Network Working Group
Internet-Draft
Intended status: Informational
Expires: July 18, 2019

B. Trammell
ETH Zurich

January 14, 2019

Optional Security Is Not An Option
draft-trammell-optional-security-not-01

Abstract

This document explores the common properties of optional security protocols and extensions, and notes that due to the base-rate fallacy and general issues with coordinated deployment of protocols under uncertain incentives, optional security protocols have proven difficult to deploy in practice. This document defines the problem, examines efforts to add optional security for routing, naming, and end-to-end transport, and extracts guidelines for future efforts to deploy optional security protocols based on successes and failures to date.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on July 18, 2019.

Table of Contents

1. Introduction

Many of the protocols that make up the Internet architecture were designed and first implemented in an envrionment of mutual trust among network engineers, operators, and users, on computers that were incapable of using cryptographic protection of confidentiality, integrity, and authenticity for those protocols, in a legal environment where the distribution of cryptographic technology was largely restricted by licensing and/or prohibited by law. The result has been a protocol stack where security properties have been added to core protocols using those protocols' extension mechanisms.

As extension mechanisms are by design optional features of a protocol, this has led to a situation where security is optional up and down the protocol stack. Protocols with optional security have proven to be difficult to deploy. This document describes and examines this problem, and provides guidance for future evolution of the protocol, based on current work in network measurement and usable security research.

2. Problem statement

Consider an optional security extension with the following properties:

1. The extension is optional: a given connection or operation will succeed without the extension, albeit without the security properties the extension guarantees.

2. The extension has a true positive probability P: the probability that it will cause any given operation to fail, thereby successfully preventing an attack that would have otherwise succeeded had the extension not been enabled. This probability is a function of the extension's effectiveness as well as the probability that said operation will be an instance of the attack the extension prevents.

3. The extension has a false positive probability Q: the probability it will cause any given operation to fail due to some condition other than an attack, e.g. due to a misconfiguration.

Moving from no deployment of an optional security extension to full deployment is a protocol transition as described in [RFC8170]. We posit that the implicit transition plans for these protocols have generally suffered from an underestimation of the disincentive (as in section 5.2 of [RFC8170]) linked to the relationship between P and Q for any given protocol.

Specifically, if Q is much greater than P, then any user of an optional security extension will face an overwhelming incentive to disable that extension, as the cost of dealing with spuriously failing operations overwhelms the cost of dealing with relatively rare successful attacks. This incentive becomes stronger when the cause of the false positive is someone else's problem; i.e. not a misconfiguration the user can possibly fix. This situation can arise when poor design, documentation, or tool support elevates the incidence of misconfiguration (high Q), in an environment where the attack models addressed by the extension are naturally rare (low P).

This is not a novel observation; a similar phenomenon following from the base-rate fallacy has been studied in the literature on operational security, where the false positive and true positive rates for intrusion detection systems have a similar effect on the applicability of these systems. Axelsson showed [Axelsson99] that the false positive rate must be held extremely low, on the order of 1 in 100,000, for the probability of an intrusion given an alarm to be worth the effort of further investigation.

Indeed, the situation is even worse than this. Experience with operational security monitoring indicates that when Q is high enough, even true positives P may be treated as "in the way".

3. Case studies

Here we examine four optional security extensions, BGPSEC [RFC8205], RPKI [RFC6810], DNSSEC [RFC4033], and the addition of TLS to HTTP/1.1

[RFC2818], to see how the relationship of P and Q has affected their deployment.

We choose these examples as all four represent optional security, and that perfect deployment of the associated extensions - securing the routing control plane, the Internet naming system, and end-to-end transport (at least for the Web platform) - would represent completely "securing" the Internet architecture at layers 3 and 4.

3.1. Routing security: BGPSEC and RPKI

The Border Gateway Protocol [RFC4271] (BGP) is used to propagate interdomain routing information in the Internet. Its original design has no integrity protection at all, either on a hop-by-hop or on an end-to-end basis. In the meantime, the TCP Authentication Option [RFC5925] (and MD5 authentication [RFC2385], which it replaces) have been deployed to add hop-by-hop integrity protection.

