How Secure is *Secure?*

Conducting *Threat-Oriented* Product Security Evaluations

Matthew Franz

Security Technologies Assessment Team

Cisco Systems

Agenda

- Introduction
- A Threat Model
- A Testing Methodology
- Sample product eval
  - SOHO Firewall/Router
- Sample protocol eval
  - IPSec

Mandatory Bio Slide

- Entered security field in ’97 after 4 years of “public service”
- Developed/taught network security courses for Govt. IW customers in San Antonio, TX
- Started working on Trinux in Spring ’98
- Brief stint as a security consultant for SBC
- Joined Cisco in May 2000 as Security Research Engineer in Security Technology Assessment Team (Austin, TX)

Mandatory Marketing Slide

Security Technologies Assessment Team (STAT)

- **Small group of Research Engineers that was originally part of WheelGroup and did NetRanger/NetSonar signature development and general purpose security/vulnerability research**
- **Currently part of Cisco Security Consulting (VPN and Security Services BU)**
- **VPN/Firewall Products, AVVID, Wireless, and misc. internal/consulting security consulting**

The Wrong Expectations

You're in the <u>wrong</u> room if:

- **You wanted to find out how to break [into] Cisco products**
- **You wanted to hear a *We're-So-Secure* sales pitch about Cisco products**
- **You wanted specific exploits against specific platforms**
- **You wanted to land a hot security job at Cisco and move to Austin**

The Right Expectations

You're in the right room if you want to learn:

- **A structured approach to conducting vulnerability testing on network gear**
- **About tools and techniques for finding stupid programmer tricks (and other security holes)**
- **Some theoretical attacks against IPSEC**

Conducting *Threat-Oriented* Security Evaluations

A Security Model

Cisco Systems

Why are we here?

When it comes to products:

- **Security is generally an afterthought**
- **Dev testing only validates desired behavior**
- **You cannot possibly check for everything**
- **The customer is always right**
- **To err is human…**
- **We learn from history…**

A matter of perspective…

White Hat

- **Finite amount of time for testing**
- **Infinite number of products and features to test**
- **You must sacrifice either coverage or depth**
- **You cannot prove it is secure**
- **Someone *will* make a BUGTRAQ post on a product you tested**

Black Hat **

- **All the time in the world**
- **None of the rules, none of the responsibility**

More Perspective: Why *this* stuff?

- **Avoid re-inventing the wheel every new project/protocol/product**
- **I'm not as smart as I'd like to be**
- **Apply old vulnerabilities to new protocols**
- **Ensure coverage**
- **Better knowledge capture/transfer**
- **Deal with management and junior engineers**
- **It at least gives me the *appearance* of knowing what I'm talking about to most customers**

CC Evaluation Framework

- **Common Criteria Home**
  - http://csrc.nist.gov/cc/
- **Functional Requirements**
  - **Design and documentation**
  - **Security Objectives**
  - **Development & Testing Procedures**
- **Assurance Requirements**
  - **Vulnerability Analysis**
  - **Penetration Testing**
  - **and much more…**

What is *threat-oriented* evaluation?

- Primarily black/gray-box testing
- Feature validation is not the major concern
- Focus is primarily on implementation errors
- Occurs [too] late in the development cycle
- Anticipate “all possible attacks,” but only conduct a few based on the level of risk
- Includes a well-defined defined threat-model and notion of security (vs. a security wish-list)
- Enter the mind of the attacker

The Real Questions

- **What aspect of security is under evaluation?**
- **What is the level of risk for a given threat?**
  - **locality**
  - **sophistication**
  - **target**
  - **outcome**
  - **technique**
  - **impact/criticality**

What is Security? (CIA^{4}N)

- **Confidentiality**
- **Integrity**
- **Authenticity**
- **Authorization**
- **Availability**
- **Accounting**
- **Non-Repudiation**

From Threats to Vulnerabilities

- **Vulnerability – weakness in a system**
- **Threat – endangers a component of security**
- **Risk – the likelihood that a threat will exploit a vulnerability**
- **By *exposing products to a range of known threats and new attacks, we can:***
  - **Discover new vulnerabilities**
  - **Provide assurance that known threats will/will not affect a product and encourage fixes**
- **We <u>cannot</u> prove a product is secure**

Threat Locality

- Source of attack (vs. perimeter)
  - Internal
  - External
- Proximity to target
  - Local
  - Remote

Threat Locality (cont.)

