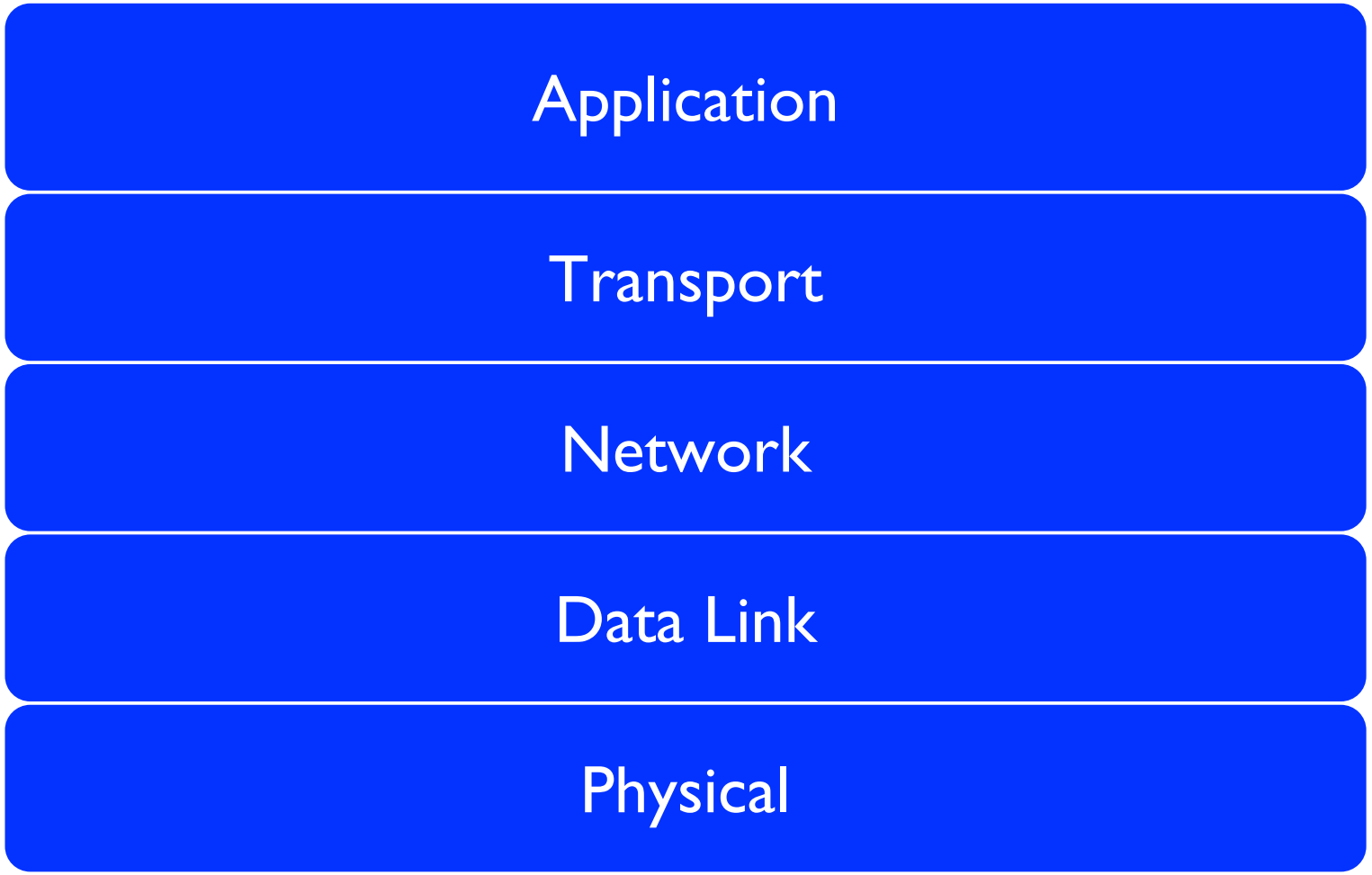
CSC 405
Introduction to Computer Security

