Internet Security

MCNC ANR April 2000
Ilia Baldine

ibaldin@mcnc.org

Overview

- The Past: "Security? What Security?"
- The Present: "The search for the silver bullet"
- The Future: "On the digital battlefield"

The Past

- November 2, 1988 - The Internet Worm
  - Written by a Cornell Graduate Student Robert T.Morris
  - Exploited several vulnerabilities
    - sendmail DEBUG mode
    - fingerd buffer overflow
    - weak passwords
    - trusted relationships (~/.rhosts, hosts.equiv)
  - Infected only VAX 4 BSD and Sun 3
  - Consisted of two parts
    - *A bootstrapping vector program*
    - *Main program precompiled for the two architectures*
  - The worm took measures to avoid detection
    - Challenge/response scheme
    - Periodical "forking" to change the process ID
    - Checked for other worms running on the same host

Common Attack Strategies

- Insider vs. Outsider
  - Insider:
    - Exploit local vulnerabilities
      - stack smashing of SUID root programs
      - cracking weak passwords of other users on the system
      - abuse of privileges
  - Outsider:
    - Learn more about the target by combining social engineering, port scans, DNS and whois queries and network mapping tools
    - Determine the weaknesses (known buggy implementations, trusted relationships, back doors etc.)
    - DDoS (Distributed Denial of Service)
    - Attacks may be exploratory or malicious in nature

Common Attack Goals

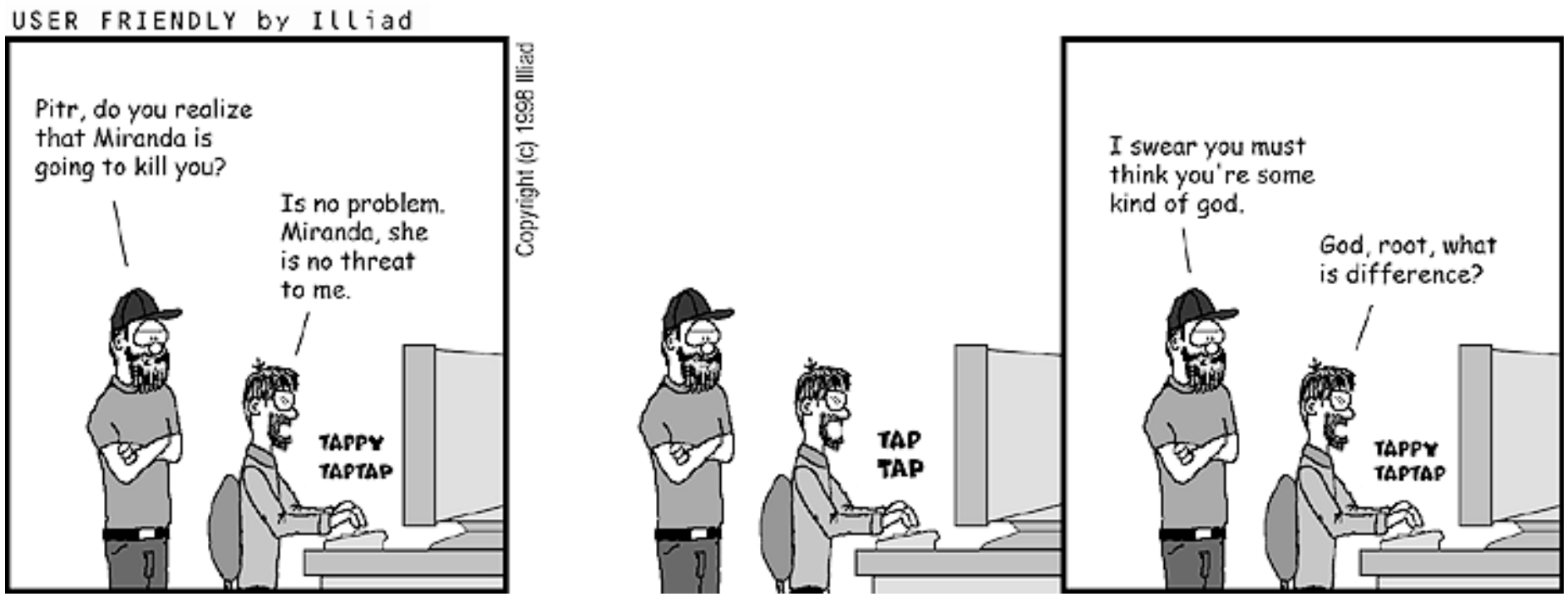
- Goal I: Gain control of the host
  - Access information stored on it or passing through it
  - Abuse a trusted relationship it might have with the target host
  - Use it as a platform for DDoS attack
- Goal II: Disable the host
  - Sheer malice and ill will
  - Spoof yourself as a disabled host to abuse the trusted relationship it might have with the target host
- Achieving either one of the goals may in fact be a stepping stone to the other goal.

