radware

Information Security Adaptation: Survival In An Evolving Threat Landscape.

Mick Stephens

General Manager. Radware, Australia & New Zealand.

radware

Or…….Are Organizations Bring a Knife to a Gunfight?

Raiders of the Lost Ark(1981)

radware

Attacked in 2012

They had the budget.
They made the investment.
And yet they went offline.

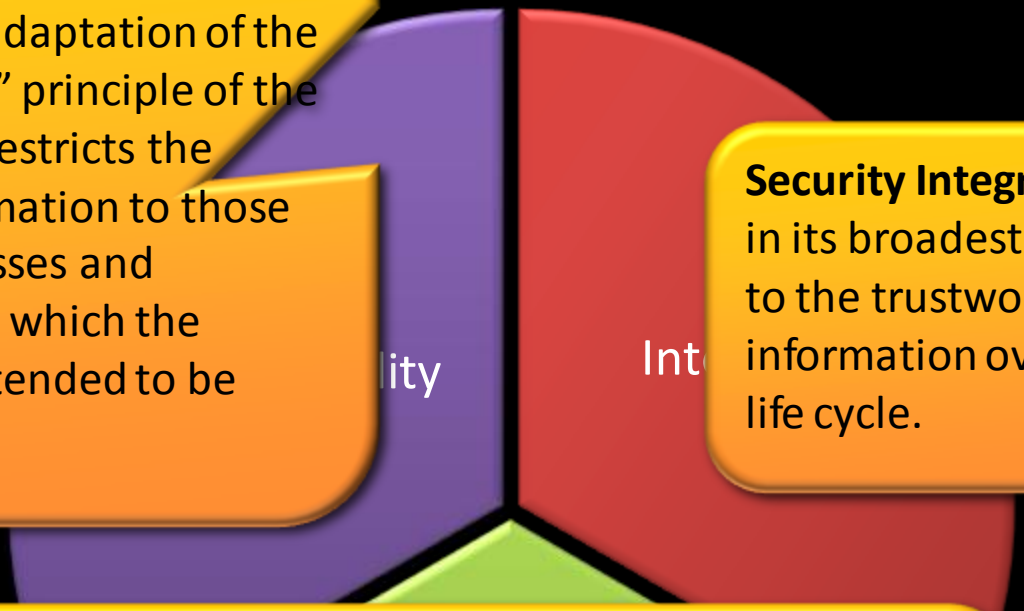
radware

AGENDA

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

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.

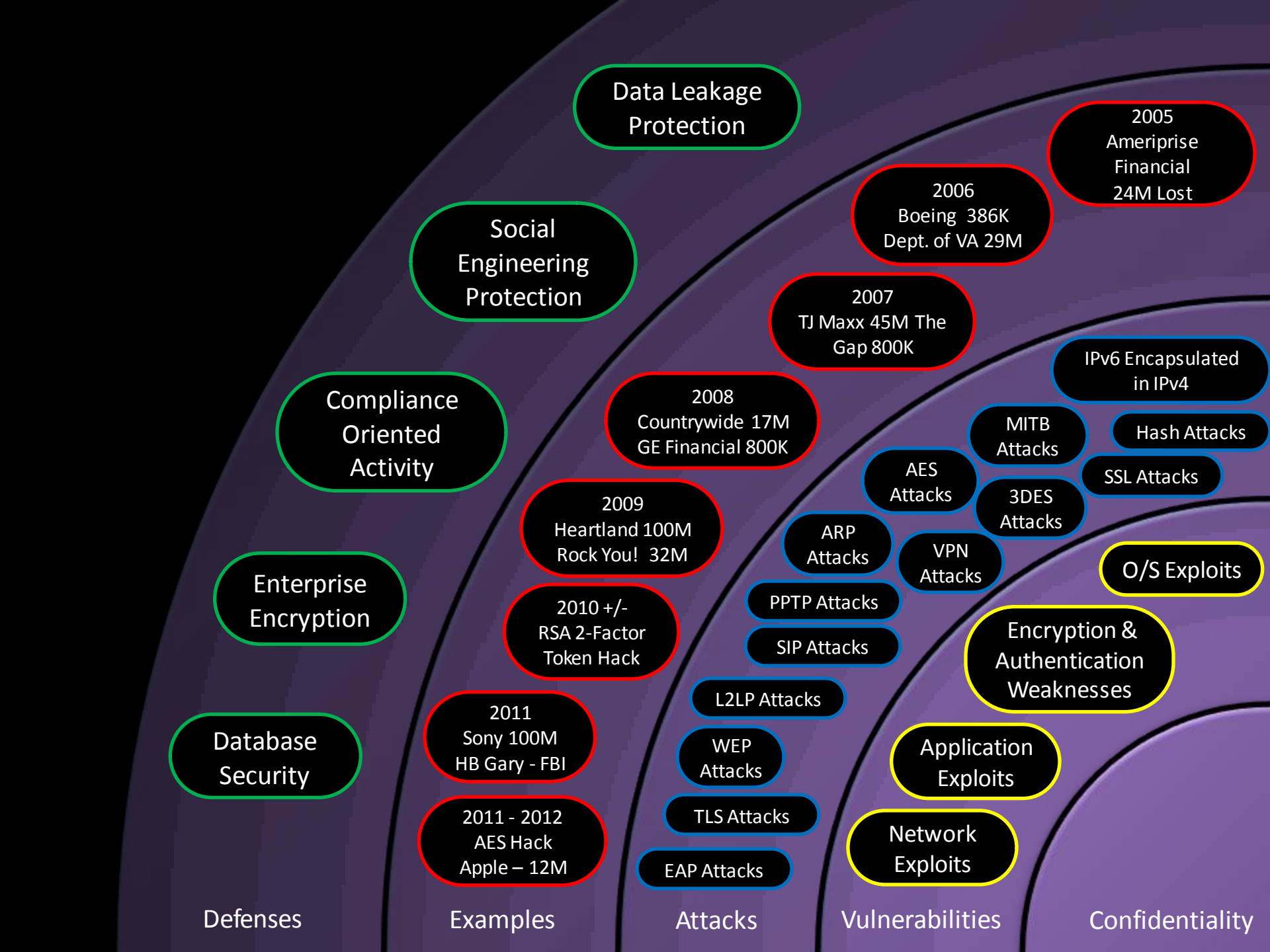


Security Integrity
in its broadest meaning refe to the trustworthiness of information over its entire life cycle.

