IPv6 is Bad for Your Privacy

Janne Lindqvist

Helsinki University of Technology
Telecommunications Software and Multimedia Laboratory
P.O. Box 5400, FIN-02015 TKK, Finland
janne.lindqvist@tml.hut.fi

Abstract. In recent years, covert channel techniques for IPv4 and more recently for IPv6 have been published by the scientific community and also presented in DEFCON 14. However, a covert channel that contains a considerable bandwidth has been overlooked, the autoconfigured IPv6 address itself. IPv6 Stateless Address Autoconfiguration is used for autoconfiguring addresses without a server in IPv6 networks. The autoconfiguration mechanism consists of choosing an address candidate and verifying its uniqueness with Duplicate Address Detection. The autoconfiguration mechanism has privacy issues which have been identified before and mitigations have been published as RFC 3041. However, we show that the privacy protection mechanism for the autoconfiguration can be used as a covert channel, and consequently, be used to harm the privacy of the user. The covert channel can be serious threat for communication security and privacy. We present practical attacks for divulging sensitive information such as parts of secret keys of encryption protocols. The scheme can also be used for very effective Big Brother type surveillance that cannot be detected by established intrusion detection systems.

1 Introduction

> A covert channel is a mechanism that is not designed for communication, but can nonetheless be abused to allow information to be communicated between parties [2].

Previously, this work has been published as [14], in this version, we take a more tutorial style and present corrections. For example, in [14] we concluded that SEcure Neighbor Discovery (SEND) [3] could prevent this covert channel, but it merely slows it down. Previously published work in TCP/IP covert channels include: how common IPv4 covert channels can be detected and how to implement detection resistant TCP steganography schemes [17], using IP fragmentation and packet sorting as covert channels [1], covert timing channels [6] and enumeration of 22 covert channels in IPv6 [15]. Privacy problems with IPv6 are not limited to covert channels, for example, Mobile IPv6 introduceslocation privacy problems [9].

64 bits	64 bits
subnet prefix	interface id

Fig. 1. IPv6 Unicast Address Format

RFC 2460 - the draft standard specification of IPv6 [8] - was published already in 1998. In addition to the specification, IPv6 introduces many additional mechanisms and protocols, one of them is the stateless address autoconfiguration.

The IPv6 *addressing architecture* is defined in RFC 4291 [10]. It has three different types of identifiers: unicast, anycast and multicast addresses. Unlike its predecessor IPv4, the address architecture is hierarchical. In this context, hierarchy means that addresses have fields for defining the scope of the address. Originally, the addressing architecture specified three scopes for unicast addresses. Today, unicast addresses have two scopes: link-local and global, since RFC 3879 formally deprecated the site-local address scope [11]. Next, we elaborate the IPv6 Stateless Address Autoconfiguration mechanism and privacy extensions for it.

The DAD procedure describe in the Introduction must be supported by all IPv6 implementations [22]. The DAD procedure uses two different Internet Control Message Protocol for IPv6 (ICMPv6) [7] messages: Neighbor Solicitation (NS) and Neighbor Advertisement (NA). The Neighbor Solicitation message is used for multicasting the tentative address to the network. The Neighbor Advertisement message is used to indicate that the tentative address is in use. The message formats are defined in RFC 2461 [20] and RFC 2462 [22].

Optimistic DAD modifies the above. RFC 4429 specifies a new *optimistic* state that can be given to an address. The address can then be used before it has been verified, but the use is not preferred if there is another usable address available. [16]

The default way to use the IPv6 Stateless Address Autoconfiguration is to use the MAC address to derive the interface identifier. However, this mechanism has serious privacy problems [18, 19], which we quote below:

> "Addresses generated using Stateless address autoconfiguration contain an embedded interface identifier, which remains constant over time. Anytime a fixed identifier is used in multiple contexts, it becomes possible to correlate seemingly unrelated activity using this identifier.
>
> The correlation can be performed by
>
> - An attacker who is in the path between the node in question and the peer(s) it is communicating to, and can view the IPv6 addresses present in the datagrams.
> - An attacker who can access the communication logs of the peers with which the node has communicated.
>
> [...]
>
> In summary, IPv6 addresses on a given interface generated via Stateless Autoconfiguration contain the same interface identifier, regardless

> of where within the Internet the device connects. This facilitates the tracking of individual devices (and thus potentially users)."

In simple terms, the privacy extensions propose to use instead of the fixed MAC-address based interface identier a random interface identifier. But when protocols use pseudorandom fields, they can be used as covert channels.

The most severe implications of the stateless address autoconfiguration covert channel is the possibility to divulge any kind of secrets, and thus, violate the privacy of the user. For example, an operating system and IPsec vendor could use the covert channel to transmit session keys when the users think they are merely protecting their privacy with the privacy extensions of the stateless address autoconfiguration protocol.

