International Journal of Advanced Smart Convergence Vol.6 No.4 56-59 (2017)
http://dx.doi.org/10.7236/IJASC.2017.6.4.8

IJASC 17-4-8

Covert Channel Based on Instruction Gadgets in Smart Sensing Devices

Jun-Won Ho

Department of Information Security, Seoul Women's University, Seoul, South Korea
jwho@swu.ac.kr

Abstract

In this paper, we design a covert channel based on instruction gadgets in smart sensing devices. Unlike the existing convert channels that usually utilize diverse physical characteristics or user behaviors or sensory data of smart sensing devices, we show that instruction gadgets could be exploited for covert channel establishment in smart sensing devices. In our devised covert channels, trojan smart sensing devices exchange attack packets in such a way that they encode an attack bit in attack packet to a series of addresses of instruction gadgets and decode an attack bit from a series of addresses of instruction gadgets.

Key words: *Covert Channel, Instruction Gadgets, Smart Sensing Devices.*

1. Introduction

Smart sensing devices could be defined as smartphones, IoT devices, and any devices being capable of sensing, computing, and communicating. Attacker could mount myriad types of attacks against smart sensing devices and harness covert channel to conceal motley attacks against smart sensing devices. For example, it is used to transfer the leaked secret information between trojan smart sensing devices. Additionally, trojan smart sensing devices can exchange attack packets through covert channels in order to evade attack packet detection. Hence, covert channel detection is essential for smart sensing device security. To devise robust covert channel detection schemes, it should be thoroughly examined how covert channels could be established in smart sensing devices. Although a variety of covert channels [1-13] have been proposed by researchers, they do not yet fully reflect all types of covert channels that could be built up in smart sensing devices. To expand the scope of covert channels in smart sensing devices, we design a covert channel with using instruction gadgets that are stored in code region of smart sensing devices. Trojan smart sensing devices exchange attack packets over our devised covert channel.

Manuscript Received: Sep. 10, 2017 / Revised: Oct. 23, 2017 / Accepted: Nov. 11, 2017
Corresponding Author: jwho@swu.ac.kr
Tel: +82-2-970-5607, Fax: +82-2-970-5981
Department of Information Security, Seoul Women's University, Korea

A trojan smart sensing device encodes an attack bit in attack packet to a sequence of addresses of instruction gadgets and sends the encoded attack bit to other trojan smart sensing device. Upon receiving the encoded attack bit, other trojan smart sensing device decodes an attack bit from a sequence of addresses of instruction gadgets. The details of how to perform encoding and decoding process are specified in Section 3. From the perspective that instruction gadgets are utilized for covert channel creation, we believe that our newly proposed covert channel will broaden the extent of covert channels, ultimately helping develop efficient and resilient covert channel detection schemes.

2. Related Work

In [1], sensors are utilized to create covert channel in android systems. In [2], packet reordering is used to build covert channel. Deshotels et la. [3] leveraged inaudible sound for covert channel setup in mobile devices. In [4], TCP timestamps are utilized for cover channel. Ho et al. [5] applied the sequential analysis to sequences of sensory data in order to build up covert channel in android systems. Lalande et al. [6] developed a number of covert channels with using system characteristics such as the screen state, process priority, and task list in android systems. Li et al. [7] proposed covert channels based on the characteristics of network layer in ad hoc wireless networks. Novak et al. [8] devised different types of covert channels based on physical media of accelerometer, camera, flash, speaker, ultrasound, and vibration in smart mobile devices. In [9], covert channels are devised under xen virtual machine environments. In [10], user behaviors are leveraged to create covert channel in smartphones. Schlegel et al. [11] devised sound-based covert channel in smartphones. Wang et al. [12] designed covert channels based on the characteristics of processor architecture. Wu et al. [13] performed research on covert channel attacks in x86-based virtual machines.

3. Covert Channel Establishment Based On Instruction Gadgets

Instruction gadget is regarded as a sequence of short instructions that reside in code region of smart sensing devices. For each executable file, we can find out a certain or substantial number of instruction gadgets. These instruction gadgets have been conventionally used for return-oriented programming (ROP) attacks in which attacker forces malicious behaviors to occur through craftily reusing instruction gadgets. Unlike this conventional usage of instruction gadgets in terms of attack, we deploy these instruction gadgets for covert channel establishment. This is a new attempt in the context of covert channels for smart sensing devices. The specific procedure of how to make use of instruction gadgets for covert channel construction is described as follows.