Common Attacks

- Achieving Goal I (Gaining Control)
  - Stack smashing (from inside or outside)
  - Password sniffing
  - TCP Spoofing
- Achieving Goal II (Disabling the Host)
  - Smurf
  - Ping of Death I and II (specific to Win95/NT3.0)
  - DDoS
  - Process Table Attack
  - SYN flood

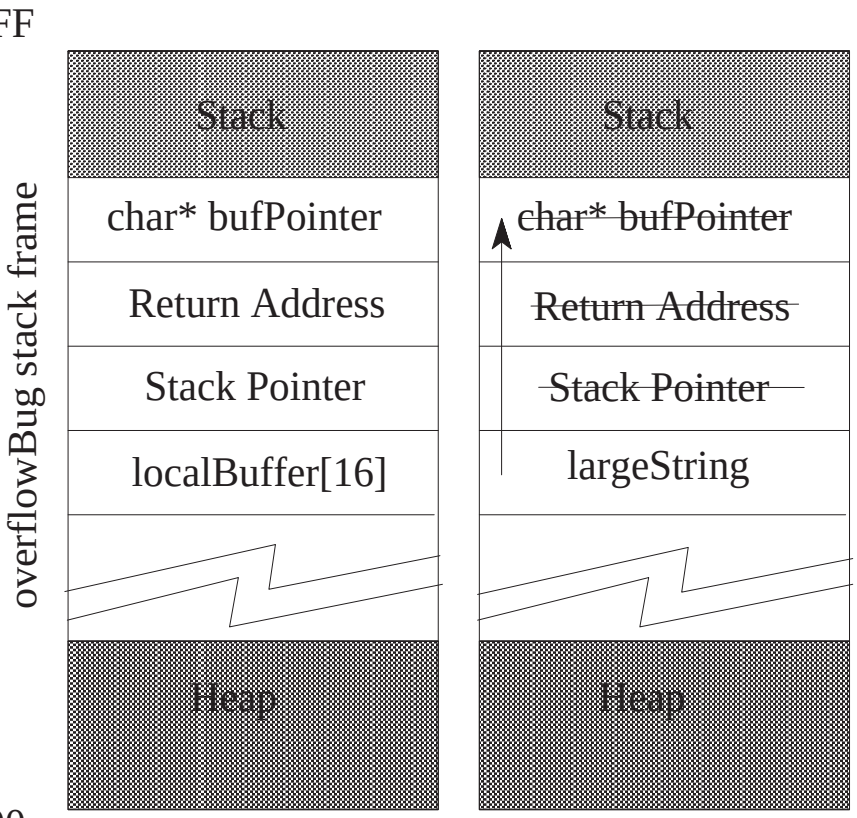
Common Vulnerabilities

- Buffer Overflow (Stack Smashing)
- Trusted relationships (.rhosts for r[login|sh|cp] services)
- Weak passwords
- IP Stack implementation weaknesses
- Race conditions
- Misconfigured network elements (routers)



Stack Smashing Attacks

- Exploit the lack of run-time array bounds checking in C
- Can be performed by injecting shellcode into
  - Environment variables
  - Function parameters
  - Interactive input
- Shellcode typically consists of a string representation for assembly code that does *execve("/bin/sh", NULL, NULL);* which gives the attacker access to a privileged shell
- Example:



