Motivation of article: *this short article is written as a response to document "Opinion 2/2002: on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6". The document was released the 30 May 2002 by the European Union's Article 29 Data Protection Working Party, an independent advisory body on data protection and privacy set up under Article 29 of Directive 95/46/EC.*

TO BE OR NOT TO BE IN THE NEXT GENERATION INTERNET

ALBERTO ESCUDERO-PASCUAL <AEP@KTH.SE>

The global telecommunication infrastructure will slowly converge toward an integrated packet switched network using the Internet Protocol as the common communication technology. First evidence of this convergence is the deployment of the third generation wireless infrastructure that brings together the radio access network and core network by introducing the next generation Internet Protocol IPv6.

Although there have been many technical efforts to insure data confidentiality in the next generation Internet, it is still not known if the new IPv6 security and mobility features will actually be enough to empower users and protect their privacy or if in fact just the opposite will occur.

One open question still remains: will the deployment of the next generation Internet bring more security and privacy to the users or the opposite will occur?

As an example, the article considers the controversial issue of the global unique identifiers in IPv6. After explaining the possible treat for privacy and the limitations of the suggested privacy extension of stateless address autoconfiguration (RFC3041), we also illustrate the new opportunities for privacy that IPv6 brings as the use of Cryptographically Generated IPv6 Address for identity management and pseudonymity.

Complex problems sometimes require no simple answers: When one door closes another door opens wide. New tools for new challenges.

Background

As evidence of the strategic importance of the development of the Internet, in year 2002 the European Union released a statement recommending a European plan of action to accelerate the implementation of IPv6, a key technology for the Next Generation Internet [1].

In response to the technology changes the European Union has also introduced a new regulatory framework that is intended to provide a coherent, reliable and flexible approach to the legal regulation of electronic communication networks and services in fast moving markets. The package of directives will be applied in all Member States from 25 July 2003 with the exception of the Directive on privacy and electronic communications, for which the date is 31 October 2003.

Date: 25 January 2003.

The Data Protection Directive (2002/58/EC) [2] on 'processing of personal data and protection of privacy in the electronic communication sector' is part of the package of new proposals and aims to adapt and update the previous Data Protection Telecommunications Directive (97/66/EC) to take account of technological developments. However, it is not well understood how this policy and the underlying Internet technology can be brought into alignment [3].

Although the Internet is rapidly becoming "the" communication network, it was not really engineered to preserve certain types of privacy. In keeping with the European Union policies regarding data protection there is a need to understand the benefits and to reduce the privacy risks of this new generation of Internet technology. Maintaining proper confidentiality with respect to location information, traffic information, and the actual data traffic itself are three of the key provisions of the new European regulatory framework for electronic communications infrastructure and associated services.

This article presents one timely and important privacy area identified during our late research at the Royal Institute of Technology (KTH) in Sweden: unique identifiers in telecommunication terminal equipments and identity management.

SHORT INTRODUCTION TO IPv6

The Internet Protocol Version 6 (IPv6), also known as IPng (IP Next Generation), is the latest version of the Internet Protocol (IP). Formally, IPv6 is a set of specifications from the Internet Engineering Task Force (IETF). IPv6 is being designed as an evolutionary set of improvements to the current IP Version 4. The most obvious improvement in IPv6 over the IPv4 are that IP addresses are lengthened from 32 bits to 128 bits which anticipates the future growth of the Internet and provides relief for what was perceived as an impending shortage of network addresses. Besides, IPv6 offers technical advantages over IPv4, including self-configuration mechanisms, enhanced security, quality of service features and native mobility support. IPv6 aims to be the protocol capable of bringing together access and core networks, the 'glue' for the deployment of the future 'all-IP' telecommunication network.

IPv6 includes a security protocol in the network layer that provides cryptographic security services that supports combinations of authentication, integrity, access control, and confidentiality. The IP Encapsulating Security Payload (ESP) and the IP Authentication Header (AH) are part of the IP Security architecture (IPSEC) described in RFC 2401 [4].

Both ESP and AH are mandatory parts of IPv6 and make sure that a third party eavesdropping on the channel can not read and/or modify any IP datagrams. The IP Authentication Header seeks to provide security by adding authentication information to each IP datagram whilst confidentiality requires the use of ESP. Nevertheless, neither AH nor ESP hide the source and destination IP addresses of the communicating parties and hence their network location.

