Current Hostname Practice Considered Harmful

draft-huitema-privsec-harmfulname-00
Huiitema@microsoft.com, dthaler@microsoft.com
IETF 93, Prague, July 2015
Connection ➔ Leaking metadata!

• Wi-Fi:
  – Leaks the MAC Address – fixed by randomization
• DHCP
  – Leaks unique ID, host name, FQDN – fixed by anonymity profile
• IPv6
  – Unique IIDs enable tracking – work in progress in 6MAN
• DNS
  – Look for many names for “background services” – fixed by DPRIVE
• MDNS, LLMNR
  – Hello, is there someone out there with name = “my name”?  
  – NOT FIXED
• And probably many more, using Host Name in discovery, pairing
Host Name Practice Considered Harmful

• Names are defined for a specific context but used everywhere

• Three common practices
  – “BrandX-123456-7890-abcdef” – unique ID
  – “huiitema-laptop” – pretty good partial identifier
  – “rosebud” – reduces search space by factor 1000 or more

• If we randomize the names “per connection,” we stop (many of) the leaks

• But this is an interesting “platform change.”
Why is it important?

• Little pieces of information go in “tracking buckets”

• Soon enough, records for
  – MAC Addresses
  – IP address & date time
  – Email address
  – Cookies
  – Traffic pattern

• After that, tracking from “partial identifiers” works very well!
Example of disclosure in DNS-SD

- Publish a service, name chosen by the user. (Fine)
- Wait for requests from potential users. (Fine)
- Respond with service advertisement. (Fine)
- Publish hostname of the laptop in the advertisement.
  - So the client can do a name to address lookup.

- Issues:
  - The user is conscious of publishing the service name, not the host name
  - The host name can be harvested by third parties

- Could we use some “anonymous name” instead?
Request to the INT Area: scrub the meta-data

- Dave and Christian cannot look at everything, need your help
- Look for the following patterns
  - Gratuitous messages sent just in case
  - Sticking names in headers because it helps management
  - Derive device names from user names
- Propose updates
  - Send messages exactly when needed
  - Scrub the messages, apply data minimization
  - Use short lived anonymous name when possible
  - Do not disclose PII in host names