Digital Cyber Security

Narudom Roongsiriwong, CISSP

E-Government Executive Program: e-GEP, June 22, 2017

About Me

- Head of IT Security and Solution Architecture, Kiatnakin Bank PLC (KKP)
- Consulting Team Member for Thailand National e-Payment project
- Committee Member of Thailand Banking Sector CERT (TB-CERT)
- Consultant for OWASP Thailand Chapter
- Committee Member of Cloud Security Alliance (CSA), Thailand Chapter.

Agenda

- Cybersecurity Trends
- The Art of (Cyber) War
- Demo: How the Attacker Attacks with Malware

Cybersecurity Trends

Security Professionals Biggest Sources of Concern Related to Cyber Attacks

Mobile Devices

58%

Data in Public Cloud

57%

Cloud Infrastructure

57%

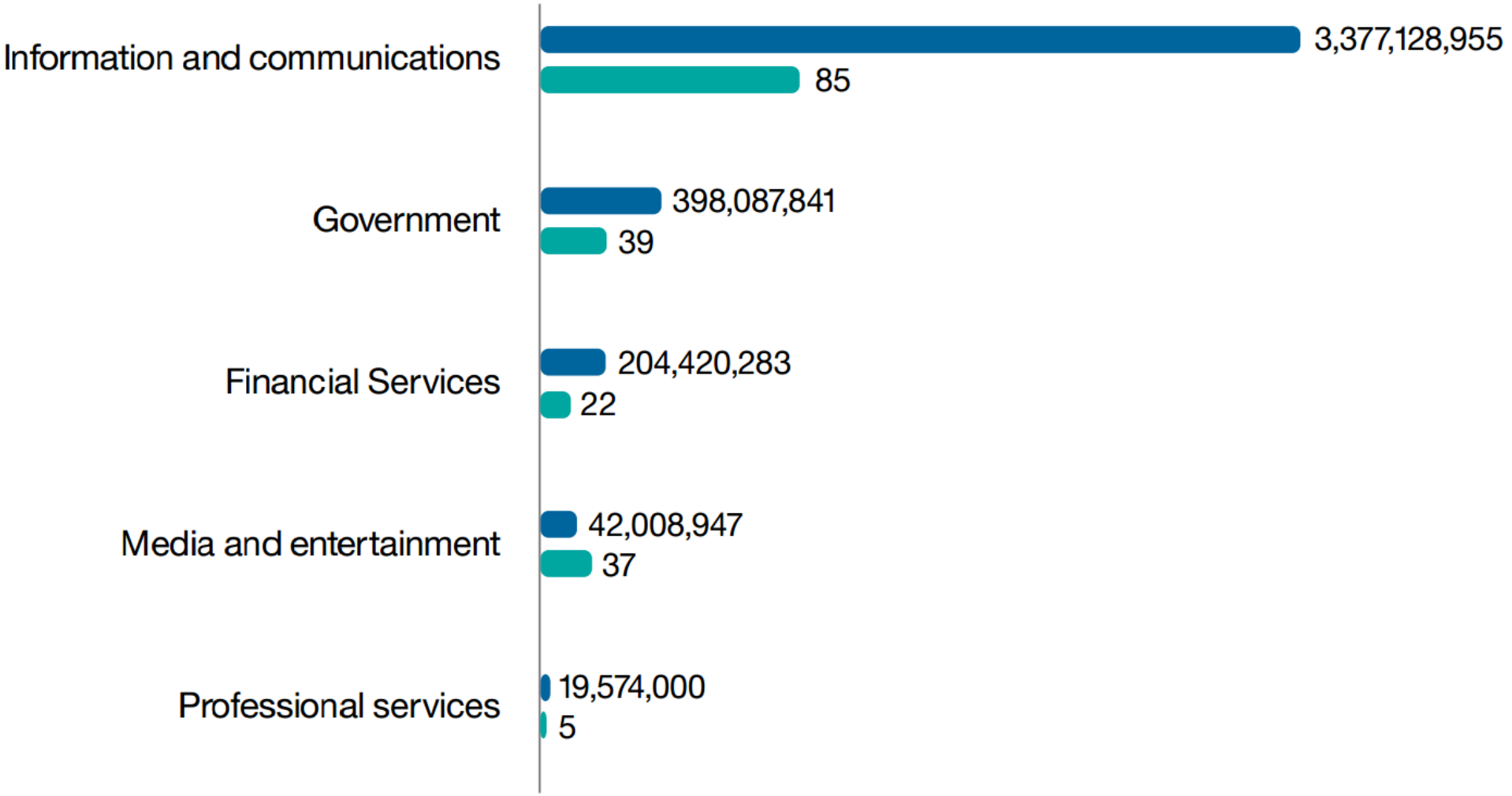
User Behavior
(For Example, Clicking Malicious Links in Email or Websites)

57%

Percentage of Security Professionals Who Find the Categories Very or Extremely Challenging

Source: Cisco 2017 Security Capabilities Benchmark Study

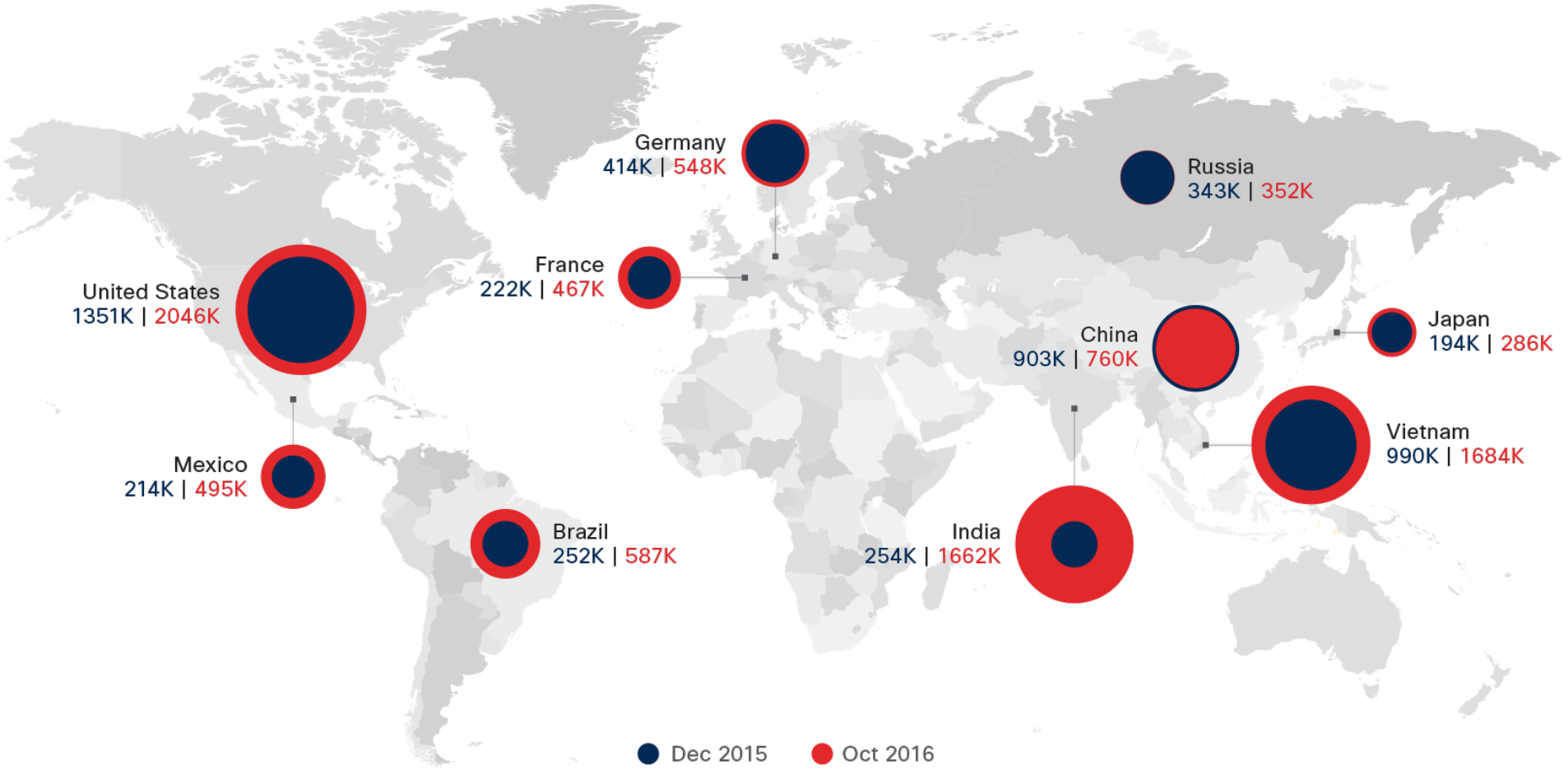
Industries Most Frequently Breached in 2016



