SPRINGER BRIEFS IN COMPUTER SCIENCE

Xinyuan Wang
Douglas Reeves

Traceback and Anonymity

Springer

SpringerBriefs in Computer Science

More information about this series at http://www.springer.com/series/10028

Xinyuan Wang • Douglas Reeves

Traceback and Anonymity

Springer

Xinyuan Wang
Department of Computer Science
George Mason University
Fairfax, VA, USA

Douglas Reeves
Department of Computer Science
North Carolina State University
Raleigh, NC, USA

ISSN 2191-5768 ISSN 2191-5776 (electronic)
SpringerBriefs in Computer Science
ISBN 978-1-4939-3439-3 ISBN 978-1-4939-3441-6 (eBook)
DOI 10.1007/978-1-4939-3441-6

Library of Congress Control Number: 2015953645

Springer New York Heidelberg Dordrecht London

Printed on acid-free paper

Springer Science+Business Media LLC New York is part of Springer Science+Business Media (www.springer.com)

Contents

Chapter 1
Introduction

Cyber attack has become a top threat to our society. With more than one billion hosts [2] connected to the Internet, our society is becoming increasingly dependent on the Internet. Now the perpetrators have plenty choices of potential targets and they could attack the chosen Internet hosts from virtually anywhere in the world and cause damages to the victims.

For example, NASA has been under repeated attacks in the past few years, and its Jet Propulsion Lab has been found compromised [43]. In the recent data breach attack on Target, 40 million customers' credit and debit card information was stolen. In the recent cyber attack on Home Depot, 56 million shoppers' credit card information was compromised. A recent survey [62] showed that "the annual average cost per company of successful cyber attacks increased to $20.8 million in financial services, $14.5 million in the technology sector, and $12.7 million in communications industries."

In certain cases, cyber attacks could even cause the victim out of business. In June 2011, attackers compromised the information system of Dutch certificate authority DigiNotar, and generated over 500 fraudulent security certificates for high-profile Web sites such as Google, Facebook, Twitter, Microsoft and Skype. Such forged certificates could be used to impersonate Websites and intercept user information. A few monthly later, DigiNotar filed bankruptcy after the news broke about the security breach [40].

Besides financial motivations, cyber attacks such as hacktivism can be politically motivated. For example, it has been reported [41] that hackers have targeted bankers' personal data as a way to support the "Occupy Wall Street" movement. McAfee Predicted [42] that there will more such Hacktivism in 2012.

One major contributor to such growing threat of network-based attacks is the lack of attack attribution. Unlike the telephone systems, the Internet was never designed for tracking and tracing users' behavior. Most existing network security mechanisms such as firewalls [31], IPSEC [25] and IDS [5, 22] are focused on intrusion prevention and detection. However, even the perfect intrusion detection

X. Wang, D. Reeves, *Traceback and Anonymity*, SpringerBriefs
in Computer Science, DOI 10.1007/978-1-4939-3441-6_1

will not be able to tell where the detected attacks come from. What is missing from existing network security mechanisms is an effective way to identify network based intruders and hold them accountable for their intrusions.

Without effective intrusion source tracing and identification, those network based intruders have all the potential gains with virtually no risk of being caught. On the other hand, an effective and accurate attack tracing capability helps to eliminate network based attack from its root by identifying and catching those perpetrators responsible for the attack. From the attacker's point of view, if the risk of being caught and the consequent penalty are high enough compared with the potential gain of network based attack, he or she would be reluctant to attack again. Thus even an imperfect attack tracing capability could help to repel potential future attacks.

Because of the current Internet architecture, it is much easier for network based attackers to conceal their origin than for defenders to trace and identify their origin. To avoid being identified and tracked, attackers use all kinds of techniques to evade detection [37] and tracking. One common technique to conceal the attack source is to launder the attack through hosts of third party. Recent trend of cloud computing enables attackers to launch attacks from rented hosts from cloud provider. Specifically, recent attack on Sony's Playstation Network used rented hosts in Amazon EC2 [44]. All these would make it harder for the attack victim to find out the true source of the attacker after identifying the attack. Consequently, there is a pressing need to develop a capability for identifying the source of detected attacks. Network based attack can not be effectively repelled or eliminated until its source is known.

Besides the needs of traceback, there are legitimate reasons to keep certain online activities anonymous. For example, to encourage candid expression of opinions, an online survey may want to keep each response anonymous. In addition, people may want to keep their online activities private and do not want others know from where they browse the Internet and what web sites they visit. To help provide the anonymity and privacy to certain online activities, various anonymity systems have been developed and deployed. Specifically, Tor [17] and Anonymizer [3] use intermediate proxies and encryption to anonymize user's internet traffic.

The goal of anonymity system is exactly the opposite to that of traceback in that it aims to remove or conceal the true identity of the user or his/her Internet activity. While anonymity system helps protect the privacy and anonymity of legitimate online activities, they can also be abused by perpetrators to disguise the source of their attacks. For example, attackers can easily launder their attacks through low-latency anonymous network such as Tor, anonymizer before attacking the final targets. Therefore, it is necessary to understand how effective existing anonymity techniques are and whether we can "break" through existing anonymity systems in order to trace the attackers behind anonymity systems.

In this paper, we want to leave the controversy about the traceback and anonymity aside, and focus on the technical aspects of achieving traceback and anonymity. Specifically, we want to investigate the interaction between traceback and anonymity, and we want to understand the fundamental limitation of both traceback and low-latency anonymity systems.