Poster: Tracking VM Attackers Based on Browser Fingerprinting

Xiaoxi Wang[1], Min Li[2], Xiaoyun Li[2], Qixu Liu[34]
[1]Beijing University of Technology, Beijing, China
[2]Beijing University of Posts and Telecommunications, Beijing, China
[3] Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
[4]School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China
destiny-xiaoxi@foxmail.com, {meizi, lxy691219491}@bupt.edu.cn, liuqixu@iie.ac.cn

***Abstract*—Web attack has occupied a majority of the attacks, and the combination of VMs and springboards has been the most common way to hide oneself. Most of related researches about virtual machines are targeting at the detection of VMs, while few of the technologies aim to track hidden attackers behind the VMs and IP proxy. With the fact that the browser is a necessary tool when attackers implementing an attack, we propose the technology of tracking VM attackers based on the browser fingerprinting. We first track the attacker separately in the VM and host by updated browser fingerprinting, and then associate the VM with host by hardware level tracking technologies. With shared information of the VM and host, our technology shows significant effect in tracking hidden attackers, moreover it even can associate the different VMs based on the same host.**

Keywords—tracking VM attackers;updated browser fingerprinting; virtual machine

I. INTRODUCTION

Attackers always browse targeted websites to sniff effective information in the physical computer, and implement attacks in virtual machine with springboards, which is the most common way for attackers to hide themselves not to be tracked. Nowadays, technologies about the virtual machine are almost targeted at the detecting aspect, and the identifying of a virtual machine is always based on system information, such as log files of system or execution results of special instructions. Attacked websites that run on the browser have no permissions to visit user's system information and execute instructions in the system. It brings too much obstacles for websites to track malicious users who implement illegal behaviors.

Browser fingerprinting was proposed by Eckersley[1] to perform the function of cookies, and play the role of identifying a user without the log in state and system authority. Since hardware of the VM is entirely based on the host, it gives users undifferentiated experience with physical computer, so does browser fingerprinting. Virtual machines and hosts can be treated as different devices in the tracking of browser fingerprinting. Besides, many of the hardware features show consistent values among VMs and hosts.

Based on the existing browser fingerprinting technology, in this paper, we update browser fingerprinting by adding hardware level features and a new type of tracking technology, to continuously track users separated in VMs and hosts. Then correlate the VMs and hosts by shared traceable hardware features, with which we can achieve the goal of tracking attackers behind the VMs and springboards.

II. APPROACH

Assuming that the attacker has multiple roles respectively using browsers of virtual machines and hosts to browse our specific website. And suppose that the attacker mainly uses one browser in a device.

Shown in Fig1, different roles of an attacker will be tracked by updated browser fingerprinting (UBF) in different "devices" (VMs and hosts), which includes the adding of fingerprint features and the new tracking technology, then we use hardware level tracking technologies to correlate VMs and hosts (CVH). With relationships of VMs and hosts, we can associate different VMs together which built on the same host.

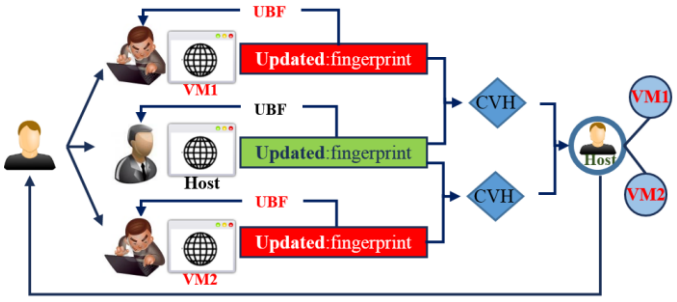

Fig. 1. Architecture of Tracking VM Attackers Based on Browser Fingerprinting

III. DESIGN

Based on the architecture, we will respectively introduce updated browser fingerprinting technology and process of correlating VMs with hosts, with the showing of related information.

A. *Updated Browser Fingerprinting*

To increase the fingerprint's stability, we add several hardware level features and a new kind of tracking technology to browser fingerprinting, including the replacing of screen resolution by screen ratio, and the adding of graphics card. We also introduce the correlation algorithm of enhanced solution[2] to identify similar fingerprints, and add history list tracking technology[3] into it, which can greatly improve the efficiency of association recognition.

The current way of measuring screen resolution cannot resolve the problem of different zoom levels caused by key function of "ctrl++" or "ctrl--", and values show differently among different browsers in the same machine. While the ratio of screen width and screen height is always the same no matter how the browser changes, and the value is consistent among different browsers from one host.

