ITL BULLETIN FOR JULY 2012

Preparing for and Responding to Certification Authority Compromise and Fraudulent Certificate Issuance

Paul Turner, Venafi

William Polk, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce

Elaine Barker, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce

1. Executive Summary

As the use of Public Key Infrastructure (PKI) and digital certificates (e.g., the use of Transport Layer Security [TLS] and Secure Sockets Layer [SSL]) for the security of systems has increased, the certification authorities (CAs) that issue certificates have increasingly become targets for sophisticated cyber-attacks. In 2011, several public certification authorities were attacked, and at least two attacks resulted in the successful issuance of fraudulent certificates by the attackers. An attacker who breaches a CA to generate and obtain fraudulent certificates does so to launch further attacks against other organizations or individuals. An attacker can also use fraudulent certificates to authenticate as another individual or system or to forge digital signatures.

These recent attacks on CAs make it imperative that organizations ensure they are using secure CAs and must also be prepared to respond to a CA compromise or issuance of a fraudulent certificate. Responding to a CA compromise may require replacing all user or device certificates or trust anchors.[1] If an organization is not prepared with an inventory of certificate locations and owners, the organization will not be able to respond in a timely manner and may experience significant interruption in its operations for an extended period of time. This document provides an overview of CA compromise and fraudulent certificate issuance scenarios and recommends steps for preparing for and responding to these incidents.

Many organizations have certificates issued from an external CA, and some organizations operate their own CAs. Nearly all organizations have users and/or systems that establish security using certificates belonging to the parties with whom they communicate. Since many of today's applications are sold with installed trust anchors that users may not be aware of or

[1] Relying parties use root certificates, referred to as trust anchors in this document, that they store locally to verify certificates they receive.

explicitly trust, anyone may be at risk if one of those CAs is compromised. Therefore, this bulletin is aimed at all users and organizations that use or rely on public key certificates.

