Introduction to Dynamic Infrastructure

By Alan G. Labouseur

MARIST SCHOOL OF COMPUTER SCIENCE & MATHEMATICS

MARIST SCHOOL OF COMPUTER SCIENCE & MATHEMATICS

IBM

MODULE EIGHT

SECURITY

Introduction to Dynamic Infrastructure

Designed, compiled, written, and edited by
Alan G. Labouseur
www.Labouseur.com / Alan.Labouseur@Marist.edu

Contents

Congratulations Joey

Remarks

This is module eight, which is DI pillar six. We are making excellent progress. Is everybody feeling like a Dynamic Infrastructure guru? (I hope so.) You can put that on your resume: *Dynamic Infrastructure Guru*. I guarantee it will be a good conversation starter in any interview you have. And since you know more about Dynamic Infrastructure than most people on this (smarter) planet, it's not even bragging.

Pretty good discussions last week on the Critical C's. We even heard from Mike Lavacca. (Did you guys even know he was in class?) Mike, welcome, and thanks for the raise-to-the-power visual pun.

I also really enjoyed the counseling discussion. There is so much more to managing technology than bits and bytes, and it's good to be reminded of the human side of things. Nice going.

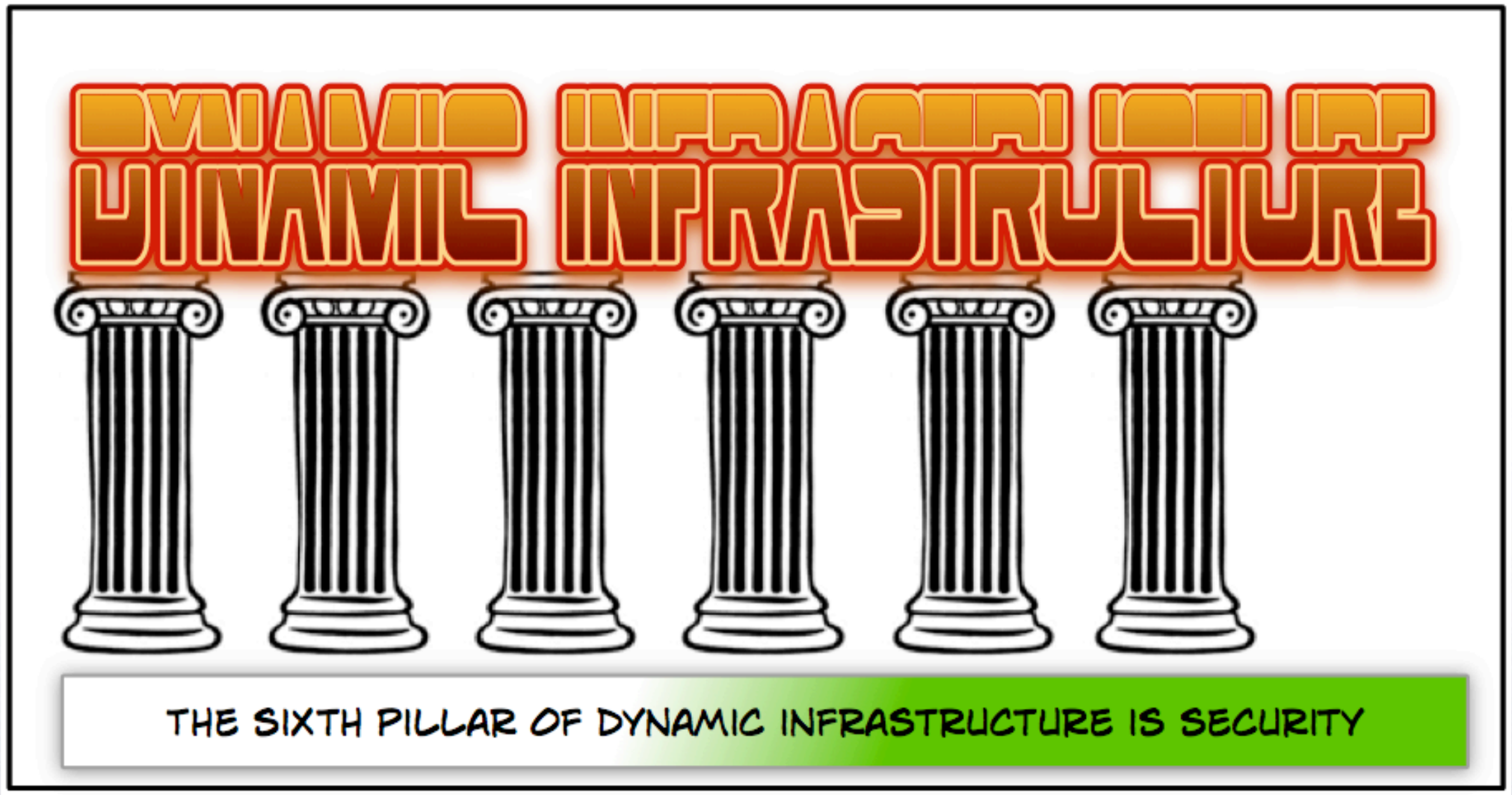
About command and control... From what I've read, it seems that you guys consider them the same, yet also different. Interesting (and at the same time, not).

