BASIC PRINCIPLES OF SECURITY DESIGN IN SMART GRIDS NETWORK SOLUTIONS ON IPV6

Lukáš Petr, Josef Horálek, Oldřich Horák

Abstract

The paper describes the basic principles of security design in network solutions based on Smart Grids in the IPv6 standard environment. The motivation for this research is described in the introduction. The second part describes the problem and the definition of basic characteristics of the environment, where the problem is to be solved. The solution is designed in the third part, when the similarities with IPv4 solutions are used as the basics of the proposed design. After the short discussion, there is the conclusion and planned future work in the last part.

Keywords: *Smart Grids, Internet Protocol, Security, Attack Defense, IPv6*

1 INTRODUCTION

Intelligent networks known as Smart Grids are specialized networks designed for monitoring the consumption and delivery of electrical energy. This monitoring provides a possibility to regulate the energy production and to control the optimal transmission trough the distribution system from power plants to customers. The carrier base of this technology is the information about the current state of the network, and the very fast transmission of this data from the control points to the operational centers of distributors, producers, and/or resellers. On the other hand, the same information is very important for customers and consumers to get a detail knowledge about the current consumption or the energy unit price in real time conditions, and to have the possibility to control their energy costs in a moment or a longerterm period.

"The concept of Smart Grid can be defined as an intelligent, self-regulating power supply, capable of transmitting energy produced from any source for centralized and decentralized production of electricity to the end customer." [4].

The aim of the Smart Grids is reliable, efficient and safe energy distribution, which is achieved through bidirectional communication between the parties involved (energy producers, distributors, customers, etc.) carried out by using of modern information and communication technologies. The transformation of traditional electricity networks to the technology of Smart Grids leads to seamless interconnection with the communication infrastructure of modern computing (PCs, mobile devices, etc.), which opens up new possibilities in the field of management, but also brings new security risks.

2 PROBLEM DESCRIPTION

The communication in the Smart Grids environment uses the standards of TCP/IP network stack. Internet protocol (IP) brings great advantages thanks to its compatibility with many components of the Smart Grids environment and existing data network technologies [2]. The older IP version (IPv4) based components and solutions are used traditionally, but the newer version (IPv6) based technologies come to foreground nowadays. In many cases, the TCP/IP suite becomes the target of various types of attack [2], i.e.:

- Smurf Attack
- Land Attack
- SYN Flood Attack

- Source Routing
- DHCP Server Spoofing
- ICMP Redirect Message Spoofing
- TCP Connection Sequence Number Disclosure

The possible prevention depends on the targeted protocols, but the solution can be different by the IP version on the network layer below. Important for security issues is to understand the differences between IPv4 and IPv6. Both of these protocols share many of the same features (IPv6 is partly derived from IPv4). Because of this similarity, most of security measures can be used to apply for IPv6 as well as for IPv4. However, the new features of IPv6 also bring new security risks that require new security measures, but also bring new opportunities in communications security.
Because of concepts of the TCP/IP, there is only difference of IP version used on the internetwork layer. The Internet Protocol works over the lower layer protocols (PPP, X.25, Ethernet, and others), and also supports a variety of transport protocols of the higher layer such as TCP, UDP, SCTP, and more. When using IPv6 or IPv4, the protocols that are above and below the network layer are the same. Therefore, if exists the risk of attacks on the higher layer and lower layer in the IPv4 environment, the same risk exists even in the IPv6 environment.