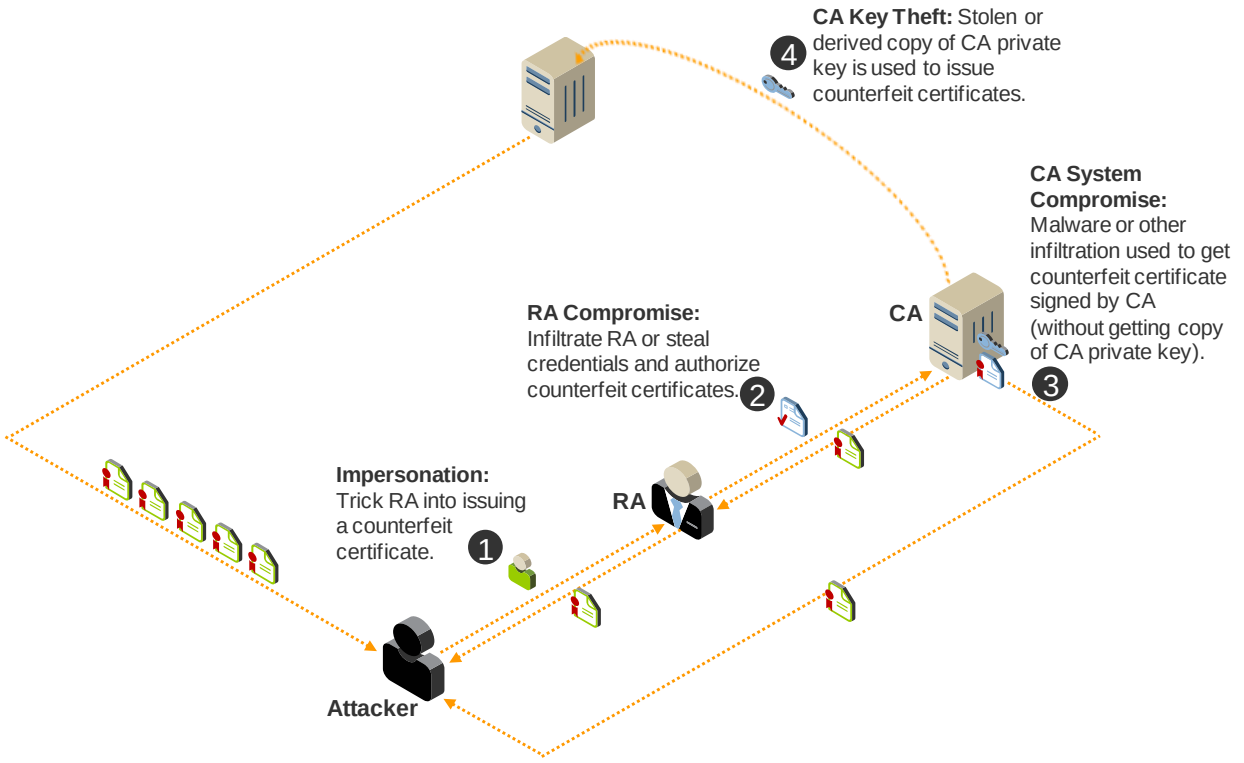
2. Public Key Infrastructure Roles

Organizations may play four primary PKI roles in the context of CA security incidents: certification authority, registration authority, subject, and relying party.

- **Certification Authority:** Certification authorities (CAs) issue certificates and certificate revocation lists (CRLs). Many organizations operate internal CA systems to issue certificates to their own devices and users. An organization may also use certificates issued by external CAs; for example, external CAs often issue the certificates that are trusted in browsers and other applications and systems.
- **Registration Authority:** Registration authorities (RAs) act as an intermediary between users and CAs, reviewing and approving certificate requests. When a certificate is being requested for a person, the RA validates that the identity of that person is appropriate for the subject name that will be included in the certificate. When a certificate is being requested for a system, the RA validates that the requester is authorized to request a certificate for the system with the specified address (e.g., DNS address). In some cases, the organization that operates the CA performs the RA role. However, organizations requesting certificates from an external CA frequently perform the RA role, since they have the local knowledge needed to validate certificate requests.
- **Subject:** A subject is the person, organization, system, application, or device to which a certificate is issued and whose identifier is provided in the certificate. Examples of subject systems include web servers and routers. Today, most organizations have systems and individuals to which certificates have been issued and consequently act in the role of a subject.
- **Relying Party:** Relying parties are individuals or systems that electronically interact or transact with the subject and rely on the subject's certificate in the process. Examples of relying parties include browsers that connect to web servers (which act as subjects with certificates installed) or servers connecting to other servers. Relying parties use locally stored trust anchors to validate the signatures on subject certificates. These trust anchors may be installed by the owner of the relying party system or by the vendor that manufactures the software (e.g., browser or operating system) on the relying party system. All organizations act as relying parties.

3. CA Compromise and Fraudulent Certificate Issuance Scenarios

This document identifies four general classes of attacks on CA operations. The type of attack used to issue fraudulent certificates and CRLs influences the steps that organizations must take to respond. The following diagram illustrates the ways that fraudulent certificates can be issued and obtained by an attacker, including:



1. **Impersonation:** The attacker successfully impersonates someone else to the registration authority (RA) and is issued a certificate with that other person's or system's name in it. For example, suppose the intended operation is the following: Alice sends digitally signed authorizations to Bob for money transfers, and Bob uses a certificate issued to Alice to verify the authorizations. An impersonation attack on this operation could be performed in the following way: Eve (the attacker) convinces a CA that Bob trusts that she is Alice, and the CA issues a certificate containing Alice's name, but Eve's public key. Eve is now able to forge Alice's signature on money transfer authorizations.
2. **RA Compromise:** The attacker infiltrates the RA and is able to authorize the issuance of one or more fraudulent certificates by the CA.
3. **CA System Compromise:** The attacker infiltrates the CA and succeeds in using the CA's issuance system to issue one or more fraudulent certificates. In this scenario, the

attacker does not obtain a copy of the CA private key, but is able to use that key to issue fraudulent certificates. In addition, having compromised the CA system at this level, the attacker can generate one or more signed counterfeit certificate revocation lists (CRLs). This can bolster the effectiveness of an attack that leverages the fraudulent certificates by providing relying parties the forged CRLs, which indicate that fraudulent certificates have not been revoked (i.e., are okay to use). Because the CA system has been compromised, it is possible that the attacker can also alter logs to obscure which certificates or CRLs were inappropriately signed.