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

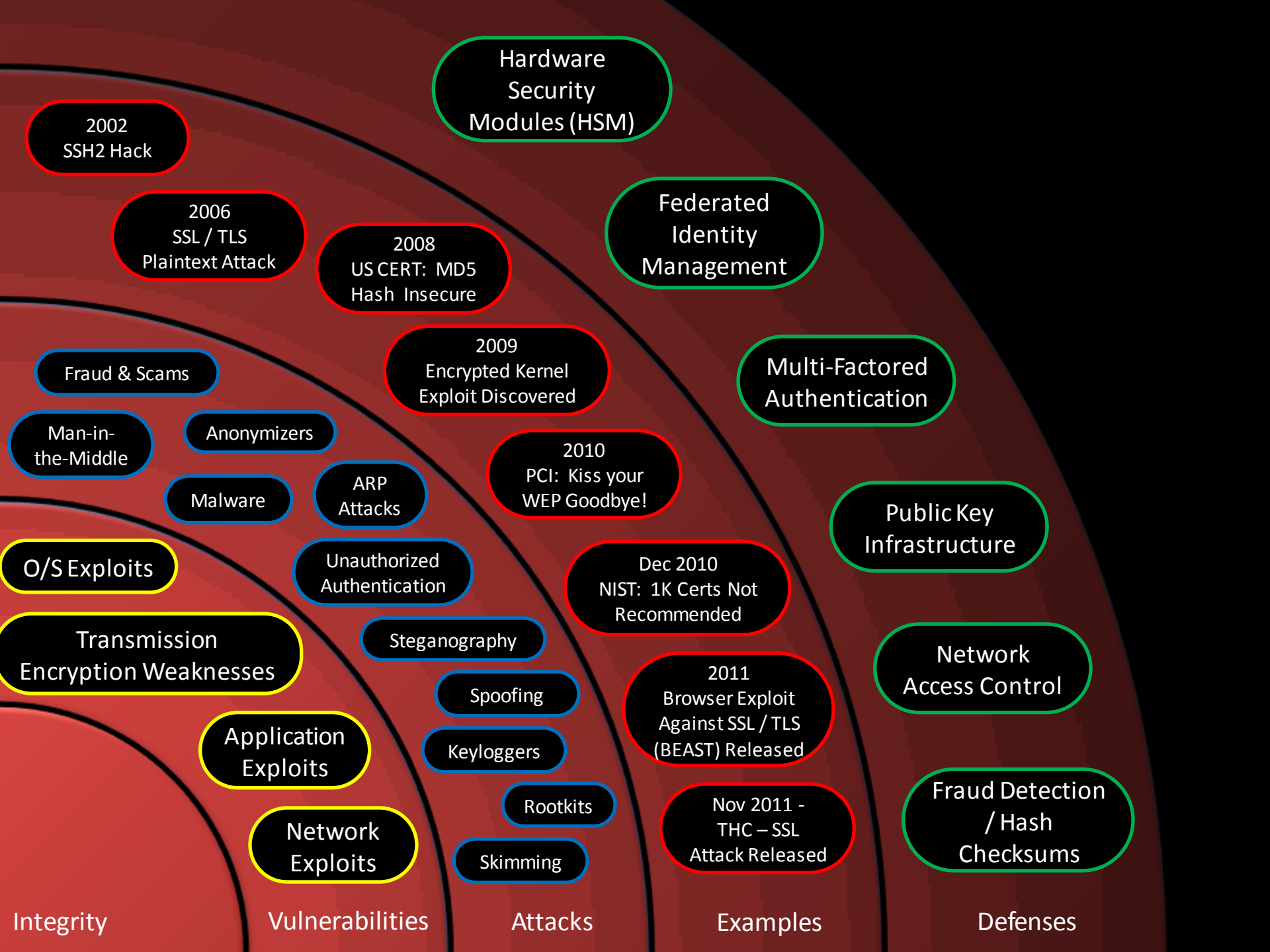

Data Leakage Protection
Social Engineering Protection
Compliance Oriented Activity
Enterprise Encryption
Database Security
2005 Ameriprise Financial 24M Lost
2006 Boeing 386K Dept. of VA 29M
2007 TJ Maxx 45M The Gap 800K
2008 Countrywide 17M GE Financial 800K
2009 Heartland 100M Rock You! 32M
2010 +/- RSA 2-Factor Token Hack
2011 Sony 100M HB Gary - FBI
2011 - 2012 AES Hack Apple – 12M
L2LP Attacks
WEP Attacks
TLS Attacks
EAP Attacks
PPTP Attacks
SIP Attacks
ARP Attacks
VPN Attacks
AES Attacks
3DES Attacks
MITB Attacks
SSL Attacks
IPv6 Encapsulated in IPv4
Hash Attacks
O/S Exploits
Encryption & Authentication Weaknesses
Application Exploits
Network Exploits
Defenses
Examples
Attacks
Vulnerabilities
Confidentiality

radware

The Security Trinity

radware

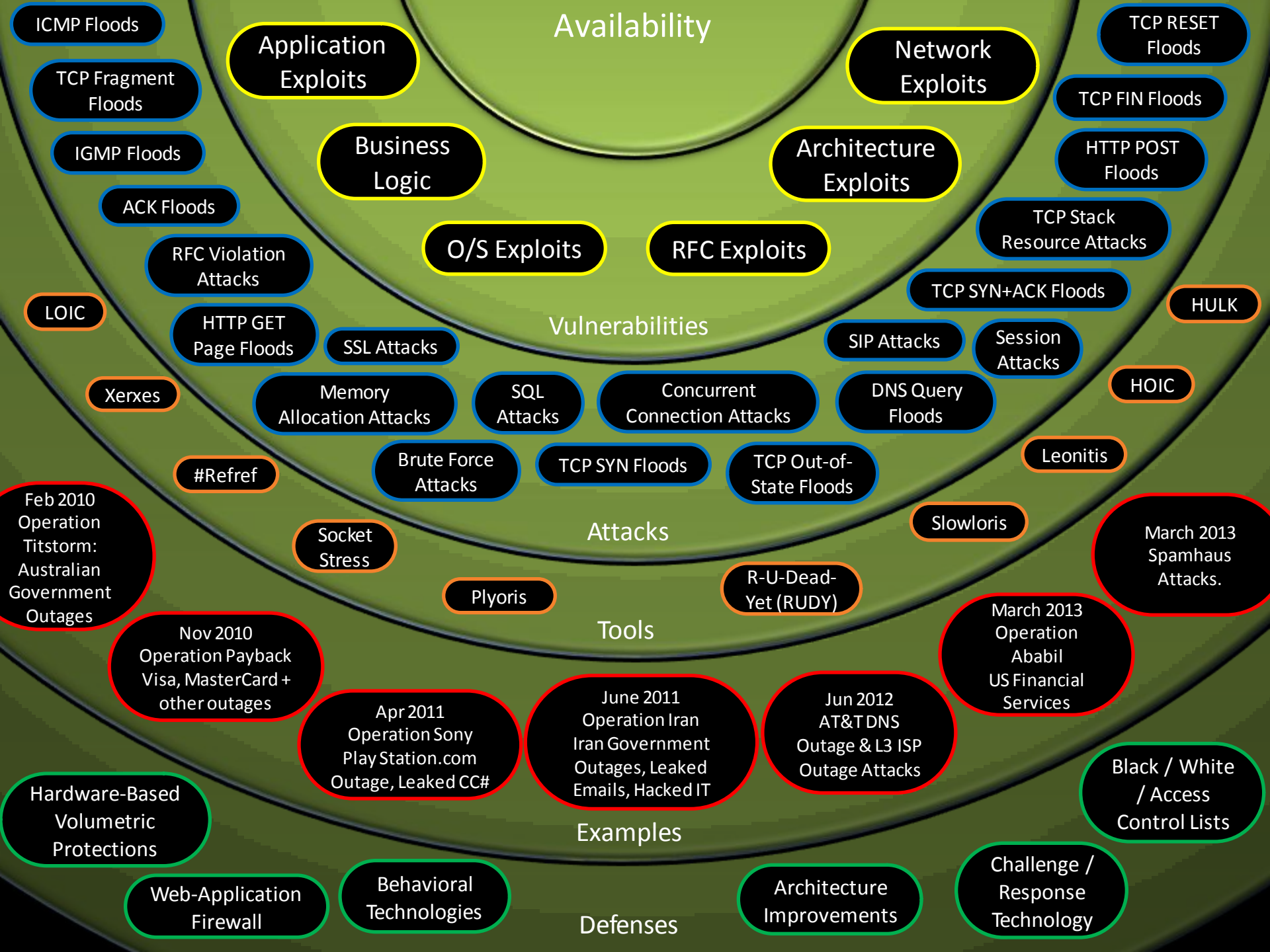
The Security Trinity


Hardware Security Modules (HSM)
2002 SSH2 Hack
2006 SSL / TLS Plaintext Attack
2008 US CERT: MD5 Hash Insecure
Federated Identity Management
2009 Encrypted Kernel Exploit Discovered
Multi-Factored Authentication
Fraud & Scams
Man-in-the-Middle
Anonymizers
Malware
ARP Attacks
2010 PCI: Kiss your WEP Goodbye!
Public Key Infrastructure
O/S Exploits
Unauthorized Authentication
Dec 2010 NIST: 1K Certs Not Recommended
Transmission Encryption Weaknesses
Steganography
Network Access Control
Spoofing
2011 Browser Exploit Against SSL / TLS (BEAST) Released
Application Exploits
Keyloggers
Rootkits
Nov 2011 - THC – SSL Attack Released
Fraud Detection / Hash Checksums
Network Exploits
Skimming
Integrity
Vulnerabilities
Attacks
Examples
Defenses