WebGL technology can be used to obtain the graphics card information. Graphics card is an unchanged feature, which can add much more stability to the browser fingerprinting, and promotion to similarity identification. Beyond that, the graphics card information shows obvious sign of virtual machine, identifying whether the "device" is a physical computer or a virtual machine, Table1 shows the comparison of different graphics infomation.

TABLE1: GRAPHICS CARD OF DIFFERENT OS

OS	Graphics Card
MAC	Intel Inc., Intel(R) Iris(TM) Graphics 6100
Window 7	Google Inc., ANGLE (Intel(R) HD Graphics 4600 Direct3D9Ex vs_3_0 ps_3_0)
(VM)Window7	Google Inc., ANGLE (VMware SVGA 3D Direct3D9Ex vs_3_0 ps_3_0)

First party websites can obtain the history list of browser to tracking users, by making use of HTTP Strict Transport Security and Content Security Policy. With the situation that, malicious users almost only use the browser of VM to carry out attacks, hence their visited list of browser may only target at several specific sites, which is distinct for a VM, and can be treated as a prerequisites in the correlation algorithm.

Fig2 shows the updated browser fingerprinting technology added the technologies above. Fingerprint, Cookie&Canvas, History List and IP Info are the analyzing conditions of two fingerprints, then the value with threshold calculated by simhash algorithm is placed in the next location to deal with the fingerprints while the first four can't identify them.

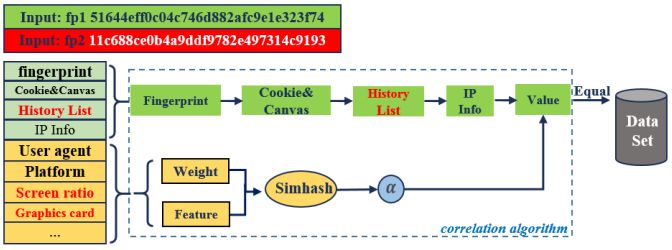

Fig. 2. Updated browser fingerprinting technology

B. *Correlate VM and host*

Virtual machines and hosts share the same hardware facilities, we extract the traceable IP network and battery information to correlate the host and VM, and associate multiple VMs with the host.

Website server can get the last hop IP address (public IP) without difficulty, although it may differ a lot among VMs and hosts because of the using of IP proxy. We can achieve the intranet IP through WebRTC technology, and then scan the network for alive hosts. By comprehensively analyzing the IPs from different sources, we can associate the virtual machine and host with the collected IP information.

Olejnik[4] has proved that current battery information, such as battery level and charging status, can be used to track users. Battery information is shared by the host and virtual machines (set to report battery information to host), and can't be forged by system settings. With its unchanged characteristics, we can identify whether the VMs are built on the specific host.

TABLE2: HARDWARE TRACKING INFORMATION

feature / host	Public IP	Intranet IP network	Battery Info
Host	111.154.89.xx	192.168.136.1(host)‖192.168.136.131; 192.168.232.1(host)‖192.168.232.138	Yes‖0.58‖00:37‖5:24
VM1	48.36.191.xxx	192.168.136.1‖192.168.136.131(host)	Yes‖0.58‖00:37‖5:24
VM2	48.36.191.xxx	192.168.232.1‖192.168.232.138(host)	Yes‖0.58‖00:37‖5:24

As can be seen from the intranet IP network shown in Table2, all the VMs' IP address can be scanned in the host, and the VMs also hold the respective IP information. Moreover, attackers may use the same IP springboard in different VMs. By comparing the information of IP information and Battery Info, we can associate the VM with host, and correlate the multi VMs which based on the same host.

IV. CONSOLUSION

This poster has proposed a technology of tracking VM attackers based on browser fingerprinting, which can effectively associate the VM and host together by updated browser fingerprinting and hardware level tracking technologies. We will continuously explore about the hardware level features in the next step, expecting to achieve the goal of cross-browser tracking of VM attackers.

V. ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their helpful comments for improving this paper. This work is supported by the Ministry of Science and Technology of China (No. 2016QY08D1602).

REFERENCES

[1] Eckersley P. How unique is your web browser?[C]//International Symposium on Privacy Enhancing Technologies Symposium. Springer Berlin Heidelberg, 2010: 1-18.

[2] Liu X, Liu Q, Wang X, et al. Fingerprinting Web Browser for Tracing Anonymous Web Attackers[C]//Data Science in Cyberspace (DSC), IEEE International Conference on. IEEE, 2016: 222-229.

[3] Yan: Weird New Tricks for Browser Fingerprinting https://zyan.scripts.mit.edu/presentations/toorcon2015.pdf

[4] L. Olejnik, G. Acar, C. Castelluccia, and C. Diaz. The leaking battery. Cryptology ePrint Archive, Report 2015/616, 2015.