Chapter 51
TCP/IP

- **Problems Packed into Packets.**

"I predict the U.S. government won't use or accept IPv4 packets after 2017."

-- Alex Lightman

Copyright Information

- Some rights reserved / Einige Rechte vorbehalten
- Michael Kafka, René Pfeiffer, Sebastian Meier
  C.a.T. Consulting and Trainings, Vienna, Austria
- You may freely use, distribute and modify this work under following agreement:
- Diese Arbeit darf frei genutzt, verbreitet und bearbeitet werden unter folgenden Bedingungen:

Authors must be referenced (also for modification)
Autoren müssen genannt werden (auch bei Bearbeitung)

Only for non commercial use
Nur für nichtkommerzielle Nutzung

Derivative work under same licence
Derivative Arbeit unter selber Lizenz

creative commons http://www.creativecommons.com

DeepSec Vienna 2007
7 Layers of Insecurity

Chapter 51
TCP/IP

- Agenda
  - Internet Protocol Family
  - TCP Initial Sequence Numbers
  - Packet Attacks
  - Spoofing
  - Covert Channels
  - Automatic Configuration
  - Packet tunnels

Internet Protocol Family

- **A Big Family with Lots of Relatives.**

IP Family

- Versions IPv4 & IPv6
- ICMP, TCP, UDP, DCCP, SCTP, …
- IGMP for multicast management
- BGP, OSPF, RIP for routing
- IPsec for encryption/authentication

IP Security Devices

- Router
  - Access lists
- Packet filter / firewalls
  - Access lists, packet normalisation
  - Protocol inspection
- Proxies
  - Separation of connections

TCP Initial Sequence Numbers

- **Numbers are Important.**

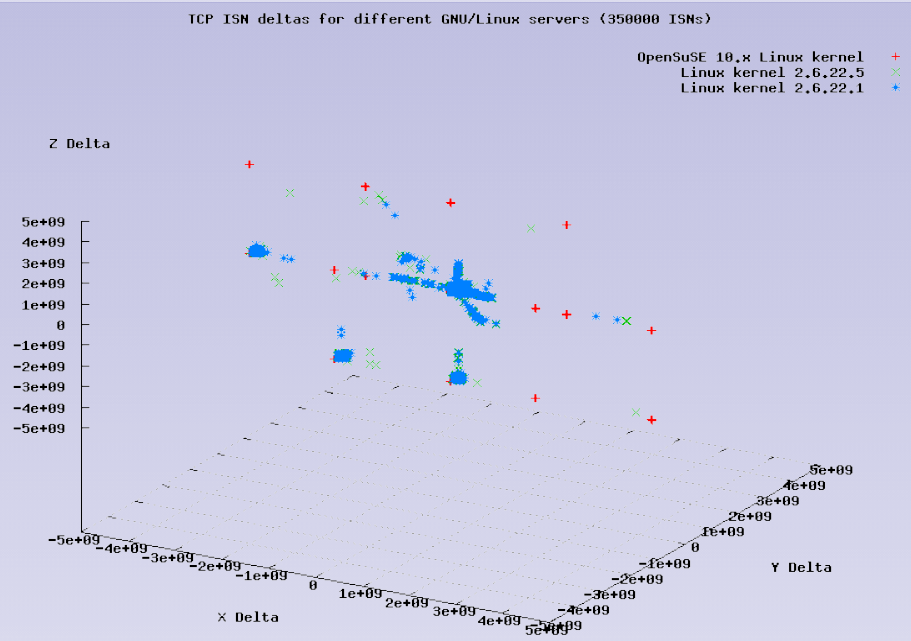
TCP Handshake

- TCP connections are opened by 3 packets
  - SYN (client)
  - SYN+ACK (server)
  - ACK (client)
- SYN packet transmits ISN
  - 32-bit ISN crucial for TCP spoofing
  - ISN should be most random
- TCP sequence number analysis

Randomness of ISNs

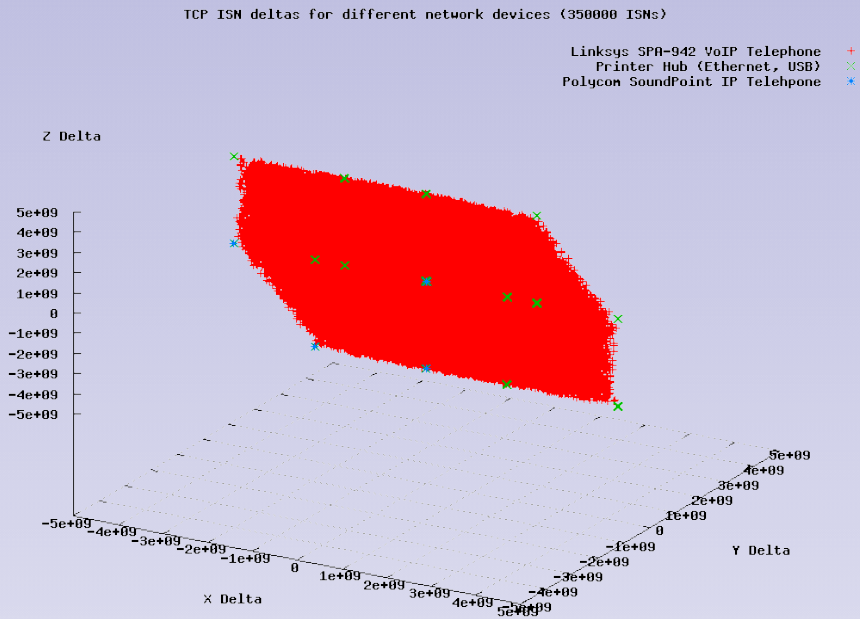
- TCP/IP stacks handle ISNs differently
- Distribution is signature for
  - OS version
  - patch level
  - quality of PRNG
- Randomness protects against
  - TCP hijacking
  - packet/data injection

