radware

# AGENDA

The Evolving Threat Landscape

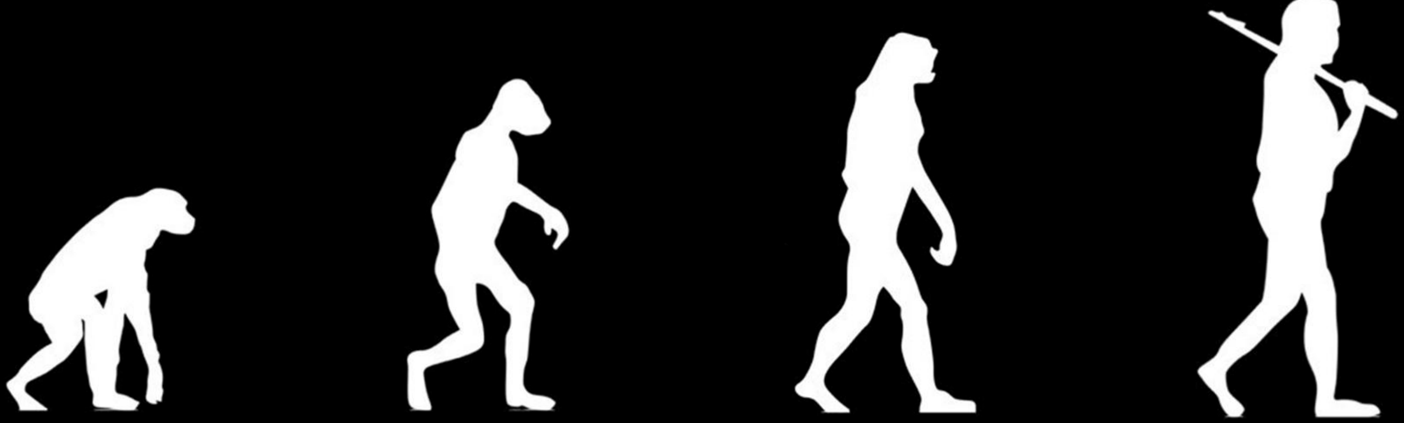
Anatomy of an Attack

Securing Tomorrow’s Perimeter

radware

AGENDA

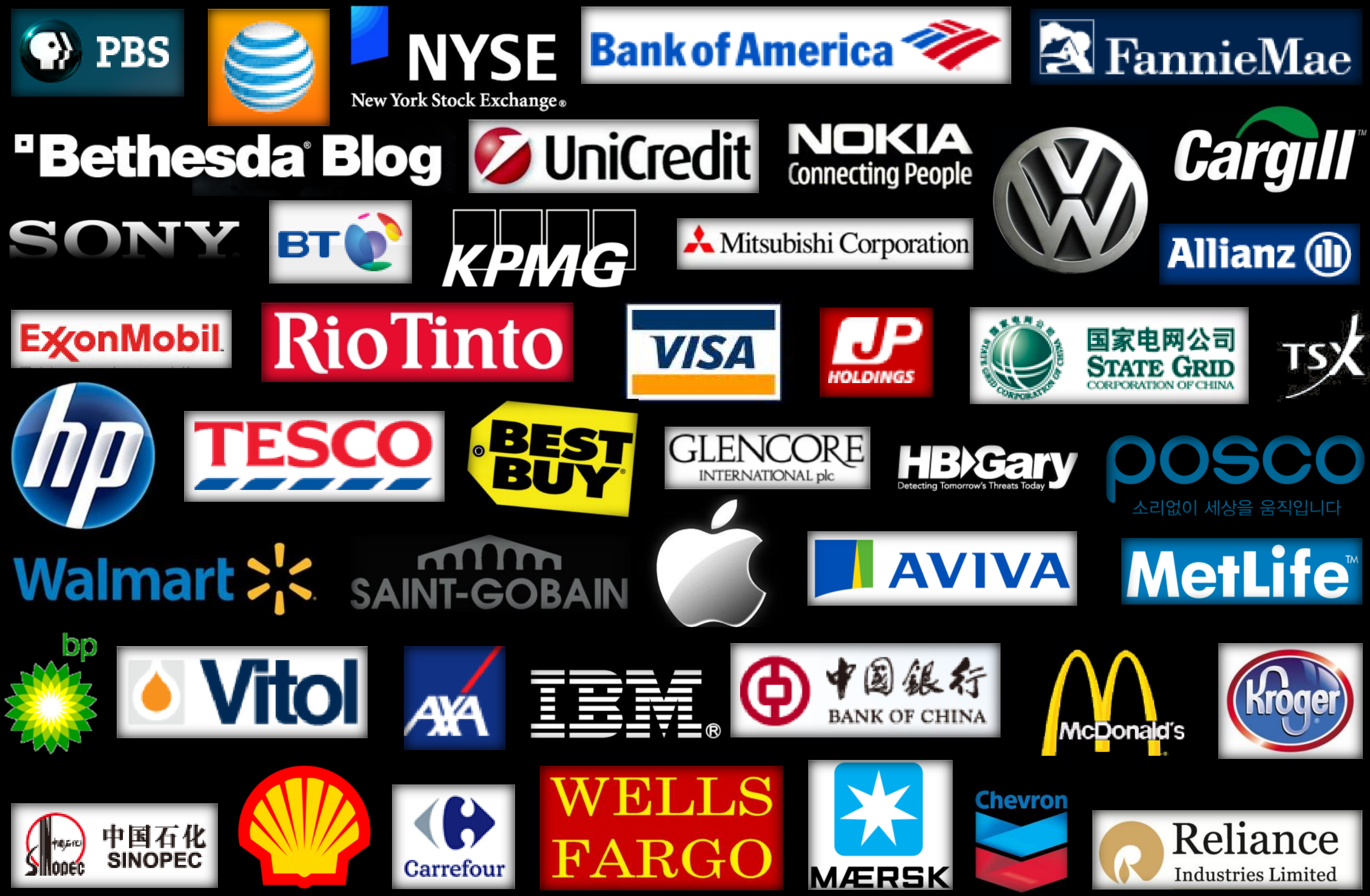
- The Evolving Threat Landscape



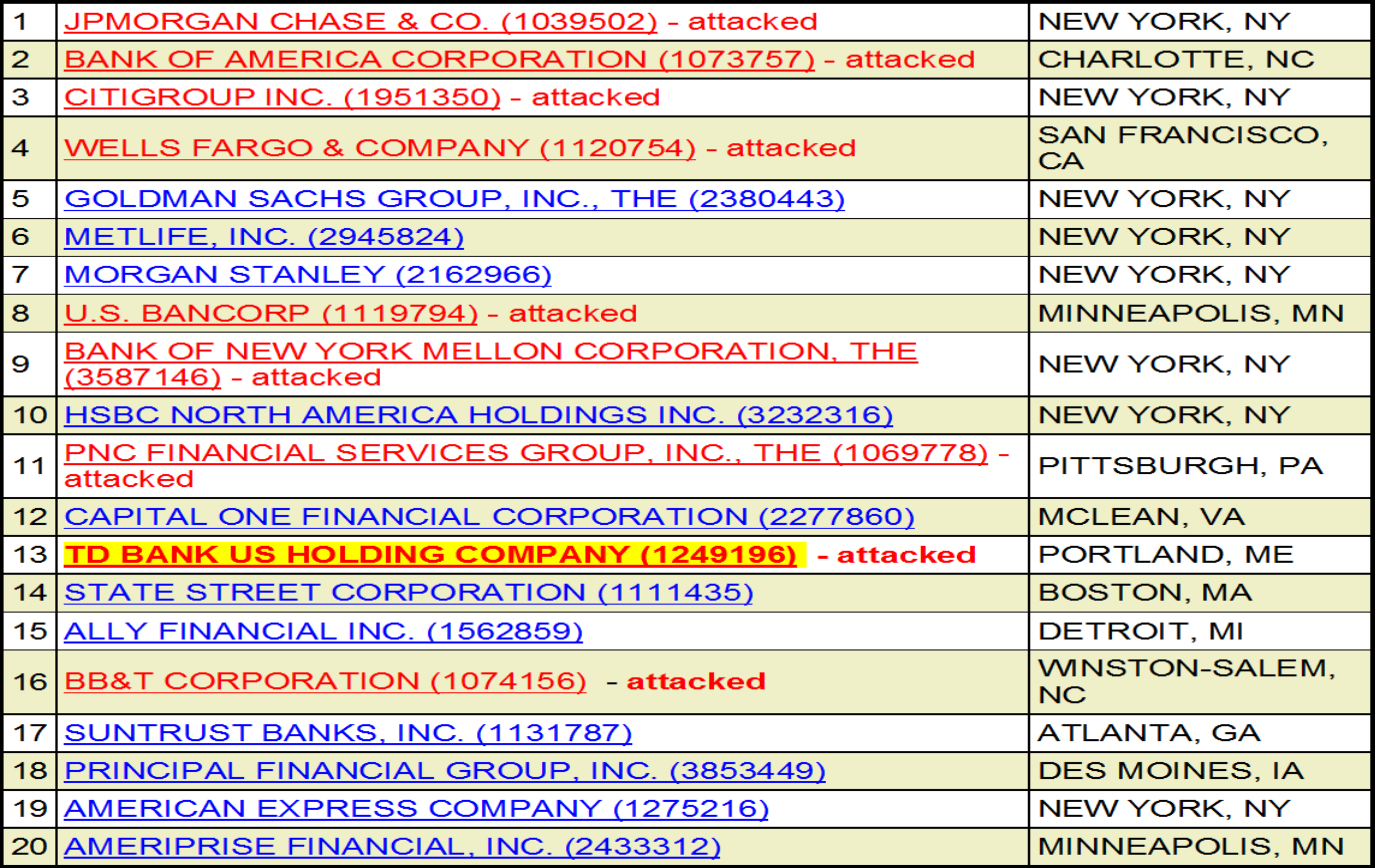
secureworld expo
is your world secure?

