

Class Three

Topics:

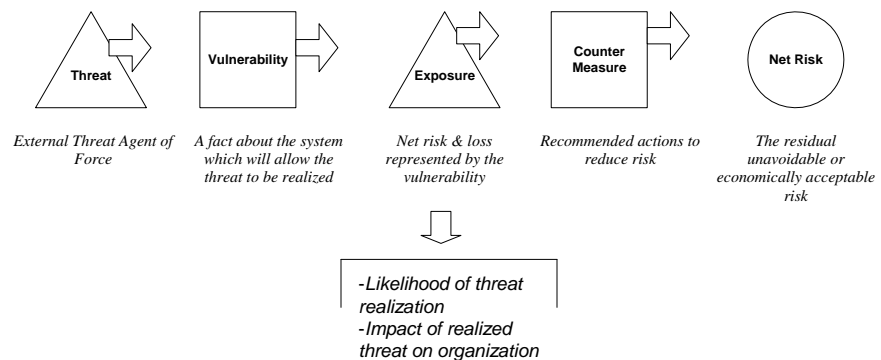
- **Types of Risk**
- **Approaches to Managing Risk**
- **The Economics of Risk**
- **Risk Identification**
- **Risk Analysis**
- **Risk Analysis Tools**
- **Identification and Authentication**
- **Factors of Identification**
- **Managing the Password**

8/24/2007

Class 3

1

Risk Analysis Model



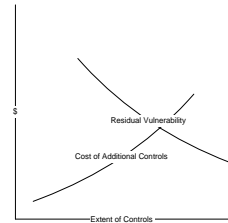
8/24/2007

Class 3

2

Approaches to Managing Risk

- Reduce - Prevent, Detect, Recover
- Assume - Bear Risk
- Assign - Pay Someone Else to Suffer the Risk
- Why a risk analysis
 - Make sure nothing serious is overlooked
 - Permit cost/benefit calculations of risk management measures



8/24/2007

Class 3

3

Approaches to Managing Risk

- **Reduce**
 - Do first, up to economic reasonable limit
 - Use if a first time risk analysis done
 - Use if cost/benefit has become more favorable since last analysis
 - Use for high loss/high likelihood events
- **Assign**
 - Use if insurance or other vehicle is readily available and is accepted practice
 - Use for high loss/low likelihood events where someone with "deep pockets" has more resources to cover the loss
- **Assume**
 - Use if there is no alternative
 - Use for low loss/low likelihood event
 - Use if the costs of assumption are built into an industry-wide cost structure (e.g., credit card fraud in banking)
 - Use if you have more profitable uses for your money (taking into account costs of being ruled negligent!)

8/24/2007

Class 3

4

Threat Taxonomy

- How should threats be categorized?
 - Complete but not overlapping categories
 - Insight into risk analysis process
- Types of classification:
 - “Massive Lists”
 - Threat categories
 - Attack or method categories
 - Result or motivation categories

8/24/2007

Class 3

5

Threat Taxonomy - The Zoological Garden (“Pest Programs”)

- An example of the “massive list” approach
 - Viruses – reproduce, require a “host” program
 - Worms – reproduce, do not require a “host”
 - Trojan Horses – Looks like a useful or innocuous program, secretly damages, spies on, or covertly controls your system
 - Zombies – Systems under control of attacker, available to do the attacker’s bidding
 - RATS – Remote Access Trojans, allows attacker to control your computer
 - Phish – Credible spoof of an institution’s Web site or email, with the intent of harvesting the target’s financial credentials
 - Logic Bombs - Malicious programs which execute on a trigger event
 - The Salami Attack – Steal a little bit at a time, through round-off, etc.
 - Data Diddling – Enter incorrect data
 - Timing Attacks – Exploit timing issues in systems (similar to check kiting)

8/24/2007

Class 3

6

Threat Taxonomy - The Zoological Garden ("Pest Programs")



