Routing Protocol Framework

Information Model

Routing Information Base

OSPF
RIPv2
BGP4

RIB
RIB
RIB

Application Layer

Network Layer

Forwarding Information Base

FIB
(Dest, NextHop, Routing Metrics)

Forwarding Algorithm

NPDU Header (Network Protocol Data Unit)

02/08/2006
ecs153

Operation Model

Routing Information Exchange

Hey, Here is the routing information I got so far

Hmm, some of them are obsolete,
Here is my update

02/08/2006
cs153
Operation Model
Route Generation and Selection

Which algorithm should I use??
Distributed Dijkstra’s algorithm or
Distributed Bellman-Ford algorithm?

Routing Information Base
application Layer

Forwarding Information Base
network Layer

Routing

I want to know
the shortest path
or simply “a path”

SRC

DST

Routers exchange local information!
Link State

Flooding

You
Your Neighbor

02/08/2006  ecs153
Link State

You tell the whole world about your relationship with your neighbor

Routing Information

• **Link State:**
  - I let the whole world knows about my relationship with my neighbors.
  - (Felix, Neighbor-X) is up!

• **Distance Vector:**
  - I let all my neighbors knows about my relationship with the rest of the world.
  - (Felix can get to Remote-Y) in 5 hops.
LSA and an LSA instance

- An **LSA** is associated with a particular link of network, which is identified by its **LS type, LS ID, Advertising Router ID**.
- An **LSA instance** gives the state of a particular LSA at a particular time, which can be differentiated by **LS sequence number, LS age, LS checksum**.

\[ 0x80000000 \rightarrow 0x7FFFFFFF \]
LSA Format

- Type (Hello, Link, Networ, Summary)
- Advertizing Router ID (Originator)
- Advertized Link or Network.
- Sequence Number
  - smallest: 0x 80000001
  - largest: 0x7FFFFFFF
- Age (0, 60 minutes)

RIB - OSPF

<table>
<thead>
<tr>
<th>LSA-ID</th>
<th>ADV</th>
<th>Seq#</th>
<th>Checksum</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>A=B</td>
<td>A</td>
<td>0x850012a7</td>
<td>0x452b</td>
<td>20:13</td>
</tr>
<tr>
<td>A=B</td>
<td>B</td>
<td>0x84230b41</td>
<td>0x3729</td>
<td>13:12</td>
</tr>
<tr>
<td>A=D</td>
<td>A</td>
<td>0x9012000e</td>
<td>0x2567</td>
<td>01:22</td>
</tr>
</tbody>
</table>

...
OSPF LSA Flooding, I

If I have not received this LSA (Link State Advertisement).

If I have received this LSA (Link State Advertisement).

OSPF LSA Flooding, II

If I have received this LSA (Link State Advertisement).
OSPF LSA Flooding, III

If I have something better/fresher/newer.. my newer copy

Sequence Number Comparison.

How to decide “freshness”??
Sequence #: old vs. new LSAs

Only accept LSAs with newer/larger Seq#.
Sequence # Self-Stabilization

(1). 0x90001112
(2). router crashes.
(3). 0x80000001.
(4). 0x90001112 an old copy still exists!
(5). 0x90001113

Sequence #: Counter Flushing

(1) 0x7FFFFFFF MaxSeq#
(2) 0x7FFFFFFF with MaxAge to purge this entry.
(3) 0x80000001.
Fresher LSA?

Three parameters for LSA:
- Sequence Number
- Checksum
- Age

A, B are treated the same.

Malicious Intermediate Routers

Flooding

All the links can be attacked.
How to Attack OSPF?

- Think...
- Try it!!
  - What is the objective?
  - How to accomplish your goal?

Problem
- Prevent/Detect compromised intermediate router(s) from tampering “Link State Advertisements (LSAs)” originated from some other routers.

This Link is UP!
Defense??

- Crypto-based
- Non-crypto-based

LSA Digital Signature

PKS

private key

public key

This Link is UP!

This Link is UP!
Advantages for PKS

- One compromised router will not be able to affect others about other links.
- With only key-MD5, one compromised router can disable all the crypto.

Public Key is Expensive

- At least, in software.
- Experiments on Pentium/133, Linux 2.027:
  - HMAC MD5: 78.37 usec
  - RSA/MD5 (verify): 88.00 msec
  - RSA/MD5 (sign): 166.00 msec
- RSA Hardware available, where MD5 is inherently hard to parallelize.
Prevention

- **LSA Originator Digital Signature** (Perlman, Murphy/Badger, Smith/JJ)

- **Debatable Concerns:** (OSPF wk-group)
  - RSA is **too expensive** (about 1,000 times worse in signature verification with 512 bit keys)
  - PKI Certificate is expensive.
  - There are **other routing infrastructure attacks** that can **not be prevented** by LSA Digital Signatures. (Cost/Market concern)
  - Political and Technical.