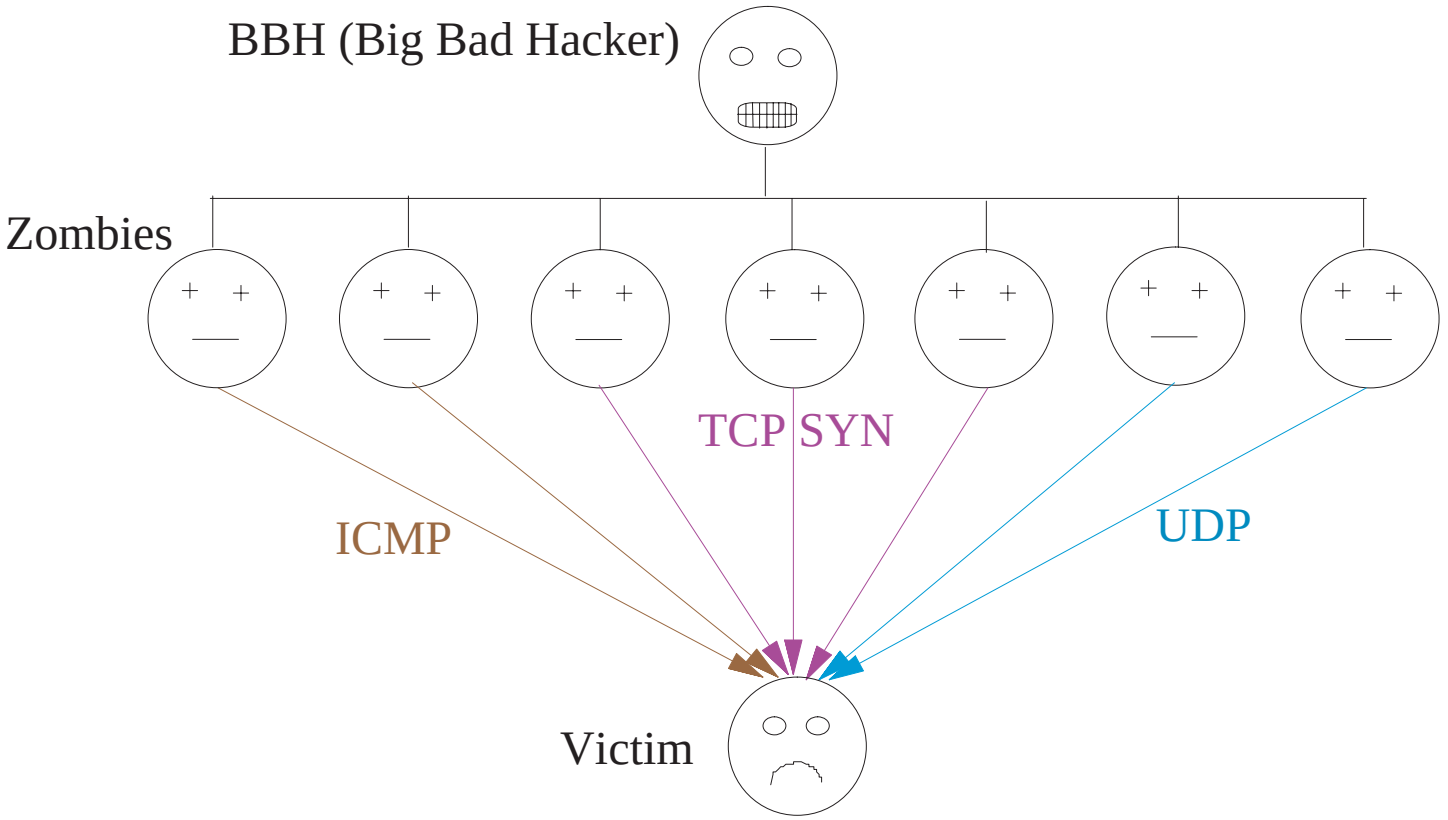

```
void overflowBug(char* bufPointer) {
        char localBuffer[16];
        strcpy(localBuffer, bufPointer);
}

void main() {
        char largeString[128];
        int i;
        for(i=0;i<128;i++)
                largeString[i]='A';
        overflowBug(largeString);
}
```