4. **CA Signing Key Compromise:** The attacker successfully gets a copy of the CA signing key and is able to use it to sign fraudulent certificates and CRLs at will. To get a copy of the CA signing key, the attacker could steal a copy or attack the key and algorithm to determine the key (e.g., use factoring or brute-force attacks). Realistically, an attacker is much more likely to succeed in obtaining a copy of the key than in attacking the key and algorithm, assuming that the key has been properly generated, because CAs have traditionally used key lengths that are long enough to make factoring or brute-force attacks infeasible. However, due to the increased sophistication and resources of attackers today and the possibility of a software defect causing poor random number generation[2] or other issues, it is a scenario that should be considered.

It is important to consider both internal and external CAs when preparing to respond to the possible occurrence of each of these types of attacks. Many organizations use greater numbers of certificates issued from their internal CAs than from external CAs. Consequently, the impact of an internal CA compromise could be as significant as an external CA, if not more so.

4. Preparing for and Responding to a CA Security Incident

The steps that an organization should take in preparing for and responding to a CA security incident depend on the PKI role(s) it plays.

a) CAs

CAs, both internal and external to an organization, must follow security best practices in order to prevent a CA compromise. Regular third-party audits and reviews should be performed to ensure that processes, policies, and security mechanisms are properly implemented and cover all possible attacks. CAs must ensure that they discover a compromise as quickly as possible by implementing tracking and detection mechanisms and performing regular manual operational sanity checks.

[2] Historically, random number generation issues have been discovered and publicly disclosed in several encryption libraries, requiring organizations to update the libraries in their environments and generate new keys.

To mitigate the effects of a possible CA compromise, CAs must establish well-defined communications plans for informing subjects, relying parties, and other stakeholders with sufficient details about the type of compromise so these parties can implement the appropriate remedial actions.

If an impersonation or RA compromise attack results in the successful issuance of fraudulent certificates, the CA must revoke the certificates and inform the organizations identified as subjects in the fraudulent certificates and all potential relying parties that might rely on those certificates. If a CA system compromise or signing key theft occurs, the CA's certificate(s) must be revoked by any CAs that have issued certificates to it, all subjects that the compromised CA has issued certificates to must be notified that they will require new certificates, and all possible relying parties must be notified.

b) RAs

RAs must ensure that they use best practices for vetting certificate requests to prevent an impersonation attack. The required practices for vetting certificate requests are documented in the certificate policies (CPs) associated with the CAs served by the RA. They must also implement security best practices to prevent an RA compromise attack. CPs also will document generic security control requirements for RAs, but more specific information may be found in NIST's Federal Information Security Management Act (FISMA) guidelines.

c) Subjects and Relying Parties

Due to the broad proliferation of certificates for the security of mission-critical systems, nearly all organizations act as subjects (with certificates issued to their systems, users, or both) and all act as relying parties (with systems that rely upon certificates from other systems or users for transactions or other operations). If a CA compromise occurs, organizations may need to replace end entity certificates and/or trusted root certificates. Organizations that are not prepared to respond may not be able to respond in a timely manner and may experience extended service interruptions.

1) Preparing for a CA Security Incident

Organizations should implement the following steps to prepare for a CA compromise:

Review existing applications and servers, identify and document applications and servers that rely on certificates for security and noting whether they:

- have end entity certificates of their own, or
- accept public key certificates from other users or servers.

Note that these conditions are not mutually exclusive; for many systems, both conditions will hold.

a) End Entity Certificates

For each system that has end entity key certificates of their own:

1. Document logistics and security information required to respond to CA compromise:
    a. Document the system or application owner, with contact information.
    b. Identify the system where the certificate and associated key material are stored.
    c. Document which CA(s) issued the current certificate(s), noting whether the certificate was issued by an internal or external CA.
    d. Document any policies asserted in the certificate policies extension.
    e. Identify the "usual" trust anchors that would be used in certificate path validation. (For commercial CAs, this is usually a root CA operated by the same corporation. For government CAs, this might be the Federal PKI's Common Policy Root CA.)
    f. Document the certificate expiration date, algorithms, and key lengths. (This is not relevant for CA compromise, but helps avoid unexpected system outages from certificate expiration or security risks due to algorithm or key length breakages.)
2. Identify or document the procedures required to replace the system or application's public key certificate.