Source: IBM X-Force Threat Intelligence Index 2017

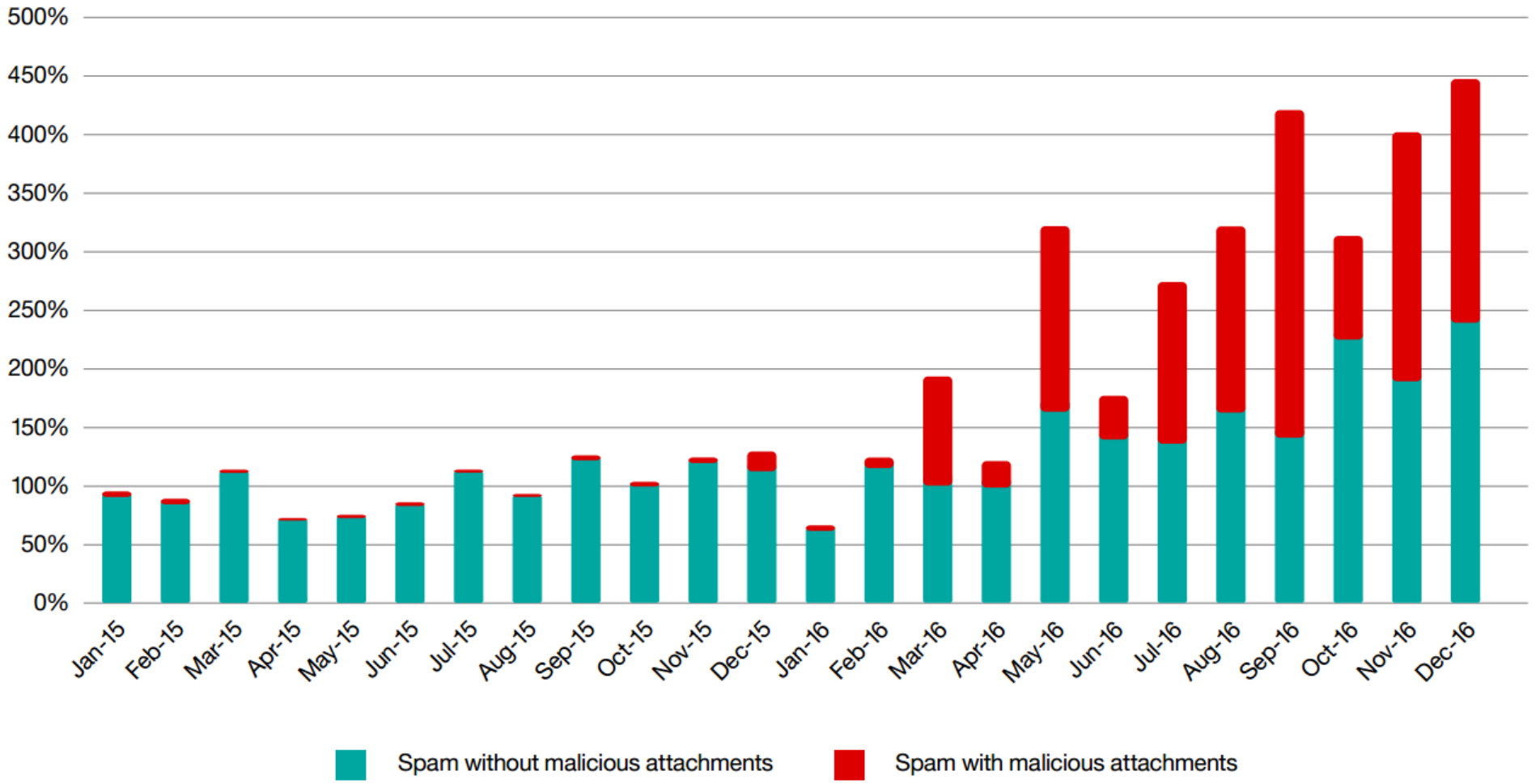
Spam Mail Source IP Blocks by Country

Dec 2015 - Nov 2016



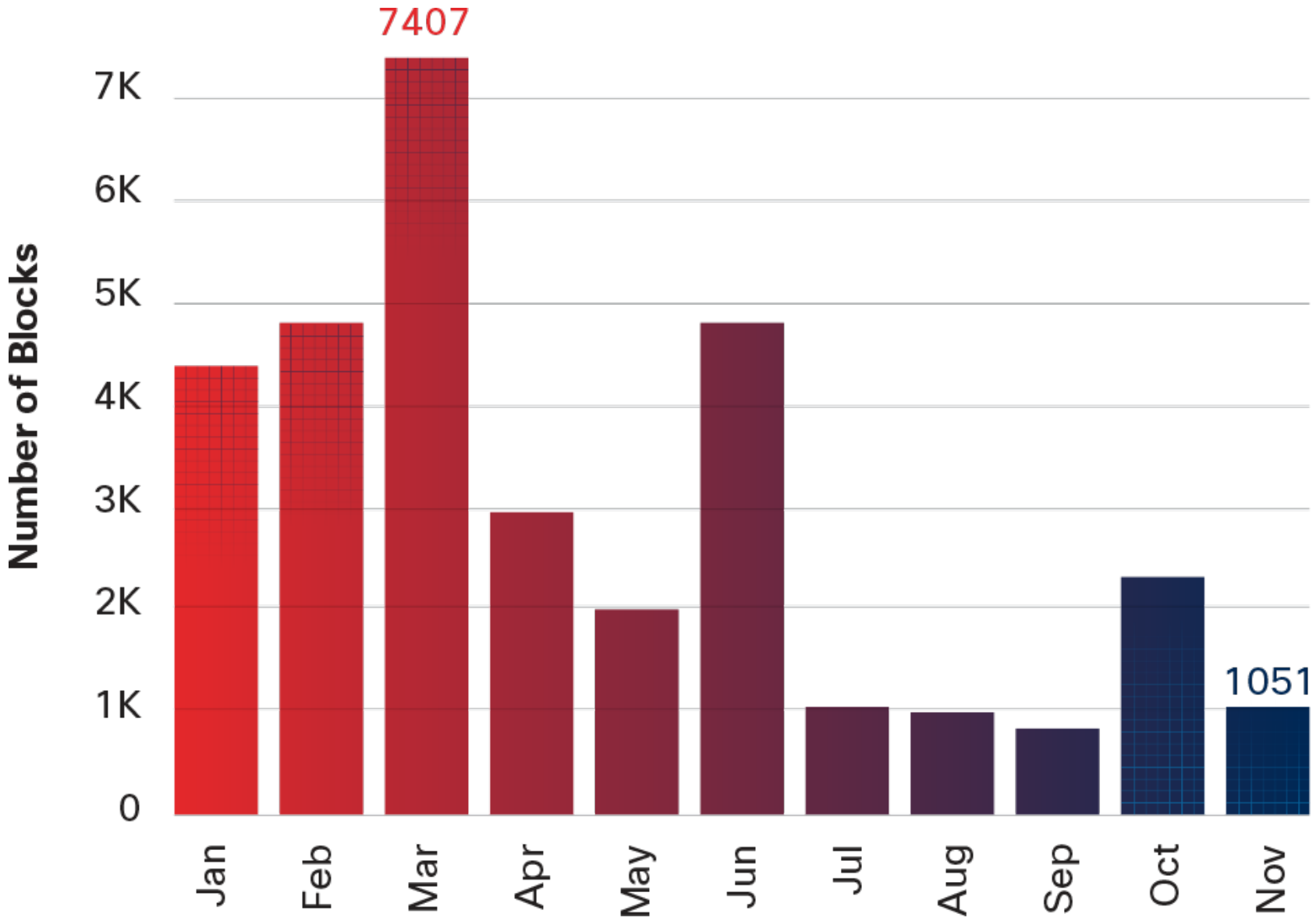
Source: Cisco Security Research

Spam Volume and Spam with Malicious Attachments



Source: IBM X-Force Threat Intelligence Index 2017

Malware in Web Page Blocks,
Jan - Nov 2016



Source: Cisco Security Research

Vulnerabilities Found by Document Type from Top 62 Critical Vulnerabilities

PDF

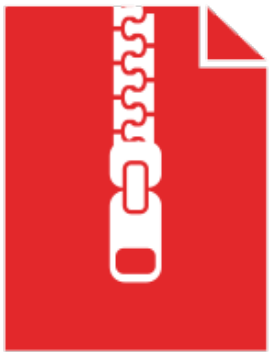
20

Image

12

Office

10



Compression

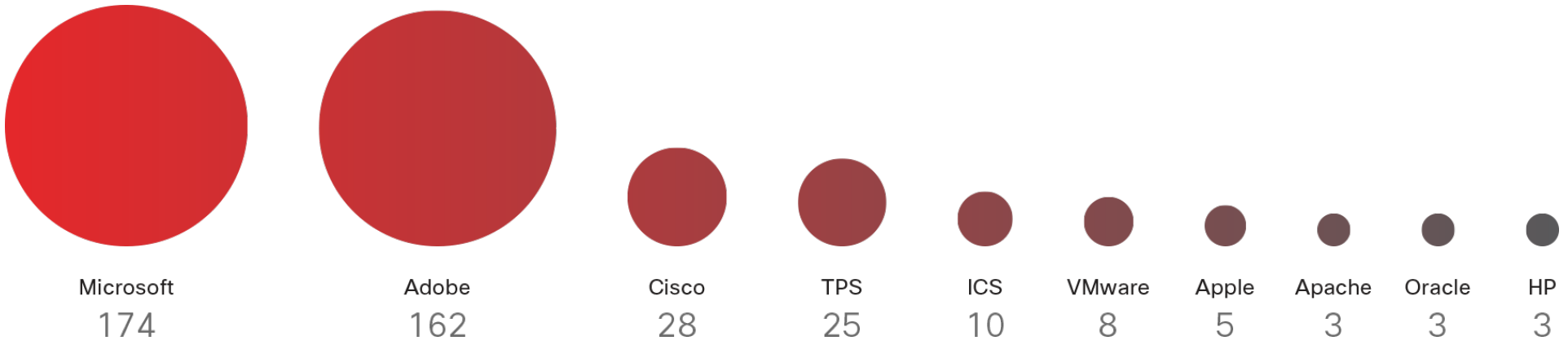
9

Other

11

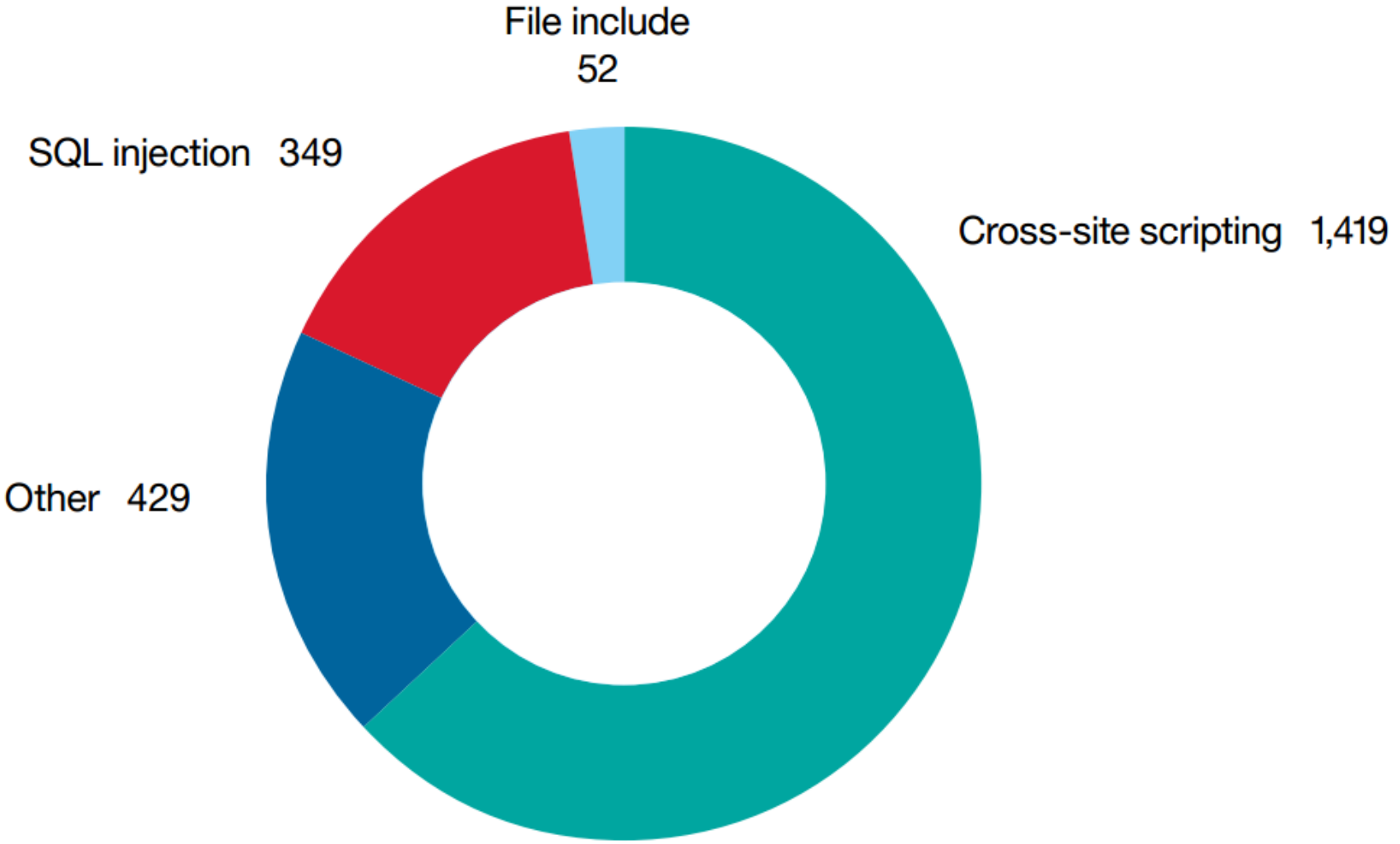
Source: Cisco Security Research

Critical Vulnerability Advisories by Vendor



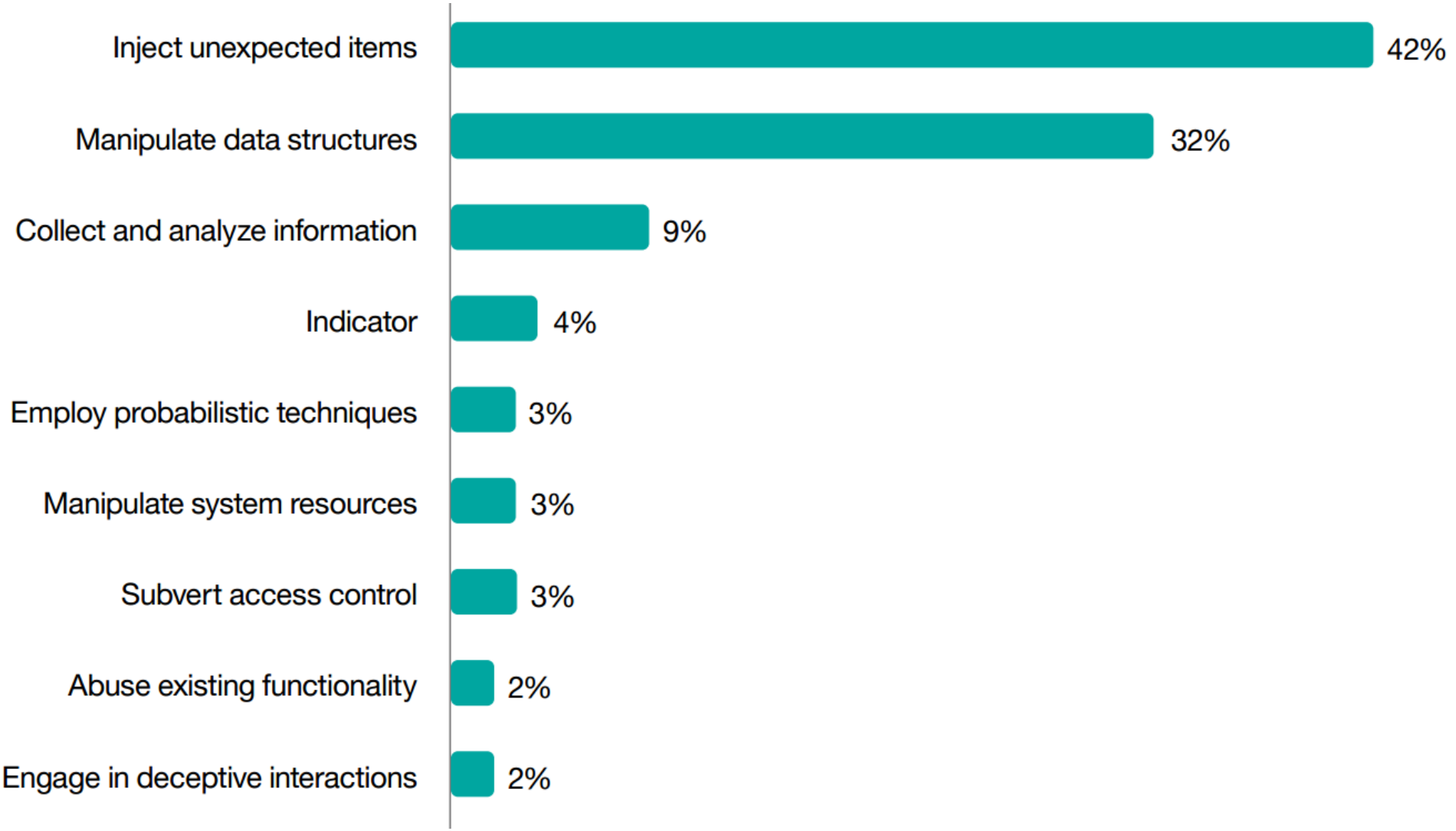
Source: Cisco Security Research

Web Application Vulnerability Disclosures in 2016



