CIS 433/533: Computer and Network Security

Prof. Kevin Butler
Winter 2013
Networking

• Fundamentally about transmitting information between two devices

• Direct communication is now possible between any two devices anywhere (just about)
  ‣ Lots of abstraction involved
  ‣ Lots of network components
  ‣ Standard protocols
  ‣ Wired and wireless
  ‣ Works in *protection* environment

• What about ensuring *security*?
Network Security

- Every machine is connected
  - What is trust model of the network?

- Not just limited to dogs as users
  - What other ‘dogs’ are out there?
Exploiting the network ...

• The Internet is extremely vulnerable to attack
  ‣ it is a huge open system ...
  ‣ which adheres to the end-to-end principle
    • smart end-points, dumb network

• Can you think of any large-scale attacks that would be enabled by this setup?
The End-to-End Argument

• Clark et. al discussed a property of good systems that says features should be placed as close to resources as possible
  ‣ In communication, this means that we want the middle of the network to be simple, and the end-points to be smart (e.g., do everything you can at the end-points
  • “Dumb, minimal network”
  ‣ This is the guiding principle of IP (Internet)
  ‣ Q: Does this have an effect on security?
• **Note:** this is a departure from the early networks which smart network, dumb terminals
Network security: the high bits

• The network is …
  ‣ … a collection of interconnected computers
  ‣ … with resources that must be protected
  ‣ … from unwanted inspection or modification
  ‣ … while maintaining adequate quality of service.

• Another way of seeing network security is …
  ‣ … securing the network infrastructure such that the integrity, confidentiality, and availability of the resources is maintained.
The network ...
The big picture . . . .

• Internet Protocol (IP)
  ‣ Really refers to a whole collection of protocols making up the vast majority of the Internet

• Routing
  ‣ How these packets move from place to place

• Network management
  ‣ Administrators have to maintain the services and infrastructure supporting everyone’s daily activities
Security Problems in the TCP/IP Protocol Suite

• Bellovin’s observations about security problems in IP
  ‣ Not really a study of how IP is misused, e.g., IP addresses for authentication, but really what is inherently bad about the way in which IP is setup
  ‣ A great overview of the basic ways in which security and the design of IP are at odds with each other

  ‣ Q: What changed in the 15 years since Bellovin wrote the original paper?
  ‣ Q: What’s changed since then?
Sequence number prediction

- TCP/IP uses a *three-way handshake* to establish a connection

1. C -> S: $Q_C$
2. S -> C: $Q_S, \text{ack}(Q_C)$ where sequence number $Q_S$ is nonce
3. C -> S: $\text{ack}(Q_S)$ … then send data

2. However assume the bad guy does not hear msg 2, if he can guess $Q_S$, then he can get S to accept whatever data it wants (useful if doing IP authentication, e.g., “rsh”)
Sequence Number Prediction (fixes)

• The only way you really fix this problem to stop making the sequence numbers predictable:
  ‣ Randomize them -- you can use DES or some other mechanism to generate them randomly
  ‣ There is an entire sub-field devoted to the creation and management of randomness in OSes

• Also, you could look for inconsistencies in timing information
  ‣ Assumption: the adversary has different timing than
  ‣ OK, maybe helpful, but far from definitive
Routing Manipulation

• RIP - routing information protocol
  ‣ Distance vector routing protocol used for local network
  ‣ Routers exchange reachability and “distance” vectors for all the sub-networks within (a typically small) domain
  ‣ Use vectors to decide which is best, notification of changes is propagated quickly

• So, the big problem is that you receive vast amounts of data that a router uses to form the routing table
  ‣ So, just forge that, and the game is up
  ‣ Manipulate paths, DOS, hijack connections, etc.

• Solutions:
  ‣ Authenticate data, but this is less than obvious how to do this efficiently (a whole lot of people are trying)
Internet Control Message Protocol (ICMP)

• ICMP is used as a control plane for IP messages
  ‣ Ping (connectivity probe)
  ‣ Destination Unreachable (error notification)
  ‣ Time-to-live exceeded (error notification)

• These are largely indispensable tools for network management and control
  ‣ Error notification codes can be used to reset connections without any

• Solution: verify/sanity check sources and content
  ‣ ICMP “returned packets”

• Real solution: filter most of ICMP, ignore it
The “ping of death” …

• In 1996, someone discovered that many operating systems, routers, etc. could be crash/rebooted by sending a single malformed packet
  ‣ It turns out that you can send a IP packet larger than 65,535 (2^{16}), it would crash the system
  ‣ The real reason lies in the way fragmentation works
    • It allows somebody to send a packet bigger than IP allows
    • Which blows up most fixed buffer size implementations
    • … and dumps core, blue screen of death, etc.
  ‣ Note: this is not really ICMP specific, but easy (try it)
    % ping -l 65510 your.host.ip.address

• This was a popular pastime of early hackers
Address Resolution Protocol (ARP)

• Protocol used to map IP address onto the physical layer addresses (MAC)
  1) ARP request: who has x.x.x.x?
  2) ARP response: me!

• Policy: last one in wins

• Used to forward packets on the appropriate interfaces by network devices (e.g., bridges)

• **Q:** Why would you want to spoof an IP address?
ARP poisoning

• Attack: replace good entries with your own
• Leads to
  ‣ Session hijacking
  ‣ Man-in-the-middle attacks
  ‣ Denial of service, etc.

• Lots of other ways to abuse ARP.
• Nobody has really come up with a good solution
  ‣ Except smart bridges, routers that keep track of MACs
• However, some not worried
  ‣ If adversary is in your perimeter, you are in big trouble
  ‣ You should never should validate the source of each pack independently (e.g., via IPsec)
• Finger user identity (my advisor hated this)
  ‣ host gives up who is logged in, existence of identities

  % finger butler
  Login: butler                     Name: Kevin Butler
  Directory: /home/faculty/butler   Shell: /bin/zsh
  Last login Thu Feb 10 23:58 (EST) on ttys000
  No Mail.
  No Plan.
  %

• This is horrible in a distributed environment
  ‣ Privacy, privacy, privacy …
  ‣ Lots of information to start a compromise of the user.
• Post office protocol - mail retrieval
  ‣ Passwords passed in the clear (duh)
  ‣ Solution: SSL, SSH, Kerberos

• Simple mail transport protocol (SMTP) - email
  ‣ Nothing authenticated: SPAM
  ‣ Nothing hidden: eavesdropping
  ‣ Solution: your guess is as good as mine

• File Transfer protocol - file retrieval
  ‣ Passwords passed in the clear (duh)
  ‣ Solution: SSL, SSH, Kerberos