Proceedings of the 29th USENIX Security Symposium

Errata Slip #3

In the paper "A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email" by Hyeonmin Lee, *Seoul National University;* Aniketh Gireesh, Amrita Vishwa Vidyapeetham; Roland van Rijswijk-Deij, *University of Twente & NLnet Labs;* Taekyoung "Ted" Kwon, *Seoul National University;* Taejoong Chung, *Rochester Institute of Technology* (Wednesday session, "Network Security," pp. 613–630 of the Proceedings), the authors have provided the following corrections.

The authors would like to correct Table 2 as follows:

Original table:

Vantage Point	Measurement Period	The number of TLSA	Certs
Oregon	2019-07-11 through 2019-10-31	11,821	10,526
Virginia		11,806	10,521
São Paulo		11,771	10,470
Paris		11,819	10,531
Sydney		11,770	10,484

Corrected table:

Vantage Point	Measurement Period	The number of TLSA	Certs
Oregon	2019-07-11 through 2019-10-31	7,897	7,308
Virginia		7,893	7,306
São Paulo		7,870	7,278
Paris		7,900	7,313
Sydney		7,867	7,218

Original text:

We used the above methodology to gather measurements by sending on average 11,972 TLSA record lookups as well as collecting the certificate chains every hour from July 11, 2019 to October 31, 2019.

Corrected text:

We used the above methodology to gather measurements by sending on average 7,819 TLSA record lookups as well as collecting the certificate chains every hour from July 11, 2019 to October 31, 2019.

In subsection 5.5 TLSA Management, the authors would like to correct the following text:

Original text:

In this subsection, we focus on how TLSA records and the corresponding public keys are managed; more specifically, we investigate if the TLSA records are used as intended and how often public and private key pairs are changed.

Corrected text:

In this subsection, we focus on how TLSA records and the corresponding public keys are managed; more specifically, we investigate how often public and private key pairs are changed.

In subsection 5.5 TLSA Management, the authors would like to remove the following text from the paper:

> **Unsuitable Usages** The primary purpose of DANE is to let domain owners use custom certificates for their TLS connections by using TLSA records with the DANE-EE or DANE-TA usage without relying on third-party CAs. If the domain owner has a certificate issued by a CA, but serves a TLSA record with the DANE-EE or DANE-TA usage, they do not benefit fully from the security measures that DANE provides (instead, they should use the PKIX-EE or PKIX-TA Certificate Usage). Moreover, the validity periods of such certificates are usually determined by CAs, which are usually short.[9] Thus, domain owners incur additional complexity as they need to update their TLSA records whenever the certificates are re-issued. Therefore, a domain name owner should avoid setting their TLSA records with the DANE-EE or DANE-TA usage when they serve a certificate issued by a CA.
>
> We first examine how the Certificate Usage field is set in TLSA records by calculating the distribution of the Certificate Usages of the TLSA records from our latest snapshot. Unsurprisingly, we observe that the vast majority of TLSA records (94.29%) use DANE-EE or DANE-TA. We then configure OpenSSL [61] to trust the set of root CA certificates in the Ubuntu 18.04 LTS root store [24]; the validation would fail if the certificates for the TLSA records are custom certificates. Surprisingly, we find that on average 90.58% and 90.37% of TLSA records with DANE-EE and DANE-TA are still valid, which means that the certificates are valid in terms of PKIX, not custom certificates. Consequently, these records could

have used PKIX-EE or PKIX-TA Certificate Usages, thus having the additional benefit of certificate validation through two independent mechanisms (DANE and PKIX). We believe operators do this because they are worried that sending SMTP servers would reject their custom certificates. However, as we will see in the next section, all of the popular email service providers (i.e., sending SMTP servers) that we test do not validate the certificates of the receiving SMTP servers when they cannot find any available TLSA records.