End-to-end protection of the integrity of BGP announcements is protected by two complementary approaches. Route announcements in BGP updates protected by BGPSEC [RFC8205] have the property that the every Autonomous System (AS) on the path of ASes listed in the UPDATE message has explicitly authorized the advertisement of the route to the subsequent AS in the path. RPKI [RFC6810] protects prefixes, granting the right to advertise a prefix (i.e., be the first AS in the AS path) to a specific AS. RPKI serves as a trust root for BGPSEC, as well.

These approaches are not (yet) universally deployed. BGP route origin authentication approaches provide little benefit to individual deployers until it is almost universally deployed [Lychev13]. RPKI route origin validation is similarly deployed in about 15% of the Internet core; two thirds of these networks only assign lower preference to non-validating announcements. This indicates significant caution with respect to RPKI mistakes [Gilad17]. In both cases the lack of incentives for each independent deployment, including the false positive risk, greatly reduces the speed of incremental deployment and the chance of a successful transition [RFC8170].

In addition, the perception of security as a secondary concern for interdomain routing hinders deployment. A preference for secure routes over insecure ones is necessary to drive further deployment of routing security, but an internet service provider is unlikely to prefer a secure route over an insecure route when the secure route violates local preferences or results in a longer AS path [Lychev13].

3.2. DNSSEC

The Domain Name System (DNS) [RFC1035] provides a distributed protocol for the mapping of Internet domain names to information about those names. As originally specified, an answer to a DNS query was considered authoritative if it came from an authoritative server, which does not allow for authentication of information in the DNS. DNS Security [RFC4033] remedies this through an extension, allowing DNS resource records to be signed using keys linked to zones, also distributed via DNS. A name can be authenticated if every level of the DNS hierarchy from the root up to the zone containing the name is signed.

The root zone of the DNS has been signed since 2010. As of 2016, 89% of TLD zones were also signed. However, the deployment status of DNSSEC for second-level domains (SLDs) varies wildly from region to region and is generally poor: only about 1% of .com, .net. and .org SLDs were properly signed [DNSSEC-DEPLOYMENT]. Chung et al found recently that second-level domain adoption was linked incentives for deployment: TLDs which provided direct financial incentives to SLDs for having correctly signed DNS zones tend to have much higher deployment, though these incentives must be carefully designed to ensure that they measure correct deployment, as opposed to more easily-gamed indirect metrics [Chung17].

However, the base-rate effect tends to reduce the use of DNSSEC validating resolvers, which remains below 15% of Internet clients [DNSSEC-DEPLOYMENT].

DNSSEC deployment is hindered by other obstacles, as well. Since the organic growth of DNS software predates even TCP/IP, even EDNS, the foundational extension upon which DNSSEC is built are not universally deployed, which inflates Q. The current DNS Flag Day effort (see https://dnsflagday.net) aims to remedy this by purposely breaking backward interoperability with servers that are not EDNS-capable, by coordinating action among DNS software developers and vendors.

In addition, for the Web platform at least, DNSSEC is not percieved as having essential utility, given the deployment of TLS and the assurances provided by the Web PKI (on which, see Section 3.3). A connection intercepted due to a poisoned DNS cache would fail to authenticate unless the attacker also obtained a valid certificate from the name, rendering DNS interception less useful, in effect, reducing P.

3.3. HTTP over TLS

Security was added to the Web via HTTPS, running HTTP over TLS over TCP, in the 1990s [RFC2818]. Deployment of HTTPS crossed 50% of web traffic in 2017.

Base-rate effects didn't hinder the deployment of HTTPS per se; however, until recently, warnings about less-safe HTTPS configurations (e.g. self-signed certificates, obsolete versions of SSL/TLS, old ciphersuites, etc.) were less forceful due to the prevalence of these configurations. As with DNS Flag Day, making changes to browser user interfaces that inform the user of low-security configurations is facilitated by coordination among browser developers [ChromeHTTPS]. If one browser moves alone to start displaying warnings or refusing to connect to sites with less-safe or unsafe configurations, then users will tend to percieve the safer browser as more broken, as websites that used to work don't anymore: i.e., non-coordinated action can lead to the false perception that an increase in P is an increase in Q. This coordination continues up the Web stack within the W3C [SecureContexts].