ISN Attractor Graphs



DeepSec Vienna 2007
7 Layers of Insecurity

ISN Attractor Graphs



DeepSec Vienna 2007
7 Layers of Insecurity

Getting “good” ISNs

- Generation of ISNs is OS-dependent
- Randomness depends on PRNG
- Mitigation
  - Use cryptographically secure protocols
  - Use RFC 1948 implementations
  - Use PRNG with added randomness

Packet Attacks

- Garbage In, Trouble Out.

Teardrop

- Create packet fragments
- Include overlapping & over-sized payload
- Mindless reassembly leads to
  - buffer overflows
  - crashes
- *Most* packet filters can deal with that
  - Use test tools such as ISIC to find out!
  - Don't rely on manuals or documentation!

Flood Mechanisms

- ICMP/UDP flood
- Smurf (send packet to broadcast addresses)
- TCP SYN flood
  - May bind resources on target
- LAND attack
  - Send packet with target as sender
  - Machine replies to itself

DoS and DDoS

- (Distributed) Denial of Service attacks
- Possible on any network link
  - Mitigated by means of rate limiting
- DDoS by Botnets is more common
  - Thousands of unique senders
  - Pattern very difficult to block

Packet Defence

- Reassemble at border firewall
  - Packet inspection
- Use rate/size limits wherever possible
  - ICMP packet length, ICMP error rates
  - TCP SYN, UDP
  - Traffic shaping
- (D)DoS may be blocked upstream

Fuzzing and Load Tests

- Periodical load and fuzzing tests
- Create traffic and monitor systems
  - Use “clean” and malformed packets
  - Mix with recorded traffic
  - Test tools can be automated
  - Monitoring provides recording
- Recommended for system upgrades
  - Use new version in stress environment

IP Spoofing

- **Packets Without Senders.**

Spoofing Methods

- Non-Blind Spoofing
  - Use of sniffed sequence numbers
- Blind Spoofing
  - Guessing sequence numbers
- Man-In-The-Middle
  - Alter content
- DoS/DDos (commonly used with spoofing)

Spoofing Countermeasures

- Proper filtering at network boundaries
  - Ingress/egress filtering
  - *Everyone* needs to do this
- Strong sequence numbers
- Packet authentication
  - VPNs do that automatically
  - Integrity checksums
- Survey State of IP Spoofing

Covert Channels

- **Hide Data in Plain Sight.**

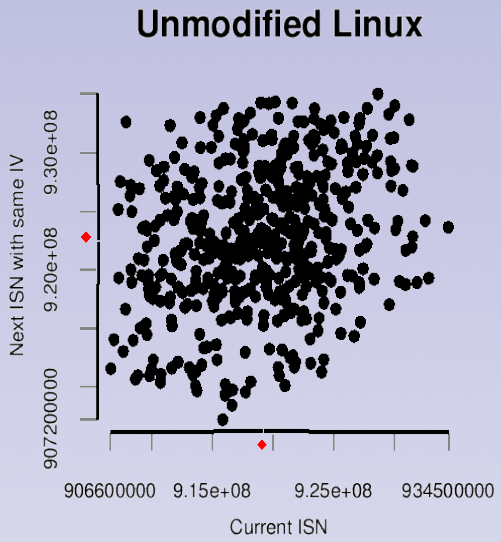
Covert Channel Data

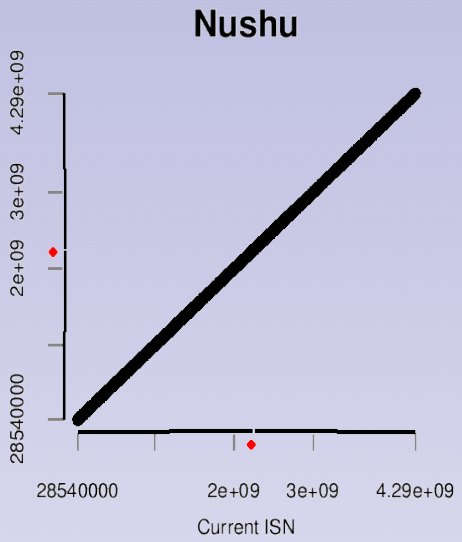
- Most protocols leave “spare room”
  - ICMP payload
  - (Un)used header fields
  - Size/order of fragments
- TCP is very promising
  - Options, TTL
  - Sequence numbers
  - Time stamps

Pattern Avoidance

- A covert channel must be covert
  - Avoid introduction of patterns
  - Use encryption/steganography
- Rarely used header fields dangerous
  - Easily seen
  - May trigger IPS/IDS