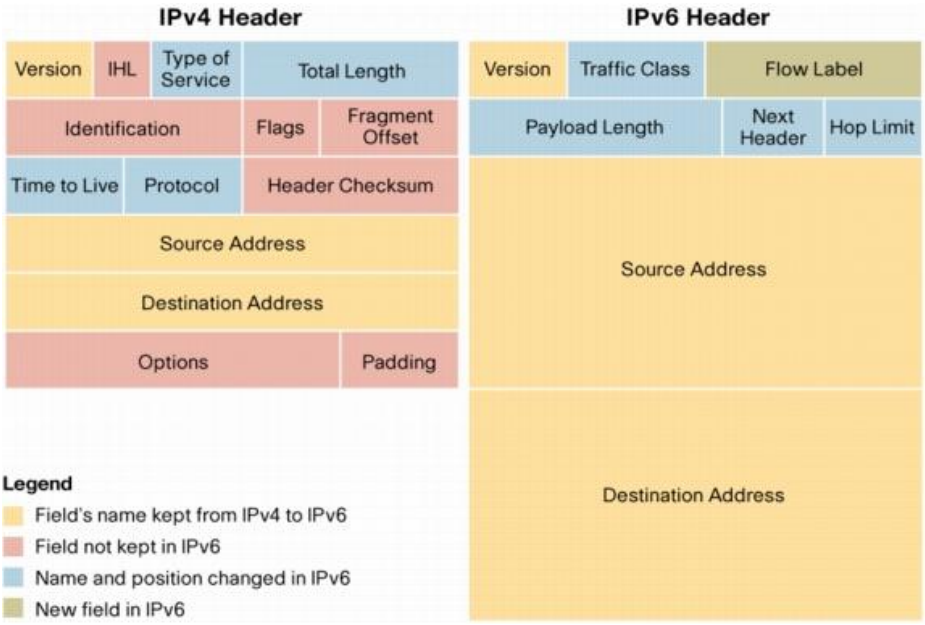

Fig. 1. Comparison of IPv4 and IPv6 header
(Source: IPv6 Extension Headers Review and Considerations [9])

Both of these protocols are responsible for routing datagrams via one or more networks and their headers structure is very similar (see Fig. 1). Both header versions contain information about the version of the protocol, QoS, data length, durability, data about higherlayer protocol, and source and destination address. Due to these same properties, the risks known in IPv4 are similar also in IPv6, including these:

- Application Layer Attacks
- Unauthorized Access
- Man-in-the-Middle Attack
- Network Traffic Eavesdrop

- DoS and DDoS Attacks
- IP Spoofing
- Router or another Active Equipment Attacks
- Physical and Link Layer Attacks

However, the IPv6 uses different solutions than in IPv4 in some areas. These solutions are changing security threats valid for IPv4 and thus are not transferred to IPv6. One of these minor changes is the expansion of header with two new fields (Flow Label and Next Header as the reference to the header extension block). The Flow Label is not yet precisely defined and therefore not used yet. Extension headers, however, are a major component of the IPv6 protocol and thus represent new ways for attacks that are specific only for IPv6 [3]:

- Brutal Force Network Scanning
- ICMPv6 Attacks
- Expansion Header Attacks
- Auto-configuration Attacks
- Transition Mechanisms Attacks
- Attacks on IPv6 Mobility

The original IPv4 did not contain any IP security mechanisms, but with the development of Internet communication, there was necessary to guard the communication on this layer safe. Currently, there are various safety mechanisms on the selected layers of the OSI RM. At the network layer, it is so-called IPsec. In the case of IPv6, the IPsec implementation was designed as mandatory, thus there was wrongly created the impression that the IPv6 was more secure than IPv4. In 2011 it was issued RFC 6434, which abolished these obligations of IPsec implementations, and instead of it only recommended it, which brought an additional security risks that would had been eliminated with IPsec applications [8].

3 PROBLEM SOLUTION

The above-identified individual threats arising from the use of the Internet Protocol. This section will describe possible security mechanisms that serve to eliminate risks. As already described, the actual IPv6 does not eliminate the safety risks, as sometimes mistakenly assumed. It is therefore necessary to propose a solution to eliminate possible attacks. These mechanisms include:

- Using of IPsec
- Defense against Scanning
- Defense against DoS
- Defense against MITM
- Application Layer Encryption

3.1. IPsec

One of the solutions is the strict implementation of IPsec that is not included but only recommended in defaults of IPv6. IPsec enables secure IP layer using two mechanisms:

- **Authentication**, which identifies the originator of the data in a way where it is possible to verify that the data was really sent by the claimed sender.
- **Encryption**, which protects the contents of transmitted data in such a way that it can be read only by designated subjects.

These mechanisms are applied through extended headers AH (Authentication Header) and ESP (Encapsulating Security Payload). The AH only provides authentication, but the ESP

provides authentication and data encryption together. Therefore, ESP provides authentication itself. Using of both mechanisms simultaneously brings some redundancy, therefore by the RFC 4301 the ESP is mandatory but the AH is only optional.

