

Anti-RAPTOR: Anti Routing Attack on Privacy for a Securer and Scalable Tor

Nguyen Phong HOANG, Yasuhito ASANO, Masatoshi YOSHIKAWA

Department of Social Informatics, Graduate School of Informatics, Kyoto University, Japan

hoang.nguyenphong.jp@ieee.org, asano@i.kyoto-u.ac.jp, yoshikawa@i.kyoto-u.ac.jp

Abstract—Regardless of Tor’s robustness against individual attackers thanks to its distributed characteristics, the network is still highly vulnerable to those very powerful adversaries, such as oppressive regimes which have control over a large proportion of the Internet. As recently confirmed by Edward Snowden, Autonomous-System level adversary is no longer theoretical, but poses a real danger to the Tor network. Therefore, through this research, we strive to propose an improved design in Tor to against the most contemporary de-anonymizing attack techniques, especially RAPTOR: Routing Attacks on Privacy in Tor. Different from most previous works, the scalability aspect of the overall Tor network is also taken into consideration in this study since the number of both end users and voluntary relays is foreseen to keep increasing in the next coming years. To against RAPTOR, we suggest that an Internet AS-level topology file should be periodically maintained and distributed by Directory Authorities. The file is only fetched by the guard and exit relays in addition to the conventional consensus network status document to preserve the scalability of the network. The user then decides to initiate her anonymous circuit based on the result of the intersection between two sets of ASes: the set of ASes between *the user and the guard relay*, and the set of ASes between *the exit relay and the final destination*. The paper concludes by summarizing pros and cons of the proposed design from various points of view including the Directory Authorities, the voluntary relays and the end users; and suggesting future works that are necessary for a state-of-the-art anonymity technique.

Keyword—About Privacy, Anonymous Communication, Tor, Autonomous System



Nguyen Phong HOANG was born in Tien Giang Province, Vietnam in 1992. He received his undergraduate degree in Business Administration majoring in Information & Communications technology (ICT) from Ritsumeikan Asia Pacific University, Japan. He is presently pursuing his graduate studies at the Graduate School of Informatics at Kyoto University in Japan. His research interests include information security, privacy and anonymous communication. He hopes to advance his research on TOR (The Onion Router), one of the most robust anonymous tools, during his graduate studies. He participated in the 16th International Conference on Advanced Communication Technology and received Outstanding Paper Award from the Conference. He has been an IEEE member since 2013.



Prof. Yasuhito ASANO received the BS, MS, and DS degrees in information science, the University of Tokyo in 1998, 2000, and 2003, respectively. In 2003-2005, he was a research associate in the Graduate School of Information Sciences, Tohoku University. In 2006-2007, he was an assistant professor in the Department of Information Sciences, Tokyo Denki University. He joined Kyoto University in 2008, and he is currently an associate professor in the Graduate School of Informatics. His research interests include web mining, network algorithms. He is a member of the IEICE, IPSJ, DBSJ, and OR Soc. Japan.



Prof. Masatoshi YOSHIKAWA received the BE, ME, and PhD degrees from the Department of Information Science, Kyoto University, in 1980, 1982, and 1985, respectively. From 1985 to 1993, he was with Kyoto Sangyo University. In 1993, he joined the Nara Institute of Science and Technology as an associate professor in the Graduate School of Information Science. From April 1996 to January 1997, he was in the Department of Computer Science, University of Waterloo as a visiting associate professor. From June 2002 to March 2006, he served as a professor at Nagoya University. From April 2006, he has been a professor at Kyoto University. His current research interests include database technologies and their application to medical and healthcare domains. He is a member of the ACM and IPSJ.