Source: IBM X-Force Threat Intelligence Index 2017

Top Attack Types
1 Jan - 31 Dec 2016



Source: IBM X-Force Threat Intelligence Index 2017

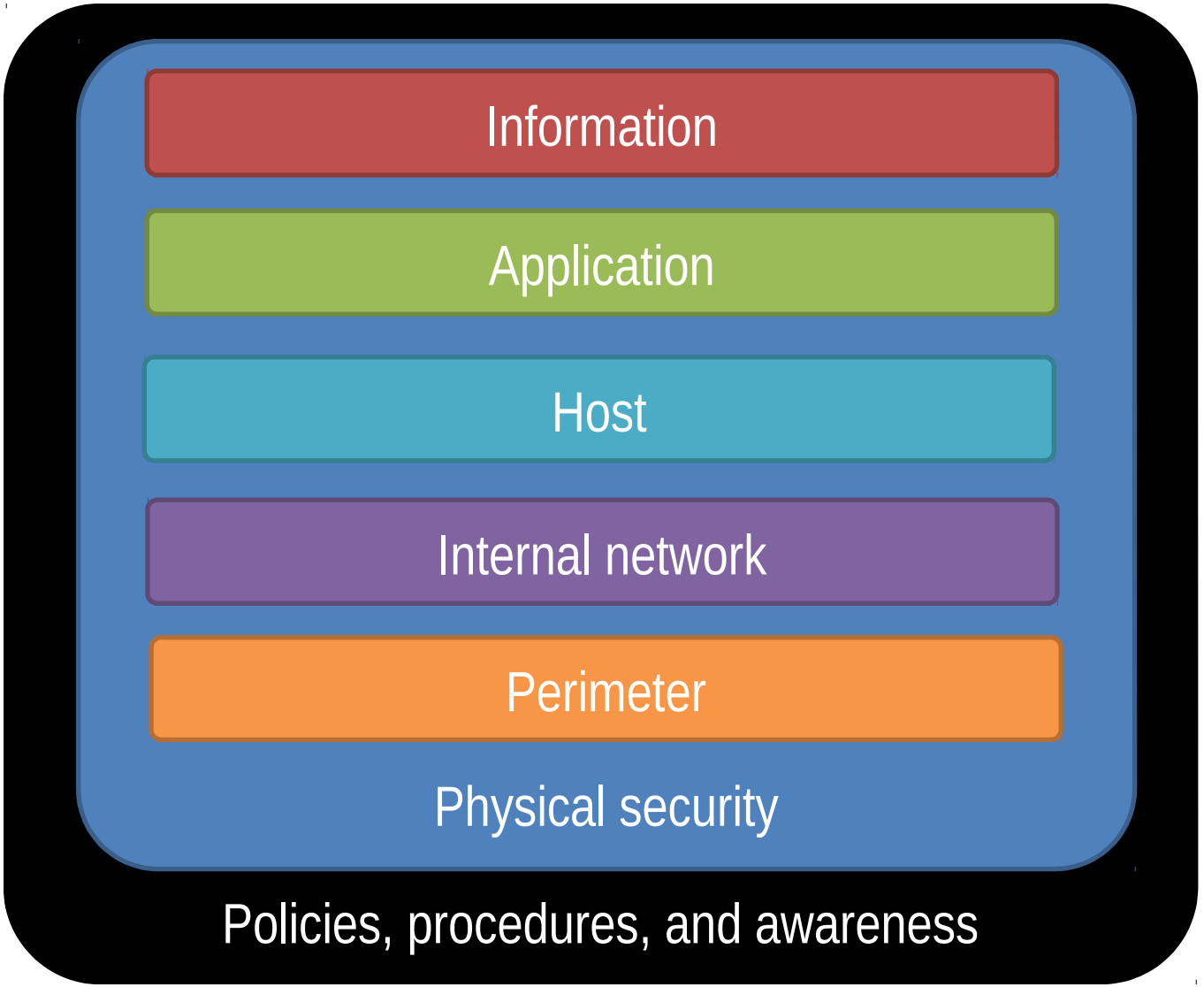
The Art of (Cyber) War

The Art of War

If you know the enemy and
know yourself, you need not fear
the result of a hundred battles.
If you know yourself but not
the enemy, for every victory gained
you will also suffer a defeat.
If you know neither the enemy
nor yourself, you will succumb in
every battle.

Sun Tzu

Know Yourself: Holistic Security



What is Information Security?

- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information
- Necessary tools: policy, awareness, training, education, technology
- C.I.A. triangle was standard based on confidentiality, integrity, and availability
- C.I.A. triangle now expanded into list of critical characteristics of information

Core Information Security Principles

