

IPv6 is Bad for Your Privacy

Janne Lindqvist

Helsinki University of Technology (TKK)

and

International Computer Science Institute (ICSI)

- 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.

- S. J. Murdoch and S. Lewis, “Embedding covert channels into TCP/IP,” in *7th Information Hiding Workshop*, June 2005.
- K. Ahsan and D. Kundur, “Practical Data Hiding in TCP/IP,” in *Proceedings of the Multimedia and Security Workshop at ACM Multimedia*, Dec. 2002.
- 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*, Oct 2004.
- C. Candolin and P. Nikander, “IPv6 source addresses considered harmful,” in *Sixth Nordic Workshop on Secure IT (NordSec)*, Nov. 2001.
- A. Escudero-Pascual, “Privacy in the next generation Internet: Data protection in the context of European Union policy,” Ph.D. dissertation, Royal Institute of Technology, 2002.

IPv6 Stateless Address Autoconfiguration

- Unicast IPv6 address consists of two parts
 - 64 bits for *subnet prefix*
 - 64 bits for *interface identifier*
- IPv6 Stateless Address Autoconfiguration is used for autoconfiguring addresses without a server
 - Does not require manual configuration or DHCPv6
- Autoconfiguration mechanism to acquire *link-local* and *global* IPv6 addresses.

Autoconfiguration and Duplicate Address Detection Procedure

- A node chooses a *tentative* address candidate
- The node then performs Duplicate Address Detection
 - The tentative address is multicasted to the link-local network.
 - If the address is already in use, the node using the address replies to the message and the first node chooses a different address.
 - If no messages are received, the address is successfully configured and can be used.

Known Issues with Autoconfiguration 1/2

- A trivial Denial of Service (DoS) attack can be launched against the DAD
 - A malicious node just replies to all tentative address solicitations that the address is already in use
 - Can be detected and mitigated with heuristics
 - e.g. the likelihood of one collision is already negligible and so is e.g. three consecutive collisions

Known Issues with IPv6 Autoconfiguration 2/2

- By default, the address interface identifier is derived from the MAC address of the network interface
 - This creates privacy problems (RFC 3041)
 - The interface identifier can be used to correlate all traffic originated from the node, and thus possibly to identify the user of the host.
 - The correlation can be performed by an attacker that is in path of two communicating peers, or an attacker that can access the logs of the peers.
 - RFC 3041 proposes privacy extensions
 - The identifier is chosen randomly

IPv6 interface identifier as a covert channel

- Since the interface identifier can be arbitrary, it can also contain useful information for an attacker.
 - 64 bits should be enough for everyone
- However, we need to assume that the attacker can somehow compromise the operating system.
 - Perhaps the OS or IPsec stack vendor is malicious
 - Perhaps you receive an innocent looking email that installs a rootkit when you click the attachment
 - Perhaps somebody just walks to your computer and..

Why is this different from other covert channels?

- The IPv6 address is in every packet that you send to the network.
- Other possible covert channels, such as, TCP sequence numbers can be encrypted into IPsec ESP payload and thus not available for third parties.
- You cannot detect the covert channel by any known means
 - Our conjecture is that you cannot detect it on the network in any case, only protecting the operating system will help.

- Let's assume a user with a WLAN device
- The attacker has compromised the WLAN device and has a database of compromised devices listed on their MAC addresses.
- The attacker can just passively listen to WLAN traffic and check if there are compromised devices nearby.
- Identified devices divulge e.g. IPsec ESP encryption keys (or partial keys) in the IPv6 addresses.

- The operating system contains a list of WWW sites.
- The web browsing is monitored by the OS and if a site that matches the list is browsed:
 - Next time the computer is rebooted the IPv6 stateless address autoconfiguration contains a preconfigured bit pattern even though the address seems random.
 - When the address is changed, it may contain another preconfigured bit pattern.
 - Now, everywhere the computer is used, it tells the passive listener

- Obvious answer is naturally:
 - Do not use autoconfiguration, use DHCPv6
 - this is not always possible, e.g. ad hoc networks
 - Use an otherwise *completely secure* operating system
- Contrary to discussion presented in the paper, SEcure Neighbor Discovery (SEND) does not help
 - SEND uses Cryptographically Generated Addresses, thus every bit in the interface identifier part has a “meaning”.
 - However, this only reduces the bandwidth of the covert channel!

- The results can be generalized:
 - When we introduce randomness to protocol identifiers to protect the privacy of the user, we introduce possible covert channels that
 1. can be used to compromise the confidentiality of communication
 2. can be used to reveal any kind of information about the user to third parties.