TCP/IP Security

Alexandros Kapravelos
akaprav@ncsu.edu

(Derived from slides by Will Enck and Micah Sherr)

Network Stack



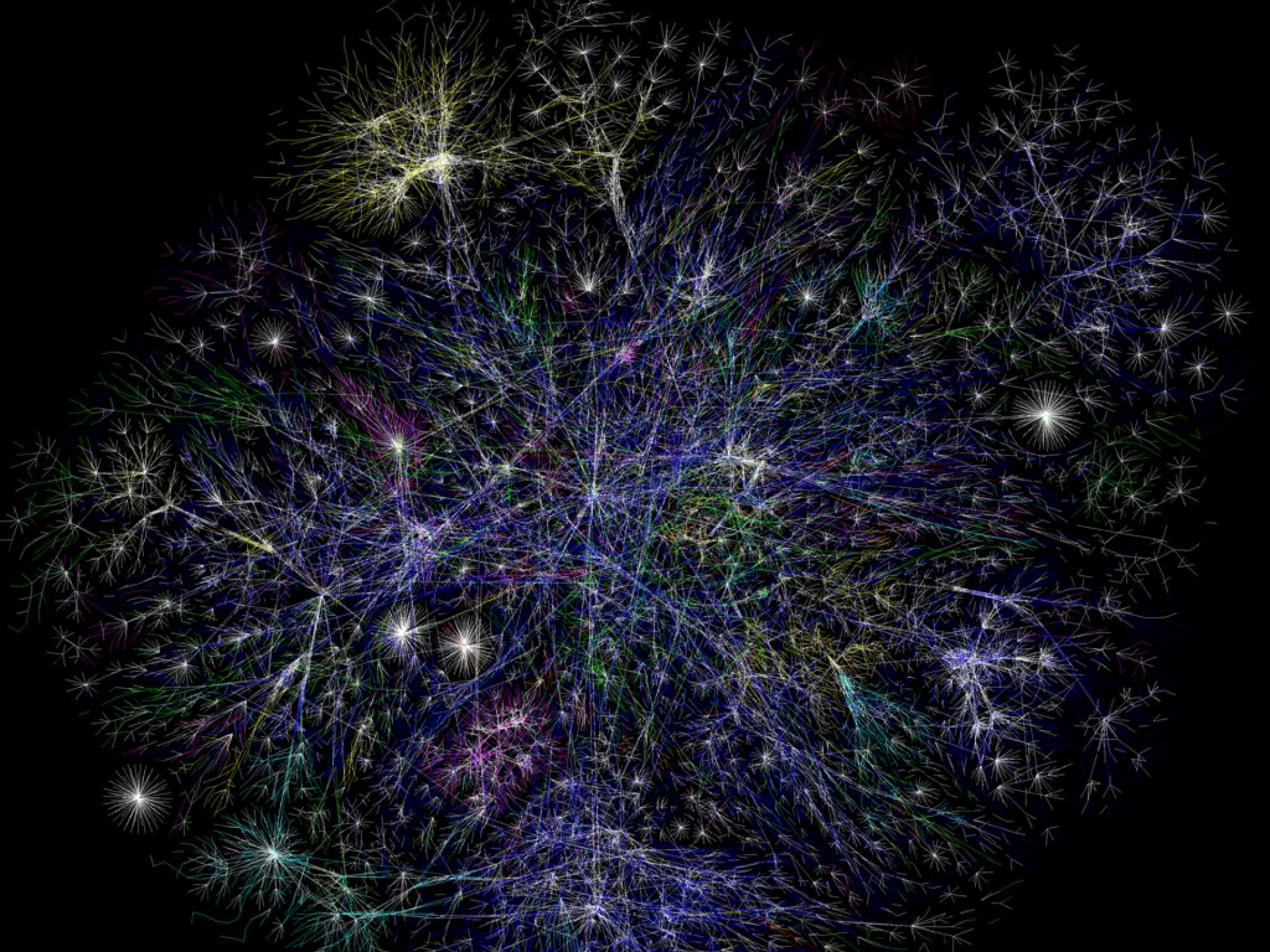
Networking

- Fundamentally about transmitting information between two devices
- Communication is now possible between any two devices anywhere (just about)
  - Lots of abstraction involved (see previous slide)
  - Lots of network components (routers)
  - Standard protocols (e.g., IP, TCP, UDP)
  - Wired and wireless
- What about ensuring security?

