SecSpider and TAR (Expanding it)

Eric Osterweil

Dan Massey

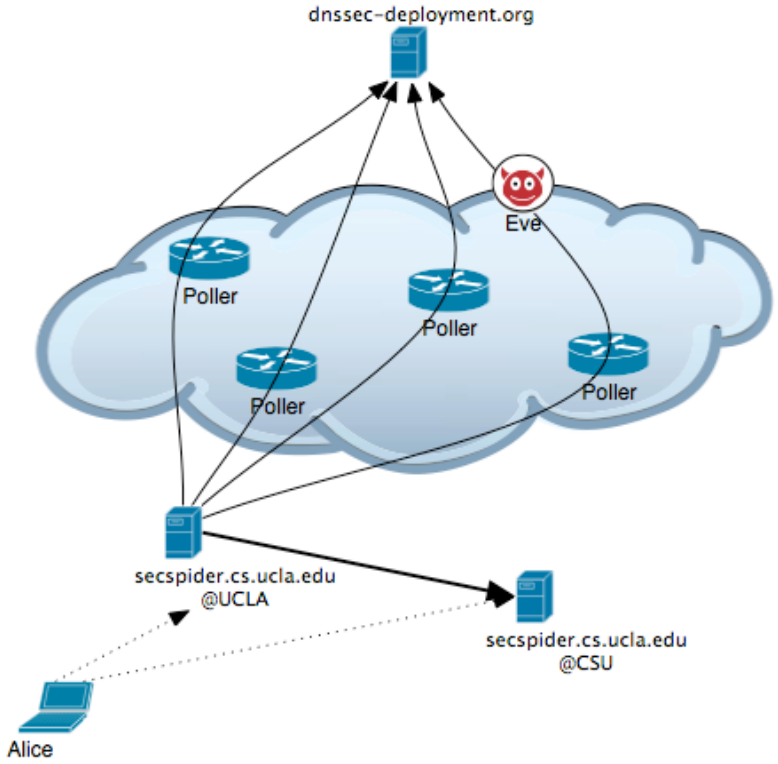
Lixia Zhang

SecSpider

- Public view of keys from distributed vantage points (pollers)
- We track the DNSKEYs for almost 12,000 zones
- Roughly 900 zones seem to serve “production” systems
  - WWW or SMTP
- We track as key lifetimes signature lifetimes, when they change/rollover, get re-signed, etc for all of them
- In addition to our web interface, we now offer our key data over DNSSEC

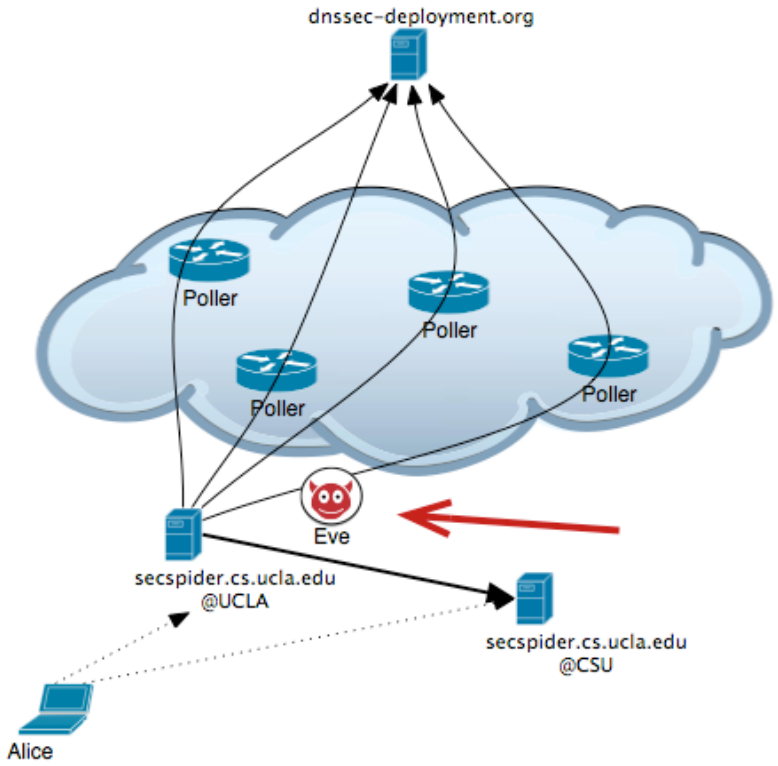
Resilience Through Distributed Polling

- We poll from around the World
- If an attacker (Eve) spoofs some of our pollers (less than *all*) we see evidence
  - Our DNS zone does not list keys if there is disagreement
- Attackers must spoof all pollers to fool us
- We use DNS redundancy (slave servers) for the zone



Local View

- We secure queries to and from each poller
  - TSIG
- Eve cannot spoof replies by interposing between SecSpider and pollers
  - She could block responses though
- She can attack the zone's server, but we push to remote nameserver(s)
  - Currently just CSU



Usage

- SecSpider can augment other approaches
- Resolvers may query TAR(s) and SecSpider
  - When data exists in a TAR the SecSpider data can be a sanity check
  - When data does *not* exist in a TAR, the resolver will have SecSpider's answer
- The dangers of using SecSpider
  - SecSpider could have been spoofed (requires a lot of coordination)
  - Others?

Summary

- SecSpider can provide information about *all* zones that have been registered
- To fool SecSpider, Eve must fool all pollers around the World
  - If zones follow best-practices, their nameservers are *also* deployed in diverse locations
- We are working to harden SecSpider more
  - Adding redundancy
  - More exhaustive polling
  - More pollers
  - Other ideas?