Announcements

Lectures 1-24 are available.
The Barnard-Columbia Chorus concert is this Friday and Saturday.
  J.S. Bach: Mass in A major, BWV 234
  Benjamin Britten: Ceremony of Carols
Projects and homeworks are due on 12/10 at 3am.
Project presentations should last 5 minutes.
Remember BGP?

- BGP does lots of things:
  - Exchanges reachable prefixes.
  - Binds prefixes to paths.
  - Learns local topology.
  - Implements policy.
- BGP has lots of knobs to tweak that change route selection.
  - That’s how policy is implemented.
  but:
  - Lots of things that can go wrong.
- BGP hides information.
  - Only propagates “best” routes.
  - Part of scaling.
Routing System Security

- Are the routes I am getting real?
  - So I can send traffic to the right place?
- Are the routes I am advertising being propagated properly?
  - So that traffic for my prefix reaches me?

- Can false routes be advertised?
- Can advertised routes be modified or removed?
Who is the Enemy?

• Outsider:
  – Someone without legitimate access to the routing system.
  – A non-peer.
  – Can be local or remote.
  – Can be a (real) host or a router.

• Insider:
  – Someone who can legitimately inject routes.
  – Yourself!
  – A (peer’s)* peer.
Targets

• Transport.
  – TCP port 179, UDP port 520, etc.
  – Denial of service/Injection of false traffic.
  – Easy to defend against: IPsec, TLS, etc.

• Routers.
  – Configuration.
  – Neighbor state.
  – RIB.

• Related protocols.
  – Breaking the IGP can affect the EGP.

• Databases.
  – Configs automatically built from scripts.
  – IRR etc.
Byzantine Robustness

• Packets sent from A to B.
• Faulty components between A and B.
• Fail-stop failures.
  – If a component goes bad, it stops forwarding packets.
• Byzantine failures.
  – Insider attacks.
  – Inject malicious traffic, modify packets, etc.

• This is not about authentication/integrity/confidentiality.

• This is about preventing denial-of-service.
Robust Flooding

- Packet gets forwarded along all downstream paths.
- If there exists an uncompromised path, packet is delivered.
- Key to robust flooding: pre-allocate resources.
- Node processor and memory must be available.
  - Allocate buffer for each potential source.
  - Use digital signatures to only accept legitimate packets.
  - Use counters to prevent replay attacks.
- Link bandwidth must be available.
  - Go round-robin on buffers.

- Without the crypto, this is the same as the OSPF LSA distribution.
- At most $n^2$ packets, vs. $O(n)$ with bridging.
Robust Routing

• Robust flooding is too wasteful for data traffic.
  – Too many packets.
  – Too many public key operations.

• Using RF, send out a route-setup packet.
• Routers need not have consistent LSDBs.
• Source-specified routing.
  – As opposed to hop-by-hop routing.
• State in each router for each flow.
  – Virtual circuits!

• If path fails, recompute.
Back to BGP

• Byzantine robustness is too expensive.
• What are the real threats in Interdomain Routing again?
  – Accidental misconfiguration.
  – Protocol interaction.
  – Subversion/hacking.
    • Steal traffic.
    • Steal resources.

• Look at draft-murphy-threat-00.txt.
Masquerading

- AS takes over a prefix it does not “own”.
- Announces wrong prefix.
  - With itself as origin.
  - With someone else as origin.

- Effects:
  - Blackholing traffic of real owner.
  - Attract traffic for interception/analysis/etc.
    - Can then forward to real owner.
Interception

- (Interception of **routing traffic**.)
- Some routing information is sensitive.
  - E.g., over private peering links.

- Threat: can use the information to mount attacks more effectively.
Modification

- *(Falsification in Murphy’s draft).*
- Attack against integrity of routing messages.
- Modify path attributes.
- Path attributes are used to select routes.
- Modifying path attributes affects route selection.

- Traffic can be diverted.
  - Congestion.
  - Loops.
  - Redirection for eavesdropping.
- Convergence may be affected.
Misuse

- Introduction of unauthorized routing information.
- Attack against authorized use.
- Injection of routing information that does not conform to policy.
- Routing behavior can be disrupted.
- Same as Modification.
- Too many routes injected/withdrawn affect performance.
- Routing messages overload.
- Churn.
- Route flap damping.
BGP Security

- Active area of research.
- http://www.rpsec.org/
- S-BGP: (Kent et al., NDSS’00)
  - Address attestations.
  - Route attestations.

- so-BGP: (draft-ng-sobgp-bgp-extensions-00.txt).
  - Verify origin of advertisements.
  - Sanity-check the path of updates.

- IRV: (Goodell et al., NDSS’03).
  - Asynchronous verification of suspect routes.

- Best we can do today: IRR.