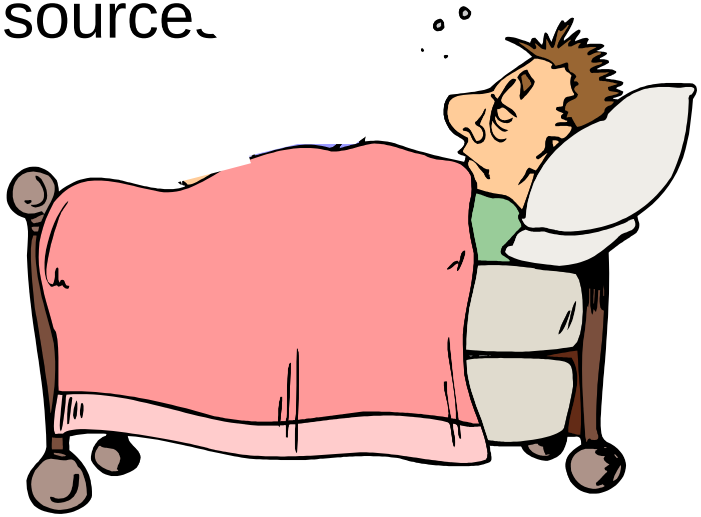
Network Security

Intrusion Detection and Prevention

Prasad Babu

What’s Keeping Security Administrators Up at Night?

- Unauthorized users and use of resources
  - Security policy violation
- Denial of Service (DoS)
  - Slowing resources down
  - Making resources unavailable
- Illegal use of network
  - Copyrighted material
  - Being used as a platform for an attack
- Stealing/Altering Data
  - From network resources (desktops/servers)
  - As it travels through the network



Security Drivers

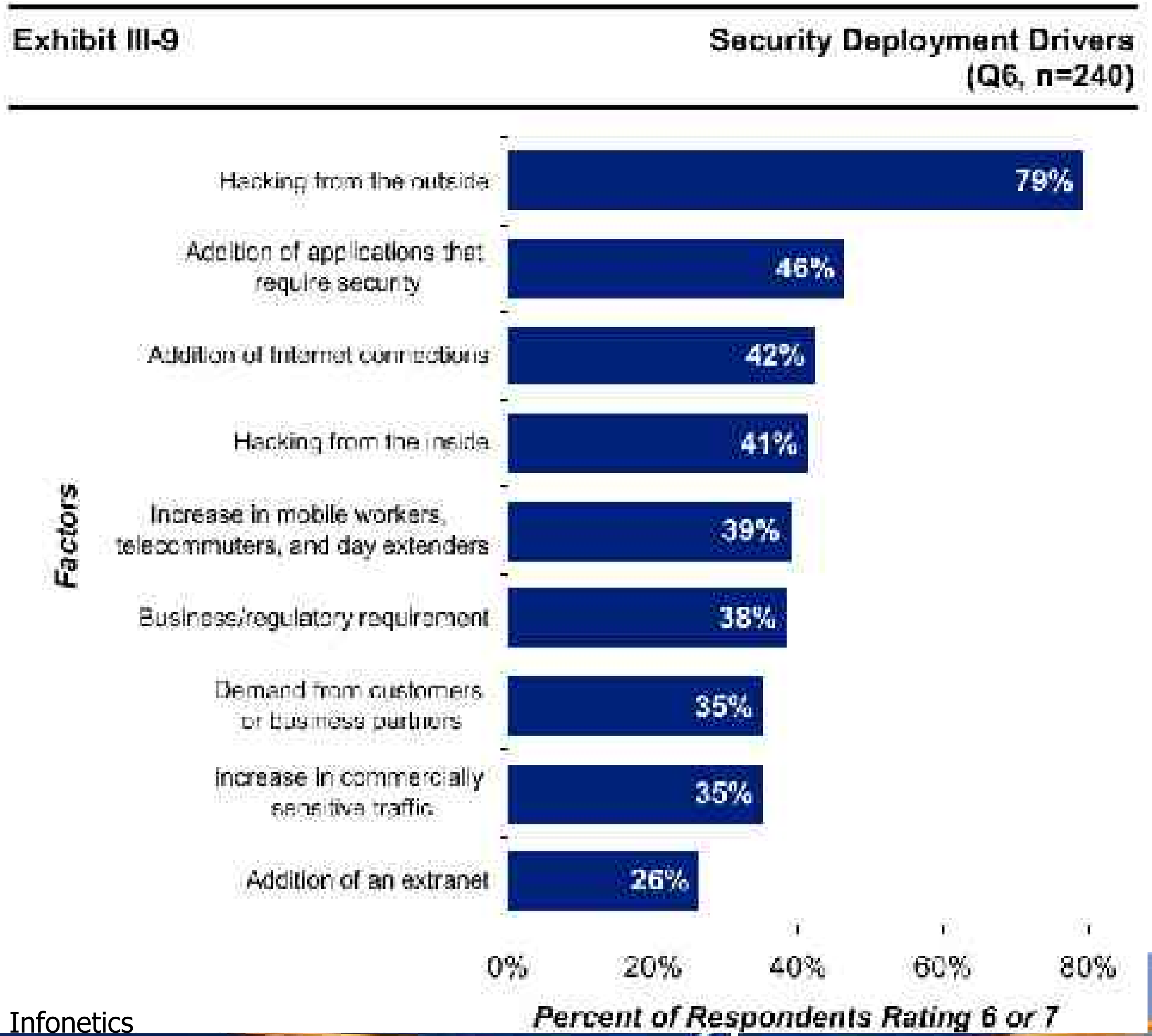


Exhibit III-9

Security Deployment Drivers
(Q6, n=240)

Source: Infonetics

Different Solutions for Different Types of Threats…

Type of Threat | **Way to Mitigate**

Physical

Access to equipment

Social engineering

→ Strong Corporate Policies

Current technologies are good at addressing…

Network

Policy violation and attacks

→ Strong Technology for Strong Network Security Policies

Majority of your time focused on…

Application

Policy violation and attacks

→ Strong Technology for Strong Application Security Policies

Challenges Unique to Application Security

Must understand what the client and server are intending to do

- Network traffic format is different from what the application generates or sees

Each application has its own “custom” attacks and therefore needs its own custom protection

Many attacks are unknown requiring a “day zero” defense

New attacks keep popping up so system should be quickly updatable

Advanced Application Analysis

Attack Protection Mechanisms:

