Networked Systems Security

Unauthorized Access

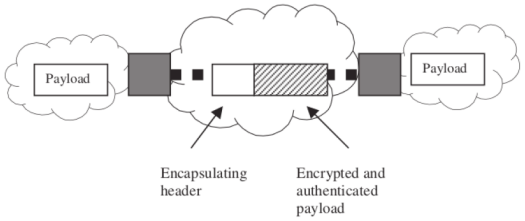
Network Protocol Tunneling

Module TA:
Hongyu Jin, hongyuj@kth.se
Mohammad Khodaei, khodaei@kth.se

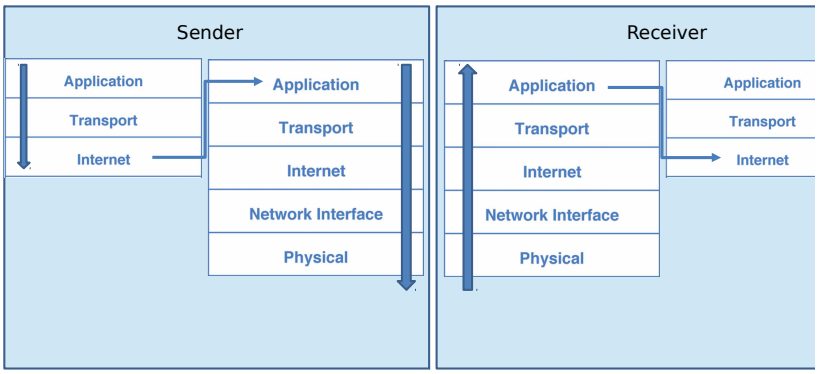
Panos Papadimitratos
Networked Systems Security Group
www.ee.kth.se/nss

Network Protocol Tunneling

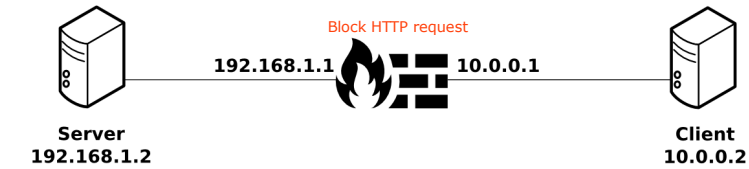
- Encapsulate the packets of a protocol in another protocol that operates in the same or higher layer
  - IPv6 over IPv4 (6to4): Encapsulate IPv6 packets in payloads of IPv4 packets
  - IPSec: Encapsulate whole IP packets with new (tunnel mode) or original (transport mode) IP headers



DNS Tunneling



Demo



Iodine Server
DNS tunnel:172.16.0.1

Iodine Client
DNS tunnel:172.16.0.2

Prevention Mechanism

- Snort rules for detecting iodine covert DNS tunneling

- # detects iodine covert tunnels (over DNS)
- alert udp any any -> any 53 (content:"|01 00 00 01 00 00 00 00 00 01|"; offset: 2; depth: 10; content:"|00 00 29 10 00 00 00 80 00 00 00|"; \
  msg: "***covert iodine tunnel request***"; ***threshold: type limit***, track by_src, count 1, seconds 300; sid: 5619500; rev: 1;)

- alert udp any 53 -> any any (content: "|84 00 00 01 00 01 00 00 00 00|"; offset: 2; depth: 10; content:"|00 00 0a 00 01|"; \
  msg: "***covert iodine tunnel response***"; ***threshold: type limit***, track by_src, count 1, seconds 300; sid: 5619501; rev: 1;)

Questions?