

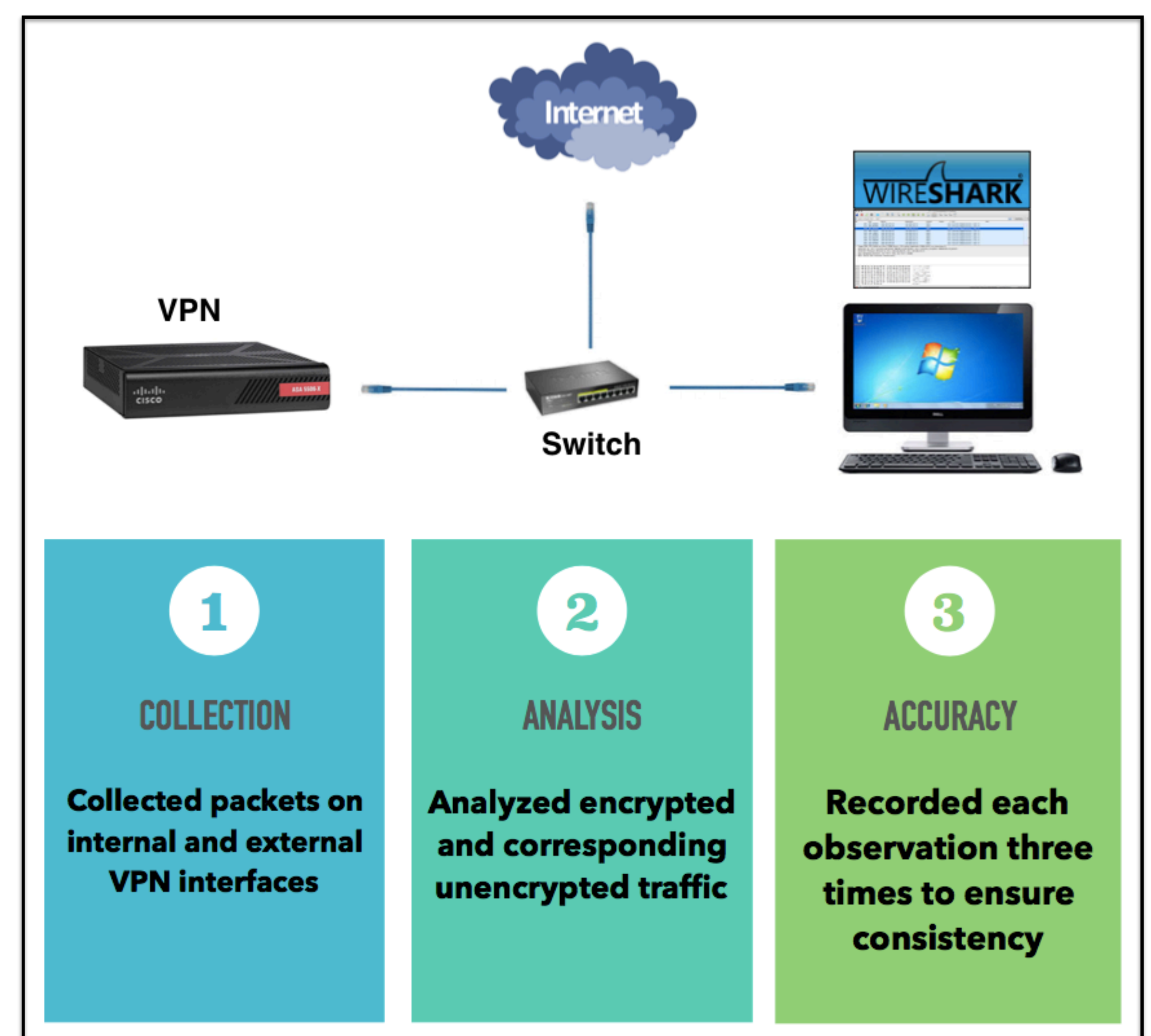
Information Leakage in a Cisco VPN Stream

Austin Klasa, Robert Morton, Daniel Sokoler
Professors: Dr. Melissa J. Dark, Dr. John A. Springer