Using of **AH** provides:

- Authentication - verification of sender
- Data Integrity - verify that data isn't changed during the transfer
- Protection against replay attack - rejecting of repeatedly sent packet

Using of **ESP** provides:

- Confidentiality of Data
- Authentication
- Data Integrity
- Protection against replay attack

Both these mechanisms work in two modes: Transport Mode – when the AH or ESP header is inserted between the extension header, and Tunneling Mode – when the original datagram is packaged as newdata datagram, which is equipped with new header (including security headers). The datagram transfer modes can be shown in Fig. 2.

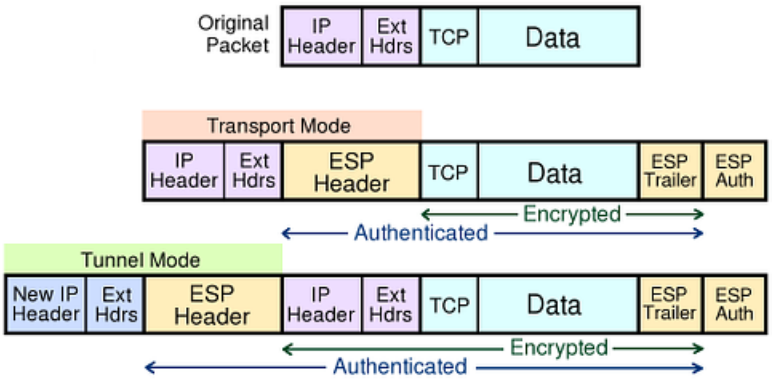

Fig. 2. Modes of IPv6 (Source: IPv6 Packet Security [9])

When used transport mode, there is encrypted the part of datagram, which follows the header, therefore the data. This ensures the confidentiality of the content of transmitted messages only. It is not prevented the interception of data from the datagram header that precede ESP, because not encrypted. This allows obtaining communication data such as addresses of the sender and receiver. Therefore, it is safer to use tunneling mode, which encrypts the entire original datagram including the header. Then an attacker eavesdropping detects only the addresses of security gateways implementing security tunnel, but not communicating devices.

3.2. Defense against Scanning

As a defense against a potential scanning, it can be used a number of proposed mechanisms that make the network scanning significantly difficult for potential attacker.

These mechanisms include:

A suitable method of limiting the possibility of scanning the network is using of unpredictable addressing structure (such as the elimination of routers numbering with the first and last address in the range). Ideally, addresses should be assigned randomly. Windows systems are already using randomly assigned addresses, but other systems, such as GNU/Linux or cisco

require additional configuration, which is important in connection with integration of the Internet of things, in which is a high premise of using those Linux systems.
Random address assignment can be put into practice by manual assignment or using a DHCPv6 server. From the perspective of comfort, using a DHCPv6 seems like a better solution, but not all implementations of DHCPv6 support this option. Managing random addresses brings high demands on the network manager, that is why it can only be recommended in parts of the network with high risk of an attack or high damage in case of an attack.

3.3. Defense against DoS

One of the measures against this type of attack is the regulation of the passing packets, and thereby mitigation of the efficiency of the attack. While configuring the firewall, it is important not to forget about including the rules, which make sure that packets from these addresses are disposed. List of faulty addresses:

- ::/128
- ::1/128
- ff00:::/8
- fe80::/10
- fec0::/10

All those addresses have their usage only in the local networks and can not be routed.
In the case of using systems, which do not reflect RFC 5095, it is important to deny the routing of a packet, which uses the routing header of type 0. This packet should not occur in the newer systems, which reflect RFC 5095 [7].
An attack using a device in a network answering a thrown ICMP request (smurf attack) can be prevented by the denial of answering ICMPv6 requests, which are addressed to the multicast address ff02::1.

3.4. Defense against MIMT

Defense against MITM can be partly taken from the mechanisms used for IPv4 and it is also needed to apply new mechanisms. One of the options for preventing this type of an attack is using the Secure Neighbor Discovery tool (developed by specification of RFC 3971). However, SEND requires more computing devices due to its cryptographic operations [8].
An attack using falsified ICMPv6 Neighbor Advertisement can be prevented by the observation of neighbors cache memory and by generating a warning after a suspicious change. NDPMon tool was developed for IPv6; it is an analogy of the ARPWatch tool used to observe ARP cache in networks built on IPv4 [5].
It is appropriate to secure a network against the usage of a false DHCPv6 server. Recommended option for alleviating the usage of a false DHCPv6 server is a presence of more servers in the network, manual configuration of key network devices such as the default gateway to stop the potential redirection of the network traffic to the device of the attacker is also recommended [1].