radware

# More Attacks. More Often.

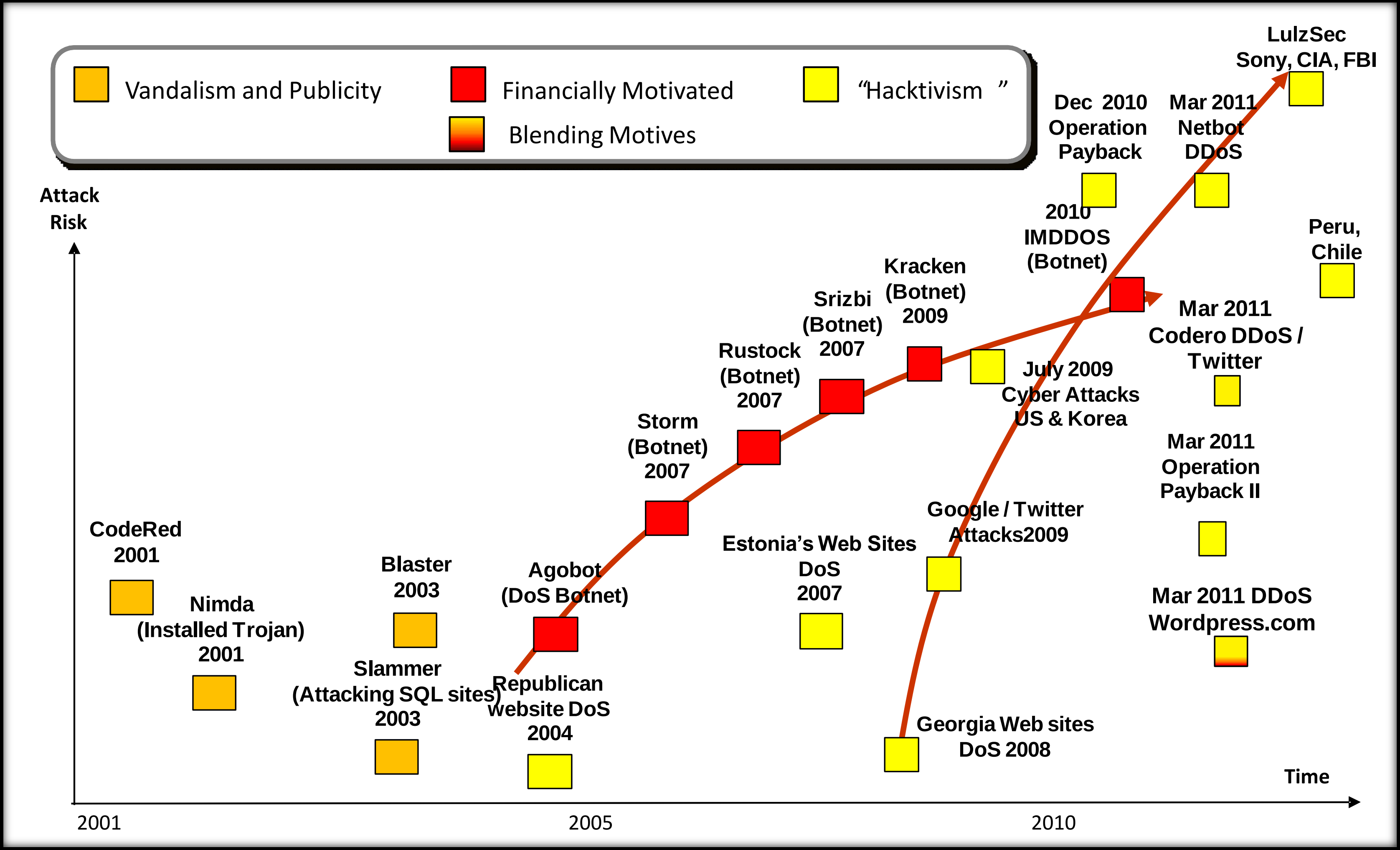


# Operation Abibal



| | | |
|---|---|---|
| 1 | JPMORGAN CHASE & CO. (1039502) - attacked | NEW YORK, NY |
| 2 | BANK OF AMERICA CORPORATION (1073757) - attacked | CHARLOTTE, NC |
| 3 | CITIGROUP INC. (1951350) - attacked | NEW YORK, NY |
| 4 | WELLS FARGO & COMPANY (1120754) - attacked | SAN FRANCISCO, CA |
| 5 | GOLDMAN SACHS GROUP, INC., THE (2380443) | NEW YORK, NY |
| 6 | METLIFE, INC. (2945824) | NEW YORK, NY |
| 7 | MORGAN STANLEY (2162966) | NEW YORK, NY |
| 8 | U.S. BANCORP (1119794) - attacked | MINNEAPOLIS, MN |
| 9 | BANK OF NEW YORK MELLON CORPORATION, THE (3587146) - attacked | NEW YORK, NY |
| 10 | HSBC NORTH AMERICA HOLDINGS INC. (3232316) | NEW YORK, NY |
| 11 | PNC FINANCIAL SERVICES GROUP, INC., THE (1069778) - attacked | PITTSBURGH, PA |
| 12 | CAPITAL ONE FINANCIAL CORPORATION (2277860) | MCLEAN, VA |
| 13 | **TD BANK US HOLDING COMPANY (1249196) - attacked** | PORTLAND, ME |
| 14 | STATE STREET CORPORATION (1111435) | BOSTON, MA |
| 15 | ALLY FINANCIAL INC. (1562859) | DETROIT, MI |
| 16 | BB&T CORPORATION (1074156) - **attacked** | WINSTON-SALEM, NC |
| 17 | SUNTRUST BANKS, INC. (1131787) | ATLANTA, GA |
| 18 | PRINCIPAL FINANCIAL GROUP, INC. (3853449) | DES MOINES, IA |
| 19 | AMERICAN EXPRESS COMPANY (1275216) | NEW YORK, NY |
| 20 | AMERIPRISE FINANCIAL, INC. (2433312) | MINNEAPOLIS, MN |

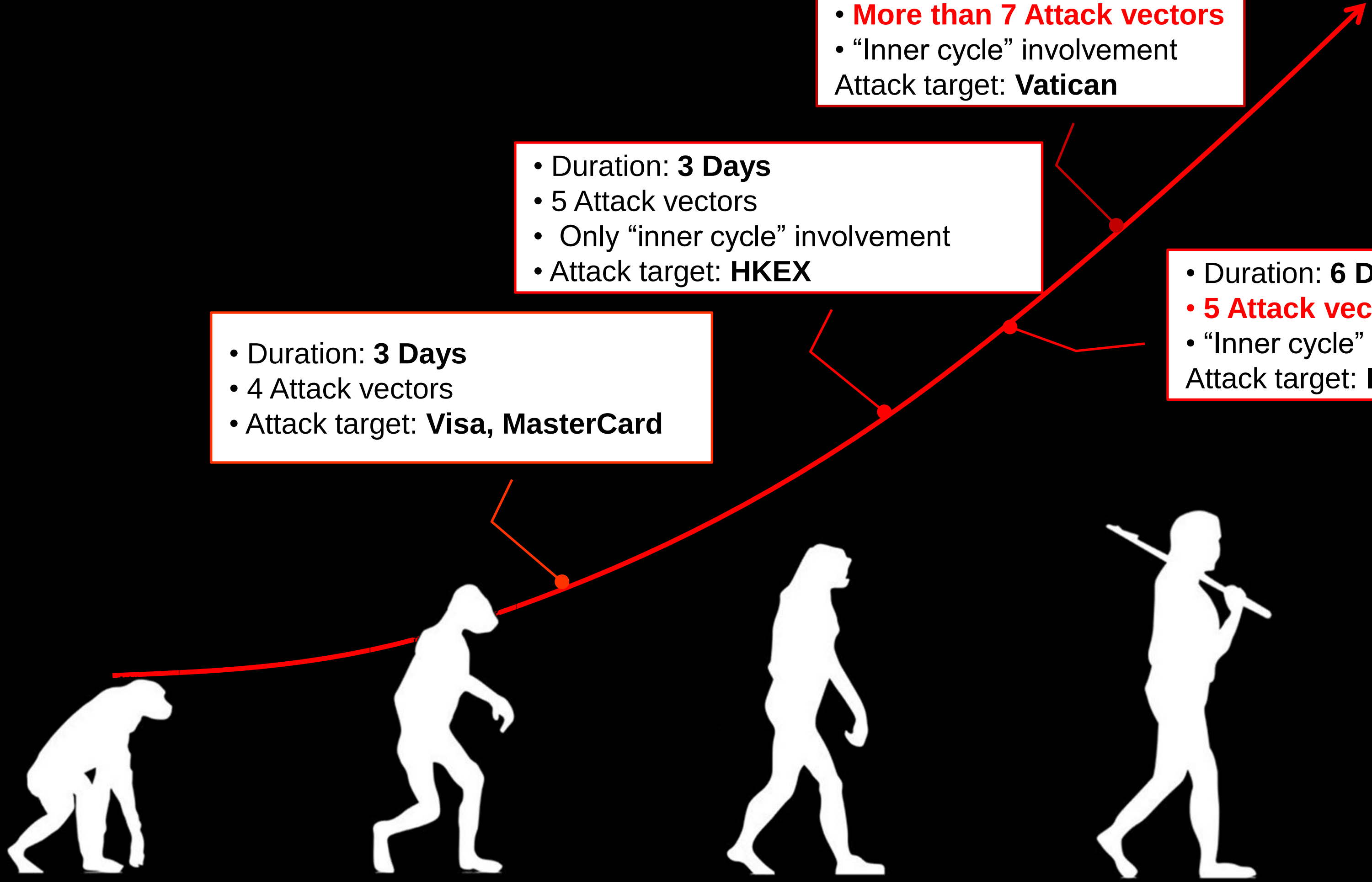
# Attack Motivation



# Hacktivism - Becomes More Campaign-APT Oriented

- **Complex**: More than seven different attack vectors at once
- **Blending:** both network and application attacks
- **Targeteering:** Select the most appropriate target, attack tools,
- **Resourcing:** Advertise, invite, coerce anyone capable …
- **Testing:** Perform short “proof-firing” prior to the attack
- **Timeline:** Establish the most painful time period for his victim

# Hacktivism - Becomes More Campaign-APT Oriented



- Duration: **3 Days**
- 4 Attack vectors
- Attack target: **Visa, MasterCard**

- Duration: **3 Days**
- 5 Attack vectors
- Only “inner cycle” involvement
- Attack target: **HKEX**

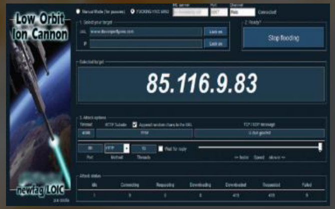
- Duration: **6 Days**
- **5 Attack vectors**
- “Inner cycle” involvement

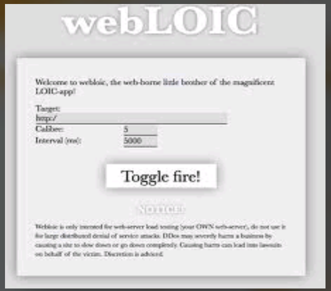
Attack target: **Israeli sites**

- Duration: **20 Days**
- **More than 7 Attack vectors**
- “Inner cycle” involvement

Attack target: **Vatican**

# The Anonymous Arms Race




webLOIC

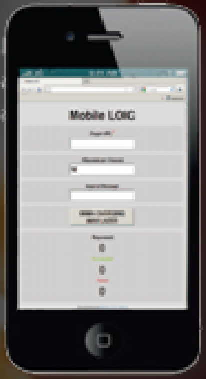
Welcome to webloic, the web-borne little brother of the magnificent LOIC-app!

Target: http:/
Calibre: 5
Interval (ms): 5000

Toggle fire!

Notice

Webloic is only intented for web-server load testing (your OWN web-server), do not use it for large distributed denial of service attacks. DDos may severly harm a business by causing a site to slow down or go down completely. Causing harm can lead into lawsuits on behalf of the victim. Discretion is adviced.



| Network | Application Flood | Low & Slow | Vulnerability Based |
|---|---|---|---|
| UDP Floods | Dynamic HTTP | RUDY | Intrusion Attempts |
| SYN Floods | HTTPS Floods | Slowloris | SQL Injection |
| Fragmented Floods | | Pyloris | #refref |
| FIN + ACK | | | xerex |

# 2012 Security Report

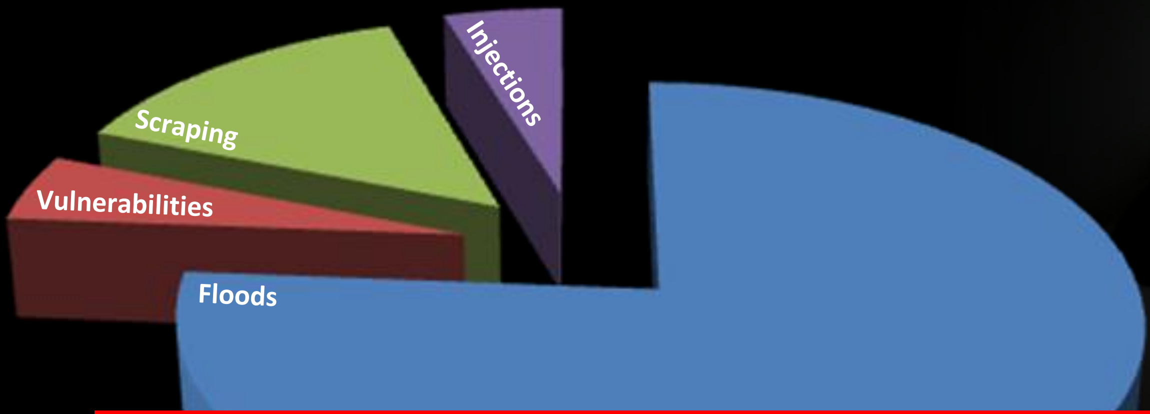
Radware Application Delivery, Security, Availability and Performance Optimization Solutions
File Edit View History Bookmarks Window Help
http://www.radware.com/
RSS
Google
Contact Us | How To Buy | Worldwide | Careers | My Account
SEARCH
radware
Home
Solutions
Products
Support
Partner
Resources
Company
News & Events
Community
radware ert
New Cyber Attacks and Tools Revealed!
Server-based botnets, HTTP layer, APTs lead the list
Get the 2012 Global Application and Network Security Report
Newest DDoS Attack Trends
Cisco ACE Buyback Program
Gartner ADC MQ

radware

# AGENDA

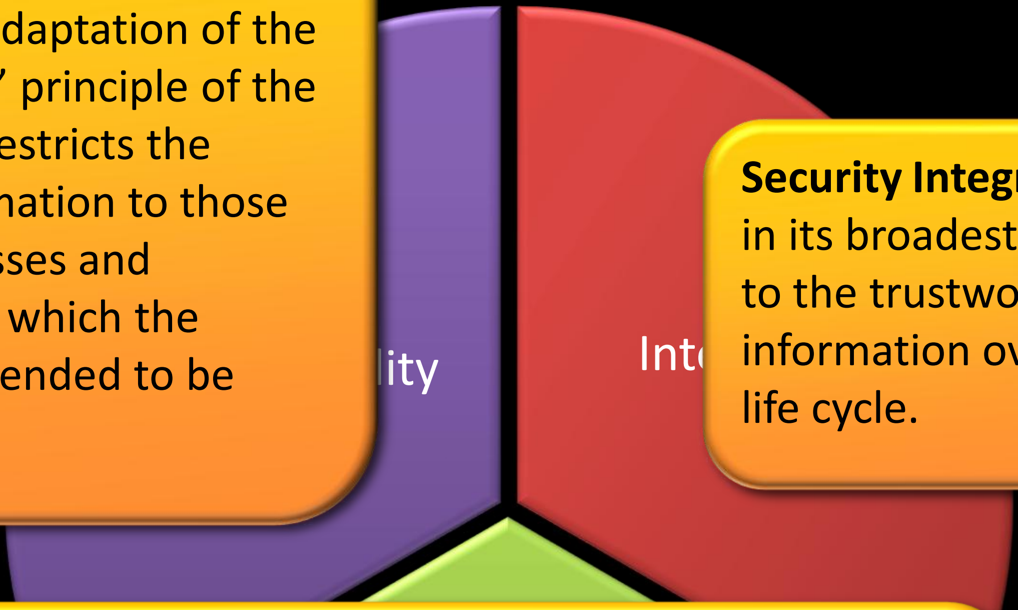
- ► Anatomy of an Attack
- The Evolving Threat Landscape
- Securing Tomorrow’s Perimeter