Network Security

- Every machine is connected
  - No barrier to entry
  - Not just limited to dogs as users

"On the Internet, nobody knows you're a dog."



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?

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.

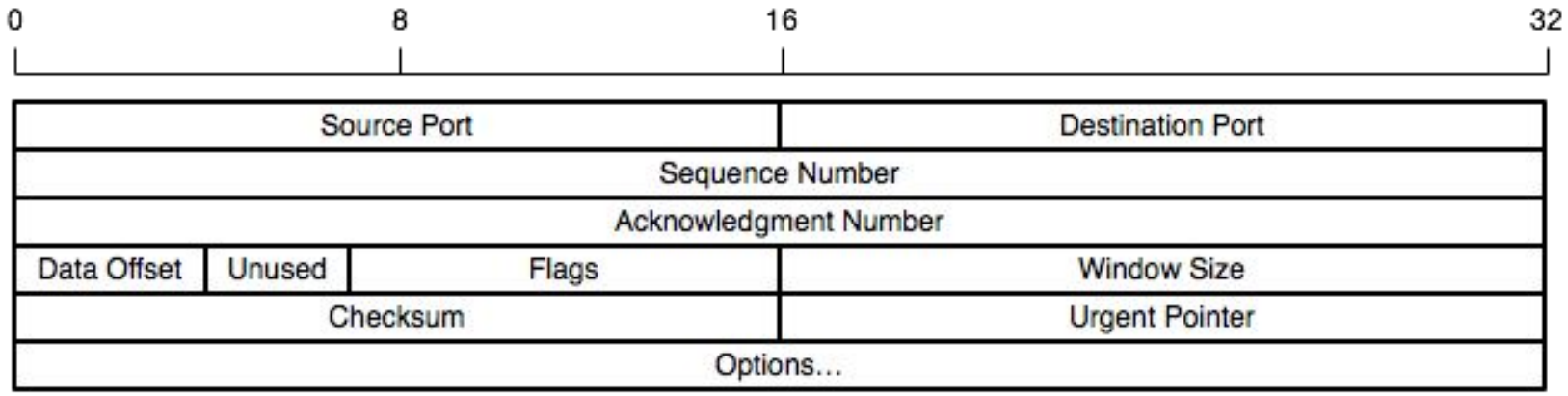
Network Security: The high bits

- Network Security (one of many possible definitions):
  - Securing the network infrastructure such that the integrity, confidentiality, and availability of the resources is maintained.

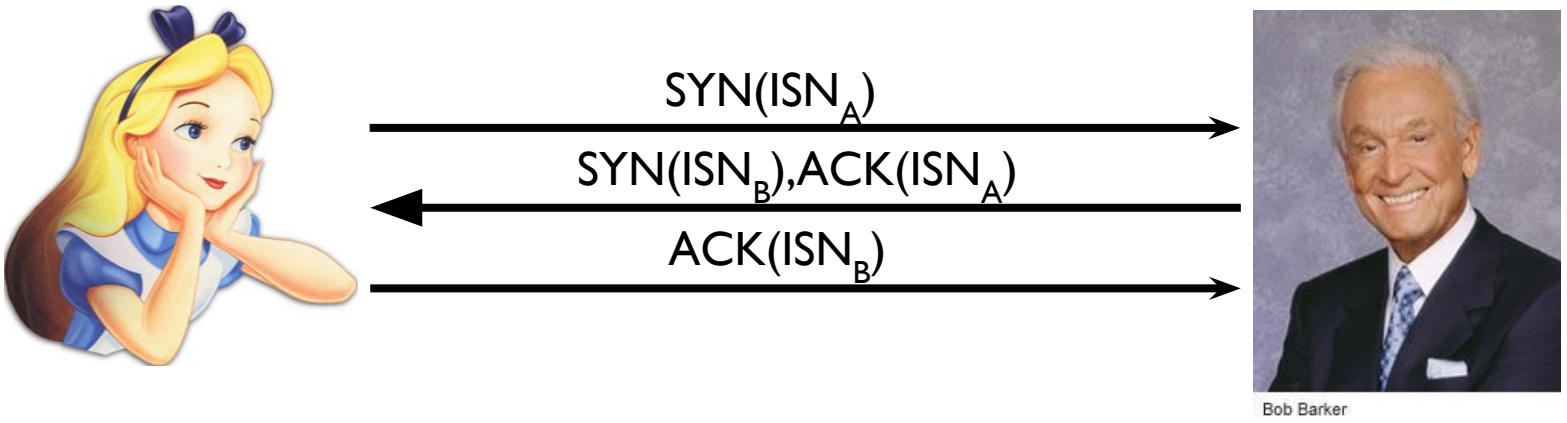
Steven Bellovin's Security Problems in the TCP/IP Protocol Suite