Distributed Denial of Service (DDoS) Attacks

- Involve a large number of "Zombie" hosts attacking one or more victims with spoofed traffic
- Proceed in stages:
  - Gaining root access to a large number of hosts ("zombies") through known vulnerabilities
  - Installation of agent software and root kits
  - Initiation of the attack using handler software
- Most popular DDoS tools
  - TFN, TFN2K, TFN3K
  - Trin00
  - Stacheldracht

DDoS Attack



Difficulties in fighting DDoS Attacks

- Attacking packets frequently carry spoofed source IP address (if not the whole address, at least the last 8 bits)
- Attack comes from many domains at the same time
- Handler is even more difficult to trace due to the use of covert channels
- High level of traffic generated by the attack overwhelmes filtering and tracing tools

The Present

- Better information security:
  - Shadow passwords
  - Secure Applications:
    - SSH, PGP
  - Secure application frameworks:
    - Kerberos
  - Secure protocols:
    - SSL, IPSec
- Mechanisms that guarantee absence of buffer overflow security holes
  - StackGuard
- Firewalls
- Intrusion-Detection mechanisms:
  - Host-Based
    - Tripwire (checks file system integrity)
  - Network-Based
    - RealSecure, NetRanger, Anzen

Encryption and Authentication

- Public Key Cryptography
  - Uses two keys - public and private. Public is available to anyone, private is secret.
  - For encryption - the message is encrypted with the public key and decrypted with the private key
  - For authentication - a signature is created with the private key and verified with the public key
  - Computationally expensive
- DES
  - Designed to be Implemented in hardware
- MD5

Kerberos

- Created at MIT as part of Athena project
- Has two purposes:
  - Access control in a distributed environment through
    - Authentication
    - Key Distribution
- All communications are encrypted
- Each user and service are principals, the principals are authenticated to each other.
- Two main servers are
  - Key Distribution Center (KDC)
  - Ticket Granting Server (TGS)

IPSec

- Specified by the IPSec IETF working group
- Employs two separate protocols:
  - AH (Authentication Header)
    - *provides origin authentication, data integrity*
  - ESP (Encapsulating Security Payload)
    - *provides data confidentiality and authentication*
  - Both provide access control through key management
- Can be used in two different modes:
  - Transport (host to host only)
    - provides security for higher layer protocols (TCP, UDP), does not protect IP header in general
  - Tunnel (host to host, host to gw, gw to gw)
    - protects the entire IP packet through encapsulation
    - does not protect outer IP header
    - Tunnel mode allows to build secure VPNs

Transport vs. Tunneling Mode

Transport Mode

IP packet with TCP payload

IP Header TCP Header Segment

IPSec AH or ESP Transport Mode Packet

IP Header AH or ESP Header TCP Header Segment

Tunneling Mode

IP packet with TCP payload

IP Header TCP Header Segment

IPSec AH or ESP Transport Mode Packet

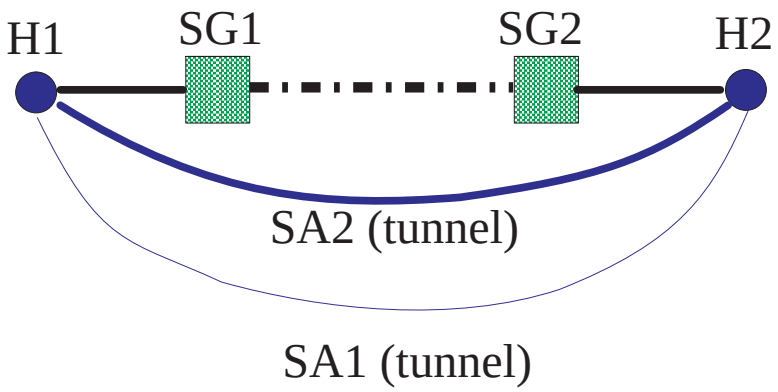
Outer IP Header AH or ESP Header IP Header TCP Header Segment

