CE 817 - Advanced Network Security

Lecture 2

Mehdi Kharrazi
Department of Computer Engineering
Sharif University of Technology

Acknowledgments: Some of the slides are fully or partially obtained from other sources. Reference is noted on the bottom of each slide, when the content is fully obtained from another source. Otherwise a full list of references is provided on the last slide.

What is Security?

- Confidentiality
- Integrity
- Availability

Confidentiality (محرمانگی)

- “The property that information is not made available or disclosed to unauthorized individuals, entities, or process [i.e. to any unauthorized system entity].” {definitions from RFC 2828]
- Not the same as privacy
- Privacy: “the right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others.”
- Privacy is a reason for confidentiality

Integrity (صحت)

- Data integrity: “The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner”
- System integrity: “The quality that a system has when it can perform its intended function in a unimpaired manner, free from deliberate or inadvertent unauthorized manipulation.”
- Often of more commercial interest than confidentiality

Availability (دسترس پذیری)

- “The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e. a system is available if it provides services according to the system design whenever users request them.”
- Turning off a computer provides confidentiality and integrity, but hurts availability. . .
- Denial of service attacks are direct assaults on availability

More Definitions

- **vulnerability (آسیب پذیری):** An error or weakness in the design, implementation, or operation of a system
- **attack (حمله):** A means of exploiting some vulnerability in a system
- **threat (تهدید):** An adversary that is motivated and capable of exploiting a vulnerability

(Definitions from Trust in Cyberspace)

Vulnerabilities

- The technical failing in the system
- The primary focus of most computer security classes
- If you can close the vulnerabilities, the threats don’t matter
- Or do They?

Threats

- Different enemies have different abilities
- Teenage joy-hackers can’t crack a modern cryptosystem
- Serious enemies can exploit the “three Bs”:
  - Burglary, bribery, balckmail
- You can’t design a security system unless you know who the enemy is

Threats

Joy Hackers

- Many are “script kiddies”; some are very competent.
- The scripts are very sophisticated.
- The hackers share tools more that the good guys do.

Are Joy Hackers a Problem?

- What would it cost you to rebuild a machine?
- What would your CEO say if you ended up on the front page of the newspapers?
- What if they’re working for someone else?

Hacking for Profit

- The hackers have allied themselves with the spammers and phishers
- The primary motivation for most current attacks is money
- The market has worked:
  - the existence of a profit motive has drawn new talent into the field
- We are seeing, in the wild, sophisticated attacks
- We're seeing less pure vandalism
- Most of today's worms and viruses are designed to turn victim computers into "bots"

Organized and Disorganized Crime

- In many cases, hacking is just another venue for ordinary criminal activity
- The same people who hack steal credit card numbers, launder money, etc.

Industrial Espionage

- Less than 5% of attacks are detected. Professionals who are after you won't use your machine to attack other companies, and that's how successful penetrations are usually found.
- Professionals are more likely to use non-technical means, too: social engineering, bribery, wiretaps, etc.
- Professionals tend to know what they want.

Inside Jobs

- Insiders know what you have.
- Insiders often know the weak points.
- Insiders are on the inside of your firewall.
- Etc., etc., etc.
  - What if your system administrator turns to the Dark Side?

Spies

- Governments may want your technology.
- Some governments lend tangible support to companies in their own countries.
- Spies tend to be sophisticated, well-funded, etc.
- Is cyberwarfare a threat?

Why Does This Matter?

- You have to build your defenses accordingly
- Security is fundamentally a matter of economics.
- How much security can you afford?
- How much do you need?

Assets

What are you protecting?

- Host-resident data?
- Bandwidth?
- CPU time?
- Knowledge of what hosts exist?

Scanning a Network

Host 192.168.2.1 appears to be up.

MAC Address: 00:04:E2:34:B6:CE (SMC Networks)

Host 192.168.2.79 appears to be up.

MAC Address: 00:11:11:5B:7A:CD (Intel)

Host 192.168.2.82 appears to be up.

MAC Address: 00:10:5A:0D:F6:D7 (3com)

Host 192.168.2.198 appears to be up.

MAC Address: 00:10:DC:55:89:27 (Micro-star Internati

Host 192.168.2.199 appears to be up.

MAC Address: 00:C0:4F:36:33:91 (Dell Computer)

Host 192.168.2.200 appears to be up.