Review

Let's review. Last time our intrepid (and smart) adventurers . . .

- The 5 success factors of business resiliency are command and control, communications, connectivity, contingency, and counseling.
- Business resiliency policies assist with regulatory compliance, improved systems availability, protection of your data and integration of IT operation risk management strategies.
- Business resiliency plans describe how an organization will resume critical functions which were interrupted from a disaster or disruption.
- There are 6 areas to address when making a plan: strategy, organization, processes, data and applications, technology, and facilities.
- Backups are used the case of a disaster so you can salvage your business data when the data could not be normally accessed.

Security



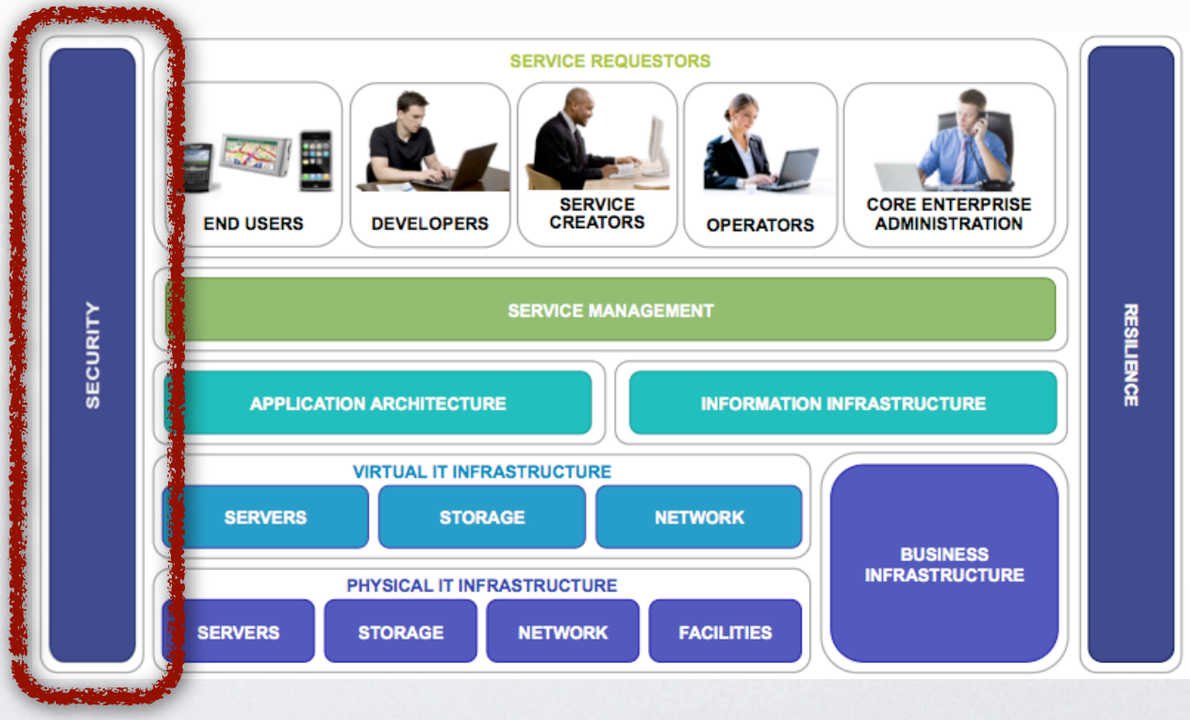
Security

Our Plan

- Preparation Questions
- Why bother?
- How Much ...?
- Strategy
- Services / Network Security / Cyber Crime
- Goals / Best Practices

Security is pervasive throughout the enterprise, ensuring resources and information are getting to (only) the right people at (only) the right time.

It also allows companies to enforce the business, local, regional, national and international rules and laws.



Security > Preparation Questions

Do you know the number of security events that have occurred in your business**?**

Do you know where your critical data is**?**

When is your data encrypted**?**

Where is your data encrypted**?**

Is security part of your Software Development process**?**

Can your prove who has looked at and/or modified personal data**?**

How hard would it be to prove that a persons data is secure**?** (Is it even possible for you to do so?)

Security › Why Bother?

Commerce, whether electronic or not, is based on trust. There's trust in the currency, trust in the merchant, trust in your own judgment… trust, trust, trust… which comes, in part, from security.

You simply cannot quantify or underestimate the damage the loss of trust in your brand image causes. The loss of trust in a brand is a devastating and sometimes fatal blow to any business. (J&J handled it right and survived. Anderson Consulting, not so much. BP… we'll see.)

"Increasingly security is viewed as a problem that is far broader than technology alone—in some instances part of the security budget comes from audit and legal departments. Some years back there were some prominent leaders of the industry who felt that security solutions would, in the final analysis, be almost exclusively technical solutions, but one would be hard-pressed to find that point of view espoused today. There have been too many data breaches driven by simple human error and carelessness." p.8

- from 2007 by Computer Security Institute

Security › How Much Money?

You cannot afford to do security just for the sake of security. You must be able to justify and explain the return on investment that information security brings to your business. Therefore understanding the financial Impact to business is a crucial step.