IPSec Security Associations

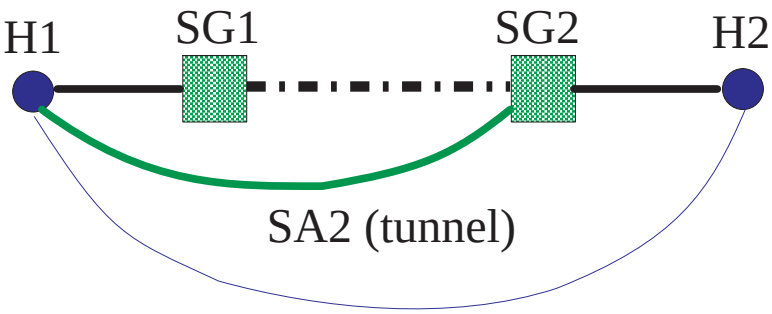
- Provide a simplex connection with a specified security service (AH or ESP)
- An SA carries information about the security protocol, the endpoints and the associated key information
- SAs can be bundled to improve security through
  - Transport adjacency
  - Iterated Tunneling

Various Tunneling Modes

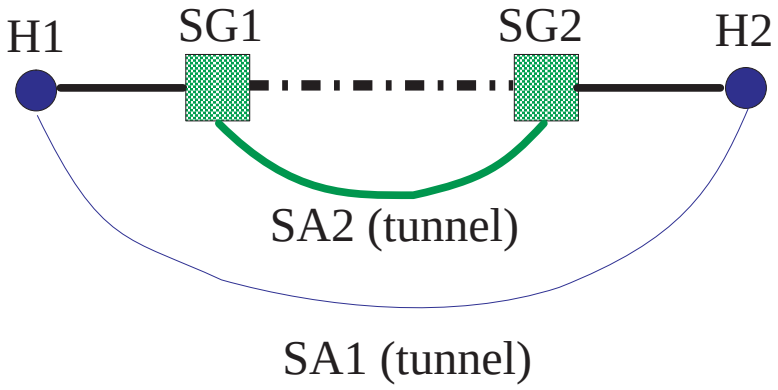
1. Both endpoints are the same



1. One common endpoint