radware

The Security Trinity

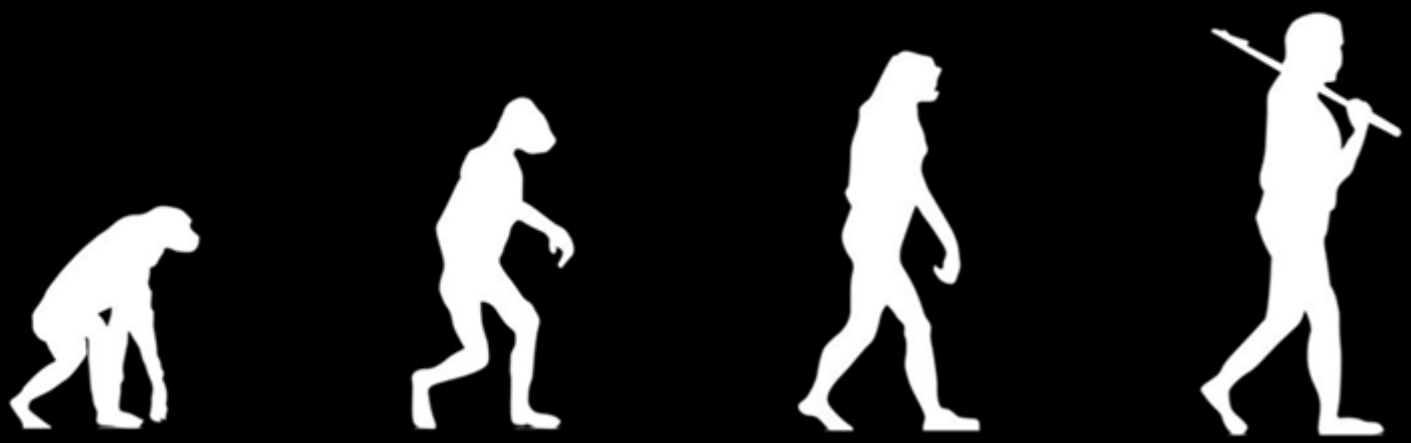
The Security Trinity


Availability
ICMP Floods
Application Exploits
Network Exploits
TCP RESET Floods
TCP Fragment Floods
TCP FIN Floods
IGMP Floods
Business Logic
Architecture Exploits
HTTP POST Floods
ACK Floods
TCP Stack Resource Attacks
O/S Exploits
RFC Exploits
RFC Violation Attacks
TCP SYN+ACK Floods
HULK
LOIC
Vulnerabilities
HTTP GET Page Floods
SSL Attacks
SIP Attacks
Session Attacks
HOIC
Xerxes
Memory Allocation Attacks
SQL Attacks
Concurrent Connection Attacks
DNS Query Floods
Leonitis
#Refref
Brute Force Attacks
TCP SYN Floods
TCP Out-of-State Floods
Feb 2010 Operation Titstorm: Australian Government Outages
Slowloris
March 2013 Spamhaus Attacks.
Socket Stress
Attacks
Plyoris
R-U-Dead-Yet (RUDY)
March 2013 Operation Ababil US Financial Services
Nov 2010 Operation Payback Visa, MasterCard + other outages
Tools
Apr 2011 Operation Sony Play Station.com Outage, Leaked CC#
June 2011 Operation Iran Iran Government Outages, Leaked Emails, Hacked IT
Jun 2012 AT&T DNS Outage & L3 ISP Outage Attacks
Black / White / Access Control Lists
Hardware-Based Volumetric Protections
Examples
Challenge / Response Technology
Web-Application Firewall
Behavioral Technologies
Architecture Improvements
Defenses

radware

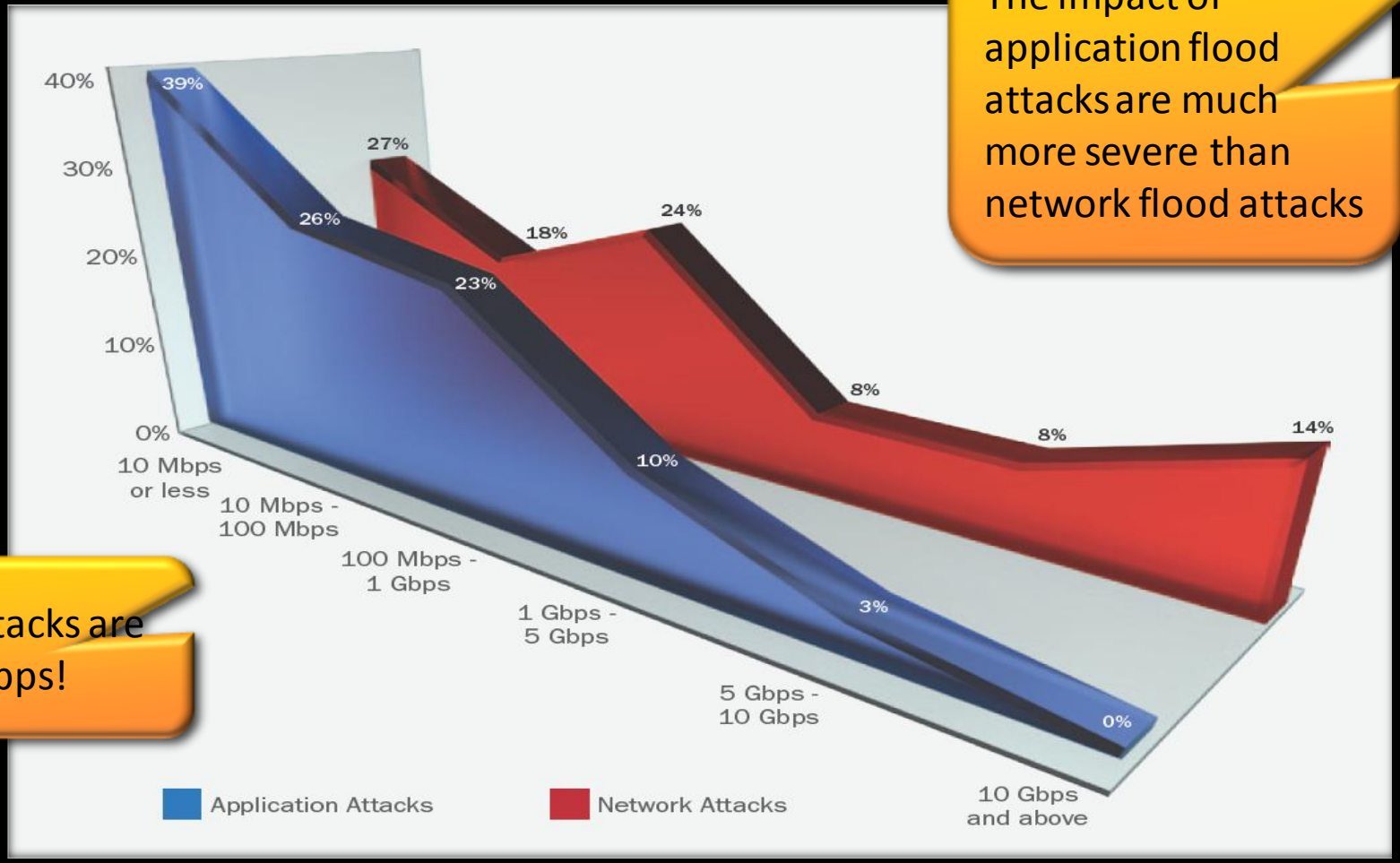
AGENDA

- The Evolving Threat Landscape



Size Does Not Matter. Honest!