Here's a handy formula:

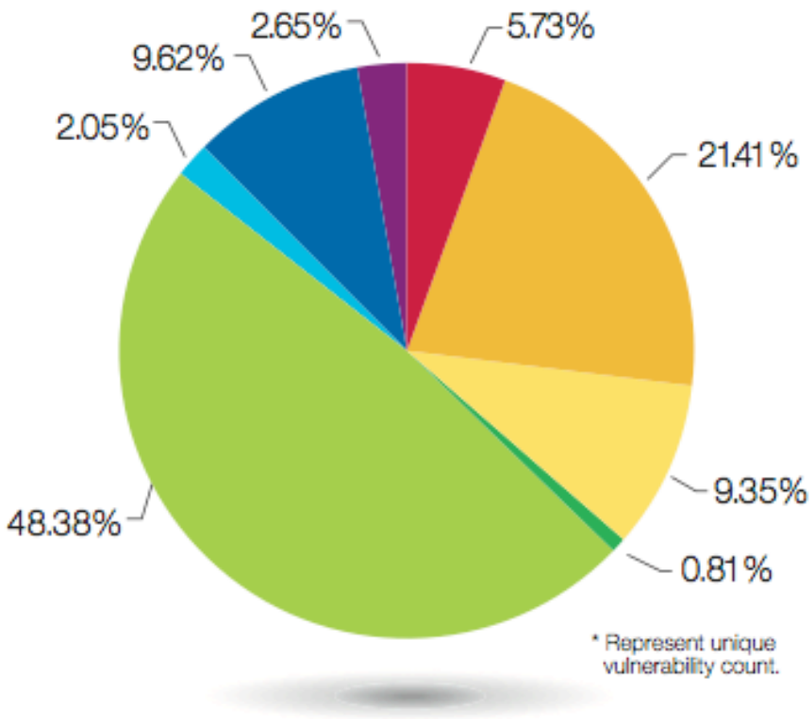
(%Chance of Attack) X (Potential Cost [direct, indirect]) = Security Budget

Security Policy - The foundation of all successful information security programs.

- Audit
  - What gets checked, gets done!
- Local Security
- Corporate Security
- External Security

Security > How Much of a Threat?

Required Reading



Source: IBM X-Force

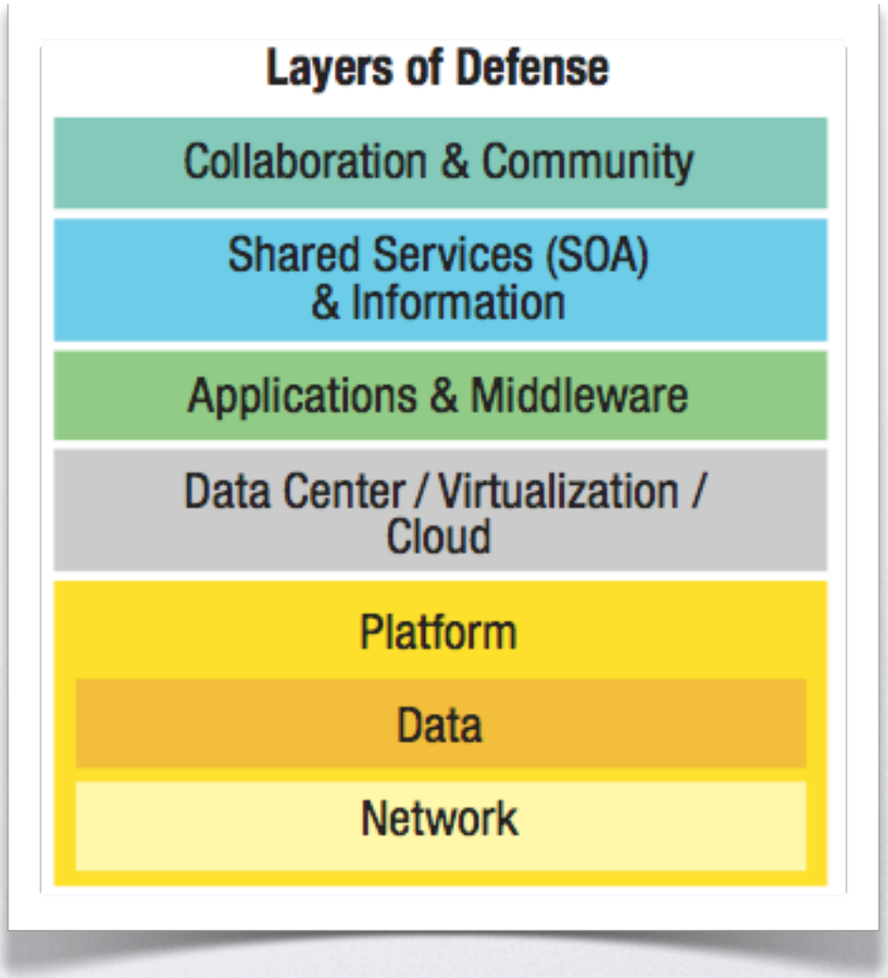
Bypass Security	Circumvent security restrictions such as a firewall or proxy, and IDS system or a virus scanner.
Data Manipulation	Manipulate data used or stored by the host associated with the service or application.
Denial of Service	Crash or disrupt a service or system to take down a network.
File Manipulation	Create, delete, read, modify, or overwrite files.
Gain Access	Obtain local and remote access. This also includes vulnerabilities by which an attacker can execute code or commands, because this usually allows the attacker to gain access to the system.
Gain Privileges	Privileges can be gained on the local system only.
Obtain Information	Obtain information such as file and path names, source code, passwords, or server configuration details.
Other	Anything not covered by the other categories.