- **Proximity to traffic**
  - **Blind**
  - **Non-Blind**
- **Network Layer under attack**
  - **Lower layer compromises expose upper layers**
  - **And sometimes vice versa**
  - **Some protocols/layers are inherently more/less secure**
- **Related to threat sophistication**

Threat Sophistication

- **Factors to consider**
  - **Availability of tools**
  - **History of attacks against product/protocol**
  - **Complexity of protocol/product**
  - **Potential rewards/impact of compromise**
  - **Resources required (time, expertise, equipment)**
  - **Window of opportunity**
- **Risk should determine scope, sequence, and depth of security evaluation tasks**

Threat Target(s)

- **Device itself**
  - **Firewall, VPN, IP Phone, Wireless AP, etc.**
- **User**
  - **Internal/external clients, protected servers**
- **Infrastructure**
  - **The Network**
  - **Supporting/Related Devices**

Threat Outcomes (technical)

- **It's all about:**
  - **Reading**
  - **Writing**
  - **Altering**
  - **Destroying**
  - **Degrading**

Threat Techniques

- Sniffing
- Spoofing
- Flooding
- Malformed data
- Out of sequence data
- Hijacking
- Replay

Threat Impact (Criticality)

- How bad?
  - Whole box (lockup, reboot, slow down)
  - Single component (kill, maim)
- How fast?
  - A single malformed packet
  - Thousands/Millions of packets
- How easy/hard?
  - Three Letter Agencies
  - 2yr/13yr/90yr old

Threat Impact (Criticality)

- **Who is affected?**
  - **Administrator**
  - **Users (internal, external, the CEO)**
  - **The Whole Internet**
- **What can be done about it?**
  - **Will a reboot/restart solve it?**
  - **Is there a work-around?**
  - **How hard/long to fix?**
  - **Is it a configuration error?**
  - **Are there existing countermeasures?**

What makes it so hard?

- **Multi-dimensional problem-- *how do you visualize it?***
- **New threats and vulnerabilities emerge every day-- *how do you integrate them into the model?***
- **How do you make it concrete enough to do something about it?**
- **Avoid paper the paper chase**

Conducting *Threat-Oriented* Security Evaluations

A Testing Methodology

Cisco Systems

Evaluation Sequence

- Conduct initial research & analysis
- Setup & configure the product
- Determine a products TCP/IP Signature
- Conduct continuous follow-on R&D
- Evaluate a product's implementation of infrastructure protocols
- Evaluate application layer protocols used by the product
- Evaluate features that don't fit with in a specific protocol

Initial Research & Analysis

- **Identify core features/functionality**
- **Research product marketing, configuration documentation, white papers, testing info (plans, test cases, etc.)**
- **Map features/protocols against security model and threat matrix**
- **Prioritize subordinate evaluation tasks based on your threat model**

Setup & Configuration

- Deploy product in a realistic environment
- Record and analyze normal system activity
  - system logs
  - sniffer traces
- Identify potential security-relevant misconfiguration errors
- Identify currently available tools for conducting protocol analysis & attacks

Determine TCP/IP Signature

- Passive/Active OS Detection
- Initial Sequence Number Generation
- Protocol Scans
  - IP Protocols (TCP, UDP, AH, ESP)
  - TCP/UDP Scans (all known types)
- Application Fingerprints
  - Login banners
  - Escape/special characters

Passive/Active OS Detection

- **TCP/IP Indicators**
  - **Window Size**
  - **TTL**
  - **IP Identification**
  - **TCP Timestamp**
  - **ICMP (see Ofir Arkin's whitepaper)**
  - **Anything else that is weird**
- **Tools**
  - **Hping, p0f, nmap, sing, etc.**

Follow-On R&D

- **Should start (and continue) in parallel as soon as you know what you are looking at/for**
- **Research all protocols/features at all layers**
  - **general research – how does it work?**
  - **vulnerability research – has it been exploited?**
  - **vulnerabilities in comparable products**
  - **analysis tools (sniffers, info gathering)**
  - **attack tools (packet building, etc.)**
  - **Open Source implementations of new protocols**

Follow-On R&D

- **Document absence of vulnerabilities or lack of interest in the hacker community**
- **Identify and develop analysis and attack tools when none are available (ISAKMP, H323, VoIP QoS, etc.)**
  - **examine Open Source implementations of relevant protocols for code reuse (to develop analysis/attack tools)**
  - **examine existing tools for easy modification**
  - **use cut-n-paste packet generation for initial testing or when performance is not an issue**
  - **build packet generation tools in Libnet and/or NASL**

Cut-n-Paste Packet Generation

- Analyze protocol with ethereal & tcpdump
- Extract relevant hex strings using iplayer (or sniffer of choice)
- Build packet generation scripts:
  - NASL
  - Sendip
  - Net::RawIP, Raw Sockets, Python, etc.
- Create stimulus/response tools

Infrastructure Protocol Attacks

- **Primarily layers 2-4**
  - **TCP, UDP, ICMP, etc.**
- **Examples**
  - **IP Fragmentation**
  - **Spoof everything from everywhere**
  - **Stateful Protocols**

    Flood at all possible states

    Send packets in all possible sequences

Infrastructure Protocol Attacks

- **More examples**
  - **Malformed Packet Permutations**

    Headers, Payload, Truncated, TLV Mismatch

  - **Loop through every possible value for all possible fields**
- **Just because its an old attack, doesn't mean the product is immune**
- **There may be collateral damage**
- **ISIC is your friend**
- **So is PacketStorm**

Learning from Naptha

- **Resource starvation attacks can be conducted against any/all states**
- **Network devices typically only worry about the initial state (SYN Flooding) but don't check for follow-on states (ESTABLISHED, LAST_ATCK)**
- **Naptha TCP Tools**
  - **synsend – generic SYN Flooder**
  - **srvr – injects spoofed TCP responses (SA, FA)**
- **See PacketStorm and http://razor.bindview.com**

