Off-Path BoF Problem/Solution Overview

Paul Francis

Cornell University

Research Goal

- Robust, secure, connection establishment
  - Robust: always works
    - Even if behind NATs, firewalls, different network layers
  - Secure: In a firewall sense---allow connections you want, disallow those you don't want

- In other words: do what *IP addresses*, *ports*, and *DNS names* were meant to do in the original IP architecture

More technology goals

- Only meant for “non-public client-server” connections
  - cnn.com can still use addr/port
- Name-based
  - User-friendly
  - Not tied to a single network layer
  - Or to a network access point
- Provide firewalls (construed broadly) with information they need to make go/no-go decisions
  - Authenticated, named endpoints and applications

More technology goals

- Be explicit about all the policy players
  - Allow for control at ends *and* middles
  - Let market/courts decide who controls what
- Negotiation of connection parameters
  - Type of security (IPsec, SSH, SSL, …)
  - Type of transport (TCP, UDP, SCTP, HIP, …)
  - Type of network (v4, v6, other?)
  - Routing through middleboxes?

Non-goals

- QoS

Ultimately: New “sockets” layer

- The set of functions an application can count on
  - In the OS and Infrastructure
- Today: IP, DNS
- Goal: Ubiquitous and generic support for signaling
  - Lets just call this “newsock” for now

BoF goals: IRTF

- Discuss creation of an IRTF group
- Drum up interest in an IRTF group
  - (assuming folks think it is a good idea)
- Why not just call up my research buddies?
  - Want mix of research and practice
  - Want a focused output---protocols and prototypes
- Why is this a TSV BoF (and not “IRTF BoF”)???
  - Some procedural thingy…

Why a signaling approach? Some observations:

- STUN + ICE + Behave
  - Looks like an increasingly effective way to get UDP through NAT boxes
  - And firewalls: an issue we'll have even with pure IPv6!
- Folks have figured out how to do this for TCP as well
- These signaling-based approaches have some nice properties
- Why not generalize this approach for data, expand to explicitly include firewall participation, and standardize its operation?

A quick technical overview

- Hosts data path is “default off”
  - Like private hosts today
- Hosts have an “default on” signaling path
  - Path decoupled
  - Goes through “policy boxes”, which may be far away from host (and which are also co-resident with hosts)
    - Allow DoS-resistant screening of “invites”
  - Access control occurs in policy boxes
    - Based on authenticated and named endpoints and applications

A quick technical overview

If an invite is approved by all involved parties:

- If legacy firewall:
  - Connection behaves as if internally initiated (at both ends)
- If newsock firewall:
  - Policy boxes create secure tokens that are used to traverse on-path firewalls

How are connections established today?

- Various ad hoc ways…
- Manual configuration of NAT/firewall box
  - SSH port, per-application ports
- DynDNS
  - Lacks privacy…
- Various IM-signaled applications
  - I.e., setup file transfer via IM “signaling”
- These push access control to the individual applications, leave the firewalls (personal or otherwise) in the cold
- Popularity of dyndns and IM apps suggests that there is a need for name-based, signaled connection establishment?

Need for newsock?

- Popularity of dyndns and IM apps suggests that there is a need for name-based, signaled connection establishment in the sockets layer…
- Would be nice if all this were standard and ubiquitously supported by OS and ISP…

Related standards efforts (AFAIK)

- IPv6
  - Has firewall traversal issue
  - Will co-exist with IPv4 for the foreseeable future: NAT traversal an ongoing issue
  - Uses DNS for naming, but privacy issue here
  - Philosophically: IPv4 originally meant as a way to allow different networks to inter-operate…newsock would hearken back to that

Related standards efforts (AFAIK)

- nsis
  - NAT/FW calls for some off-path signaling method (i.e. to find IP address of remote host)
  - NAT/FW still very addr/port centric
  - nsis could serve as the on-path component
  - Newsock and nsis are complementary
- HIP
  - Newsock and HIP are also complementary
  - Newsock could be used to negotiate the use of HIP, and to discover the HIP ID
  - HIP ID could serve as the secure token provided by newsock policy boxes

Related standards efforts (AFAIK)

- TiSPAN
  - Not sure about this…looks very provider-centric and massive (includes QoS, for instance)
- Midcom
  - Is this defunct?
- SIMPLE
  - Related in many ways
  - But focused on a specific application (presence and messaging)
- Dynamic DNS
  - Not really signaling

Proposed IRTF group activity

- Mix of research and practice
- Focused: goal to produce protocol and prototype
- Develop requirements: find the simplicity/functionality sweet-spot
- Design on-path and off-path protocols
  - Blank-slate approach…only later see if existing protocols can be exploited

Many open problems

- Policy box discovery
- Attacks on policy boxes
  - DoS, others
- Design of off-path signaling protocol (lessons learned from SIP?)
  - Naming
  - Negotiation
  - Mobility?
- Dealing with endpoints that lie
  - Derive trust from endpoint domain?
  - Trusted Platform Module hardware?
- Design of on-path signaling protocol
  - Out-of-band? (nsis), in-band? (HIP)
- Coupling of off-path and on-path phases (security issues?)
- Dealing with legacy firewalls
- Dealing with legacy applications
  - Sockets interception library