- Bellovin's observations about security problems in IP
  - Not really a study of how IP is misused (e.g., IP addresses for authentication), but rather what is inherently bad about the way in which IP is set up
- A really, really nice overview of the basic ways in which security and the IP design is at odds

TCP Header

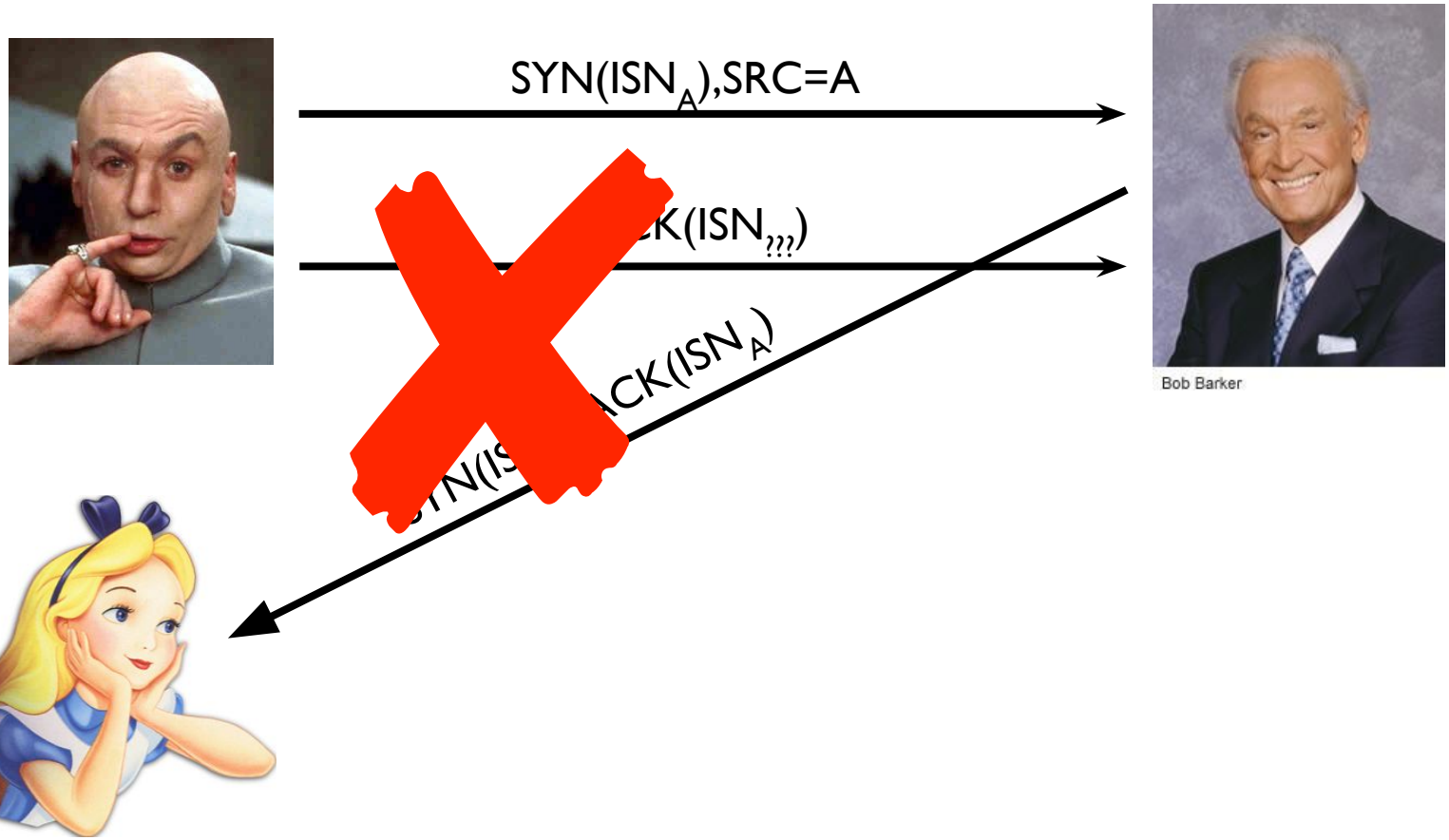

0
8
16
32
Source Port
Destination Port
Sequence Number
Acknowledgment Number
Data Offset
Unused
Flags
Window Size
Checksum
Urgent Pointer
Options…

TCP Sequence Numbers



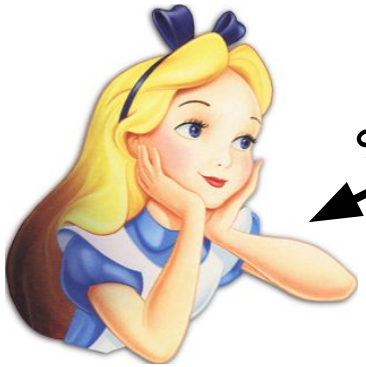
- TCP's "three-way handshake":
  - each party selects Initial Sequence Number (ISN)
  - shows both parties are capable of receiving data
  - offers some protection against forgery -- WHY?

