Network Operation in an All-Encrypted World

John Mattsson, Ericsson Research

Abstract. In this position paper we give our view on Internet security and how strong end user protection should guide the use of security mechanisms. If the Internet community and the mobile industry cooperate to drive technologies that enable network management, content delivery, and value added services that work also in an all-encrypted world; we believe that an ecosystem where there is no tradeoff between end user privacy and quality of service is achievable.

Introduction

The mobile industry has a long history of promoting secure communication, including encryption of sensitive traffic. Mobile access networks encrypt all user data, and this protects both operators and their customers from various kinds of attacks. We believe that security and trusted relationships are opportunities for communication networks.

Public Wi-Fi networks are often not encrypted, meaning that attackers can easily take control of user accounts by eavesdropping on authentication cookies, so called session hijacking. The most famous such attack was the hijacking of Mark Zuckerberg's own Facebook account [1], an event that convinced Facebook and Twitter to offer secure communication. For web sites, it is in general the content owner who determines the use or mandate of HTTPS, not the end user or the browser.

The evolution of the Internet is affected by the Internet community, which consists of organizations (IETF, W3C, IRTF, etc.) and individuals that participate in the open debate, but in the end it is the industry that determines what to deploy or not. The recent revelations on pervasive surveillance have raised the general awareness of privacy and illustrated the need to encrypt sensitive data for privacy reasons. The Internet community has reacted strongly and is now treating security and privacy as top prioritizations. New protocols like HTTP/2, WebRTC, and TLS 1.3 will likely have protection mandated or on by default. Since "sensitivity" of data is not an easily defined concept, the community has chosen the same approach as the mobile access networks, to encrypt all data. W3C and IAB have recently summarized [2] [3] the conclusions taken by the community.

While security and privacy have driven the recent increase of secure communication in standardization, it must be stressed that the industry usage is also driven by a desire to control the delivery end-to-end (e.g. to avoid potential problems caused by network intermediaries) and to protect the integrity and exclusive ownership of analytics data. A recent article states that HTTPS now accounts for 50 % of all HTTP connections [4]. While this is good for end user security and privacy, it may complicate operators' ability to manage their network, optimize content delivery, and offer value added services. But for many use cases, mechanisms such as heuristics (where the frequency and sizes of packets are analyzed) and IP based classification continues to work well also for encrypted traffic.

To address the network problems caused by the increased use of secure communication, IAB arranged a workshop focusing on endpoint-middlebox cooperation [5] and GSMA released a document exploring technologies for network management of encrypted traffic [6]. We strongly support such initiatives and encourage further cooperation between the Internet community and the mobile industry.

Our Position

We believe that strong end user protection should guide the use of security mechanisms, in standardization as well as products:

- Communication should be protected: Implemented as technical solutions as well as secure operational processes.
- The right to privacy should be protected: Including secure storage and secure transmission of data.
- All access to information and data should be authorized: There must be proper security mechanisms for authentication and authorization.
- Manipulation of data in the networks should be possible to detect: The owner or the receiver of any data or communication should be able to assess that information in its original form, or be able to detect if it has been manipulated.
- Security should require minimum effort from users: Security solutions must be usable, scalable, manageable and non-intrusive.

Nevertheless, there are legitimate reasons for law enforcements authorities to intercept the communication of certain individuals and organizations. We understand the need for lawful intercept authorized by court orders, and as this intrudes private communication, a tradeoff between lawful intercept and end user privacy is necessary.

With the right technical solutions and standards, we do not see a conflict between the need for tomorrow's network to work with protected traffic, while at the same time providing value to all stakeholders. There is no single solution that can ensure this; a number of tools are needed. Already deployed mechanisms, such as heuristic analysis will be evolved and new tools will be developed. We believe in collaborative solutions where networks operators, content providers, and browser vendors work together:

- Mechanisms for cooperative path-endpoint signaling, e.g. new network APIs where both clients and servers can securely negotiate capabilities with the network, enabling more predictable quality of service for the service provider, while still addressing privacy needs.
- New in-band classification identifiers beyond the five-tuple, so that endpoints can disclose chosen application semantics enabling the correct traffic optimizations to be applied, something that otherwise requires access to plaintext.
- Technical solutions to enable caching of content close to the end users, lowering latency and reducing bandwidth for both content providers and operators, in a way that maintains end user privacy as well as content provider control.
- New more flexible security solutions that ensure end-to-end protection of sensitive data while still enabling intermediaries like caches, conference servers, and proxies. This increases the security level and enables new business models for operators by lowering the barrier to let operators run the application servers in virtualized data centers.

If the Internet community and the mobile industry cooperate to drive technologies that enable network management, content delivery, and value added services that work also in an all-encrypted world; we believe that an ecosystem where there is no tradeoff between end user privacy and quality of service is achievable.

References

[1] "After Mark Zuckerberg's Account is Hacked, Facebook Ups its Security Measures" Forbes, January 2011
http://www.forbes.com/sites/kashmirhill/2011/01/26/after-mark-zuckerbergs-account-is-hacked-facebook-ups-its-security-measures/

[2] IAB, "IAB Statement on Internet Confidentiality", November 2014
https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/

[3] W3C TAG, “Securing the Web”, January 2015
http://www.w3.org/2001/tag/doc/web-https

[4] Naylor, David et al. “The Cost of the ‘S’ in HTTPS”, December 2014
https://www.cs.cmu.edu/~dnaylor/CostOfTheS.pdf

[5] IAB, “IAB Workshop on Stack Evolution in a Middlebox Internet (SEMI)”, January 2015
https://www.iab.org/activities/workshops/semi/

[6] GSMA, “Network Management of Encrypted Traffic v1.0”, February 2015
http://www.gsma.com/newsroom/all-documents/wwg-04-network-management-of-encrypted-traffic-v1-0-2/