# Example Stock Exchange Attack



| Attack Vector | Time Stamp | Attack Peak |
|---|---|---|
| Fragmented UDP Flood | 1:00 AM | 95 Mbps<br>10K PPS |
| LOIC UDP | 4:00 AM and 8:00 PM - 11:00 PM | 50 Mbps<br>5K PPS |
| TCP SYN Flood | 1:40 PM | 13.6 Mbps<br>24K PPS |
| R.U.D.Y | 4:00 PM | 2.1 Mbps<br>0.7K PPS |
| LOIC TCP | 11:00 PM - 3:30 AM | 500 Kbps<br>0.2K PPS |
| Mobile LOIC | 6:00 PM- 8:30 PM | 86 Kbps<br>13 PPS |
| #RefRef | 9:45 PM | Few packets |

# The Security Trinity



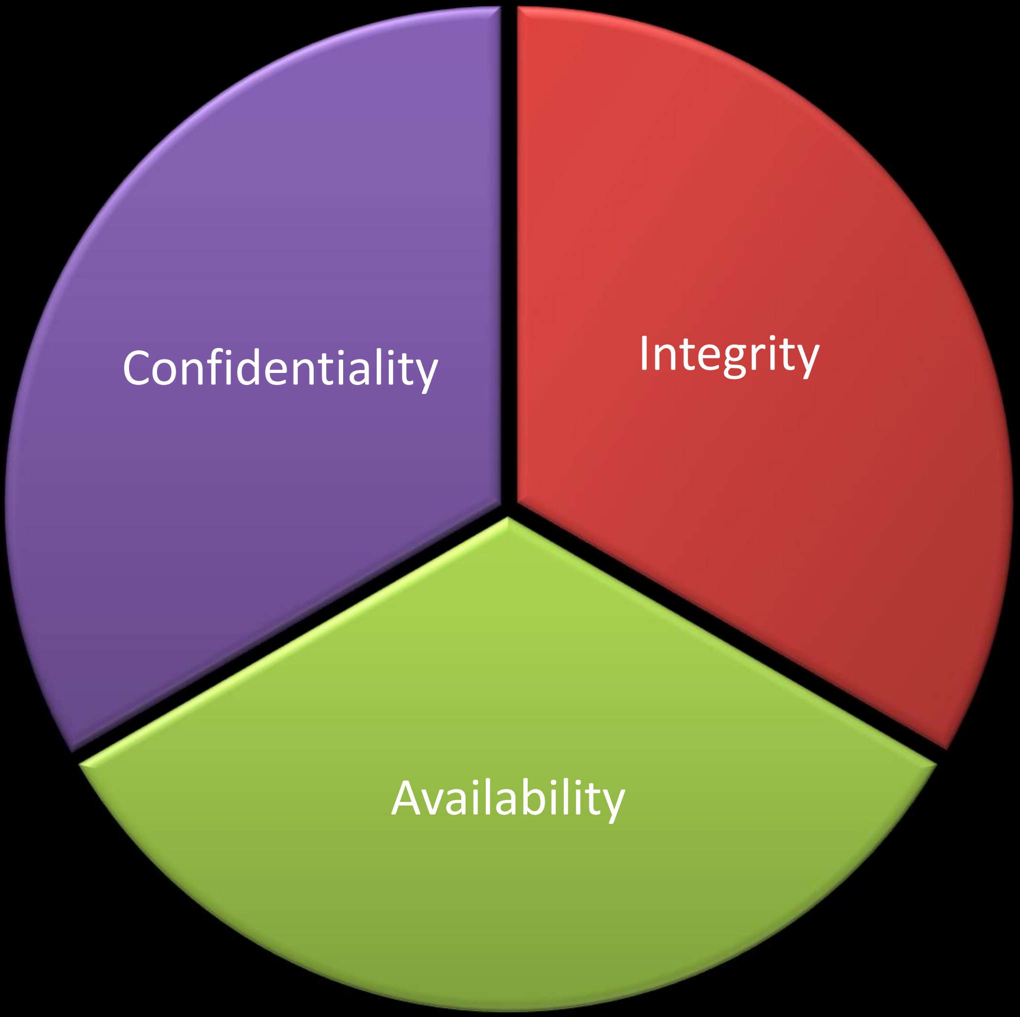
**Security Confidentiality**, a mainstream adaptation of the “need to know” principle of the military ethic, restricts the access of information to those systems, processes and recipients from which the content was intended to be exposed.

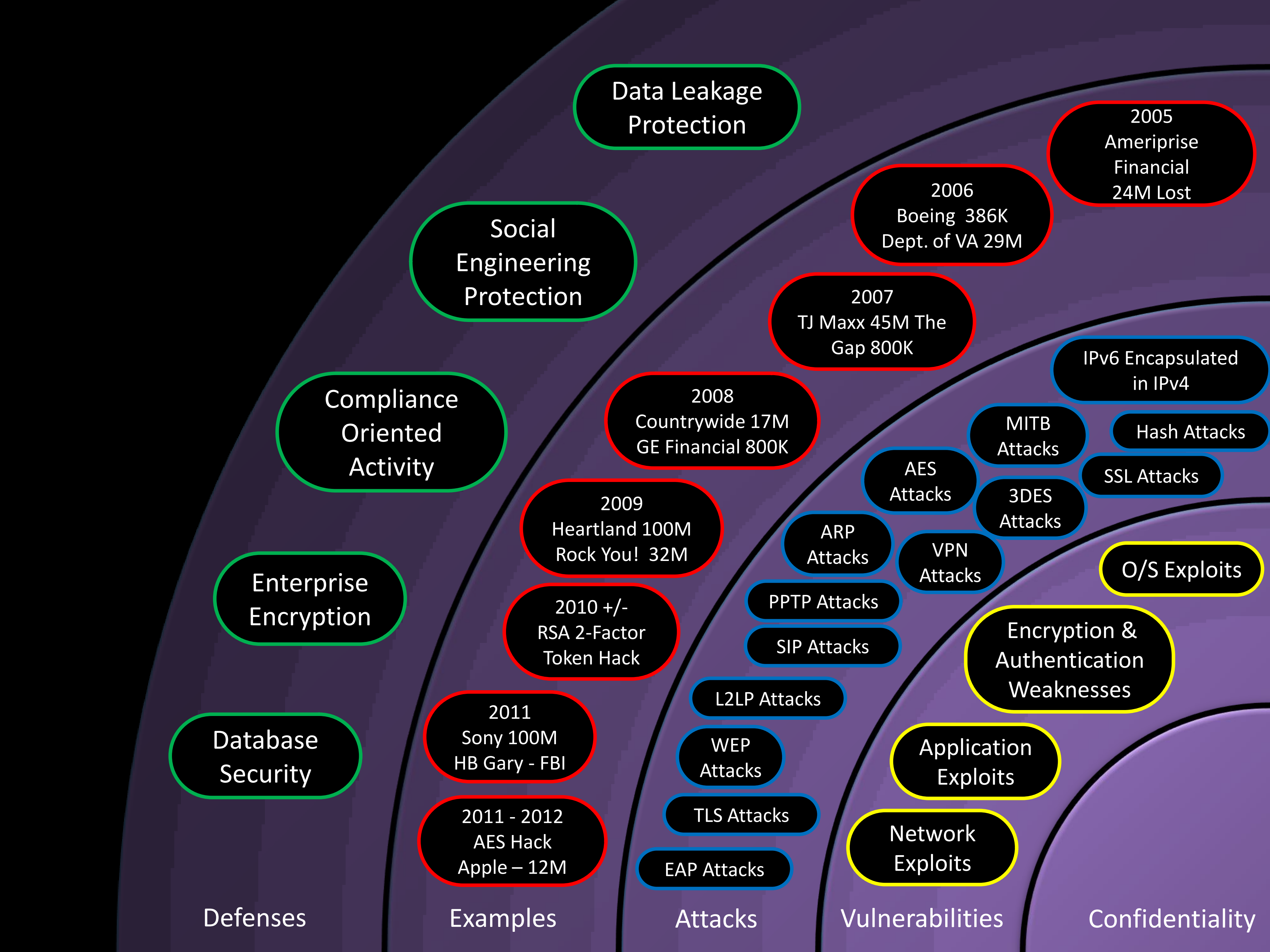
**Security Integrity**
in its broadest meaning refers to the trustworthiness of information over its entire life cycle.

**Security Availability**
is a characteristic that distinguishes information objects that have signaling and self-sustaining processes from those that do not, either because such functions have ceased (outage, an attack), or else because they lack such functions .