The protocol operation defined for mobility in IPv6 is known as MobileIPv6 [5] and allows a mobile node to move from one link to another without changing the mobile node's IP address. A mobile node is always addressable by its "home address", an IP address assigned to the mobile node within its home subnet, i.e., with the network prefix of its home link. Packets may be routed to the mobile node using this address regardless of the mobile node's current point of attachment to the Internet, and the mobile node may continue to communicate with other nodes while using this address, even after moving to a new link. With specific support for mobility in IPv6, packets destined to a mobile node would be able to reach it even while the mobile node is away from its home network. The home IP address identifies the mobile device regardless of its current location.

In summary, IPv6 provides new security opportunities which include message integrity, authentication, and confidentiality (IPSEC) and the possibility for a mobile node to be always addressable by its "home address" (MobileIP). All these functionalities rely on treating the fixed IP address of the node as an identifier. In the case of IPSEC end-to-end security uses the fixed IP address as part of the security association and mobility requires to the mobile node to send the fixed home address included in a destination option.

In the next section we describe how a possible threat for privacy occurs when an IP identifier can be linked with personal identifiable information as a "personal device" and how the existing privacy extension (RFC3041) has not taken into consideration that the user might be also interested in hiding the fact that is using the privacy extension itself.

After presenting two limitations of the RFC3041 we briefly introduce the role that Cryptographically Generated Addresses (CGA) can play as a technical solution for identity management.

Stateless address autoconfiguration and privacy extension

The stateless address autoconfiguration defines the mechanism for a IPv6 device to generate a global unique address (128 bits) without the need of an external DHCP server. The IPv6 address is formed by using the information of the network interface identifier (IID) as right-most 64 bits and the network prefix received in a router announcement as the left-most 64 bits. For example, if we consider a device with an ethernet the Interface Identifier is based on the EUI-64 identifier derived from the interface's built-in 48-bit IEEE 802 address (MAC address).

In summary, the IPv6 addresses generated via Stateless Autoconfiguration contain the same interface identifier regardless of the location the mobile node is attached to the Internet. The right-most 64 bits are persistence and hence devices can be tracked regardless of the point of attachment to the Internet [6].

A privacy extension for stateless address autoconfiguration was introduced in the RFC3041 based on the idea of generating random interface identifiers periodically instead of using the built-in MAC address of the network device. If we consider the definition of privacy introduced by Alan Westin in 1967 [7]:

> "Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others."

While the RFC3041 represents a clear privacy improvement with respect to the stateless address autoconfiguration proposal, we found that the proposed privacy extension has two important limitations:

- **Privacy preference observability:** the use of the RFC3041 also implies that the so called universal/local bit or "u" bit needs to be set to 0. As shown in [6], the fact that a device is using the privacy extension is observable (i.e. an address generated using the privacy extension differ in structure from the others and hence the user's privacy option is public to any communicating party).

- **IP identifier vs IP identity:** while in absence of any other information a set of RFC3041-addresses originated during a period of time can not be linked to one single user (device), but it is far more desirable that the users could determine for themselves, when, how and to what extent the IP information about them is communicated to others. For example, the user could use the IPv6 information as a pseudoidentity. The desired goal is to provide a mechanism that enables authentication against any selected parties while concealing from any third parties that two IP addresses are associated to any given user.

In the following section we introduce the concept of Cryptographically Generated IPv6 Address as a technical mean to enhance privacy while providing authentication in IPv6.

Cryptographically Generated IPv6 Address

The Cryptographically Generated Identifiers and Addresses [8], otherwise known as Crypto-Based Identifiers (CBID's), are identifiers derived via a one-way function applied to a public key. Roughly, $CBID = f(PK, i)$ (Eq. 1) where $f()$ is a well-known one-way function (typically involving a cryptographic hash function), PK is the public key used to produce the corresponding CBID and i is any other inputs to the one-way function. Hence, CBID's are secure representations of that public key.