Security > Strategy

"Defense in Depth" is the principle of ensuring that security is not done at just one layer of the enterprise. Do it at all layers.

(That's the "deep" part, but it's easy to understand, so not so deep after all, eh?)

- Workstation Layer
  - configuration and patching
  - Anti-virus / Anti-malware
  - Firewall
- Network Layer
  - Device configuration
  - Network Architecture
  - Firewall
  - Intrusion detection
- Server Layer
  - configuration and patching
  - Authentication and Access
  - Anti-virus / Anti-Malware
  - Firewall
  - Intrusion detection

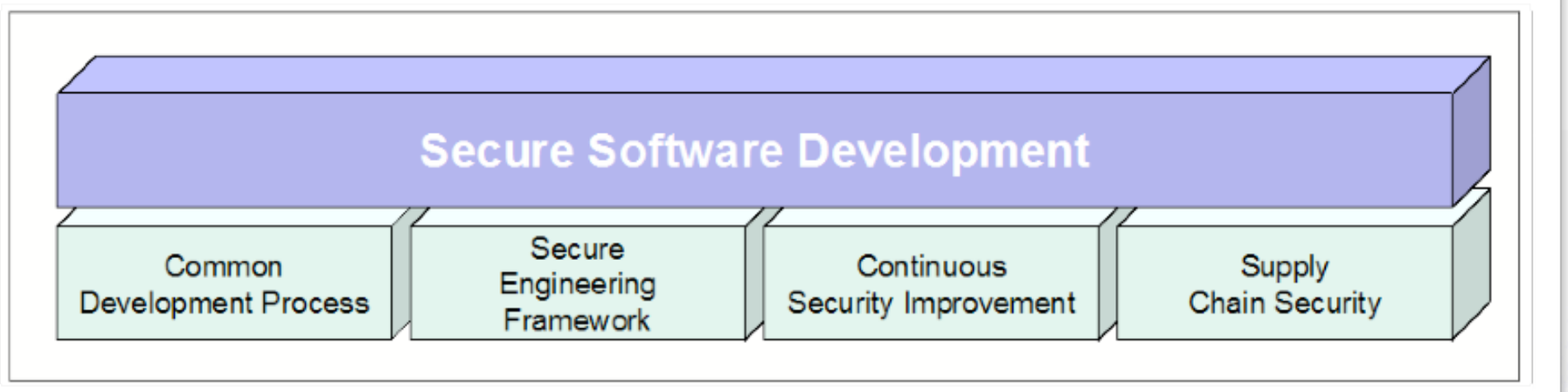


Security > Strategy

"Security Management Lifecycle" is the complete closed loop of managing an information security program over time

Required Reading

- Plan
- Implement
- Maintain
- Assess
- Repeat



Secure Software Development

- Follow secure engineering practices for software products.
- Take an end-to-end approach to product delivery, with security taken into account at each step.
- Employ a common development process to provide consistent management, technical oversight, and accountability across the entire range of hardware, software, services, and solution development projects.
- Establish a set of enforceable and measurable standards and directives for secure software development.

Security > Services

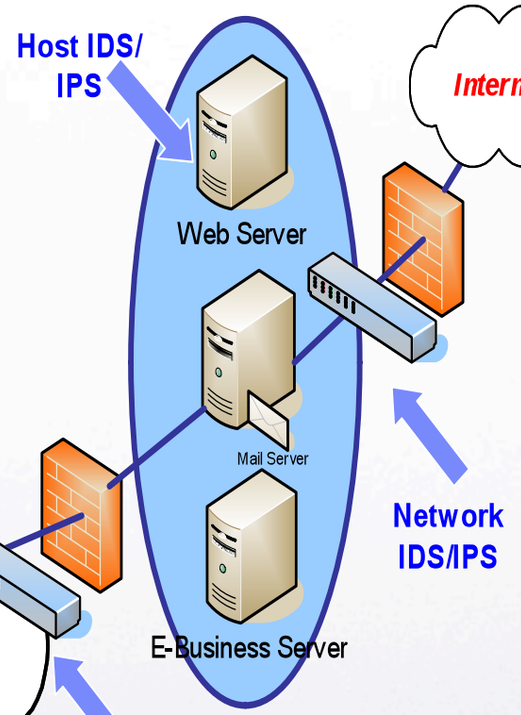
Vulnerability

- Assessment
  - Penetration tests including scanning as well as hands-on attempts to ethically break into systems on a periodic subscription basis.
  - Vital business servers
  - e-Commerce environments
  - Cryptography of transaction servers
  - There are a number of process steps in vulnerability assessment
- Scanning
  - A complete network scan of all services running on a system and any vulnerabilities that may be present in those services by a robust combination of open source and proprietary tools.
    - Nessus – Open source project vulnerability scanner
  - Scans servers on automated basis for proactive vulnerability discovery
  - Checks all services running on a system and any vulnerabilities that may be present