Backdoor

- Trojans and Worms

Traffic Anomaly

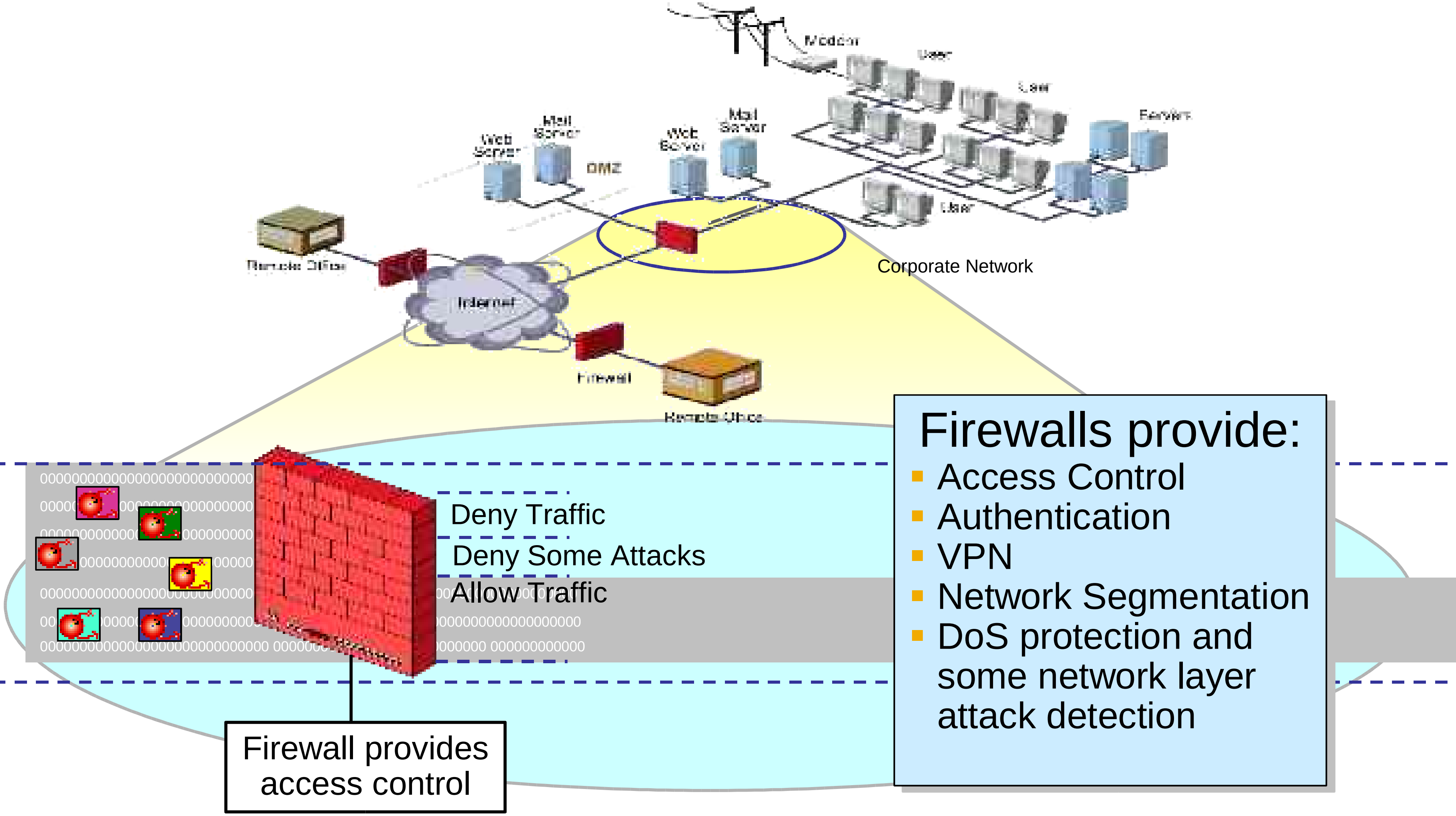
- Reconnaissance Attacks

Profile-Based

- Sudden changes in the way the network and applications are being used

More…

A Firewall is the 1st Layer of Defense



Firewalls provide:

- Access Control
- Authentication
- VPN
- Network Segmentation
- DoS protection and some network layer attack detection

Firewall provides access control

Traditional Solutions for Applications Security : IDS

Monitors for Application Attacks

Detects application attacks using:

- Protocol conformance
- Service field pattern matches (Stateful Signatures)
- May implement other sophisticated attack protection mechanisms

Easily evaded

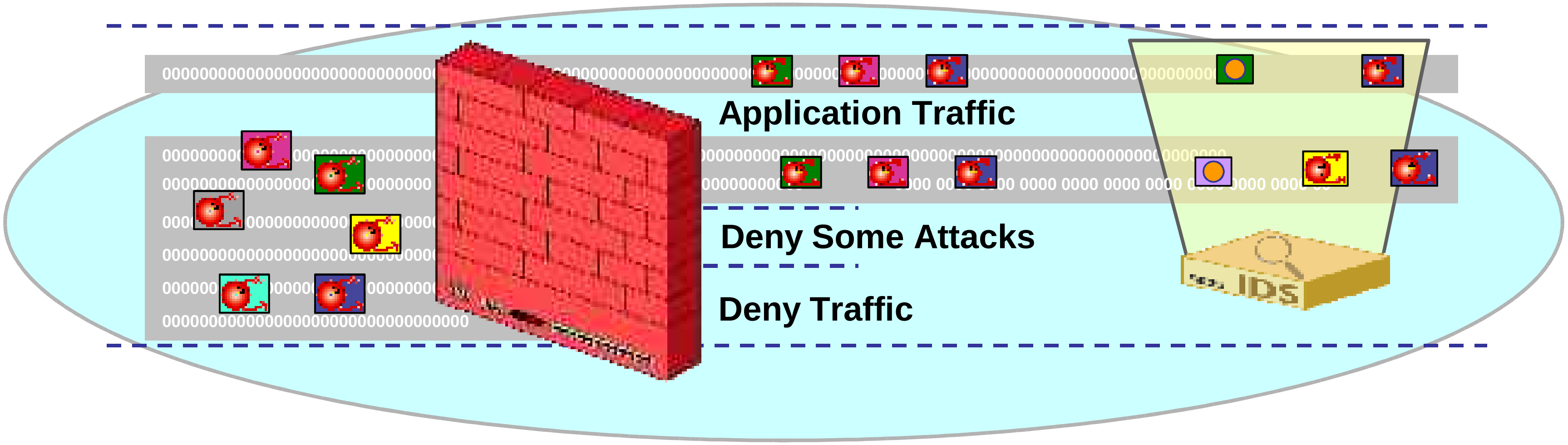
Passive Response Mechanisms

- Sends alerts
- All attacks initiate investigation and manual response

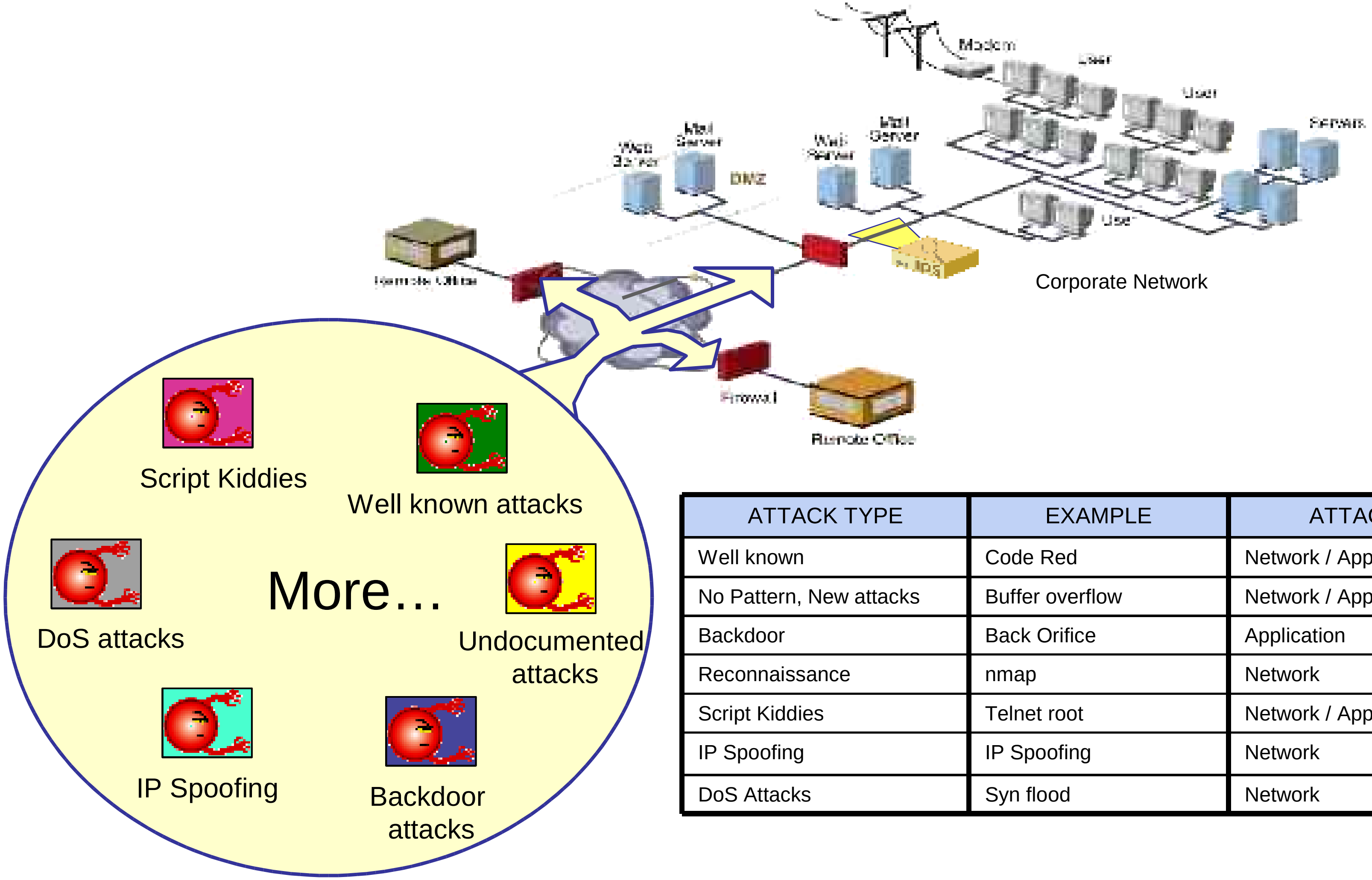
Traditional Solutions: IDS

Security	—	Cannot Prevent Attacks, Easily Evaded
High Performance	+	Meets network requirements
Reliable Connectivity	N/A	Not a networking device
Ease of Use	—	Lots of logs to monitor and respond to, burden on human resources

