University of Glasgow

Secure Communications

Networked Systems (H) – Lecture 3

2019-2020

Colin Perkins | https://csperkins.org/ | Copyright © 2020 University of Glasgow | This work is licensed under the Creative Commons Attribution-NoDerivatives 4.0 International License.
To view a copy of this license, visit http://creativecommons.org/licenses/by-nd/4.0/ or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

Lecture Outline

- The Need for Secure Communications
- Principles of Secure Communication
- Transport Layer Security (TLS) v1.3
- Discussion

Colin Perkins | https://csperkins.org/ | Copyright © 2020 University of Glasgow

The Need for Secure Communications

- Network Traffic Monitoring
- Protecting Privacy
- Protecting Message Integrity
- Preventing Protocol Ossification

Colin Perkins | https://csperkins.org/ | Copyright © 2020 University of Glasgow

Numerous Organisations Monitor Internet traffic

- Governments, intelligence agencies, and law enforcement
  - Good reasons to monitor *some* traffic
  - Edward Snowden showed pervasive monitoring of *all* traffic
- Business “Your call may be monitored for quality and training purposes”
  - Regulatory requirements to record some traffic – e.g., banking
  - To profile customers for advertising
- Network operators
  - To support network operations and trouble-shooting
  - To profile customers for advertising
- Criminals and malicious users
  - Steal data and user credentials; identity theft; active attacks



Edward Snowden

S. Farrell and H. Tschofenig, “Pervasive Monitoring is an Attack”, IETF, May 2014, RFC 7258 https://tools.ietf.org/html/rfc7258

K. Moriarty and A. Morton, “Effect of Pervasive Encryption on Operators”, IETF, July 2018, RFC 8404 https://tools.ietf.org/html/rfc8404

G. Fairhurst and C. Perkins, “Considerations around Transport Header Confidentiality, Network Operations, and the Evolution of Internet Transport Protocols”, IETFJanuary 2020, Work in progress, https://datatracker.ietf.org/doc/draft-ietf-tsvwg-transport-encrypt/

Colin Perkins | https://csperkins.org/ | Copyright © 2020 University of Glasgow

Protecting Privacy

- Mechanisms that protect privacy against malicious attackers will also prevent benign monitoring
- No known way to stop criminals and malicious attackers from accessing private data that doesn't also stop law enforcement



Edward Snowden

S. Farrell and H. Tschofenig, "Pervasive Monitoring is an Attack", IETF, May 2014, RFC 7258 https://tools.ietf.org/html/rfc7258

K. Moriarty and A. Morton, "Effect of Pervasive Encryption on Operators", IETF, July 2018, RFC 8404 https://tools.ietf.org/html/rfc8404

G. Fairhurst and C. Perkins, "Considerations around Transport Header Confidentiality, Network Operations, and the Evolution of Internet Transport Protocols", IETFJanuary 2020, Work in progress, https://datatracker.ietf.org/doc/draft-ietf-tsvwg-transport-encrypt/

Colin Perkins | https://csperkins.org/ | Copyright © 2020 University of Glasgow

Protecting Message Integrity

- Numerous organisations may want to change messages in transit
  - Governments, intelligence agencies, and law enforcement
    - Many governments require ISPs to censor or modify DNS responses
    - Many governments require ISPs to censor messages containing certain content
  - Businesses and network operators
    - To enforce legal restrictions on content, terms of service, or to prevent copyright infringement
  - Criminals and malicious users
    - Phishing scams and identity theft
- Mechanisms to protect messages from malicious attackers also prevent benign actors
  - e.g., web browsers deploy DNS-over-HTTPS (DoH) to ensure integrity of DNS responses → protects against phishing attacks that modify DNS replies → stops ISPs modifying DNS responses to prevent access to domains hosting illegal material
- No technical way to distinguish beneficial integrity violations from malicious attacks