Security > Services

Intrusion Detection

- Steps
  - Monitors attacks directed against your enterprise (IDS)
  - Prevents attacks directed against your enterprise (IPS)
  - Delivers security reports designed to enable business decisions on security defenses
  - Monitors intrusions 24x7x365 within a Security Operations Center



- Services
  - Network and host-based intrusion detection services are available to monitor and detect intrusions directed against the enterprise.
  - Global visibility into the condition of the Internet
  - Operational, Infrastructure and Analytical monitoring
  - Over 800 Global NIDS and 900 HIDS

Security > Services

Incident Management

- Determines
  - What actually happened?
  - How did the incident occur?
  - How widespread is the damage from this incident?
  - Recovery and prevention strategies.
- Involvement of other IT services
- Patch management as outcome
  - Security incident management key is the incident process

Threat Advisories and Alerts

- A “Daily Radar” report may be used with truly actionable information for the Information Security manager and technical staff. The content only includes those issues that are of vital importance.
- Collected from hundreds of global sources both technological and human.
- Emergency notification service for critical threats or emerging crisis situations
- Escalation of notification as threats increase

Security > Services

Virus Advisories and Alerts

- Management of the infrastructure which protects a network from a major malware outbreak
- To be enterprise wide it should support desktop, gateway & server anti-virus solutions
- Research into newly discovered malware.
- Malware or malicious software is software designed to infiltrate or damage a computer system without the owner's informed consent. It is a combination of the words "malicious" and "software". The expression is a general term used mean a variety of forms of hostile, intrusive, or annoying software or program code. Malware includes the following terms:
  - Virus
  - Worm
  - Trojan
  - Bots
  - Adware
  - Spyware
  - Ransomware
  - Search bar modifiers
  - Rootkits
  - Backdoors
  - Loggers
  - Dialers

Security > Services

Security Policy Verification

- An agent that runs on servers to verify that security settings and patches are implemented in accordance with an agreed upon security policy

Network security

- Integrated Security Monitoring
  - Enterprise wide collection and correlation of security events from a range of sources.
  - Security events can occur from many devices
  - Devices and security functions provided by specialized providers
- Firewall Management
- Don’t forget about wireless security
  - Rogue Access Points
  - War Drivers
  - Wireless Hacking
  - Policy Violations

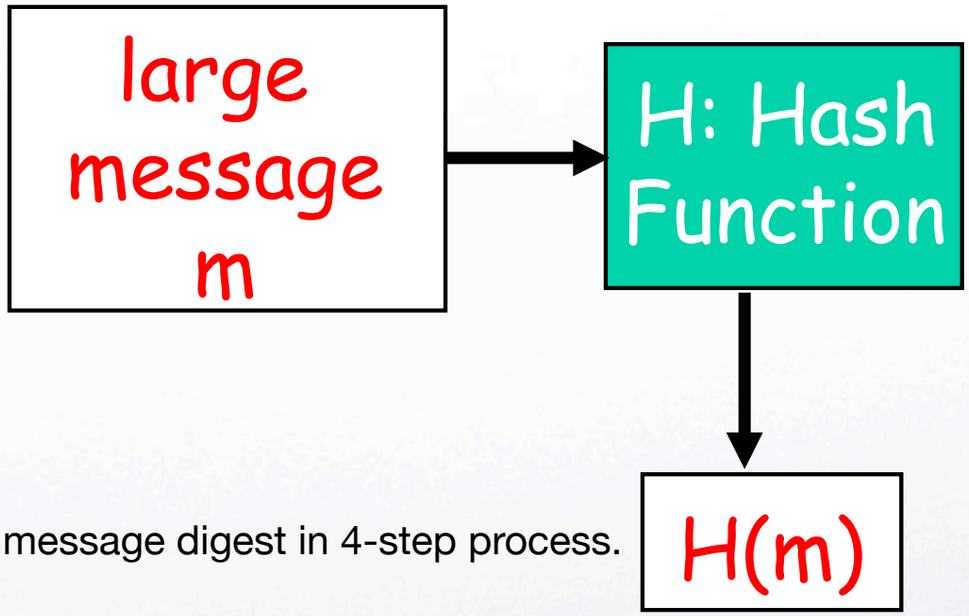
Let’s look closer at Network Security . . .

Network Security is

- **Confidentiality**
  - Only sender, intended receiver should “understand” message contents.
    - Sender encrypts message.
    - Receiver decrypts message.
- **Authentication**
  - Sender, receiver want to confirm identity of each other.
- **Message Integrity**
  - Sender, receiver want to ensure the message is not altered (in transit, or afterwards) without detection.
  - What can go wrong?
    - eavesdrop: intercept messages
    - actively insert messages into connection
    - impersonation: can fake (spoof) source address in packet (or any field in packet)
    - hijacking: “take over” ongoing connection by removing sender or receiver, inserting himself in place
    - denial of service: prevent service from being used by others (e.g., by overloading resources)
- **Access and Availability**
  - Services must be accessible and available to users.