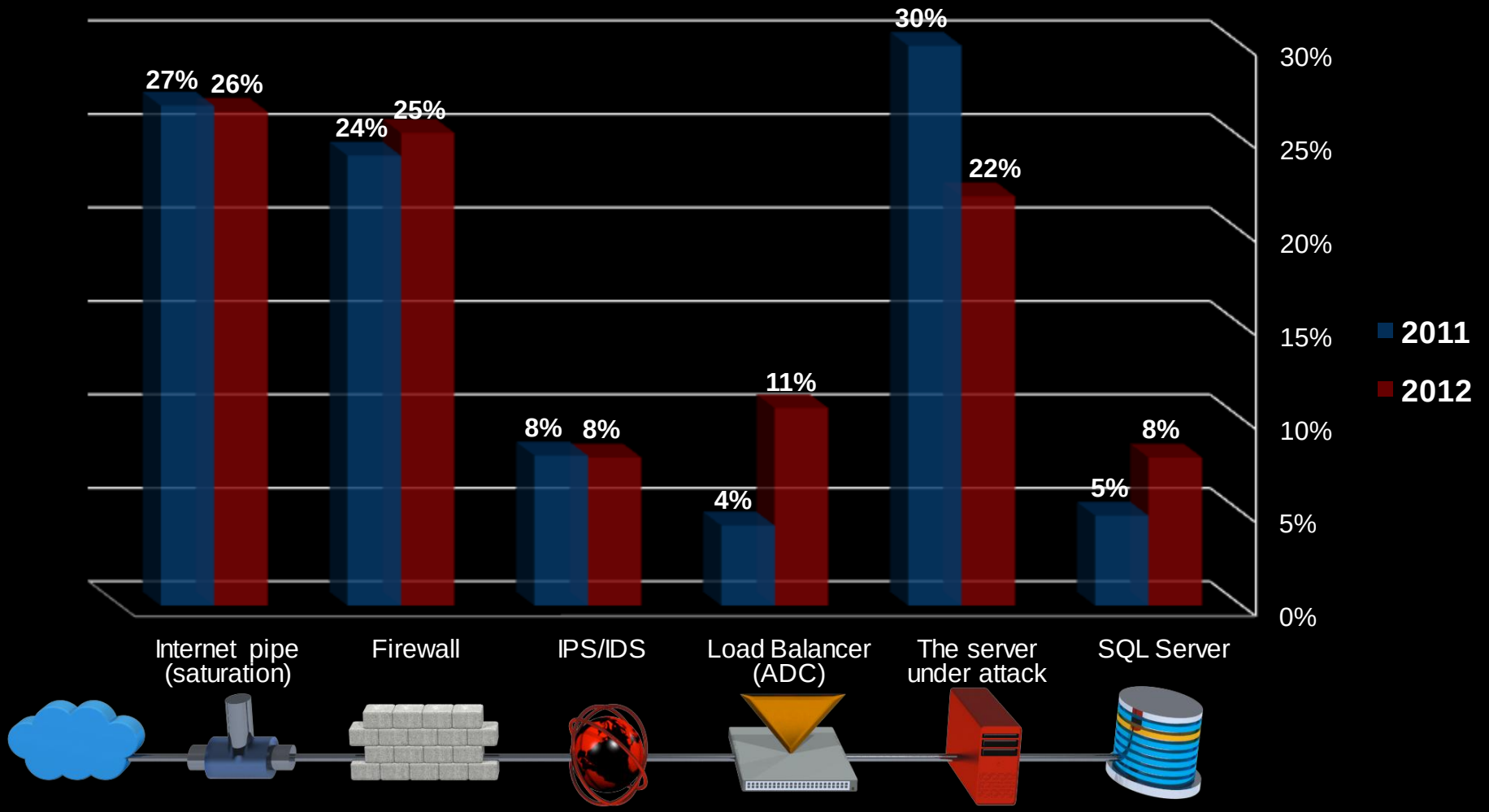
The impact of application flood attacks are much more severe than network flood attacks



76% of attacks are below 1Gbps!

Data: Radware Global Application & Network Security Report 2012.

Entities that are the Bottlenecks in DDoS Attacks

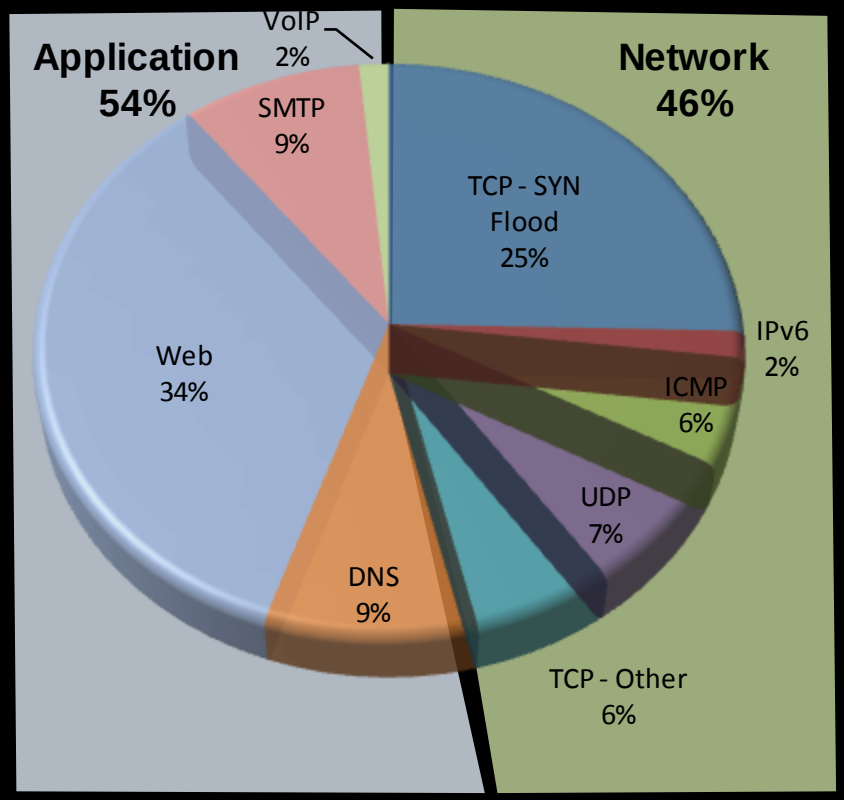


Data: Radware Global Application & Network Security Report 2012.

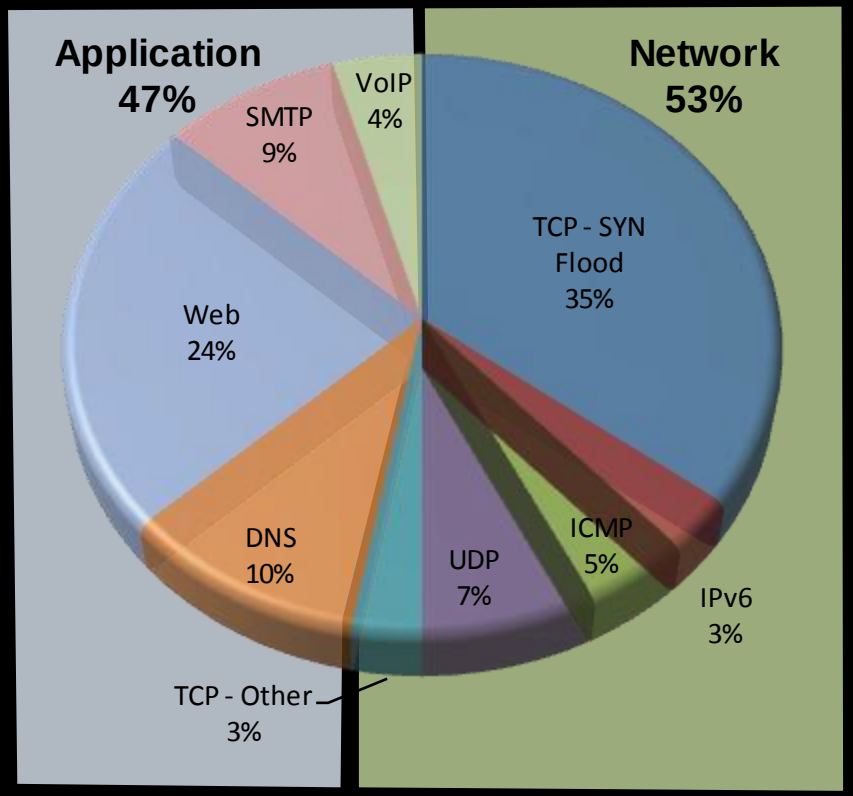
Attack Vectors Trends.

