Journal of Network and Computer Applications 48 (2015) 44–57

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review

# Man-At-The-End attacks: Analysis, taxonomy, human aspects, motivation and future directions

Adnan Akhunzada [a,*], Mehdi Sookhak [a], Nor Badrul Anuar [a], Abdullah Gani [a], Ejaz Ahmed [a], Muhammad Shiraz [a], Steven Furnell [b], Amir Hayat [c], Muhammad Khurram Khan [d]

[a] *Centre for Mobile Cloud Computing Research (C4MCCR), Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia*
[b] *Information Security & Network Research Group, School of Computing, Communications and Electronics, University of Plymouth, Plymouth, United Kingdom*
[c] *Applied Security Engineering Research Group, Dept. of Computer Science, COMSATS Institute of Information Technology, Pakistan*
[d] *Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia*

## ARTICLE INFO

*Article history:*
Received 26 May 2014
Received in revised form
8 October 2014
Accepted 23 October 2014
Available online 11 November 2014

*Keywords:*
Man-At-The-End
Software protection
Information security
Digital rights management
Digital assets
Distributed software systems

## ABSTRACT

Man-At-The-End (MATE) attacks and fortifications are difficult to analyze, model, and evaluate predominantly for three reasons: firstly, the attacker is human and, therefore, utilizes motivation, creativity, and ingenuity. Secondly, the attacker has limitless and authorized access to the target. Thirdly, all major protections stand up to a determined attacker till a certain period of time. Digital assets range from business to personal use, from consumer devices to home networks, the public Internet, the cloud, and the Internet of Things – where traditional computer and network security are inadequate to address MATE attacks. MATE is fundamentally a hard problem. Much of the extant focus to deal with MATE attacks is purely technical; though security is more than just a technical issue. The main objective of the paper is to mitigate the consequences of MATE attacks through the human element of security and highlight the need for this element to form a part of a holistic security strategy alongside the necessary techniques and technologies. This paper contributes by taking software protection (SP) research to a new realm of challenges. Moreover, the paper elaborates the concept of MATE attacks, the different forms, and the analysis of MATE versus insider threats to present a thematic taxonomy of a MATE attack. The ensuing paper also highlights the fundamental concept of digital assets, and the core protection mechanisms and their qualitative comparison against MATE attacks. Finally, we present state-of-the-art trends and cutting-edge future research directions by taking into account only the human aspects for young researchers and professionals.

**Contents**

[*] Corresponding author. Tel.: +60 1116431032; fax: +60 379579249.
*E-mail addresses:* a.adnan@siswa.um.edu.my (A. Akhunzada), m.sookhak@ieee.org (M. Sookhak), badrul@um.edu.my (N.B. Anuar), abdullahgani@ieee.org (A. Gani), imejaz@siswa.um.edu.my (E. Ahmed), muh_shiraz@um.edu.my (M. Shiraz), sfurnell@plymouth.ac.uk (S. Furnell), amir.hayat@comsats.edu.pk (A. Hayat), mkhurram@ksu.edu.sa (M. Khurram Khan).

http://dx.doi.org/10.1016/j.jnca.2014.10.009
1084-8045/© 2014 Elsevier Ltd. All rights reserved.

## 1. Introduction

Any security system, no matter how intelligent, well-designed, properly configured, thoroughly deployed, and meticulously maintained, will have to rely on people. The most stimulating and overarching issue in security is the human element – and dealing with it is perhaps one of the biggest challenges we face today. Trying to design information security solutions without due consideration of the complex human nature may prove to be an Achilles heel, "If the human factor is not considered, information security might be just an illusion" (Svensson, 2013). Technological advancements and innovations make the armory more and more impressive, but according to Schneier a high degree of security is in our hands. He further argues that if you think technology can resolve your security problems, then you neither understand the problems nor the technology (Frangopoulos et al., 2013). Despite the implied focus on technology, it is increasingly recognized that mere technology cannot provide a complete solution; however, what has only started receiving extensive recognition relatively recently is the role and importance of people as part of the solution (Furnell and Clarke, 2012).

