draft-ietf-6man-ipv6-address-generation-privacy-00

Alissa Cooper
Fernando Gont
Dave Thaler

Goal and scope

- Provide unified privacy and security assessment of address generation techniques

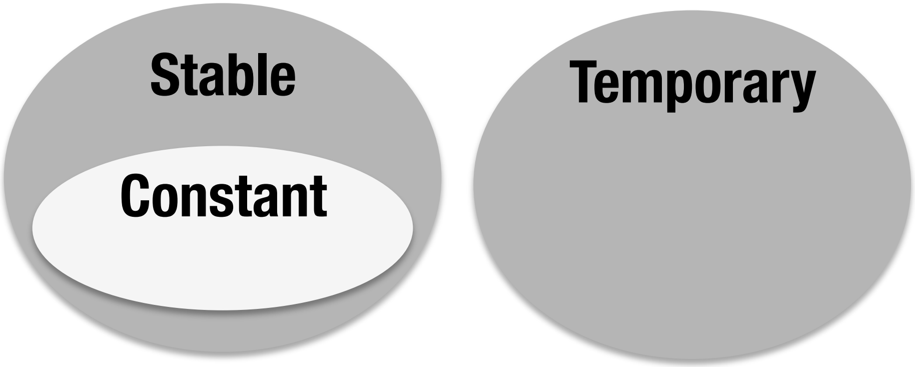
Address terminology

- **Stable address** does not vary over time within the same network.
- **Temporary address** varies over time within the same network.

- **Public address** has been published in a directory or other public location, such as the DNS, a SIP proxy, an application-specific DHT, or a publicly available URI. A host's public addresses are intended to be discoverable by third parties.

IID terminology

- **Constant IID** is globally stable; does not vary from network to network.
- **Stable IID** is stable within some specified context.
  - Globally stable == constant
  - Stable per network
- **Temporary IID** varies over time.



Mechanism terminology

- **Temporary** -- RFC 4941
- **Stable, semantically opaque --** draft-ietf-6man-stable-privacy-addresses
- **Constant, semantically opaque --** Microsoft Windows

Weaknesses in IEEE identifier-based IIDs

- Correlation of activities over time
- Location tracking
- Address scanning
- Device-specific vulnerability exploitation

Privacy and security properties

Mechanism	Correlation	Location tracking	Address scanning	Device exploits
IEEE identifier	Possible for *device* lifetime	Possible for *device* lifetime	Possible	Possible
Static manual	Possible for *address* lifetime	Depends on generation mechanism	Depends on generation mechanism	Depends on generation mechanism
Constant, semantically opaque	Possible for *OS* lifetime	Possible for *OS* lifetime	No	No
CGA	Typically possible for *public key* lifetime	Typically possible for *public key* lifetime	No	No

Privacy and security properties cont'd

Mechanism	Correlation	Location tracking	Address scanning	Device exploits
DHCPv6	Possible for *lease* lifetime (typically hours)	No	Depends on DHCPv6 server implementation	
Stable, semantically opaque	Possible for *OS* lifetime	No	No	No
Temporary	Only possible for *temporary address* lifetime	No	No	No

Privacy and security properties overview

Mechanism	Correlation	Location tracking	Address scanning	Device exploits
IEEE identifier	Possible for device lifetime	Possible for device lifetime	Possible	Possible
Static manual	Possible for address lifetime	Depends on generation mechanism	Depends on generation mechanism	Depends on generation mechanism
Constant, semantically opaque	Possible for OS lifetime	Possible for OS lifetime	No	No
CGA	Typically possible for public key lifetime	Typically possible for public key lifetime	No	No
DHCPv6	Possible for lease lifetime (typically hours)	No	Depends on DHCPv6 server implementation	No
Stable, semantically opaque	Possible for OS lifetime	No	No	No
Temporary	Only possible for temp address lifetime	No	No	No

Discussion