Some security aspects of HOMEGATE
Hiroshima, November 2009

Paul Hoffman, VPN Consortium
Overview

• Security protocols that gateways should not thwart
• Security model
• Threat model (current)
• Good security practices
Some gateways and firewalls by default break...

- DNSSEC
  - Already covered in BCP 152 / RFC 5625
- IPsec
  - Tries to “help” IKEv1 and fails
- NATs in general hurt
  - ESP needs to use UDP encapsulation
- Screwing up fragmentation hurts IKE
Security model for HOMEGATEs

• Regardless of what security geeks would want to be true...
• Default configuration has no public keys (such as for trust anchors)
• System configuration is updated over DHCP with no authentication
• At that point, an attacker can do anything bad that does not require authentication
Current threat models

• Botted PCs can compromise gateways
• Run DDoS even if the PC is turned off
• Change the DNS and gateway values gotten from DHCP to point to compromised DNS servers and gateways
  – Used to infect and re-infect PCs on the LAN
Good security practices

• Specific advice about not breaking protocols
• Do not make the admin password easily guessable
  – Typically done using the LAN’s MAC address
• Consider getting some trust anchors from addresses given in DHCP
  – Useful for secure firmware update (RFC 4108), distributing DNSSEC trust anchors, and so on