How do we accomplish Message Integrity? - Message Digests

- Function H( ) that takes as input an arbitrary length message and outputs a fixed-length string: “message signature”
- Note that H( ) is a many-to-1 function, oftentimes called a “hash function”.
- Desirable properties:
  - Easy to calculate
  - Irreversibility: Can’t determine m from H(m)
  - Collision resistance: Computationally difficult to produce m and m’ such that H(m) = H(m’)
  - Seemingly random output

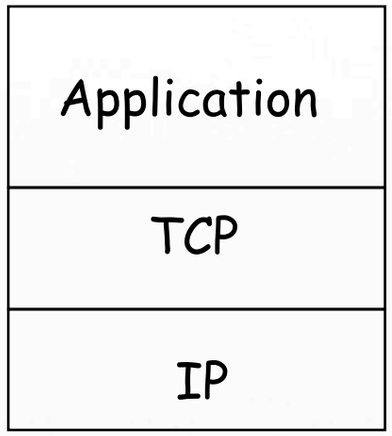


Has Function Algorithms

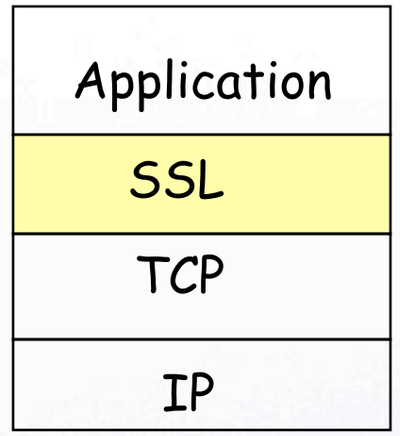
- MD5 hash function widely used (RFC 1321), computes 128-bit message digest in 4-step process.
- SHA-1 is also used.
  - US standard [NIST, FIPS PUB 180-1], 160-bit message digest
- HMAC - Popular MAC standard, addresses some subtle security flaws
  - Concatenates secret to front of message, hashes concatenated message, concatenates the secret to front of digest, hashes the combination again. (*Cool*.)

Secure Sockets Layer

- Widely deployed security protocol
  - Supported by almost all browsers and web servers (HTTPS)
  - Tens of billions spent per year over SSL
- Originally designed by Netscape in 1993
  - Number of variations:
    - TLS: transport layer security, RFC 2246
- Provides confidentiality, integrity, and authentication
- Original goals:
  - Had web e-commerce transactions in mind
  - Encryption (especially credit-card numbers)
  - Web-server authentication
  - Optional client authentication
  - Minimum hassle in doing business with new merchant
- Available to all TCP applications via secure socket interface



Normal Application



Application with SSL

What is Confidentiality at the Network Layer?

- Between two network entities:
  - Sending entity encrypts the payloads of datagrams. Payload could be:
    - TCP segment, UDP segment, ICMP message, OSPF message, etc.
  - All data sent from one entity to the other would be hidden:
    - Web pages, e-mail, P2P file transfers, TCP SYN packets, etc.

Virtual Private Networks

- Institutions often want private networks for security.
  - Costly! Separate routers, links, DNS infrastructure.
- With a VPN, institution's inter-office traffic is sent over public Internet instead.
  - But inter-office traffic is encrypted before entering public Internet.

How do we implement this stuff? IPsec, that's how.

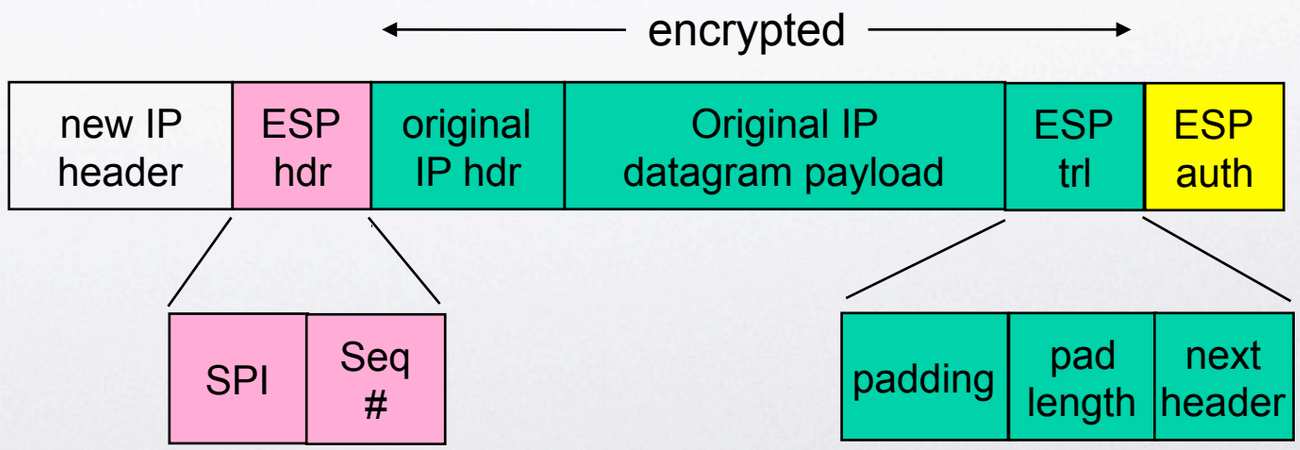
- What?