radware

# The Security Trinity





Data Leakage Protection

Social Engineering Protection

Compliance Oriented Activity

Enterprise Encryption

Database Security

Defenses

2005 Ameriprise Financial 24M Lost

2006 Boeing 386K Dept. of VA 29M

2007 TJ Maxx 45M The Gap 800K

2008 Countrywide 17M GE Financial 800K

2009 Heartland 100M Rock You! 32M

2010 +/- RSA 2-Factor Token Hack

2011 Sony 100M HB Gary - FBI

2011 - 2012 AES Hack Apple – 12M

Examples

IPv6 Encapsulated in IPv4

MITB Attacks

Hash Attacks

AES Attacks

SSL Attacks

3DES Attacks

ARP Attacks

VPN Attacks

PPTP Attacks

SIP Attacks

L2LP Attacks

WEP Attacks

TLS Attacks

EAP Attacks

Attacks

O/S Exploits

Encryption & Authentication Weaknesses

Application Exploits

Network Exploits

Vulnerabilities

Confidentiality

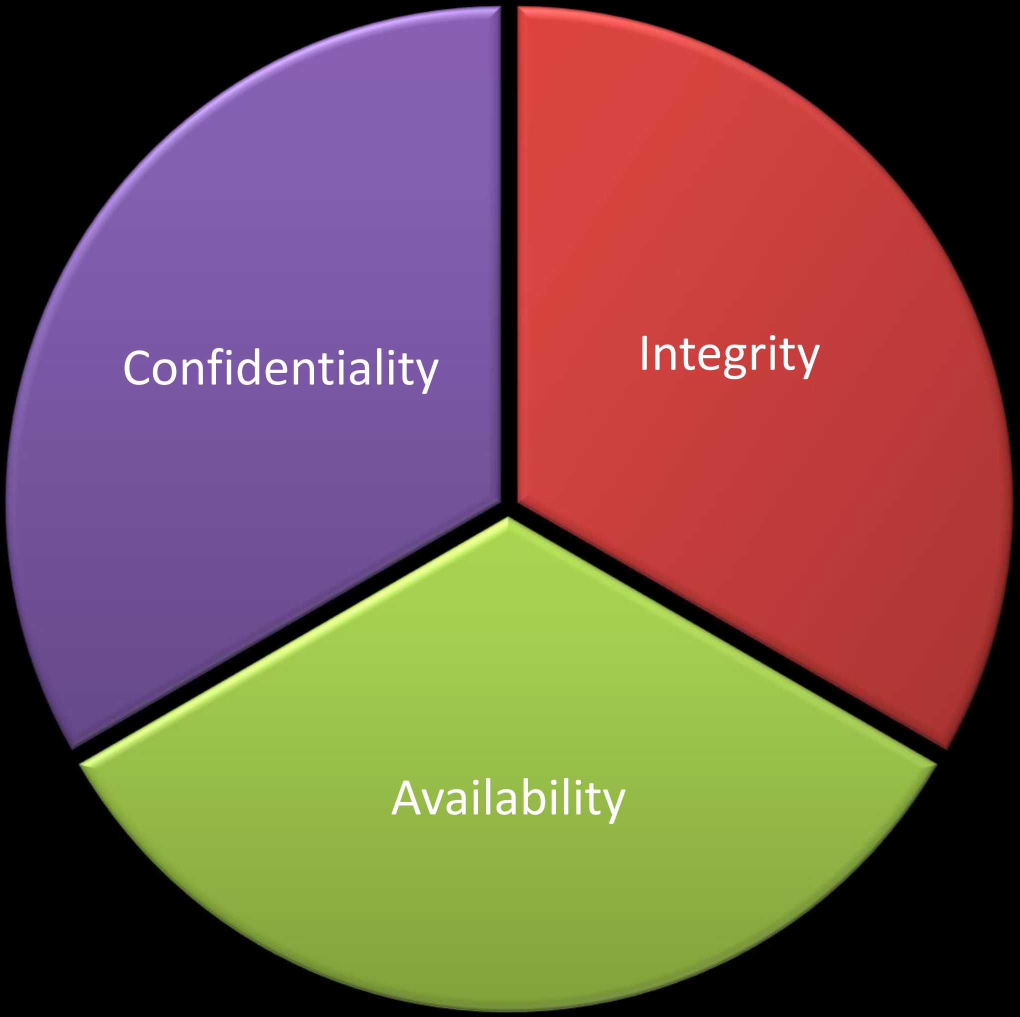
# The Security Trinity

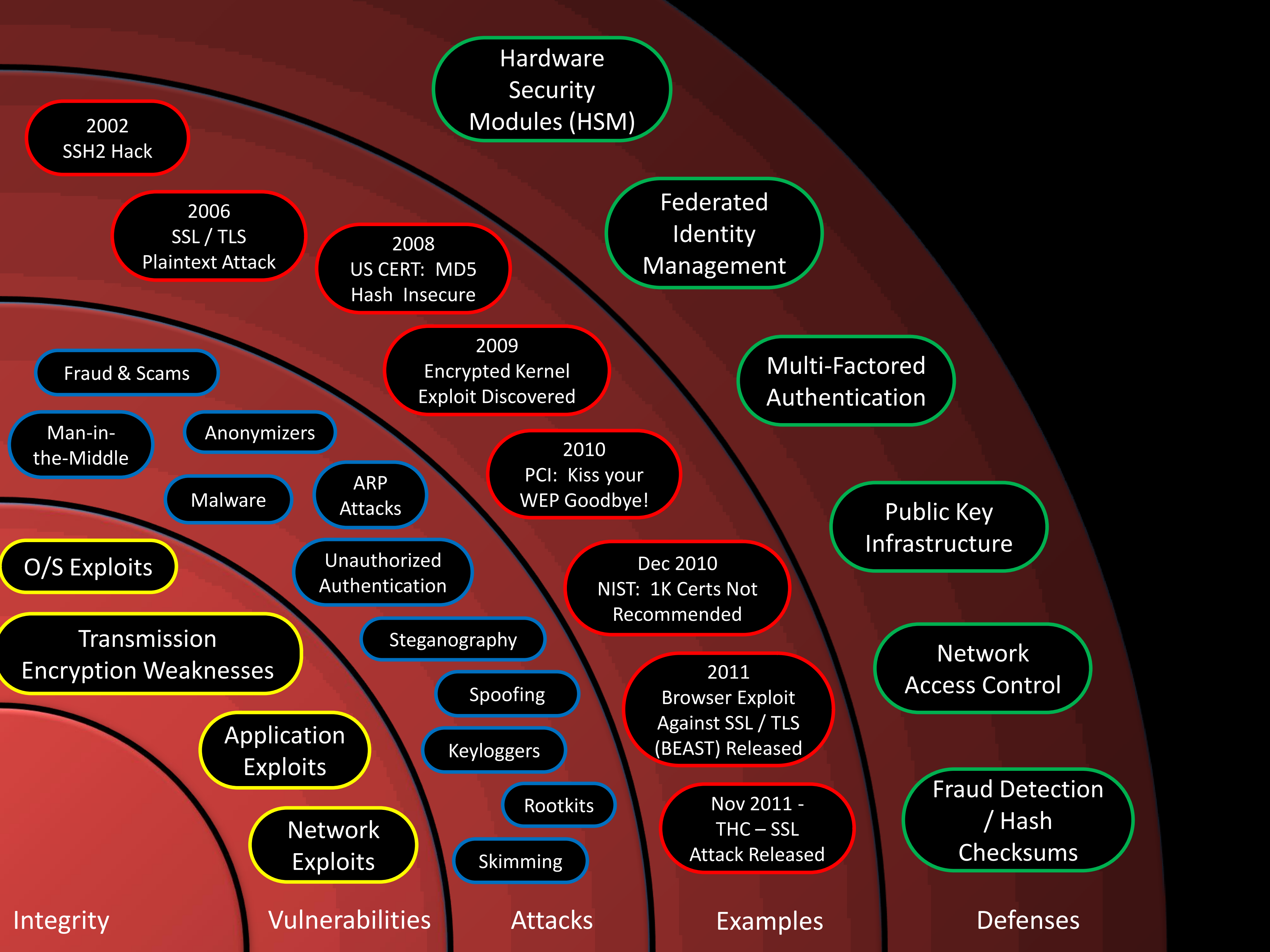
Confidentiality

Integrity

Availability

# The Security Trinity





Integrity

Vulnerabilities

O/S Exploits

Transmission Encryption Weaknesses

Application Exploits

Network Exploits

Attacks

Fraud & Scams

Man-in-the-Middle

Anonymizers

Malware

ARP Attacks

Unauthorized Authentication

Steganography

Spoofing

Keyloggers

Rootkits

Skimming

Examples

2002 SSH2 Hack

2006 SSL / TLS Plaintext Attack

2008 US CERT: MD5 Hash Insecure

2009 Encrypted Kernel Exploit Discovered

2010 PCI: Kiss your WEP Goodbye!

Dec 2010 NIST: 1K Certs Not Recommended

2011 Browser Exploit Against SSL / TLS (BEAST) Released

Nov 2011 - THC – SSL Attack Released

Defenses

Hardware Security Modules (HSM)