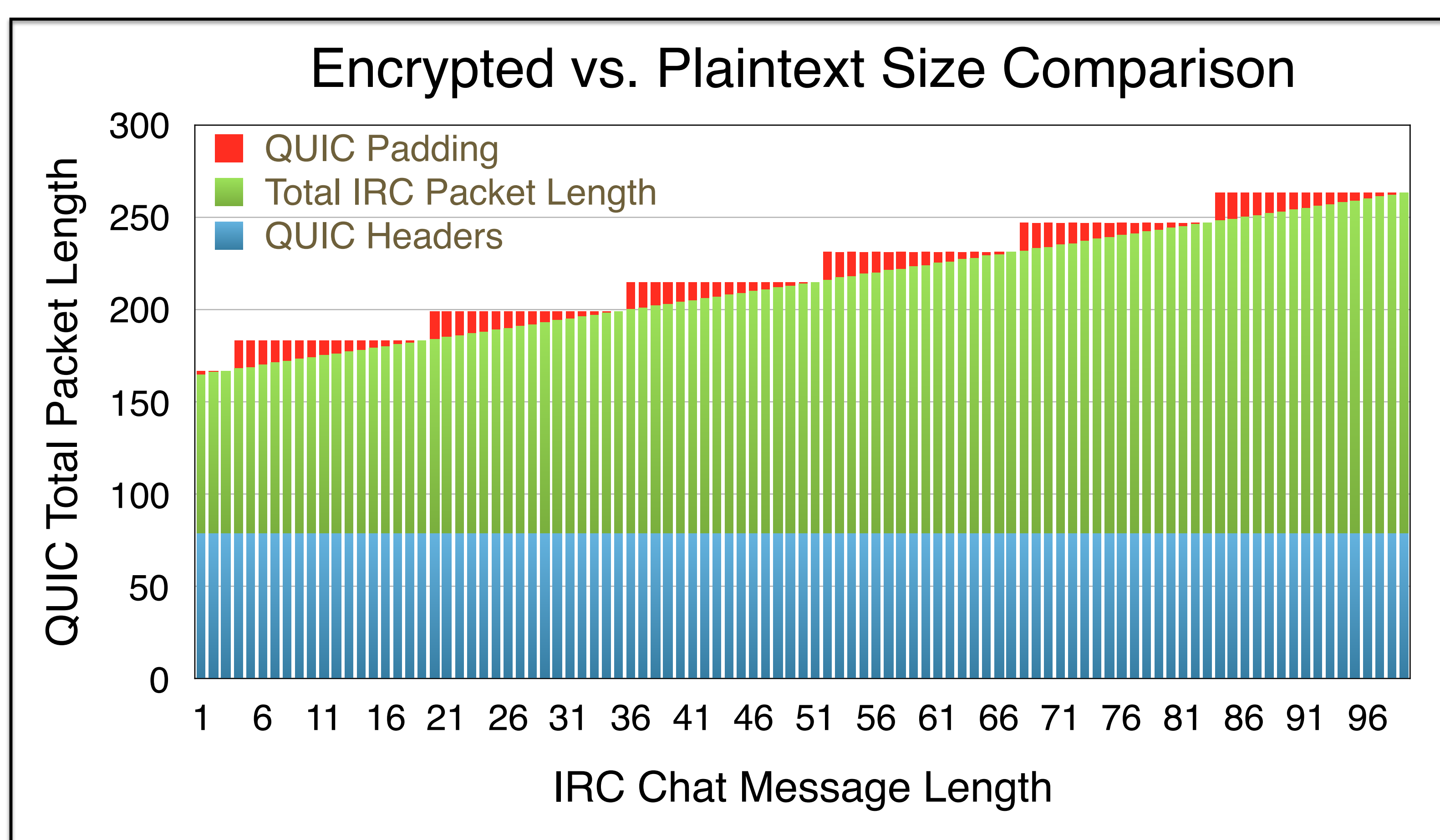
Abstract: This study investigated the phenomena of information leakage from encrypted traffic for a Cisco ASA 5506 Virtual Private Network (VPN)

Research Question: What information, if any, can be derived from an encrypted Cisco VPN stream by observing the source and destination Internet Protocol (IP) address, the protocol used, packet sizes, and time stamps?

Collection Method



Salient Results



Literature Review



Exposure of sensitive communications



This research is a part of the Information Security Research and Education (INSuRE) project. INSuRE is a partnership between successful and mature Centers of Academic Excellence in Information Assurance Research (CAE-R) and the National Security Agency (NSA), the Department of Homeland Security and other federal and state agencies and laboratories to design, develop and test a cybersecurity research network. INSuRE is a self-organizing, cooperative, multi-disciplinary, multi-institutional, and multi-level collaborative research project that can include both unclassified and classified research problems in cybersecurity.



This work was funded under NSF grants award No. 1344369 and No. 1027493.