Covert Channel with Pattern





DeepSec Vienna 2007
7 Layers of Insecurity

Automatic Configuration

- **Automatically Confuse Machines.**

Simple Service Discovery Protocol (SSDP)

- Expired IETF draft by Microsoft® & HP
- SSDP uses UDP multicast and unicast
  - Multicast address is 239.255.255.250
  - Port is usually 1900
  - Speaks HTTP over UDP (!)
- Provides discovery of services
- Server-based notification
- Route discovery

Uses for SSDP

- ~~Attackers~~ Clients can discover services
  - Little/no static configuration necessary
  - Easily access device information
- Use of SSDP open to any application
- No authentication per design
- Risk: low Impact: depends
  - Use access controls for *any* service

Universal Plug & Play (UPnP)

“The goal of UPnP technology is to make home networking "simple and affordable for users so the connected home experience becomes a mainstream experience for users experience and great opportunity for the industry". UPnP architecture offers pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices.”

Article from the Cover Pages web site

UPnP Design

- Covers layers 3 to 7
  - IP/UDP/TCP, HTTP, XML
- Service discovery is done by SSDP
- Service offers description in XML
- Built-in controls and “eventing”
- UPnP supports NAT
  - UPnP packets traverse UPnP-aware “packet filters”
  - Configuration “happens” automagically

UPnP Security

- UPnP completely trusts
  - all local users
  - all local devices
- UPnP uses HTTP over UDP (uni-/multicast)
- No authentication
- UPnP should be turned off
  - Block 49152/TCP, 1900/UDP & 5000/UDP
  - Block UPnP multicast traffic

Zeroconf

- Automagically connect devices
  1. Allocate addresses without DHCP server
  2. Translate addresses without DNS server
  3. Find services without directory server
  4. Allocate multicast addresses without MADCAP server
- Targeted at personal computing

Zeroconf Methods

- Link local configuration (IPv4, Ipv6)
  - IPv4 clients use 169.254.0.0/16
  - IPv6 base address on MAC
- Rendezvous / Bonjour
  - Service discovery similar to UPnP
  - No controls (no command channel)
  - No authentication
  - Can be contained to local link

Packet Tunnels

- Tunnels feature Lights of Oncoming Trains.

Tunnel Techniques

- Tunnel usually encapsulate packets
  - Useful for routing
  - Protocol-in-protocol transport
- Done by PPP, PPTP, PPPoE, L2TP, GRE, …
- Tunnels make job for filters harder/impossible
  - Headers change, protocol changes
  - Needs scheme for decoding
- Tunnel is a “uncovert” channel

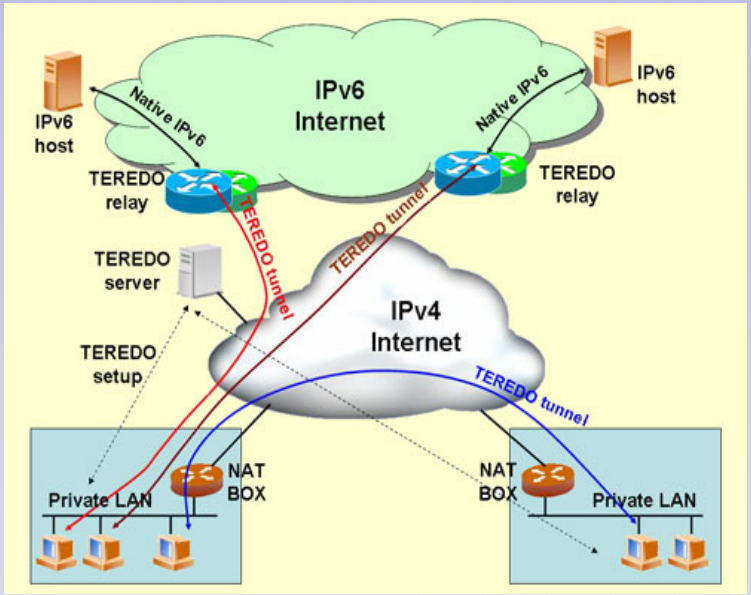
6to4 IPv6 Surprise

- 6to4 means IPv6 transported by IPv4
  - 6to4 tunnels link IPv6 networks
  - IPv6 confined to prefix *2002::/16*
- IPv6 packets may appear in internal network
  - if tunnel endpoint routes and
  - if firewall doesn't block IPv6

Teredo IPv6 Surprise

- Teredo allows NAT traversal for Ipv6
  - Autodetect NAT type
  - Full autoconfiguration
  - Transport of IPv4 via UDPv4 packets
- Client requires Teredo server and relay
- Teredo uses prefix *2001:0000::/32*
  - NAT type, Teredo server, UDP port and NAT public IP encoded in Teredo address

Teredo Overview



Chapter 51
TCP/IP

- Summary
  - Know your TCP/IP stack well.
  - Stress and fuzz your perimeter.
  - Don't forget ingress filtering.
  - Keep an eye open for IPv6 and tunnels.

Thank You

- Questions?

DeepSec Vienna 2007
7 Layers of Insecurity

Chapter 51
TCP/IP

- **Problems Packed into Packets.**

DeepSec Vienna 2007
7 Layers of Insecurity

"I predict the U.S. government won't use or accept IPv4 packets after 2017."