Federated Identity Management

Multi-Factored Authentication

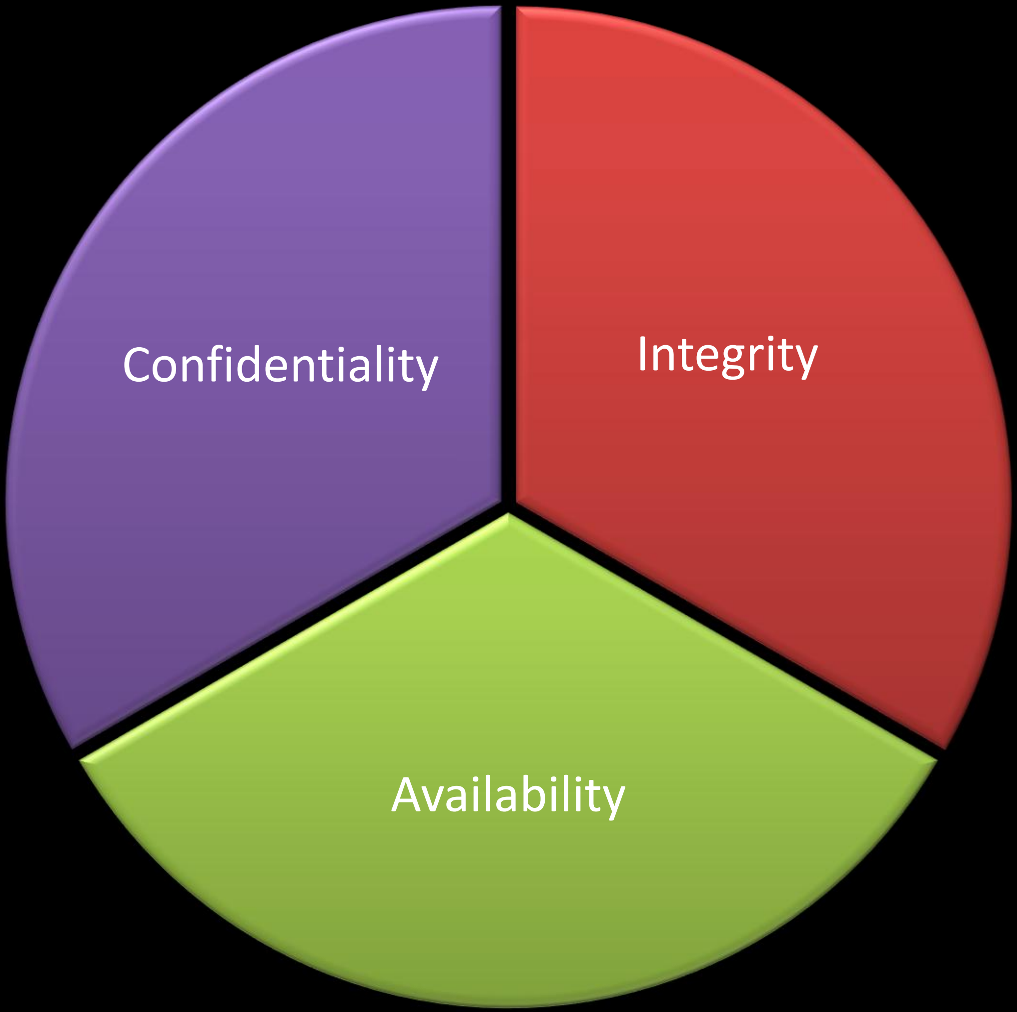
Public Key Infrastructure

Network Access Control

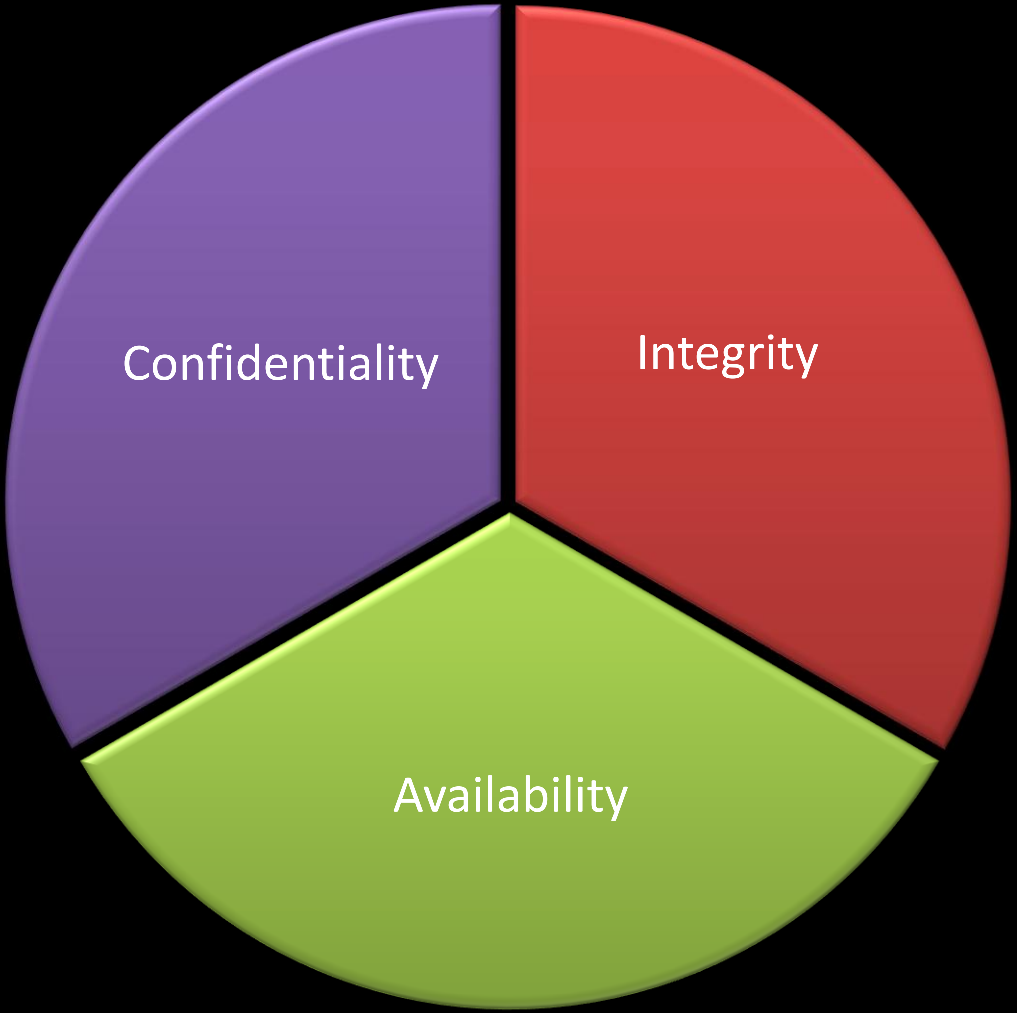
Fraud Detection / Hash Checksums

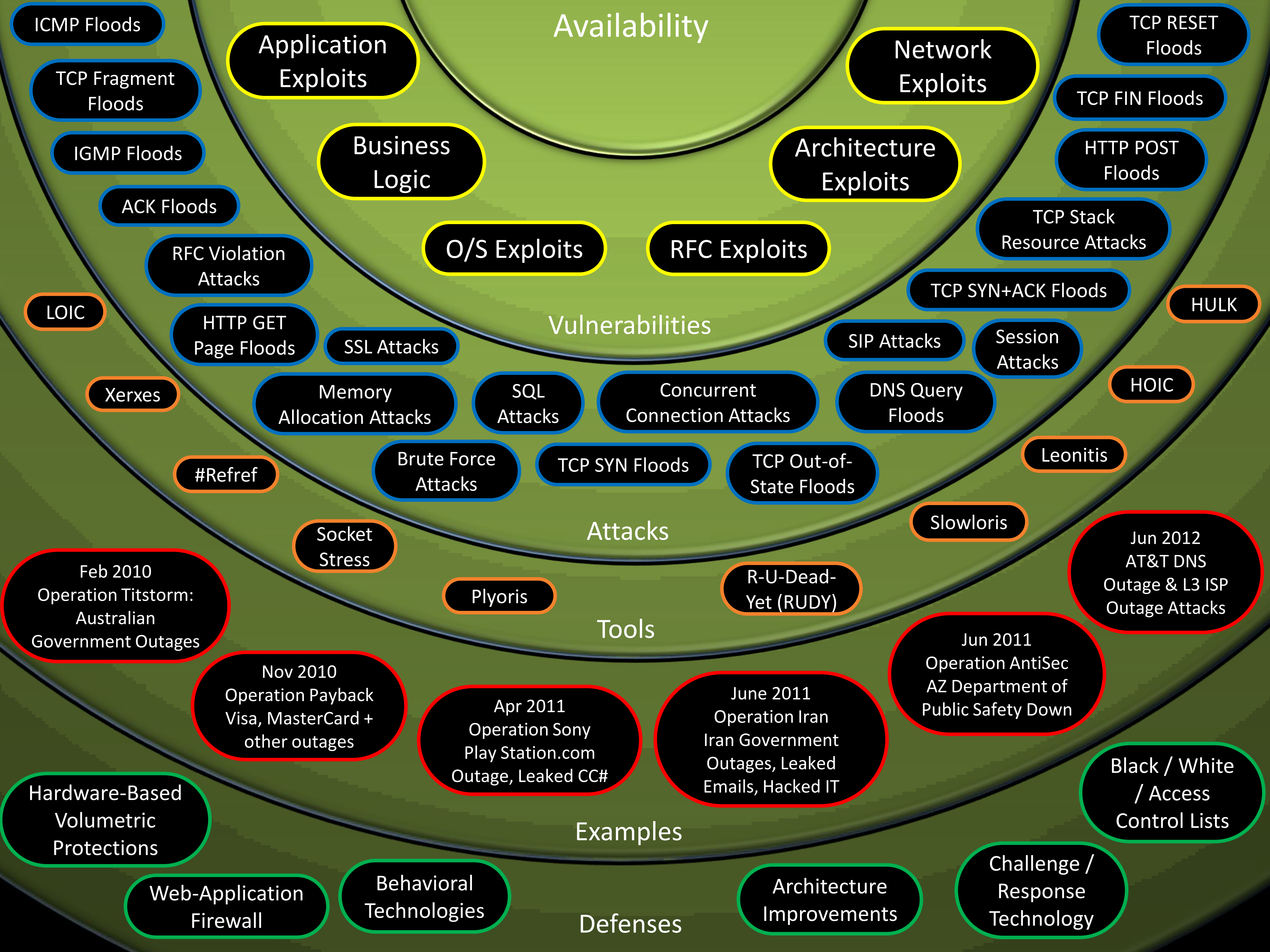
radware

# The Security Trinity



# The Security Trinity





Availability

Application Exploits

Network Exploits

Business Logic

Architecture Exploits

O/S Exploits

RFC Exploits

Vulnerabilities

ICMP Floods

TCP Fragment Floods

IGMP Floods

ACK Floods

RFC Violation Attacks

HTTP GET Page Floods

SSL Attacks

Memory Allocation Attacks

SQL Attacks

Concurrent Connection Attacks

DNS Query Floods

Brute Force Attacks

TCP SYN Floods

TCP Out-of-State Floods

SIP Attacks

Session Attacks

TCP SYN+ACK Floods

TCP Stack Resource Attacks

HTTP POST Floods

TCP FIN Floods

TCP RESET Floods

Attacks

LOIC

Xerxes

#Refref

Socket Stress

Plyoris

R-U-Dead-Yet (RUDY)

Slowloris

Leonitis

HOIC

HULK

Tools

Feb 2010 Operation Titstorm: Australian Government Outages

Nov 2010 Operation Payback Visa, MasterCard + other outages

Apr 2011 Operation Sony Play Station.com Outage, Leaked CC#

June 2011 Operation Iran Iran Government Outages, Leaked Emails, Hacked IT

Jun 2011 Operation AntiSec AZ Department of Public Safety Down

Jun 2012 AT&T DNS Outage & L3 ISP Outage Attacks

Examples

Hardware-Based Volumetric Protections

Web-Application Firewall

Behavioral Technologies

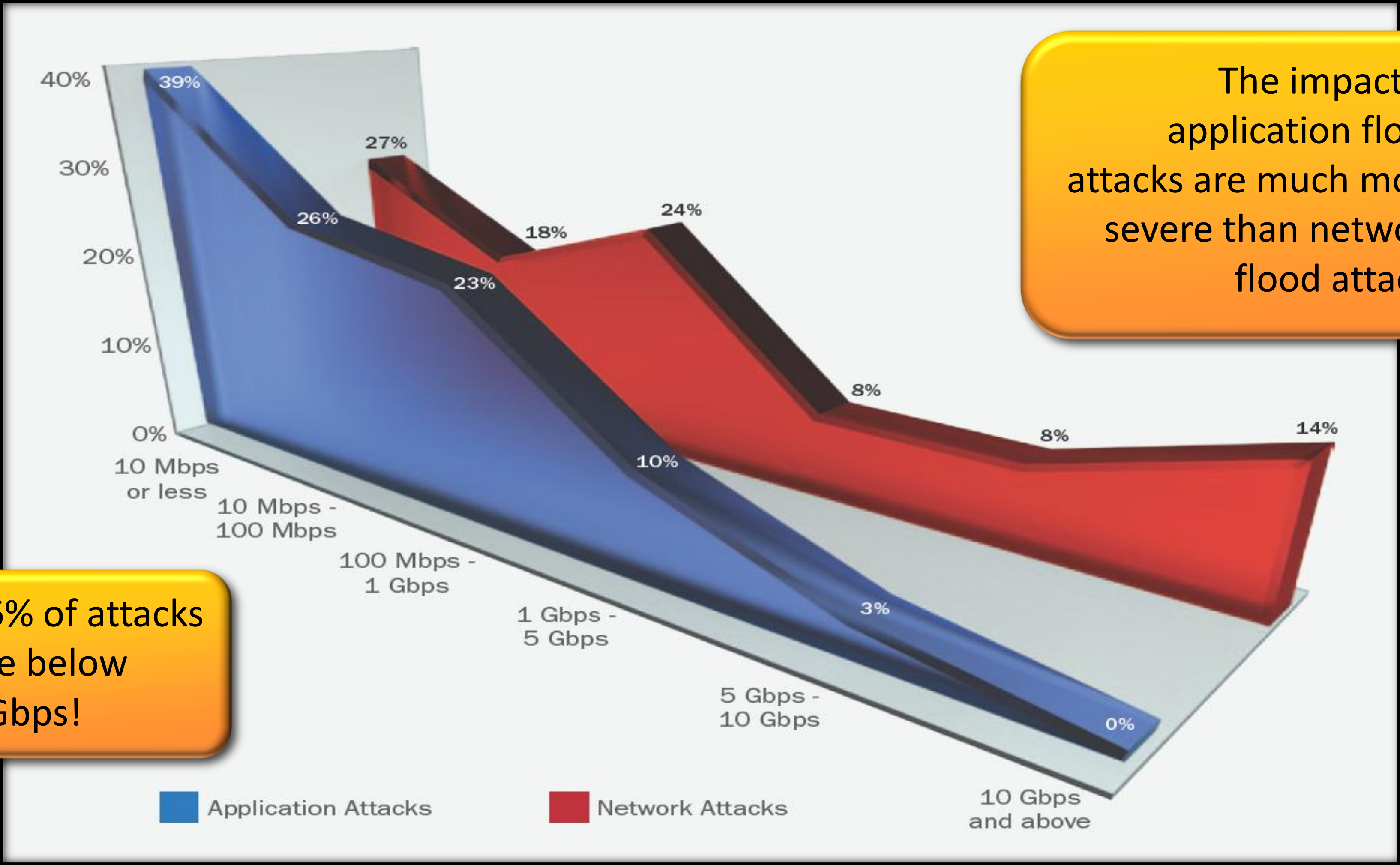
Architecture Improvements

Challenge / Response Technology

Black / White / Access Control Lists

Defenses

# Size Does Not Matter. Honest.



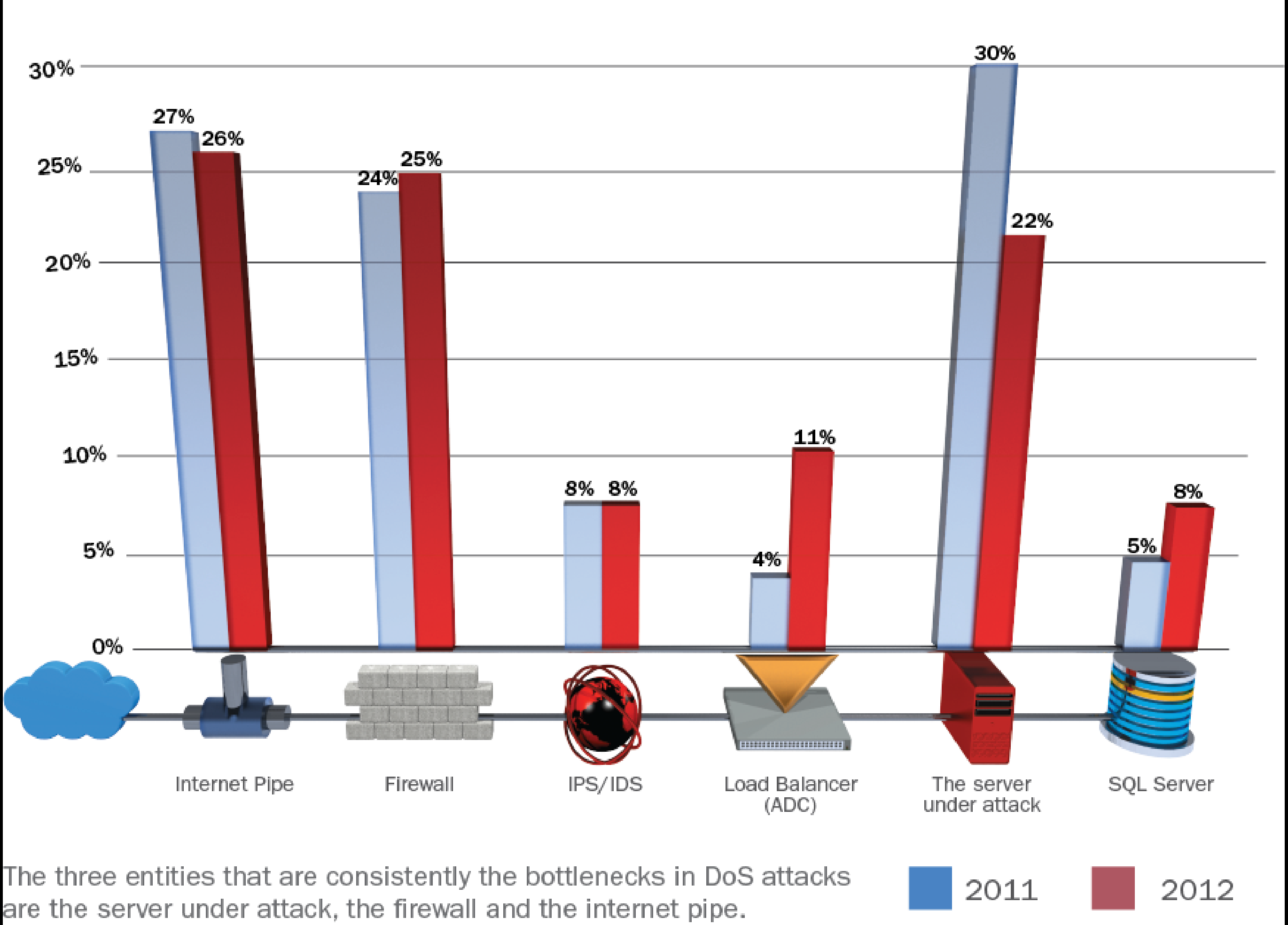
The impact of application flood attacks are much more severe than network flood attacks

76% of attacks are below 1Gbps!

