DKIM Threat Analysis

Jim Fenton <fenton@cisco.com>

Threat Analysis – Current Version Summary

- draft-fenton-dkim-threats-01.txt
- Current version was written to assist the chartering decision

  Describe the threat landscape

  DKIM’s effectiveness against it
- Four major sections:

  Who are the bad actors?

  What are their capabilities?

  Where are the bad actors?

  What are the bad actors trying to do?

What the Threat Analysis Doesn’t Say

- Doesn’t characterize the threat in terms of spam and phishing
    - Although the bad acts will sound familiar!
    - The point is that there is still benefit
- Doesn’t characterize the bad acts as “forgery”
    - It’s clear from discussion on the list that forgery is different things to different people
    - DKIM doesn’t provide an assertion of authorship
- Doesn’t discuss repudiation
    - Another term with wide-ranging meaning

Scope of the Threat Analysis

- Threat Analysis is specific to DKIM
  - Current version was written to support the DKIM WG chartering decision
  - WG may decide to extend its scope, reorganize, etc.
    - Just like any WG draft
- Analysis focuses on threats DKIM is trying to address
  - There are other threats not addressed by DKIM
  - Other WGs may be chartered in this space if there are approaches which address more/different threats

Scope (continued)

- Focus is on the threat environment, more than on new threats to DKIM
  - More detail on threats to DKIM in the Security Considerations sections of the drafts
  - Difficult to be certain of threats to DKIM until it is finalized
- A few important threats thought to be inherent in all DKIM-like protocols are discussed
  - Message “replay” attack
  - Handling of unsigned messages
  - Look-alike and throw-away domains
  - Key management vulnerabilities

Going Forward

- Threat Analysis is the first deliverable in proposed WG charter
  - Likely to change considerably from -01 draft
  - Needs to focus on issues that can be determined in advance of the final design
- Effect[iveness] of SSP needs specific consideration
- WG/Security Area will need to define boundaries
  - What threats are protocol threats?
    - Stephen Farrell’s timing attack example
    - Jim Fenton’s bribery attack example

Summary

- Focus for dkim-threats-01 (and -00) was to answer questions related to chartering
  - Does DKIM do something useful?
- Threat analysis is also a proposed WG deliverable
  - The WG document is likely to be considerably different
  - WG will need to decide what belongs in it
- Remember that the threat analysis is the first WG deliverable
  - Set expectations accordingly

Backup Slides

Table of Contents (-01)

- 1. Introduction
- 2. The Bad Actors
- 3. Capabilities of the Bad Actors
- 3.1. General capabilities
- 3.2. Advanced capabilities
- 4. Location of the Bad Actors
- 4.1. Externally-located Bad Actors
- 4.2. Within Claimed Originator's Administrative Unit
- 4.3. Within Recipient's Administrative Unit
- 5. Representative Bad Acts
- 5.1. Use of Arbitrary Identities
- 5.2. Use of Specific Identities
- 5.2.1. Exploitation of Social Relationships
- 5.2.2. Identity-Related Fraud
- 5.2.3. Reputation Attacks
- 6. Attacks on Message Signing
- 6.1. Unsigned Messages
- 6.2. Use of Throw-Away Addresses
- 6.3. Message Replay
- 6.4. Control of Key Management
- 7. IANA Considerations
- 8. Security Considerations
- 9. Informative References

Who are the Bad Actors?

- Wide range of sophistication/motivation
  - Senders of unwanted mail using commercial tools
  - Professional bulk senders of unwanted mail
    - Deploy specific infrastructure and register domains
    - May use zombies
  - Fraud perpetrators who may have substantial financial benefit
    - May attack DNS or routing infrastructure

What are the Bad Actors' Capabilities?

- Everyone has
  - Access to public keys
  - Access to messages signed by various domains
  - Ability to sign messages on behalf of domains they control
- Some have ability to:
  - Generate substantial numbers of messages
  - Construct arbitrary messages and submit them through unprotected MTAs with arbitrary envelope information
  - Resend previously-signed messages, potentially very quickly

Capabilities (cont)

- A few have:

  Ability to manipulate IP routing information

  Ability to influence DNS, at least locally and for a limited duration

  Access to significant computing resources, perhaps through the use of zombies

  Ability to wiretap other Internet traffic

Where are the Bad Actors?

- External to originator and recipient
  - Prime focus of DKIM
  - Trust relationships do not generally exist to permit alternative approaches
- In the claimed originator's administrative unit
  - Generally addressed by authenticated submission to gain access to signing MTA
  - Not directly addressed by DKIM
- In the recipient's administrative unit
  - Authenticated submission to prevent introduction of messages with forged authentication results
  - Not directly addressed by DKIM

What are the Bad Acts?

- **Send messages with arbitrary origin address**
  - **Bad actors may sign messages from domains they control**
    - **Accountability limited by domain registration**
    - **Future reputation/accreditation systems may help**
  - **Unable to sign messages from “phantom” domains**
- **Send messages with specific origin address**
  - **Exploitation of social relationships**
  - **Identity-related fraud**
  - **Attacks on reputation**

Important Attacks on DKIM

- Unsigned or incorrectly signed messages
  - Since unsigned messages aren’t necessarily bad, how to handle them?
  - SSP helps, but is not perfect either
- Throw-away addresses
  - Exploits lack of accountability in domain registration
- Message replay
- Control of key management
  - Absent DNSSEC, this is a problem for DNS-based key management