INTRODUCTION TO IT SEC

Introduction to Penetration Testing

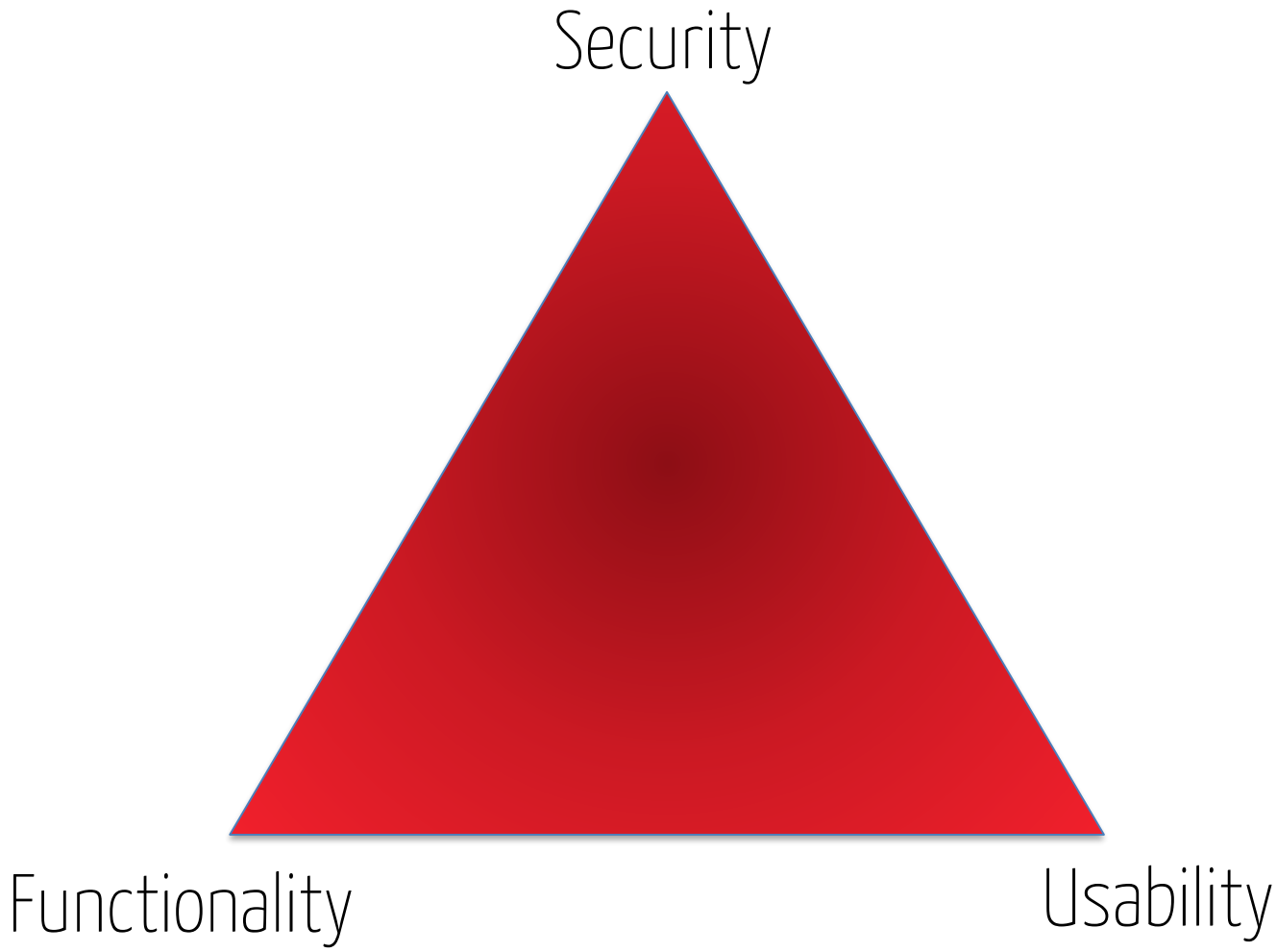
WHY THE NEED FOR SECURITY

- Evolution of technology focused on ease of use.
- Increasing complexity of computing infrastructure administration.
- Incidents of hacking is under reported in mainstream media.
- A majority of incidents are covered up to protect the reputation of the organization.
- Decreasing level of skills & knowledge required to hack.