---

**Can we do it without PKI?**

- Preventing compromised intermediate routers???
Can we detect the problem?

• Authenticated LSAs but the authentication information is kept until a session is over.

Prevention versus Detection

• Prevention: pay a fixed price anyway, even no bad guy exists.
• Detection/Isolation: “hopefully” pay less when no bad guy exists, pay more when trying to isolate the bad guys.
• Self-Stabilization Time:
  - (Detection + Isolation)
Let’s look at the attack again!!

- Why do we need to ADD something to handle OSPF attacks?

Sequence #: old vs. new LSAs

0x80000001
Next: 0x80000002
Only accept LSAs with newer/larger Seq#.
Attack

Seq#
(1) 0x90001112

ATM
- 0x90001111
- 0x90001112 (later)
- 0x90001113

02/08/2006
ecs153
35

Attack and Fight-Back

Seq#
(1) 0x90001112
(2) 0x90001113
(3) 0x90001114
fight-back

02/08/2006
ecs153
36
**Seq++ Attack and Fight-Back**

1. 0x90001112
2. 0x90001113
3. 0x90001114

(1) 0x90001112
(2) 0x90001113
(3) 0x90001114

fight-back

02/08/2006
ecs153
37

**Current Seq# 9123abe0**

Attacking Seq# 9123abe1

Responding Seq# 9123abe2

Originator??

02/08/2006
ecs153
38
OSPФ Security Strength

- In most cases, if something goes wrong, the advertising router will detect it and try to correct it.
- The bad guy has to persistently inject bad LSAs.
- Self-Stabilization Protocols: can not handle continuous faults but force the attacker to perform only persistent attacks.
A Principle/Heuristic Rule of Intrusion Detection

- Hit-and-Run Attacks: Hard to Detect/Isolate
  - Inject one (or very few) bad packet causing permanent or long term damage.
- Persistent Attacks:
  - The bad guy has to continuously inject attack packets.

Network Protocol/System Design

- If we can force the attackers to only launch “persistent attacks,” we have a better chance to detect and isolate the attack sources.
- OSPF Flooding, for example, does a fairly good job. (still need some formal/theoretical research work here...)
Attacks on OSPF/RFC

One “sort-of” Hit-and-Run attack in OSPFv2 RFC is the “External-Forwarding-Link LSA Attack,” and it cannot be prevented by Digital Signature.

MaxSeq# attack (○) was a Persistent Attack in OSPF/RFC, but, with implementation bugs, it becomes a Hit-and-Run attack (●).
Results for OSPF:

- According to the RFC, all the known Digital-Signature-preventable attacks can be efficiently detectable. (There are no known Hit-and-Run OSPF attacks that can be prevented by PKS digital-signature.)
- According to the OSPF Implementations, one such Hit-and-Run attack does exist.

Max-Sequence Number Attack

- Block LSA updates for one hour by injecting one bad LSA. (You can hit it once and come back in an hour.)
- Implementation Bug! (Two Packages)
- MaxSeq# LSA Purging has not been implemented correctly!!
Sequence #: Counter Flushing

(1) 0x7FFFFFFFF
MaxSeq#

(2) 0x7FFFFFFF with
MaxAge to purge
this entry.
(3) 0x80000001.
Properties of MaxSeq# Attacks

- Hit-and-Run for an Hour. The bad guy can "control" the topology database for an hour.
- The Victim continuously argues with its (very likely, honest) neighbors about which LSA is fresher. (0x7FFFFFFF versus 0x80000001).
- To eliminate the problem before one hour, "All" routers must be shut down "simultaneously."
- Or, have an active process to pump the purging packets into the network.
Max-Sequence Number Attack

- Block LSA updates for one hour by injecting one bad LSA. (You can hit it once and come back in an hour.)
- Implementation Bug! (Two independently developed OSPF packages.)
- MaxSeq# LSA Purging has not been implemented correctly!!

Detection ➔ Isolation

- Detection
- Understand
- Isolation
EVE can cheat FOO about BAR’s topology without being detected by BAR. (EVE can intercept the tampered BAR’s LSAs from FOO to BAR.)

But….  

- Any packets from FOO to BAR will pass EVE anyway. (I.e., EVE already has the access to all the packet streams between FOO and BAR.)  
- It is not necessary for EVE to attack the routing information exchange protocols.
Is the network partitioned?

- **YES.**
  - The bad guy doesn’t need to attack RIB!

- **NO.**
  - With OSPF, the bad LSAs should flowed back to the originator.
  - The originator will fight back to correct the problem. (Self Stabilization)
  - The bad guy has to persistently attack.