1. No common endpoints

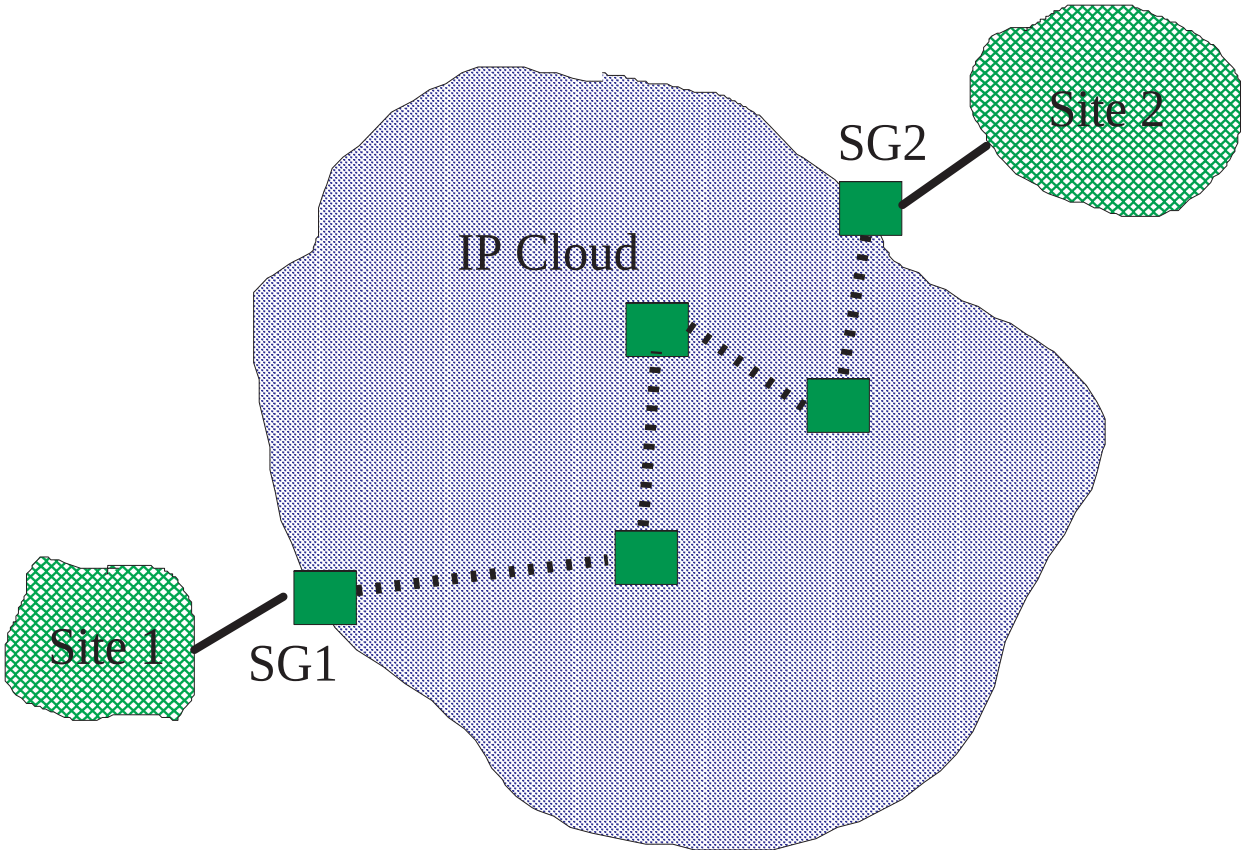


IPSec Databases

- Each host must maintain
  - Security Policy Database (SPD) that defines the protocols to be used for a particular selector
    - with entries for INBOUND and OUTBOUND traffic
    - must afford three choices to traffic
      - Discard
      - Apply IPSec
      - Bypass IPSec
    - crossreferenced to SAD for outbound traffic
  - Security Association Database (SAD)
    - maintains the list of all open SAs