Industry Security Survey – Attack Count by Type

2011



2012



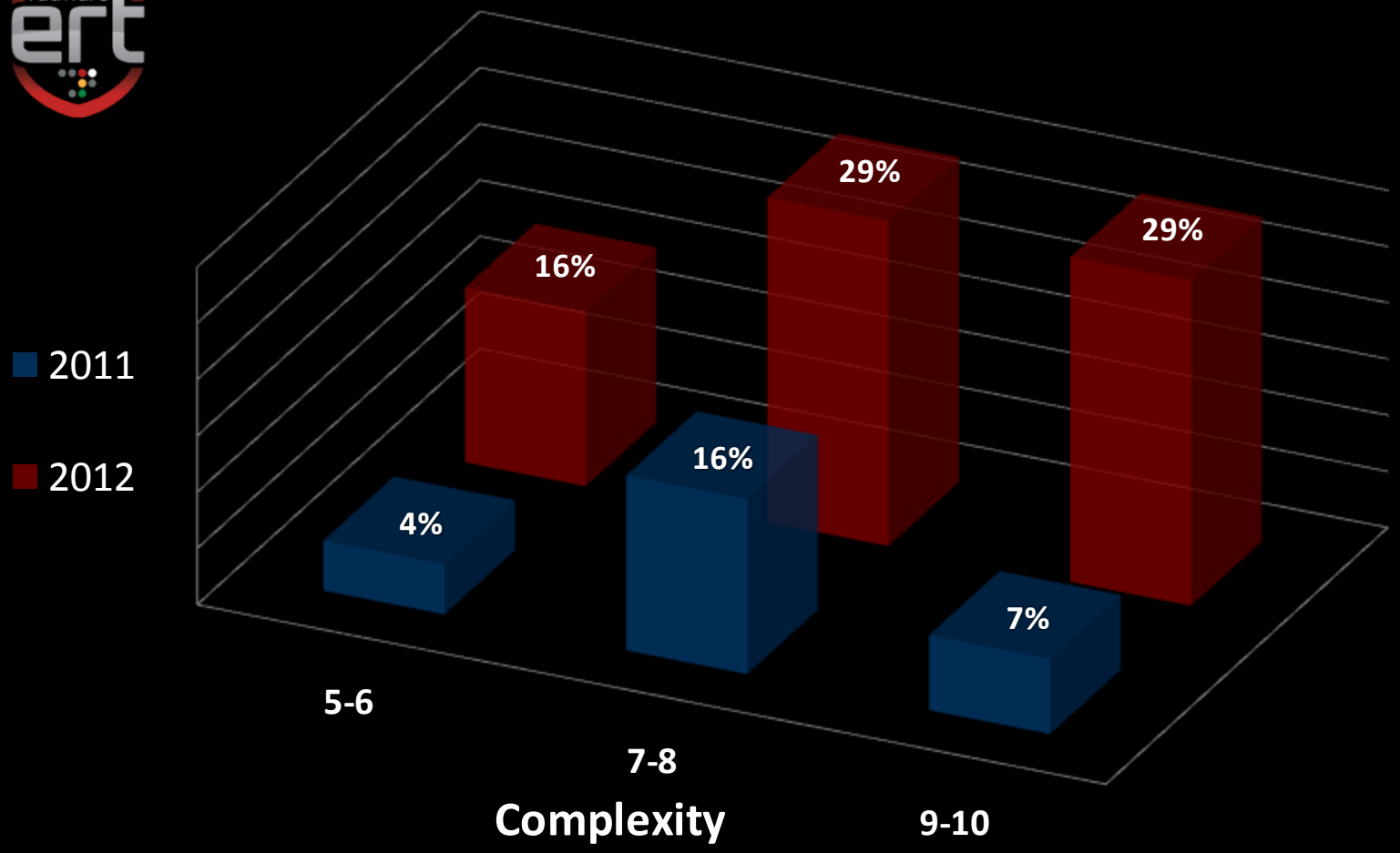
Attack remained diversified between different attack types.
This reflects attackers using multi-vector attacks.

Data: Radware Global Application & Network Security Report 2012.

Hacktivism - Becomes More Campaign-APT Oriented

- **Complex**: Typically more than seven different attack vectors.
- **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

Radware ERT Cases – Attack Vectors Trends



Attacks are more complex: 2012 DoS/DDoS attacks have become more sophisticated, using more complex attack vectors. Note the number of attacks using a complexity level of 7-10.

Hacktivism - Becomes More Campaign-APT Oriented

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

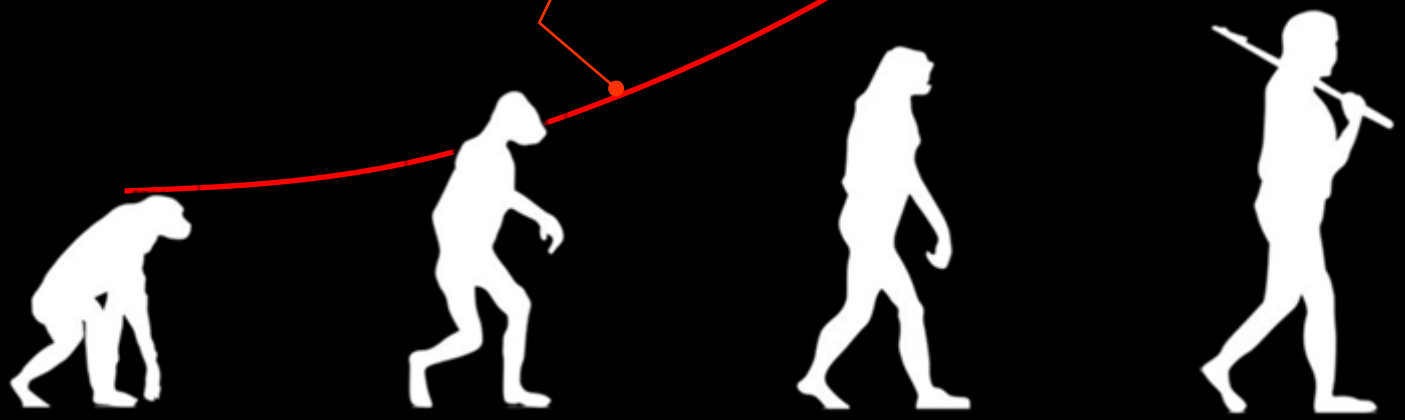
- Duration: **3 Days**
- 5 Attack vectors
- Only "inner cycle" involvement
- Attack target: **HKEX**

