SECURITY VERIFICATION™
What's your exposure ?

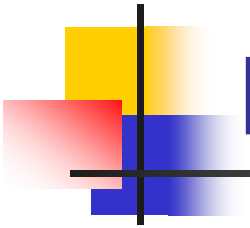
Stealth Data Dispersion

ICMP Moon-Bounce

Saqib A. Khan, Principal
khan@SecurityV.com

Latest Version @ http://SecurityV.com/research

SECURITY VERIFICATION™
What's your exposure ?



Definition

Stealth Data Dispersal is an asynchronous covert channel

Project Goal

Reside small amounts of data on the “ether” (within network traffic) rather than fixed physical storage.

Project Benefit

Data becomes highly survivable in case of catastrophic failure/removal of Network Hosts

Preferred Embodiment

- Dispersal of small amounts of data (< 1500 bytes = PPP MTU)
- Data stays "alive" on the wire vs. a storage device, as long as possible
- Data is retrieved or refreshed before data expires on the "wire"

SECURITY VERIFICATION™
What's your exposure ?

Core TCP/IP Impediment

TTL limits all TCP/IP packets to expire automatically after 255 hops!

Packets which reach limit are automatically discarded

Candidate TCP/IP Protocols

1. ICMP (Inet Control Message Protocol)
   - Implementation required on all TCP/IP stacks
   - Echo Replies required to echo back original "Request" data
   - Universally available – Print servers, etc
   - Fair amount of ICMP traffic always present on the wire, ergo stealthy

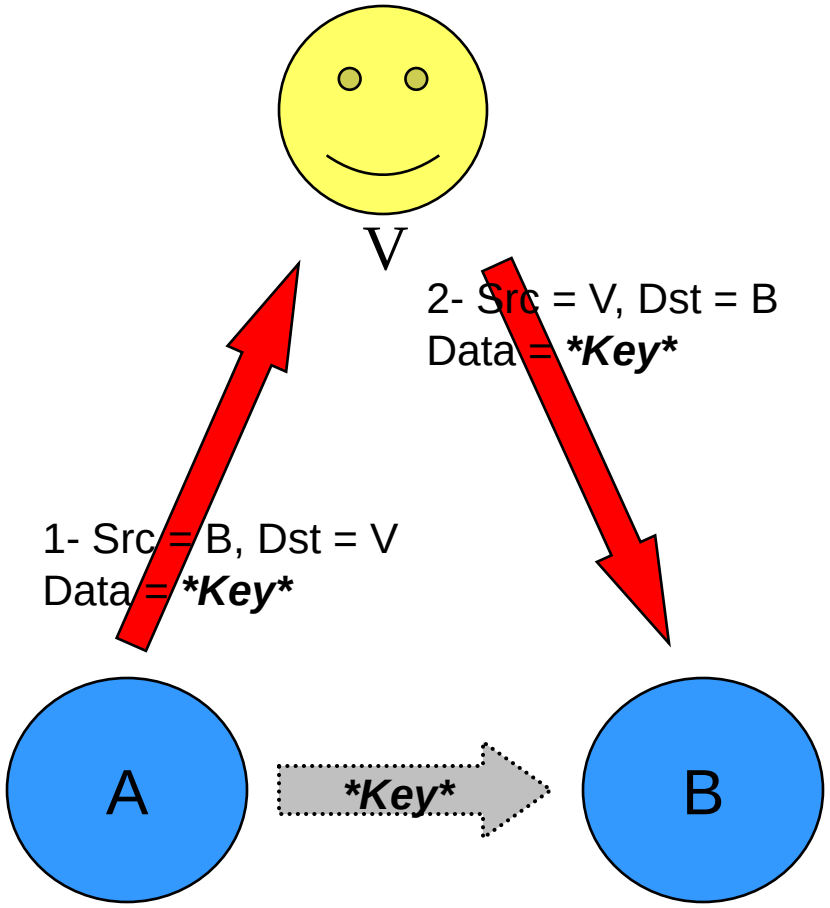
Candidate TCP/IP Protocols

2. Multicast/IGMP (Inet Group Mgmt Protocol)
   - Designed for communicating between single Source to multiple Destinations (utilizing single transmission)
   - Very large amount of data can be found on the wire at any time (being used to broadcast numerous audio streams, etc), ergo very stealthy!