IPsec Services

- Data integrity
- Origin authentication
- Replay attack prevention
- Confidentiality

Two protocols providing different service models:

- Authentication Header (AH) protocol
  - Provides source authentication & data integrity but not confidentiality.
- Encapsulation Security Protocol (ESP)
  - Provides source authentication,data integrity, and confidentiality.
  - More widely used than AH.
  - Has cooler name.



Security > Cyber Crime

2007 Cyber Crime Survey

- The average annual loss reported inshot up to $350,424 from $168,000 a year before.
- Almost one-fifth (18 percent) of those respondent said they'd suffered a "targeted attack".
- Financial fraud overtook virus attacks as the source of the greatest financial losses.
- Insider abuse of network access or e-mail (such as trafficking in pornography or pirated software) edged out virus incidents as the most prevalent security problem, with 59 and 52 percent.
- When asked generally whether they'd suffered a security incident, 46 percent of respondents said yes, down from 53 percent the prior year.
- The percentage of organizations reporting computer intrusions to law enforcement continued upward after reversing a multi-year decline over the past two years, standing now at 29 percent as compared to 25 percent in the prior year's report.
  - Why do companies fail to report cyber crime?
  - (*This sounds like a good discussion topic*.)

A Brief History of Computer Crime

1988

- a "worm program" written by a college student shut down about 10 percent of computers connected to the Internet. This was the beginning of the era of cyber attacks.
- Today we have about 10,000 incidents of cyber attacks which are reported and the number grows.

1994

- A 16-year-old music student named Richard Pryce, better known by the hacker alias Datastream Cowboy, is arrested and charged with breaking into hundreds of computers including those at the Griffiths Air Force base, Nasa and the Korean Atomic Research Institute. His online mentor, "Kuji", is never found.
- Also this year, a group directed by Russian hackers broke into the computers of Citibank and transferred more than $10 million from customers' accounts. Eventually, Citibank recovered all but $400,000 of the pilfered money.

1995

- In February, Kevin Mitnick is arrested for a second time. He is charged with stealing 20,000 credit card numbers. He eventually spends four years in jail and on his release his parole conditions demand that he avoid contact with computers and mobile phones.
- On November 15, Christopher Pile becomes the first person to be jailed for writing and distributing a computer virus. Mr Pile, who called himself the Black Baron, was sentenced to 18 months in jail.
- The US General Accounting Office reveals that US Defense Department computers sustained 250,000 attacks in 1995.

A Brief History of Computer Crime

1999

- In March, the Melissa virus goes on the rampage and wreaks havoc with computers worldwide. After a short investigation, the FBI tracks down and arrests the writer of the virus, a 29-year-old New Jersey computer programmer, David L Smith.
- More than 90 percent of large corporations and government agencies were the victims of computer security breaches in 1999

2000

- In February, some of the most popular websites in the world such as Amazon and Yahoo are almost overwhelmed by being flooded with bogus requests for data.
- In May, the ILOVEYOU virus is unleashed and clogs computers worldwide. Over the coming months, variants of the virus are released that manage to catch out companies that didn't do enough to protect themselves.
- In October, Microsoft admits that its corporate network has been hacked and source code for future Windows products has been seen.

Who Cares About Cyber Crime?

Some of the sites which have been compromised

- U.S. Department of Commerce
- NASA
- CIA
- Greenpeace
- Motorola
- UNICEF

Some sites which have been rendered ineffective

- Yahoo
- Microsoft
- Amazon
- ... and many more

Security > Cyber Crime

Common Cyber Crime Activities

- Hacking
- Social Engineering
- Virus technologies
- Adware/spyware planting
- Online extortion
- Industrial spying and mobile phone dialers

Security > Services

Other Security Services

- Standards and controls
- Physical security
- Compliance Checking
- Security Advisories
- Education

Security overlaps with many other areas of Smart Business Infrastructure

- Software Distribution
- Event Management
- Operations Management
- Network Management
- Inventory
- Resource Management
- Reporting Management
- SLA Management
- Knowledge Management
- Asset Management
- Notification and Escalation Management
- Problem Management
- Change Management

The Business of Information Security

- Security Management Vendors – can we trust them?
  - Almost all vulnerability research is done underground.
  - Successful and powerful exploits have a long lifespan.
  - Dangerous exploits can be released immediately after vulnerability disclosure.
- Who's attacking us and why?
  - Amateurs
    - Because they can. Pranks, just curious, seeking notoriety.
    - Joy riding
    - Gaining skills
  - Professionals / Organized Crime
    - Monetary gain
    - Espionage
    - Venting anger at another company/firm
    - Terrorism

Security > Services

Some Security Management Products

- IBM Tivoli Federated Identity Manager and Access Manager
- LanDesk Security Patch Management
- Secure Resolutions functions to thwart spyware
- Symantec is a leader in antivirus and adware detection software
- Entrust software provides security policy and auditing
- McAfee firewall, antivirus, and anti-spyware
- Autonomic Software has automated patch detection and vulnerability detection
- Safeboot Software specializes in securing hardware
- Dorian Software has user logon and logoff enforcement products
- eEye Digital Security is for vulnerability management
- Check Point Software includes system intrusion detection and prevention
- Arcsight is a premier software for compliance management and insider threats with logging

Security > Summary of Goals

End-to-end Risk Management

- Adopt a business-driven strategic approach to security.
- Start with a security risk assessment.
- Implement security controls to holistically address compliance requirements.

