TITLE:	**DISCUSSION DOCUMENT FROM THE EUROPEAN COMMISSION IPV6 TASK FORCE TO ARTICLE 29 DATA PROTECTION WORKING GROUP**
AUTHORS	**EC IPV6 TASK FORCE**
DATE:	**FEBRUARY 17TH 2003**
VERSION:	**1.2 (FINAL)**
DISTRIBUTION:	**PUBLIC**
DOCUMENT NUMBER:	**28**

Introduction:

On 30 May 2002 the 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, released a document titled "Opinion 2/2002: on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6". The document describes the possible threats for privacy on the use of unique identifiers in telecommunication terminal equipments and illustrates some of those concerns using as a concrete example the case of next generation protocol IPv6.

While the EC IPv6 Task Force (EC IPv6 TF) recognises that the use of unique identifiers in any kind of technology or communication media (e.g. Ethernet, WLAN, GSM, ID cards, IPv4, and IPv6) represents a potential threat for privacy, the Task Force also notes that the use of stable identifiers is an important practical requirement in any communication system. The Task Force is also concerned that the referred document, which aims to create awareness about possible privacy threats in the development of the Internet, can result in an unbalanced view of the benefits that can be obtained by adoption of IPv6, especially when compared to what exists now for IPv4.

All communications are subject to privacy issues, and IPv6 is no exception, but IPv6 has provided a mechanism (RFC3041) that goes a long way to solving the problem, potentially providing a higher degree of protection to the users than is possible with IPv4. In addition, IP security (IPSec) mechanisms are available in full IPv6 implementations (RFC2460)[1]. Although their use is not mandated, this offers an improvement over IPv4, where IPSec support is not present by default.

Technical Rationale:

The following key considerations must be taken in account when reviewing the privacy implications with IP-based communications, both for the existing IPv4 and the emerging IPv6:

1. IPv4 has privacy issues with static IP addresses being used as identifiers. These can be tracked just as other devices and items used by a person can be.
2. IPv6 by default *where stateless autocofiguration is used*[2] will construct IPv6 addresses that allow correlation of activity where the same device is connected to different networks, because a constant identifier (based on hardware in the device) is embedded in the IPv6 address.
3. RFC3041[3] fixes the problems of correlation by allowing an IPv6 device to generate a random identifier to embed in the address.
4. Many Internet systems use IP addresses as a (weak) authentication mechanism. Use of Privacy Extensions prevents such authentication being used. However, IPv6 includes IPSec by default, allowing stronger authentication methods to be used.
5. IPv6's Privacy Extensions enable a static host (e.g. workstation in an office) to use different IPv6 source addresses through time (e.g. a different IPv6 source address daily), allowing greater privacy for such non-mobile devices and users.
6. It is normal practice for IPv6 devices to have multiple addresses, where IPv4 devices usually have one address. It is thus possible for future IPv6 applications to use multiple (dynamic) IPv6 addresses, e.g. to reduce traceability in peer-to-peer applications.
7. Further research may introduce new classes of IPv6 addresses, for example cryptographically generated addresses. This is only possible with IPv6.

[1] RFC2460: The Internet Protocol, Versión 6, specification (section 4), http://www.ietf.org/rfc/rfc2460.txt
[2] There are other methods to acquire an IPv6 address, e.g. manual configuration or DHCPv6
[3] RFC3041: Privacy Extensions for Stateless Address Autoconfiguration in IPv6 (http://www.ietf.org/rfc/rfc3041.txt).

8. The EC IPv6 TF strongly recommends that vendors implement RFC3041 by default in all systems. The TF notes that some vendors that have already done so.
9. There should be easy user-controllable mechanisms for RFC3041 to be enabled or disabled, per device/interface or per application. This could also be automatic depending on the initiated traffic (in-bound or outbound), pre-configured by default or customized. These may require further work or research. Again, such enhancements are only possible with IPv6.

Balancing Security, Privacy and Usability:

It is often not the content of a communication that is necessarily important, but the identity of the devices that are communicating, and their owners. In such cases, those snooping traffic may choose to take certain actions based on who they perceive is communicating with who, regardless of the message content. "Guilt by association" is a common paradigm for a number of environments. Also, privacy protection is required to protect citizens against any serious breach of conduct by other individuals, companies, or rogue organizations.

When a security gateway (creating a VPN, via tunnel mode IPSec) is used, end host identities are hidden; only the addresses of the VPN gateways are visible outside of the encrypted data. In contrast, in IPsec end-to-end transport mode, the IP addresses of the communicating hosts are visible, even if the data is encrypted. Both these models can be used in IPv4 and IPv6 networks, but IPv6's much larger address space means end-to-end transport mode IPSec (for new, novel services and applications) will be far more common than it is in the IPv4 world.

Because IPv6 vastly increases the available address space, there is no need for Network Address Translation (NAT) devices (which complicate application development, which make it difficult to run services *into* networks, which make plug and play networking harder, and which limit the end-to-end transparency of the Internet)[4]. In an IPv6 world, it is not expected that NAT will be used.

Another issue to be considered is the balance of privacy against the ability to detect hacking and other types of attack on the network. For example RFC 3041 improves privacy, but it makes denial of service attacks harder to detect. It also makes per-host IP-based authentication very difficult (although this may be argued as a good thing, as IP-based authentication is a weak method, and IPv6 enables stronger IPSec methods to be used in its place).

The privacy issue is one (important) piece of larger chess-game of security, transmission, e-business, open-government, law-enforcement, and even good-governance. So in any inter-governmental recommendations on this area it would be useful to see more interdisciplinary approach emerging in future.

Summary:

The EC IPv6 TF believes that the new built-in properties in IPv6 provide a set of necessary and unique tools to empower a user's privacy in ways that are not possible in IPv4. The combination of the availability of IPSec support in full IPv6 implementations combined with these new properties makes IPv6 a potentially powerful tool to improve the possibilities for user privacy.

The TF strongly recommends the implementation of RFC3041 by all IPv6 vendors. However, it is clear that in any communication medium a balance needs to be struck between usability and privacy. For example, further work would be desirable on allowing user-controllable enabling of the IPv6 privacy extensions on a per-application basis.

[4] RFC2775: Internet Transparency, B. Carpenter, February 2000, http://www.ietf.org/rfc/rfc2775.txt