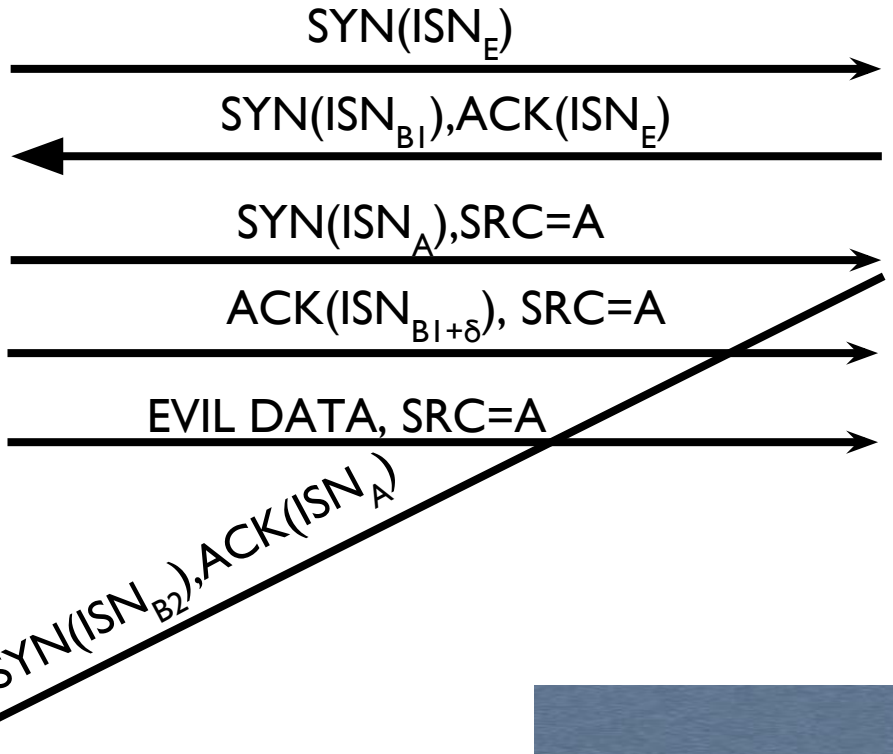
TCP Sequence Numbers



TCP Sequence Numbers

Bob Barker





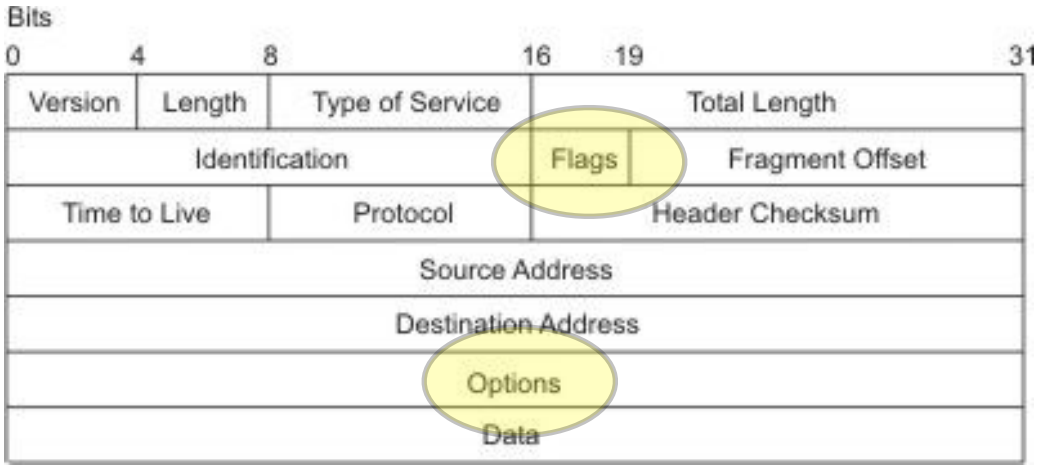
In many TCP implementations, ISNs are predictable -- based on time (e.g,. ++ each 1/128 sec)

How do we fix this?

- More rapidly change ISNs
- Randomize ISNs

Source Routing

- Standard IP Packet Format (RFC791)
- Source Routing allows sender to specify route
  - Set flag in Flags field
  - Specify routes in Options field



Source Routing

Bob Barker

R2

R4

R5

Source Routing

- Q: What are the security implications of Source Routing?
  - Access control?