MAC Address: 00:0C:41:22:CC:01 (The Linksys Group)

Does That Matter?

- The number of computers an organization has roughly corresponds to the number of people in it
- How large is you competitor?

Attacker Powers

- Note the MAC addresses in that output
- Those can only be determined from on-LAN
- Does the attacker have that ability?

Bandwidth Attacks

- Clog you bandwidth -- denial of service attacks
- Use you bandwidth to attack some one else
- May not require penetrating your hosts:
  - Reflector attacks

Reflector Attack

- Find a UDP-based service, such as DNS, where the response is much larger that the query
- Send some server a small query, but forge the source address to point to your victim
- The innocent server sends a large reply to the victim, generating more bandwidth than you could, and absorbing the blame

Network Identity Attacks

- Suppose you want to offer illegal content
- Hack someone else's machine, and run a server there
- They'll get blamed, not you
- (Note: the same trick works for clients doing illegal things)

Eavesdropping

- So-called “sniffer” program can pick up traffic, especially passwords
- Done to major backbones even today.

Sniffing Credit Cards

- It’s hard to pick up passwords -- they are some times sent one character per packet
- Credit card numbers are easy: they are 15 or 16 digits, and self-checking

Vulnerabilities

Problem

- We are dealing with the host world and the network world
- We need to protect against both classes of vulnerabilities
- Techniques differ

Host Vulnerabilities

- Our goal: keeping the bad guy from penetrating the networked host (generally via a buggy application)
- If a penetrated application is used to break host security, it is probably an OS and application security issue
- If the application itself can be tricked into doing nasty things, it is probably a network security problem
- No, the categories are not neat and clean

Network Vulnerabilities

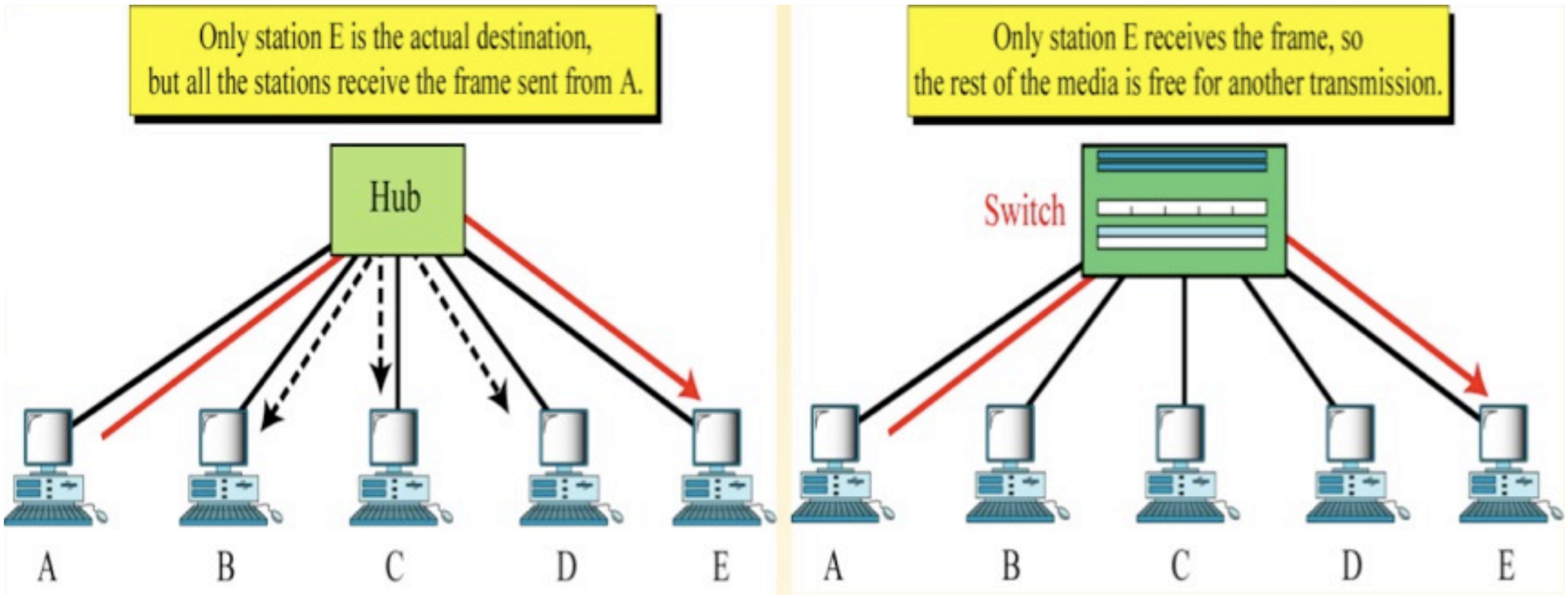
- What can the attacker do?
- Where is the attacker located?
- What are you trying to protect?

