University of Glasgow

Secure Communications

Networked Systems (H)

Lecture 3

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 – no reason to believe such monitoring has now stopped
- 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://datatracker.ietf.org/doc/rfc7258/

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

G. Fairhurst and C. Perkins, “Considerations around Transport Header Confidentiality, Network Operations, and the Evolution of Internet Transport Protocols”, IETF,July 2021, RFC 9065, https://datatracker.ietf.org/doc/rfc9065/

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://datatracker.ietf.org/doc/rfc7258/

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

G. Fairhurst and C. Perkins, "Considerations around Transport Header Confidentiality, Network Operations, and the Evolution of Internet Transport Protocols", IETF,July 2021, RFC 9065, https://datatracker.ietf.org/doc/rfc9065/

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

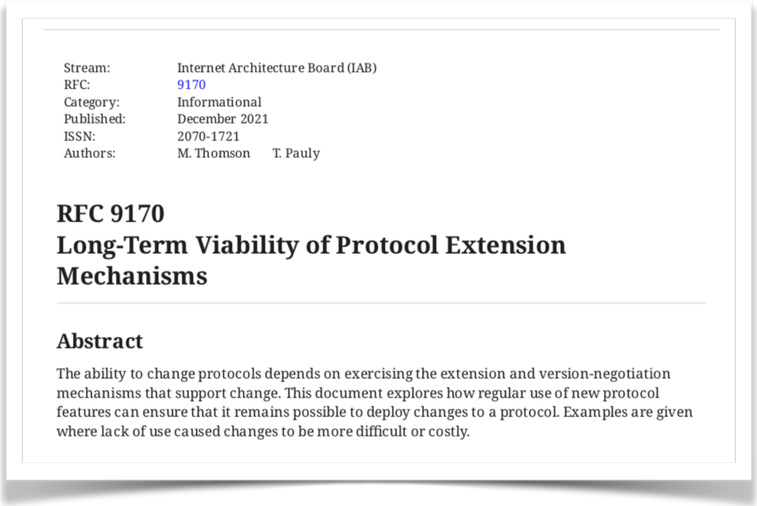
Protecting Message Integrity

- 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 and/or modify traffic:
  - NATs, firewalls, monitors, traffic shaping, filtering, etc.
  - Some are necessary and beneficial, others are less so
- Middleboxes must understand the protocols used:
  - 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
- 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



Stream: Internet Architecture Board (IAB)
RFC: 9170
Category: Informational
Published: December 2021
ISSN: 2070-1721
Authors: M. Thomson T. Pauly

RFC 9170
Long-Term Viability of Protocol Extension Mechanisms

Abstract

The ability to change protocols depends on exercising the extension and version-negotiation mechanisms that support change. This document explores how regular use of new protocol features can ensure that it remains possible to deploy changes to a protocol. Examples are given where lack of use caused changes to be more difficult or costly.

M. Thomson and T. Pauly, "Long-term Viability of Protocol Extension Mechanisms", Internet Architecture Board, December 2021, RFC 9170. https://datatracker.ietf.org/doc/rfc9170/

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

Security and Policy: Encryption and Key Escrow

- Strong reasons to protect privacy, prevent modification of data in transit, and prevent protocol ossification using end-to-end encryption and authentication
- But doing so can complicate the job of law enforcement and those performing legitimate network monitoring – numerous proposals for key escrow, targeted weakening of end-to-end encryption, and other forms of exceptional access
- 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

CC BY ND

Security and Policy: End-system Content Monitoring

- If data is encrypted end-to-end, protecting data in transit from malicious attacks, should law enforcement be able to monitor traffic at the end-points?
- Does the answer change if both end-points are personal devices vs. if one of the end-points is a data centre?
- How do the expectations for privacy, law enforcement access, and abuse protection differ between one-to-one conversations, group conversations, social networks, and other situations?



arXiv:2110.07450v1 [cs.CR] 14 Oct 2021

Bugs in our Pockets:
The Risks of Client-Side Scanning

Hal Abelson Ross Anderson Steven M. Bellovin
Josh Benaloh Matt Blaze Jon Callas Whitfield Diffie
Susan Landau Peter G. Neumann Ronald L. Rivest
Jeffrey I. Schiller Bruce Schneier Vanessa Teague
Carmela Troncoso

October 15, 2021

Executive Summary

Our increasing reliance on digital technology for personal, economic, and government affairs has made it essential to secure the communications and devices of private citizens, businesses, and governments. This has led to pervasive use of cryptography across society. Despite its evident advantages, law enforcement and national security agencies have argued that the spread of cryptography has hindered access to evidence and intelligence. Some in industry and government now advocate a new technology to access targeted data: *client-side scanning* (CSS). Instead of weakening encryption or providing law enforcement with backdoor keys to decrypt communications, CSS would enable on-device analysis of data in the clear. If targeted information were detected, its existence and, potentially, its source, would be revealed to the agencies; otherwise, little or no information would leave the client device. Its proponents claim that CSS is a solution to the encryption versus public safety debate: it offers privacy—in the sense of unimpeded end-to-end encryption—and the ability to successfully investigate serious crime.

In this report, we argue that CSS neither guarantees efficacious crime prevention nor prevents surveillance. Indeed, the effect is the opposite. CSS by its nature creates serious security and privacy risks for all society while the assistance it can provide for law enforcement is at best problematic. There are multiple ways in which client-side scanning can fail, can be evaded, and can be abused.

Its proponents want CSS to be installed on all devices, rather than installed covertly on the devices of suspects, or by court order on those of ex-offenders. But universal deployment threatens the security of law-abiding citizens as well as law-breakers. Technically, CSS allows end-to-end encryption, but this is moot if the

1

H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, J. Callas, W. Diffie, S. Landau, P. G. Neumann, R. Rivest, J. I. Schiller, B. Schneier, V. Teague, and C. Troncosco. “Bugs in our pockets: The risks of client-side scanning”. October 2021. https://arxiv.org/abs/2110.07450

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