The Automated Certificate Management Environment [ACME] has further accelerated the deployment of HTTPS on the server side, by drastically reducing the effort required to properly manage server certificates, reducing Q by making configuration easier than misconfiguration. Let's Encrypt leverages ACME to make it possible to offer certificates at scale for no cost with automated validation, issuing 90 million active certificates protecting 150 million domain names in December 2018 [LetsEncrypt2019].

Deployment of HTTPS accelerated in the wake of the Snowden revelations. Here, the perception of the utility of HTTPS has changed. Increasing confidentiality of Web traffic for openly-available content was widely seen as not worth the cost and effort prior to these revelations. However, as it became clear that the attacker model laid out in [RFC7624] was a realistic one, content providers and browser vendors put the effort in to increase implementation and deployment.

The ubiquitous deployment of HTTPS is not yet complete; however, all indications are that it will represent a rare eventual success story in the ubiquitous deployment of an optional security extention. What can we learn from this success? We note that each endpoint deciding to use HTTPS saw an immediate benefit, which is an indicator of good chances of success for incremental deployment [RFC8170]. However, the acceleration of deployment since 2013 is the result of the coordinated effort of actors throughout the Web application and operations stack, unified around a particular event which acted as a

call to arms. While there are downsides to market consolidation, the relative consolidation of the browser market has made coordinated action to change user interfaces possible, as well as making it possible to launch a new certificate authority (by adding its issuer to the trusted roots of a relatively small number of browsers) from nothing in a short period of time.

4. Discussion and Recommendations

It has been necessary for all new protocol work in the IETF to consider security since 2003 [RFC3552], and the Internet Architecture Board recommended that all new protocol work provide confidentiality by default in 2014 [IAB-CONFIDENTIALITY]; new protocols should therefore already not rely on optional extensions to provide security guarantees for their own operations or for their users.

In many cases in the running Internet, the ship has sailed: it is not at this point realistic to replace protocols relying on optional features for security with new, secure protocols. While these full replacements would be less susceptible to base-rate effects, they have the same misaligned incentives to deploy as the extensions the architecture presently relies on.

The base rate fallacy is essential to this situation, so the P/Q problem is difficult to sidestep. However, an examination of our case studies does suggest incremental steps toward improving the current situation:

- When natural incentives are not enough to overcome base-rate effects, external incentives (such as financial incentives) have been shown to be effective to motivate single deployment decisions. This essentially provides utility in the form of cash, offseting the negative cost of high Q.

- While "flag days" are difficult to arrange in the current Internet, coordinated action among multiple actors in a market (e.g. DNS resolvers or web browsers) can reduce the risk that temporary breakage due to the deployment of new security protocols is perceived as an error, at least reducing the false perception of Q.

- Efforts to automate configuration of security protocols, and thereby reduce the incidence of misconfiguration Q, have had a positive impact on deployability.

Coordinated action has demonstrated success in the case of HTTPS, so examining the outcome (or failure) of DNS Flag Day will provide more information about the likelihood of future such actions to move

deployment of optional security features forward. It is difficult to see how insights on coordinated action in DNS and HTTPS can be applied to routing security, however, given the number of actors who would need to coordinate to make present routing security approaches widely useful. We note, however, that the MANRS effort (https://www.manrs.org) provides an umbrella activity under which any future coordination might take place.

We note that the cost of a deployment decision (at least for DNSSEC) could readily be extracted from the literature [Chung17]. Extrapolation from this work of a model for determining the total cost of full deployment of DNSSEC (or, indeed, of comprehensive routing security) is left as future work.

5. Acknowledgments

Many thanks to Peter Hessler, Geoff Huston, and Roland van Rijswijk-Deij for conversations leading to the problem statement presented in this document. Thanks to Martin Thomson for his feedback on the document itself, which has greatly improved subsequent versions. The title shamelessly riffs off that of Berkeley tech report about IP options written by Rodrigo Fonseca et al., via a paper at IMC 2017 by Brian Goodchild et al.