Different Layers

- Each layer has it’s own vulnerabilities
- Link layer example: ARP-spoofing
- Network layer example: IP address forgery
- TCP example: Sequence number guessing attack
- Application example: email-borne worms

Security of Ethernet Architecture

- Originally Hub/shared bus model. Currently mostly switched.
- Advantages of switched: Latency, Bandwidth, Security.



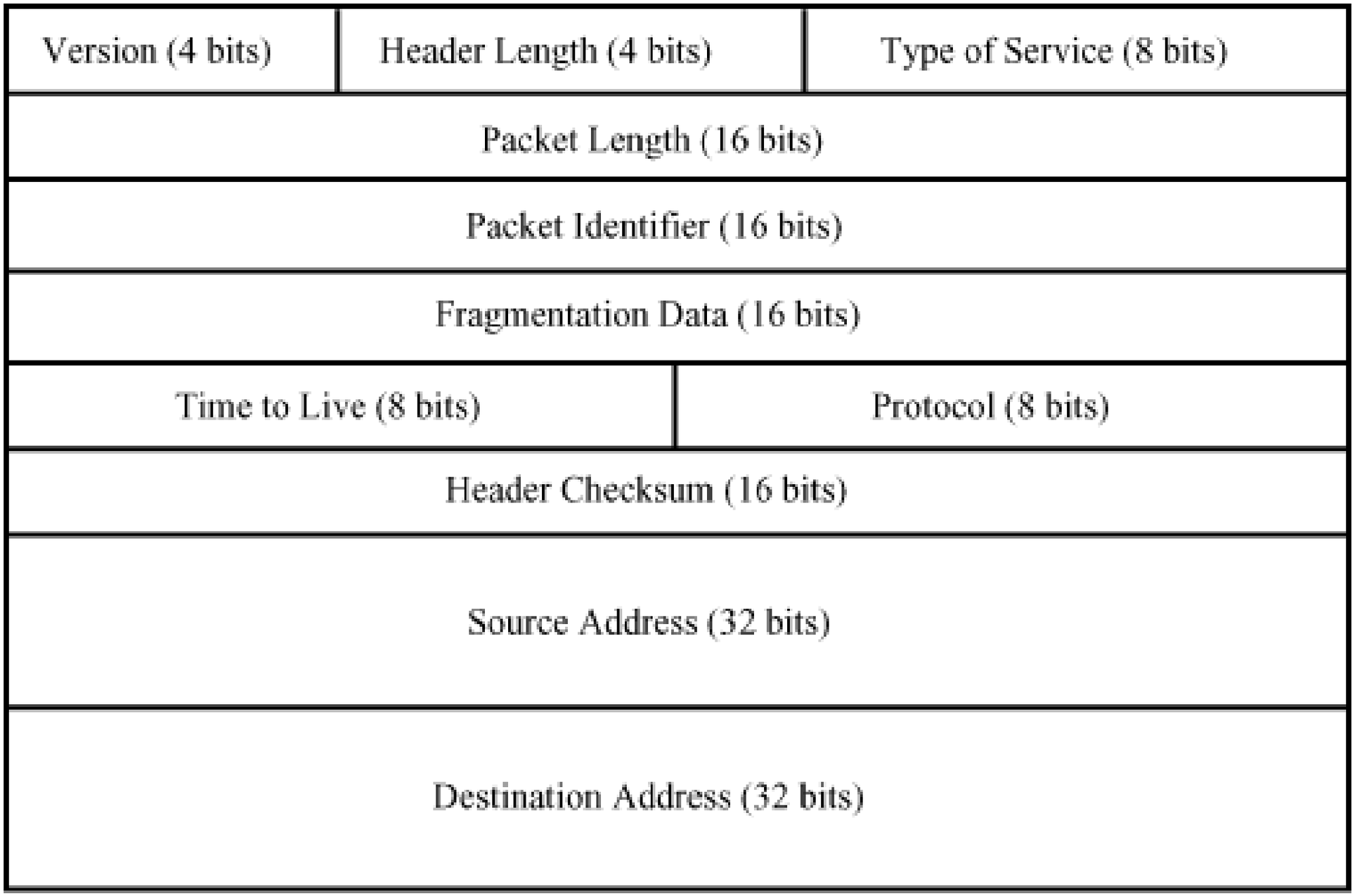
Switched Security

- Switched network prevents non-recipients from seeing Ethernet frames by filtering them at the switch. This prevents some type of network sniffing.
- Does it prevent all sniffing?
- NO
  - Switch admins can activate port-mirroring or monitoring.
  - Switch can be forced to become a hub.
  - Switch can be fooled to thinks additional MAC address are behind a specific port.
  - Broadcast and multicast traffic is still available.
  - ARP spoofing can cause source to send traffic to attacker's machine.
    - ARP is used to map from IP address to Ethernet MAC address.
  - Cable can be physically tapped.

ARP Spoofing

- ARP is used to map IP address into Ethernet addresses:
    - arp who-has ce.sharif.edu tell me.ce.sharif.edu
    - arp reply ce.sharif.edu is-at fe:50:12:fa:bc:11
- Another machine can reply; first reply generally wins

IP Header



http://www.softlookup.com/tutorial/vc++/39vcu02.gif

IP Fragmentation

- Flags:
  - DontFragment, LastFragment
- Fields:
  - Identification: 16 bit identifier of each fragment
- Security Risks of fragmentation:
  - Hides information
    - fragmented packets hard to analyze unless reconstructed
  - Denial of Service
    - reconstructing fragmented packets can take a lot of memory and cpu, specially if OS implements poorly