The transmission of secret keys may need more bits than can fit in the IPv6 address. However, depending on key sizes, only partial information of the key may suffice. The fundamental issue is that any kind of information can be divulged. For example, perhaps organization X is interested in what computers in a country visit particular sites when they are mobile. This information can be divulged with a single bit in the interface identifier part. The computer can remember the visits to a list of sites and after the boot-up send the information in the new statelessly autoconfigured IPv6 address. Additionally, an encoding scheme can be formulated to ensure that the particular bit is not accidentally used. The subtle detail in this scenario is that the information can be passed after boot-up, there is no need to change the IPv6 address before that.

2 Covert Channels in IPv6 Addresses

Using the duplicate address detection for covert channels is possible because the interface identifier part of the address can be chosen in random. In IPv6 enabled Ethernets, the 64 bits of the 128 bit IPv6 address are reserved for the interface identifier (Figure 1). The interface identifier of the address distinguishes individual devices in a local area network [8]. The 64 bits can be used for carrying a message. The 64 bits is a major covert channel and threat because it is always present in the IPv6 packets. Many covert channels presented in the related work section can be protected from the outside attackers by using e.g. IPsec ESP.

To illustrate how large 64 bits is as a covert channel we consider IPsec ESP CBC-mode ciphersuites. RFC 2451 [21] specifies popular key sizes for IPsec ESP CBC-mode ciphersuites. For example, CAST-128 and RC5 algorithms popular sizes include 40 bits, which can be transmitted in a single IPv6 header. 3DES algorithm default and popular size is 192 bits, which requires three different addresses. Naturally, when the encryption schemes evolve and key sizes increase, the 64 bits will become less drastic for secret key divulding purposes. Despite this, even partial keys can be used to crack.

2.1 Generic Attack Scheme

In this section, we present how e.g. a hardware manufacturer can use the IPv6 Stateless Address Autoconfiguration to divulge secret keys of almost any security protocol or other sensitive information.

The hardware manufacturer produces essentially embedded systems such as PDAs. The operating system and the hardware is controlled by the manufacturer.

A wireless mobile device needs to use many addresses on different layers of the protocol stack for identification purposes. One of these addresses is the MAC address of the link layer protocol. For demonstration purposes, we consider the IEEE 802.11b [13] standard based Wireless LAN (WLAN)

The IEEE 802.11b uses a 48-bit address to identify the link-layer network interface [12]. The address is set by the hardware manufacturer or can be configured from the operating system if the device driver allows it.

The MAC address of the device is used to identify the contaminated devices. The first 24 bits of the address indicate Organizationally Unique Identifier (OUI), which is assigned by the IEEE. The rest of the bits are determined by the particular vendor organization.

The manufacturer can use, for example, the 8 bits after the OUI to indicate a contaminated device. Thus, a packet capture software can easily be extended to spot contaminated devices from an area covered by the radio device.

The operating system is modified as follows. The secret key (K_s) of a secure communication protocol is encoded with information on e.g. what type of key it is, what actual session or user it refers to and other necessary information. This information is encrypted with an encryption scheme and a global key known only by the attacker. The "encryption" scheme can be simply protocol and the first applicable bits of the MAC address are operands in XOR operation, and the result is the network interface identifier of an IPv6 address. The XOR operation hides the key from outsiders that do not know the encoding scheme. The operation is illustrated below.

$$K_s \oplus \text{MAC address} = \text{interface id}$$

Agents of the vendor have a database of the contaminated devices on their laptops. The laptops automatically recognize the contaminated devices when scanning the WLAN radio frequencies. When they recognize the contamined devices, the laptops start to record the IP and above level communications and record the IPv6 addresses. The IPv6 address contains the secret key, which can be used to decrypt the encrypted communication. For secret keys larger than the 64 bits, we may use a similar encoding scheme presented in next section. This requires naturally multiple stateless address autoconfiguration procedures that are nevertheless likely to be used for trying to protect the privacy of the user. However, depending on the key length and the used encoding scheme, only single address can be enough, and the remaining bits of the key can be revealed with brute force attack.

The above scenario can naturally be exploited with rootkit malware, received from an email message, for example. The malware checks out the MAC address of the particular device and contaminates the operating system. The MAC address is sent to the attackers computer. Thus, the attacker can now easily track the correct traffic in the radio network. However, this additional scenario requires the sending of the MAC address, and thus, can be more easily noticed compared to the exploitation by the hardware manufacturer.

3 Conclusions

The IPv6 Stateless Address Autoconfiguration can be considered inherently harmful for the privacy of the user. It either 1. introduces the risk that all the traffic originating from the host in different places can be linked to the user or 2. introduces a way to divulge sensitive information about the user or even the secret keys of encrypted communication.

The IPv6 address as a covert channel is a major threat since it exists in every packet even though the payload is protected by IPsec ESP. If the traffic is protected with IPsec ESP, the covert channels of e.g. TCP are not visible for outsiders. Also, we can assume that most computers do not have sophisticated intrusion detection systems and even if they do, most users cannot use them. But, the networks where the users reside, may have intrusion detection systems that monitor the traffic. Thus, e.g. opening a new connection to divulge sensitive information or secret keys is likely to be noticed, but not the covert channel scheme in IPv6 addresses.

