The results of the experimental part of this study allow to conclude that municipalities in Bulgaria to comply with laws regarding the budget process and its stages. In this sense, the proposal to build a business intelligence system in a municipal administration would allow much easier budget planning based on operational data. It will also enable the creation of optimistic and pessimistic versions of local budgets, and assist in decision making.

ABOUT CERTAIN VULNERABILITIES OF PSEUDO-M-ROUTERS

Maciej SZMIT
Computer Engineering Department of
Technical University of Lodz (Poland)

This article provides the results of the tests carried out on two models of inexpensive network devices (called „routers", though their functions go beyond the range of the meaning of this term), which are designed for the use in home networks and shows potential dangers which can result from non-standard behaviour of these machines.

Introduction

When the issues regarding network computers are discussed, it is sometimes mentioned about certain incoherency, which takes place between reference model ISO/OSI assumptions and the particular network protocols, and between the network protocols and their specific hardware or software implementations. However, the subject does not attract much attention, especially in the publications on network traffic engineering, which in many cases satisfy themselves with providing information on simplified models[1] and conducting, on their base, computer simulations. Meanwhile, although the ISO/OSI reference model is thirty years old[2], and the basic of the TCP/IP stack protocols came into being more or less at the same time[3], the implementation of the rules and algorithms they provide leave a lot to be desired, causing unforeseen behaviours of their software or hardware. In practical solutions such unforeseen or non-typical behaviour of a specific device can usually lead to its

---

[1] Model means „simplified reflection of a phenomenon, system, process etc., (. . .), schematic presentation of a fragment of reality, where the insignificant parts are omitted to allow a better explanation of the operation, form or structure of the fragment" [Błaszczuk 2006] s.21. "Model is a depiction of a theory or causal situation, which is assumed to generate the data being observed" [Kendall, Buckland 1986] page 102. "Model (…) is a formal mathematical notation of regularities (…) occurring in the reality" [Witkowska 2005] page 28.

[2] The origin date for the model is considered to be the year 1977, while its present standard was formed in [ISO 7498-1:1994] standard.

[3] [RFC 791] and [RFC 793] are dated 1981

replacement (usually produced by a different vendor); only single cases of such strange behaviours happen to be investigated and characterized in professional publications[1]. Yet reliability, which means the capability of the functional unit to perform a required function in the defined environment and in the defined period of time[2], is one of the safety attributes of computer systems[3]and the information.

Multicast frames and packets

In the article [Szmit, Tomaszewski 2007] we presented non-standard behaviours of the router-switch devices from D-Link and Lucent with respect to frames addressed with Ethernet multicast. In the case of receiving frames with Ethernet multicast as designation MAC-address, - apart from sending multicast frames to their ports – they made a peculiar routing by sending additionally a packet in the frame with unicast designation address, whereas the receiver's frame MAC address was the MAC address of the computer, of which IP was contained in the packet that was carried by the frame. Interestingly, router-switch was sending both of the frames to all of its ports including the one, from which received the multicast frame (Figure 1), therefore its operation is something between operation of a classical switch (which should send the multicast frame to all ports like a hub and an m-router) or a switch with IGMP-snooping handling technique, which should send it to appropriate address, that is to the multicast group members). In the case of using in the packet IP broadcast address, unicast frames with broadcast destination address packet were forwarded by the devices to the particular computers in the network.

In this article, within the scope of this research, two behaviours of today's (in sale in 2011) devices of cable and wireless routers Edimax BR-6314K and Belkin F5D7234-4-H V5 has been tested. Both devices are equipped with four RJ-45 ports dedicated to a LAN and one port dedicated to a WAN, besides the Belkin router has also got WLAN 802.11. Both contain a series of functions, among others 2nd ISO/OSI layer switch, router with Network Address Translation and firewall in the architecture of screening router with statefull packet inspection and webpages URL filtering.

---

1 It is worth mentioning two articles here: [Mogul 2003] in which the Author analysed the dangers connected with the use of the technique of TCP Offloading Engine; among other things, in workstations, in which the driver is delivered by the manufacturer of the equipment supporting TOE, it does not have to properly work with some other – for example those changed in the installation process of patches – versions of the systems libraries serving TCP/IP protocol stack and [UoBC 2004], where two case studies are described connected with problems caused by non-standard service of the multicast by switches. One of them concerned Norton Ghost program using one of the agents applying IGMP ver. 2, which hung up in the presence of the switches applying IGMP-snooping for IGMP ver.3, the second – over-intelligent switch applying PIM (of what wasn't aware his administrator), which won the process of choosing of the designated router PIM, that caused the redirection of the multicast traffic to improper network and in consequence blocking all of the services in the corporate m-internetwork operating with the basis of multicasts

