Automated Attack Discovery in TCP Congestion Control Using a Model-guided Approach

Samuel Jero
Purdue University
sjero@purdue.edu

Endadul Hoque
Florida International University
ehoque@fiu.edu

David Choffnes
Northeastern University
choffnes@ccs.neu.edu

Alan Mislove
Northeastern University
amislove@ccs.neu.edu

Cristina Nita-Rotaru
Northeastern University
c.nitarotaru@neu.edu

ABSTRACT

In this work, we propose an automated method to find attacks against TCP congestion control implementations that combines the generality of implementation-agnostic fuzzing with the precision of runtime analysis. It uses a model-guided approach to generate abstract attack strategies by leveraging a state machine model of congestion control to find vulnerable state machine paths that an attacker could exploit to increase or decrease the throughput of a connection. These abstract strategies are then mapped to concrete attack strategies, which consist of sequences of actions such as injection or modification of acknowledgements. We design and implement a virtualized platform, TCPwn, that consists of a proxy-based attack injector to inject these concrete attack strategies. We evaluated 5 TCP implementations from 4 Linux distributions and Windows 8.1. Overall, we found 11 classes of attacks, of which 8 are new.

ACM Reference Format:

Samuel Jero, Endadul Hoque, David Choffnes, Alan Mislove, and Cristina Nita-Rotaru. 2018. Automated Attack Discovery in TCP Congestion Control Using a Model-guided Approach. In *ANRW '18: Applied Networking Research Workshop, July 16, 2018, Montreal, QC, Canada*. ACM, New York, NY, USA, 1 page. <https://doi.org/10.1145/3232755.3232769>

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

ANRW '18, July 16, 2018, Montreal, QC, Canada

© 2018 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-5585-8/18/07.

<https://doi.org/10.1145/3232755.3232769>