A straightforward countermeasure to the covert channel attack is not to allow stateless address autoconfiguration. The use of stateful server-based assignment such as DHCPv6 [5] mitigates the problem effectively. However, this is not possible e.g. for ad hoc networks and, thus, the applicability of the mitigation is limited. Also, the DHCPv6 may introduce administrative burden that otherwise would be relieved with the IPv6 Stateless Address Autoconfiguration mechanism.

SEcure Neighbor Discovery (SEND) [3] protocol has been proposed to replace the Neighbor Discovery protocol. SEND uses Cryptographically Generated Addresses (CGA) [4] which mitigate many attacks against Neighbor Discovery and stateless address autoconfiguration. The idea behing CGA is that the interface identifier is actually a host identifier. The host has a public/private key pair and a hash of the public key is used in the IPv6 address interface identifier. It might seem that CGA effectively mitigates the possibility to use the addresses as covert channels because every bit has meaning. If the address does not match the has of public key used in SEND, it is trivial to deduce something is wrong. However, the attacked needs just to pre-create key pairs that hash to a wanted string that can be used as the address field.

References

1. K. Ahsan and D. Kundur. Practical Data Hiding in TCP/IP. In *Proceedings of the Multimedia and Security Workshop at ACM Multimedia*, Dec. 2002.

2. R. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems.* John Wiley & Sons, Inc., 2001.
3. J. Arkko, J. Kempf, B. Zill, and P. Nikander. RFC 3971: SEcure Neighbor Discovery (SEND), Mar. 2005. Status: Proposed Standard.
4. T. Aura. RFC 3972: Cryptographically Generated Addresses (CGA), Mar. 2005. Status: Proposed Standard.
5. J. Bound, B. Volz, T. Lemon, C. E. Perkins, and M. Carney. RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6), July 2003. Status: Proposed Standard.
6. S. Cabuk, C. E. Brodley, and C. Shields. IP covert timing channels: design and detection. In *Proceedings of the 11th ACM conference on Computer and communications security*, pages 178–187, 2004.
7. A. Conta and S. Deering. RFC 2463: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, Dec. 1998. Status: Draft Standard.
8. S. Deering and R. Hinden. RFC 2460: Internet Protocol, Version 6 (IPv6) Specification, Dec. 1998. Status: Draft Standard.
9. A. Escudero-Pascual. *Privacy in the next generation Internet: Data protection in the context of European Union policy.* PhD thesis, Royal Institute of Technology, 2002.
10. R. Hinden and S. Deering. RFC 4291: IP Version 6 Addressing Architecture, February 2006. Status: Draft Standard.
11. C. Huitema and B. Carpenter. RFC 3879: Deprecating Site Local Addresses, Sept. 2004. Status: Proposed Standard.
12. IEEE. *IEEE Std 802-1990, IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture.* The Institute of Electrical and Electronics Engineers, Inc., 1990. ISBN: 1-55937-052-1.
13. IEEE. *Std 802.11b-1999, Supplement to IEEE Standard for Information Technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz band.* The Institute of Electrical and Electronics Engineers, Inc., 1999.
14. J. Lindqvist. IPv6 Stateless Address Autoconfiguration Considered Harmful. In *Proceedings of the Military Communications Conference - MILCOM 2006*, Oct. 2006.
15. N. B. Lucena, G. Lewandowski, and S. J. Chapin. Covert Channels in IPv6. In *PET 2005, LNCS 3856*, June 2006.
16. N. Moore. RFC 4429: Optimistic Duplicate Address Detection (DAD) for IPv6, April 2006. Status: Proposed Standard.
17. S. J. Murdoch and S. Lewis. Embedding covert channels into TCP/IP. In *7th Information Hiding Workshop*, June 2005.
18. T. Narten and R. Draves. RFC 3041: Privacy Extensions for Stateless Address Autoconfiguration in IPv6, Jan. 2001. Status: Proposed Standard.
19. T. Narten, R. Draves, and S. Krishnan. Privacy Extensions for Stateless Address Autoconfiguration in IPv6: draft-ietf-ipv6-privacy-addrs-v2-04. Internet draft, IETF, May 2005. Work in progress. Expired Nov. 2005.
20. T. Narten, E. Nordmark, and W. Simpson. RFC 2461: Neighbor Discovery for IP Version 6 (IPv6), Dec. 1998. Status: Draft Standard.

21. R. Pereira and R. Adams. RFC 2451: The ESP CBC-Mode Cipher Algorithms, Nov. 1998. Status: Proposed Standard.
22. S. Thomson and T. Narten. RFC 2462: IPv6 Stateless Address Autoconfiguration, Dec. 1998. Status: Draft Standard.