    - Ping of Death

Ping of death

- A ping is normally 64 bytes in size (or 84 bytes when IP header is considered)
- Many computer systems cannot handle a ping larger than the maximum IP packet size, which is 65,535 bytes.
- MTU is usually 1500 bytes, so how do you send a 65,536 byte ping?
  - Use IP fragments
  - Buffer overflow occurs when the target computer reassembles the packet
    - often causes a system crash.

Smurf Attacks (ICMP Ping)

- Smurf attacks (ICMP Ping)
  - The attacker sends ICMP ping packets with spoofed source addresses to the broadcast address of a subnet.
  - Every machine in the subnet sends a ICMP response packet to the “target” source machine.
  - If sufficient pings are sent by the attacker to a number of broadcast networks, the target gets flooded with ping response packets.
  - Magnification occurs because for each attack packet, N damage packets are sent to target.
  - Occurs because the ping source address is trusted and “broadcast” pings are routed.
  - Gradually being fixed by changing the RFC’s to prohibit routing “broadcast” pings. They can now only be used locally.

Normal TCP 3-Way Handshake

- A client C tries to contact a server S :

  C → S : SYN (ISNc)

  S → C : SYN (ISNs), ACK (ISNc)

  C → S : ACK (ISNs)

  C → S : data

- In older TCPs, the ISN (Initial Sequence Number) is incremented by a constant amount k after each connection and every half-second.

Sequence Number Guessing Attack

- X opens a legitimate connection to S to learn ISNs
- X → S : SYN (ISNx)
- S → X : SYN (ISNs), ACK (ISNx)

- X impersonates T :

- X → S : SYN (ISNx), SRC = T
- S → T : SYN (ISNs + k), ACK (ISNx)
- X → S : ACK (ISNs + k), SRC = T
- X → S : ACK (ISNs + k), SRC = T , nasty-data