-- Alex Lightman

Copyright Information

- Some rights reserved / Einige Rechte vorbehalten
- Michael Kafka, René Pfeiffer, Sebastian Meier
  C.a.T. Consulting and Trainings, Vienna, Austria
- You may freely use, distribute and modify this work under following agreement:
- Diese Arbeit darf frei genutzt, verbreitet und bearbeitet werden unter folgenden Bedingungen:


Authors must be referenced (also for modification)
Autoren müssen genannt werden (auch bei Bearbeitung)


Only for non commercial use
Nur für nichtkommerzielle Nutzung


Derivative work under same licence
Derivative Arbeit unter selber Lizenz

creative commons http://www.creativecommons.com

© November 2007 51 - TCP/IP 2

DeepSec Vienna 2007
7 Layers of Insecurity

This presentation is published under the CreativeCommons License which can be viewed in detail on their hompage: http://creativecommons.org/licenses/by-nc-sa/2.0/at/

Read more on http://www.creativecommons.com

You are free:


to Share — to copy, distribute and transmit the work


to Remix — to adapt the work

Under the following conditions:


Attribution. You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).


Noncommercial. You may not use this work for commercial purposes.


Share Alike. If you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

- **For any reuse or distribution, you must make clear to others the license terms of this work. The best way to do this is with a link to this web page.**
- **Any of the above conditions can be waived if you get permission from the copyright holder.**
- **Nothing in this license impairs or restricts the author's moral rights.**

Chapter 51
TCP/IP

- Agenda
  - Internet Protocol Family
  - TCP Initial Sequence Numbers
  - Packet Attacks
  - Spoofing
  - Covert Channels
  - Automatic Configuration
  - Packet tunnels

DeepSec Vienna 2007
7 Layers of Insecurity

Internet Protocol Family

- A Big Family with Lots of Relatives.

DeepSec Vienna 2007
7 Layers of Insecurity

IP Family

- Versions IPv4 & IPv6
- ICMP, TCP, UDP, DCCP, SCTP, …
- IGMP for multicast management
- BGP, OSPF, RIP for routing
- IPsec for encryption/authentication

DeepSec Vienna 2007
7 Layers of Insecurity

IP Security Devices

- Router
  - Access lists
- Packet filter / firewalls
  - Access lists, packet normalisation
  - Protocol inspection
- Proxies
  - Separation of connections

DeepSec Vienna 2007
7 Layers of Insecurity

TCP Initial Sequence Numbers

- **Numbers are Important.**

DeepSec Vienna 2007
7 Layers of Insecurity

TCP Handshake

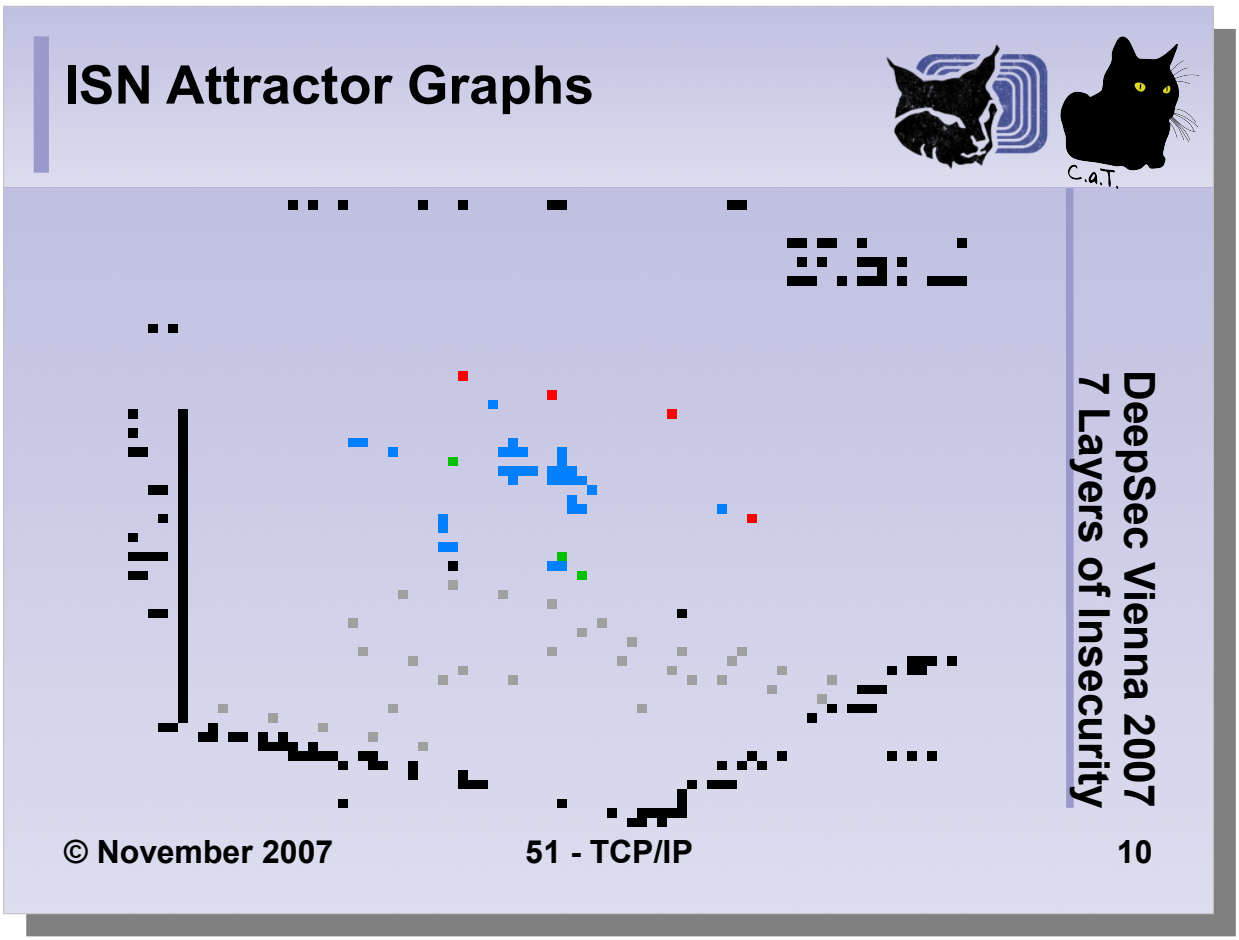
- TCP connections are opened by 3 packets
  - SYN (client)
  - SYN+ACK (server)
  - ACK (client)
- SYN packet transmits ISN
  - 32-bit ISN crucial for TCP spoofing
  - ISN should be most random
- TCP sequence number analysis

