Improving PKI Revocation

An approach to improving the reach and efficiency of revocation checking for SSL/TLS

Research by Dartmouth College
and New York University
Reported by: Scott Rea
Sr. PKI Architect, DigiCert Inc.

Research Advisory

Research

- This is a report on research and development activities being undertaken by Dartmouth College and New York University in collaboration with industry and other partners.
- Collaborators:
  - NYU: Prof. Massimiliano Pala pala@nyu.edu
  - NYU: Mallik Arjun mallik.v.arjun@gmail.com

  - Dartmouth: Alexandra Grant Alexandra.C.Grant.12@Dartmouth.edu
  - Dartmouth: Prof. Sean Smith sws@cs.dartmouth.edu

NYU Dartmouth

CAs : High Value Targets

- Attackers are seeking to get control of credentials issued by trusted CAs via a process known as a Man-in-the-Middle (MitM) attack
- Targeting CAs = potential for more generous results over single websites
- If successful:
  - Allows the attacker to generate as many keys as it wants
  - Compromise many domains vs single domain

NYU Dartmouth

ICAs in the News…

- **Comodo** – Mar 2011
  - **Multiple RA breaches** : mis-issuance of at least 9 certificates
  - Italian & Brazilian RAs were targeted
- **StartCom** – Jun 2011
  - **Breach of Server** : no certificates mis-issued
  - DoS of services to StartCom customers result
- **DigiNotar** – Jul 2011 (didn't disclose until Aug 2011)
  - **Major Breach** : 500+ certs issued caused by poor security
  - CA now out of business
- **Globalsign** – Sept 2011
  - **Breach of Server** : but no certificates were mis-issued
- **DigiCert Malaysia** (no relationship to US company) – Oct 2011
  - Issues certificates with weak keys, lacking extensions to revoke them
  - Bad certs were re-purposed to sign **malware**
  - CA certificate was revoked
- **KPN** (another Dutch CA) – Nov 2011
  - **Breach of Server** : no certificates mis-issued
  - DoS of services to KPN customers result

NYU Dartmouth

Inconsistent Revocation

- Experience post CA attacks reveals Revocation is not handled as consistently as it needs to be by web clients
  - Revocation information is not obtained in a timely manner
  - CRL validity lengths are often too long (lack of fresh data due to caching)
  - OCSP is not deployed as consistently as it needs to be, nor consumed by relying parties in a consistent manner
  - Difficult to manage root TA revocation

NYU Dartmouth

CAB Forum Response

- In light of recent attacks, the ICA industry has also mobilized to address the deficiencies.
- CAB Forum is focusing on the following areas to bolster ICA consistency, security, and reduce the potential for breakdowns due to the weakest link principle:
  - Published a minimum set of security standards for operations and identity vetting to which EVERY ICA must attest
  - Support implementation of available Revocation mechanisms and define more timely, available, and efficient protocols to be implemented in the future
  - Implement controls that enhance the system's ability to discover and repel MitM Attacks
  - Working with industry audit professionals to define stronger audit controls that can be applied to demonstrate compliance with standards and best practices

NYU Dartmouth

CABF Revocation WG

- **CAB Forum has instantiated an Industry Working Group to address the deficiencies in Revocation**
  - Participants from ICAs, Browsers, Research & EDU, IETF, major Relying Parties
  - Monthly conference calls, 1st Face-to-Face at NYU in April
- **A couple of different problems to solve from different perspectives**
  - Revocation Data Availability Problem
  - Access time to revocation services
  - High maintenance costs for high-volume environments
  - How to manage revocation of Trust Anchor Roots
- **Initial Proposals**
  - **Short term** → Lightweight OCSP Profile [RFC5019] + CDN friendly
  - **Mid term** → push for OCSP over DNS
  - **Long term** → CA whitelists

