PILOT: Password and PIN information leakage from obfuscated typing videos[1]

Article type: Research Article

Authors: Balagani, Kiran (https://content.iospress.com:443/search?q=author%3A%28%22Balagani, Kiran%22%29)[a; 2] | Cardaioli, Matteo (https://content.iospress.com:443/search?q=author%3A%28%22Cardaioli, Matteo%22%29)[b; d; *] | Conti, Mauro (https://content.iospress.com:443/search?q=author%3A%28%22Conti, Mauro%22%29)[b] | Gasti, Paolo (https://content.iospress.com:443/search?q=author%3A%28%22Gasti, Paolo%22%29)[a] | Georgiev, Martin (https://content.iospress.com:443/search?q=author%3A%28%22Georgiev, Martin%22%29)[c; 3] | Gurtler, Tristan (https://content.iospress.com:443/search?q=author%3A%28%22Gurtler, Tristan%22%29)[a; 4] | Lain, Daniele (https://content.iospress.com:443/search?q=author%3A%28%22Lain, Daniele%22%29)[b; 5] | Miller, Charissa (https://content.iospress.com:443/search?q=author%3A%28%22Miller, Charissa%22%29)[a; 6] | Molas, Kendall (https://content.iospress.com:443/search?q=author%3A%28%22Molas, Kendall%22%29)[a] | Samarin, Nikita (https://content.iospress.com:443/search?q=author%3A%28%22Samarin, Nikita%22%29)[a; 7] | Saraci, Eugen (https://content.iospress.com:443/search?q=author%3A%28%22Saraci, Eugen%22%29)[b] | Tsudik, Gene (https://content.iospress.com:443/search?q=author%3A%28%22Tsudik, Gene%22%29)[c] | Wu, Lynn (https://content.iospress.com:443/search?q=author%3A%28%22Wu, Lynn%22%29)[a; 8]

Affiliations: [a] New York Institute of Technology, USA | [b] University of Padua, Italy | [c] University of California, Irvine, USA | [d] GFT Italy, Italy

Correspondence: [*] Corresponding author. E-mail: matteo.cardaioli@gmail.com (mailto:matteo.cardaioli@gmail.com).

Note: [1] Submitted to the ESORICS 2018 special issue.

Note: [2] Authors are listed in alphabetical order.

Note: [3] Current affiliation: University of Oxford.

Note: [4] Current affiliation: University of Illinois at Urbana-Champaign.

Note: [5] Current affiliation: ETH Zurich.

Note: [6] Current affiliation: Rochester Institute of Technology.

Note: [7] Current affiliation: University of California, Berkeley.

Note: [8] Current affiliation: Bryn Mawr College.

Abstract: This paper studies leakage of user passwords and PINs based on observations of typing feedback on screens or from projectors in the form of masked characters (∗ or ·) that indicate keystrokes. To this end, we developed an attack called Password and Pin Information Leakage from Obfuscated Typing Videos (PILOT). Our attack extracts inter-keystroke timing information from videos of password masking characters displayed when users type their password on a computer, or their PIN at an ATM. We conducted several experiments in various attack scenarios. Results indicate that, while in some cases leakage is minor, it is quite substantial in others. By leveraging inter-keystroke timings, PILOT recovers 8-character alphanumeric passwords in as little as 19 attempts. When guessing PINs, PILOT significantly improved on both random guessing and the attack strategy adopted in our prior work (In European Symposium on Research in Computer Security (2018) 263–280 Springer). In particular, we were able to guess about 3% of the PINs within 10 attempts. This corresponds to a 26-fold improvement compared to random guessing. Our results strongly indicate that secure password masking GUIs must consider the information leakage identified in this paper.

Keywords: Authentication, information leakage, shoulder-surfing attacks, PIN inference, password inference

DOI: 10.3233/JCS-191289

Journal: Journal of Computer Security (https://content.iospress.com:443/journals/journal-of-computer-security), vol. 27, no. 4, pp. 405-425, 2019

Published: 18 July 2019

Price: EUR 27,50