DeepSec Vienna 2007
7 Layers of Insecurity

Randomness of ISNs

- TCP/IP stacks handle ISNs differently
- Distribution is signature for
  - OS version
  - patch level
  - quality of PRNG
- Randomness protects against
  - TCP hijacking
  - packet/data injection

DeepSec Vienna 2007
7 Layers of Insecurity



The graphic was generated by collecting TCP ISNs from handshakes. The simple 3D representation was plotted by applying the method of "delayed coordinates" to the sequence of ISNs.

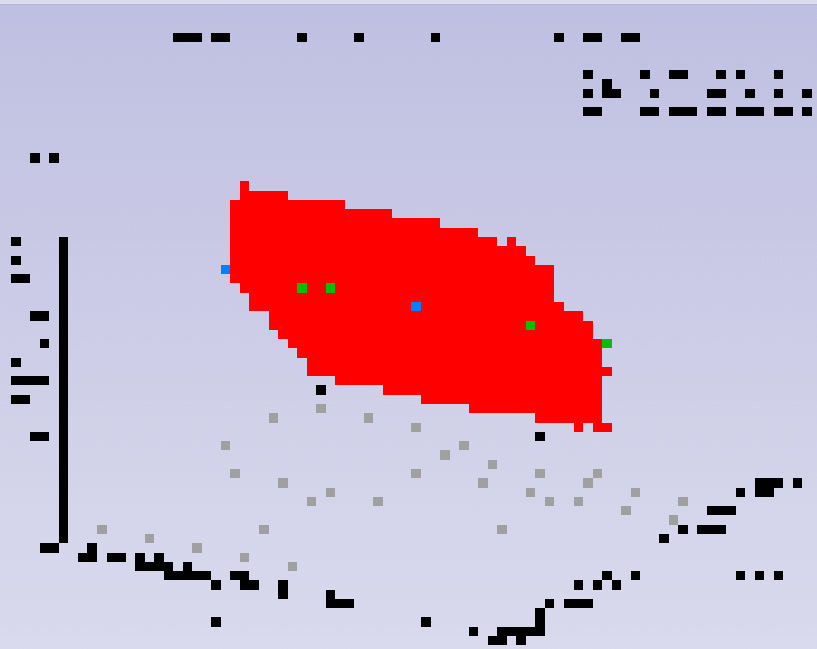
$x_n = isn_{n-2} - isn_{n-3}$

$y_n = isn_{n-1} - isn_{n-2}$

$z_n = isn_n - isn_{n-1}$

This is a common method for analysing dynamic systems. The graphical representation of the data often yields attractors whose shapes can be seen in the data plots. The simple plot shown doesn't reflect the density of the values well. Clusters must be extracted by scaling and zooming into interesting areas of the plot. Note that the shape alone doesn't correlate with the randomness of the ISN sequences, but it unveils possible correlations of the ISNs themselves. These correlations can be used to find systems that are more likely to produce predictable ISNs. Prediction can be done with statistical analysis and a suitable algorithm.

ISN Attractor Graphs



DeepSec Vienna 2007
7 Layers of Insecurity

Getting “good” ISNs

- Generation of ISNs is OS-dependent
- Randomness depends on PRNG
- Mitigation
  - Use cryptographically secure protocols
  - Use RFC 1948 implementations
  - Use PRNG with added randomness

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 51 - TCP/IP 12

RFC 1948 proposes to partition the sequence space by connection identifiers such as local address and port and the remote address and port of a connection. This methods “stirs things up” a bit, but it doesn't rule out playing games with previously-owned IP addresses and ports.