For simplicity, we consider trojan smart sensing devices S_u and S_v such that S_u and S_v act as encoder and decoder, respectively. We assume that a sequence of random numbers $r_1, r_2, \ldots, r_k \ldots_{(k \geq 1)}$ is shared by S_u and S_v. We denote this sequence of random numbers by R_k. Note that the value of each random number in this sequence ranges from 1 to T ($T \geq 1$). Furthermore, we assume that S_u wants to send S_v an attack packet consisting of attack bits $a_1, a_2, \ldots, a_{k\ (k \geq 1)}$.

If attack bit $a_i=1_{(i \geq 1)}$, S_u randomly selects r_i instruction gadgets that contain stack instructions such as pop or push, encodes $a_i=1$ to a sequence of addresses of the chosen r_i instruction gadgets, sends S_v the encoded value of $a_i=1$. Upon receiving the encoded value of $a_i=1$, S_v searches for a sequence of r_i instruction gadgets corresponding to the encoded value and checks if each instruction gadget in that sequence includes stack instruction. If so, S_v successfully decodes attack bit $a_i=1$ from a sequence of addresses of r_i instruction gadgets.

If attack bit $a_i=0_{(i \geq 1)}$, S_u randomly selects r_i instruction gadgets that do not contain stack instructions such as pop or push, encodes $a_i=0$ to a sequence of addresses of the chosen r_i instruction gadgets, sends S_v the

encoded value of a_i=0. Upon receiving the encoded value of a_i=0, S_v searches for a sequence of r_i instruction gadgets corresponding to the encoded value and checks if each instruction gadget in that sequence includes stack instruction. If so, S_v successfully decodes attack bit a_i=0 from a sequence of addresses of r_i instruction gadgets.

Since sequences of addresses of instruction gadgets are consecutively sent to S_v, they could be suspected as parts of ROP attack packets and thus attacker may adopt interleaving strategy in which garbage packets are placed between two adjacent sequences of addresses of instruction gadgets, leading to decrease in chance of being regarded as portions of ROP attacks. In interleaving strategy, both S_u and S_v generate the same series of random numbers and set each random number to each number of garbage packets that are interleaved between two consecutive sequences of addresses of instruction gadgets.