    Note: In exceptional cases, the public key certificate may be hard coded into the application itself, so replacing the certificate would require updating or replacing the operating system or application.
3. Document the availability requirements for the system, based on the consequences of an extended system outage.

b) Certificate Authorities in Use

Review the collection of CAs that have issued certificates to applications and systems in the organization.

1. Identify backup source(s) for rapid acquisition of new certificates with appropriate policies.

2. For each system or application, identify a primary and optionally a backup source for new certificates in the event of compromise of the current certificate's issuing CA.[3]

c) Trust Anchors

For each system that accepts public key certificates from other users or servers to establish security:

1. Identify the system or application owner and contact information.
2. Document a list of all trust anchors on the system.
3. Document contents/source of installed trust anchors (especially any deviation from the manufacturer's baseline).
4. Identify or document the mechanism(s) used to establish or replace trust anchors.
    a. If the mechanism is centrally managed by the manufacturer or organization, ensure it is on and ready to handle updates; and
    b. Ensure that policies and procedures include teleworkers!
5. Remove any trust anchors that should not be trusted.
6. Identify or document the mechanism(s) used to manage end user or end system certificates recognized by the system, i.e., if the system uses a white list or links to Active Directory.
7. Document configuration of path validation mechanisms, including revocation checking and any policy settings. If path validation or status checking is not in use, document why the certificates can be accepted without validation. If certificate policy restrictions are not in place, document why policy restrictions are unnecessary.

d) Applications

Organizations should also develop policies for applications development and procurement:

1. For applications that have public key certificates of their own, procurement requirements should ensure that CA independent mechanisms exist to obtain new system/application certificates.
2. For applications that accept public key certificates from other users or servers to establish security, procurement requirements should ensure that mechanisms are provided for trust anchors management, and that mechanisms for client certificate

[3] The creation of a new CA or establishment of a relationship with a new external CA after a CA compromise can cause significant delays in issuing new certificates, so it is prudent to establish backup CAs as a precautionary measure.

management mechanisms (e.g., policy-based validation or approved user white lists) can implement the application's security requirements.

Once a baseline describing current practices has been established, organizations should establish written certificate management policies to ensure sound deployment and management practices, including the tracking of certificate locations and ownership. Ensure that all stakeholders are aware of and follow the policies.

2) Responding to a CA Security Incident

If a CA security incident occurs, organizations must ensure that they understand the type of compromise that has occurred.

If the security incident was the result of an impersonation or RA compromise, an organization should need to take action only if the fraudulent certificate(s) identified one of their systems or users. In this case, the organization should ensure that the fraudulent certificates have been revoked by the CA, and new certificates have been issued. This action will alert all relying parties of the problem, providing that revocation checking is enabled.

If a CA system or signing key compromise occurs, the organization should perform the following steps:

1. Ensure that certificates issued to the organization's systems or users from the compromised CA are revoked.
2. Notify all owners of the affected certificates about the CA compromise and establish a point of contact or helpdesk for responding to questions and providing guidance and instructions.
3. Replace all certificates from the compromised CA with new certificates from a different CA.
4. Ensure that all relying parties have the certificate trust chains required to validate certificates from the new CA.
5. Ensure that revocation checking is enabled on all relying party systems.

If the compromised CA is a root CA, the root certificate from the compromised CA must be removed from all relying party systems.

5. Conclusions

Successful attacks on CAs have made CA compromises a tangible threat to which organizations must be prepared to respond. Because organizations so broadly rely upon TLS and SSL to secure systems and data, a CA compromise may require the replacement of end entity certificates, trusted root certificates, or both on hundreds or thousands of systems. To ensure that they can

respond in a timely manner, organizations must take preparatory steps and establish well-defined response plans for CA security incidents.

ITL Bulletin Publisher:
Elizabeth Lennon, Writer/Editor
Information Technology Laboratory
National Institute of Standards and Technology
Email

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.