*BSD and Linux try to add randomness from their local entropy pool to the algorithm that creates ISNs:

• Linux: TCP Random Initial Sequence Numbers

• OpenBSD's network stack

CERT® Advisory CA-2001-09 Statistical Weaknesses in TCP/IP Initial Sequence Numbers

Packet Attacks

- Garbage In, Trouble Out.

DeepSec Vienna 2007
7 Layers of Insecurity

Teardrop

- Create packet fragments
- Include overlapping & over-sized payload
- Mindless reassembly leads to
  - buffer overflows
  - crashes
- *Most* packet filters can deal with that
  - Use test tools such as ISIC to find out!
  - Don't rely on manuals or documentation!

DeepSec Vienna 2007
7 Layers of Insecurity

ISIC is short for *IP Stack Integrity Checker*. This tool can created IP packets with random header content. It is mainly used as a test tool for load and fuzzing tests. ISIC was used to find flaws in a version of the NAI Gauntlet firewall.

SING (Send ICMP Nasty Garbage) is a tool for creating ICMP packets of any shape, code, type, colour and content.

nmap can also be used as a packet generator in load tests.

Flood Mechanisms

- ICMP/UDP flood
- Smurf (send packet to broadcast addresses)
- TCP SYN flood
  - May bind resources on target
- LAND attack
  - Send packet with target as sender
  - Machine replies to itself

DeepSec Vienna 2007
7 Layers of Insecurity

DoS and DDoS

- (Distributed) Denial of Service attacks
- Possible on any network link
  - Mitigated by means of rate limiting
- DDoS by Botnets is more common
  - Thousands of unique senders
  - Pattern very difficult to block

DeepSec Vienna 2007
7 Layers of Insecurity

Packet Defence

- Reassemble at border firewall
  - Packet inspection
- Use rate/size limits wherever possible
  - ICMP packet length, ICMP error rates
  - TCP SYN, UDP
  - Traffic shaping
- (D)DoS may be blocked upstream

DeepSec Vienna 2007
7 Layers of Insecurity

Fuzzing and Load Tests

- Periodical load and fuzzing tests
- Create traffic and monitor systems
  - Use “clean” and malformed packets
  - Mix with recorded traffic
  - Test tools can be automated
  - Monitoring provides recording
- Recommended for system upgrades
  - Use new version in stress environment

DeepSec Vienna 2007
7 Layers of Insecurity

IP Spoofing

- **Packets Without Senders.**

DeepSec Vienna 2007
7 Layers of Insecurity

Spoofing Methods

- Non-Blind Spoofing
  - Use of sniffed sequence numbers
- Blind Spoofing
  - Guessing sequence numbers
- Man-In-The-Middle
  - Alter content
- DoS/DDos (commonly used with spoofing)

DeepSec Vienna 2007
7 Layers of Insecurity

Spoofing Countermeasures

- Proper filtering at network boundaries
  - Ingress/egress filtering
  - *Everyone* needs to do this
- Strong sequence numbers
- Packet authentication
  - VPNs do that automatically
  - Integrity checksums
- Survey State of IP Spoofing

DeepSec Vienna 2007
7 Layers of Insecurity

Covert Channels

- **Hide Data in Plain Sight.**

DeepSec Vienna 2007
7 Layers of Insecurity

Covert Channel Data

- Most protocols leave “spare room”
  - ICMP payload
  - (Un)used header fields
  - Size/order of fragments
- TCP is very promising
  - Options, TTL
  - Sequence numbers
  - Time stamps

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 51 - TCP/IP 23

There are some publications describing various methods and implementations of covert channels in TCP/IP streams.