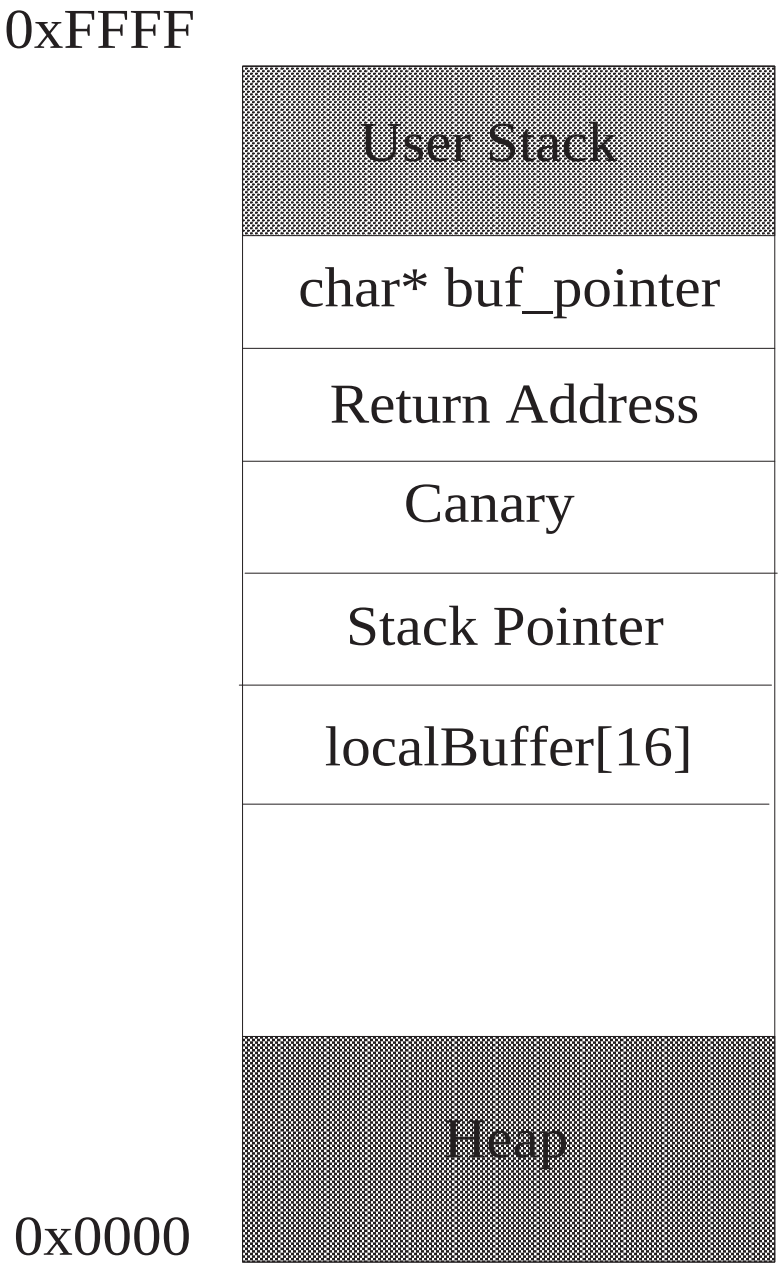
IPSec Key Management

- Can be manual for host-to-host and small VPNs
- Automated through IKE protocol



StackGuard

- Works by preventing buffer overflow at run-time
- Through minor alterations to the compiler places a "canary" - a predetermined value, above the return address on the stack. A function checks the canary value for alterations before returning.
- When an alteration is detected the program halts raising an alert
- A canary can be
  - Fixed
  - Random
  - 0x00000000



Firewalls

- Firewalls can be of several types:
  - Packet Filtering
    - limiting in nature
    - speed is an advantage
  - Circuit-level (proxy)
    - require client support
    - providing inbound services is problematic
  - Application-level
    - can only be applied to a limited number of applications
- Linux and FreeBSD come with packet-filtering firewall code included

The Future

- Statistical IDS
- New Approaches to IDS
  - UNM Research into computer immunology
- Infrastructure Protection
- Integrated Security Mechanisms
  - Celestial
- Integrated host- and network-based Intrusion Detection
  - IETF CIDF
  - Deciduous

Statistical vs. Signature-based ID

- Signature-based IDS works by comparing the sequence of events against a "signature" of a known attack.
  - RealSecure (ISS)
- Statistical IDS maintains a profile of a "healthy" system and issues an alert when something out of the ordinary happens
  - NIDES system (SRI)

Advantages and Disadvantages

- Signature-based IDS works only against known attacks. Needs constant updates with new attack profiles.
- Statistical IDS can detect unknown attacks, but is hampered
  - potentially large number of "false-positives"
  - slow response
  - detection is non-sepcific (e.g. "something is wrong")

Common Intrusion Detection Framework (CIDF)

- ID systems need to be able
  - to exchange intrusion even information
  - to exchange attack profile information
  - communicate with response systems
- CIDF defines
  - the framework in which this type of communication takes place
  - the language and the protocols used in the exchange