In the context of IPv6, the term CBID is used to refer to either of the following two types of entities: a) Crypto-Based Address (CBA) is an address whose leftmost 64 bits are set to a valid prefix (as per normal IPv6 usage), and whose rightmost 64 bits (interface identifier) are set to a 64-bit entity obtained via a one-way function such as shown in Eq. (1) and, b) Crypto-Based Identifier (CBI) is a fixed length entity in which the entire identifier (typically 128 bits) is derived as shown in Eq. (1).

These identifiers have four very important properties:

(1) They are statistically unique, because of the collision-resistant property of the cryptographic hash function used to generate them.
(2) Since a node can prove ownership of its CBID. Thus, they are securely bound to a given node. A node accomplishes this "proof of ownership" by revealing the public key, PK, used to generate the CBID (along with any other values used as input to the one-way function). It then proves that it knows the corresponding private key, SK, by digitally signing a message.
(3) They do not rely on any centralized security service such as a PKI or Key Distribution Center.
(4) Their binding to any particular entity or user may be kept private at the discretion of the CBID creator (typically the entity or user itself).

Related work [8] shows how CBID's are very useful to secure Mobile IPv6. Further work [9] combines CBID's with SPKI-style authorization certificates to solve the proof-of-membership problem. In summary, the resultant scheme allows a user or host to prove to any third party that it is a member of a given group without the requirement of revealing its identity.

Conclusions

The default mechanism to obtain an IPv6 address based on stateless address autoconfiguration introduces a new threat for privacy as the interface identifier remains constant regardless of time and point of attachment to the network. While the privacy extension (RFC3041) is a clear privacy improvement with respect to the stateless address autoconfiguration proposal, it has important limitations as the users can not determine by simple means, when, how and to what extent the IP information about them is communicated to others.

While IPv6 introduces new possible threats for privacy it also provides the possibility to use new schemes as the Crypto Based Identifiers that can be well adapted to Privacy and Identity Management. For example, the use of CBA in IPv6 can not only solve the address ownership problem and secure Mobile IPv6, but also can be used as a privacy enhancement technology (PET) [6].

With this article we propose and encourage to investigate the use and implementation of Crypto Based Identifiers as a Privacy Enhanced Technology (PET) in the context of ubiquitous networking and as promising technology that can be used to technically enforce the Directive on privacy and electronic communications (2002/58/EC).

Acknowledgments. To Claude Castelluccia (INRIA, Rhône-Alpes) and Gabriel Montenegro (Sun Microcrosystems Labs, Grenobe) for their input to the CBA section. See working document "Crypto Based Identifiers (CBID) for Privacy and Identity Management (PIM)", proposal for future research in IPv6, November 2002. `http://www.it.kth.se/~aep/publications/aep-claude-gab-cbid-4-pim.pdf`

About the author. Dr. Alberto Escudero-Pascual <aep@kth.se> is researcher at the Royal Institute of Technology in Sweden since 1999 in the area of privacy in mobile Internetworking. His research interests vary from security in wireless networks to legal aspects of data retention and cybercrime. Further info at: `http://www.it.kth.se/~aep`

References

[1] European Commission, Next Generation Internet priorities for action in migrating to the new Internet protocol IPv6, COM(2002) 96 final, Brussels, 21st February 2002.

[2] European Parliament, European Telecommunication New Regulatory Framework, 2000-2002.

[3] Article 29 Working Party, Opinion 2/2002: on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6, 30 May 2002.

[4] S. Kent and R. Atkinson,Security Architecture for the Internet Protocol, RFC 2041.

[5] D. Johnson and C. Perkins, Mobility Support in IPv6, draft in progress.

[6] A. Escudero, Privacy in the next generation Internet, Data Protection in the context of European Union Policy. Conclusions of PhD Thesis. Royal Institute of technology, December 2002.

[7] A. F. Westin, Privacy and Freedom, Atheneum Press, New York, USA. 1967.

[8] G. Montenegro and C. Castelluccia, Statistically Unique and Cryptographically Verifiable Identifiers and Addresses, ISOC NDSS02, San Diego, February 2002.

[9] C. Castelluccia and G. Montenegro, Dynamic and Secure Group Membership in Ad Hoc and Peer-to-Peer Networks (short paper), ACM MC2R, October 2002.