Colin Perkins | https://csperkins.org/ | Copyright © 2020 University of Glasgow

Preventing Protocol Ossification

- Network operators deploy **middleboxes** to monitor/modify traffic:
  - NATs, firewalls, monitors, traffic shaping, filtering, etc.
  - Some are necessary and beneficial, others perhaps less so
- Middleboxes must understand protocols used by the network traffic:
  - e.g., NAT has to know where to find IP addresses and ports in packets, if it is to translate them
  - e.g., traffic shapers, that limit TCP throughput for users exceeding their monthly bandwidth use cap, need to parse TCP packets and know how to change them to influence congestion control
- This can lead to **protocol ossification** – cannot change end-to-end protocols, because doing so interacts poorly with middleboxes that don't understand the changes



Is it Still Possible to Extend TCP?

Michio Honda[*], Yoshifumi Nishida[*], Costin Raiciu[†], Adam Greenhalgh[‡], Mark Handley[‡], Hideyuki Tokuda[*]

Keio University[*], Universitatea Politehnica Bucuresti[†], University College London[‡]

{micchie,nishida}@sfc.wide.ad.jp, costin.raiciu@cs.pub.ro

{a.greenhalgh,m.handley}@cs.ucl.ac.uk, hxt@ht.sfc.keio.ac.jp

ABSTRACT

We've known for a while that the Internet has ossified as a result of the race to optimize existing applications or enhance security. NATs, performance-enhancing-proxies, firewalls and traffic normalizers are only a few of the middleboxes that are deployed in the network and look beyond the IP header to do their job. IP itself can't be extended because "IP options are not an option" [10]. Is the same true for TCP?

In this paper we develop a measurement methodology for evaluating middlebox behavior relating to TCP extensions and present the results of measurements conducted from multiple vantage points. The short answer is that we can still extend TCP, but extensions' design is very constrained as it needs to take into account prevalent middlebox behaviors. For instance, absolute sequence numbers cannot be embedded in options, as middleboxes can rewrite ISN and preserve undefined options. Sequence numbering also must be consistent for a TCP connection, because many middleboxes only allow through contiguous flows.

We used these findings to analyze three proposed extensions to TCP. We find that MPTCP is likely to work correctly in the Internet or fallback to regular TCP. TcpCrypt seems ready to be deployed, however it is fragile if resegmentation does happen—for instance with hardware offload. Finally, TCP extended options in its current form is not safe to deploy.

Categories and Subject Descriptors

C.2.2 [**Computer-communication Networks**]: Network Protocols; C.2.6 [**Computer-communication Networks**]: Internetworking

General Terms

Measurement, Design, Experimentation, Standardization

Keywords

Middleboxes, Measurements, TCP, Protocol design

Permission to make digital or hard copies of all or part 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. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

IMC'11, November 2–4, 2011, Berlin, Germany.

Copyright 2011 ACM 978-1-4503-1013-0/11/11 ...$10.00.

1. INTRODUCTION

The Internet was designed to be extensible; routers only care about IP headers, not what the packets contain, and protocols such as IP and TCP were designed with options fields that could be used to add additional functionality. The great virtue of the Internet was always that it was *stupid*; it did no task especially well, but it was extremely flexible and general, allowing a proliferation of protocols and applications that the original designers could never have foreseen.

Unfortunately the Internet, as it is deployed, is no longer the Internet as it was designed. IP options have been unusable for twenty years[10] as they cause routers to process packets on their slow path. Above IP, the Internet has benefited (or suffered, depending on your viewpoint) from decades of optimizations and security enhancements. To improve performance [2, 7, 18, 3], reduce security exposure [15, 29], enhance control, and work around address space shortages [22], the Internet has experienced an invasion of middleboxes that *do* care about what the packets contain, and perform processing at layer 4 or higher *within* the network.

