SECURITY ISSUES OF BOOTSTRAP ROUTER MECHANISM IN PROTOCOL INDEPENDENT MULTICAST SPARSE MODE

Vladimír Veselý
Doctoral Degree Programme (1), FIT BUT
E-mail: xvesel38@stud.fit.vutbr.cz

Supervised by: Miroslav Švéda, Petr Matoušek
E-mail: {sveda, matousp}@fit.vutbr.cz

ABSTRACT

This paper describes security issues of the Bootstrap mechanism that is supposed to help an automatic configuration of rendezvous points inside PIM domain working in sparse mode. Firstly there are shown successful implementations of possible attacks, secondly the paper concerns about known precautions to those threats and security suggestions to minimize a possible risk of vulnerability.

1. INTRODUCTION

As a part of my Multicast in IPv6 dissertation research I am interested in Protocol Independent Multicast (PIM) because it's nowadays mostly used multicast routing protocol. Its variant PIM sparse mode [1] (PIM-SM) is deployed in topologies with more than one source of multicast because it uses effectively source and shared distribution trees. In order to PIM-SM work properly in scope of PIM domain, there must exist one mutually agreed point (so called **rendezvous point**, henceforth RP), which is used to correctly build up above mentioned trees. Sources of multicast are connected with RP by source trees – source of multicast is the root of a source tree. RP is connected with multicast receivers by shared trees – RP is the root of shared tree. Multicast data are traversing from sources down by source tree to RP and from here down by shared tree to receivers. PIM-SM can't work properly as long as all PIM routers in a network don't know exactly which router is RP for a given multicast group. This knowledge could be set up by a static configuration or by automatic configuration. But according to dynamic characteristic of multicast the static configuration isn't scalable enough. One of the most widely deployed protocols for automatic RP configuration is the Bootstrap router mechanism extension [2] to PIM.

2. BOOTSTRAP ROUTER MECHANISM

The Bootstrap router mechanism (BSRM) creates in the scope of one PIM domain a hierarchy of active network devices (generally under terms of this article by the expression *router* is ment classical L3 router or L3 switch capable of multicast routing):

- **Candidate-RP (C-RP)**: These routers know about a source of multicast data and they could become an RP for a given multicast group;

- **Candidate-BSR (C-BSR)**: These routers form a set of candidates from which one could be elected as a BSR;
- **Boostrap Router (BSR)**: This router is a moderator of multicast in the PIM domain. Every C-RP announces to BSR its candidacy for being the RP for a given multicast group. From all of these announcements the BSR chooses a subset that is distributed to all PIM routers.

2.1. EXTENSION OF PROTOCOL

The original set of control messages of PIM as shown in [2] is extended by two new messages. Let’s analyze their structure because their parameters play important role in attacks described below.

First message is *PIM Bootstrap* which assists in communication between all PIM routers. C-BSR uses it to announce its priority for the election. The BSR informs with it RP mapping to given multicast addresses. This message lets all PIM routers know the address of the elected BSR.

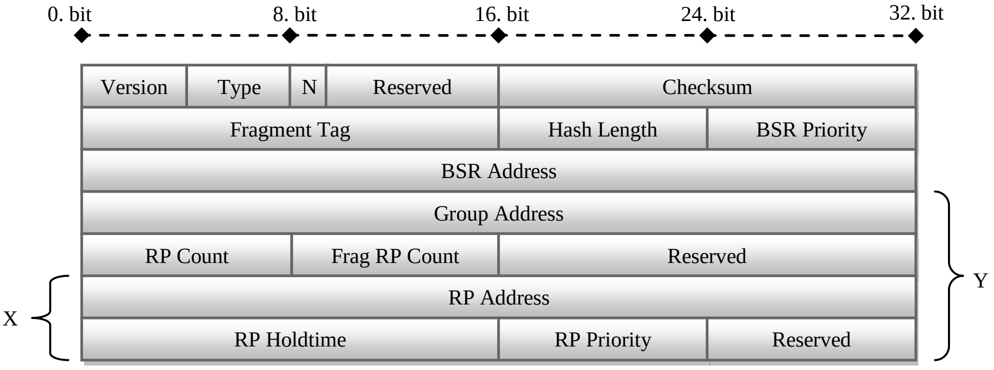

Figure 1 – Structure of *PIM Bootstrap* message

I mention just parameters which are relevant to attacks:

- **BSR Priority** – C-BSR sends in this parameter its priority for BSR election. Value is in the range of 0 to 255 (higher value means better chance to be elected);
- **BSR Address** –All C-BSR are sending their addresses as in case that no router has been elected yet. After election this field contains the address of the BSR;
- **Group Address** – Group multicast address that is mapped to following RP;
- **RP Address** – C-RP address;
- **RP Holdtime** – Period in seconds when C-RP address is valid;
- **RP Priority** – Priority of this C-RP to multicast group mapping. Value is in the range of 0 to 255 (lower value is more preferred).