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

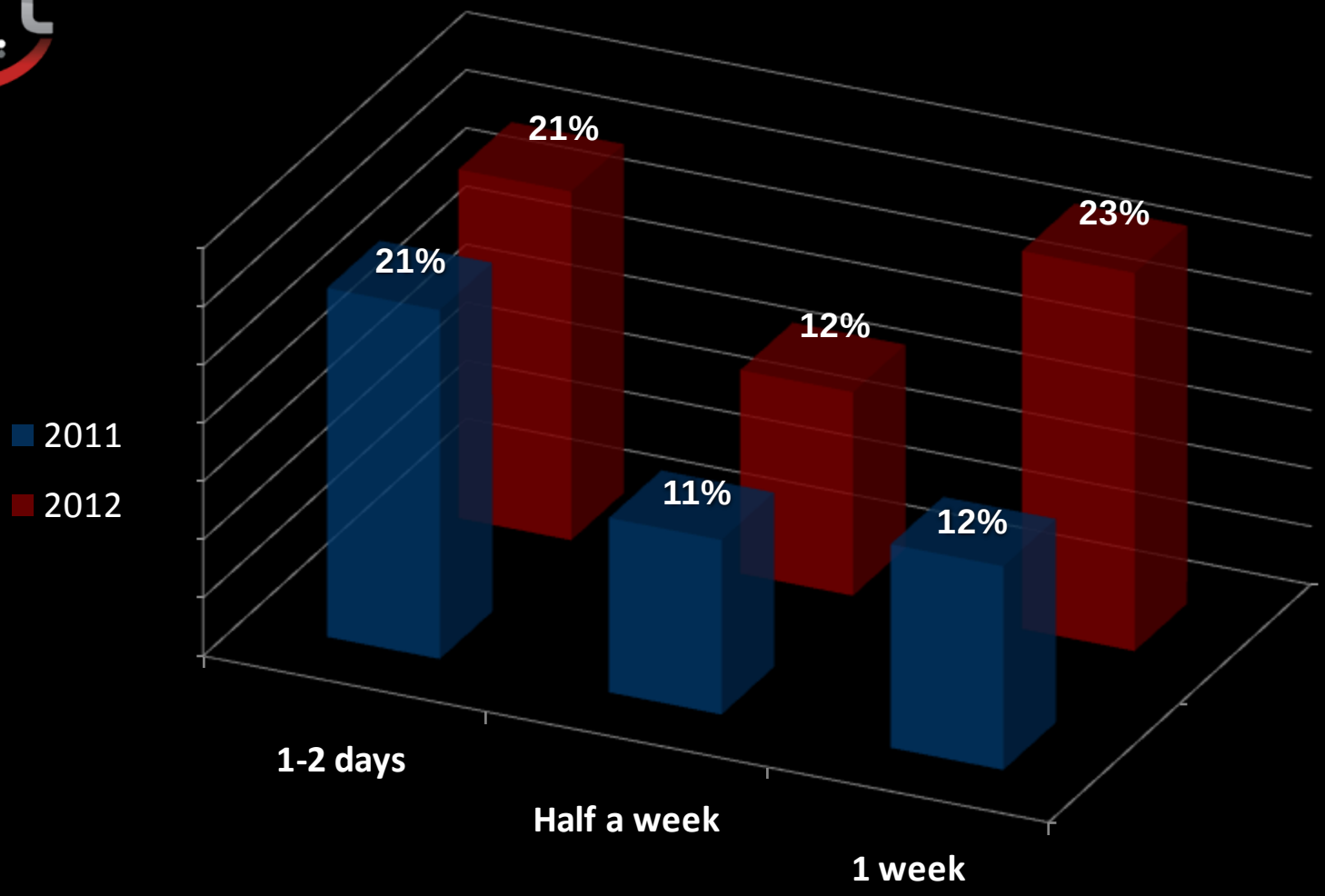
Attack target: **Vatican**

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

Attack target: **Israeli sites**



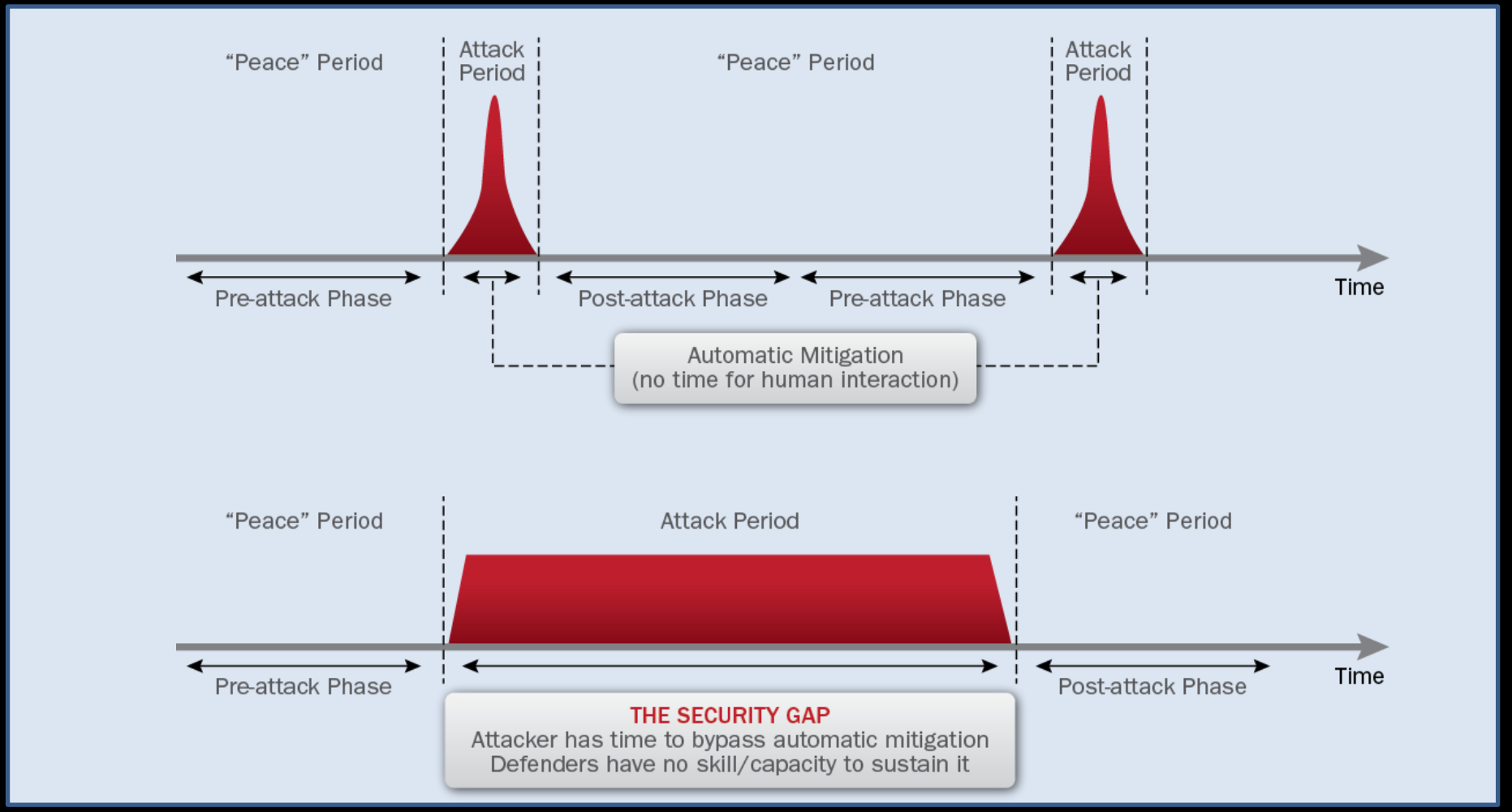
Radware ERT Cases – Attack Duration Trends



Attacks last longer: The number of DoS attacks lasting over a week had doubled in 2012