To ensure protection against unauthorized access to or use of confidential information

To ensure that information and vital services are assessable for use when required

To ensure the accuracy and completeness of information to protect university business processes

Confidentiality

“การรักษาความลับ” (Confidentiality) หมายความว่า การรักษาหรือสงวนไว้เพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์จากการเข้าถึง ใช้ หรือเปิดเผยโดยบุคคลซึ่งไม่ได้รับอนุญาต

พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

Integrity

“การรักษาความครบถ้วน” (Integrity) หมายความว่า การดำเนินการเพื่อให้ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์อยู่ในสภาพสมบูรณ์ขณะที่มีการใช้งาน ประมวลผล โอน หรือเก็บรักษา เพื่อมิให้มีการเปลี่ยนแปลง แก้ไข ทำให้สูญหาย ทำให้เสียหาย หรือถูกทำลายโดยไม่ได้รับอนุญาตหรือโดยมิชอบ

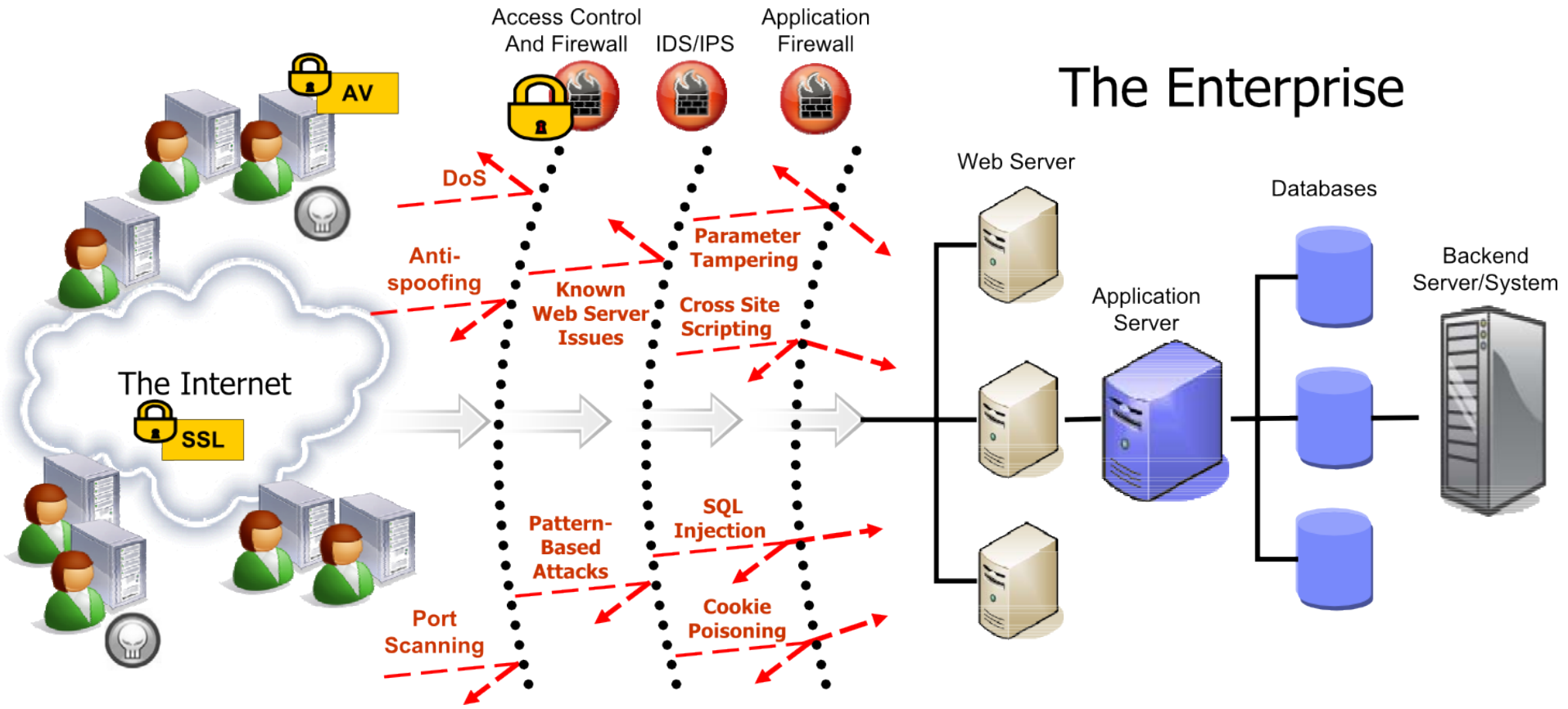
พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

