Ballot SC28 - Logging and Log Retention

Background

Both the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (BR) and the Network and Certificate System Security Requirements (NSR) stipulate that CAs must collect and retain log files concerning a number of events. These events are separated into three categories, CA key lifecycle management events, Subscriber Certificate lifecycle management events, and security events.

While the purpose for the retention requirements for the CA key lifecycle management events and CA and Subscriber Certificate lifecycle management events is well understood, the purpose for the same retention period for security events is less clear. Security event logs decrease in relevancy and value as time passes from the time of the event. The requirements for what is included in security events are ambiguous and can generate a significant amount of log data. The current requirements require CAs to maintain a significant amount of data that CAs consider to be of low value, and has a significant amount of compliance overhead.

Logging retention requirements for subscriber certificates comes into question, because the allowed lifetime of subscriber certificates continues to decrease. The industry is moving toward a certificate lifetime of one year, however the retention requirements have not been updated to correspond to the decreasing lifetimes.

Purpose

The proposed changes seek to clarify the relationship between audit logging obligations under Network and Certification System Security Requirements and Baseline Requirements and to reduce the retention period for log data, when appropriate. The proposed change also provides clarification by specifically cross-referencing the Baseline Requirements.

Event Logs Most data retention standards do not specify retention requirements for the underlying systems that process transactions. In drafting this ballot it was considered the primary use of these system logs is in the event of an incident and an investigation is required. The IBM and Ponemon Institute's 2019 Cost of a Data Breach Report found on average it took 206 days to identify a data breach had occurred. To provide enough history for incident investigation two years of supporting system logs will provide more than enough time to detect and investigate the incident.

The current log retention requirements for subscriber certificates require certificate validation and certificate activity to be retained for seven years, while the lifetime of a certificate is only two years. There does not seem to be a justification for retaining logs three times as long as the

lifetime of the certificate. As certificate lifetimes move to one year this further supports a reduction in log retention.

Risk vs Benefits

The benefit of this ballot is to reduce data retention requirements for those log elements which most CAs consider as having limited long-term value. As an example, firewall and router activity logs are of significant size and thus impose significant storage requirements. These logs serve a benefit when investigating a potential security event, however, these logs lose value with the passage of time. Logs containing firewall traffic that is several years old provide little value in the investigation of a contemporary incident. Additionally, certificate validation and issuance logs have little value after a certificate has expired. The log size for many CAs is measured in terabytes, each year and the overhead of storing these logs and monitoring for compliance is significant. The benefit for reducing retention is considered high.

The primary risk of accepting this ballot is a CA experiences a security event or certificate mis-issuance, does not identify the event for more than two years and does not have the required logs needed to fully investigate the impact of the event. This risk is mitigated because a CA environment is considered a high security environment and is required to have robust security monitoring and alerting. There is a reduced likelihood a CA would have a security event go undetected for more than two years. In the event a security event was undetected for a year, the reliability of the logs also decreases. The value of logs supporting the mis-issuance of a certificate multiple years after the certificate has expired is also low. Overall the risks associated with this ballot are low.

Proposal

The following ballot is proposed by Neil Dunbar of TrustCor Systems and endorsed by Trevoli Ponds-White of Amazon and Dustin Hollenback of Microsoft.

— MOTION BEGINS —

Delete the following Section 5.4.1. from the “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”, version 1.6.7, which currently reads as follows:

The CA and each Delegated Third Party SHALL record details of the actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved. The CA SHALL make these records available to its Qualified Auditor as proof of the CA’s compliance with these Requirements.

The CA SHALL record at least the following events:

1. CA key lifecycle management events, including:

    a. Key generation, backup, storage, recovery, archival, and destruction; and

    b. Cryptographic device lifecycle management events.

2. CA and Subscriber Certificate lifecycle management events, including:

    a. Certificate requests, issuance, renewal, and re-key requests, and revocation;

    b. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;

    c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;

    d. Acceptance and rejection of certificate requests; Frequency of Processing Log

    e. Issuance of Certificates; and

    f. Generation of Certificate Revocation Lists and OCSP entries.

3. Security events, including:

    a. Successful and unsuccessful PKI system access attempts;

    b. PKI and security system actions performed;

    c. Security profile changes;

    d. System crashes, hardware failures, and other anomalies;

    e. Firewall and router activities; and

    f. Entries to and exits from the CA facility.

Insert in Section 1.6.1 (Definitions) of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", the following (after the definition of "Certification Practice Statement"):

Certificate Profile: A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7 of the Baseline Requirements. e.g. a Section in a CA's CPS or a certificate template file used by CA software.

Insert, as Section 5.4.1. (Types of events recorded) of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", the following:

Section 5.4.1

The CA and each Delegated Third Party SHALL record details of the actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved. The CA SHALL make these records available to its Qualified Auditor as proof of the CA's compliance with these Requirements.

The CA SHALL record at least the following events:

1. CA certificate and key lifecycle events, including:
    1. Key generation, backup, storage, recovery, archival, and destruction;
    2. Certificate requests, renewal, and re-key requests, and revocation;
    3. Approval and rejection of certificate requests;
    4. Cryptographic device lifecycle management events;
    5. Generation of Certificate Revocation Lists and OCSP entries;
    6. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. Subscriber Certificate lifecycle management events, including:
    1. Certificate requests, renewal, and re-key requests, and revocation;
    2. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;
    3. Approval and rejection of certificate requests;
    4. Issuance of Certificates; and
    5. Generation of Certificate Revocation Lists and OCSP entries.
3. Security events, including:
    1. Successful and unsuccessful PKI system access attempts;
    2. PKI and security system actions performed;
    3. Security profile changes;
    4. Installation, update and removal of software on a Certificate System;
    5. System crashes, hardware failures, and other anomalies;
    6. Firewall and router activities; and
    7. Entries to and exits from the CA facility.