# Main Bottlenecks During DoS Attacks - ERT Survey

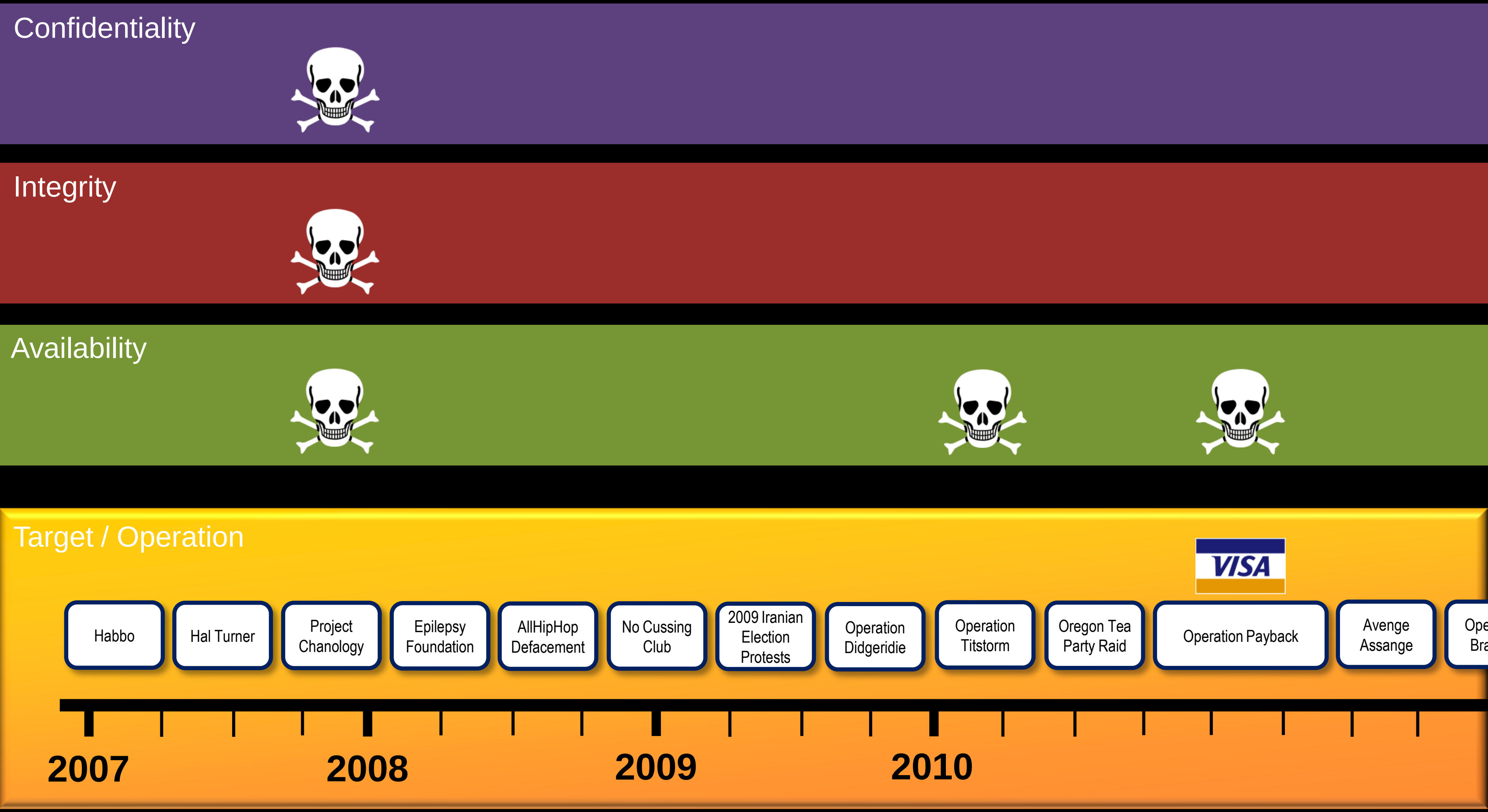
**Radware Securlty Survey**

Which services or network elements are (or have been the bottleneck) of DoS?

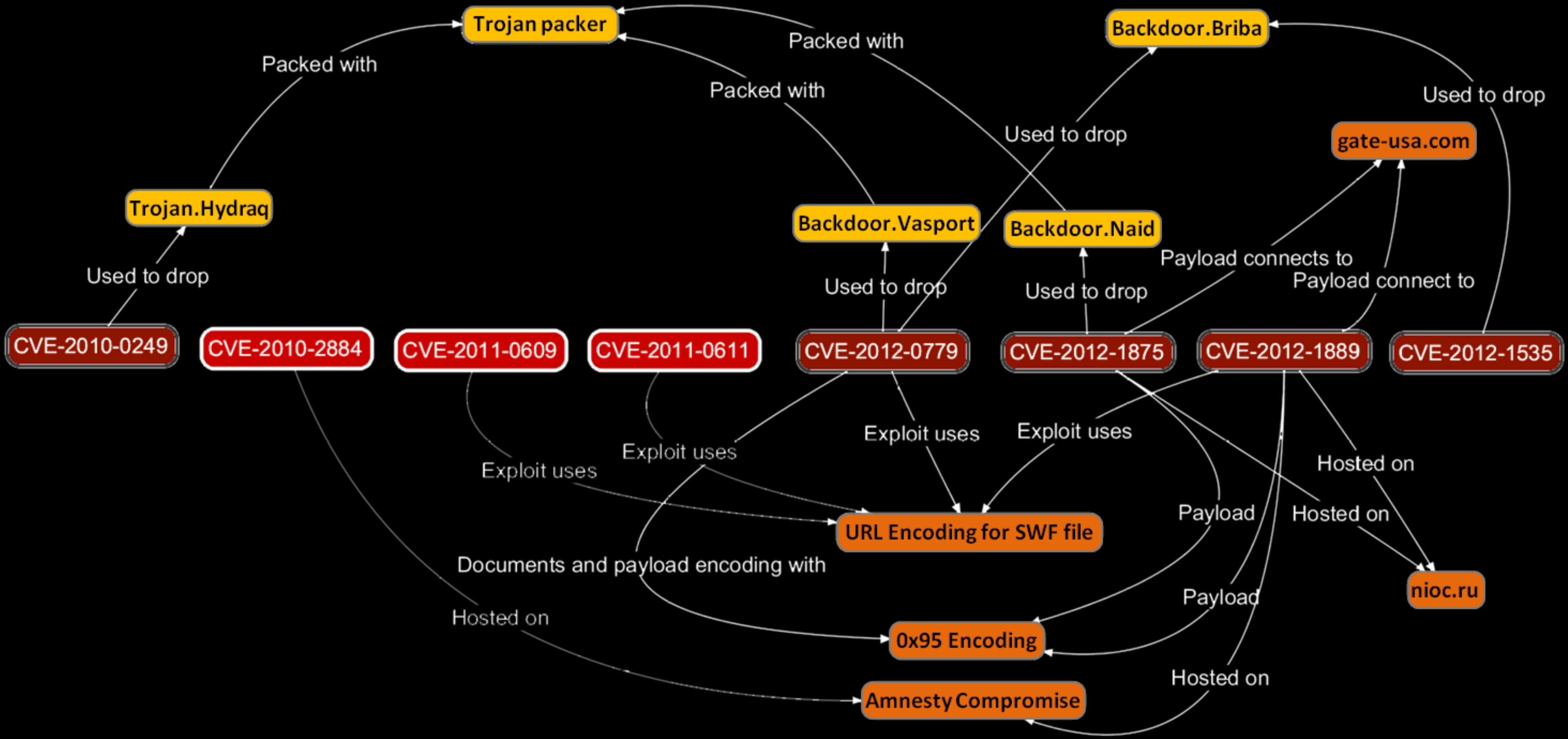


The three entities that are consistently the bottlenecks in DoS attacks are the server under attack, the firewall and the internet pipe.

# The Impact


Confidentiality
Integrity
Availability
Target / Operation
VISA
Habbo
Hal Turner
Project Chanology
Epilepsy Foundation
AllHipHop Defacement
No Cussing Club
2009 Iranian Election Protests
Operation Didgeridie
Operation Titstorm
Oregon Tea Party Raid
Operation Payback
Avenge Assange
Ope Bra
2007
2008
2009
2010

# APTs & Zero-Day Resolution Intensifies



radware

# Defense Blind Spot Map

| Protection Purpose | Firewall | IPS | WAF | Router ACLs | Next Gen FW | Anti-DoS Appliance (CPE) | DLP | Cloud Anti-DoS |
|---|---|---|---|---|---|---|---|---|
| Data-At-Rest Protections (Confidentiality) | 🔴 | 🟠 | 🔴 | 🔴 | 🔴 | 🔴 | 🟢 | 🔴 |
| Data-At-Endpoint (Confidentiality) | 🔴 | 🟠 | 🔴 | 🔴 | 🔴 | 🔴 | 🟢 | 🔴 |
| Data-In-Transit (Confidentiality) | 🟠 | 🟠 | 🟢 | 🟠 | 🟠 | 🟢 | 🟢 | 🔴 |
| Network Infrastructure Protection (Integrity) | 🟢 | 🔴 | 🔴 | 🟠 | 🟢 | 🟠 | 🔴 | 🔴 |
| Application Infrastructure Protection (Integrity) | 🔴 | 🔴 | 🟢 | 🔴 | 🟠 | 🟠 | 🔴 | 🟠 |
| Volumetric Attacks (Availability) | 🔴 | 🔴 | 🟠 | 🟠 | 🔴 | 🟢 | 🔴 | 🟢 |
| Non-Volumetric Resource Attacks (Availability) | 🔴 | 🟠 | 🔴 | 🔴 | 🔴 | 🟢 | 🔴 | 🔴 |

# Gartner Sep 2012: Anti-DoS “BlindSpot”

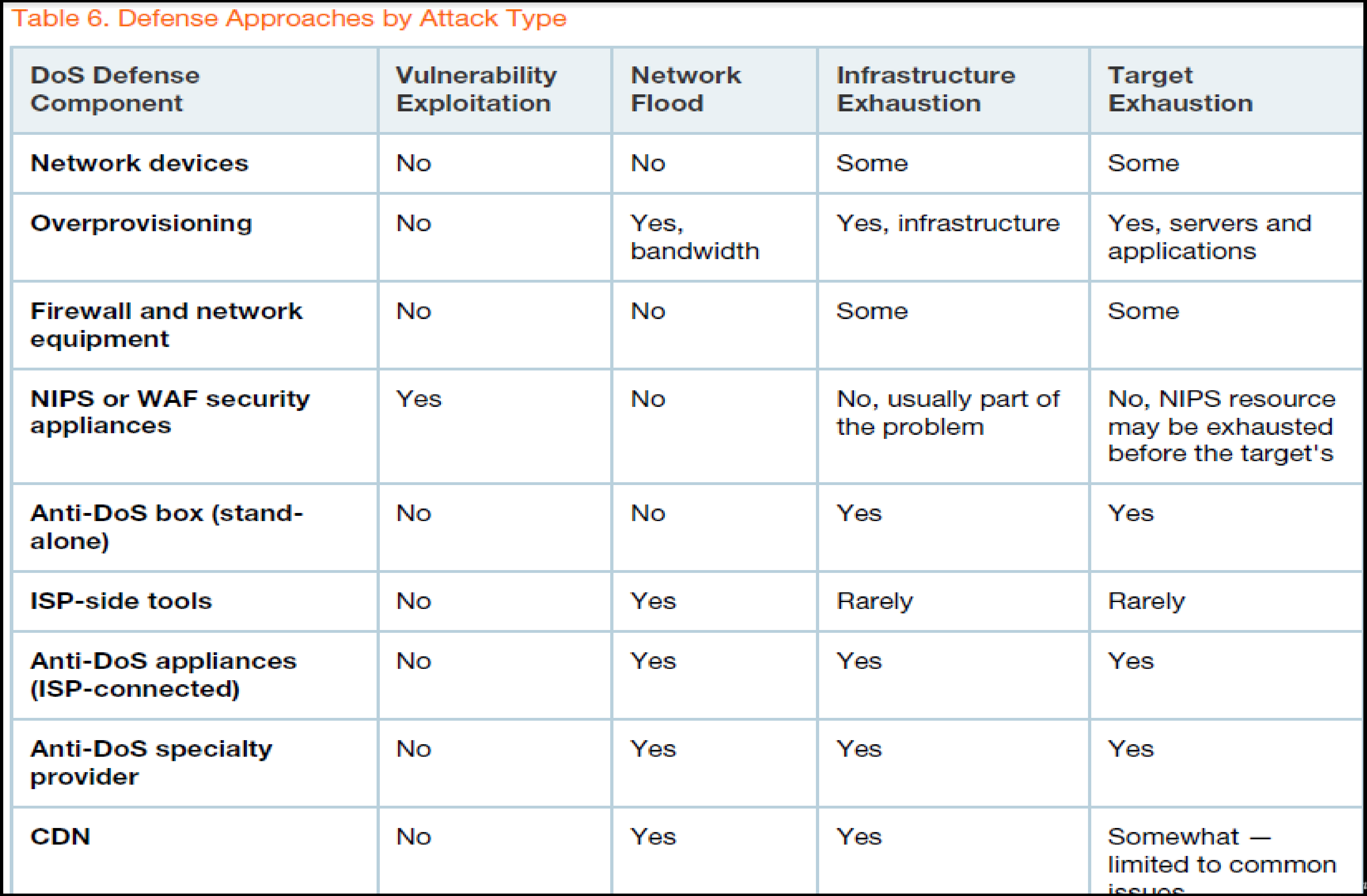


Table 6. Defense Approaches by Attack Type

| DoS Defense Component | Vulnerability Exploitation | Network Flood | Infrastructure Exhaustion | Target Exhaustion |
|---|---|---|---|---|
| **Network devices** | No | No | Some | Some |
| **Overprovisioning** | No | Yes, bandwidth | Yes, infrastructure | Yes, servers and applications |
| **Firewall and network equipment** | No | No | Some | Some |
| **NIPS or WAF security appliances** | Yes | No | No, usually part of the problem | No, NIPS resource may be exhausted before the target's |
| **Anti-DoS box (stand-alone)** | No | No | Yes | Yes |
| **ISP-side tools** | No | Yes | Rarely | Rarely |
| **Anti-DoS appliances (ISP-connected)** | No | Yes | Yes | Yes |
| **Anti-DoS specialty provider** | No | Yes | Yes | Yes |
| **CDN** | No | Yes | Yes | Somewhat — limited to common issues |