Despite technological progression, the problem of Man-At-The-End (MATE) attacks is primarily harder (and, under very general circumstances, difficult to resolve) than other, more common studied problems in security. The reason behind this is the very liberal attack model that software protection (SP) researchers and practitioners must cope with: it is presumed that an all-powerful adversary who has complete access to our software and hardware, can examine, utilize his or her capabilities, modify, and probe it at will (Ceccato et al., 2013; Falcarin et al., 2011; Gu et al., 2011). Fundamentally, a MATE attack happens in a setting where an adversary gains physical access to a device and compromises it by tampering or inspecting the hardware itself or the software it contains (Jakubowski et al., 2011). MATE attacks, therefore, essentially encompass an adversary gaining an advantage by violating software or hardware under their control, directly or via a remote connection also known as Remote Man-At-The-End (RMATE) (Collberg, 2011; Collberg et al., 2011). Protection mechanisms against MATE attacks are recognized as anti-tamper techniques, digital asset protection, or, more commonly, software protection (Falcarin et al., 2011).

Due to the powerful attacks launched in a MATE scenario, we typically do not expect any technique in SP to hold off an attack for an indefinite period of time (Collberg et al., 2011). Subsequently, no piece of software, no matter how well protected, is likely to survive unscathed for a long period of time. However, an attractive opportunity for MATE attackers is, in fact, today's open environments, where the attackers prey on every single line of code, and commercial off-the-shelf systems include a plenitude of unpatched and known software vulnerabilities (Broadhurst and Chang, 2013). Moreover, in this dynamic world where digital content mainly relies on software for its storage, consumption, creation, and distribution, it is becoming an essential obligation that we protect digital assets by continuously upgrading the protections in their associated software. However, today, an increasing number of applications are vulnerable to MATE attacks, and there is a need for comprehensive SP techniques that deliver a nontrivial level of security against determined attacks by skilled adversaries (Jakubowski et al., 2011). Besides, firewalls are classic solutions to mitigate the threat of remote attackers (i.e., Man-In-The-Middle) who try to break into software systems; however, these typical approaches do not help in defending software systems when the attacker is MATE (Ceccato et al., 2013) and it is equally hard to define and measure the MATE attacker's capabilities (Collberg et al., 2011; Falcarin et al., 2011).

The literature available on MATE is very limited. To the best of our knowledge, this is the first effort that studies MATE in detail. The paper elaborates the concept of MATE attacks, its different forms, and its analysis and characteristics. Moreover, we devise MATE attacks taxonomy by critically analyzing and reviewing the previous taxonomies in different fields of information systems and security. Furthermore, we present three elements in properly securing digital assets, i.e., SP, hardware-based software protection and MATE. However, the bygones of SP research are only based on two elements: hardware and, software-based protection, and some of the latest experts' opinions put forward the co-design of hardware and software (Gu et al., 2011), where MATE assessment has been addressed indirectly. Directly addressing the MATE, however, in the security chain has largely been neglected. The paper highlights the need for human aspects to form part of a holistic security strategy alongside the necessary techniques and technologies in SP research. The paper elaborates the concepts of digital assets and review efforts that endeavor to mitigate MATE attack consequences. MATE attacks and their role and effectiveness on high-value digital assets are studied. We contribute by taking SP research to a whole new realm of challenges and present the state-of-the-art trends and future directions that researchers should explore while addressing MATE attacks. These novel directions directly take into account the human aspects, i.e., mental capabilities, skills and expertise, different security-related and cross-cultural behaviors, curiosity, fear, direct MATE aspects on software resilience, and finding the actual behavior of MATE. Exploring these future research challenges could have a high impact and provide greater insight into properly addressing MATE attacks. This in turn enhances the defense capabilities of high-value digital assets with improved extant techniques and leads to innovate and develop state-of-the-art next-generation security tools and technologies (to properly secure distributed software systems and digital assets).

The remainder of this paper is organized as follows. Section 2 describes MATE attacks in details, which includes the concept of MATE attacks, the different forms, and the characteristics and analysis of MATE versus insider threats. Critical analysis and a comprehensive taxonomy of MATE attacks are also devised in this section. Section 3 elaborates the fundamental concept of digital assets; the core protection mechanisms and their qualitative comparison against MATE