Feature/Protocol Attacks

- Apply threat model and map security components against protocol functionality
- Identify weaknesses in supporting protocols (TCP/UDP) that could lead to compromise
- Identify existing tools to analyze/attack the protocol
- Identify new tools that need to be developed
- Test relevant historical vulnerabilities
- Develop new attacks based on gaps in above

Conducting *Threat-Oriented* Security Evaluations

Sample Product Evaluation

Broadband Firewall

Cisco Systems

Sample Product Evaluation

- Device
  - Broadband Router/Firewall
  - Integrated 10/100 Switch
- Deployment Environment
  - Home Cable/DSL
- Cost
  - Less than $300

Initial Research & Analysis

- Layer 2 Protocols
  - 10/100 Ethernet Switching
  - PPPoE, ARP
- Layer 4 Protocols
  - TCP, UDP, ICMP, IGMP (?)
- Address Management
  - DHCP Client
  - DHCP Server
- Routing
  - RIP, RIP-2
  - Port Forwarding & NAT

Initial R&A (cont.)

- Packet Filtering
  - “protocol” -- IP proto, src, dst, established
  - “generic” – bitmask
  - Filter Sets & Rules
- Management
  - HTTP
  - Telnet
  - Console
- Misc
  - DNS Proxy

Security/Feature Matrix

- **Confidentiality**
  - **Remote Passive/Active OS Detection**
- **Authenticity**
  - **Cleartext Telnet/FTP Login**
  - **HTTP Authentication**
  - **DNS Spoofing**
- **Authorization**
  - **Traffic Filtering**
  - **Routing Protocol attacks**

Security Feature Matrix

- **Availability**
  - **Flooding/Malformed/Out of Sequence attacks to and through the device at all layers**
- **Accounting**
  - **Are attacks logged?**
  - **How effective is deception?**

Setup & Configuration

- It works out of the box
- Default configuration
  - User: admin Password: 1234
  - DHCP Client/Server Enabled
  - Port forwarding disabled
  - Default IP: 192.168.0.1 (LAN)

Protocol Scans

- Nmap IPPROTO
  - no info
- UDP Scan
  - no info
- TCP Scans (external)
  - SYN – Filtered
  - FIN – Open
  - etc.

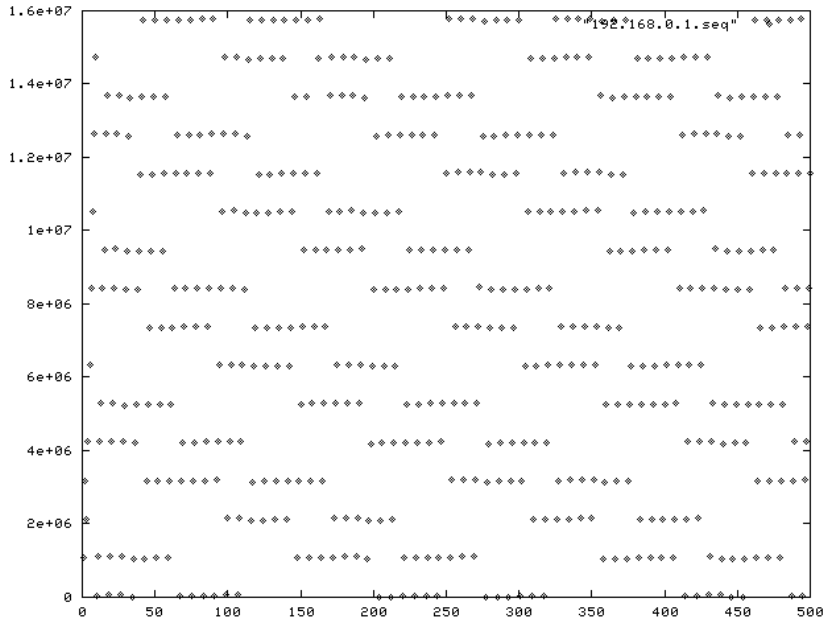
Broadband FW TCP/IP Signature

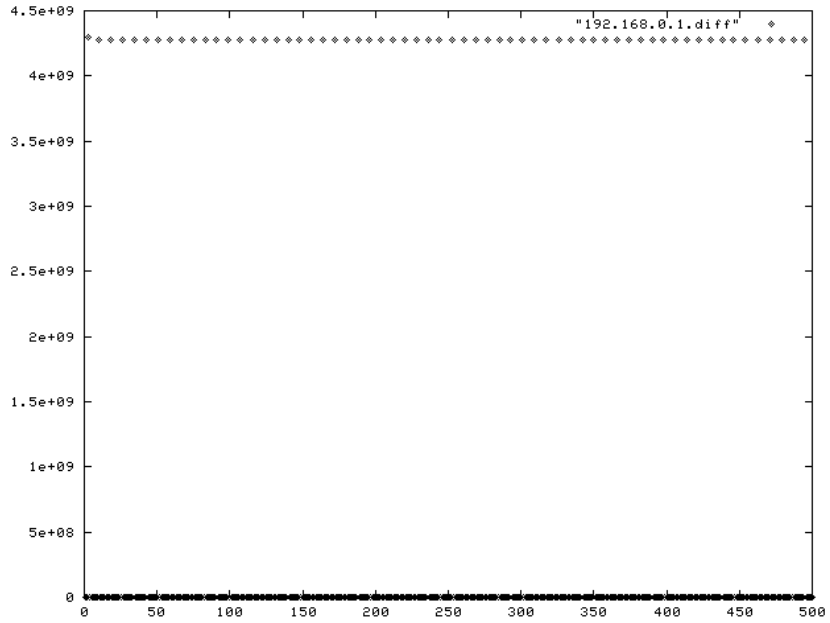
- **Uses entire 16-bit port range for source ports including privileged ports**
- **Only a single connection allowed per port**
- **Sends RST on port 21 during Nmap OS probes**