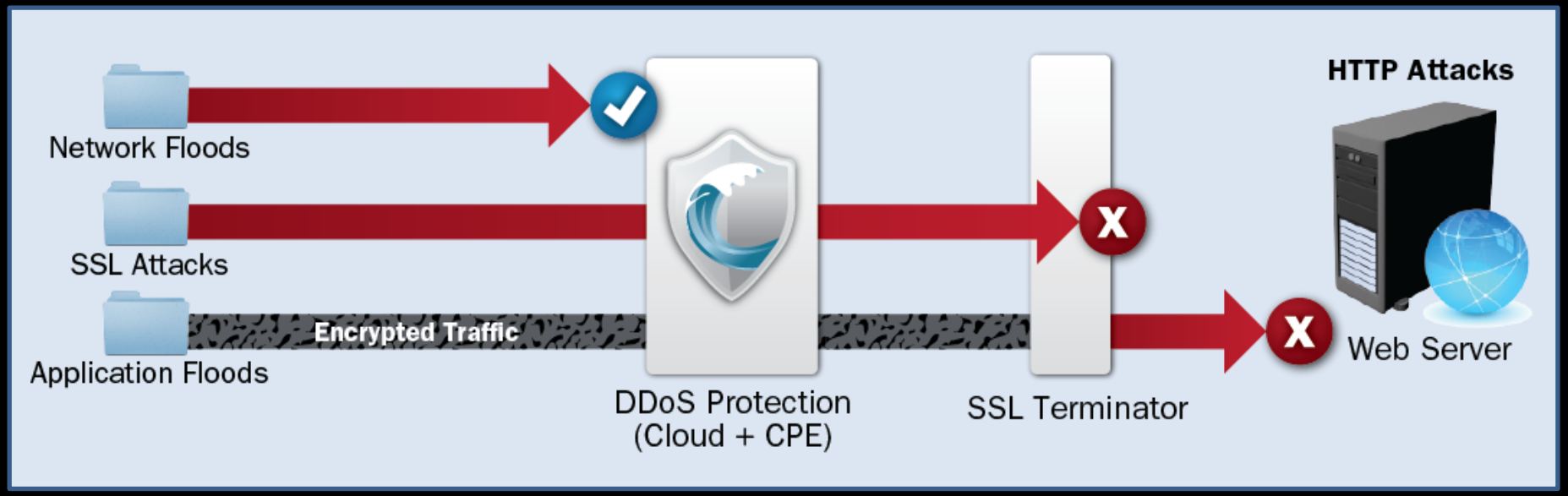
Attack Duration Requires IT to Develop New Skills

War Room Skills Are Required.

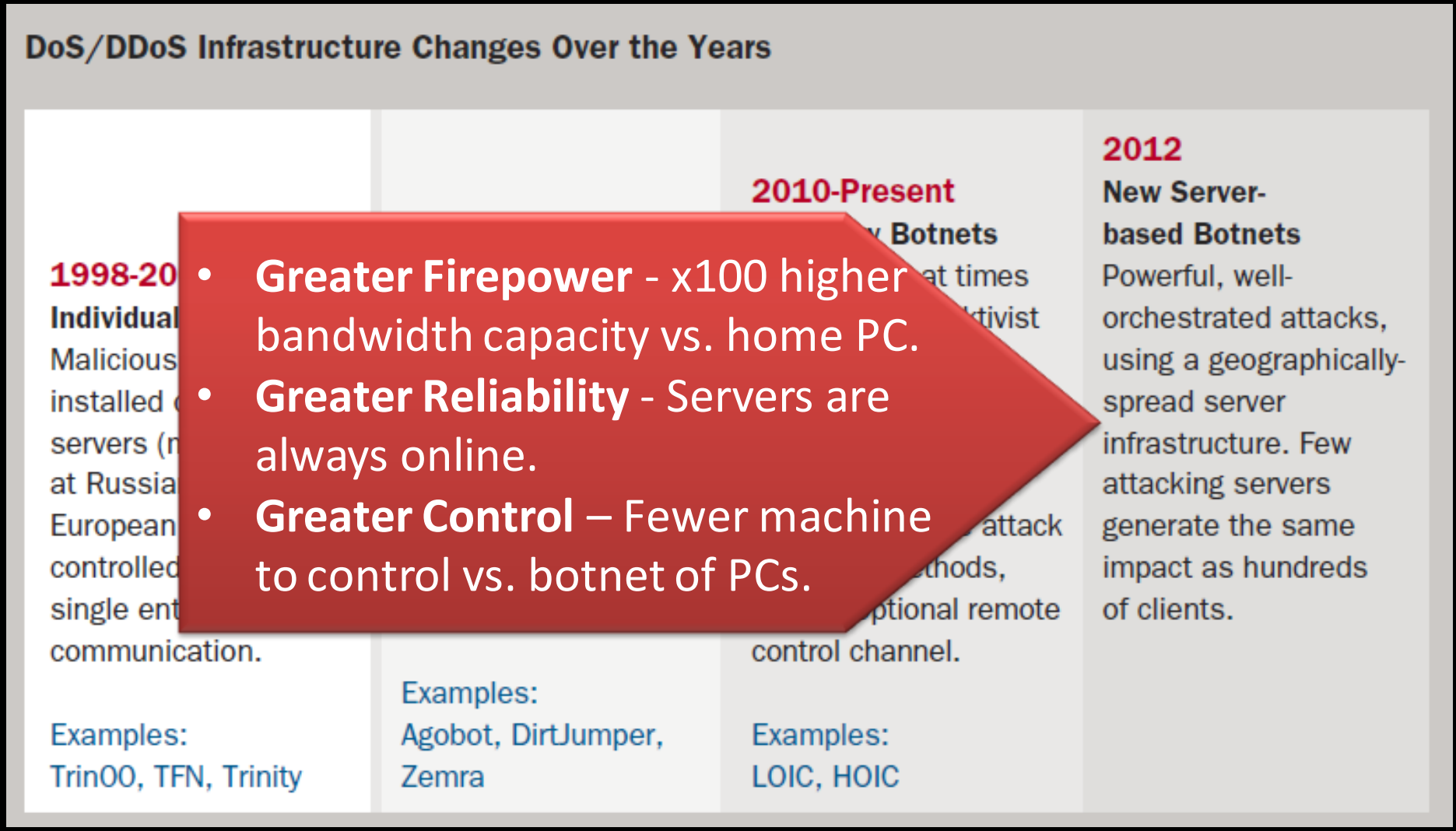


HTTPS Based Attacks

- HTTPS based attacks are on the rise!
- SSL traffic is not terminated by DDoS Cloud Scrubbers or DDoS solutions
- SSL traffic is terminated by ADC or by the web server
- SSL attacks hit their target and bypass security solutions