8/24/2007

Class 3

7

Threat Taxonomy - Attack Agents

- Hacker
- Spy (corporate and national)
- Inside Criminal
- Outside Criminal
- Political Group
- Disgruntled Employee
- Incompetent/poorly trained employee
- Vendor
- Customer
- Litigant

8/24/2007

Class 3

8

Threat Taxonomy - Attack Methods

- Dumpster Diving
- Shoulder Surfing
- Social Engineering
- Keyboard Capture
- Network Sniffing
- Protocol Failure (SYN attacks, etc.)
- Operating System/Software Failures
- Password Cracking/Breaking Authentication
- Network Scanning
- War Dialing
- War Driving

8/24/2007

Class 3

9

Threat Taxonomy - Attack Objectives

- Vandalism
- Revenge
- “Prestige”
- National Espionage
- Industrial Espionage
- Embezzlement
- Management Fraud
- Achieving a political goal
- Stalking or personal harassment
- Trade Secret Theft
- Identity theft
- Obtain Free Computer Services
- Theft of Information for:
 - Investigative reporting
 - Civil litigation
 - Unlawful police surveillance
 - Internal political advantage
- Warfare or other political conflicts between nations

8/24/2007

Class 3

10

Estimating Risk: Qualitative vs. Quantitative Approaches

- Qualitative
 - High/Medium/Low
 - Results in relative ranking
 - Can give priorities, provides general risk strategy guidance
 - With fixed resources, can help choose most essential items "to do"
- Quantitative
 - Dollar value of asset at risk, and probability of loss, extent of loss if event occurs
 - Actuarial
 - Used for budgeting, or setting an internal "risk premium"
 - The "Holy Grail" of security

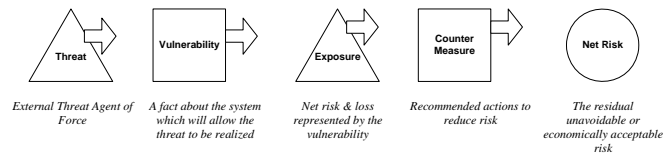
8/24/2007

Class 3

11

General approach to a Risk Analysis

- Identify vulnerabilities
- Identify threats
- Determine likelihood
- Determine impact (potential losses) – includes information valuation
- Determine risk - product of likelihood and impact
- Evaluate and select countermeasures



8/24/2007

Class 3

12

Risk Economics - Annual Loss Expectancy

- $ALE = (\text{Loss per Incident}) \times (\text{Frequency of Incident})$
- Loss per incident is called Single Loss Expectancy or SLO
- Note: Frequency is reciprocal of probability over given time period. Sometimes called Annualized Rate of Occurrence or ARO.

Examples:

Risk:	Frequency:	Loss/Incident:	ALE:
Earthquake	once/30 yrs	\$1.5Million	
Hacking	once/yr	\$70,000	
Credit Card Fraud	100/yr	\$500	

8/24/2007

Class 3

13

Risk Economics - Valuing Information

- Cost to replace or re-generate information
- Loss to firm if information not available for intended use
- Loss to firm if competitor gets information (e.g. trade secret)
- What the information could be sold for (e.g. copyrighted material)
- The value which the information adds to the business during its transaction flow

8/24/2007

Class 3

14

Alternative Risk Analysis Model

- Follows security-specific scenarios of loss
 - Security breach as a chain of events occurring over time, rather than a single event occurring at an instant
 - Multiple countermeasures must be breached in sequence for attacker to be successful
 - Emphasizes ability to reduce security losses at various steps
 - Allows more focused definition of counter-measures (avoids complex combinations)
- Paper by Katherine Morse, SAIC, elaborates