Each *PIM Bootstrap* message contains at least one group multicast address (in Fig. 1 block marked by Y), which is mapped to at least one associated RP (in Fig. 1 block marked by X).

Second message is the *PIM Candidate-RP-Advertisement*, which helps C-RP to announce to BSR their candidacy for RP. BSR chooses a subset of candidates (RP-set) which broadcasts to all PIM routers in domain. Each of those messages contains at least one group multicast address to which C-RP reports itself as RP (in Fig. 2 block marked by Z). Parameters have the same meaning as those described above for *PIM Bootstrap* message.

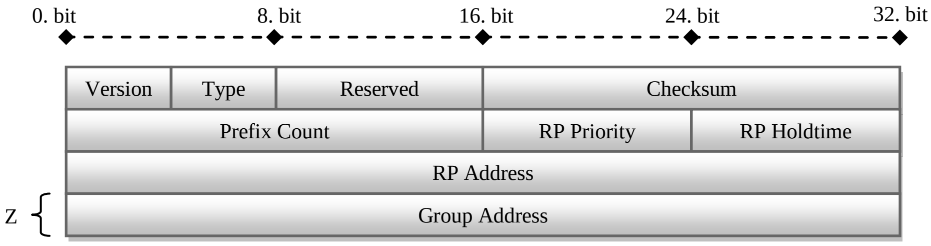

Figure 2 – Structure of *PIM Candidate-RP-Advertisement* message

2.2. Election of BSR

PIM Bootstrap messages are periodically send by all PIM routers every 60 seconds by default. These messages are used, apart from distribution of RP to multicast group mappings, also in election process of BSR. Router with highest *BSR priority* is elected as BSR for given PIM domain. The highest IP address is used as tie-breaker if two or more routers share the same *BSR priority*.

BSR is pronounced dead in case it doesn't send any new *PIM Bootstrap* within default period of 150 seconds. New BSR is elected from C-BSR-set to take up its place.

3. ATTACKS

Security issues and possible attacks are firstly mentioned in the BSRM specification [2]. Attacks could be divided into two groups according to their overall impact on a network – **denial of service** (DoS) and **traffic diversion**. RFC just outlines that traffic can be prevented from reaching the intended recipients by subverting a BSM, and specifying RPs that won't actually forward traffic or by registering with the BSR as a C-RP, and then not forwarding traffic. I decided to implement (and improve) these two attacks described in RFC along with other ones which I proposed (e.g. "Ignorance" or "Subversion" variants).

In all scenarios the role of an attacker is conducted by XORP v1.6 [3], which is the SW implementation of router supporting different routing protocols (e.g. PIM-SM, OSPF, BGP). Source codes of XORP were properly modified to achieve intended attackers' misbehavior. Fig. 3 shows a network where attacks were performed:

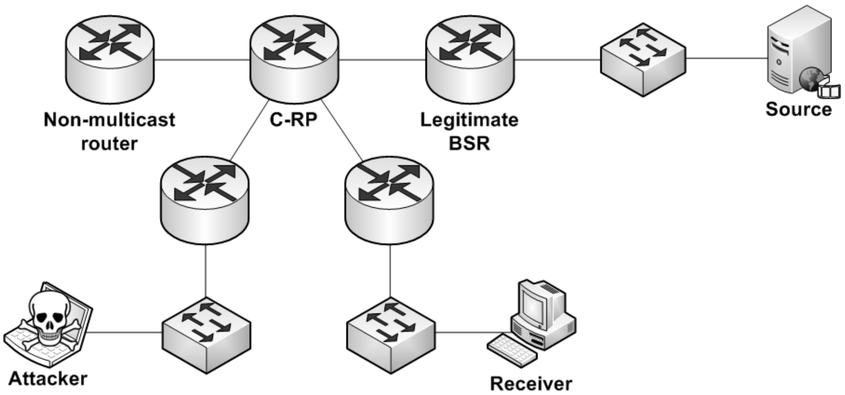

Figure 3 – Attacks' demonstration topology

3.1. Attacker as false BSR

To implement an attack I started with default behavior of routers where standard proposes default *BSR Priority* value of 64 (CISCO devices have implicit value of 0). Attackers' workstation connects itself to a network with priority 255 (highest possible). In PIM domain, even if there exists legitimately elected BSR after period of 150 seconds the attacker will become new BSR.