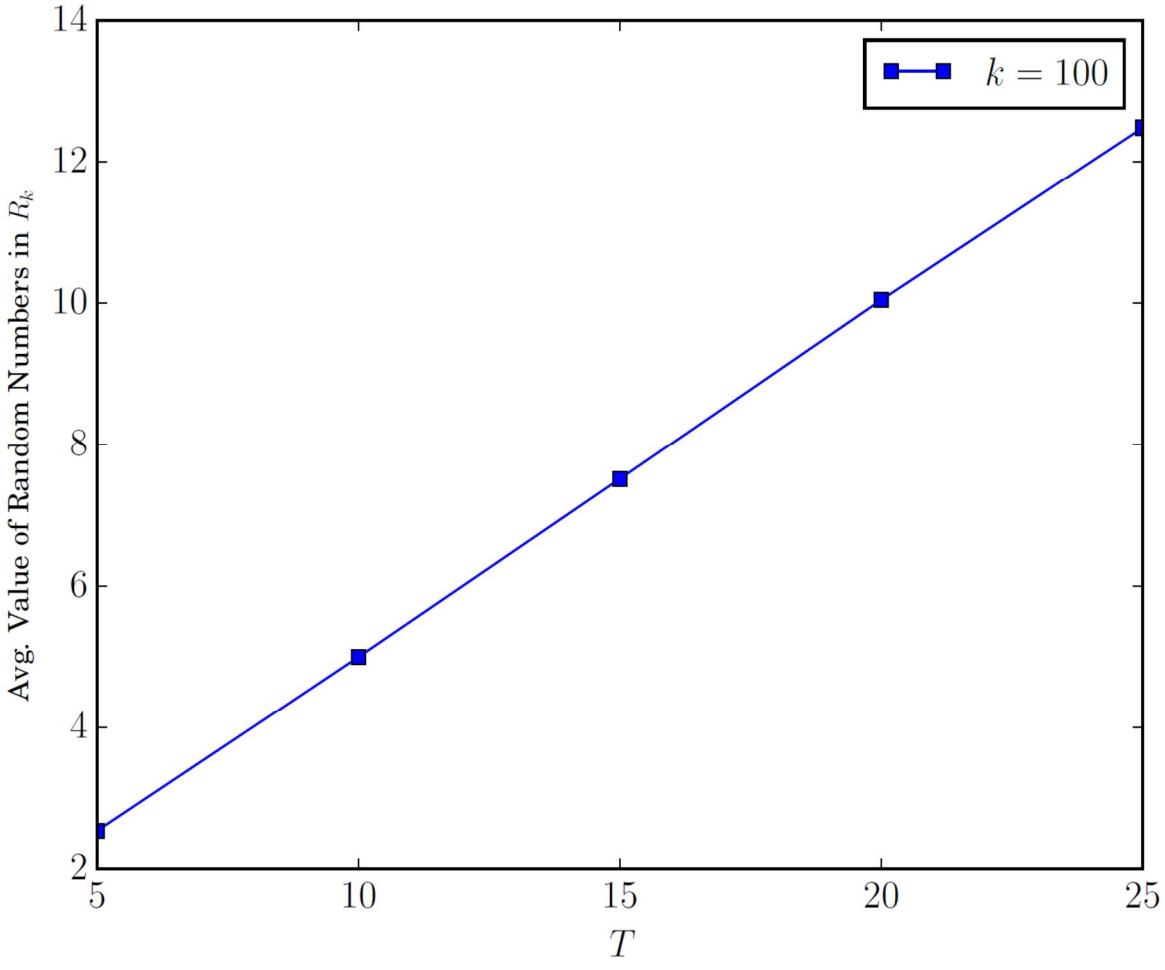

Figure 1. The effect of T on an average value of random numbers in R_k

We perform a simple simulation to investigate the effect of T on an average value of random number in R_k. We conduct simulations 1000 times and display the average results of 1000 iterations. Figure 1 shows how T

impacts on an average value of random numbers in sequence R_k when k=100. We see that an average value of random numbers in sequence R_k increases as T rises. We also discern that an average value of random numbers in sequence R_k is approximately half of T.

4. Conclusions

In this paper, we devise a covert channel based on instruction gadgets in smart sensing devices. Our designed covert channel leverages the instruction gadgets that are already placed in the code region of smart sensing devices. In the sense that the covert channels are built up with using instruction gadgets in smart sensing devices, they are considered to be new approach and contribute to the expansion of covert channel research area in smart sensing devices.

Acknowledgment

This work was supported by a research grant from Seoul Women's University (2017). This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2016R1C1B1014126).

References

[1] A. Al-Haiqi, M. Ismail, and R. Nordin. A New Sensors-Based Covert Channel on Android. The Scientific World Journal, 2014.
[2] A. El-Atawy and E. Al-Shaer, Building covert channels over the packet reordering phenomenon, In IEEE INFOCOM, 2009.
[3] L. Deshotels, Inaudible sound as a covert channel in mobile devices, In WOOT, 2014.
[4] J. G. N, R. Greenstadt, P. Litwack, and R. Tibbetts, "Covert messaging through tcp timestamps," In Workshop on Privacy Enhancing Technologies, 2002.
[5] J. Ho, K. Won, and J. Kim. POSTER: Covert Channel Based on the Sequential Analysis in Android Systems. In ACM CCS, 2017.
[6] J. Lalande and S. Wendzel. Hiding Privacy Leaks in Android Applications Using Low-Attention Raising Covert Channels. In ARES, 2013.
[7] S. Li and A. Epliremides, A network layer covert channel in ad- hoc wireless networks, In IEEE SECON, 2004.
[8] E. Novak, Y. Tang, Z. Hao, Q. Li, and Y. Zhang. Physical media covert channels on smart mobile devices. In UbiComp, 2015.
[9] K. Okamura and Y. Oyama, Load-based covert channels between xen virtual machines, In SAC, 2010.
[10] W. Qi, Y. Xu, W. Ding, Y. Jiang, J. Wang, and K. Lu. Privacy Leaks When You Play Games: A Novel User Behavior Based Covert Channel on Smartphones. In ICNP, 2015.
[11] R. Schlegel, K. Zhang, X. Zhou, M. Intwala, A. Kapadia, and X. Wang. Soundcomber: A Stealthy and Context-Aware Sound Trojan for Smartphones. In NDSS, 2011.
[12] Z. Wang and R. B. Lee, Covert and side channels due to processor architecture, In ACSAC, 2006.
[13] Z. Wu, Z. Xu, and H. Wang, Whispers in the hyper-space: High-speed covert channel attacks in the cloud, In USENIX Security, 2012