8/24/2007

Class 3

15

Threat Trees

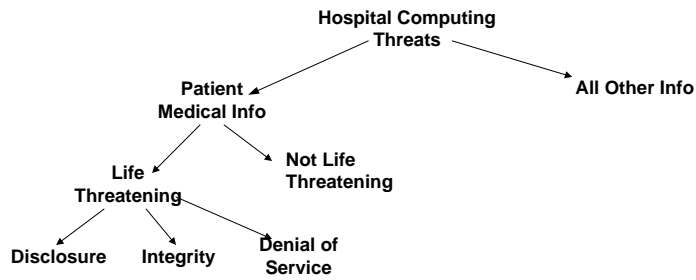
- Method to develop complete, consistent, non-overlapping list of threats
- Standard engineering methodology
- Process:
 - Start with most generic definition of threat to the system in question
 - Introduce level-wise refinement, categorization of threat types based on what is threatened, results of threat, and how the threat is realized
 - Identify nodes as disjunctive or conjunctive

8/24/2007

Class 3

16

Threat Trees - from Amoroso

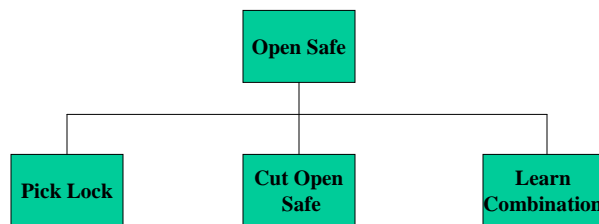


8/24/2007

Class 3

17

Another View of Threat Trees - Bruce Schneier



- Attacker Point of view
- Root Node is the goal of the attack
- Leaf Nodes are attack methods

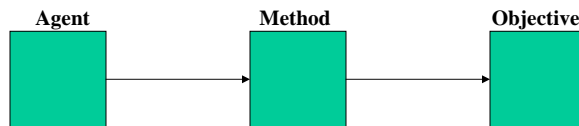
8/24/2007

Class 3

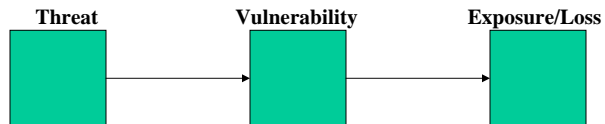
18

Threat Tree - Agent, Method, Objective

What They See



What You See



8/24/2007

Class 3

19

Finding Quantitative Risk Information - Hacking and Security Breaches

- Quality information difficult to find:
 - Laws requiring reporting are weak or non-existent
 - Difficulty in consistent definition of computer breach
 - Reluctance of firms to report breaches, due to adverse publicity
 - Many sites never know they have been hacked
 - Hacking follows “fads”, impossible to predict
- Note important difference between:
 - Surveys of actual/perceived security breaches
 - Penetration studies of vulnerabilities
 - Studies of Internet “noise” as “fallout” from attacks (Internet “telescope”)

8/24/2007

Class 3

20

Finding Quantitative Risk Information – Useful Sources

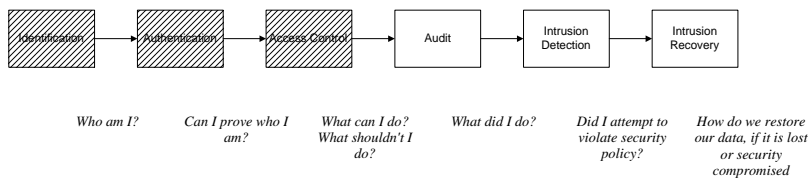
- Specific Vulnerabilities:
 - How can a given type of host be attacked?
 - Bugtraq, CVE, CERT Advisories
 - Vendor bulletins and warnings
- Countermeasure Effectiveness:
 - Of a sample of sites, how many actually had vulnerabilities
 - Sometimes, how effective is the incident response process?
 - GAO DoD Study (1999)
- Threats
 - How many attempts are made to exploit certain vulnerabilities?
 - CERT Summary reports
 - “Honeypot” surveys
 - Attack “Fallout” studies
- Losses
 - How often have “we” been attacked, and how much have “we” lost
 - CSI/FBI annual surveys
 - ASIS Intellectual Property Surveys (periodic)