This role gives attacker great opportunities from which the following have been tested:

- **Ignorance**: Attacker as BSR ignores *PIM Candidate-RP-Advertisement* messages and no information about RP to multicast group mapping are broadcasted to PIM domain. All PIM routers will have forgotten given RP mappings after *RP Holdtime* timer will timeout. Such attack results in multicast DoS;
- **Subversion**: Attacker as BSR subverts its own information about RP to multicast group mapping. Generally there are three cases of this attack according to RP:
  a) Either address of RP doesn't exist in a network or subverted RP is a device not capable of multicast routing. In both cases PIM isn't able to build its distribution trees and again the result is multicast DoS;
  b) Address of RP corresponds with multicast capable router other than C-RP. Multicast data is traversing in not-intended paths, which results in diversion of traffic. But attacker could also map all active multicast groups to the same RP. In compliance with usually large amount of multicast data (e.g. video streaming), this could lead to malfunction of RP with insufficient HW and cause not even multicast DoS but DoS on other services provided by this router;
  c) Address of RP is an address of attacker or other multicast capable device under the domination of attacker. Hence, the attacker could easily compromise all data for the given multicast group (e.g. subverting own multicast source). This results in traffic diversion and alternation.

3.2. ATTACKER AS FALSE C-RP

Attacker pretending to be C-RP is just different variant of "Subversion" attack described above where legitimate BSR provides distribution of false information.

4. CURRENT SITUATION

I successfully performed above mentioned attacks and show their threat to network integrity. Let's have a look at existing ways how to prevent those attacks.

4.1. EXISTING SOLUTIONS

Static configuration is the only current solution provided by manufacturers of active network devices.

It's possible to manually enable or disable sending and receiving of BSRM messages on an interface of each router in PIM domain. This approach is called **delimiting borders**. CISCO devices command for this feature is:

```
(config-if)#ip pim bsr-border
```

Filtration of certain RPs mapped to multicast groups is another commonly used option that can prevent compromising of C-RP announcements to BSR. CISCO devices command for this feature is:

```
(config)#ip pim accept-rp RP ACL
```

4.2. TROUBLESHOOTING

Best known practices according to suggestions of manufacturers in [4] and [5] how to successfully monitor and alleviate impacts of attacks are the following:

- Record at least every *PIM-1-INVALID_RP_REG* Syslog message, which can show and track possible compromising of RP mapping;
- Send at least SNMP trap *PimRPMappingChange* and *PimInvalidRegister* and also send trap for every false change in multicast topology with *PimInvalidJoinPrune*.

5. CONCLUSION, FUTURE WORK AND ACKNOWLEDGMENT

The Bootstrap router mechanism is thoroughly described as standardized extension of the multicast routing protocol PIM in this work. From these pieces of knowledge I proposed and demonstrated series of attacks that prove its security weaknesses.

Following up I mentioned the current approach of manufactures to overcome these issues in real world. But it’s important to realize that above mentioned solutions (delimiting borders and filtration) spoil the idea of a fully automated protocol distributing RP mappings with drawbacks of static configuration. On the one hand we must manually configure RP to multicast group mapping on every PIM router in networks without BSRM. On the other hand if we want to use the secure BSRM, we have to configure filtration on every PIM router and besides that, we must also delimit borders of BSRM on all routers (even non-multicast devices) in a network. Hence, the overhead for the reliable network management is rising unproportionally.

Future work and the part of my dissertation will be a proposal to update BSRM to be secure without a help of additional static configuration. Relevant solution could be introducing the authentication into BSRM. Mutually shared hashed password which will be send in the header of *PIM Bootstrap* and *PIM Candidate-RP-Advertisement* could be possible good enough. This is proven (in case of OSPF, BGP, EIGRP) approach how to get rid of above mentioned security issues.

This work was partially supported by the BUT FIT grant FIT-10-S-1 and the research plan MSM0021630528.

BIBLIOGRAPHY

[1] **B., Fenner, et al.** Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised). [Online] August 2006. [Cited: February 22, 2010.] http://tools.ietf.org/html/rfc4601.

[2] **N., Bhaskar, et al.** Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM). [Online] January 2008. [Cited: February 24, 2010.] http://tools.ietf.org/html/rfc5059.

[3] **XORP Inc.** *XORP - eXtensible Open Router Platform.* [Online] [Cited: February 24, 2010.] http://www.xorp.org/.

[4] **Cisco Systems Inc.** IP Multicast Network Management Overview. [Online] August 2007. [Cited: February 27, 2010.] http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6552/prod_white_paper0900aecd80595d81.html.

[5] **Juniper Networks.** PIM Configuration Guideline. [Online] [Cited: February 27, 2010.] http://www.juniper.net/techpubs/software/junos/junos72/swconfig72-multicast/download/pim-config.pdf.