Extended Security Considerations for the Automatic Certificate Management Environment (ESecACME)

Tobias Fiebig, Kevin Borgolte

TU Delft

The Problem: Domain Validation

- The ACME protocol is a tool to automate Domain Validation (DV)

- Uses proxies to assert authority
  - DNS names pointing to something, having a certain mail address,…

Problem I: *-use-after-free

- Attackers can re-use IP addresses if a stale DNS record still point to them
  - Serious problem (found >700,000 Domains only with Amazon EC2)
- Holds for any other proxy resource

Problem II: (Forced)-on-path-attacks

- Normal Monkey-in-the-Middle
- BGP attacks

Problem III: Attacks on DNS

- Cache poisoning
  - Various forms of varying efficiency
  - Most recent ‘attack’: Overwrite additional section with fragmentation

Problem III: Attacks on DNS

- Cache poisoning
  - Various forms of varying efficiency
  - Most recent ‘attack’: Overwrite additional section with fragmentation
- Force-use-stale (if dnsop-serve-stale)
  - Force use of stale record when rolling over VMs (related to use-after-free)

Mitigation

- *-use-after-free
  - Require a TLSA record for the key to be in set and DNSSEC validation to be in place
  - Use proof-of-prior-key-ownership based validation
- (Forced)-on-path-attacks
  - See above
  - + Multi vantage point validation
- DNS fnordery
  - Check for small MTU packets
  - Chase additional section yourself
  - Validate DNSSEC!
  - Do not do dnsop-serve-stale and do not serve for validation from cache

Why a draft?

- Explicit operational requirements for operators using ACME in a CA
- draft-ietf-acme-acme-16 Sec/Ops requirements hold a subset of suggestions
  - Contains:
    - DNSSEC
    - Trusted infrastructure
    - Multi-vantage-point
    - Buried deep in the draft
  - Misses:
    - When to be more strict
    - *-use-after-free
    - TLSA (No trust on first use needed for HTTP)
    - Chasing additional

History

- First paper February 2018
- Presented in ACME WG at IETF102
- Write a draft here, so we can take a better look
- Moved to secdispatch after ML discussion because it is not protocol specific