


	CIS-162 Introduction to Network Security Comptia Security+ Exam Domain 1 General Security Concepts <small>Trang D. Nguyen</small>

	What are you trying to protect?
	<ul style="list-style-type: none">• What are you trying to protect?<ul style="list-style-type: none">• Host• Network• Application• Information• Security<ul style="list-style-type: none">• Computer Security• Network Security• Information Security• Information Assurance <small>Trang D. Nguyen</small>

	The "CIA" of Security
	Triad of Security <ul style="list-style-type: none">• Confidentiality• Integrity• Availability <small>Trang D. Nguyen</small>

Who are they? 

- Hackers and Phreaks
 - Attempt to break in
 - Attempt to circumvent security
- Crackers
 - Break in to do harm
- Script-kiddies
 - Babes in cyberspace
 - Hacking / cracking students

Trang D. Nguyen

You against the World. Are you ready?



Trang D. Nguyen Capture the Flag - Defcon 6.0 - 1998

Attacks on the CIA

Name	CIA Type	Date
Morris Worm	Availability	1988
Melissa	Availability	1999
W32.SirCam	Confidentiality	2001
Code Red II	Integrity	2001
Blaster Worm	Availability & Integrity	2003

Trang D. Nguyen

	<h3>Morris Worm</h3> <ul style="list-style-type: none"> • Availability attack - Denial of Service (DOS) • Exploit "finger" and "sendmail" vulnerabilities • Threat <ul style="list-style-type: none"> • No perimeter defense (Internet direct connect) • Multiple services on same system • Unpatched system • Defense <ul style="list-style-type: none"> • Separation of services • Least privilege • Apply patches <p style="font-size: small;">Trang D. Nguyen</p>
--	---

	<h3>Melissa Virus</h3> <ul style="list-style-type: none"> • Availability attack - mail server DOS • New virus easily slipped through • Users activated macro • Threat <ul style="list-style-type: none"> • Danger of monoculture (MS Office) • Inadequate security awareness • Failure to use principle of least privilege • Defense <ul style="list-style-type: none"> • Simpler email (without macro capabilities) • Mail traffic monitor to set off alarm <p style="font-size: small;">Trang D. Nguyen</p>
--	---

	<h3>Operation Model of Security</h3> <p style="text-align: center;">Protection = Prevention + (Detection + Response) General Concept More Later</p> <table border="1" style="width: 100%;"> <tr> <td style="width: 20%;">Prevention</td> <td>Access Controls Firewalls Encryption</td> </tr> <tr> <td>Detection</td> <td>Audit logs Intrusion Detection Systems Honeypots</td> </tr> <tr> <td>Response</td> <td>Backups Incident response teams Computer forensics</td> </tr> </table> <p style="font-size: small;">Trang D. Nguyen</p>	Prevention	Access Controls Firewalls Encryption	Detection	Audit logs Intrusion Detection Systems Honeypots	Response	Backups Incident response teams Computer forensics
Prevention	Access Controls Firewalls Encryption						
Detection	Audit logs Intrusion Detection Systems Honeypots						
Response	Backups Incident response teams Computer forensics						

	Risk Model
	<p style="text-align: center;">Risk = Threat x Vulnerability General Concept More Later</p> <p>Threat is any potential danger to the CIA Vulnerability is a weakness or absence of safeguard</p> <p>Do not confuse the operational model of security with the risk model.</p> <p><small>Trang D. Nguyen</small></p>

	Security Principles (Part 1)
	<ul style="list-style-type: none">• Ignore security issues• Give up and become an Amish• Security through obscurity (hiding it)• Keeping it simple• Principle of Least Privilege• Separation of Duties <p><small>Trang D. Nguyen</small></p>

	Security Principles (Part 2)
	<ul style="list-style-type: none">• Defending individual hosts• Defending the network• Layered Defense - Defense in Depth - Onion• Diversity of Defense• Access control• Authentication <p><small>Trang D. Nguyen</small></p>