Solution Needs to Be In-line to Provide Protection



Attacks Are More Sophisticated



Corporate Network

Script Kiddies

Well known attacks

DoS attacks

More…

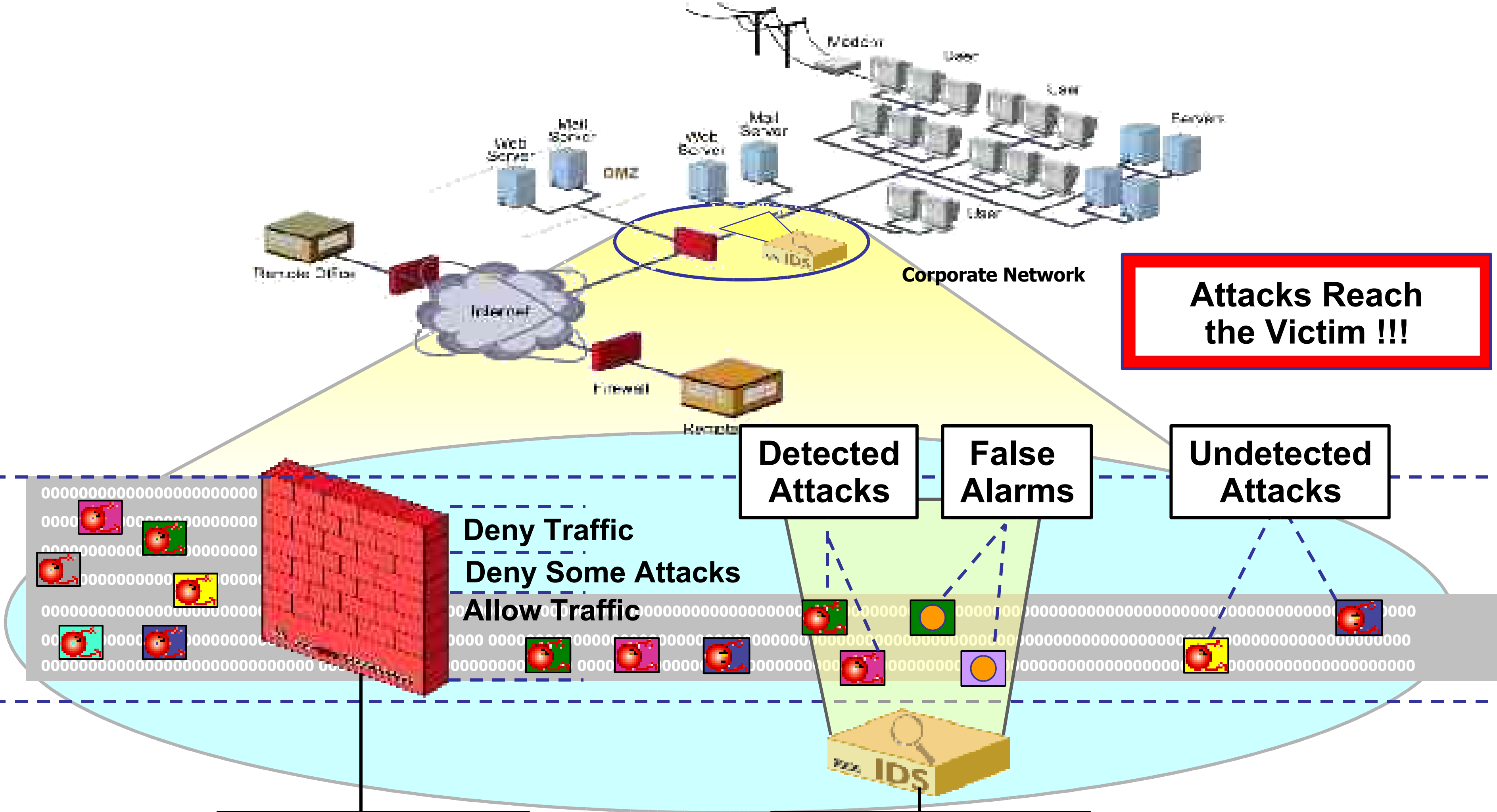
Undocumented attacks

IP Spoofing

Backdoor attacks

ATTACK TYPE	EXAMPLE	ATTACK LEVEL
Well known	Code Red	Network / Application
No Pattern, New attacks	Buffer overflow	Network / Application
Backdoor	Back Orifice	Application
Reconnaissance	nmap	Network
Script Kiddies	Telnet root	Network / Application
IP Spoofing	IP Spoofing	Network
DoS Attacks	Syn flood	Network

IDS as the 2nd Layer of Defense…. ?



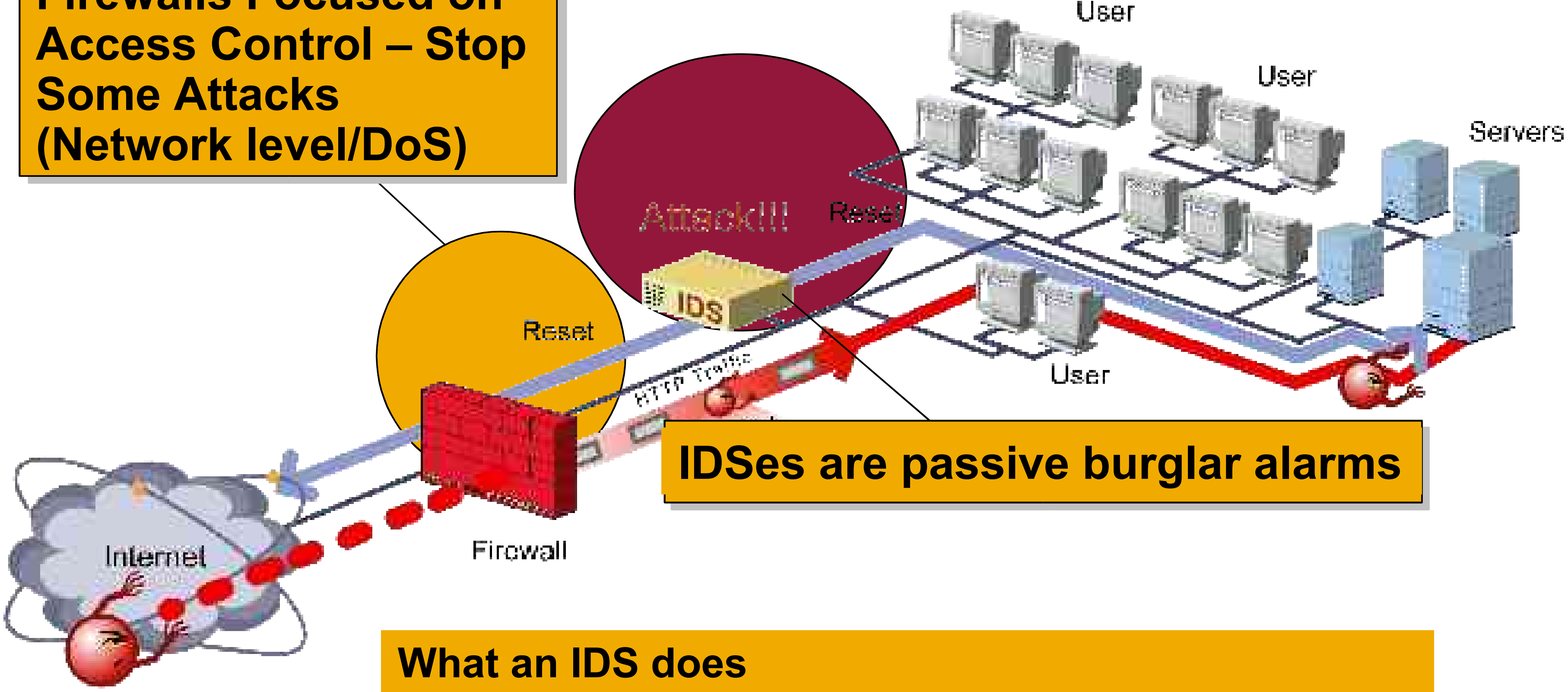
Attacks Reach the Victim !!!

Firewall provides access control

IDS provides attack monitoring

What is Prevention?

