Sniffing cable modems

Guy Martin <gmsoft@tuxicoman.be>
Defcon 16 - Aug 2008 – Las Vegas

Agenda

- What is DOCSIS ?
  - Use of DOCSIS
  - General architecture
  - Registration process
  - Encryption on the link
- Cool, how can I sniff it ?
  - DVB-C card
  - Packet-o-matic to the rescue

Agenda

- Doable things
  - Privacy
  - Modem SNMP hacks
  - Misc
- References
  - DOCSIS
  - MPEG
  - Packet-o-matic

What is DOCSIS

- Use of DOCSIS
  - Internet : The most known application of the DOCSIS protocol
  - Telephony : Most cable modems have a built-in ATA (Analog Telephone Adapter)
  - Digital TV decoders : built-in cable modems to monitor/feedback data from end users

What is DOCSIS

- General architecture
  - CMTS on the ISP side broadcast packets to end users on a common single frequency
  - Modems on end user side send packets back to CMTS on another frequency during its timeslot
  - A CMTS serves from a small neighborhood to a whole city
  - Downstream frequency is in the same range than TV ones
  - Uses MPEG packets like normal digital TV to encapsulate data

What is DOCSIS

- Registration process
  - Aquire and lock the downstream frequency
  - From this, find out the upstream parameters
  - Get an IP address
  - Download the modem configuration via TFTP
  - Apply the configuration and enable forwarding of packets

What is DOCSIS

- Encryption on the link
  - Encryption and authentication are NOT mandatory
  - BPI (Baseline Privacy Interface) provides a mechanism for authentication and/or encryption
  - DES and AES are the two possible encryption algorithms

How to sniff it

- DVB-C card
  - Possible because protocols and frequencies are purposely similar to digital TV ones
  - Inexpensive
  - Only the downstream traffic can be captured
  - Different hardware like USRP could be used to capture both upstream and downstream

How to sniff it

- Packet-o-matic to the rescue
  - Input module capture the traffic
  - Packets are processed and matched using match, helpers and conntrack modules
  - Eventually the target module process the packets to produce the desired output
  - Everything occurs real-time
  - Telnet and XML-RPC interface available

Doable things

- Privacy
  - Sniff data destinated to all ISP users
  - Reassemble streams real-time and extract useable files on the fly (mail, phone and IM conversations, ...)
  - DoS by reinjecting TCP RST (tcpkill) packets or ICMP error packets

Doable things

- Modem SNMP hacks
  - Change IP filters of the modem's ethernet bridge
  - Deny access to the server polling the download/upload quota
  - Reboot the modem
  - Anything else the modem's SNMP interface allows

Doable things

- Misc
  - Bypass modem filters by reinjecting sniffed packets in the LAN
  - Create a virtual network interface (tap device) so other tools can be used

References

- DOCSIS
  - http://www.cablelabs.com/
  - http://www.cablemodem.com/specifications/
- MPEG
  - ISO/IEC 13818-1
- Packet-o-matic
  - http://www.packet-o-matic.com