# Distributed Firewalls

*Steven M. Bellovin*

`smb@research.att.com`

973-360-8656

AT&T Labs Research

Florham Park, NJ 07932

# Firewalls are Obsolescent

- Extranets penetrate the perimeter.
- Employee laptops and home computers live outside the firewall.
- Different organizations and computers within the company have different security needs.
- Too many protocols are being passed through the firewall.

# But Firewalls are Necessary

- Too many protocols are broken.
- Too many implementations are buggy.
- Too many computers are poorly managed.
- Organizations often wish to enforce a common security policy.

# What is a Firewall?

- A single point of control.
- A filter that blocks harmful protocols.
- A shield for buggy implementations.

Today's firewalls exploit accidents of older topologies. But enforcing topological constraints is an artifact, not a goal.

# The Distributed Firewall

- Control remains centralized.
- Can block undesirable protocols.
- Can shield buggy implementations.
- Does not rely on topology.
- No single point of failure.

# Basic Tools

- Configuration management packages (asd, rdist, SMS, etc.)
  Note — must be secured, probably via digital signatures.
- IPSEC
- Public key certificates.

# General Philosophy

- System manager uses a high-level language to describe the endpoints and to specify the security policy.
- A compiler translates the policy into filter rules.
- The management tool distributes the policy to all endpoints
- Endpoints accept or reject packets, based on the filter rules and cryptographically-verified identities..

⇒ Filtering is done at the IPSEC layer.

⇒ Topology is irrelevant; identity matters.

# Enforcement

- Ship new certificates with filter rules and software patches:
  `inside = {(x509)"/org=research.att.com/date>19990517/..."};`
- Machines with old certificates are outsiders.
- Run UNIX or Windows NT to guard against user non-cooperation. (But even today, it's hard to guard against insiders who won't co-operate.)

# References

`http://www.research.att.com/~smb/papers/distfw.ps` (or `.pdf`)

`mailto:smb@research.att.com`