Firewalls Focused on Access Control – Stop Some Attacks (Network level/DoS)



IDSes are passive burglar alarms

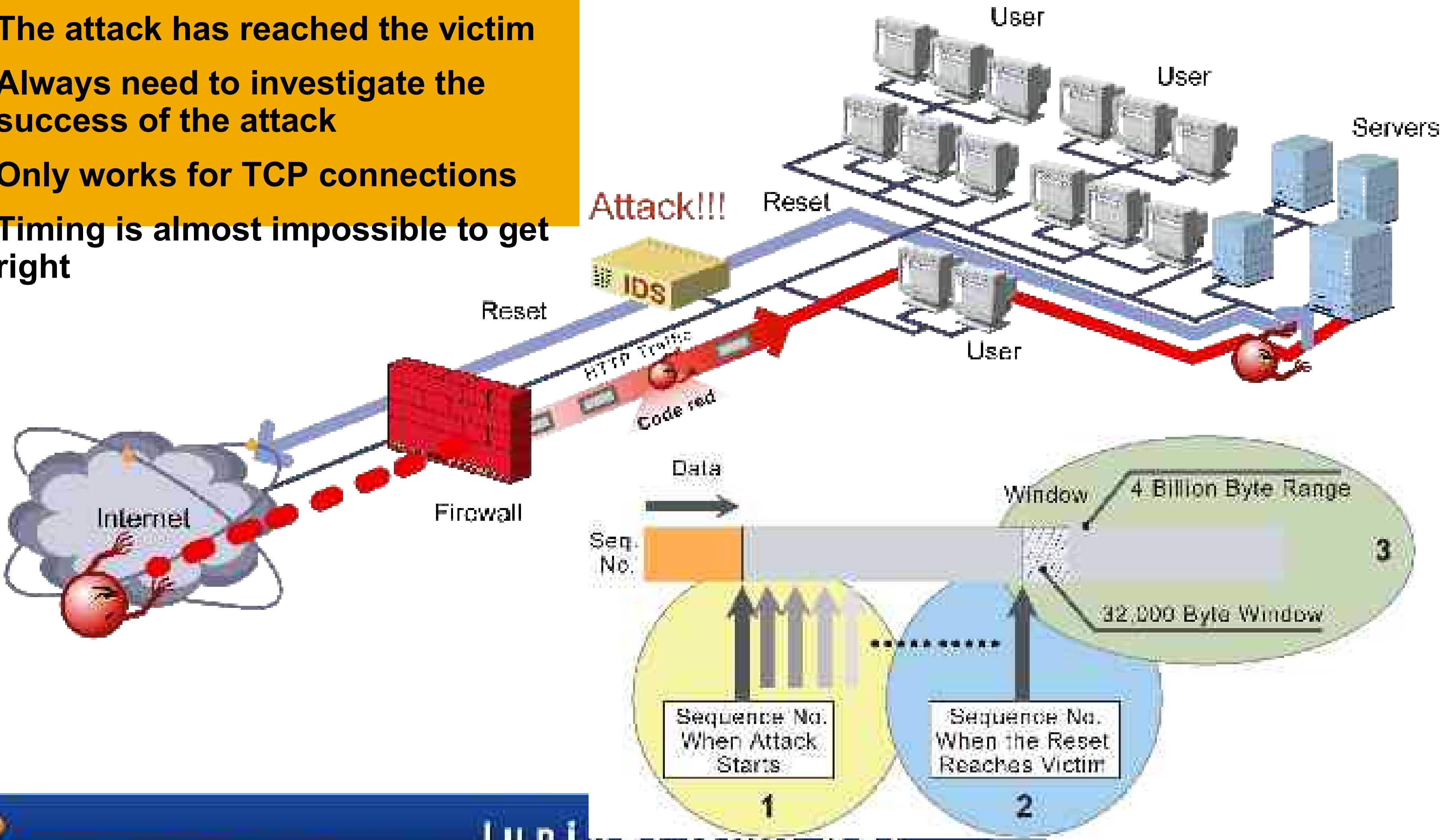
What an IDS does

- **A TCP Reset can stop an attack**
- **Firewall signaling (IP blocking) can stop an attack**

TCP Reset

Challenges

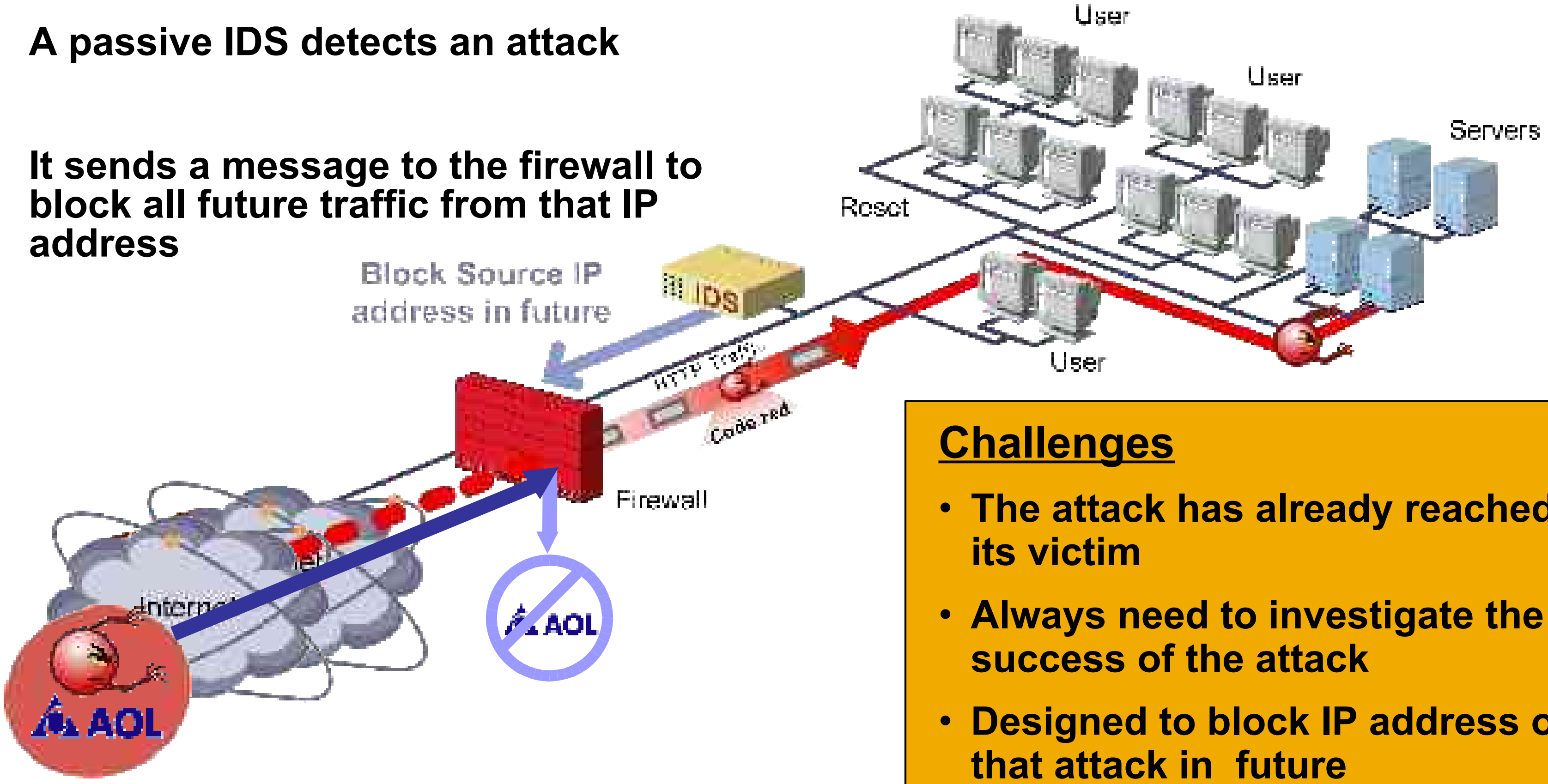
- **The attack has reached the victim**
- **Always need to investigate the success of the attack**
- **Only works for TCP connections**
- **Timing is almost impossible to get right**



