# Client Puzzles for IKEv2

- Yoav Nir
- draft-nir-ipsecme-puzzles-00

# Background

- An IKE gateway that is willing to accept IKE initiation from arbitrary sources on the Internet is vulnerable to DoS attacks.
  - A single IKE_INITIAL request creates a half-open SA that lasts for a while.
  - The gateway allocates memory and generates a D-H key-pair.
  - If you can send a legitimate-looking IKE_AUTH request, the gateway also finishes the D-H calculation and attempts to decrypt.

# Background

- IKEv2 has the "cookie" mechanism.
- When activated, a single IKE_INIT request does not create state.
  - Effective against an attacker sending multiple IKE_INIT requests from spoofed addresses.
- Does not help if the attacker uses a real source address and can continue the handshake.
- Not effective against DDoS attacks such as those performed by bot-nets.

# Purpose of Puzzles

- Increase the cost of each half-open SA to the attacker.
  - Do this only when under attack.
  - Require the client to solve a puzzle to discover the cookie.
  - Cost of the puzzle should be tolerable to a legitimate client.
    - About 1 second of calculation is about right.
- Problem is, not all clients are clreated equal.

# Puzzles

```
   Initiator                                  Responder

-------------------------------------------------------------
   HDR(A,0), SAi1, KEi, Ni  -->
                                <--  HDR(A,0), N(PUZZLE)
   HDR(A,0), N(COOKIE), SAi1,
       KEi, Ni  -->
                                <--  HDR(A,B), SAr1, KEr,
                                         Nr, [CERTREQ]
   HDR(A,B), SK {IDi, [CERT,]
       [CERTREQ,] [IDr,] AUTH,
       SAi2, TSi, TSr}  -->
                              <--  HDR(A,B), SK {IDr, [CERT,]
                                       AUTH, SAr2, TSi, TSr}
```

# Puzzles

- Puzzles have proved to be effective at mitigating DoS attacks in the past.
- Puzzles could take many forms: completing a partial pre-image of a hash, completing a partial encryption key, partial HMAC key, partial private key for a public EC key.
  - My draft uses a partially given cookie, and a hash of said cookie.
- Setting the right difficulty is a lot harder today than it was 6 years ago.

# Design Decisions

- Responder sends a Cookie, or a puzzle, or neither. Never both.
- “Legacy” initiators will balk at puzzles.
  - But work fine when gateway is not under attack.
- The solution to the puzzle is sent as a Cookie, not some special new notify type.
- Using partial hash pre-image.
- Possible to tune difficulty level to level of attack
  - But not to Initiator capabilities.

# Mea Culpa

- Forgive me, for I have sinned.
- I have violated the IPR rules.
- I know of a patent regarding this technology, and I have not made an IPR disclosure.
- The patent is owned by Oracle. I have talked to them before submitting this draft. They asked that I submit the draft so that they can publish the IPR disclosure.
- Last I heard (last week), their lawyers are still working on it.

# Questions?