This work is partially supported by the European Commission under Horizon 2020 grant agreement no. 688421 Measurement and Architecture for a Middleboxed Internet (MAMI), and by the Swiss State Secretariat for Education, Research, and Innovation under contract no. 15.0268. This support does not imply endorsement.

6. Informative References

[ACME] Barnes, R., Hoffman-Andrews, J., McCarney, D., and J. Kasten, "Automatic Certificate Management Environment (ACME)", draft-ietf-acme-acme-18 (work in progress), December 2018.

[Axelsson99] Axelsson, S., "The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection (in ACM CCS 1999)", 1999, <http://www.raid-symposium.org/raid99/PAPERS/Axelsson.pdf>.

[ChromeHTTPS] Schechter, E., "["A milestone for Chrome security - marking HTTP as \"not secure\" (Google blog post)", nil]", July 2018, <https://www.blog.google/products/chrome/milestone-chrome-security-marking-http-not-secure/>.

[Chung17] Chung, T., van Rijswijk-Deij, R., Choffnes, D., Levin, D., Maggs, B., Mislove, A., and C. Wilson, "Understanding the Role of Registrars in DNSSEC Deployment", November 2017, <https://conferences.sigcomm.org/imc/2017/papers/imc17-final53.pdf>.

[DNSSEC-DEPLOYMENT] Internet Society, ., "State of DNSSEC Deployment 2016", December 2016, <https://www.internetsociety.org/resources/doc/2016/state-of-dnssec-deployment-2016/>.

[Gilad17] Gilad, Y., Cohen, A., Herzberg, A., Schapira, M., and H. Schulman, "Are We There Yet? On RPKI's Deployment and Security (in NDSS 2017)", November 2017, <https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/are-we-there-yet-rpkis-deployment-and-security/>.

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

[LetsEncrypt2019] Aas, J., "Looking Forward to 2019 (Let's Encrypt blog post)", December 2018, <https://letsencrypt.org/2018/12/31/looking-forward-to-2019.html>.

[Lychev13] Lychev, R., Goldberg, S., and M. Schapira, "BGP Security in Partial Deployment - Is the Squeeze Worth the Juice? (in SIGCOMM 2013)", 2013, <https://conferences.sigcomm.org/sigcomm/2013/papers/sigcomm/p171.pdf>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[RFC2385] Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option", RFC 2385, DOI 10.17487/RFC2385, August 1998, <https://www.rfc-editor.org/info/rfc2385>.

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, DOI 10.17487/RFC2818, May 2000, <https://www.rfc-editor.org/info/rfc2818>.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <https://www.rfc-editor.org/info/rfc3552>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/info/rfc4033>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

[RFC5925] Touch, J., Mankin, A., and R. Bonica, "The TCP Authentication Option", RFC 5925, DOI 10.17487/RFC5925, June 2010, <https://www.rfc-editor.org/info/rfc5925>.

[RFC6810] Bush, R. and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol", RFC 6810, DOI 10.17487/RFC6810, January 2013, <https://www.rfc-editor.org/info/rfc6810>.

[RFC7624] Barnes, R., Schneier, B., Jennings, C., Hardie, T., Trammell, B., Huitema, C., and D. Borkmann, "Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement", RFC 7624, DOI 10.17487/RFC7624, August 2015, <https://www.rfc-editor.org/info/rfc7624>.

[RFC8170] Thaler, D., Ed., "Planning for Protocol Adoption and Subsequent Transitions", RFC 8170, DOI 10.17487/RFC8170, May 2017, <https://www.rfc-editor.org/info/rfc8170>.

[RFC8205] Lepinski, M., Ed. and K. Sriram, Ed., "BGPsec Protocol Specification", RFC 8205, DOI 10.17487/RFC8205, September 2017, <https://www.rfc-editor.org/info/rfc8205>.

[SecureContexts] van Kesteren, A., "Secure Contexts Everywhere", January 2018, <https://blog.mozilla.org/security/2018/01/15/secure-contexts-everywhere/>.

Author's Address

Brian Trammell
ETH Zurich
Universitatstrasse 6
8092 Zurich
Switzerland

Email: ietf@trammell.ch