Firewall Signaling

1. A passive IDS detects an attack

3. It sends a message to the firewall to block all future traffic from that IP address

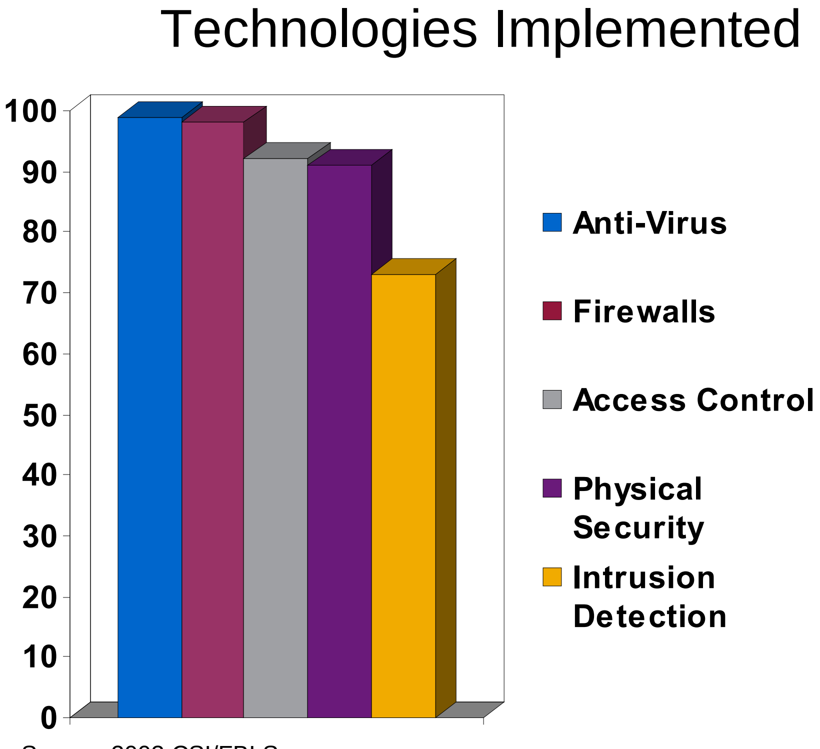


If attacker used or spoofed an AOL address, all future AOL traffic would be dropped

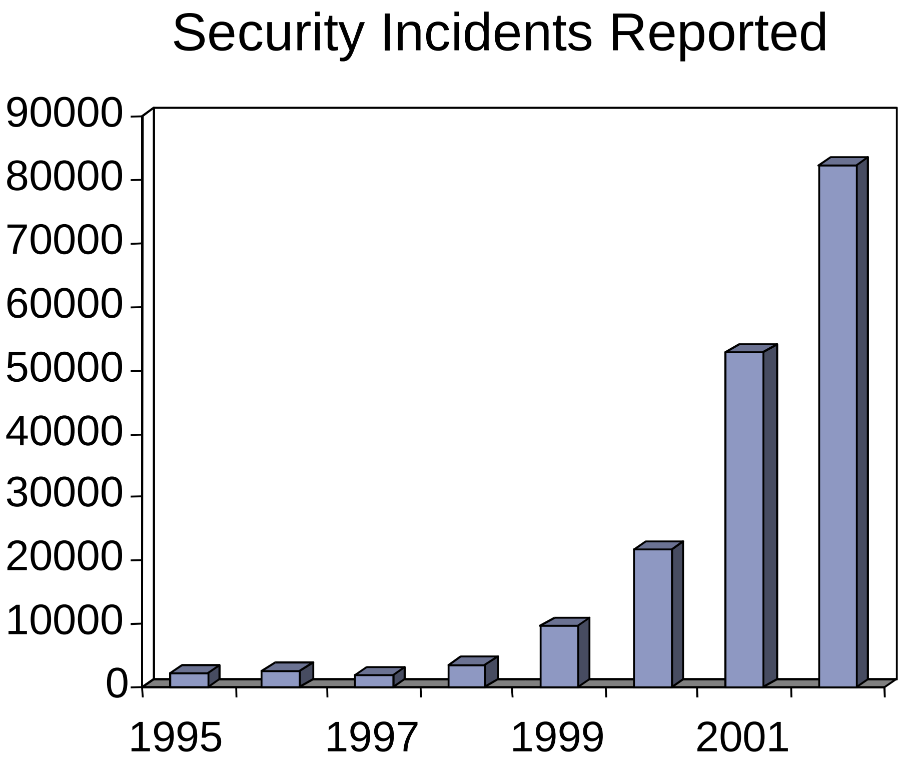
Challenges

- The attack has already reached its victim
- Always need to investigate the success of the attack
- Designed to block IP address of that attack in future
- Sets the system up for a Denial of Service Attack

Are These Layers Enough?



Source: 2003 CSI/FBI Survey



Source: CERT Coordination Center: 2002

If organizations have all of these security technologies deployed, why are security incidents on the rise?

Security Breaches Result in

- Loss of time spent investigating
- Loss of productivity, resulting from disruption in network services
- Loss of time and resources spent recovering
- Damage from the exploit

New Technologies

Intrusion Prevention Systems (IPS/IDP)

- IPS was specifically designed to prevent attacks against applications
  - Understand the protocols without implementing full client and server
  - Operates in-line to drop the malicious packet/connection

- Implements: protocol conformance + Stateful Signatures + other sophisticated detection mechanisms
  - Backdoor, Traffic Anomaly, Profile-Based, Many others…

New Technologies

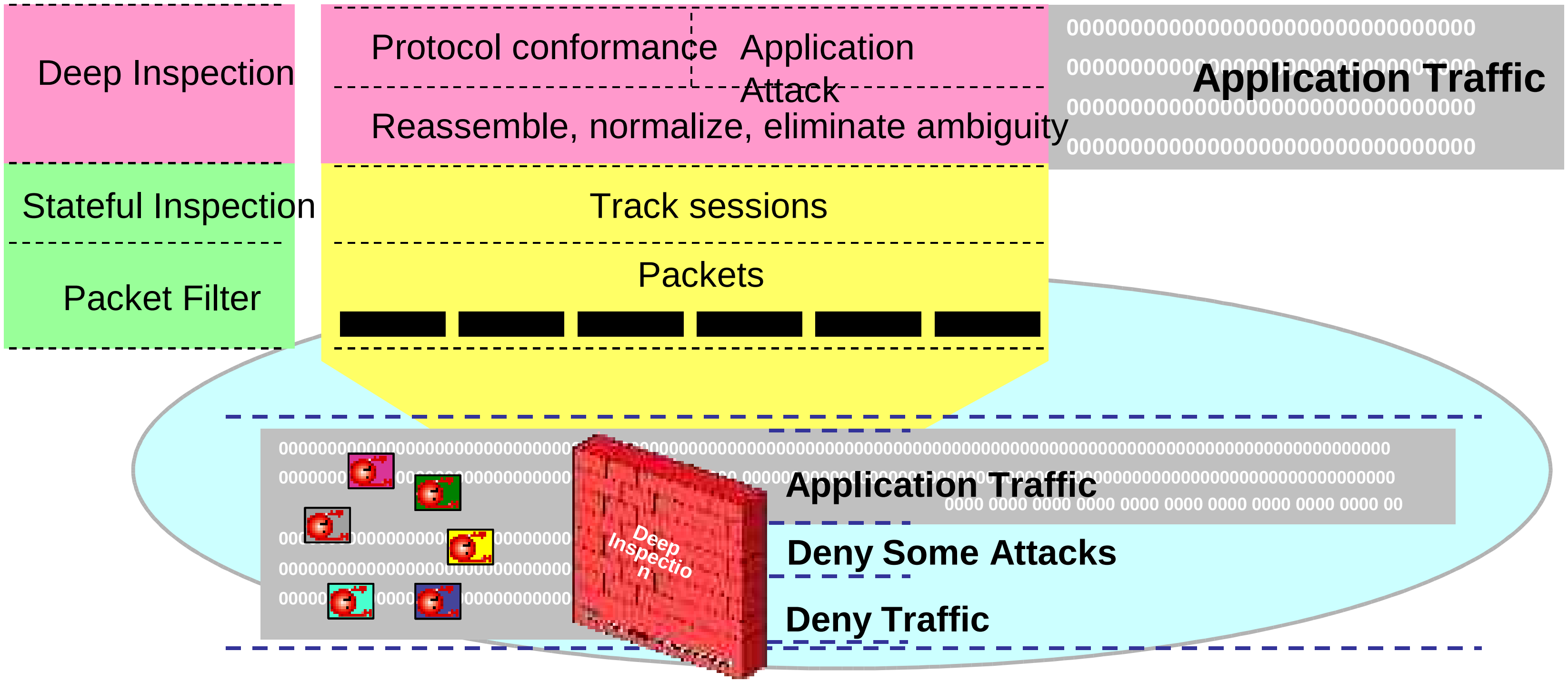
Deep Inspection

Application Security at the Gateway

- Builds on strengths of Stateful Inspection Firewalls and Intrusion Prevention Technology
  - Understand the protocols without having to implement full client and server
- Performs Protocol Conformance Verification and Attack Pattern Matches in relevant Service Fields
  - Supports Internet facing protocols (Web, e-mail, FTP, DNS)
  - Easy to add new protocols, Stateful Signatures
- Performance meets network requirements
- High-Availability