Availability

“การรักษาสภาพพร้อมใช้งาน” (Availability) หมายความว่า การจัดทำให้ทรัพย์สินสารสนเทศสามารถทำงาน เข้าถึง หรือใช้งานได้ในเวลาที่ต้องการ

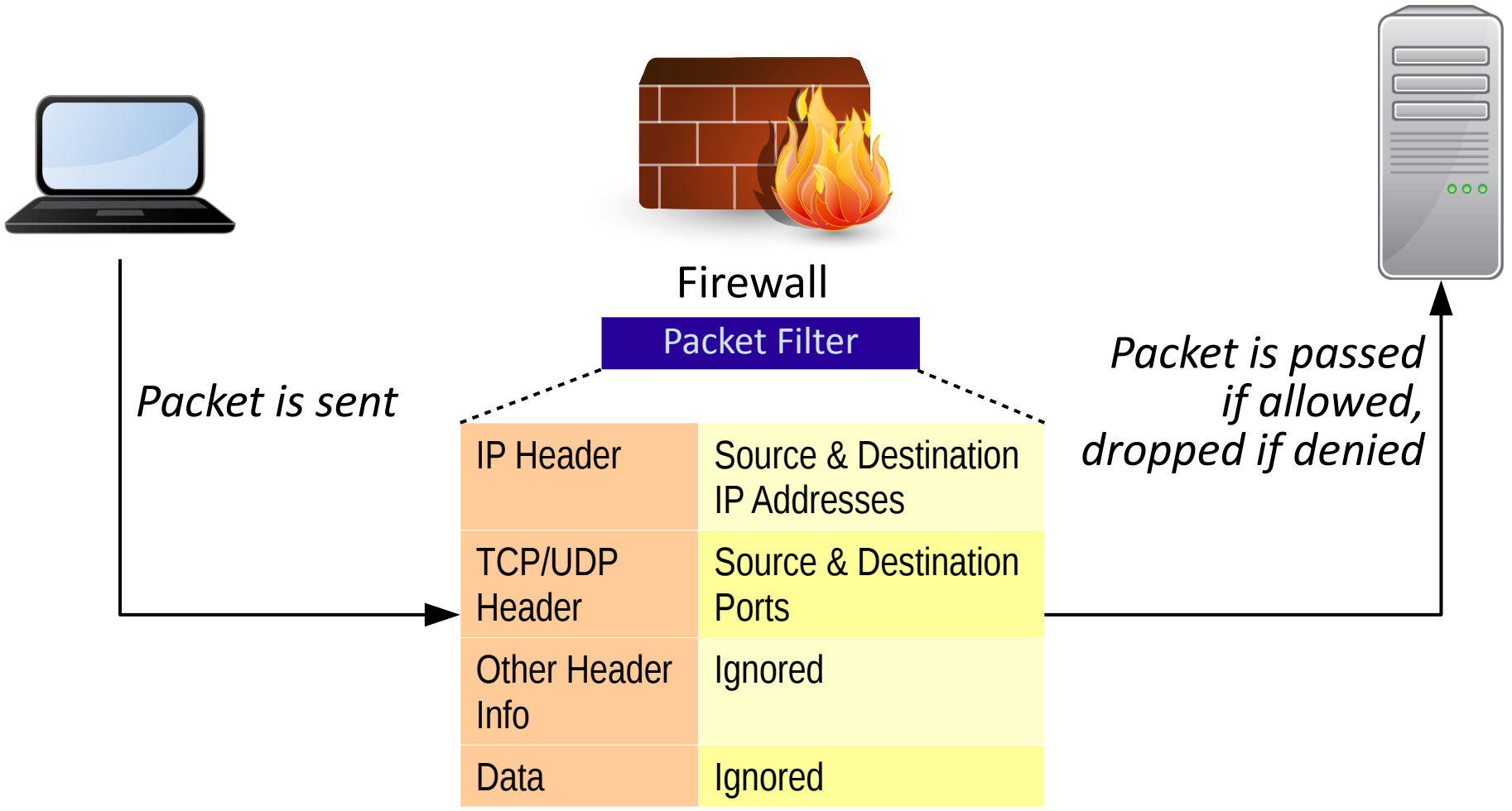
พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

Know Your Enemies #1: Attacks Directly to Servers



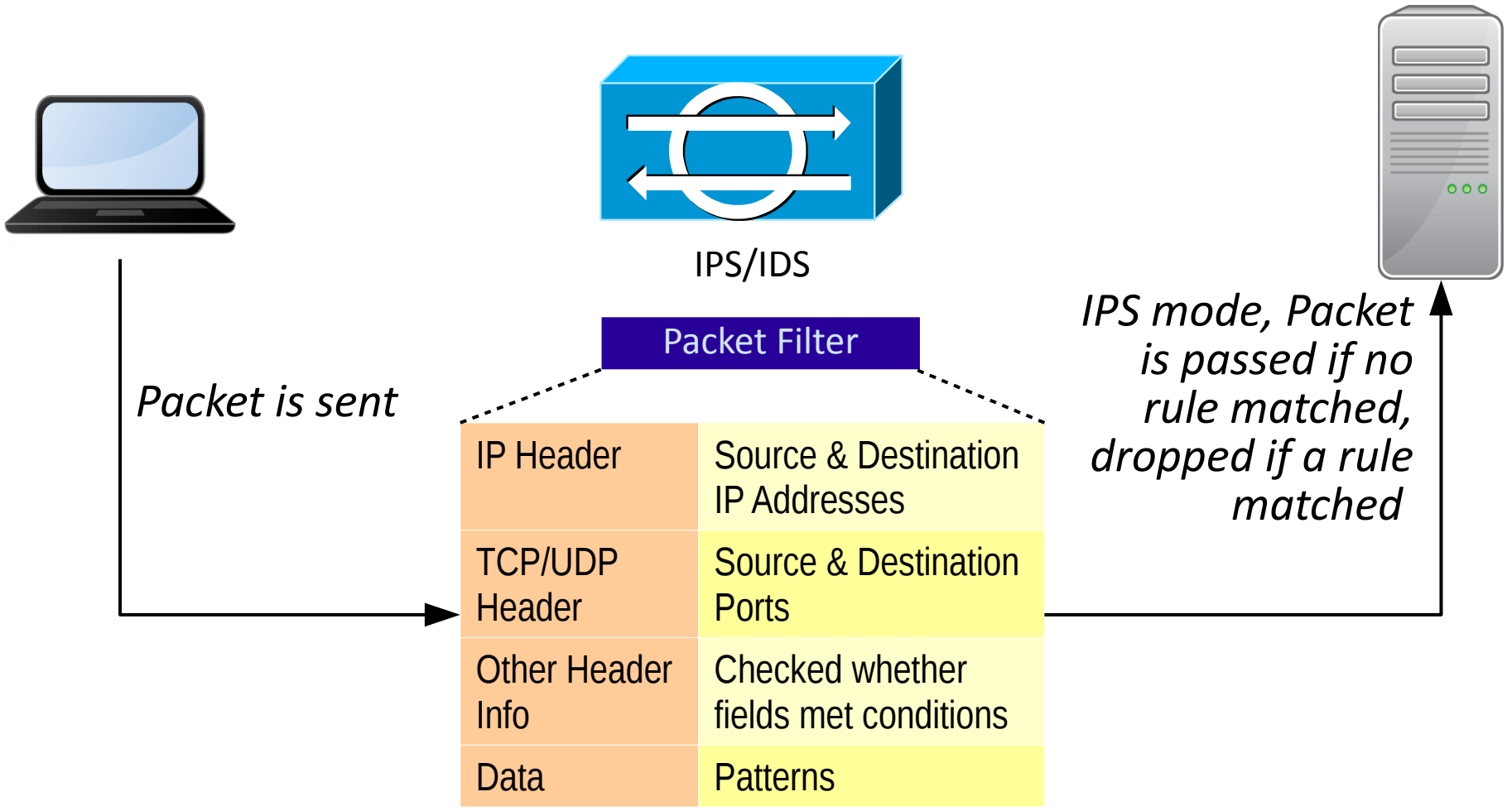
Source: IBM Software Group, Rational Software