DDoS Infrastructure Changes



radware

The Impact

Confidentiality

Integrity

Availability

Target / Operation

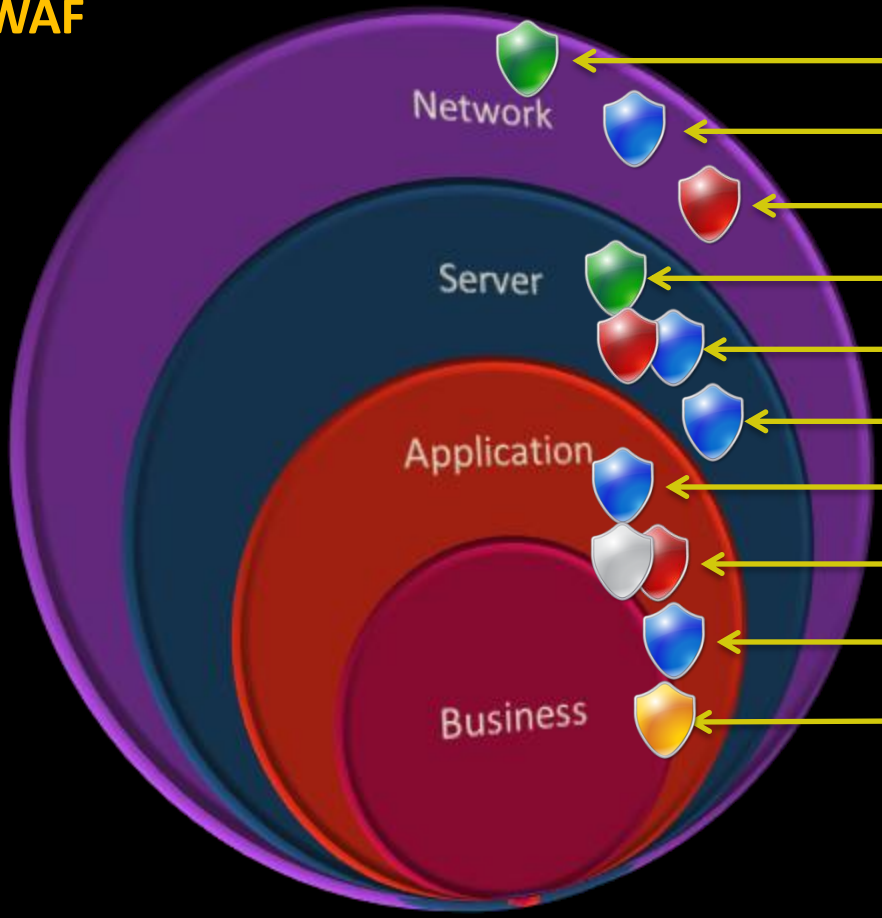
Habbo | Hal Turner | Project Chanology | Epilepsy Foundation | AllHipHop Defacement | No Cussing Club | 2009 Iranian Election Protests | Operation Didgeridie | Operation Titstorm | Oregon Tea Party Raid | Operation Payback | Avenge Assange | Ope Bra

2007 2008 2009 2010


radware
Securing Tomorrow's Perimeter
AGENDA

Mapping 'Availability' Security Protection Tools

- DoS Protection (Anti-DOS)
- Behavioral Analysis (NBA)
- IPS
- IP Reputation
- WAF



Large volume network flood attacks

Network scan

Intrusion

SYN flood

"Low & Slow" DoS attacks

Port scan

Brute force attack

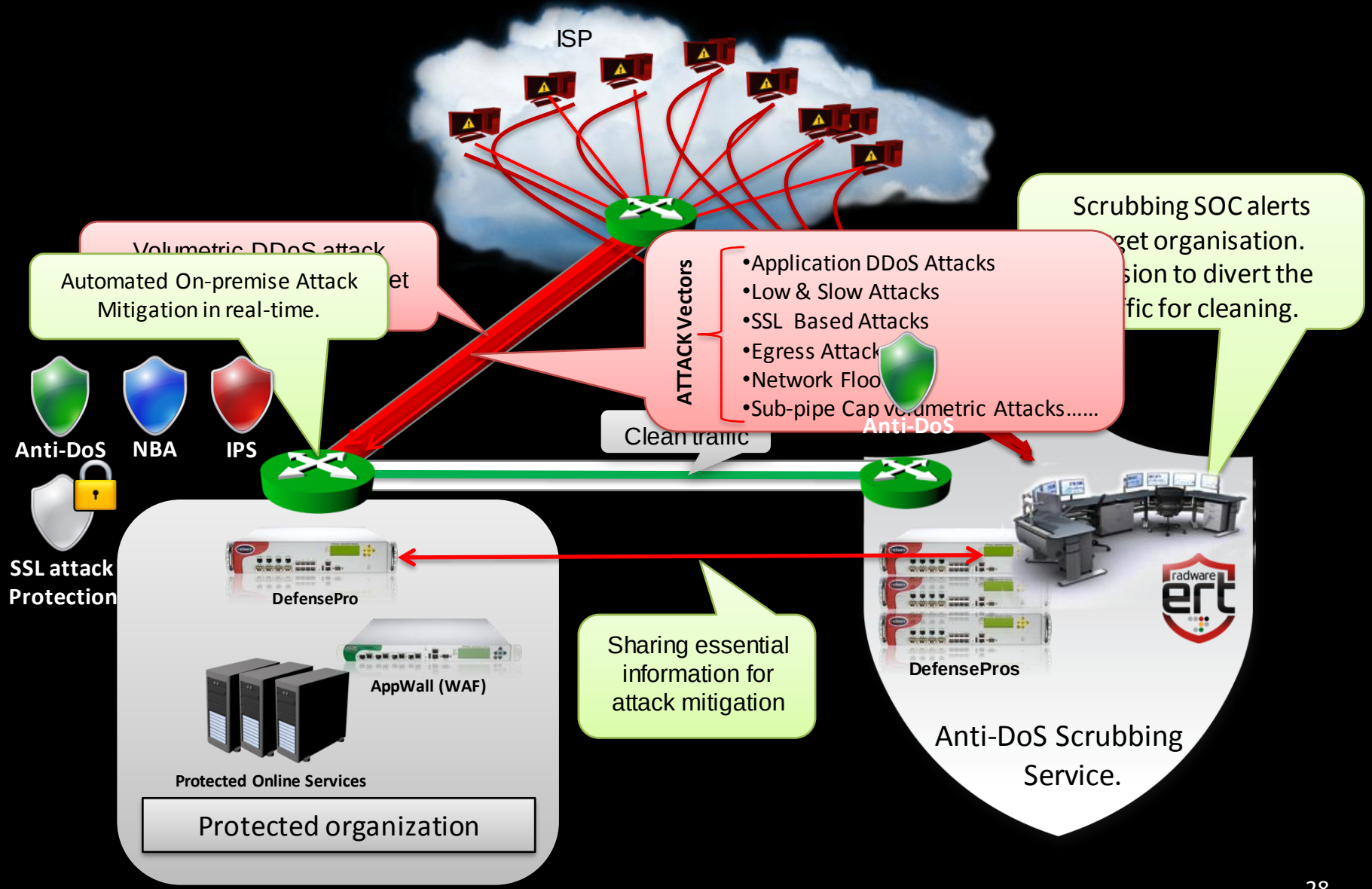
Intrusion, Malware

High & Low rate application DoS attacks

Web application attacks

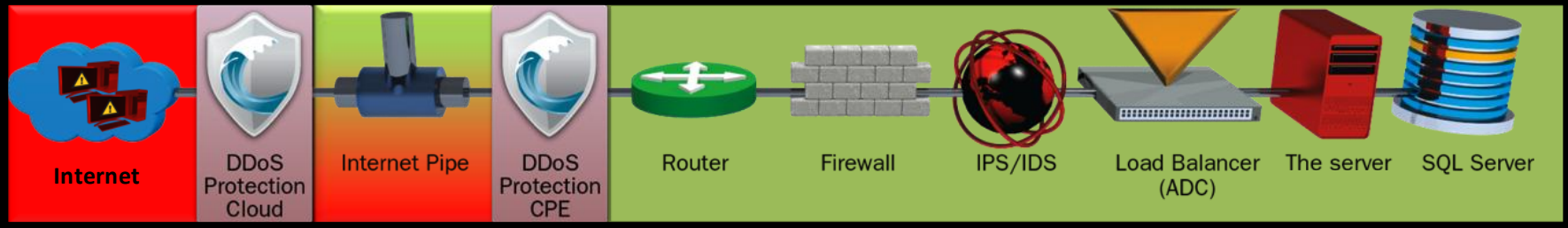
(e.g. XSS, Injections, CSRF)

Taking DDoS of the threat radar.



Taking DDoS of the Threat Radar.

- Don't under estimate DDoS attacks as a vector in a broader, orchestrated attack campaigns.
- Acquire capabilities to sustain a long sophisticated cyber attack.
- Attack tools are known. Test yourself.
- Carefully plan the position of DoS / DDoS mitigation within network architecture.
  - On premise capabilities.
  - In the cloud capabilities.
- Integrate offense into your security strategies?????
  - "A counter-offensive is considered to be the most efficient means of forcing the attacker to abandon offensive plans." – *Vom Kriege. Carl Philipp Gottfried von Clausewitz, c.1832.*



radware

Thank You

www.radware.com