BASIC REQUIREMENTS

- Confidentiality
  - Only allow access to data for which the user is permitted.
- Integrity
  - Ensure data is not tampered with by an unauthorized user.
- Availability
  - Ensure the system and the data is available to authorized users when needed.

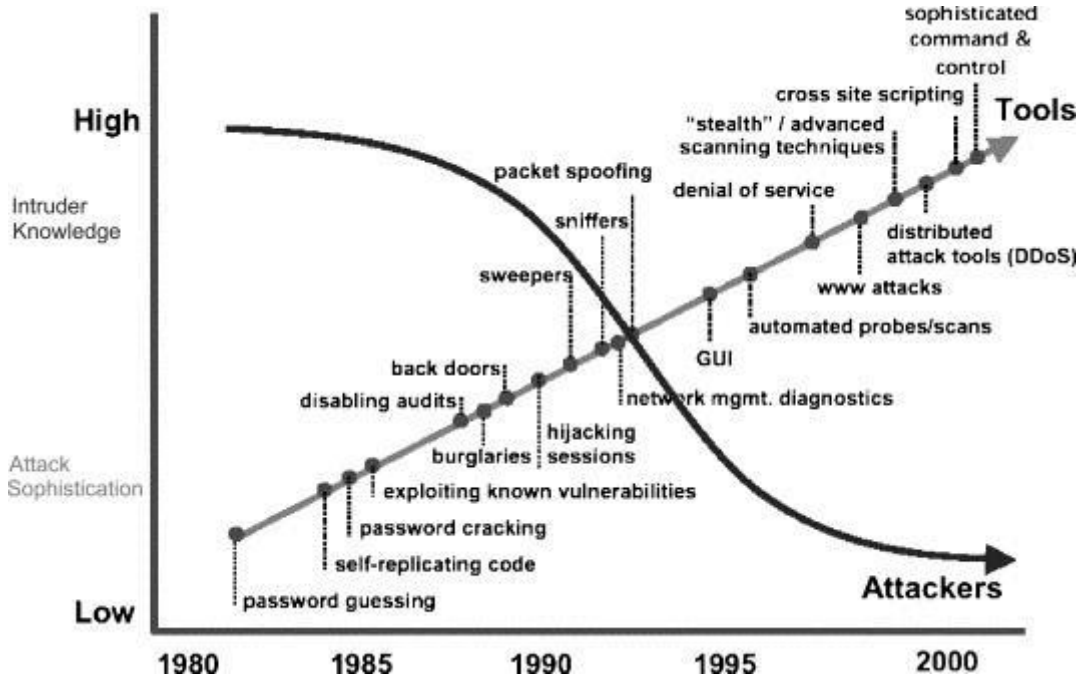
SECURITY, FUNCTIONALITY, USABILITY



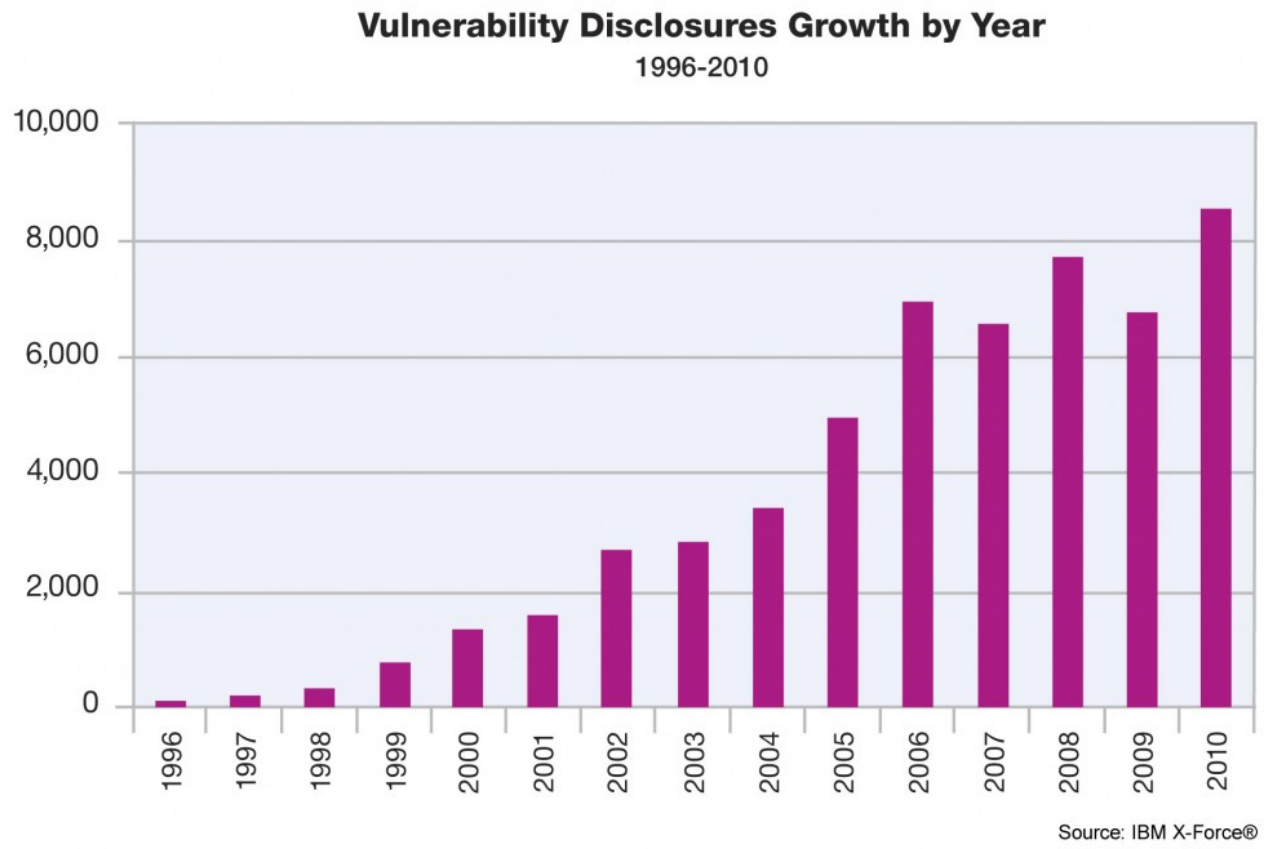
ESSENTIAL TERMINOLOGIES

- Threat
  - An event that could potentially compromise security.
- Vulnerability
  - A weakness in design or implementation in software that could lead to the compromise of security.
- Exploit
  - A piece of code or script that takes advantage of a vulnerability.
- Payload
  - The actual instruction set that gets executed by the exploit.