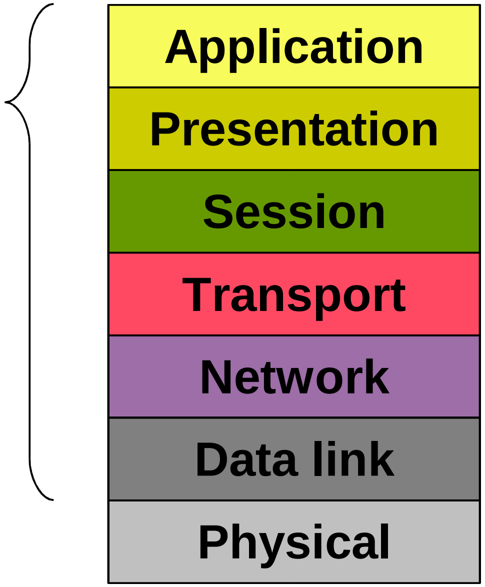
Deep Inspection

Security	+	Protects against network and many application attacks, both known and unknown – Internet facing protocols
High Performance	+	Meets requirements
Reliable Connectivity	+	Most products Supports HA
Ease of Use	+	Manage network and application protection



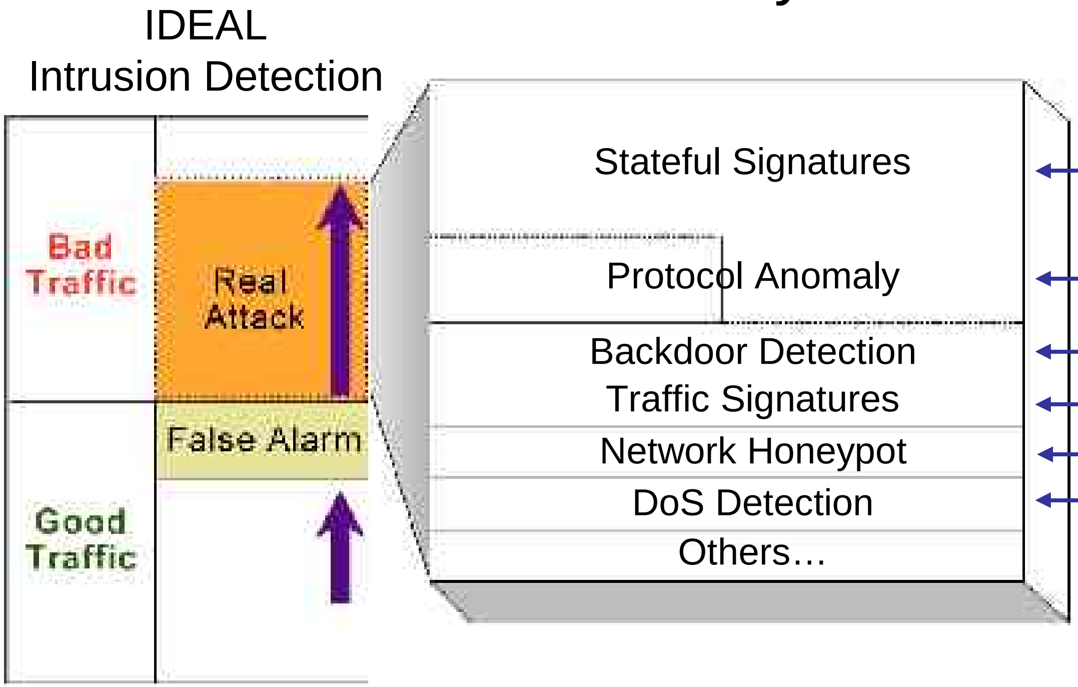
Application Level Protection

- IDP Complements your Firewall
  - Gives you control and visibility into network traffic from Layer 2-7
  - Blocks Application-layer based attacks that your firewall can't block
  - Prevents unwanted protocols from making connections on common ports
  - Policy-based rule-set with user-selected actions (allow, drop, log, etc…)



Maximizing Attack Detection

Using Multi-Method Attack Detection to identify all attacks



Stateful Signatures

Protocol Anomaly

Backdoor Detection

Traffic Signatures

Network Honeypot

DoS Detection

Others…

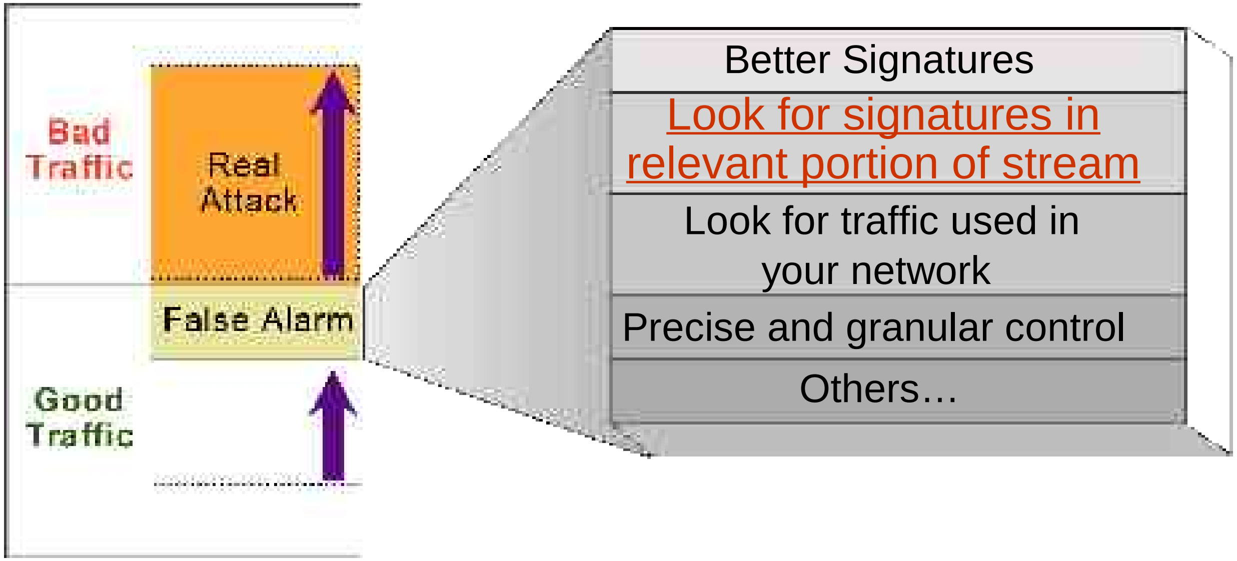
Examples

- Code Red
- Buffer overflows
- Back Orifice
- Port scans, network sweeps
- Script Kiddie Telnet root
- Invalid connections from multi-connection protocols

…While Minimizing False Alarms

Using Stateful Signatures with stream reassembly, normalization and regular expression support

