffic's arrival rate reaches 18.78, the utility by DDoS attack reaches 75.1%. Thus, the overall utility of the call center reaches 100% (=24.9% + 75.1%). When the call arrival rate is larger than 18.78, the emergency call waiting time is more than 20 minutes on average according to (1), which is not acceptable for emergencies. Practically, this makes the 911 service unavailable for the public.

When applying our cushion system, the service duration for CAPTCHA test(automatically drop the wireless call and send CAPTCHA test) must be very short under SUSPECTED_ATTACK state. For successful DDoS attack by zombie smart-phones, the utility of the call center must be 1 (100%). The equation (2) formulates when the utility of the call center reaches 1 according to k1 and service duration($D_{i,j,}$ where i = wireless call) under the SUSPECTED_ATTACK state. Note that all wireless calls under the the SUSPECTED_ATTACK state will be automatically dropped and have to solve CAPTCHA test.

$$\lambda_i = M(1-k1)/D_{i,j} \qquad (2)$$

Where M is the number of call operators, k1 is the utility for entering the SUSPECTED_ATTACK state. This equation assumes that all calls below k1 are innocent. Thereby, equation (2) expresses how many DDoS calls per minute after k1 must be arrived in order to make the emergency call center service unavailable. Figure 3 shows the number of DDoS calls per minute to make the emergency call center service unavailable according to k1 and the service duration for wireless calls under the SUSPECTED_ATTACK state.

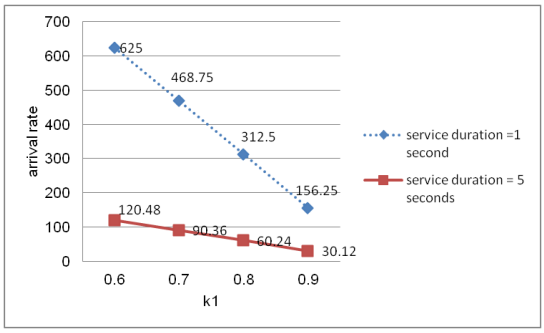

Figure 3. Arrival Rate According to K1 and Service Duration

For example, if k1 is 0.8 (80%), M is 25, and $D_{i,j}$ for i = wireless call is 5 second(0.083 minutes), then the number of DDoS call per minute must be about 60(=25(1-0.8)/0.083) calls for successful DDoS attack. In this case, the emergency call center with the cushion system is about 3 times stronger than the emergency call center without the cushion system (319% = (60/18.78)*100). If k1=0.6 and the service duration for wireless call is 1 second, the number of DDoS call per minute must be more than 625. In this case, the emergency call center with cushion system is about 33 times stronger than the emergency call center without the cushion system (3,328% = (625/18.78)). How much stronger the call center with the cushion system is compared with the call center without the cushion system, which depends on k1, M, and Di,j. However, when adopting the cushion system, the emergency call center must be stronger without the cushion system. Therefore, adopting the cushion system is valuable in many situations.

4. Conclusion

The smart-phone, which is interoperable between telecom networks and Internet, is dangerous conduits for Internet security threats to reach the telecom networks. One of most dangerous attacks to the telecom networks is DDoS attack to the emergency call center such as 911 service, resulting in national crises.

The problem is that there is no difference between innocent wireless call and DDoS wireless call, while DDoS traffics in Internet have some patterns to be differentiate from innocent traffics in Internet. Moreover, the call admission control in telecom networks also does not have a feature that differentiate between innocent wireless call and DDoS wireless call. Therefore, to prevent the emergency call center from DDoS attack by zombie smart-phone, we need a method to differentiate between innocent wireless call and DDoS call. This paper proposed using CAPTCHA test, which cannot be automatically solved by malicious software, to differentiate between innocent wireless call and DDoS call. Also, this paper proposed DDoS defense model using CAPTCHA test, called cushion system. The proposed cushion system can be implemented as a PBX extension, which is a part of CTI. Before adopting cushion system, in order for emergency call center manager to approximately know the effect of cushion system, the paper formulates an equation which expresses how much DDoS call volume per minute is required to make emergency call center service unavailable. Because emergency call centers have their own policies for unintentional wireless calls and have each different number of call operators, this paper cannot show exact effect when adopting the cushion system for each situation, but the emergency call center manger can calculate the effect of the cushion system using that equation. However, this paper showed examples of the effect of the cushion system based on the equation. One of examples showed

that, in order to make the emergency call center service with the proposed system unavailable, more than 33 times minutely call volume is required comparing with the emergency call center without the proposed system. Therefore, adopting the proposed system can be worthy of considering in order to protect the emergency call center from DDoS attacks using zombie smart-phones.

Reference

[1] M. Hypponen, "State of cell phone malware in 2007", http://www.usenix.org/events/sec07/tech/hypponen.pdf , **(2007)**.
[2] C. Guo, H. J. Wang and W. Zhu, "Smart-phone attacks and defenses", Third Workshop on Hot Topics in Networks, **(2004)** November 15-16; San Diego USA.
[3] L. von Ahn, M. Blum, N. Hopper and J. Langford, "Captcha: Using Hard AI Problems for Security", EUROCRYT 2003, **(2003)** May 4-8; Warsaw Poland.
[4] L. Liu, X. Zhang, G. Yan and S. Chen, "Exploitation and Threat Analysis of Open Mobile Devices", ACM/IEEE Symposium on Architectures for Networking and Communications Systems, **(2009)** October 19-20; Princeton, USA.
[5] E. Gelenbe and I. Mitrani, "Analysis and Synthesis of Computer Systems", Academic Press, London, **(1980)**.
[6] WTB report. http://www.scribd.com/doc/311371/US-Federal-Communications-Commision-FCC-Official\Release-DA023413A1.
[7] H. Jasso, C. Baru, T. Fountain, W. Hodgkiss, D. Reich and K. Warner, "Using 9-1-1 call data and the space-time permutation scan statistic for emergency event detection", Proceedings of the 9th annual International Digital Government research Conference, **(2008)** May 18-21; Montreal, Canada.
[8] 911 statistics. http://www.lapeercounty911.org/files/Total%20Stats.pdf.

Authors

Seung Wook Jung

He received the the PhD degree in engineering from the University of Siegen of German in 2006, is currently a senior research associate at Korea Internet and Security Agency(KISA), and is currently a adjunct professor at the Soongsil Unversity of Korea. His research interests include the information security and privacy such as cryptography, information security system architecture, identity management, and the development of national-wide privacy policy