State of PKI for SSL/TLS

NIST Workshop on Improving Trust in the Online Marketplace

Russ Housley
Vigil Security, LLC

Introduction

State of the PKI for SSL/TLS:

- Mostly working, but too fragile
- Facing motivated attackers
- Straightforward improvements at hand

Attacker Incentive

- CAs suffer a large economic asymmetry
- Huge economic or political value to CA compromise
  - Single targeted certificate can have such a large value that attacker might deploy huge resources
  - What is the value of a certificate for “*.google.com”?
- Attackers have caused significant financial harm to CAs in order to gain unfettered access to selected commercial websites

Web PKI is Fragile

- Certificate Status Checking
- Certificate Subject Names
- Cryptographic Algorithms
- Deviation from Standards

Browser Certificate Status Checking

- Certificate status checking is often turned off
  - Extra round trips make path validation too slow
- When certificate status cannot be found, certificate is considered good
- Inconsistent checking by different browsers
  - Some check OCSP, but do not check CRLs
  - Some use OCSP only for end entities; use CRLs for CAs
  - Some implement OCSP stapling; some do not

Browser Certificate Status Checking

- Certificate status checking is often turned off
  - Extra round trips make path validation too slow
- When certificate status cannot be found, certificate is considered good
- Inconsistent checking by different browsers
  - Some check OCSP, but do not check CRLs
  - Some use OCSP only for end entities; use CRLs for CAs
  - Some implement OCSP stapling; some do not
- **Conclusion: Need consistent revocation checking**

Certificate Subject Names

- CAs in the Web PKI are not aligned to the hierarchical domain name space
- Any CA can issue for any domain name
  - No way for the relying party to know if the domain owner wanted the certificate to be issued
  - No way for the domain owner to control which CA issues a certificate containing their name
- All CAs must defend against attacks
  - Web PKI trust requires all CAs to be well protected
  - All domain names are at risk from the failure of *one* CA

Certificate Subject Names

- CAs in the Web PKI are not aligned to the hierarchical domain name space
- Any CA can issue for any domain name
  - No way for the relying party to know if the domain owner wanted the certificate to be issued
  - No way for the domain owner to control which CA issues a certificate containing their name
- All CAs must defend against attacks
  - Web PKI trust requires all CAs to be well protected
  - All domain names are at risk from the failure of *one* CA
- **Conclusion: Need to leverage the hierarchical structure of the DNS**

Cryptographic Algorithms

- Many CAs still have certificates with obsolete hash algorithms or short keys in the trust anchor store
- Better and better attacks on obsolete hash algorithms
  - MD5: Wang in 2004; Stevens in 2007; Flame in 2012
  - Serious problem for Web PKI when these are combined with redirection attacks

Cryptographic Algorithms

- Many CAs still have certificates with obsolete hash algorithms or short keys in the trust anchor store
- Better and better attacks on obsolete hash algorithms
  - MD5: Wang in 2004; Stevens in 2007; Flame in 2012
  - Serious problem for Web PKI when these are combined with redirection attacks
- **Conclusion: Issue new certificates from a CA using SHA-256 and 4096-bit public key**
- **Conclusion: Use DNSSEC to reduce opportunities for redirection attacks**

Deviation from Standards

- Web PKI deviates from RFC 5280
- Web PKI handles Certificate Path Construction, Constraints, and Extended Key Usage differently
- Deviation from the standards has consequences
  - Leads to lack of interoperability
  - Inconsistency leads to complexity
  - Sometimes leads to significant surprises

Deviation from Standards

- Web PKI deviates from RFC 5280
- Web PKI handles Certificate Path Construction, Constraints, and Extended Key Usage differently
- Deviation from the standards has consequences
  - Leads to lack of interoperability
  - Inconsistency leads to complexity
  - Sometimes leads to significant surprises
- **Conclusion: We need to align standards and actual practice**

Summary

- Browsers inconsistently check for revocation
- Browser trust anchor model is fundamentally flawed
  - Any CA can issue a certificate for any DNS name
- CAs still using obsolete hash algorithms and small keys
- Browsers and CAs deviate from RFC 5280
  - Inconsistency in browsers makes it hard for CAs to tackle the above problems
  - Inconsistency in CAs makes it hard to demand that browsers reject ill-formed certificates