Covert Channels in the IP Time To Live Field

Covert Messaging Through TCP Timestamps

21C3 Passive covert channels in the Linux kernel

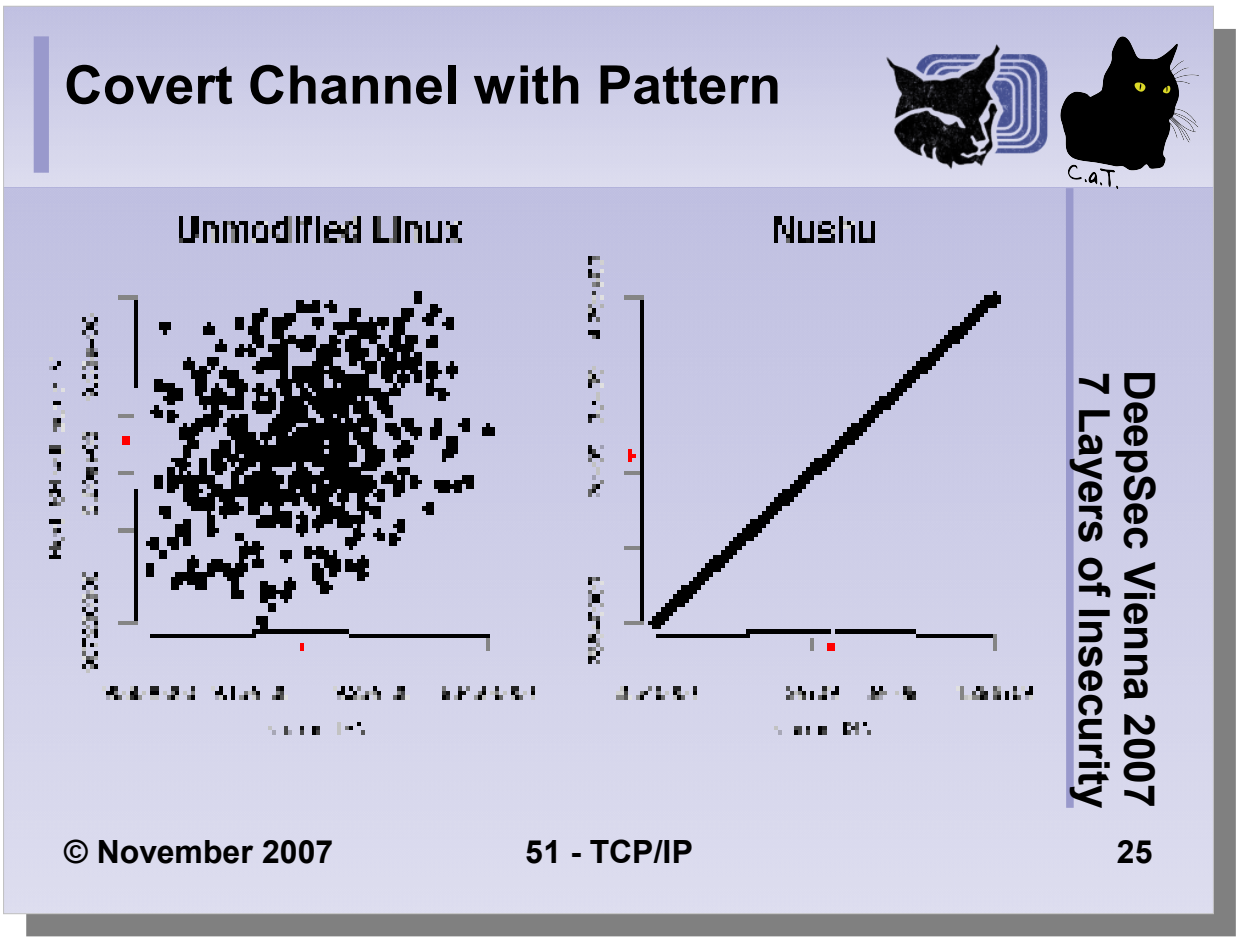
22C3 Covert channels in TCP/IP: attack and defence

LNCS 3856 - Covert Channels in IPv6

Pattern Avoidance

- A covert channel must be covert
  - Avoid introduction of patterns
  - Use encryption/steganography
- Rarely used header fields dangerous
  - Easily seen
  - May trigger IPS/IDS

DeepSec Vienna 2007
7 Layers of Insecurity



The graphic show the behaviour of an unmodified Linux kernel compared to a kernel with the NUSHU Passive Covert Channel developed by Joanna Rutkowska. The diagrams were taken out of the presentation Covert channels in TCP/IP: attack and defence by Steven J. Murdoch. NUSHU uses the TCP/IP sockets of the data transmission together with a DES key as input for the next ISN. By using fixed address/port combinations the presence of a covert channel can be seen. When designing mechanisms for covert data transmissions this has to be taken into account, and it leaves a possibility for detection by suitable data analysis.

Automatic Configuration

- Automatically Confuse Machines.

DeepSec Vienna 2007
7 Layers of Insecurity

Simple Service Discovery Protocol (SSDP)

- Expired IETF draft by Microsoft® & HP
- SSDP uses UDP multicast and unicast
  - Multicast address is 239.255.255.250
  - Port is usually 1900
  - Speaks HTTP over UDP (!)
- Provides discovery of services
- Server-based notification
- Route discovery

DeepSec Vienna 2007
7 Layers of Insecurity

Uses for SSDP

- ~~Attackers~~ Clients can discover services
  - Little/no static configuration necessary
  - Easily access device information
- Use of SSDP open to any application
- No authentication per design
- Risk: low Impact: depends
  - Use access controls for *any* service

DeepSec Vienna 2007
7 Layers of Insecurity

Universal Plug & Play (UPnP)

“The goal of UPnP technology is to make home networking "simple and affordable for users so the connected home experience becomes a mainstream experience for users experience and great opportunity for the industry". UPnP architecture offers pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices.”

Article from the Cover Pages web site

DeepSec Vienna 2007
7 Layers of Insecurity

UPnP is a protocol designed for convenience, not for security. Apart from the control functions it provides there may be the usual bugs in the implementation (because the vendor wanted to ship the product with just-in-time-firmware just-in-time for Christmas, Easter or your birthday). There are UpnP-capable routers with “firewall” function for sale that may open ports whenever a UPnP device feels like requesting it. To quote from the Gentoo UPnP HOWTO: *UPnP (Universal Plug n Play) is useful for applications such as Azureus and MSN messenger.*

Mitigation:

• Turn UPnP functionality off.

• Filter UPnP multicast traffic and traffic to 49152/TCP and 1900/UDP.