  - DoS?
- Q: What are the possible defenses?
  - A: Block packets with source-routing flag

Routing Manipulation

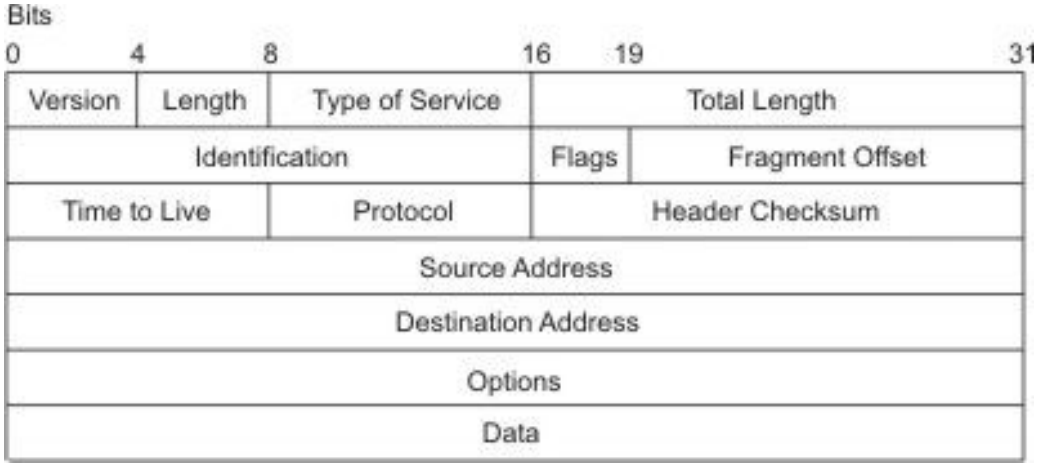
- RIP - Routing Information Protocol
  - Distance vector routing protocol used for the local network
  - Routers exchange reachability and "distance" vectors for all the sub-networks within (a typically small) domain
  - Use vectors to decide which route is best
- Problem: Data (vectors) are not authenticated
  - Forge vectors to cause traffic to be routed through adversary
  - or cause DoS
- Solutions: ? (still an open problem)