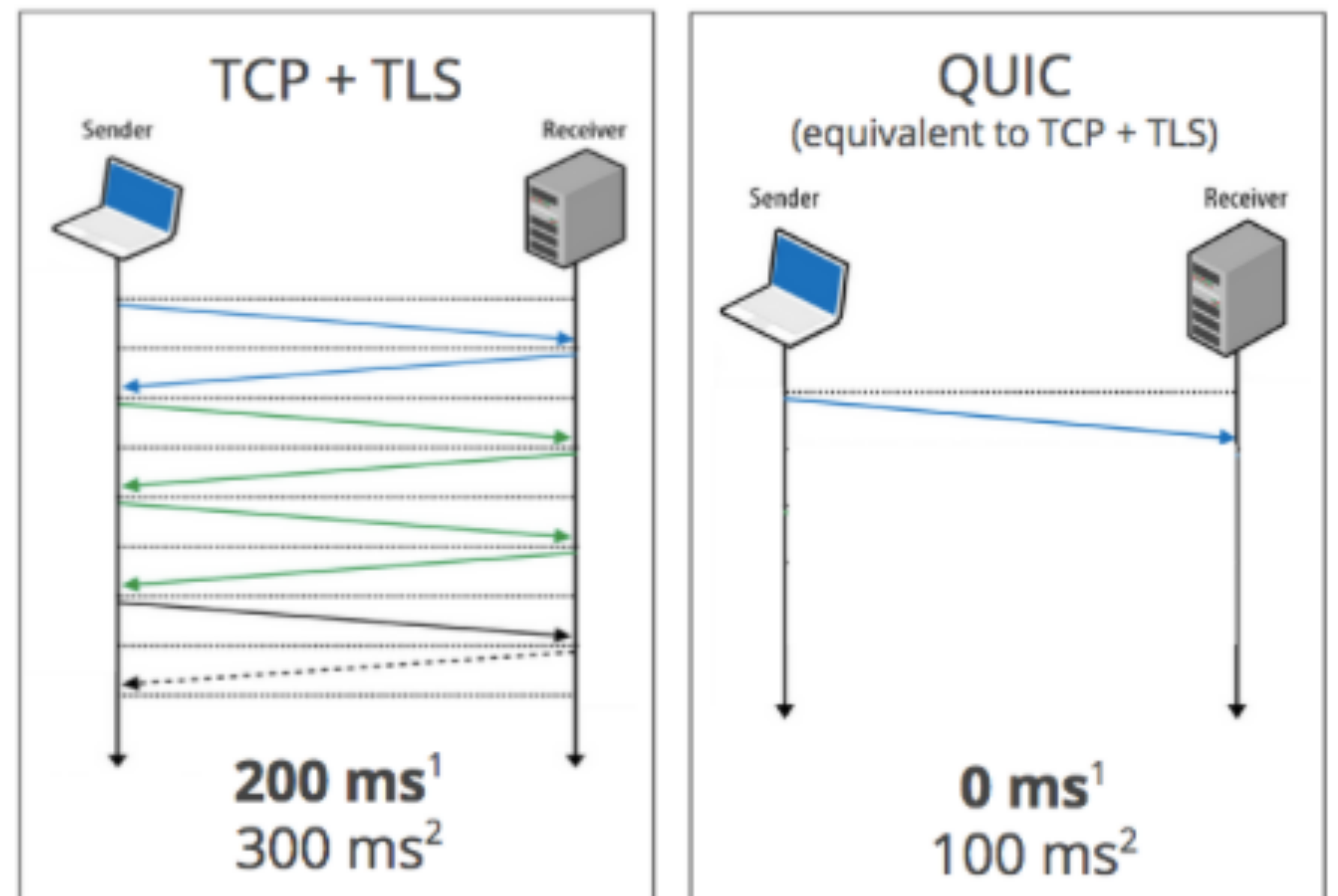


Information Leakage in a Cisco VPN Stream

Austin Klasa, Robert Morton, Daniel Sokoler
Professors: Dr. Melissa J. Dark, Dr. John A. Springer

QUIC

(Quick UDP Internet Connections, pronounced *quick*) is a protocol designed by Google, used by over 1 billion users worldwide, that **leaks the plaintext length**. If an eavesdropper observes the length of a password, the eavesdropper could use this information to successfully guess an individual's password.



RING-ROAD VULNERABILITY DISCLOSURE

The Ring-Road Bug is a serious vulnerability in transport security protocols that leaks the length of passwords allowing attackers to bypass user authentication. The Internet Engineering Task Force for HTTP/2 led by Google is working to create a patch to protect transport security protocols vulnerable to Ring-Road.



Future Work

Can we quantify the damage done by leaking the password length?

The authors wish to thank Mark Loepker, William Layton, Dr. Jeremiah Blocki, Dr. Eugene Spafford, Steven Frank and Adam Hammer.



This research is a part of the Information Security Research and Education (INSuRE) project. INSuRE is a partnership between successful and mature Centers of Academic Excellence in Information Assurance Research (CAE-R) and the National Security Agency (NSA), the Department of Homeland Security and other federal and state agencies and laboratories to design, develop and test a cybersecurity research network. INSuRE is a self-organizing, cooperative, multi-disciplinary, multi-institutional, and multi-level collaborative research project that can include both unclassified and classified research problems in cybersecurity.



This work was funded under NSF grants award No. 1344369 and No. 1027493.