The problem now faced by designers of new protocols is that there is no longer a well defined or understood way to extend network functionality, short of implementing everything over HTTP[25]. Recently we have been working on adding both multipath support[11] and native encryption[5] to TCP. The obvious way to do this, in both cases, is to use TCP options. In the case of multipath, we would also like to stripe data across more than one path. At the end systems, the protocol design issues were mostly conventional. However, it became increasingly clear that no one, not the IETF, not the network operators, and not the OS vendors, knew what will and what will not pass through all the middleboxes as they are currently deployed and configured. Will TCP options pass unchanged? If the sequence space has holes, what happens? If a retransmission has different data than the original, which arrives? Are TCP segments coalesced or split? These and many more questions are crucial to answer if protocol designers are to extend TCP in a deployable way. Or have we already lost the ability to extend TCP, just like we did two decades ago for IP?

In this paper we present the results from a measurement study conducted from 142 networks in 24 countries, including cellular, WiFi and wired networks, public and private networks, residential, commercial and academic networks. We actively probe the network to elicit middlebox responses that violate the end-to-end transparency of the original Internet architecture. We focus on TCP, not only because it is by far the most widely used transport protocol, but also because while it is known that many middleboxes modify TCP behavior [6], it is not known how prevalent such middleboxes are, nor precisely what the *emergent behavior* is with TCP extensions that were unforeseen by the middlebox designers.

101

M. Honda, Y. Nishida, C. Raiciu, A. Greenhalgh, M. Handley, and H. Tokuda, "Is it still possible to extend TCP?", Proceedings of the ACM Internet Measurement Conference, Berlin, Nov. 2011. https://dx.doi.org/10.1145/2068816.2068834

- The more of a protocol that is encrypted, the easier it is to change – since middleboxes cannot understand or modify the data – but the harder it is for middleboxes to provide useful services

CC BY ND

Security and Policy

- Strong reasons to protect privacy, prevent modification in data in transit, and prevent protocol ossification
- The consequences of this protection are sometimes problematic
- Dialogue between engineers, protocol designers, operators, policy makers, and law enforcement crucial – to understand constraints and concerns



Keys Under Doormats:

MANDATING INSECURITY BY REQUIRING GOVERNMENT ACCESS TO ALL DATA AND COMMUNICATIONS

Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matthew Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Peter G. Neumann, Susan Landau, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, Daniel J. Weitzner

Abstract

Twenty years ago, law enforcement organizations lobbied to require data and communication services to engineer their products to guarantee law enforcement access to all data. After lengthy debate and vigorous predictions of enforcement channels "going dark," these attempts to regulate the emerging Internet were abandoned. In the intervening years, innovation on the Internet flourished, and law enforcement agencies found new and more effective means of accessing vastly larger quantities of data. Today we are again hearing calls for regulation to mandate the provision of exceptional access mechanisms. In this report, a group of computer scientists and security experts, many of whom participated in a 1997 study of these same topics, has convened to explore the likely effects of imposing extraordinary access mandates.

We have found that the damage that could be caused by law enforcement exceptional access requirements would be even greater today than it would have been 20 years ago. In the wake of the growing economic and social cost of the fundamental insecurity of today's Internet environment, any proposals that alter the security dynamics online should be approached with caution. Exceptional access would force Internet system developers to reverse "forward secrecy" design practices that seek to minimize the impact on user privacy when systems are breached. The complexity of today's Internet environment, with millions of apps and globally connected services, means that new law enforcement requirements are likely to introduce unanticipated, hard to detect security flaws. Beyond these and other technical vulnerabilities, the prospect of globally deployed exceptional access systems raises difficult problems about how such an environment would be governed and how to ensure that such systems would respect human rights and the rule of law.

H. Abelson, *et al.*, "Keys under doormats: Mandating insecurity by requiring government access to all data and communications", MIT Computer Science and Artificial Intelligence Lab, technical report MIT-CSAIL-TR-2015-026, July 2015. http://dspace.mit.edu/handle/1721.1/97690

Colin Perkins | https://csperkins.org/ | Copyright © 2020 University of Glasgow

The Need for Secure Communications

- Network Traffic Monitoring
- Protecting Privacy
- Protecting Message Integrity
- Preventing Protocol Ossification

Colin Perkins | https://csperkins.org/ | Copyright © 2020 University of Glasgow