TCP/IP Signature

- **HTTP Server**
  - **ZyXEL-RomPager/3.02 (AllegroSoft)**
- **Telnet Negotiation Options**
  - **telnetfp- http://teso.scene.at/releases.php**

Broadband FW: ISN Plots

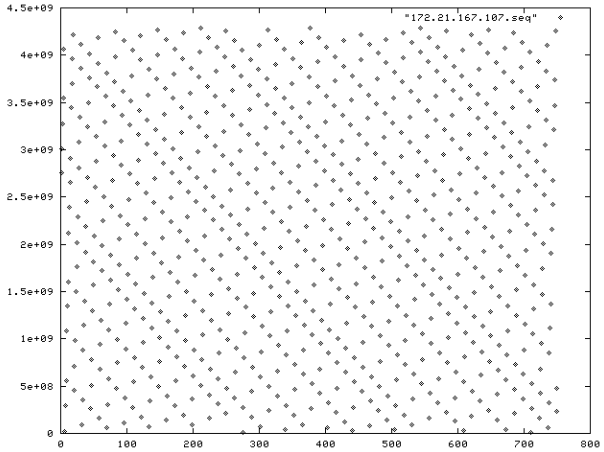


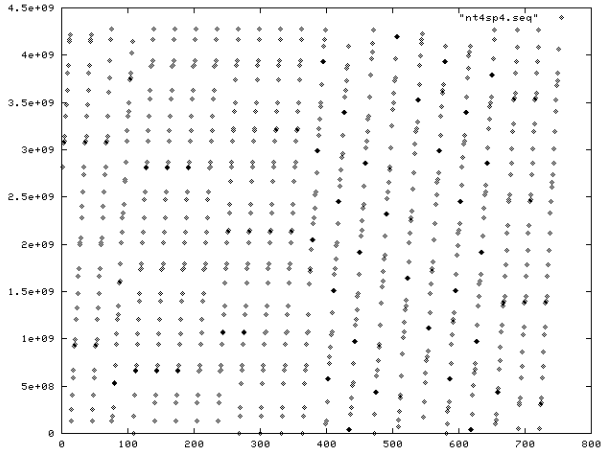


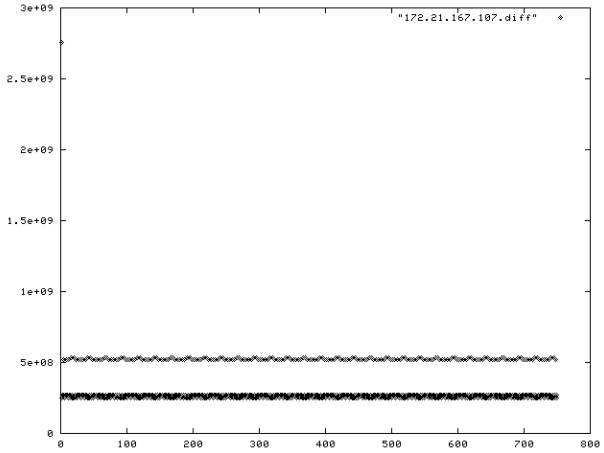
Raw ISN Plot

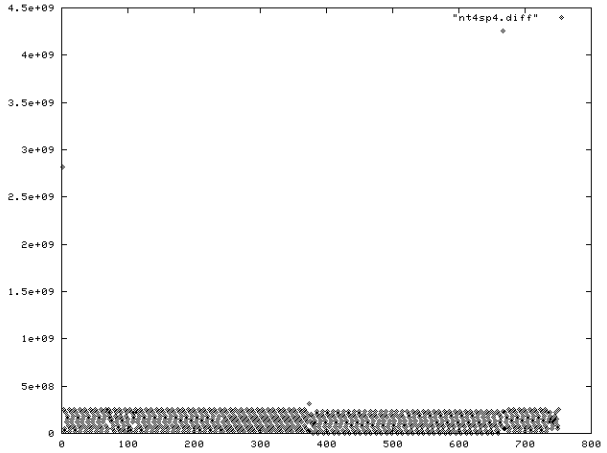
$ISN^{n+1} - ISN^{n}$

Fun Windows ISN Plots

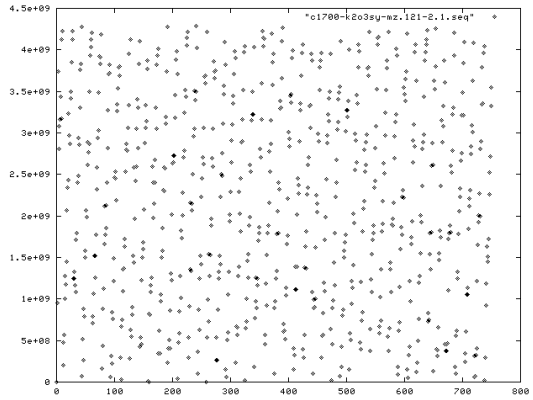


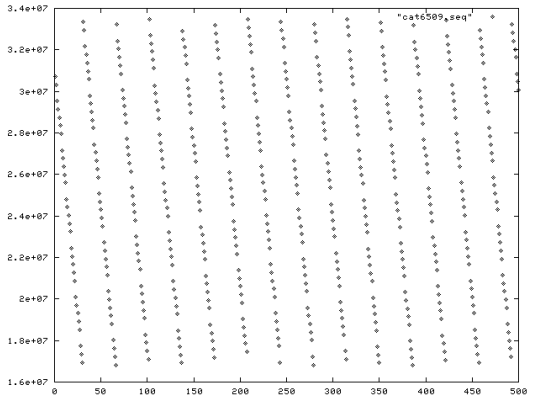


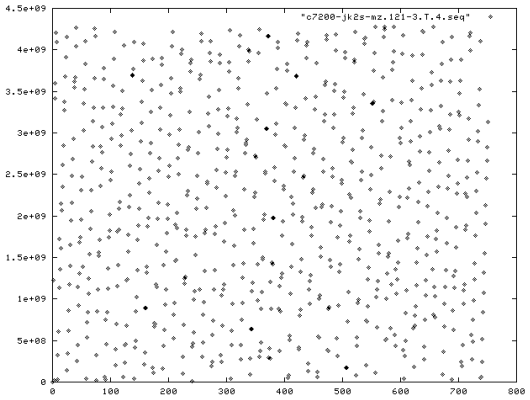


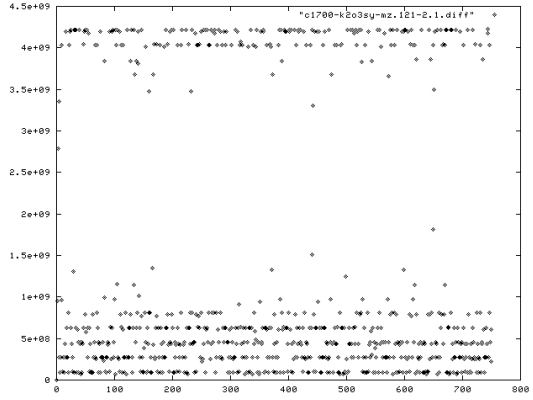


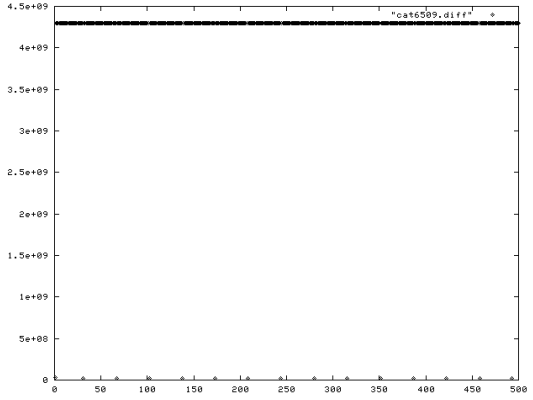
Fun Cisco ISN Plots

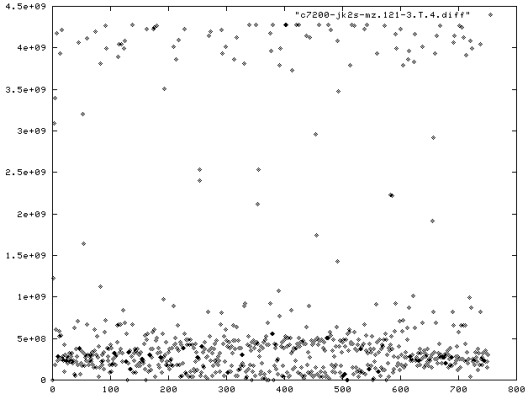




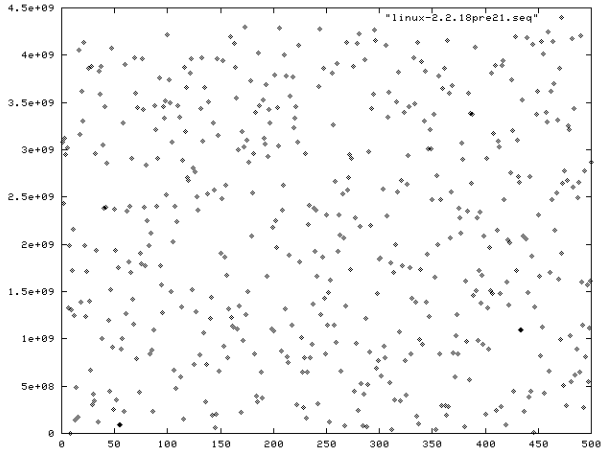


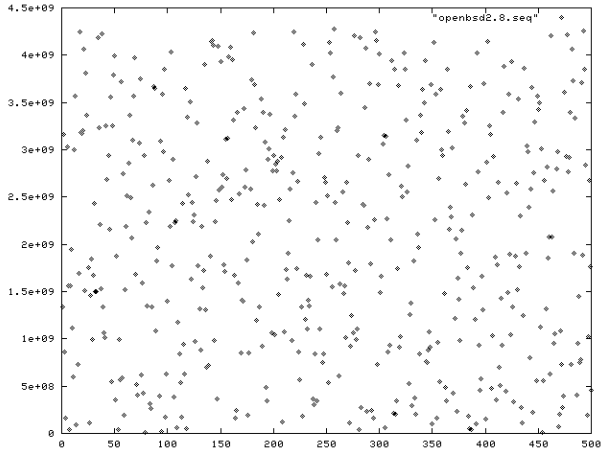


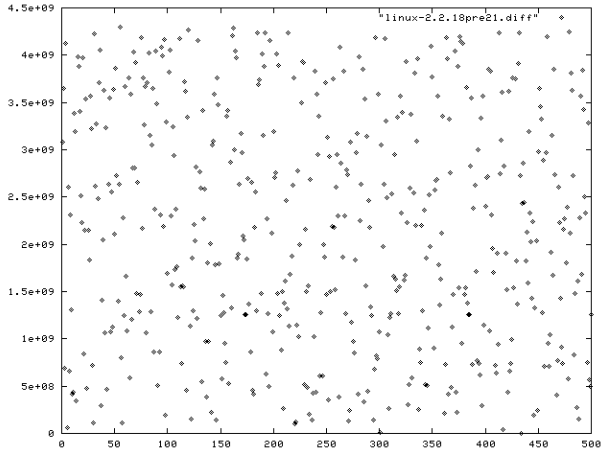


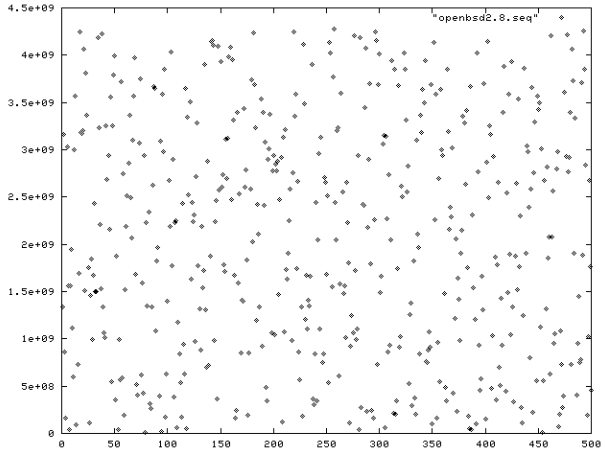


Linux & OpenBSD ISN Plots