Sequence Number Guessing Attack

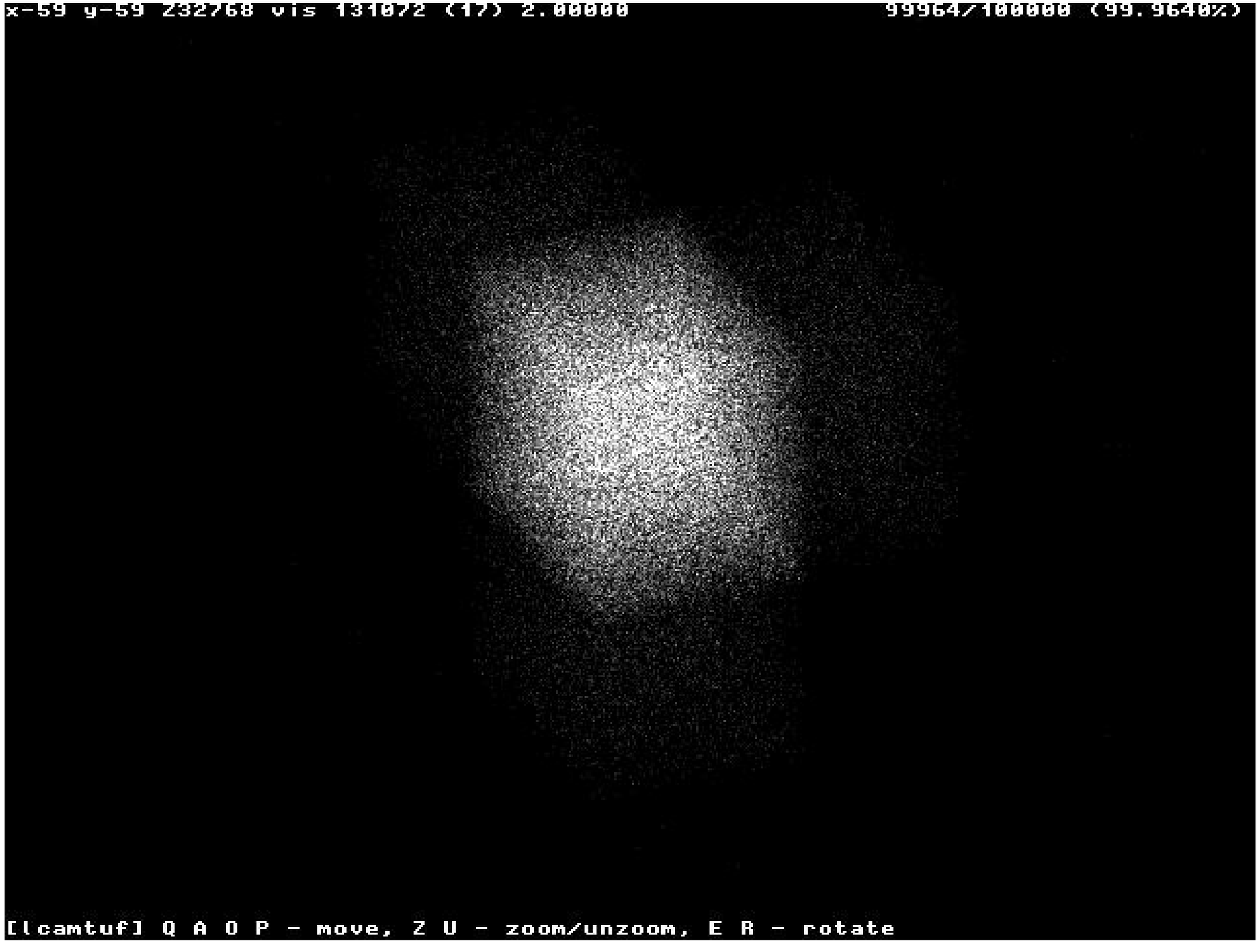
- When T sees the SYN/ACK packet from S , it will try to respond with a RST
- X has to prevent this
- Could impersonate a dead host or use a denial of service attack to block T
- New research result: built-in firewall software prevents hosts from seeing packets for connections they didn’t initiate; T will never see that packet, and hence will never send the RST. . .