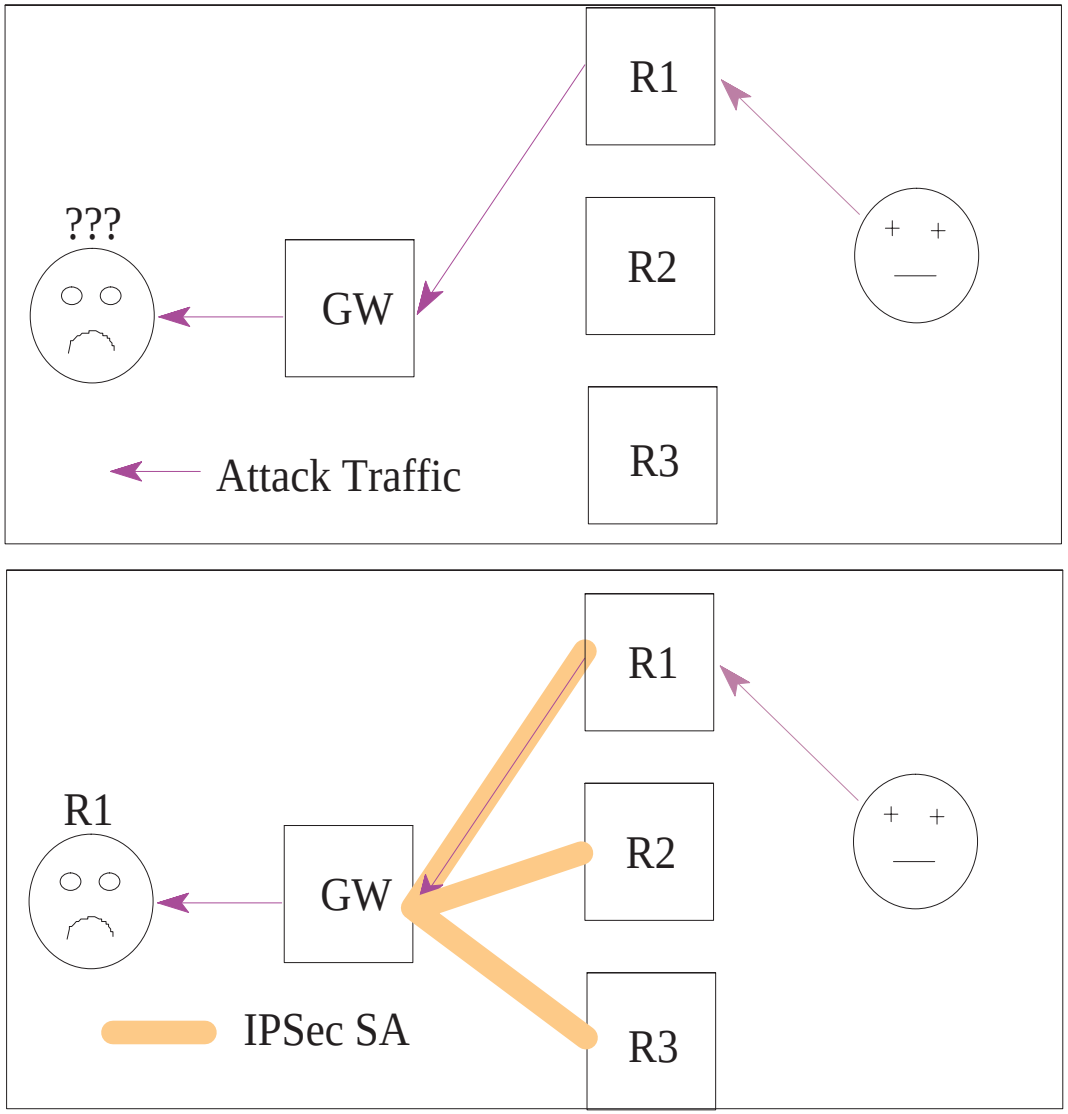
ICMP Traceback Extensions

- IP has to source authentication
- It is impossible to trace which routers packets follow
- Idea: ICMP Traceback
  - A traceback packet is generated every 20,000 packets or so by a router
  - It consists of
    - Back Link (previous hop)
    - Forward Link (next hop)
    - Timestamp
    - Traced packet
    - Authentication

Deciduous (Decentralized Identification of Intrusion Sources)

- IP has no source authentication mechanism
- IPSec can authenticate traffic between hosts or gateways
- If we can create SAs between the victim's gateway and all neighbouring routers, we can find out where the attack traffic is coming from

Deciduous in Action



Celestial
Security Management System

- Goals
  - Make security services from heterogeneous mechanisms available to applications through a simple API
  - Provide end-to-end security services using multiple distributed security mechanisms
  - Enhance survivability through dynamic service reconfiguration
  - Create an integrated framework for security management, and intrusion detection and response coordination

Sources of Information

- IETF ID Working Group
- IETF IPSec Working Group
- COAST Archive (www.cs.purdue.edu/coast)
- SANS Institute (www.sans.org)
- Hacking Websites:
  - RootShell.com
  - L0Ft Heavy Industries/@Stake (www.l0ft.com)
  - genocide2600.com
  - PacketStorm Security (www.securify.com/packetstorm)
- ID manufacturers
  - SRI (www.sri.com)
  - ISS (www.iss.net)
  - Cisco Systems (www.cisco.com)
  - Tripwire Security (www.tripwiresecurity.com)