Certificate Revocation With CRL

Keith Bogart

CCIE #4923

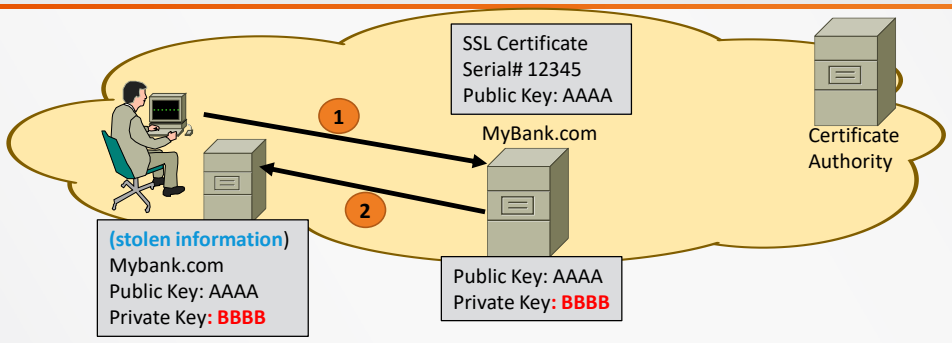
- kbogart@ine.com
- @keithbogart1
- linkedin.com/in/keith-bogart-2a75042

CCIE Routing & Switching

Topic Overview

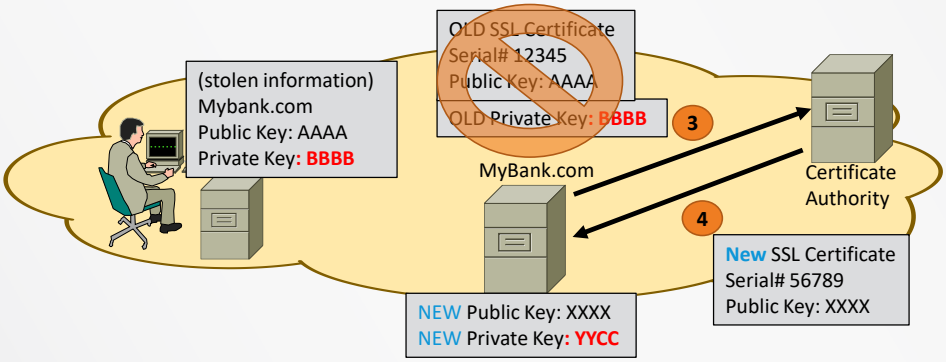
- Why Certificates Must Sometimes Be Revoked
- Methods For Revocation Checks
- Certification Revocation Lists

Worst Case Scenarios



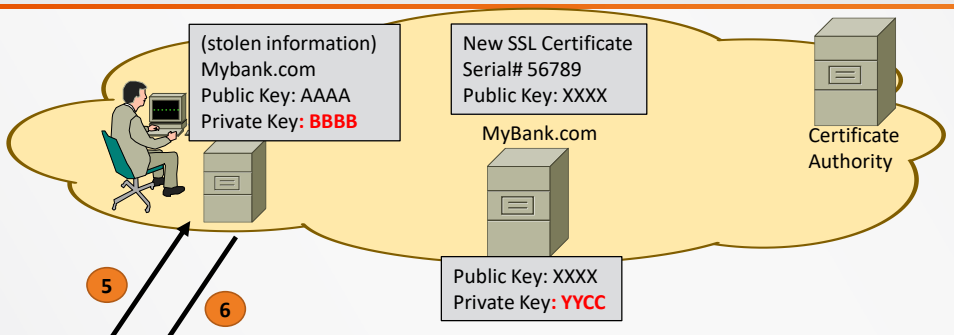
1. Attacker successfully hacks server hosting MyBank.com
2. Retrieves server's certificate AND RSA Private Key

Worst Case Scenarios



3 & 4. Realizing that Private Key has been compromised, MyBank.com revokes current Certificate and obtains a new one.