Follow-on R&D

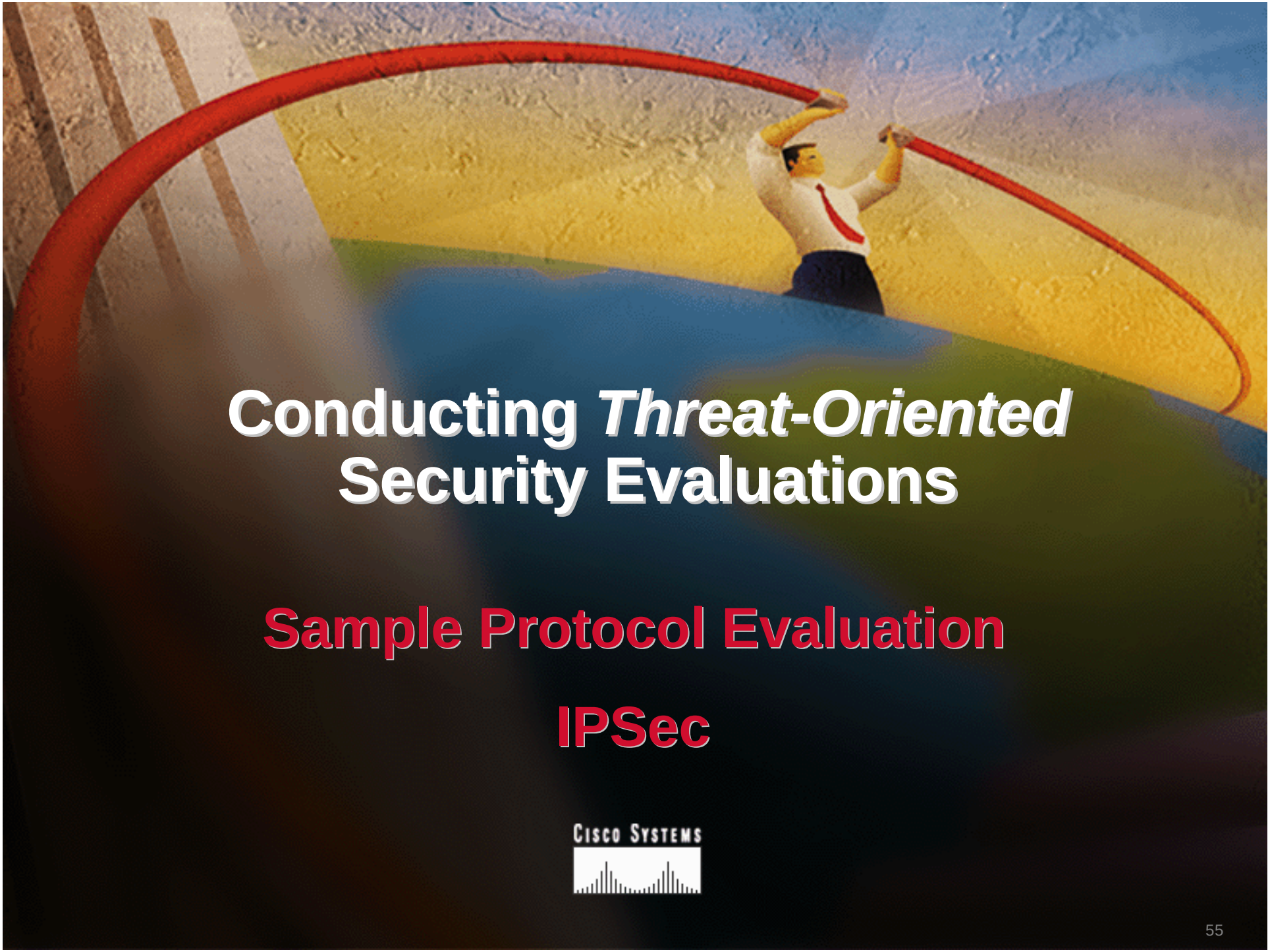
- **Research Topics**
  - **Other ZyXEL Products**
  - **Allegrosoft RomPager Embedded Toolkit**

Infrastructure Attacks (just a few)

- Malformed TCP/UDP/ICMP/IGMP
- Fragmentation Attacks
- Bad TCP/IP options
- Sequence Number Attacks
- One of ISIC tools will break it (I promise)

Protocol/Feature Eval Tasks

- DHCP (client/server)
- HTTP
- Packet Filter Penetration
- PPPoE (?)
- RIP/RIP-2
- DNS Proxy



Conducting *Threat-Oriented* Security Evaluations

Sample Protocol Evaluation

IPSec

Cisco Systems

Proto Evaluation: IPSEC

- Overview
- Threat model
- Client issues
- Gateway issues
- Some theoretical attacks

IPSEC Overview

- IKE (UDP port 500)
  - Key Exchange
  - Manages Security Associations
- AH/ESP (IP Protocol 50,51)
  - Data integrity
  - Data confidentiality
  - Data origin authentication

Security/Functionality Matrix