Delete the following Section 5.4.3. from the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", version 1.6.7, which currently reads as follows:

> The CA SHALL retain any audit logs generated for at least seven years. The CA SHALL make these audit logs available to its Qualified Auditor upon request.

Insert, as Section 5.4.3. Retention Period for Audit Logs of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", the following:

The CA SHALL retain, for at least two years:

1. CA certificate and key lifecycle management event records (as set forth in Section 5.4.1 (1)) after either:
    a. the destruction of the CA Private Key; or
    b. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 `basicConstraints` extension with the `cA` field set to `true` and which share a common Public Key corresponding to the CA Private Key, whichever event occurs later.
2. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1 (2)) after the revocation or expiration of the Subscriber Certificate.
3. Any security event records (as set forth in Section 5.4.1 (3)) after the event occurred.

Delete from "Network and Certificate Systems Security Requirements", Version 1.3, Section 3.b

b. Identify those Certificate Systems under the control of CA or Delegated Third Party Trusted Roles capable of monitoring and logging system activity and enable those systems to continuously monitor and log system activity;

Insert new "Network and Certificate Systems Security Requirements", Version 1.3, Section 3.b with the following text:

B. Identify those Certificate Systems under the control of CA or Delegated Third Party Trusted Roles capable of monitoring and logging system activity, and enable those systems to log and continuously monitor the events specified in Section 5.4.1 (3) of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates;

— MOTION ENDS —

*** WARNING ***: USE AT YOUR OWN RISK. THE REDLINE BELOW IS NOT THE OFFICIAL VERSION OF THE CHANGES (CABF Bylaws, Section 2.4(a)):

A comparison of the changes can be found at:

https://github.com/cabforum/documents/compare/16a5a9b...neildunbar:5480a95

Effective as of the date this Ballot becomes incorporated into a Final Guideline.

This ballot proposes two Final Maintenance Guidelines

The procedure for approval of this ballot is as follows:

Discussion (7+ days)

Start Time: <INSERT>

End Time: <INSERT>

Vote for approval (7 days)

Relevant provisions

From the BR

5.4. AUDIT LOGGING PROCEDURES

5.4.1. Types of Events Recorded

The CA and each Delegated Third Party SHALL record details of the actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved. The CA SHALL make these records available to its Qualified Auditor as proof of the CA's compliance with these Requirements. The CA SHALL record at least the following events:

1. *CA key lifecycle management events, including:*
    a. *Key generation, backup, storage, recovery, archival, and destruction; and*
    b. *Cryptographic device lifecycle management events.*
2. *CA and Subscriber Certificate lifecycle management events, including:*
    a. *Certificate requests, renewal, and re-key requests, and revocation;*
    b. *All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;*
    c. *Date, time, phone number used, persons spoken to, and end results of verification telephone calls;*
    d. *Acceptance and rejection of certificate requests;*
    e. *Issuance of Certificates; and*
    f. *Generation of Certificate Revocation Lists and OCSP entries.*
3. *Security events, including:*
    a. *Successful and unsuccessful PKI system access attempts;*
    b. *PKI and security system actions performed;*
    c. *Security profile changes;*
    d. *System crashes, hardware failures, and other anomalies;*
    e. *Firewall and router activities; and*
    f. *Entries to and exits from the CA facility.*

Log entries MUST include the following elements:

1. *Date and time of entry*
2. *Identity of the person making the journal entry; and*
3. *Description of the entry.*

5.4.2. Frequency for Processing and Archiving Audit Logs

5.4.3. Retention Period for Audit Logs

The CA SHALL retain any audit logs generated for at least seven years. The CA SHALL make these audit logs available to its Qualified Auditor upon request.

5.5. RECORDS ARCHIVAL
5.5.1. Types of Records Archived
5.5.2. Retention Period for Archive
The CA SHALL retain all CA and Subscriber Certificate lifecycle management event audit logs*, for at least seven years after any Certificate based on that documentation ceases to be valid.*

From the NSR

3. LOGGING, MONITORING, & ALERTING

Certification Authorities and Delegated Third Parties SHALL:

a. *Implement a Security Support System under the control of CA or Delegated Third Party Trusted Roles that monitors, detects, and reports any security-related configuration change to Certificate Systems;*
b. *Identify those Certificate Systems under the control of CA or Delegated Third Party Trusted Roles capable of monitoring and logging system activity and enable those systems to continuously monitor and log system activity;*
c. *Implement automated mechanisms under the control of CA or Delegated Third Party Trusted Roles to process logged system activity and alert personnel, using notices provided to multiple destinations, of possible Critical Security Events;*
d. *Require Trusted Role personnel to follow up on alerts of possible Critical Security Events;*
e. *Conduct a human review of application and system logs at least once a month to validate the integrity of logging processes and ensure that monitoring, logging, alerting, and log integrity verification functions are operating properly (the CA or Delegated Third Party MAY use an in-house or third-party audit log reduction and analysis tool); and*
f. *Maintain, archive, and retain logs in accordance with disclosed business practices and applicable legislation.*