3.5. Encryption on the Application Layer

Superstructural solution in case of the attacker getting our transferred data or him trying to fake the data, despite our security solutions, is the implementation of encryption in the higher layers of RM ISO. In case of Smart grid networks and its important communication channels, it is recommended not to rely purely on the encryption on the network layer, but to apply encryption algorithms on the application layer. In case of eavesdropping and potential decryption of the data, the potential attacker gets only the data encrypted on the higher layers.

By using the encryption on the application layer, flexibility in the selection of technologies and algorithms, size of keys, etc. can be achieved. Devices realizing the transmission are not so flexible and they must comply established standards given by the lower layers, it is also not necessary to decrypt transferred data. Implementation of the cryptographic tools is necessary on the end devices and thereby it is important to take into consideration the technological and computing limitations of those devices, so encrypting on those devices is possible (for example smart meters, etc.)

4 DISCUSSION

For the transmission of datagrams on this level of network, the IP (internet protocol) is used, it is the most used protocol for the data transmission and it is also used in the Internet. IP is available in two versions, IPv4 and IPv6. Nowadays, the IPv4 does not provide enough addresses for all devices around the world, due to its 32-bit length, and it is gradually replaced by the IPv6 which provides enough addresses for all devices thanks to its 128-bit length. Some older devices do not support addressing via IPv6 and thereby while building an infrastructure it is important to plan for using IPv4.

5 CONCLUSION AND FUTURE WORK

The principles of Smart Grids security are mainly inherited from the background technologies. If the network solution uses the IPv6 protocol suite, there is necessary to design an additional focus on the similarities and differences against commonly used IPv4 solutions. If the common security solution solves given problem, it can be not enough secure in the new protocol version problematics.

There is a big deal for design of new security solutions, which has to be devel-oped in the future. Each type of attacks needs to be defended and the security tech-nics needs to be tested. However, it not excludes the possibility of new, unknown types of attack have to be defended in the future.

Sources

1. A Complete Guide on IPv6 Attack and Defense. SANS Institute InfoSec Reading Room. 2011. http://www.sans.org/reading-room/whitepapers/detection/complete-guide-ipv6-attack-defense-33904
2. ALOUL, F., AL-ALI, A.R., Al-DALKY, R., AL-MARDINI, M., and EL-HAJJ, W. *Smart Grid Security: Threats, Vulnerabilities and Solutions*. International Journal of Smart Grid and Clean Energy. 2012, vol. 1. ISSN 2315-4462.
3. HOGG, S., VYNCKE, E. *IPv6 security*. Issue 3. Indianapolis: Cisco Press, 2009, xxi, ISBN 978-1-58705-594-2.
4. HORÁLEK, J., SOBĚSLAV, V. *Technologie a požadavky na inteligentní sítě pro SmartGrid*. Elektrorevue. 2012, vol. 65. ISSN 1213-1539. http://www.elektrorevue.cz/cz/clanky/energetika--vykonova-elektronika--elektrotechnologie/0/technologie-a-pozadavky-na-inteligentni-site-pro-smart-grid/
5. NDPMon. 2012. http://ndpmon.sourceforge.net/
6. RFC 3971. In: IETF. 2005. http://tools.ietf.org/html/rfc3971
7. RFC 5095. In: IETF. 2007. http://tools.ietf.org/html/rfc5095
8. RFC 6434. In: IETF. 2011. http://tools.ietf.org/html/rfc6434
9. SATRAPA, P. *IPv6*. Issue 3. Praha: CZ.NIC, 2011, ISBN 978-80-904248-4-5.

Contact
Mgr. Ing. Lukas Petr
University of Hradec Kralove, Department of Physics,
Rokitanského 62, Hradec Králové, Czech Republic
Tel: +420 727969150
email: lukas.petr@uhk.cz

Mgr. Josef Jan Horálek, Ph.D
University of Hradec Kralove, Department of Information Technologies,
Rokitanského 62, Hradec Králové, Czech Republic
Tel: +420 493332247
email: josef.horalek@uhk.cz

Ing. Oldřich Horák, Ph.D.
University of Pardubice, Institute of System Engineering and Informatics
Studenstká 84, Pardubice, Czech Republic
Tel: +420 466 036 038
email: Oldrich.Horak@upce.cz