- **Confidentiality**
  - **DES/3DES, Diffie-Helman KE, Entropy of Cleartext Values (cookies, msgid's, etc.)**
- **Integrity**
  - **MD5/SHA**
- **Authenticity**
  - **Keyed MD5/SHA, Cookies, Perfect Forward Secrecy**
- **Authorization**
  - **Cookies, PSK, X.509, Group Name, CA**

Security/Functionality Matrix

- **Availability**
  - **Key Exchange is the weak link (we attack IKE)**
- **Accounting**
  - **Are attacks logged?**

Overview of IKE

- **Purpose**
  - **Establish secure channel for exchanging key material**
- **Phase 1 (Main Mode)**
  - **Establishes “master secret” used for deriving all future key material**
- **Phase 2 (Quick Mode)**
  - **Negotiate (and renegotiate) Security Associations for protecting user data**
  - **Protected (Encrypted/Authenticated) by SA established in Phase 1**

IKE Phase 1 & 2

```
 1  0.000000 192.168.1.250 -> 192.168.1.235 ISAKMP Identity Protection (Main Mode)
 2  0.174295 192.168.1.235 -> 192.168.1.250 ISAKMP Identity Protection (Main Mode)
 3  0.219402 192.168.1.250 -> 192.168.1.235 ISAKMP Identity Protection (Main Mode)
 4  0.858957 192.168.1.235 -> 192.168.1.250 ISAKMP Identity Protection (Main Mode)
 5  0.958503 192.168.1.250 -> 192.168.1.235 ISAKMP Identity Protection (Main Mode)
 6  1.186073 192.168.1.235 -> 192.168.1.250 ISAKMP Identity Protection (Main Mode)
 7  1.196803 192.168.1.250 -> 192.168.1.235 ISAKMP Quick Mode
 8  1.627906 192.168.1.235 -> 192.168.1.250 ISAKMP Quick Mode
 9  1.690614 192.168.1.250 -> 192.168.1.235 ISAKMP Quick Mode
10  1.996207 192.168.1.250 -> 192.168.1.235 ESP ESP (SPI=0x9b9b5735)
11  2.996010 192.168.1.250 -> 192.168.1.235 ESP ESP (SPI=0x9b9b5735)
12  3.996101 192.168.1.250 -> 192.168.1.235 ESP ESP (SPI=0x9b9b5735)
13  4.233021 192.168.1.235 -> 192.168.1.250 ESP ESP (SPI=0x20a21f90)
```