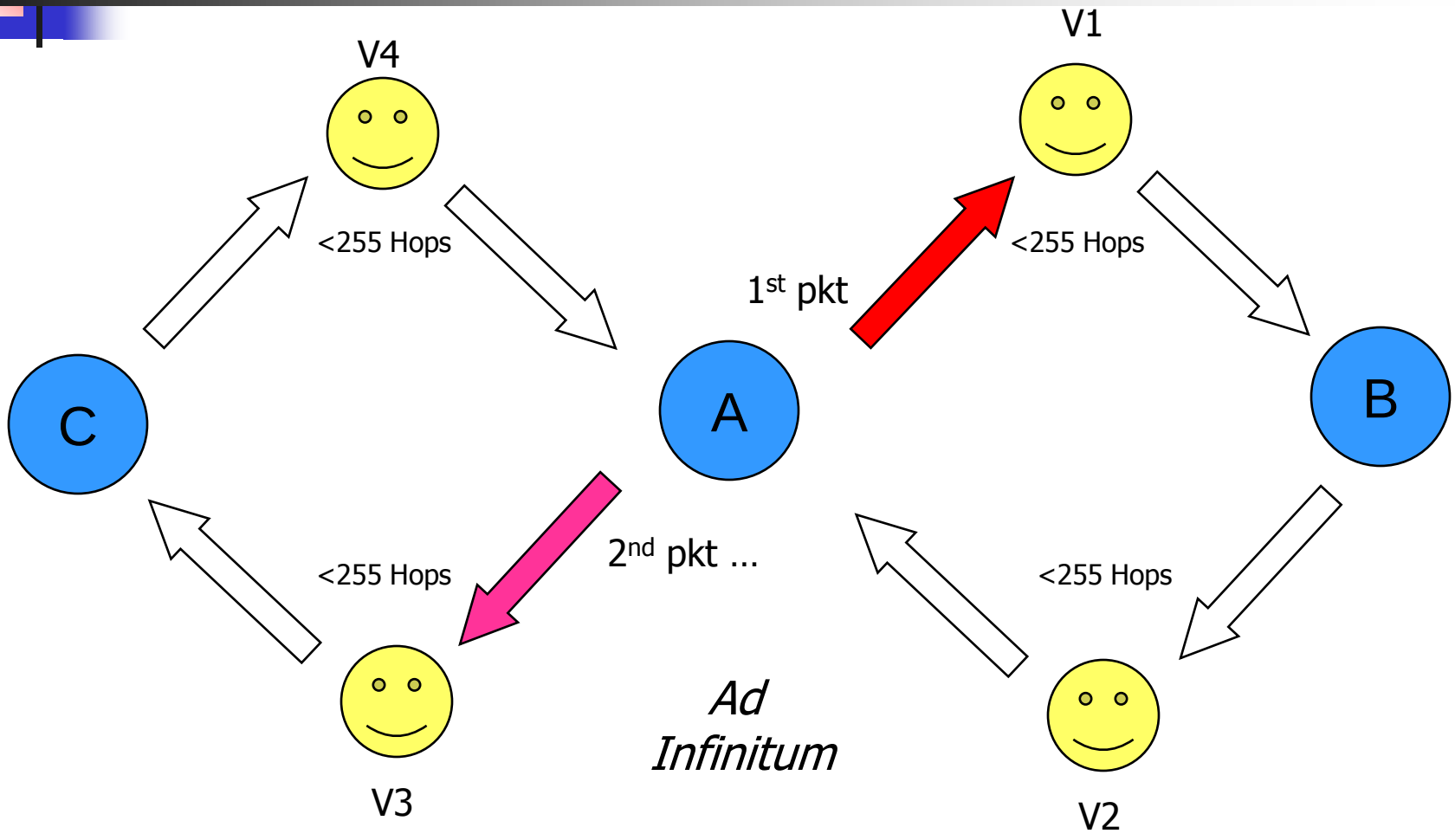
ICMP Moon-Bounce

- Basic Operation: Bounce data between 2 Hosts utilizing an intermediary Victim Host.
- Process:
  1. A sends spoofed Echo Request pkt -> V (w/ B's Src Addr)
  2. V Echo Reply's -> B, inadvertently echo-ing A's data
  3. B Ack's A directly, signaling data received.
  4. B repeats A's procedure to return data
- Data is now bouncing between 2 Hosts!

PS - Doubles as a good synchronous covert channel, as well!



Moon-Bounce Dispersal



Moon-Bounce Accomplishes

1. Possible data dispersal over 1020 hops (255 x 4) per co-operating Host! (as long as routes are chosen carefully)
2. Double your pleasure! (double hops available utilizing spoofing)
3. Delayed packet releases over mulitple routes ensures intermediary Hosts capable of detecting failure and responding!

Conclusions

1. Stealth Data Dispersal is possible utilizing current TCP/IP Protocol manipulation
2. It can be achieved very efficiently
3. It can very stealthy and should be able to bypass most defenses unhindered
4. The ICMP Moon-bounce has been *rumored* to be used as a covert channel by *dark government agencies*!!!

- Further research on using Multicast/IGMP and proof of concept tools, etc currently under way @
  - http://SecurityV.com/research
    - Thank you!