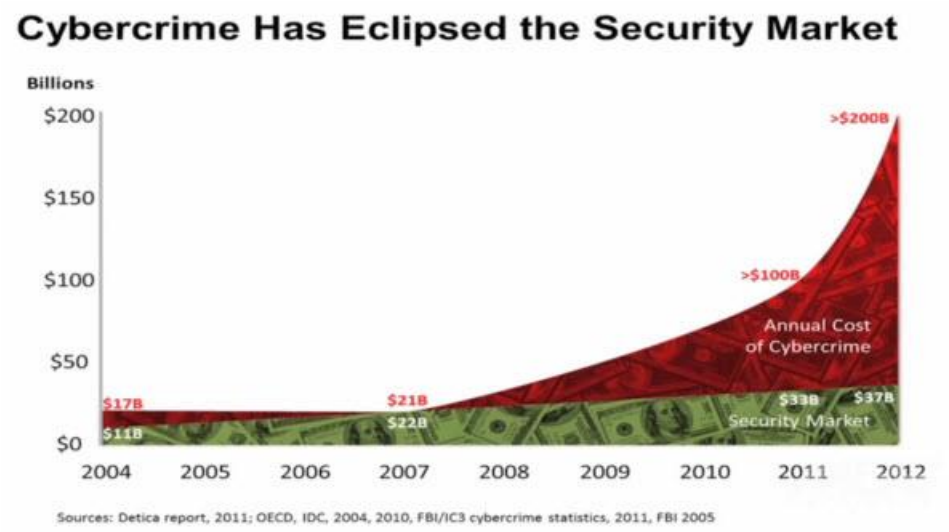
ATTACK SOPHISTICATION



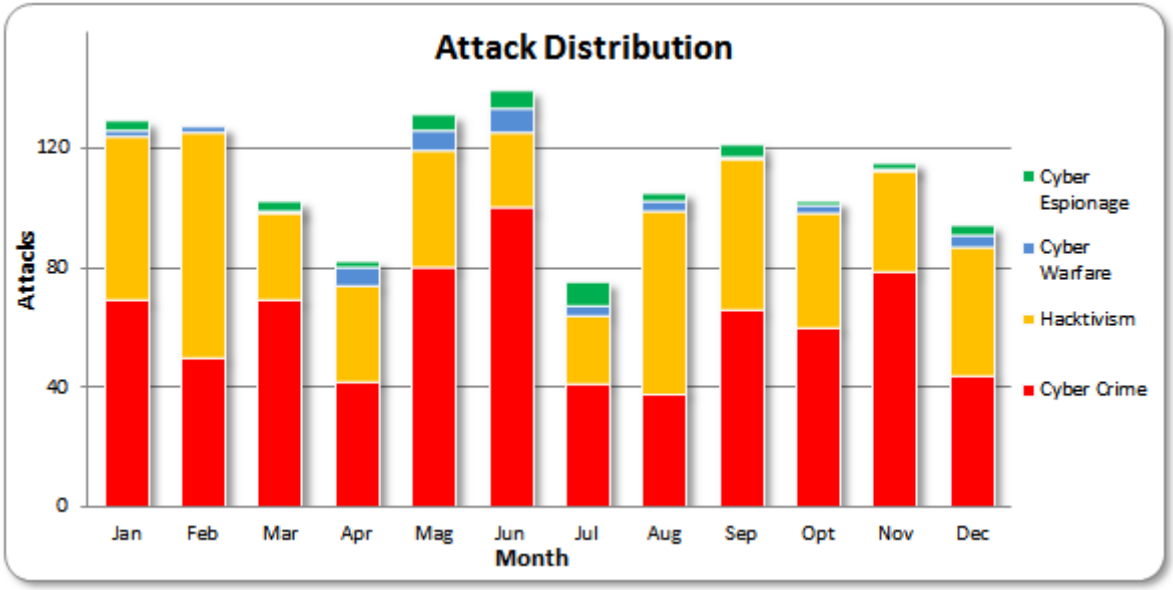
CYBER ATTACK TREND



CYBER ATTACK TREND



CYBER ATTACK TREND

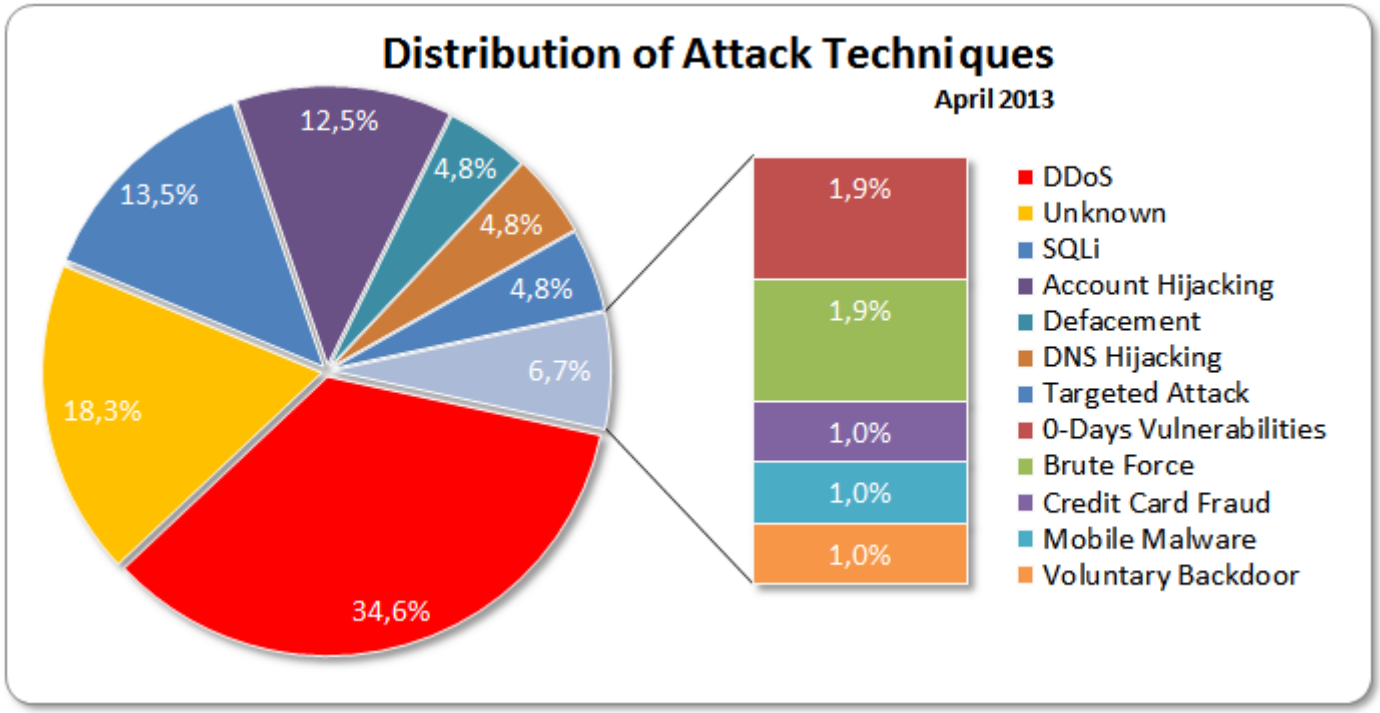


Source: http://paulsparrows.files.wordpress.com/2012/06/2012-attack-distribution.png

TYPES OF THREATS

- Server-side vulnerabilities
- Client-side vulnerabilities
- Web attacks
- Denial of Service (DoS & DDoS)
- Network vulnerabilities
- Social engineering
- Man in the middle
- Phishing
- Malware

TYPES OF THREATS



Source: http://paulsparrows.files.wordpress.com/2013/05/techniques-april-2013.png

TYPES OF THREATS

- 30% of attacks are carried out by employees internally.
- 70% of damage is caused by internal attacks.

- 70% of attacks are carried out over the Internet.
- 30% of damage is caused by external attacks.

CASE STUDY

ars technica

MAIN MENU ▾ MY STORIES: ▾ FORUMS SUBSCRIBE NOW

LAW & DISORDER / CIVILIZATION & DISCONTENT

Anonymous speaks: the inside story of the HBGary hack

After interviews with the hackers from Anonymous who invaded HBGary Federal …

by **Peter Bright** - Feb 16, 2011 2:00 am UTC

BLACK HAT INTERNET CRIME

It has been an embarrassing week for security firm HBGary and its HBGary Federal offshoot. HBGary Federal CEO Aaron Barr thought he had unmasked the hacker hordes of Anonymous and was preparing to name and shame those responsible for co-ordinating the group's actions, including the denial-of-service attacks that hit MasterCard, Visa, and other perceived enemies of WikiLeaks late last year.