IDEAL
Intrusion Detection



Better Signatures

Look for signatures in relevant portion of stream

Look for traffic used in your network

Precise and granular control

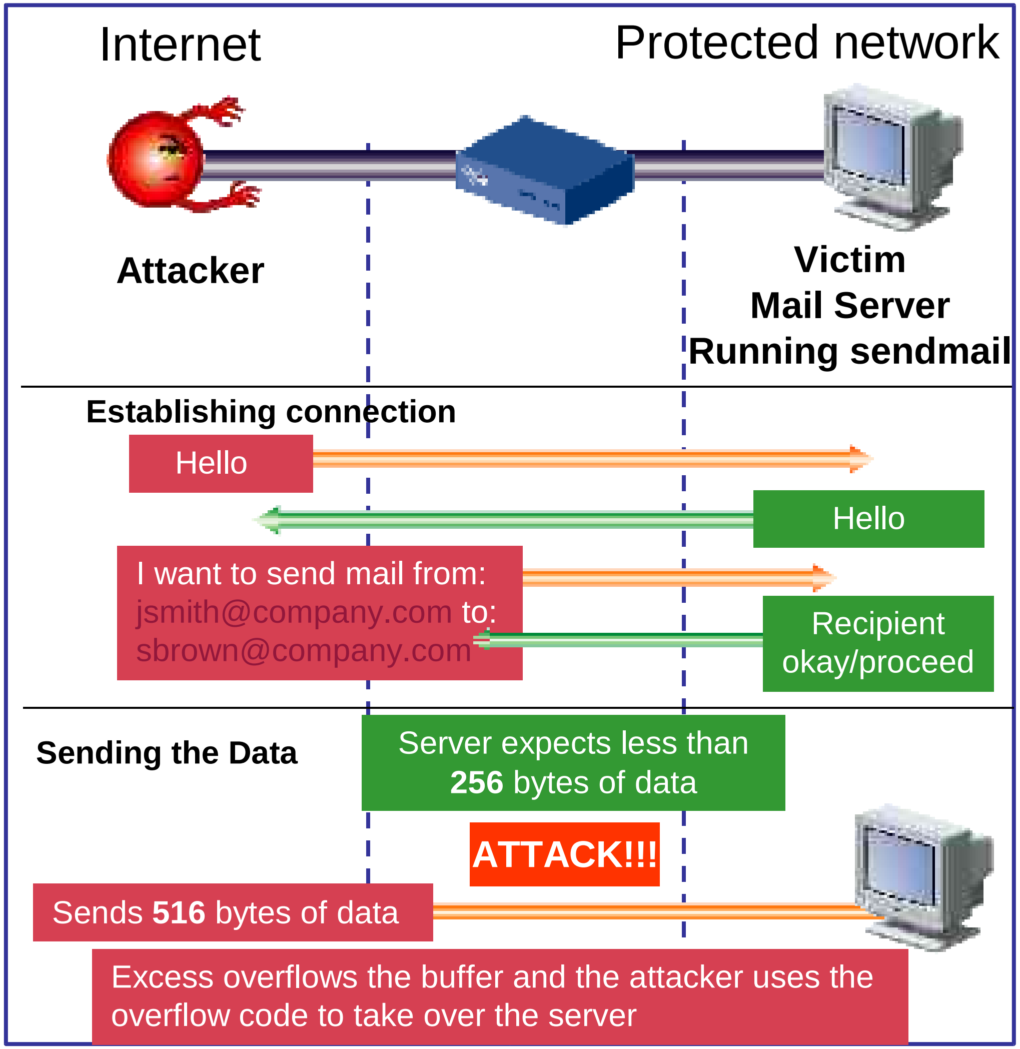
Others…

Application Specific Analysis: Protocol Conformance

Optimal detection method for custom and “day zero” (Exploit class) attacks

- Identifies traffic anomalies (i.e. specification non-conformance)
- Classifies anomalies based on their impact
- Treats high-impact anomalies as attacks

SendMail Example: Specific exploit doesn’t exist, but sendmail vulnerabilities could enable a buffer overflow attack to gain root access = Attacker gains complete control



Internet
Protected network
Attacker
Victim
Mail Server
Running sendmail
Establishing connection
Hello
Hello
I want to send mail from: jsmith@company.com to: sbrown@company.com
Recipient okay/proceed
Sending the Data
Server expects less than 256 bytes of data
ATTACK!!!
Sends 516 bytes of data
Excess overflows the buffer and the attacker uses the overflow code to take over the server

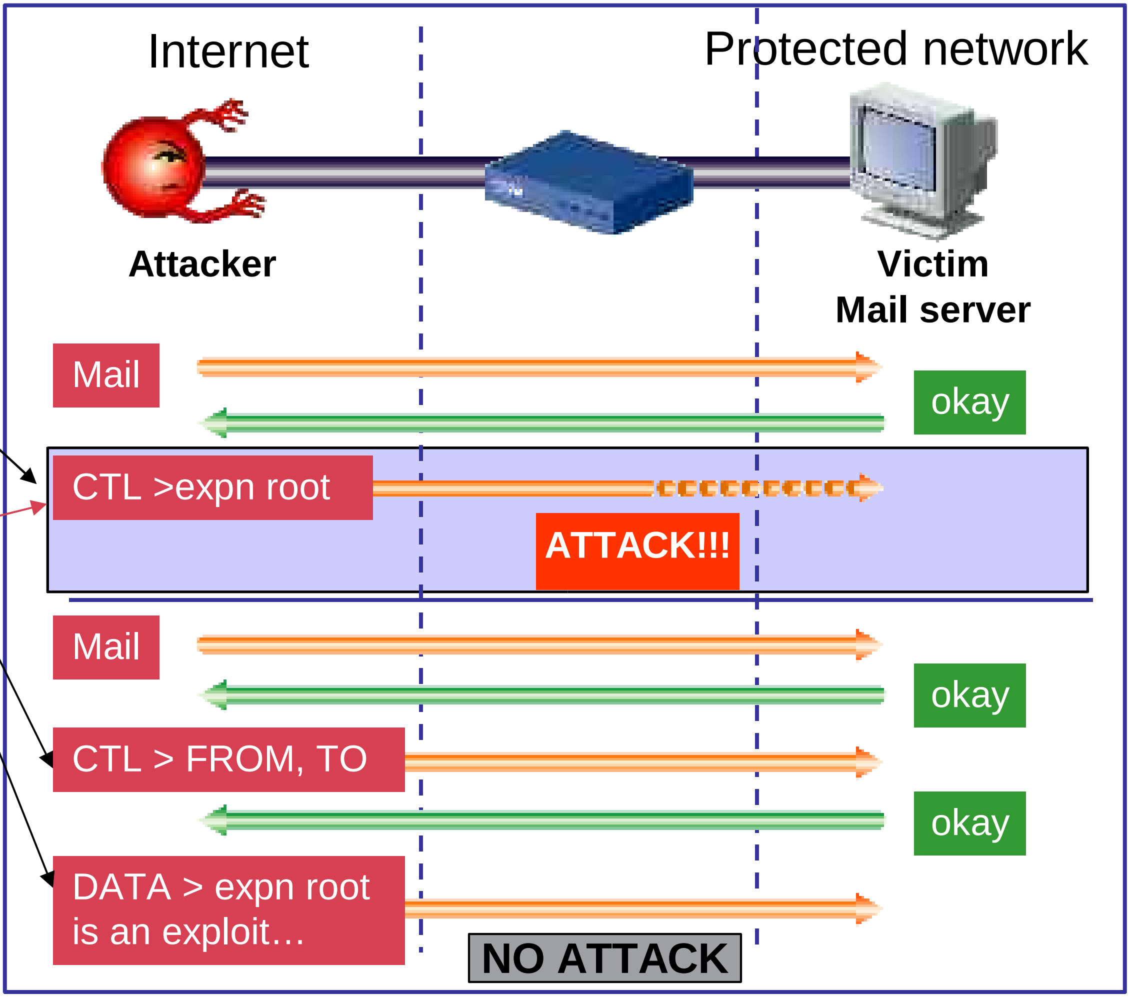
Application Specific Analysis:
Stateful Signatures

Optimal for Well known Attacks (Specific Exploits)

Looks for attack pattern in <u>relevant service fields</u> and matches where the attack can be perpetrated

Example: Attacker connects to Victim Mail server. Exposes mailing list using "expn root" command during <u>control portion</u> of session.

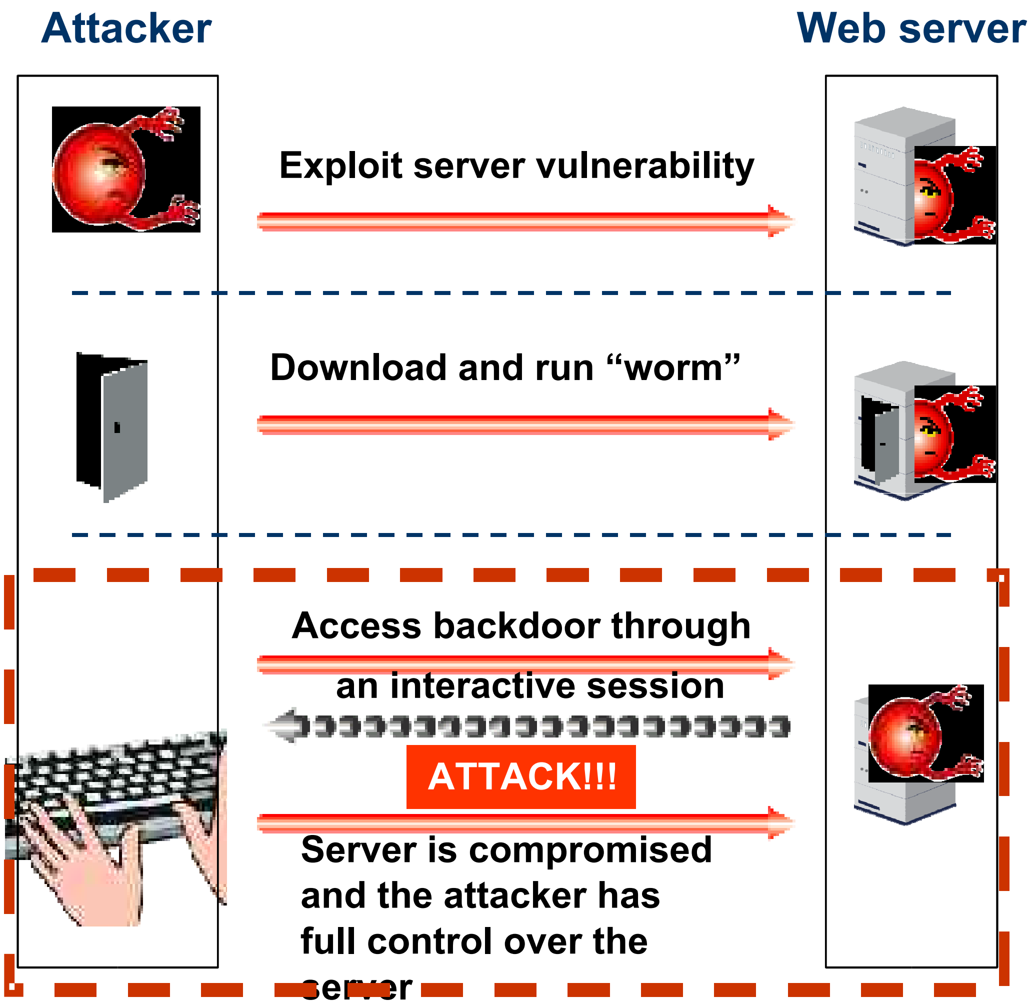
Only looks for match during the control portion of the session- where the attack is perpetrated