8/24/2007

Class 3

21

Security Transaction Life Cycle - Where Identification, Authentication and Access Control Occur



8/24/2007

Class 3

22

Defining Identification and Authentication




- **Identification:** Who you are
- **Authentication:** Proof that you are who you claim to be
 - Importance to **Accountability**, the tracing of responsibility for actions to a single individual
 - Essential to access controls - without proof of identity, it is impossible to restrict or permit access based on identity

8/24/2007

Class 3

23

Factors of Identification

What you know		Password PIN
What you have		Token
Who you are	<i>Suspect 1</i> 	Biometrics

8/24/2007

Class 3

24

Password Authentication - Good Password Management Techniques

- Minimum length
- "3 Strikes"
- Audit log of access attempts (successful or not)
- Force periodic or as needed password changes
- Don't use easily guessed words
- Don't use any word in a dictionary
- Don't permit cleartext passwords anywhere
- Consider computer generated passwords
- Beware of:
 - Default passwords for system or software
 - Allowing system access without passwords
 - Shared or "group" passwords
 - Active passwords belonging to terminated staff
 - Leaving unused accounts' passwords active

**A Password is Like a Toothbrush:
Use it Daily, Change it Frequently, and Don't Share it**

8/24/2007

Class 3

25

Attacks on Passwords

- Disclosure
 - At the host
 - In transit
 - At the workstation
 - By the user
 - Knowingly
 - Unknowingly (Social Engineering)
- Guessing
- Off-Line attacks against encrypted password master file
 - Dictionary Attacks
 - Brute force exhaustive testing of entire password space
- Sniffing (tool used to disclose in transit)
- Password Grabbers (login process impostors)
- Keystroke loggers (hardware and software)

8/24/2007

Class 3

26

How to Avoid Password Exposures:

- Policies to discourage disclosure and selection of weak passwords
- Encrypt transmissions
- Control workstation software configuration
- Ensure hosts encrypt passwords securely
- Protect host password files from downloading
- Log "bad" access attempts and take action
- Lock out terminals and/or accounts if more than 3 bad passwords entered
- Change passwords frequently to lessen exposure if compromised
- Avoid desktop operating systems which allow easy bypassing of password entry

8/24/2007

Class 3

27

Idle workstations should time-out:
Use password-protected screen savers!

8/24/2007

Class 3

28

Rules for Good Passwords:

- Better password selection methods have higher “**entropy**”
- More Entropy = Large number possible + random distribution
 - *Note: Entropy is a very important concept in cryptography*
- Best - Entirely random set of characters
- Better:
 - First letter of each word of a memorable phrase
 - Randomly generated pronounceable non-words
 - Words with random capitalization and non-alpha characters
 - English words, selected at random and glued together with non-alpha character
- If this is too hard, in the next class we will look at alternatives to passwords!

8/24/2007

Class 3

29

Extra Material – Setting the password policy in Windows 2000/XP

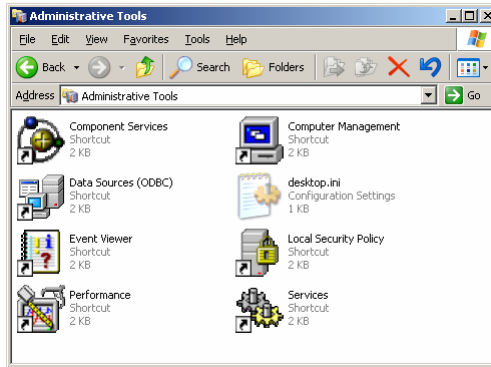
- Windows security policies may be set for:
 - Individual systems
 - Domain authentication to an entire group of Windows servers
- We will cover local system authentication policies only, though domain policy definition is similar
- Local system authentication policies are defined:
 - In the Control Panel
 - Under Administrative Tools
 - Using the Local Security Policy tool
- Domain authentication policies are set on the Domain Controller using the Microsoft Management Console, with the proper plug-in
- Domain authentication policies take precedence over local machine policies.