ISN Patterns

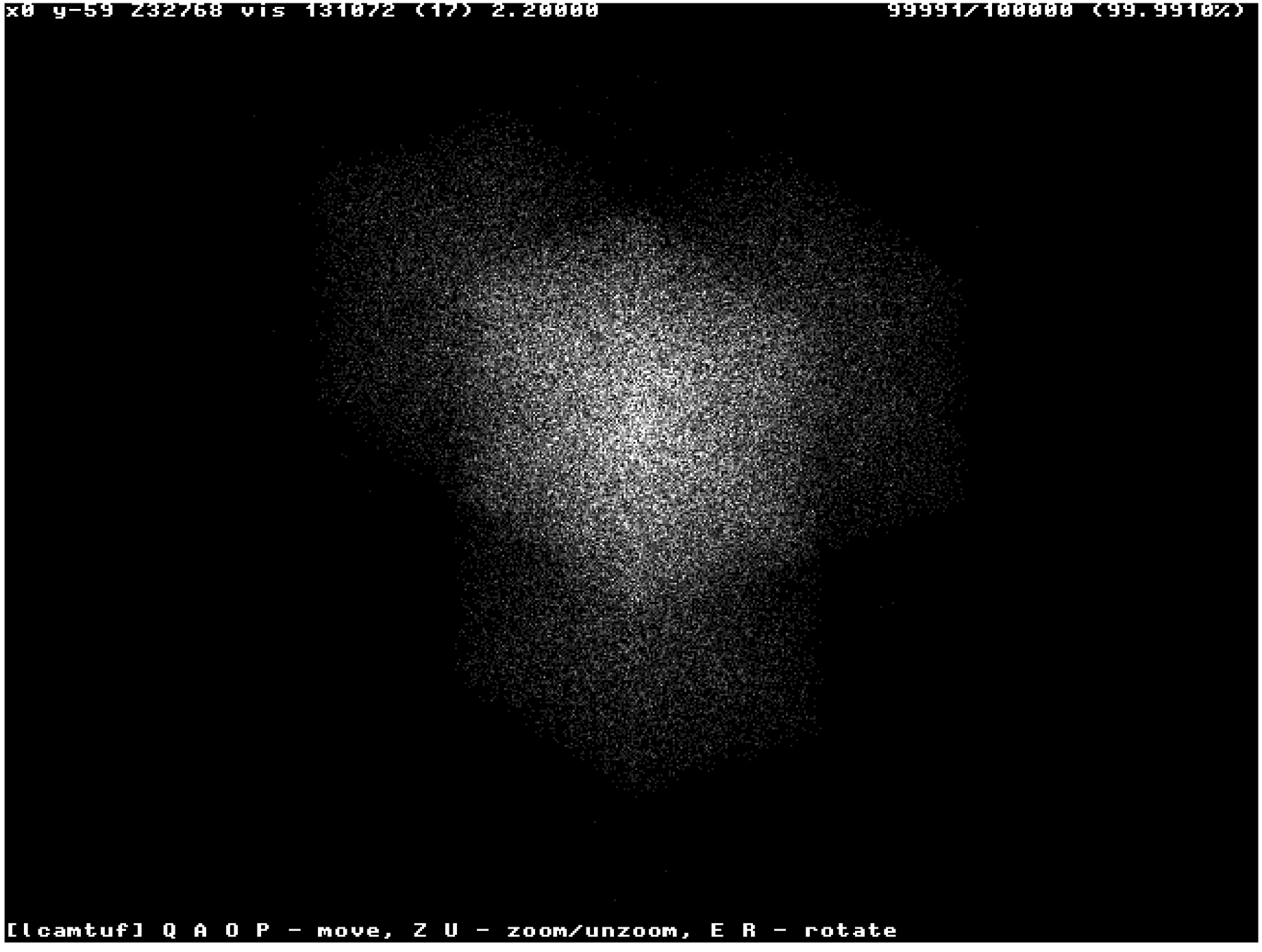
- Are there any patterns to these ISNs?
- A study by Michal Zalewski gathered and graphed the ISN sequences for a variety of OS's.
- 100,000 ISN's were graphed for each OS