ISAKMP Message Format

- **Header**
  - **Initiator & Responder Cookie**
  - **Next Payload**
  - **Version**
  - **Exchange Type**
  - **Flags**
- **Payloads**
  - ***n* x TLV's**

ISAKMP Header

```
User Datagram Protocol
    Source port: 500 (500)
    Destination port: 500 (500)
    Length: 184
    Checksum: 0x03d4
Internet Security Association and Key Management Protocol
    Initiator cookie
    Responder cookie
    Next payload: Security Association (1)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
    Flags
        .... ...0 = No encryption
        .... ..0. = No commit
        .... .0.. = No authentication
    Message ID
    Length: 176
```

IKE Phase 1 (Main Mode)

1. Send proposals (auth/encr key, DH group)
2. Respond with a single proposal accepted
3. Send nonce, DH public value (g^x)
4. Send nonce, DH public value (g^y)
5. Authenticate using PSK/Digital Cert
6. Authenticate using PSK/Digital Cert

IKE Threat Model

- **UDP Vulnerabilities**
  - **Spoofing/packet injection is easy**
  - **Connectionless**
  - **No sequence numbers**
- **Main Mode (Phase 1)**
  - **Remote Attacks -- msg 1 (SA Payload)**
  - **Non-Blind Attacks – msg 2-4 (until Ph 2)**

IKE VPN Client Issues

- Usually Microsoft based
  - UDP Scans are accurate
  - IP Protocol Scans are accurate
- How is IKE implemented?
  - Application
  - Service
- Usually impacted by malformed/flooded ISAKMP, GRE, AH, etc. packets
- You should limit access to protocols/ports via a host-based firewall
- Split Tunneling???

IKE VPN Gateway Issues

- **Remote Access VPNs**
  - **Must accept ISAKMP proposals from everyone**
  - **Aggressive Mode is more resistant to DoS because shared secret is required**
- **LAN to LAN VPNs**
  - **Limit ISAKMP proposals to valid security gateways and limited number**

Malformed ISAKMP

- **UDP Payload**
  - **udpsic –s rand,500 –d victim,500**
- **ISAKMP Payload**
  - **paste in ISAKMP Headers**
  - **TLV Mismatches**

IKE Proposal Flooding
(Remember Naptha)

- **Requirements**
  - **Valid / Invalid IKE Proposal (Main Mode)**
  - **Valid group name (Aggressive Mode)**
- **Window**
  - **Depends on ACLs for LAN to LAN VPNs**
  - **Unlimited for remote access VPNs**

IKE Termination

- **Requirements**
  - **Know (or guess) the initiator cookie and generate a spoofed MSG 2 back to the Initiator with a bogus cookie**
  - **When the real MSG 2 arrives, it will be dropped because the cookie does not match**
- **Optional**
  - **Know which proposals sent by the initiator and send a proposal that was not in that list**

Malformed AH/ESP

- **Requirements**
  - **Generate zero-length or other invalid AH/ESP Datagram**
- **Window**
  - **Unlimited until fixed**
- **Tools**
  - **Nmap IPPROTO Scans**
  - **Sendip**
  - **ISIC (isic)**

IKE Attack Tools

- Linux FreeS/WAN
- Libnet (modified to generate ISAKMP)
- Ethereal/Tcpdump/iplayer
- NASL
- Sendip or other UDP packet generator
- Tcpkill (modified to inject ISAKMP msgs)

Tools

- **Trinux**
  - **http://www.trinux.org or http://trinux.sourceforge.net**
- **Isic**
  - **http://www.packetfactory.net/Projects/ISIC/**
  - **See Trinux isic package for modifications**
- **Ethereal**
  - **Use tcpdump to capture, ethereal/tethereal toanalyze**
  - **http://ethereal.zing.org**
- **NASL**
  - **Attack engine for Nessus**
  - **http://www.nessus.org**

Tools (cont.)

- **Sendip**
  - http://www.earth.li/projectpurple/progs/sendip.html
- **Hping2**
  - http://www.kyuzz.org/antirez/hping.html

Good Reading

Using IPSec to Construct Secure Virtual Private Networks

http://www-4.ibm.com/software/network/library/whitepapers/vpn/

Phrack 56-6 (Project Area52 – "Delirium Tremens")

http://www.phrack.com/search.phtml?view&article=p56-6

Computer Vulnerabilities by Eric Knight

http://securityfocus.com/data/library/compvuln_draft.pdf

ICMP Usage in Scanning by Ofir Arkin

http://www.sys-security.com/html/papers.html

Contact Info

Personal Email

mdfranz@io.com

Work Email

mfranz@cisco.com

Web Sites

http://www.trinux.org

http://trinux.sourceforge.net