Firewall



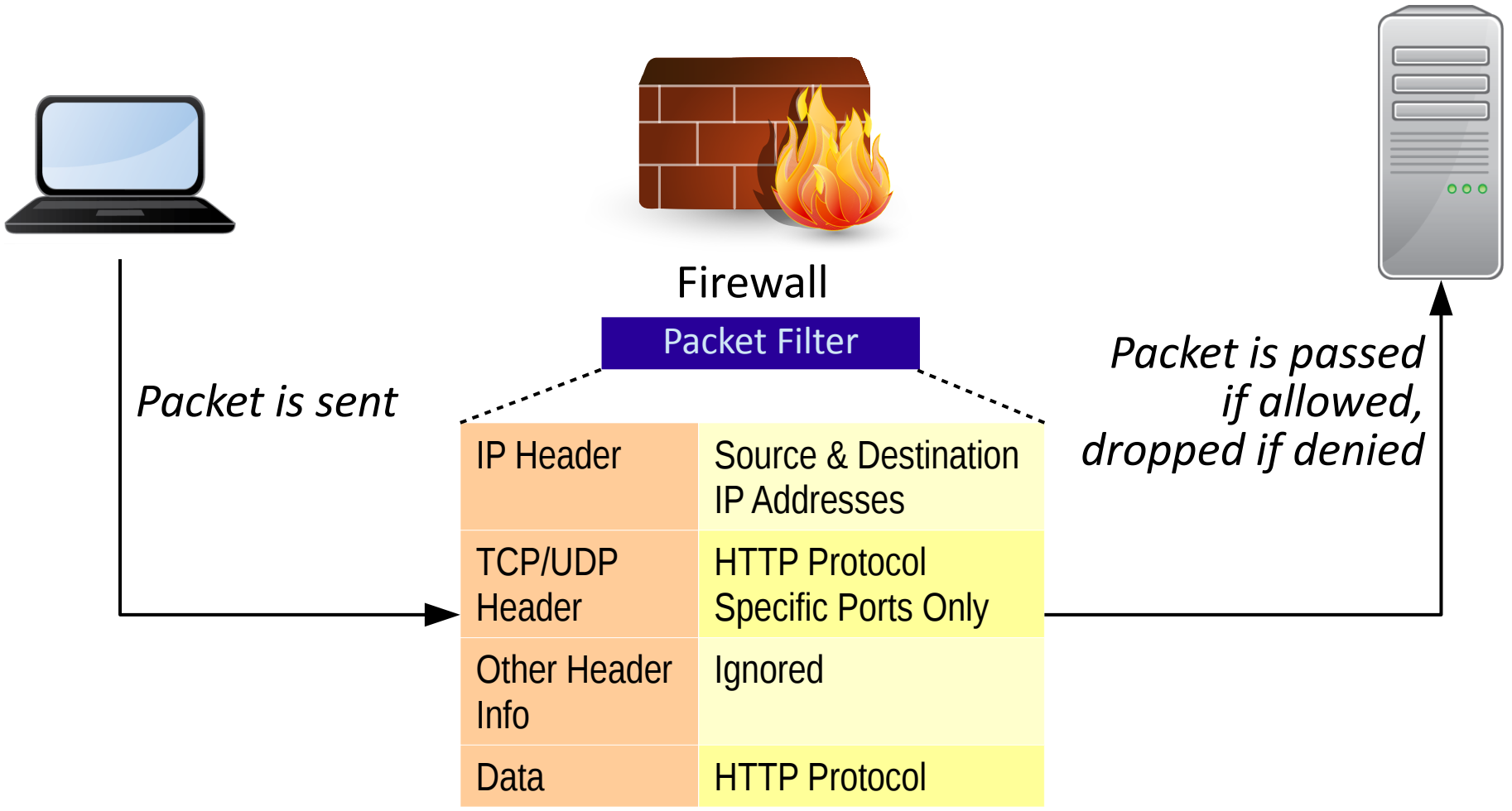
Packet is matched against filter rules and state table

IPS/IDS



Packet is matched against data patterns in rules
IPS = Intrusion Prevention System, drop if a rule matches
IDS = Intrusion Detection System, not drop but alert on a rule matches

Web Application Firewall (WAF)



Packet is matched against filter rules and HTTP specific request and response messages.
Some WAF can learn page sequence behaviors.

Steps for Conducting Crime to Servers

- Reconnaissance (Foot Printing)
- Enumeration & Fingerprinting
- Identification of Vulnerabilities
- Attack – Exploit the Vulnerabilities
- Gaining Access
- Escalating Privilege
- Covering Tracks
- Creating Back Doors

Attackers Have Shifted Their Focus to Target Applications.

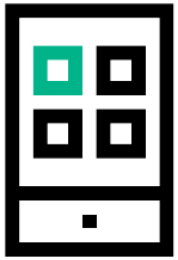
Improving user accessibility and ease of use also increases ease of access for attackers.

Application exploit toolkits are increasingly available on the attack marketplace.

Many major breaches in 2015 targeted applications.

Source: Cyber Risk Report 2016 highlights, Hewlett Packard Enterpr

Key Takeaways for Application Security



Web and mobile applications offer hackers new entry points to steal sensitive enterprise data.

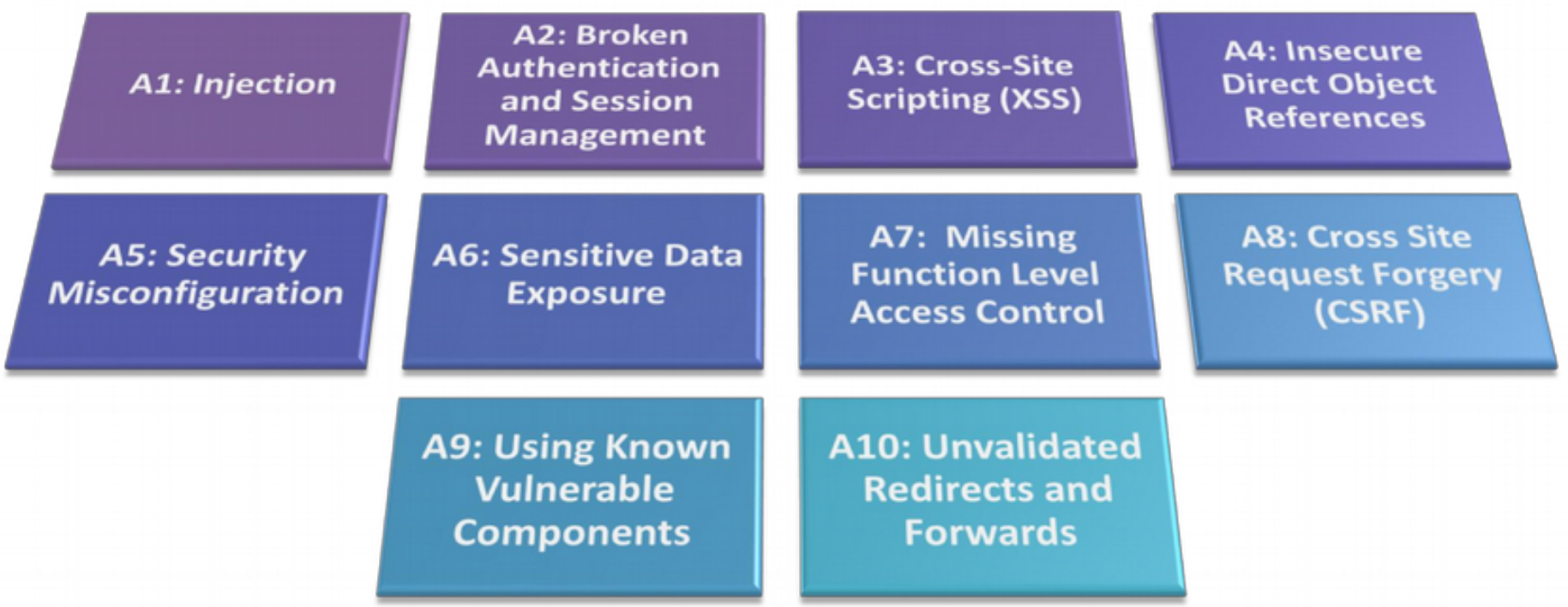
Fundamental coding errors with security implications are still prevalent.