ISN Patterns for Windows 95

ISN Patterns for Windows 2000



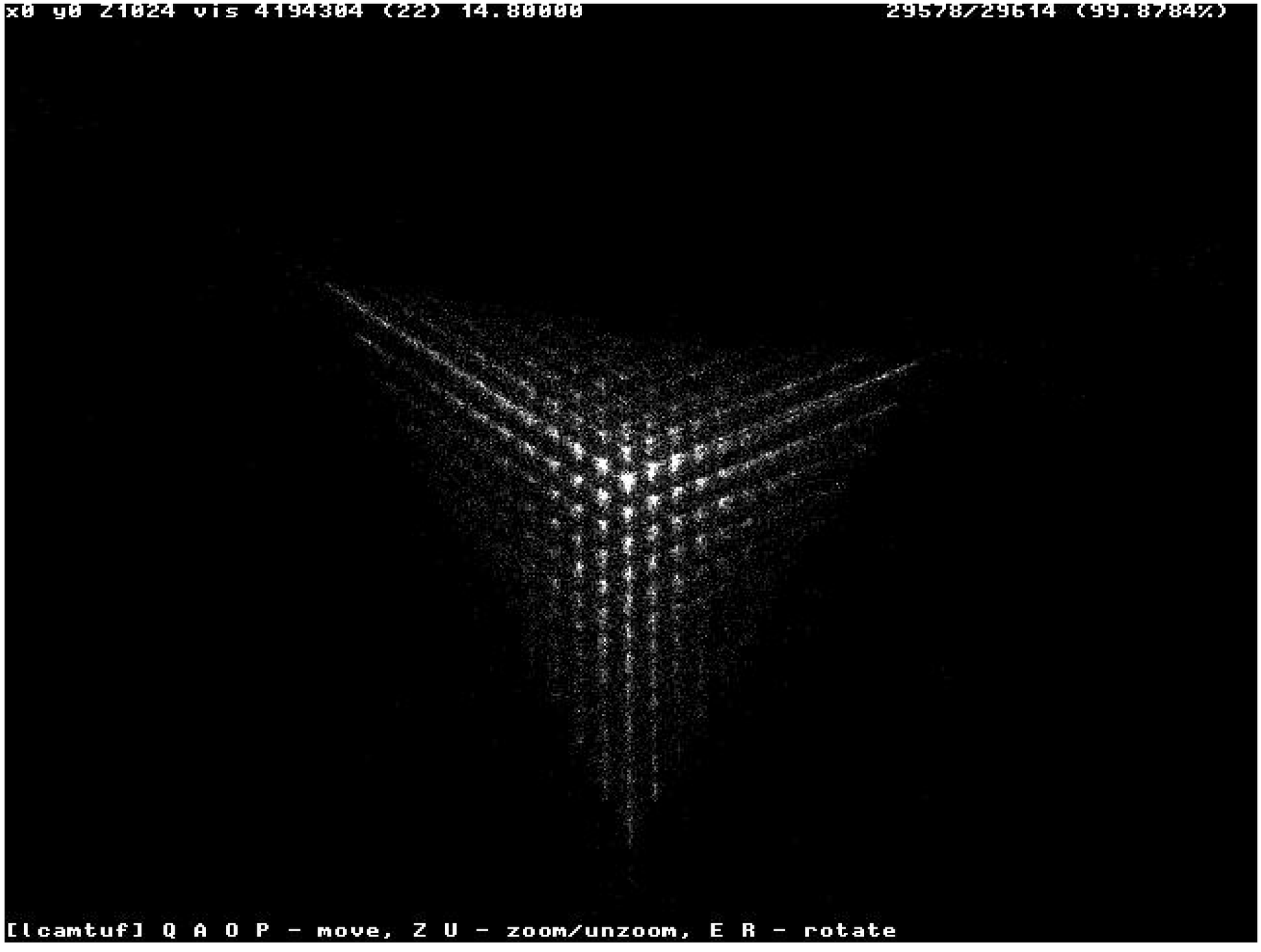
ISN Patterns for Windows XP



IOS Patterns for Mac OS 9

IOS Patterns for Mac OS X

ISN Patterns for Cisco IOS 12.0 (unpatched)



ISN Patterns for Cisco IOS 12.0 (patched)

ISN Patterns for IOS 12.2.10a

ISN Patterns

- Each OS uses a different algorithm for generating ISN's. So if we can detect the algorithm we can detect the OS.

Acknowledgments/References

- [Bellovin 06] COMS W4180 — Network Security Class Columbia University, Steven Bellovin, 2006.
- [Stanton 08] Network Security, CS 192/286, George Washington University, Jonathan Stanton, 2008.
- [Zalewski1] Strange Attractors and TCP/IP Sequence Number Analysis, Michal Zalewski, http://lcamtuf.coredump.cx/oldtcp/tcpseq.html
- [Zalewski2] Strange Attractors and TCP/IP Sequence Number Analysis - One Year Later , Michal Zalewski , http://lcamtuf.coredump.cx/newtcp/