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)
- Some ICMP messages cause clients to alter behavior
  - e.g., TCP RSTs on destination unreachable or TTL-exceeded
- ICMP messages are easy to spoof: no handshake
- Enables attacker to remotely reset others' connections
- Solution:
  - Verify/sanity check sources and content
  - Filter most of ICMP

Background: IP Fragmentation

- 16-bit "Total Length" field allows 2^{16}-1=65,535 byte packets
- Data link (layer 2) often imposes significantly smaller **Maximum Transmission Unit** (MTU) (normally 1500 bytes)
- Fragmentation supports packet sizes greater than MTU and less than 2^{16}
- 13-bit Fragment Offset specifies offset of fragmented packet, in units of 8 bytes
- Receiver reconstructs IP packet from fragments, and delivers it to Transport Layer (layer 4) after reassembly

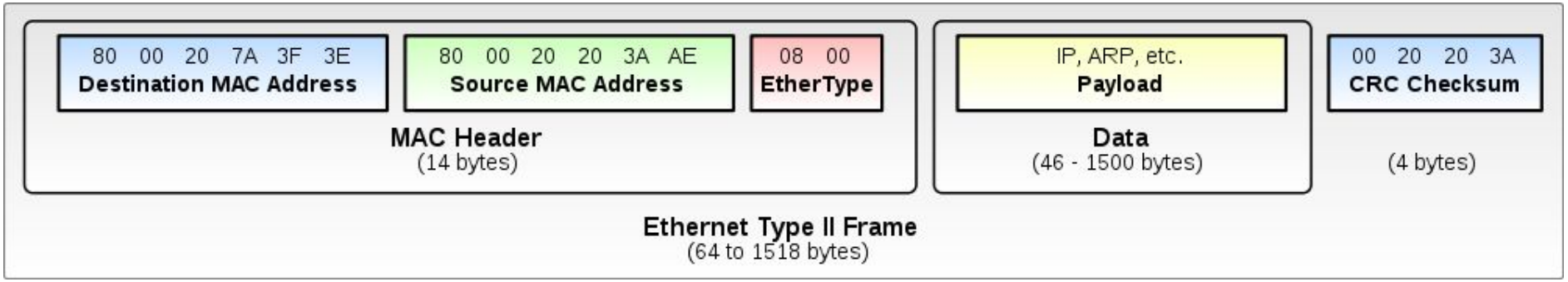


Ping-of-Death

- Maximum packet size: 65,535 bytes
- Maximum 13-bit offset is $(2^{13} - 1) * 8 = 65,528$
- In 1996, someone discovered that many operating systems, routers, etc. could be crash/rebooted by sending a **single** malformed packet
  - If packet with maximum possible offset has more than 7 bytes, IP buffers allocated with 65,535 bytes will be overflowed
  - ...causing crashes and reboots
- Not really ICMP specific, but easy
  - % ping -s 65510 your.host.ip.address
- Most OSes and firewalls have been hardened against PODs
- This was a popular pastime of early hackers