When Barr told one of those he believed to be an Anonymous ringleader about his forthcoming exposé, the Anonymous response was swift and humiliating. HBGary's servers were broken into, its e-mails pillaged

THE HBGARY SAGA

Colbert Report features Ars Anonymous/HBGary coverage

Anonymous vs. HBGary: the aftermath

Black ops: how HBGary wrote backdoors for the government

Spy games: Inside the convoluted plot to bring down WikiLeaks

(Virtually) face to face: how Aaron Barr revealed

CASE STUDY

FierceCIO
THE EXECUTIVE IT MANAGEMENT BRIEFING

NEWS TOPIC

TOPICS: Data and Business Intelligence | Leadership and Best Practices | Security and Privacy

Lessons learned from an internal hack event

July 23, 2006

SHARE

Email

Share

TOOLS

The recent trial and last week's conviction of an systems admin charged with hacking the network at employer UBS PaineWebber was prominent in the news for the past month or so. As experts relate, however, the most interesting aspect of the criminal case is hitting home now as the logic bomb event that crashed 2,0000 servers on the trading company's network is bringing some good lessons learned and best practices into play. Security pundits say the case illustrates how internal threats are just as dangerous and require just as much attention as external threats and that poor internal security can actually help malcontents pull off such malicious attacks. Companies need to shore up monitoring and auditing of network administrator's work and keep a good close eye on those who have the power, access and the skills to do such damage.

TYPES OF ATTACKERS

- Black hats
  - Extraordinary computer skills
  - Skills used for malicious intent.
- White hats
  - Extraordinary computer skills
  - Skills used for defensive intent.
- Grey hats
  - A cross breed of black hat and white hat.

BASIC SECURITY MEASURES

- Policy
- Risk management
- Security architecture & design
- User issues
- System & network management
- Authentication & authorization
- Monitor & audit
- Physical security
- Continuity planning & disaster recovery

BASIC SECURITY MEASURES

Policy

- Security policies are written rules detailing how computer systems should be configured and how the employees should operate them.
- They must be well maintained and implemented.
- Serves as a baseline for implementations.

BASIC SECURITY MEASURES

Risk Management

- Identifying critical assets and the risks to those assets.
- Identify adverse impacts when risks to critical assets are realized.
- Quantify the financial impact to the greatest extent possible.
- Have a risk mitigation plan ready.

BASIC SECURITY MEASURES

Security Architecture & Design

- Maintain a complete system inventory.
- Identify which assets to secure the most and why.
- The assets may include:
  - Hardware
  - Software
  - Data
  - Devices

BASIC SECURITY MEASURES

User Issues

- Employees should be trained by a professional on basic security practices to provide more awareness.
- Some security breaches are in fact due to the lack of awareness. For example, connecting a company laptop to a public wireless network.
- Accountability must be enforced on employees.

BASIC SECURITY MEASURES

System & Network Management

- Consider the user of access controls on your network.
- Use encryption technologies such as VPN for remote connections to the company network.
- Do regular checks to verify software integrity.
- Do regular checks for malware.
- Provide procedures to ensure secure configuration of all deployed assets.
- Keep your network diagrams up-to-date.
- Perform security assessments on a periodic bassis.
- Regularly perform back up procedures.
- Review log files.

BASIC SECURITY MEASURES

Authentication & Authorization

- The following access controls should be enforced:
  - File level
  - Network level
  - System level
  - Application level
- Restrict access to authorized tasks and time.

BASIC SECURITY MEASURES

Monitor & Audit

- Use appropriate monitoring and auditing tools and solutions.
- Assign responsibilities for monitoring, responding and reporting off system and network events.
- Provide training to employees who are tasked with monitoring and audit.

BASIC SECURITY MEASURES

Physical Security

- Physical security is just as important as network security.
- The danger of a stolen laptop is not the cost of the hardware but the confidential data in it.
- Enforce physical security in your security policies.
- Physical devices must always be protected at all cost.
- Educate employees to detect and manage social engineering attacks.

BASIC SECURITY MEASURES

Continuity Planning & Disaster Recovery

- It's always important to plan on how to recover from a disaster so that the business can't go on.
- You should establish a plan to acquire equipment as a failover incase of a disaster.
- Disaster recovery drills should also be performed to test if the DR plan actually works.