*ure?*

# Gartner Sep 2012: Anti-DoS “BlindSpot”

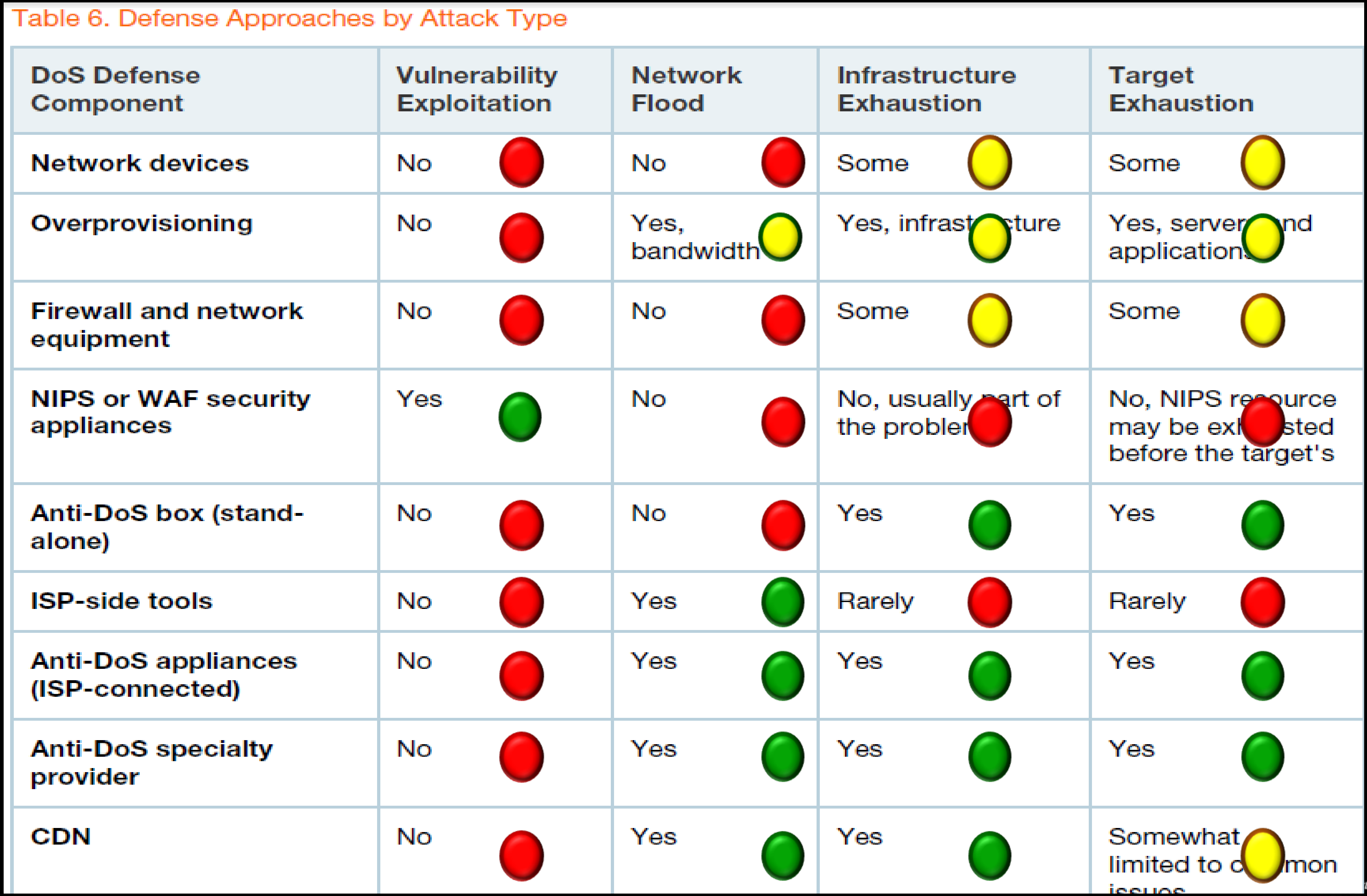


Table 6. Defense Approaches by Attack Type

| DoS Defense Component | Vulnerability Exploitation | Network Flood | Infrastructure Exhaustion | Target Exhaustion |
|---|---|---|---|---|
| Network devices | No 🔴 | No 🔴 | Some 🟡 | Some 🟡 |
| Overprovisioning | No 🔴 | Yes, bandwidth 🟡 | Yes, infrastructure 🟡 | Yes, server and applications 🟡 |
| Firewall and network equipment | No 🔴 | No 🔴 | Some 🟡 | Some 🟡 |
| NIPS or WAF security appliances | Yes 🟢 | No 🔴 | No, usually part of the problem 🔴 | No, NIPS resource may be exhausted before the target's 🔴 |
| Anti-DoS box (stand-alone) | No 🔴 | No 🔴 | Yes 🟢 | Yes 🟢 |
| ISP-side tools | No 🔴 | Yes 🟢 | Rarely 🔴 | Rarely 🔴 |
| Anti-DoS appliances (ISP-connected) | No 🔴 | Yes 🟢 | Yes 🟢 | Yes 🟢 |
| Anti-DoS specialty provider | No 🔴 | Yes 🟢 | Yes 🟢 | Yes 🟢 |
| CDN | No 🔴 | Yes 🟢 | Yes 🟢 | Somewhat limited to common issues 🟡 |

ure?

radware

AGENDA

- Securing Tomorrow’s Perimeter

radware

# What We Should Work Toward

- 100% Architecture Protection. Varied Deployment Models.
- Understand the behavior beyond protocol and content
- It’s an eco-system….collaboration is key
- Emergency response & triage: Practice cyber war rooms
- Integrate offense into your security strategies.

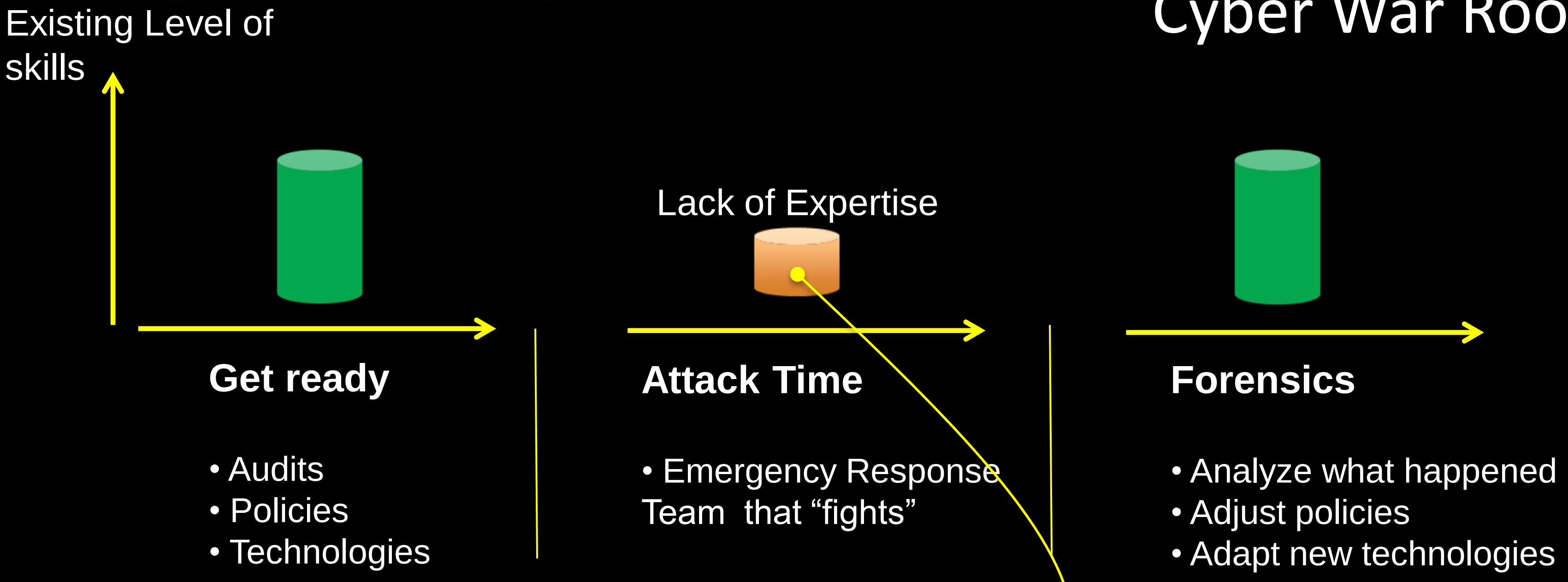
# Perimeter Defense Planning

# Perimeter Defense Planning

Any gap in coverage represents a vulnerability. That will be exploited.

# Perimeter Defense Planning

# Emergency Response Teams & Cyber War Rooms



Existing Level of skills

Lack of Expertise

**Get ready**

- Audits
- Policies
- Technologies

**Attack Time**

- Emergency Response Team that "fights"

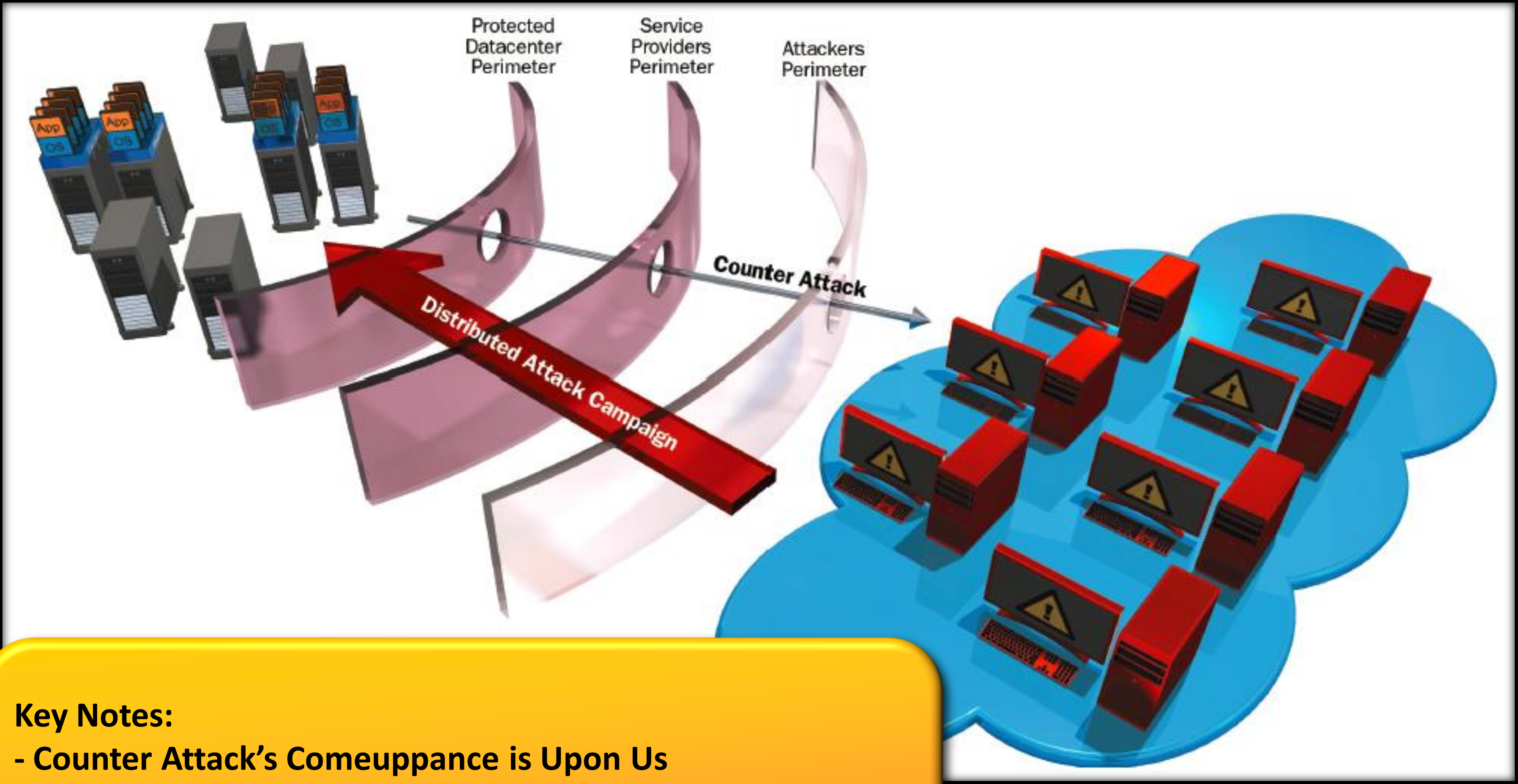
**Forensics**

- Analyze what happened
- Adjust policies
- Adapt new technologies

- **Required expertise during attack campaign**
  - Complex risk assessment
  - Tracking and modifying protections against dynamically evolved attacks
  - Real time intelligence
  - Real time collaboration with other parties
  - Counter attack methods and plans
  - Preparation with cyber "war games"