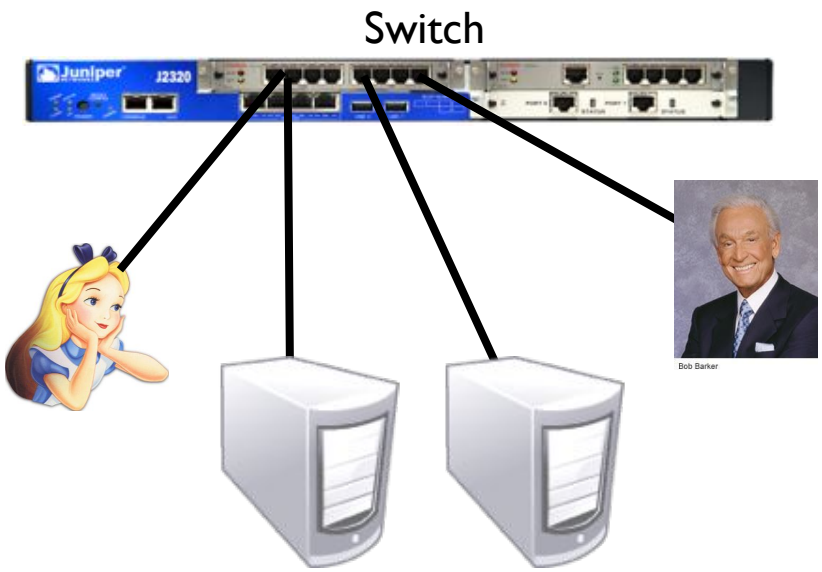

WARNING!
The system is either busy or has become unstable. You can wait and see if the system becomes available again and continue working or you can restart your computer.
* Press any key to return to Windows and wait.
* Press CTRL+ALT+DEL again to restart your computer. You will lose any unsaved information in all applications.
Press any key to continue _

ARP Spoofing: Background: Ethernet Frames



ARP Spoofing: Background: ARP

- Address Resolution Protocol (ARP): Locates a host's link-layer (MAC) address
- Problem: How does Alice communicate with Bob over a LAN?
  - Assume Alice (10.0.0.1) knows Bob's (10.0.0.2) IP
  - LANs operate at layer 2 (there is no router inside of the LAN)
  - Messages are sent to the switch, and addressed by a host's link-layer (MAC) address
- Protocol:
  - Alice broadcasts: "Who has 10.0.0.2?"
  - Bob responses: "I do! And I'm at MAC f8:1e:df:ab:33:56."



ARP Spoofing

- Each ARP response overwrites the previous entry in ARP table -- **last response wins**!
- Attack: Forge ARP response
- Effects:
  - Man-in-the-Middle
  - Denial-of-service
- Also called **ARP Poisoning** or **ARP Flooding**

ARP Spoofing: Defenses

- Smart switches that remember MAC addresses
- Switches that assign hosts to specific ports

Port Scanning

- Side-channel attack on network protocol and implementation properties
- Used to efficiently gather information on target networks
  - Network topology
  - Access control policy
  - Network service availability, versions
- Classic network reconnaissance technique
  - Sometimes a precursor to actual attacks

Portscan Types

- Connect scan
  - Use connect syscall to attempt full three-way TCP handshake
  - Available to unprivileged users, but slow
- SYN scan
  - Use raw sockets to directly inject a TCP SYN packet and wait for SYN-ACK response
  - Much more efficient
- UDP scan
  - Send UDP packets and wait for ICMP error response

Port Knocking

- Port knocking: a technique for hiding the existence of server ports from reconnaissance techniques like port scans
  - Client must issue a secret sequence of packets before being able to connect to a service, like a secret knock
- Many variations
  - Simple: TCP SYN to ordered list of ports before connecting to real port
  - Can also incorporate rate limiting, multiple protocols, cryptographic challenges, …

OS Detection

- Differences in TCP/IP implementations useful for *fingerprinting* remote machines
  - Due to flaws or specification ambiguity
- Fingerprints recorded for known systems, collectively form a fingerprint database
  - Database can be matched against runtime responses to identify a likely remote OS
  - Both active (nmap) and passive (p0f) classifiers

POP/SMTP/FTP

- Post office protocol - mail retrieval
  - Passwords passed in the clear
  - Solution: SSL, SSH, Kerberos
- Simple mail transport protocol (SMTP) - email
  - Nothing authenticated: SPAM
  - Nothing hidden: eavesdropping
  - Solution: ?
- File Transfer protocol - file retrieval
  - Passwords passed in the clear
  - Solution: SSL, SSH, Kerberos

Lessons Learned?

- The Internet was built for robust communication
- Smartness occurs at the end-hosts
- Does this design support or hinder network security?

And if we had to start all over again, could we do better?