NYU Dartmouth

CABF Rev WG: Review

- **ICAs Current Best Practices**
  - Multiple revocation sources e.g. CRL and OCSP
  - Pre-computed responses where possible for OCSP
  - Publication every few hours / once a day
  - Geographically dispersed validation authorities to get revocation data as close as possible to Relying Party requestors
  - Use different distribution mechanisms → CDNs, Stapling
- **Issues**
  - Only GET (POST can not be cached) → clients still use POST!
  - Different encoding of the request → CDNs cache miss!
  - High costs for deploying OCSP servers
- **Opportunities**
  - OCSP as small CRLs
    - No need for OCSP requests
    - Need to provide OCSP responses as efficiently as possible

NYU Dartmouth

Short-Term Approaches

- **Promote Best Practices in ICA Community**
  - Particularly:
    - Pre-computed responses
    - Geographically dispersed validation authorities to get revocation data as close as possible to Relying Party requestors
    - Create a number of best practices whitepapers
- **CRL Sets for Intermediates**
- **Update for RFC5019**
  - Determine what if any changes might be required in RFC 5019 Lightweight OCSP
  - Use different distribution mechanisms → CDNs, Stapling
  - Multi-stapling support
- **Address Implementation Issues**
  - Encourage/contribute to clients moving to GET mechanism
  - Encourage/contribute to servers supporting OCSP Stapling by default

NYU Dartmouth

Mid-Term Approaches

- **DNS can be used to distribute OCSP responses**
  - No need for request/response protocol
  - Allows to lower the costs of distributing revInfo to clients
    - **Use of the DNS caching system**
  - Possible for SSL/TLS certificates for larger sites
- **Current Challenges**
  - OCSP responses waste bits on the wire if cert is valid
  - DNS allows for single UDP packet (if resp < 512bytes)
  - Use of EC keys might be advisable
  - Definition of DNS-based URLs for OCSP distribution
  - Allow for fallback URLs for backward compatibility
    - **Some clients only query the first URL in AIAs**

NYU Dartmouth

Mid-Term Approaches

- **Lightweight Internet Revocation Tokens**
  - Similar to Request-less OCSP
  - Client-known data is not included in the response
  - Small size (< 200~300 bytes with EC signatures)
  - Compatible with different transport protocols
    - **HTTP (CDNs), DNS, Peer-to-peer**

- **Proposal for a new I-D within IETF for ALIRT**
  - Alternative Lightweight Internet Revocation Tokens (ALIRTs**)**

NYU Dartmouth

Long-Term Approaches

- **CA whitelisting**
  - Need for a mechanism to select different level of trust for CAs
  - Possibly build a common CA accreditation body (CAB Forum WIP)
- **Short Lived Certificates**
  - Is there benefit and capability to implement a SLCS service for TLS?
- **Solutions are being discussed in CAB Forum**
  - No common vision, yet
  - Costs and operational barriers
  - … summarizing, stay tuned to this space..!

NYU Dartmouth

Summary

- **Recent attacks on Internet CAs highlighted the need to address deficiencies in Revocation practices**
- **CAB Forum has instantiated an Industry Working Group to address this**
  - Participants from ICAs, Browsers, Research & EDU, IETF, major Relying Parties
  - Mailing List, regular meetings, agreed work items and time table
  - Initial Proposals
    - **Short term** → Lightweight OCSP Profile [RFC5019] + CDN friendly, including promoting OCSP Stapling support in Servers and GET methods for Clients, CRL Sets for Intermediates
    - **Mid term** → push for OCSP over DNS, ALIRTs
    - **Long term** → CA whitelists, SLCS
  - Collaboration to produce and promote a number of industry whitepapers
- **This WG represents a Work-In-Progress to attempt to address the issue with inefficient revocation**

NYU Dartmouth

Questions

- **Questions?**
  - **Anyone interested in participating/contributing to the CABFRev WG should send an email to me scott@DigiCert.com or ben@DigiCert.com requesting such, and indicate a relevant reason/commitment for doing so…**

NYU Dartmouth

DigiCert Contacts

Website: http://www.DigiCert.com/

Email: support@DigiCert.com

Scott Rea: (801) 701-9636, Scott@DigiCert.com
http://www.digicert.com/news/bios-scott-rea.htm

NYU Dartmouth