2 PN-ISO/IEC 2382-14:2001 – 14.01.03

3 Compare against [Korzeniowski 2008] p. 133, [Jašek, Dolejšová, Rosman 2007] p. 21.

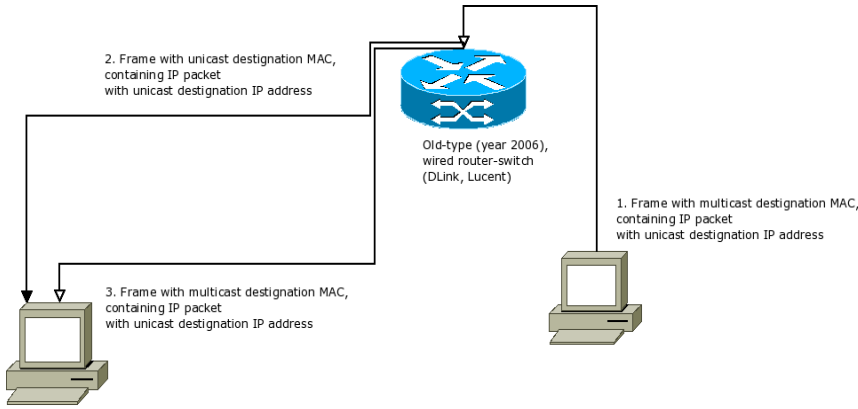

Figure 1. **Handling of Ethernet multicast by pseudo-m-router-switches. By [Szmit, Tomaszewski 2007].**

Results

Both routers behave in a different way than previously tested devices, however still not quite properly. Handling of the packets with broadcast destination addresses has been improved: multicast frames containing broadcast destination addresses are simply passed on to other ports without any changes.

In the case of Belkin router the change of multicast to unicast MAC address take place only on the WAN interface. The LAN interfaces do not handle multicasting at all. (i.e. do not forward any frames or packets contained in them). So possible problems concern two situations: the trial of using the router as a m-router (what will not succeed) and the possible malicious attempts of the user, who has access to the WAN interface. In the last case still one more oddity needs to be taken into consideration regarding this router: if the multicast frame carries a packet with a random source IP address, even out of either inner or outer network, it will also be passed forward (i.e. as a unicast frame with the proper destination address it will get to the WAN). Moreover, sending such a frame from the multicast MAC address source will cause change of address into the MAC of the router interface (see Figure 2). This is then an alternative of the Source Network Address Translation.

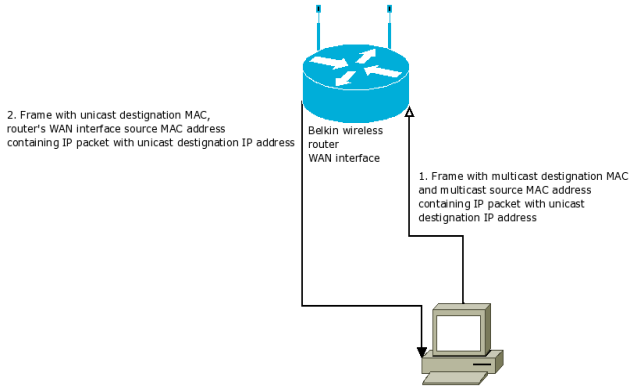

Figure 2. **Handling of Belkin router. Source: own study.**

This kind of behaviour could be risky, since it enables in certain cases fairly effectively committing of an attack being something between a Smurf attack and a Distributed Denial of Service with Reflection (DRDoS). In particular in amateur networks, in which individual home networks are connected to the Internet Service Provider with this type of access devices (see Chart 3).