	Privilege Models
	<ul style="list-style-type: none"> • Principle of least privilege <ul style="list-style-type: none"> • Associated with DAC (Discretionary Access Control) • Example: Users have enough access to perform their jobs • Need to know <ul style="list-style-type: none"> • Associated with MAC (Mandatory Access Control) • Required to access compartmentalized resources • Example: MAC security label control of information • Separation of duties <ul style="list-style-type: none"> • Example: Divide duties among administrators • Dual administrator accounts <ul style="list-style-type: none"> • Example: Administrator with an end-user and an administrator account • Not to be confused with classic operating system information security models <p style="font-size: small; margin-top: 10px;">Trang D. Nguyen</p>

	Classic Information Security Models
	<ul style="list-style-type: none"> • Bell-LaPadula (1976) - Confidentiality • Biba - Integrity • Clark-Wilson - Transaction Integrity • Lattice access matrix <p style="text-align: center; margin-top: 20px;">In depth discussion in CIS-163</p> <p style="font-size: small; margin-top: 10px;">Trang D. Nguyen</p>

	Basis of Privilege Models
	<ul style="list-style-type: none"> • User based • Group based • Role based • Reflecting configuration <ul style="list-style-type: none"> • MAC (Mandatory Access Control) • DAC (Discretionary Access Control) • RBAC (Role Access Control) <p style="font-size: small; margin-top: 10px;">Trang D. Nguyen</p>

	Access Control Models
	<ul style="list-style-type: none"> • Mandatory Access Control (MAC) • Discretionary Access Control (DAC) • Role-Based Access Control (RBAC) • Rule-Based Access Control (RBAC/ACL) • List-Based Access Control (LBAC/ACL) <ul style="list-style-type: none"> • Access Control List <ul style="list-style-type: none"> • NTFS file permission • Firewall filters
	Trang D. Nguyen

	Discretionary Access Control
	<ul style="list-style-type: none"> • Discretionary Access Control (DAC) <ul style="list-style-type: none"> • Defined in DoD Orange Book • File Attributes • Owner can change object attributes • Owner can authorize access • Based on identity of subjects and/or group
	Trang D. Nguyen

	Mandatory Access Control
	<ul style="list-style-type: none"> • Mandatory Access Control (MAC) <ul style="list-style-type: none"> • Defined in DoD Orange Book • System in control • Labels attached to subjects and objects • User cannot change object labels • Cannot read-up and write-down • Read-down and write-up is permitted
	Trang D. Nguyen

	Access Control Models
	<ul style="list-style-type: none"> • Role-Based Access Control (RBAC) <ul style="list-style-type: none"> • Based on subject role or job functions • Access Control List (ACL) <ul style="list-style-type: none"> • Rule-Based Access Control (RBAC) • List-Based Access Control (LBAC)
	Trang D. Nguyen

	Authentication
	<ul style="list-style-type: none"> • Something you have • Something you are • Something you know
	Trang D. Nguyen

	IAA and AAA of Security
	<ul style="list-style-type: none"> • Identification <ul style="list-style-type: none"> • Who you are or What something is • Authentication <ul style="list-style-type: none"> • Confirming identity based on <ul style="list-style-type: none"> • Something you have • Something you are • Something you know • Where you are? • Authorization <ul style="list-style-type: none"> • Approval, Permission, Empowering, Enablement • Auditing
	Trang D. Nguyen

	Authentication
	<ul style="list-style-type: none">• User name and password• Multi-factor (strong authentication)• Kerberos (KDC, AS, TGT, TGS) <small>RFC1510</small>• PAP, SPAP and CHAP (PPP) <small>RFC1334</small>• Digital Certificates <small>RFC2459</small>• Security Token (passive, active)<ul style="list-style-type: none">• One-time-password device (OTP)• Mutual Authentication• Biometrics (physical, behavioral) <p data-bbox="245 653 310 667"><small>Trang D. Nguyen</small></p>
