When Human Cognitive Modeling Meets PINs: User-Independent Inter-Keystroke Timing Attacks

Ximing Liu, Yingjiu Li, Robert H. Deng, Shujun Li, Bing Chang

PII:	S0167-4048(18)30273-6
DOI:	https://doi.org/10.1016/j.cose.2018.09.003
Reference:	COSE 1394

To appear in: *Computers & Security*

Received date:	28 March 2018
Revised date:	20 August 2018
Accepted date:	16 September 2018

Please cite this article as: Ximing Liu, Yingjiu Li, Robert H. Deng, Shujun Li, Bing Chang, When Human Cognitive Modeling Meets PINs: User-Independent Inter-Keystroke Timing Attacks, *Computers & Security* (2018), doi: https://doi.org/10.1016/j.cose.2018.09.003

When Human Cognitive Modeling Meets PINs: User-Independent Inter-Keystroke Timing Attacks

Ximing Liu[1], Yingjiu Li[1], Robert H. Deng[1], Shujun Li[2], Bing Chang[3]
[1]School of Information Systems, Singapore Management University, Singapore
[2]Department of Computer Science, University of Surrey, UK
xmliu.2015, yjli, robertdeng, bingchang@smu.edu.sg; shujun.li@surrey.ac.uk

ABSTRACT

This paper proposes the first user-independent inter-keystroke timing attacks on PINs. Our attack method is based on an inter-keystroke timing dictionary built from a human cognitive model whose parameters can be determined by a *small* amount of training data on any users. Our attacks can thus be potentially launched in a large scale in real-world settings. We investigate inter-keystroke timing attacks in different online attack settings and evaluate their performance on PINs at different strength levels. Our experimental results show that the proposed attack performs significantly better than random guessing attacks. We further demonstrate that our attacks pose a serious threat to real-world applications and propose various ways to mitigate the threat.

Keywords

PIN, Authentication, Human Cognitive Model, Timing Attack, Human Behavior, Keystroke Dynamics

1. INTRODUCTION

Inter-keystroke timing attacks, which make use of the leaked keystroke timing information to infer a user's PIN, pose a serious threat to real-world applications, especially for online financial services whose authentication systems are based on PINs. Such attacks have triggered increasing interests in recent years due to the development of many practical approaches to obtaining users' keystroke timing information via different side channels, including CPU cache [29, 42, 47, 28, 36], shared event loops [64], I/O interrupts [19, 35, 76], and SSH [55]. Some approaches do not even require attackers to be physically close to victims or install malware on victims' devices, which significantly lower the barrier for launching inter-keystroke timing attacks in real-world scenarios.

Most of the existing inter-keystroke timing attacks on PINs or passwords are user-dependent. Since the seminal work published by Dawn Song et al. in 2001 [55], the Hidden Markov Model (HMM) has been exploited as a major technique to launching the inter-keystroke timing attacks [76, 32]. However, HMM is user-specific in a sense that it relies on the distribution of inter-keystroke times of a specific user typing each possible key pair (which represents a hidden state in HMM) so as to infer the user's PIN from the user's inter-keystroke timing information about a PIN entry. In other words, HMM requires that a sufficiently large amount of time intervals for each possible key pair that can be part of any PIN be typed by a specific user for model training so as to make the attacks to that specific user's PIN entry accurate and useful. It is usually difficult for an attacker to collect such large amount of inter-keystroke data about a victim before launching an effective attack. Even if it is possible, such attacks are not scalable. If an attacker intends to compromise a new victim, he/she needs to collect the new victim's inter-keystroke timing data about all possible key pairs and retrain his/her HMM for the new victim. In addition, the success rate of such attacks is too low to be practical in online attack settings since the number of guesses that is allowed to launch an online attack is usually restricted to small numbers (e.g., 3, 10, 100) in common practice.

In this paper, we propose a user-independent approach to exploit inter-keystroke timing information for PIN inference, which makes inter-keystroke timing attacks much more scalable and practical. The model in our attacks is not user specific, which can be trained from a small amount of training data (e.g., a few key pairs instead of all possible key pairs) about *any* users (e.g., attackers or people recruited by attackers) instead of the target victims. In addition, our approach can be applied to attack *any* new victim without retraining the model. The success rate of our attacks is significantly higher than random guessing attacks, which poses a serious threat when applied to users in a large scale, even in online attack settings.

Our proposed approach leverages a human cognitive model to capture the common characteristics across *all* skilled users typing PINs. The human cognitive model is derived from several PIN typing behavioral phenomena which we summarize from the cognitive psychology literature. These PIN typing behavioral phenomena are universal to *all* skilled users. The parameters of our cognitive model can be estimated by a few key pairs from any user such as the attacker himself. Once the cognitive model is built, it can be used to attack any user inputting any PIN on a particular keypad whose geometric measurement is known.

At a high level, our attacks proceed as follows. First, an attacker builds a timing dictionary including all possible PINs and their corresponding timing sequences. The timing sequence of each PIN is derived from our cognitive model. Second, the attacker obtains the timing sequence of a victim's PIN entry via various side-channels (e.g., CPU cache, shared event loops, I/O interrupts, and SSH). Third, the attacker measures the cosine similarity between the observed inter-keystroke timing sequence and each entry in the timing dictionary and ranks all candidate PINs in the dictionary by their similarity values. Lastly, with a ranked list of candidate PINs, the attacker may launch online attacks using the PINs successively from the ranked list until he/she succeeds or the target account is locked (or the attacker aborts before the account is locked).

Besides the cognitive model that captures the common characteristics across all users typing PINs, another contributing factor