Continuous Measurement Platforms can help Mitigate Pervasive Surveillance

Julian Kornberger juliank@tzi.org Carsten Bormann cabo@tzi.org
RAIM Workshop, Saturday, 2015–10–31, Yokohama, JP

Introduction

Operators of Internet-based communications platforms now have a clear mission to make it harder for their societies to slip into pervasive surveillance [RFC7258]. Work on this is underway on a number of places and for a number of communication modes. For E-Mail, significant effort has gone into making the client-to-server communications more secure, but the server-to-server relationship is still fundamentally based on any MTA (mail transfer agent) being able to set up communication to any other MTA communications, which often cannot be secured. Opportunistic Encryption [RFC7435] can help, but is easily downgraded by an active attacker, which may want to benefit from targeting specific MTA-MTA relations. Downgrade resistance may be provided by MTAs publishing information about themselves in a secure way [draft-ietf-dane-smtp-with-dane], but that requires both the sending and receiving MTA operators to act. The present paper discusses ways for the sending MTA to provide downgrade resistance based on information published by a measurement platform about other MTAs.

This position paper reports on work done by Julian Kornberger in late 2014/early 2015 [Korn15].

Opportunistic Encryption in Mail Transfer Today

MTAs such as Postfix can be configured to attempt setting up TLS for outgoing mail. This makes the outgoing mail inaccessible to passive monitoring, subject to the limitations of TLS and its implementations. An active attacker can use a man-in-the-middle attack to cause the sending MTA to downgrade, possibly to no security at all, or to a “secure” connection to an unauthenticated server (which may be the man in the middle). As a result of a successful downgrade attack, surveillance is again possible.

Postfix can be configured to require certain levels of TLS usage specifically for each destination. A mail administrator that is aware that, e.g., Google offers TLS on their incoming SMTP ports, can configure their MTA to not deliver any mail to specific Google destinations unless a secure TLS connection based on valid and trusted certificates can be established. This mitigates the man-in-the-middle attack (if persistent, the attack turns into a denial of service).

While a mail administrator may be able to perform this manual configuration for a few carefully hand-picked target MTAs, scaling this manual method up to the millions of MTAs in operation is not an option. DANE may be used by an MTA to publish information about its availability of TLS support [draft-ietf-dane-smtp-with-dane], however, DANE (and the underlying DNSSEC) are only slowly becoming more widespread.

An Opportunistic Security Downgrade Blacklist (OSDBL)

The basic idea of the present work is to collect comprehensive information about the set of MTAs present in the Internet today and the availability of Opportunistic Security with each of these MTAs. This information is then made available in the form of a DNS-based policy service (similar to the way spam blacklists are run today) that can be used by MTAs to decide whether opportunistic security is expected for a target MTA or not.

The Measurement Platform

Using zmap [DWH13] and zgrab, we periodically collect the set of IPv4 hosts responding to TCP connections on port 25 (SMTP). Approximately 15 million SMTP hosts can be found, of which nearly 5 million complete a TLS handshake (3 million support TLS 1.0 and 1.2, 2 million only TLS 1.0). 69 % of the server certificates offered are self-signed (many by a single piece of software providing a server administration panel, often no longer valid), 30 % are valid and have a certificate chain that we classify as trustable, 1 % are invalid while classifying as trustable. We still find 3566 certificates with keys that have been compromised in the Debian pseudo-random generator incident [CVE–2008–0166].

Additionally, we use the Alexa Top 1 Million websites to collect a set of potential DNS names that could also provide SMTP services. Approximately 0.85 million of these DNS names provide an MX record, indicating SMTP service. A very small number (201) of these has a TLSA record, which is usable (certificate is available in the TLS handshake and agrees) in 191 cases. Many of the MX records point to popular mail service providers, with the most popular one being Google (15 %). Of the domain names with MX records for which mail servers were actually reachable, 82 % support STARTTLS, and about half of those (40 %) provide a valid certificate with a correct hostname and a certificate chain that we classify as trustable.

Creating and Using the OSDBL

The purpose of an OSDBL is to provide a sending MTA with a mapping from a next hop address to a TLS policy level such as that provided by Postfix. Clearly, if this mapping is to be provided via DNS, the DNS requests need to be secured against man-in-the-middle attacks; DNSSEC is the obvious solution. To query the OSDBL, an DNS client with DNSSEC support is needed. Unfortunately, since DNS clients often do not provide detailed information about errors occurring, not every DNS client is really useful for querying a DNSSEC-based OSDBL. Some additional implementation work may be required here.

For Postfix, the policy mapping is performed as follows:

- Is a TLSA entry available? If yes, use “dane-only”, otherwise:
- Is STARTTLS available? If no, use “may”, otherwise:
- Is the certificate valid and trustable? If yes, use “verify”.
- Otherwise, use “encrypt”

The TLS policy server (OSDBL) is implemented in Go. It performs the translation of MX hostnames to A/AAAA records, as well as the querying of the resulting IP address, either from the cache or by obtaining new information. If no (or only outdated) policy information is instantly available, the measuring process for this address is initiated; no DNS response is returned to the DNS client, which will retry and obtain the information at that time now probably available in the cache.

The TLS policy client is implemented in Python and can be integrated easily in Postfix.

Security and Deployability

Clearly, the OSDBL is a valid target in its own right for an attacker and there are various conceivable attacks, both on the way from the using MTA to the OSDBL (e.g., by inserting false responses for the OSDBL) and on the way from the measurement platform underlying the OSDBL towards the target MTAs. Mitigations for these attacks are not being discussed in this short position paper, but various approaches come to mind.

The most important limitation of the approach described here is that, if an adversary successfully attacks both the path between the measurement platform and the target MTA and the path between the sending and the target MTA, no additional protection is derived from using the OSDBL. Various mitigations could be developed, including a more distributed measurement platform as well as some sanity checking, including limited stickyness of observed support for opportunistic security. (An interesting side effect of such limited stickyness would be that it would increase the downside for an administrative decision to switch off opportunistic security support at a mail domain.)

An important problem to be discussed is how a mail administrator would realistically be willing to make use of the services of an OSDBL. If the OSDBL becomes a single point of failure or creates a large number of small helpdesk incidents, it will not be used. Creating good strategies for the usage of OSDBLs and the necessary support in MTAs to implement these strategies is therefore an important next step towards the viability of this approach.

[CVE–2008–0166]

CVE–2008–0166. Available from MITRE, CVE-ID CVE–2008–0166. Jan. 2008. url: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE–2008–0166

[draft-ietf-dane-smtp-with-dane]

Viktor Dukhovni and Wesley Hardaker: “SMTP security via opportunistic DANE TLS”, Internet-Draft, 2015–05–29, <draft-ietf-dane-smtp-with-dane–19.txt>

[Korn15]

Julian Kornberger: “Eine TLS-Policy-Datenbank für sicheren E-Mail-Transport”, Diplomarbeit, Fachbereich 3: Mathematik und Informatik, Universität Bremen, July 2015.

[DWH13]

Zakir Durumeric, Eric Wustrow und J. Alex Halderman: »ZMap: Fast Internet-Wide Scanning and its Security Applications«. In: Proceedings of the 22nd USENIX Security Symposium. Aug. 2013.

[RFC7258]

S. Farrell, H. Tschofenig: »Pervasive Monitoring Is an Attack«. May 2014. (Also BCP0188) (Status: BEST CURRENT PRACTICE) (DOI: 10.17487/RFC7258)

[RFC7435]

V. Dukhovni: »Opportunistic Security: Some Protection Most of the Time«. December 2014. (Status: INFORMATIONAL) (DOI: 10.17487/RFC7435)