UPnP Design

- Covers layers 3 to 7
  - IP/UDP/TCP, HTTP, XML
- Service discovery is done by SSDP
- Service offers description in XML
- Built-in controls and “eventing”
- UPnP supports NAT
  - UPnP packets traverse UPnP-aware “packet filters”
  - Configuration “happens” automagically

DeepSec Vienna 2007
7 Layers of Insecurity

UPnP Security

- UPnP completely trusts
  - all local users
  - all local devices
- UPnP uses HTTP over UDP (uni-/multicast)
- No authentication
- UPnP should be turned off
  - Block 49152/TCP, 1900/UDP & 5000/UDP
  - Block UPnP multicast traffic

DeepSec Vienna 2007
7 Layers of Insecurity

Zeroconf

- Automagically connect devices
  1. Allocate addresses without DHCP server
  2. Translate addresses without DNS server
  3. Find services without directory server
  4. Allocate multicast addresses without MADCAP server
- Targeted at personal computing

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 51 - TCP/IP 32

The Multicast Address Dynamic Client Allocation Protocol (MADCAP) is a mechanism in order to allow hosts to request multicast address allocation services from designated servers. It works similar to DHCP and allows clients to dynamically use multicast address ranges.

Zeroconf Methods

- Link local configuration (IPv4, Ipv6)
  - IPv4 clients use 169.254.0.0/16
  - IPv6 base address on MAC
- Rendezvous / Bonjour
  - Service discovery similar to UPnP
  - No controls (no command channel)
  - No authentication
  - Can be contained to local link

DeepSec Vienna 2007
7 Layers of Insecurity

Packet Tunnels

- Tunnels feature Lights of Oncoming Trains.

DeepSec Vienna 2007
7 Layers of Insecurity

Tunnel Techniques

- Tunnel usually encapsulate packets
  - Useful for routing
  - Protocol-in-protocol transport
- Done by PPP, PPTP, PPPoE, L2TP, GRE, …
- Tunnels make job for filters harder/impossible
  - Headers change, protocol changes
  - Needs scheme for decoding
- Tunnel is a “uncovert” channel

DeepSec Vienna 2007
7 Layers of Insecurity

6to4 IPv6 Surprise

- 6to4 means IPv6 transported by IPv4
  - 6to4 tunnels link IPv6 networks
  - IPv6 confined to prefix *2002::/16*
- IPv6 packets may appear in internal network
  - if tunnel endpoint routes and
  - if firewall doesn't block IPv6

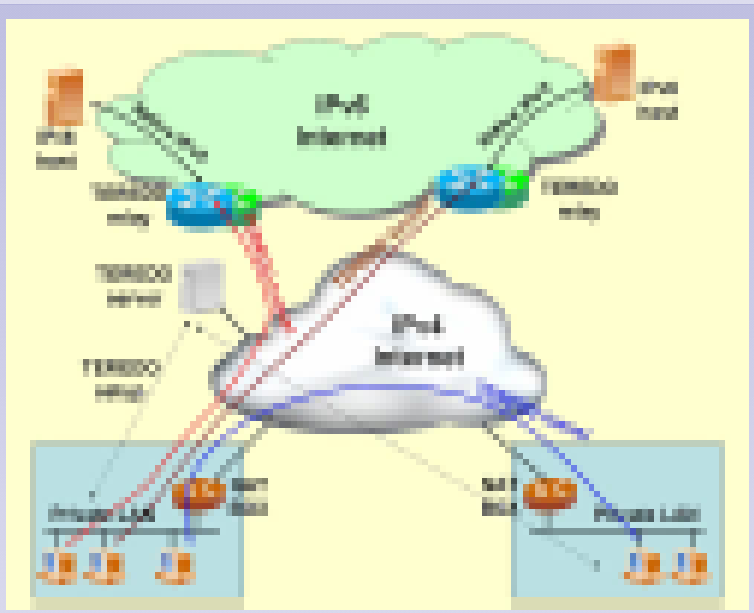
DeepSec Vienna 2007
7 Layers of Insecurity

Teredo IPv6 Surprise

- Teredo allows NAT traversal for Ipv6
  - Autodetect NAT type
  - Full autoconfiguration
  - Transport of IPv4 via UDPv4 packets
- Client requires Teredo server and relay
- Teredo uses prefix *2001:0000::/32*
  - NAT type, Teredo server, UDP port and NAT public IP encoded in Teredo address

DeepSec Vienna 2007
7 Layers of Insecurity

Teredo Overview



DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 51 - TCP/IP 38

This diagram shows the operation of Teredo IPv6 tunnels. The clients sit behind NAT routers in their private LANs. The Teredo client contacts a Teredo server (which sits in IPv4 space) in order to set up a tunnel and to assign the client a Teredo IPv6 address. After the setup phase the client can use Teredo relay servers for IPv6 and IPv4 packet forwarding. The tunnels created can then be used to reach IPv6 space and vice versa. Note that another Teredo client sitting in a different LAN with a NAT device can be reached as well (and vice versa). Teredo only requires outgoing UDP traffic and replies to these packets (any stateful inspection firewall can provide this connectivity, it is similar to DNS traffic with respect to the UDP state).

The diagram was taken from an article about Teredo connectivity.

Chapter 51
TCP/IP

- Summary
  - Know your TCP/IP stack well.
  - Stress and fuzz your perimeter.
  - Don't forget ingress filtering.
  - Keep an eye open for IPv6 and tunnels.

DeepSec Vienna 2007
7 Layers of Insecurity

Thank You

- Questions?

DeepSec Vienna 2007
7 Layers of Insecurity