Backdoor Detection

The approach to detect Worms and Trojans

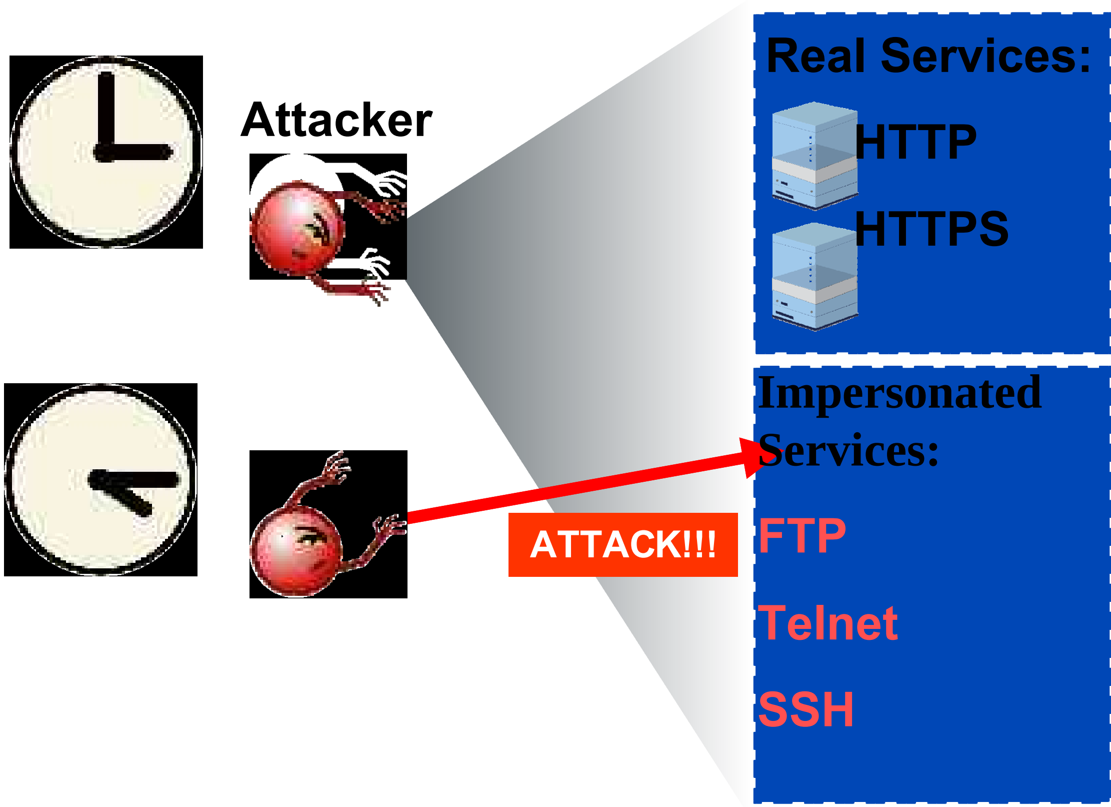
- Looks for interactive traffic
- Detects unauthorized interactive traffic, based on what the administrator defines is allowed.
- Detects virtually any backdoor, even if the traffic is encrypted and the protocol is unknown.


Attacker
Web server
Exploit server vulnerability
Download and run "worm"
Access backdoor through an interactive session
ATTACK!!!
Server is compromised and the attacker has full control over the server

Network Honeypot

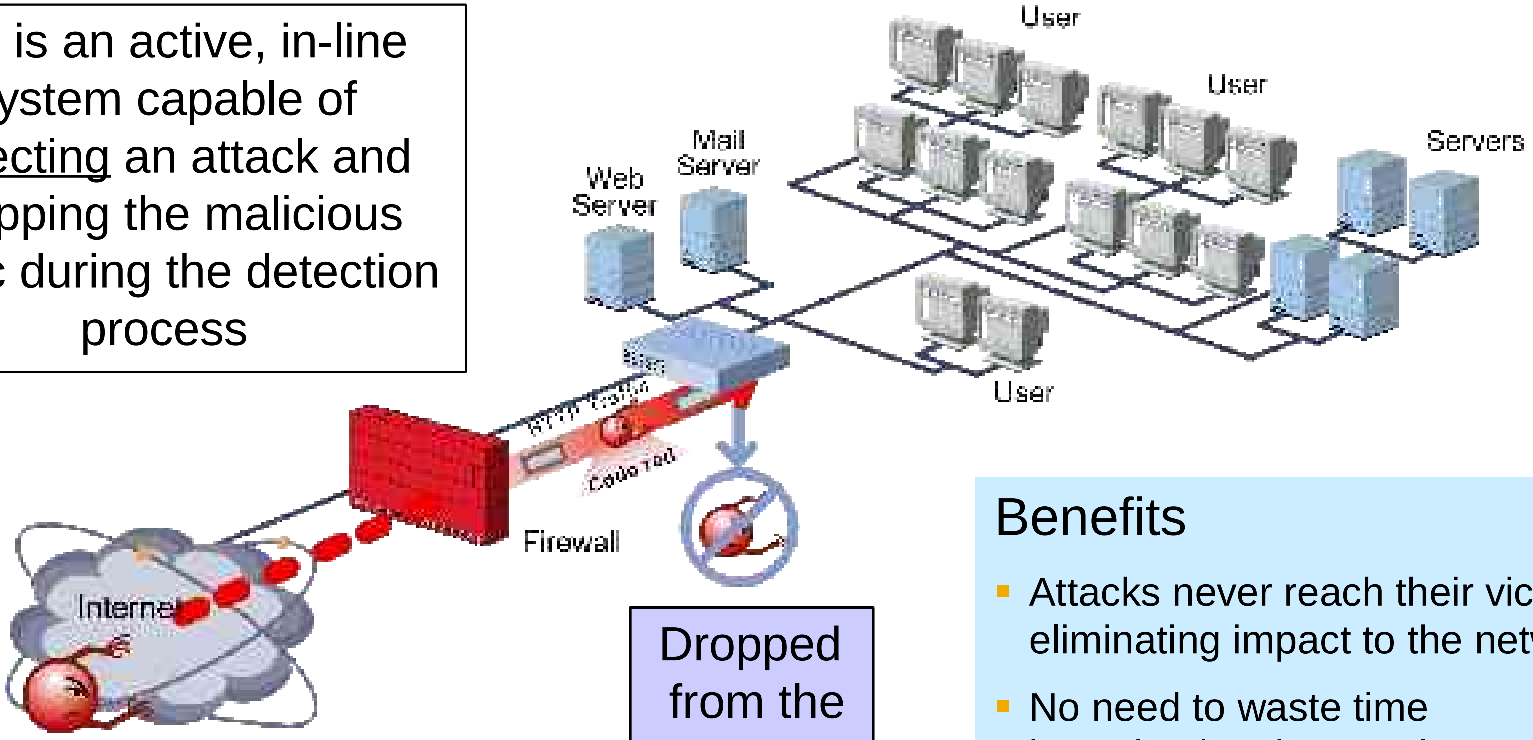
A Good Way to Reduce the "Noise" of Script Kiddies

- Impersonates services, sending fake information in response to scans to try an entice attackers to access the non-existent services.
- There is no reason for legitimate traffic to access these resources because they don't exist, so any attempt to connect constitutes an attack.



Active Intrusion Detection and Prevention

IDP is an active, in-line system capable of detecting an attack and dropping the malicious traffic during the detection process



Dropped from the network

Benefits

- Attacks never reach their victim, eliminating impact to the network
- No need to waste time investigating the attack
- Works for all traffic (IP, TCP, UDP, etc.)
- Drops only the offending traffic

Thank You