WHEN TO USE DHCP

Ted Lemon <mellon@fugue.com>

HISTORY

- DHCPv4
  - configure the stack (IP address, default route, MTU, etc)
  - configure DNS
  - configure time server, domain search list, lpr, syslog, hostname
  - provide bootstrap information for network boot
- Assumptions:
  - Safe network
  - Host is in fixed location

MORE HISTORY

- DHCPv6
  - Not everyone wanted it
  - We decided not to kitchen-sink the config parameters
  - Still had the old safe network/static host model somewhat in mind

MAKE DHCP SAFE FOR HUMANITY

- DHCP Security
  - Many failed attempts
  - Keying is hard
  - Threat model isn't clear
  - Nobody really cared enough to make this happen
- Why not?
  - Because our vague vision for security assumed the old, historical model: hosts don't move around

THE DHCP FLOW

- DHCP happens every time you change networks
- This means that DHCP makes sense when you need to configure something that changes every time you change networks
- Services that you want to use regardless of the network to which you are attached do not have this property.
- e.g., IMAP, SMTP, HTTP, SSH, NFS...
- DHCP also doesn't have choice semantics. You get what you get. So e.g. you don't want to discover your printer using DHCP unless you will only ever have one printer, even though the printer is a local resource.

THE BIG THROW-DOWN

- The scene: the DHC Working Group Meeting
- The combatants: me and Cullen
  - Two geeks enter. Two geeks leave.
- The question to be decided: when is it appropriate to configure services using DHCP
- The service in question: I don't remember, probably SIP

ARGUMENTS IN FAVOR

- We need something to configure SIP servers
- DHCP is something
- We don't have anything else
- Let's use DHCP

ARGUMENTS AGAINST

- DHCP provides *zero* authentication
- Hosts roam, so even if you trust the network, is the DHCP server on *this* network the one that is authoritative for your (e.g.) SIP server?
- Do we want hosts to just use the SIP server on the local network?
- What is the trust model? Since it's not DHCP, does SIP solve this?
- Is there a general principle here?

REJOINDERS

- We could just use DHCP the first time, and then cache the SIP server info (or whatever)
- But we don't even know if the first network is trustworthy

CONCLUSION

- In order to use DHCP safely, there has to be a trust model for the specific service being configured using DHCP
- In general, DHCP is actually a crappy protocol to use for solving this problem even if you have a trust model
- And of course, since the trust model is entirely semantic, there's no way to verify that it's being followed
- Therefore, using DHCP to configure anything other than the basic parameters of the network, which you have to trust to use the network anyway, is a Bad Idea
- Also, use DNSSEC and validate in the stub, because otherwise your DHCP-provided DNS resolver, which is a service, can attack you.