8/24/2007

Class 3

30

Extra Material – Setting the password policy in Windows 2000/XP



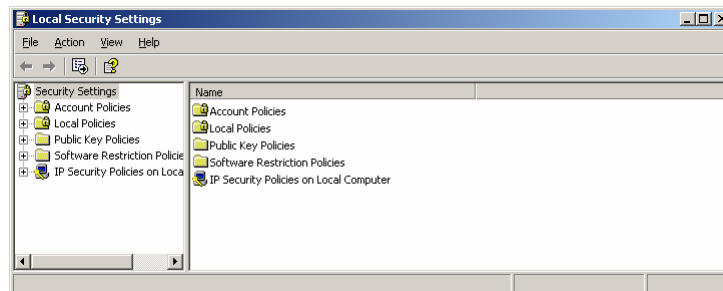
In the Control Panel, Select Administrative tools, then Click on Local Security Policy...

8/24/2007

Class 3

31

Extra Material – Setting the password policy in Windows 2000/XP



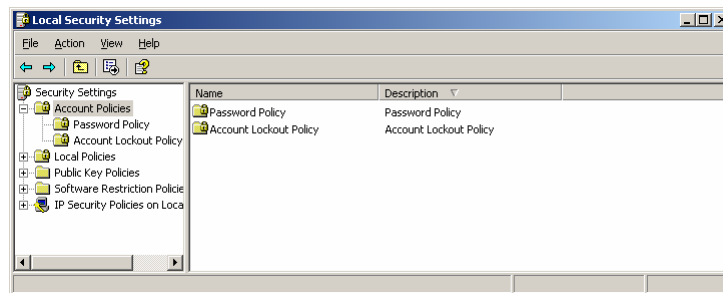
Click on Account Policies...

8/24/2007

Class 3

32

Extra Material – Setting the password policy in Windows 2000/XP



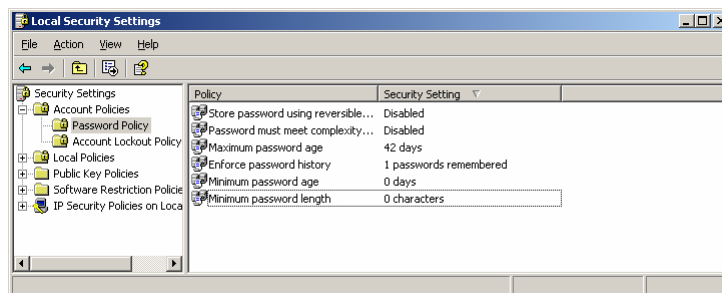
Click on Password Policy...

8/24/2007

Class 3

33

Extra Material – Setting the password policy in Windows 2000/XP



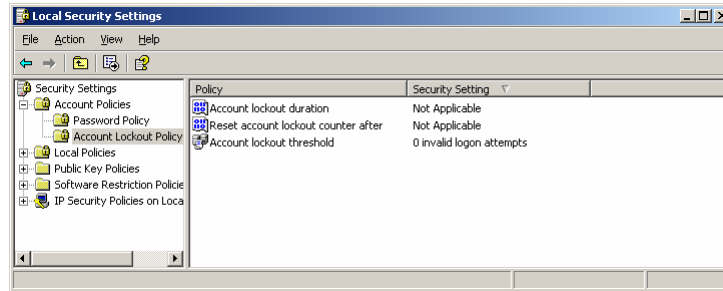
Oops, not a good minimum password length or age!

8/24/2007

Class 3

34

Extra Material – Setting the password policy in Windows 2000/XP



Account lockout policy needs some work too!