Strategy

# The Best Defense Is A…


Protected Datacenter Perimeter
Service Providers Perimeter
Attackers Perimeter
App
OS
Counter Attack
Distributed Attack Campaign

**Key Notes:**

- Counter Attack's Comeuppance is Upon Us
- Key IR Assumptions are wrong – e.g. Law enforcement
- Attack Mitigation Talent is Low.  Knowledge must increase.
- Corporate Policies are IR not ERT focused

radware

AGENDA

Anatomy of an Attack

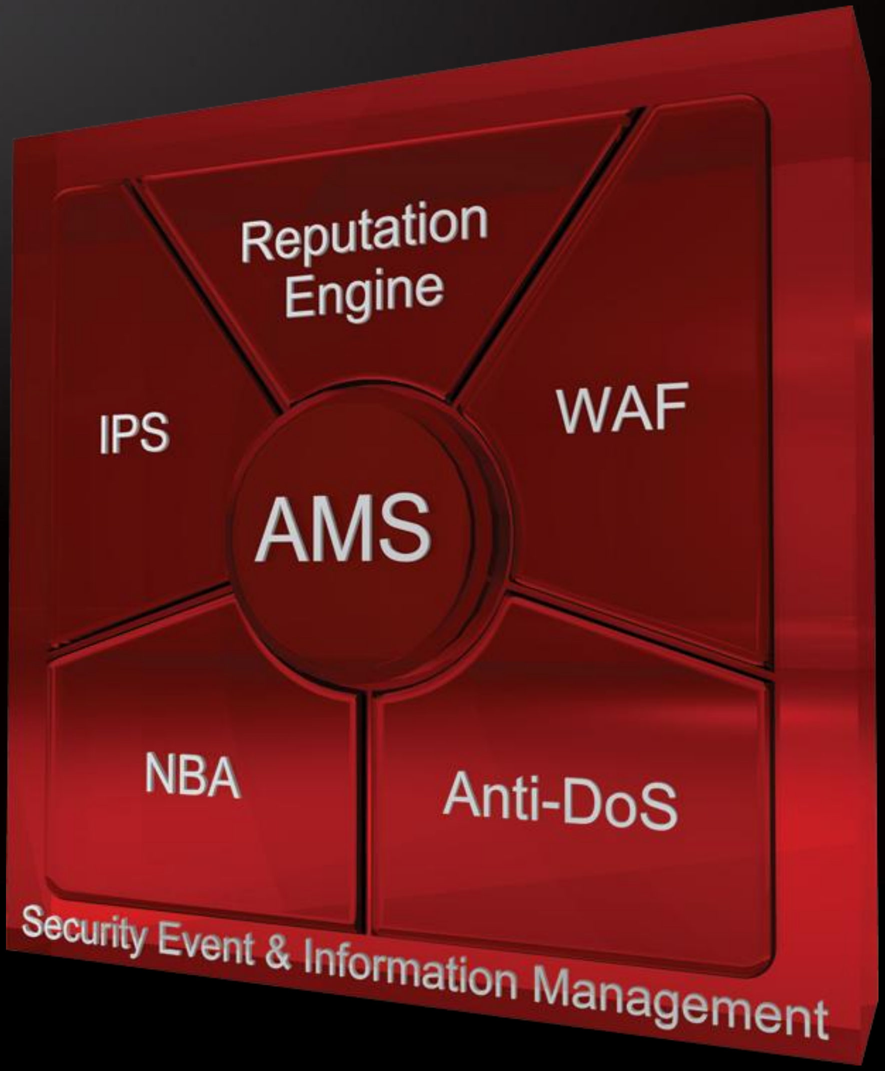
The Evolving Threat Landscape

Securing Tomorrow’s Perimeter

# Recommendations

1. Assess DDoS vulnerabilities
2. Look beyond large attacks
3. Plan ahead – Can’t stop attacks without a game plan
4. Secure potential bottlenecks – Which of YOUR devices will fail first?
5. Watch what’s happening on the network – Do you have signals?
6. Be aware of all threat surfaces - including mobile phones
7. Beware of application-layer attacks - Not just DDoS anymore
8. Watch for blended attacks
9. Partner up with companies that know how to counter attack

# Thank You

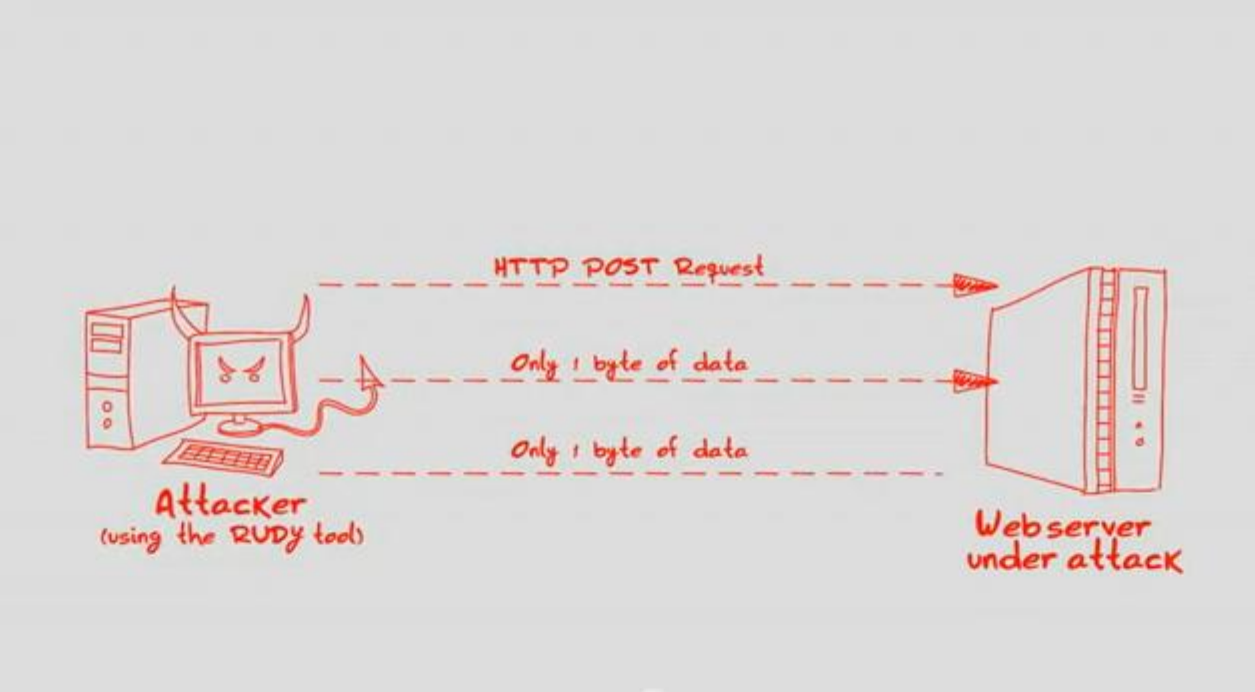


Carl Herberger
VP, Security Solutions
Radware
carl.herberger@radware.com

# Low & Slow

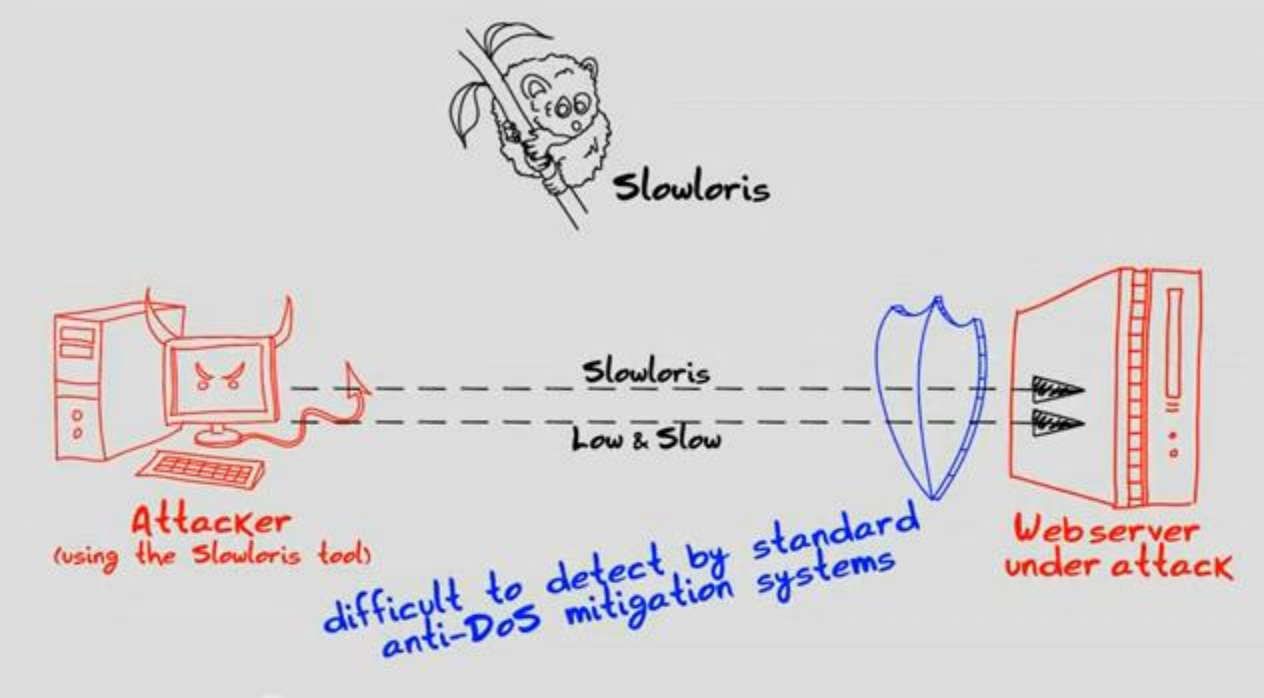
- **Slowloris**
- **Sockstress**
- **R.U.D.Y.**
- **Simultaneous Connection Saturation**

# R.U.D.Y (R-U-Dead-Yet)



**R.U.D.Y. (R-U-Dead-Yet?)**
R.U.D.Y. (R-U-Dead-Yet?) is a slow-rate HTTP POST (Layer 7) denial-of-service tool created by Raviv Raz and named after the Children of Bodom album "Are You Dead Yet?" It achieves denial-of-service by using long form field submissions. By injecting one byte of information into an application POST field at a time and then waiting, R.U.D.Y. causes application threads to await the end of never-ending posts in order to perform processing (this behavior is necessary in order to allow web servers to support users with slower connections). Since R.U.D.Y. causes the target webserver to hang while waiting for the rest of an HTTP POST request, by initiating simultaneous connections to the server the attacker is ultimately able to exhaust the server's connection table and create a denial-of-service condition.

# Slowloris


Slowloris
Slowloris
Low & Slow
Attacker
(using the Slowloris tool)
difficult to detect by standard anti-DoS mitigation systems
Webserver under attack

**Slowloris**

Slowloris is a denial-of-service (DoS) tool developed by the grey hat hacker “RSnake” that causes DoS by using a very slow HTTP request. By sending HTTP headers to the target site in tiny chunks as slow as possible (waiting to send the next tiny chunk until just before the server would time out the request), the server is forced to continue to wait for the headers to arrive. If enough connections are opened to the server in this fashion, it is quickly unable to handle legitimate requests.

Slowloris is cross-platform, except due to Windows’ ~130 simultaneous socket use limit, it is only effective from UNIX-based systems which allow for more connections to be opened in parallel to a target server (although a GUI Python version of Slowloris dubbed PyLoris was able to overcome this limiting factor on Windows).