Remediation of vulnerabilities is taking too long.

Source: Cyber Risk Report 2016 highlights, Hewlett Packard Enterprise

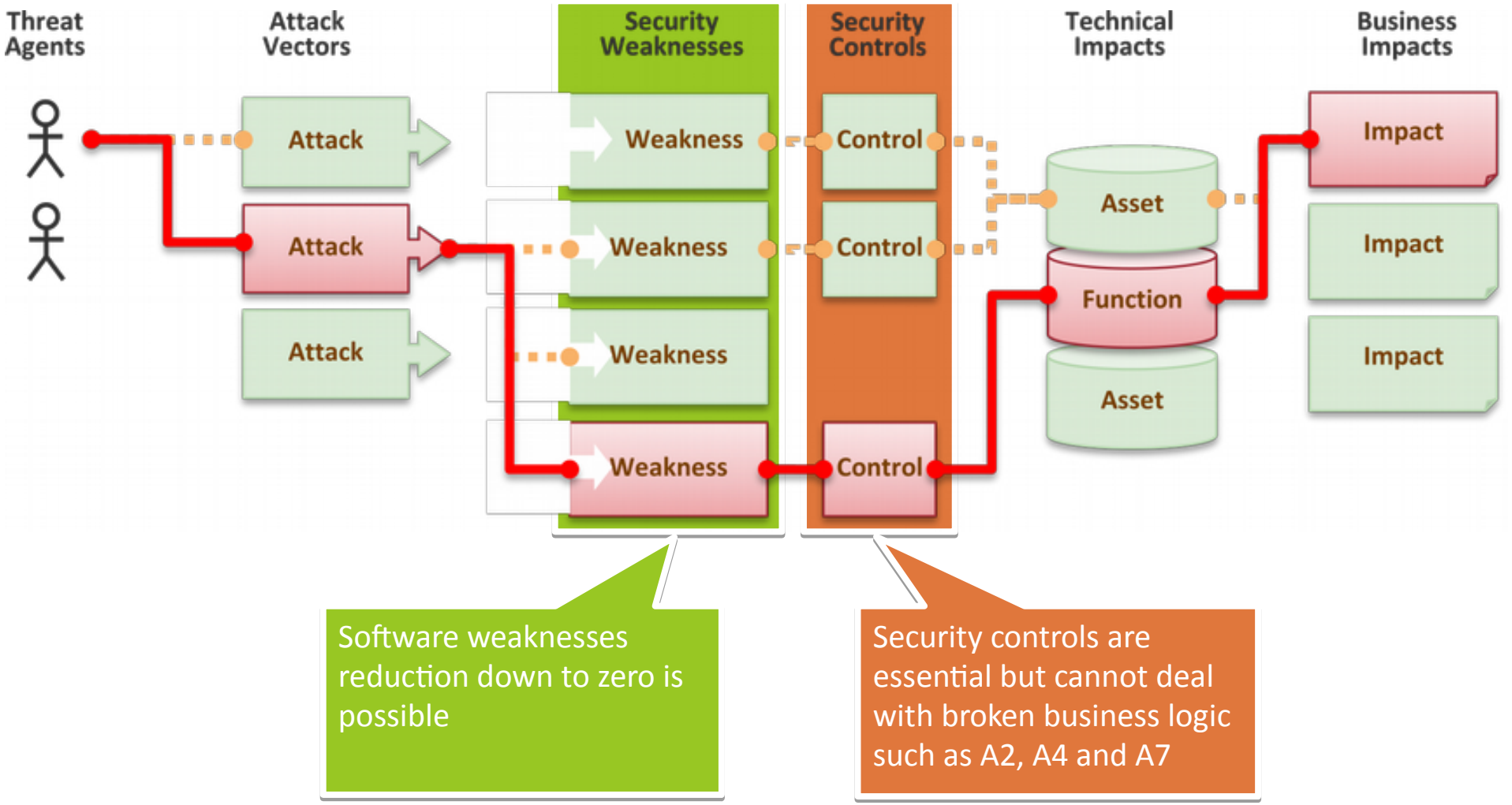

Secure Your
Applications

OWASP Top 10 2013 Risk

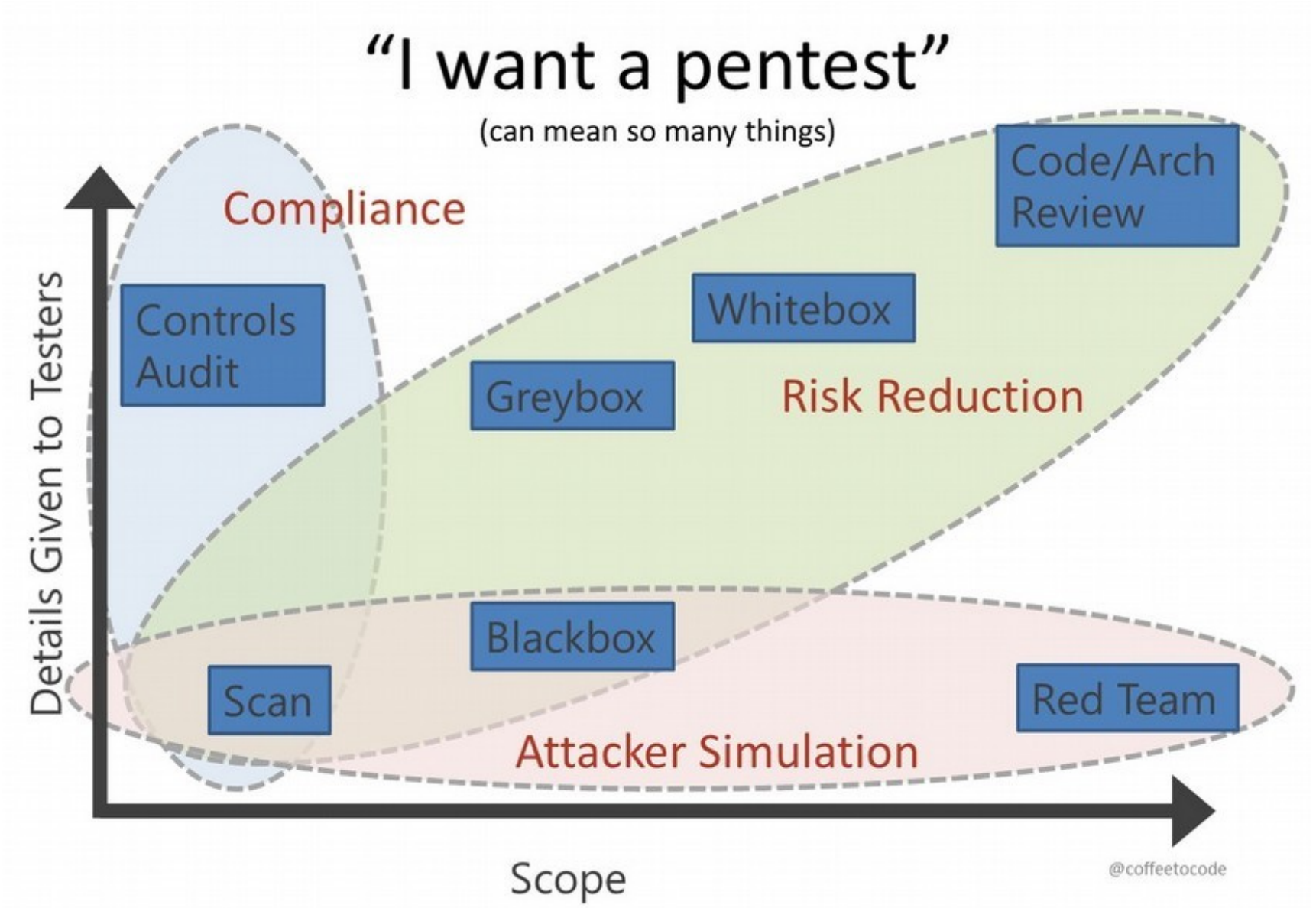


Source: OWASP: Open Web Application Security Project

Reduce Security Weaknesses vs Increase Security Controls

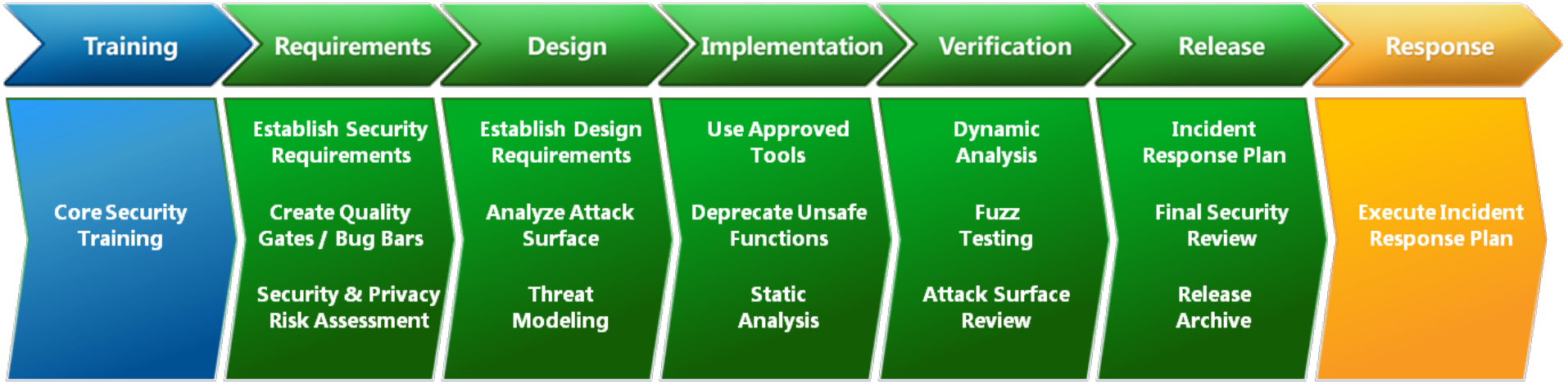


Source: OWASP: Open Web Application Security Project



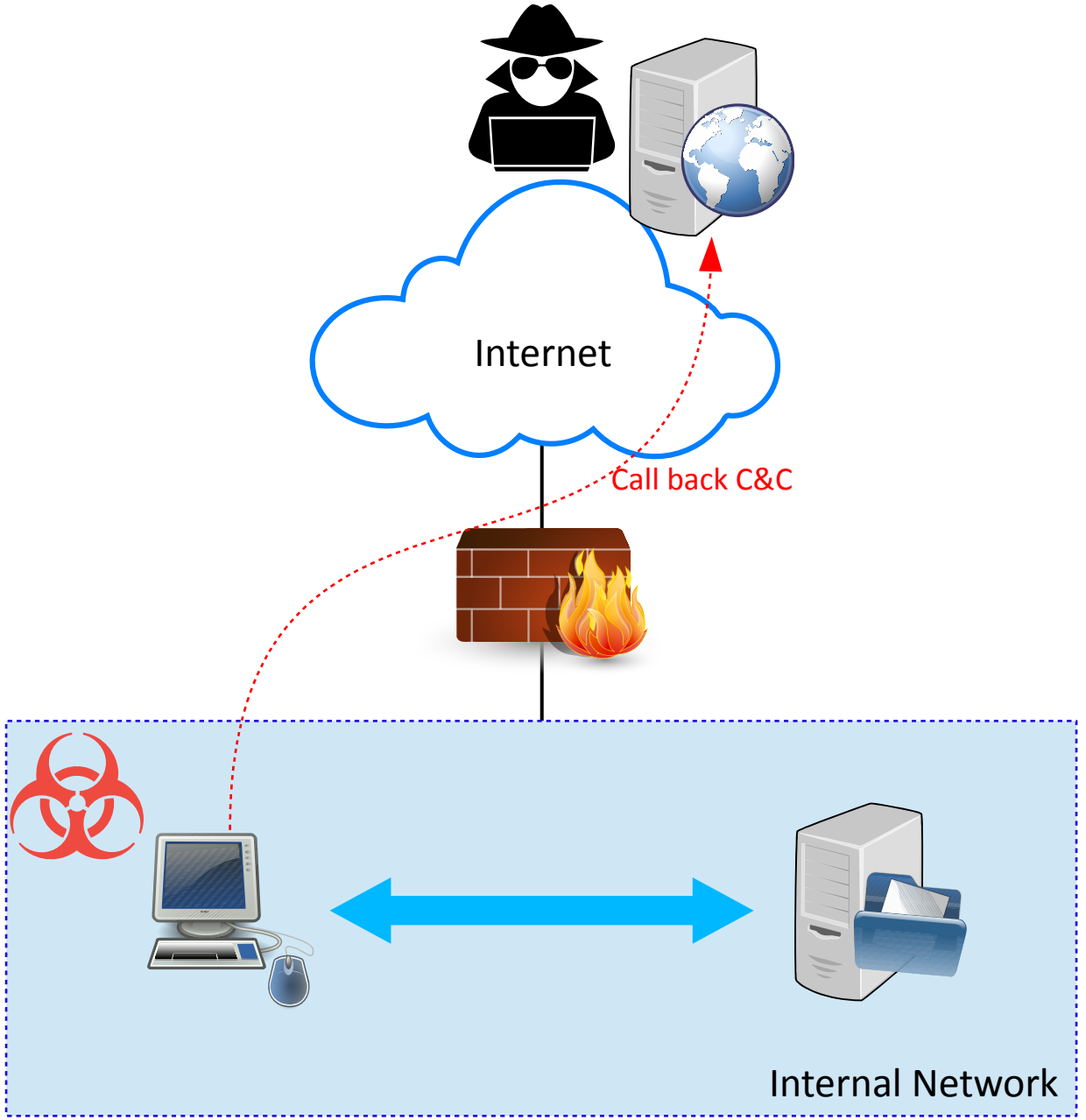
Source: Patrick Thomas (twitter @coffeetocode)

Software Security Development Lifecycle



https://www.microsoft.com/en-us/sdl

Know Your Enemies #2: Attacks with Malware



Steps for Conducting Crime with Malware

- Reconnaissance (Foot Printing)
- Assembly (Criminal creates, customizes, or otherwise obtains malware to satisfy attack requirements)
- Delivery (Malware propagation occurs)
- Compromise (Malware infection occurs)
- Command (Malware capabilities are unleashed)
- Execution (Malware delivers data to malware operator or otherwise accomplishes attack objective)

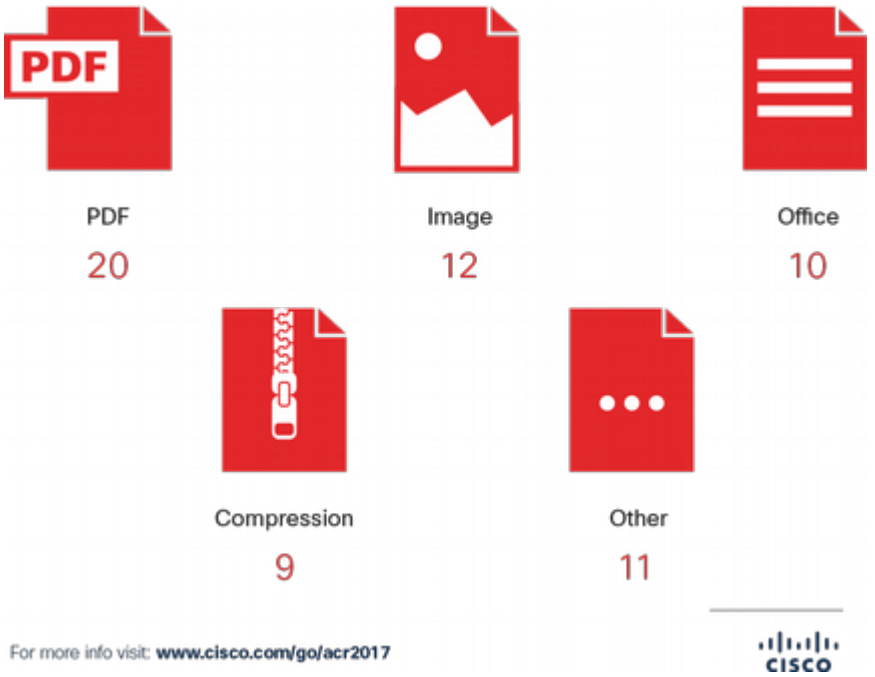

Secure Your
Workstations

Stop Conducting Crime with Malware

- ~~Stop Reconnaissance (Foot Printing).~~ Unable
- ~~Stop Assembly (Criminal creates, customizes, or otherwise obtains malware to satisfy attack requirements).~~ Unable
- Stop Delivery
- Stop Compromising
- Stop Command
- Stop Execution

Stop Delivery

- Always patch or eliminate vulnerable softwares used to open top hit vulnerable documents



- Security awareness training

User Behavior
(For Example, Clicking Malicious Links in Email or Websites)

57%

- Other security controls
  - Mail gateway
  - IPS/IDS

Stop Compromising/Command/Execution

- Workstation patches
- Workstation protections
  - End point protection
  - Advance malware protection
- Internet outgoing command detection and response
  - Need threat intelligence
  - What about encrypted channels?

Conclusion

- Know your weaknesses and reduce them
- Know your enemies and stop or delay them
- Application is the servers' last line of defense, secure software development is necessary
- Stop attacking with malware since delivery stage

Demo: How the Attacker Attacks with Malware


Q&A