Worst Case Scenarios



5. Malicious Actor somehow redirects Web Client to his own, malicious copy of MyBank.com

6. Web Client initiates successful TLS connection to MyBank.com (attacker's version) and encrypts username/password using shared secret key.

Malicious Actor may use DNS poisoning, malvertising, or any one of numerous ways to get you to think that you need to go to your banking website…and they'll provide all the information you need to redirect you to their server.

-

If you are using the Malicious Actor's Public key to establish a TLS session, your webclient will derive a shared, encryption key and send that back to their server…encrypting it with their Public Key (that you THOUGHT was MyBank's public key).

-

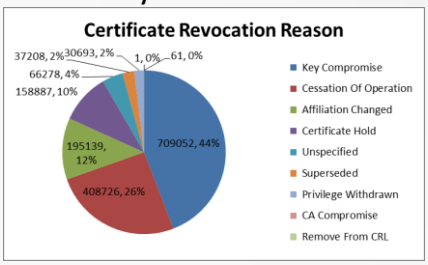
Malicious Actor will decrypt the shared, secret key you've uploaded using their Private Key (that was stolen from MyBank) and now present to you the encrypted website (a duplicate with possible minor visible differences) which will probably prompt you to input critical information (username/password).

-

Once you give them that information…they don't even need to TRY to pretend anymore. No matter what they display to you at that point, they can now login to the REAL banking website, using your credentials, and drain your account dry.

Revoking Certificates

- There are a variety of reasons Digital Certificates may need to be revoked prior to their expiration dates;
  - Compromise of the Private Key
  - Change to the DNS Record
  - Website closes down
  - Company change of ownership



https://www.grc.com/revocation/ocsp-must-staple.htm

- Clients that receive Server Certificates need to know if that Certificate has been revoked in order to detect spoofed websites.

Some statistics say that 44% of all revoked certificates are due to Private Key compromise.
https://www.grc.com/revocation/ocsp-must-staple.htm

-

Cessation of Operation is the second largest cause of revocation.

-

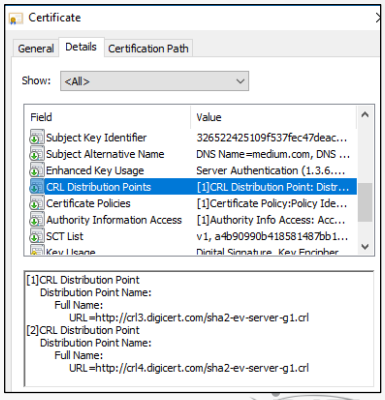
Pie chart taken from https://www.grc.com/revocation/ocsp-must-staple.htm

Methods For Revocation Checks

- CRL – Certificate Revocation Lists
- CRLSets
- OSCP – Online Certificate Status Protocol
  - OSCP with Soft-Fail
  - OSCP Stapling
  - Must-Staple Extension

Certificate Revocation Lists

- CRL = a list of the serial numbers of unexpired security certificates which ***have been revoked by their issuer*** and should no longer be trusted.
- Historically, the first method developed.
- Each CA maintains their own CRL
- CA provides pointer to CRLs within Certificates they generate.
- The problem:
  - CRLs have become very long over time (up to 28M Bytes)
  - Reaching a CRL requires reachability to the CA from the Web Client.
  - May slow down the TLS transaction.



CRLs contain millions of revoked Serial Numbers, and are in a continual state of change as old certificates expire off the lists (no longer trusted anyway due to their age) and serial numbers of newly revoked certificates are added.

-

CRL architecture introduces the dependency between client and CA infrastructure, making it prone to the CA server's availability issues and downtimes.

-

CRLs are typically updated every 24-hours by CA's, and are valid for 1-week (some are updated only weekly).

-

CRLs are still the most secure way to anonymously determine revocation status of any given Cert (OCSP is also good…but is not anonymous as we'll see).

-

Unfortunately, CRLs are effectively ignored by most end-clients.