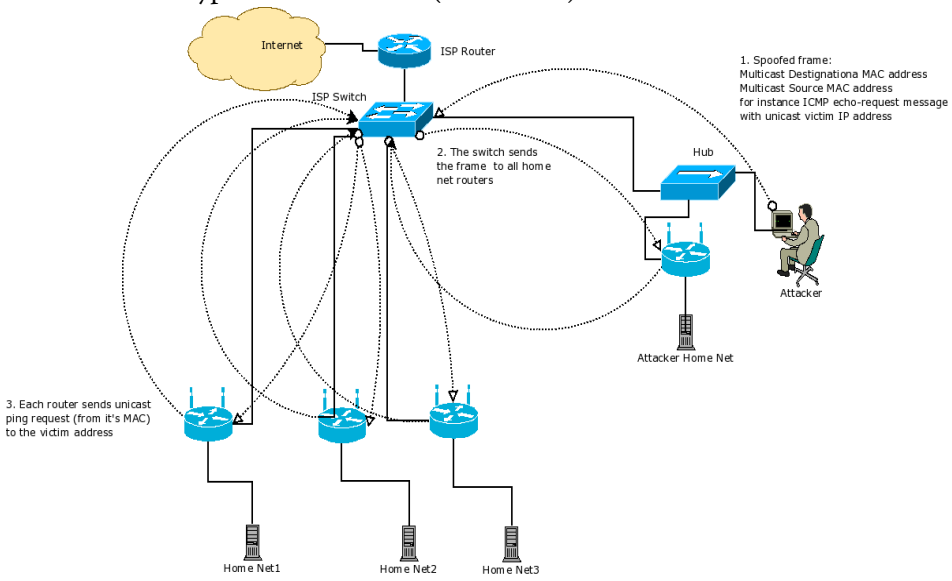

***Figure* 3. Scheme of attack. Source: own study.**

The attack scenario proceeds as follow:

1. The attacker places in the network the multicast frame (with the multicast MAC addresses of a sender as well as a receiver), containing the packet (with one of the routers or the computers from one of the others from the home networks), launching an attack, (in the figure it is one of the ICMP echo request, but it might as well, for instance, be the TCP SYN, if the attacker intends to carry the SYN-flood type of attack).
2. The frame is sent via the switch to all the users of the provider's connected networks.
3. Each of the routers „corrects" the frame giving it its own source MAC address, destination MAC of the Internet Access Gateway installed by the provider and leaving the IP address of the routers or computers from one of the home networks (what allows to avoid their possible filtering by the firewall of the Internet provider). In this way it will be multiplied.
4. Even in the case of possible traffic logging on the provider's side there will only be information, that few routers sent a packet from beyond its own network. Without a 3rd layer switch, i.e. the device, that analyses and filters incoming packets (according to the IP address) and frames (according to MAC address) on each of its ports, there will be no chance to reveal the perpetrator of the

attack. Routers of the home network will then serve the role of something halfway between the reflector of the DRDoS attack and an amplifier of the Smurf attack (efficiently hiding the source of the carried attack).

The EDIMax router, similarly to the Belkin router has an improved handling of the broadcast packets contained in the multicast frames, while in the case of the multicast frames carrying the unicast packets it comes up their duplication: apart from the original frame, – created by the router – the frame with the unicast receiver address is transferred. This is even, when the router is connected to the switch, where such a frame appears (the router „ping-pongs back" two frames to the switch). Theoretically it could happen – similarly like in the previous examples – serve to boost the Smurf type attack. In practice this could also be used for detection of the presence of such a device in the network.

References:

1. [Błaszczuk 2006] Błaszczuk D.: Wstęp do prognozowania i symulacji, PWN, Warszawa 2006
2. [ISO 7498-1:1994] ISO 7498-1:1994 Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model
3. [Jašek, Dolejšová, Rosman 2007] Jašek R,, Dolejšová M., Rosman P.: Informační technologie ve veřejné správě, UTB, Zlín 2007
4. [Kendal, Buckland 1986] Kendal M. G., Buckland W. R.: Słowik terminów statystycznych, PWE, Warszawa 1986
5. [Korzeniowski 2008] Korzeniowski L. F.: Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych, EAS, Kraków 2008.
6. [Mogul 2003] Mogul J. C.: TCP offload is a dumb idea whose time has come, Proceedings of the 9th conference on Hot Topics in Operating Systems - Volume 9, http://www.usenix.org/events/hotos03/tech/talks/mogul_talk.pdf
7. [RFC 791] Postel J. (ed.): Internet Protocol, Defense Advanced Research Projects Agency, Information Processing Techniques Office, 1981, http://www.rfc-editor.org/rfc/rfc791.txt
8. [RFC 793] Postel J. (ed.): Transmission Control Protocol, Defense Advanced Research Projects Agency, Information Processing Techniques Office, 1981, http://www.rfc-editor.org/rfc/rfc793.txt
9. [Szmit, Tomaszewski 2007] Szmit M., Tomaszewski M: Huby w pajęczynach i złośliwe m-routery [in:] „Hakin9" Nr 1/2007, s. 36-41
10. [UoBC 2004] Multicast on the LAN, Multicast Workshop. University of British Columbia. Vancouver, BC. May, 2004, http://andrew.triumf.ca/AG/multicast/internet2-multicast-workshop-may-2004-2-LAN- SSM.pdf
11. [Witkowska 2005] Witkowska D.: Podstawy ekonometrii i teorii prognozowania, Oficyna ekonomiczna, Kraków 2005