Ensure secure service delivery

- Effectively manage risk for key business services in an On-Demand 24/7 world.
- Start with security policy, standards, and procedures development.
- Implement threat and vulnerability management solutions.
- Automate security and compliance administration, management and reporting.

Security > Summary of Goals

Reduce the cost of security

- Meet changing business needs.
- Start with Total Cost of Ownership (TCO) challenge offering, security standards and process assessments, and design.
- Deploy products and outsourced services to reduce cost and risks from people and identities, data and information, applications and infrastructure.

Respond with speed and agility

- Gain control over risk posture and incident response.
- Start with a regulatory compliance assessment.
- Deploy automated incident response products or services.
- Implement SIEM products or managed services to drive improved insight.

Required Readings

Web Sites

- IBM Business Security Portal at www-03.ibm.com/security

Videos

- Frontline CyberWar at http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/
- State-Sponsored Terrorist Cyber Attacks at www.youtube.com/watch?v=F30NbJChNTI

Papers (already linked from the prior slides)

- IBM X-force: Threat Insight from April 2010 [*pdf*]
- Secure Software Development [*pdf*]
- Cyber Security in Government [*pdf*]

You should be a little paranoid about getting advice from this android. The "Secure Software Development" paper is actually a little long. But interesting. And cool. Rilly.

Optional Readings

Websites

- Microsoft Warns of Spike in Java Attacks- http://www.pcworld.com/businesscenter/article/208171/microsoft_warns_of_spike_in_java_attacks.html?tk=hp_new
- IBM introduces Security Services to Protect Cloud Environments- http://www.eweek.com/c/a/Security/IBM-Introduces-Security-Services-to-Protect-Cloud-Environments-490885/
- Information on Nessus- http://www.nessus.org/nessus/
- Malware Measures and Vulnerabilities- http://www.sitesecuritymonitor.com/blog/bid/41361/Large-Companies-Don-t-Protect-From-Malware
- How to track down rogue access point- http://www.smallbusinesscomputing.com/webmaster/article.php/3590656/How-to-Track-Down-Rogue-Wireless-Access-Points.htm

Papers

- Testing for Software Vulnerability Using Environmental Perturbation [pdf]
- Malware Future Trends [pdf]
- Security for the Internet Protocol [pdf]
- The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers - [pdf]

Self-test

What is the difference between AH Protocol, and Encapsulation Security Protocol?

Why is security important?

How do companies test vulnerability?

How does VPN work?

What are cyber crime activities, and why do people attack?

What is security policy verification?

What is a Rogue Access Point?

Self-test Answers

What is the difference between AH Protocol, and Encapsulation Security Protocol?

- Encapsulation Security Protocol provides confidentiality as well as source authentication and data integrity.

Why is security important?

- Security ensures that resources and information are getting to only the right people at the right time.

How do companies test vulnerability?

- Companies do penetration tests. Penetration attempts include scanning and hands-on attempts to try to break into systems.

How does VPN work?

- VPN allows inter office activity to go through the public Internet, but is encrypted before entering the public Internet.

What are cyber crime activities, and why do people attack?

- Cyber crimes are hacking, virus technologies, online extortion etc. People attack for money anger, terrorism, or just for fun.

What is security policy verification?

- An agent that runs on servers to verify that security settings and patches are implemented in accordance with agreed upon security policy

What is a Rogue Access Point?

- A wireless access point that has been installed in a secure company network without authorization, or has been created to allow a hacker to conduct man-in-the-middle attack

Discussions

Why do companies fail to report cyber crime?

Describe some “social engineering” attacks and why they might be successful.

Remember our discussion expectations and guidelines.

Acknowledgements

The great Cyber Crime material is adapted from my dear friend and colleague Anne Matheus.

The Network Security section is adapted from **Computer Networking: A Top Down Approach** ,5th edition by Jim Kurose and Keith Ross, published by Addison-Wesley, April 2009.

Some of the earlier source material and a few of the graphics in this module came from the IBM World Wide Client Technology Centers's very own Frank De Gilio.

Some additional source material was provided by David Graves and Paul Kontogiorgis of IBM in 2006. There would be little here without it.

More additional material from:

- IBM Security Portal at www-03.ibm.com/security
- IBM Institute for Advanced Security at www-304.ibm.com/industries/publicsector/us/en/rep/!!/xmlid=192485

Thanks again to Carley Keefe for her tireless work correcting Alan's writing.

Colophon

This work was authored in Keynote by Alan G. Labouseur in July 2010 from his home in Pleasant Valley, NY.

Sometimes he feels a little "lost in space".

Distractions that made writing slower:

- The Classic Lost in Space project at Sci-Fi meshes at www.scifi-meshes.com
  - Specifically, user "Avian" who made the Jupiter 2 render, pictured here.
- WIRED Magazine, Still more of "Under the Dome" by Stephen King (It's a long book.)

Music that made writing faster:

- iTunes Genius Mixes: Classic Rock
- Specific artists: Dave Weckl / Stanton Moore / Joss Stone / Jaco Pastorius / Mötley Crüe