

CS574

Computer Security

San Diego State University

Spring 2008

Lecture #1

Today's Structure

- Welcome
- Administrative Trivia (Administrivia)
- Lecture
- Crashers

Administrivia

- Class web page
<http://www-rohan.sdsu.edu/~stremmler/CS574>
- Email
- Syllabus
- Accounts
- Crashers

Administrivia

- Drop/Add Dates
- Course Forgiveness (none)
- Cheating Policy
 - Immediate failure
 - Judicial Services
 - Permanent record

Administrivia

How to Avoid Cheating

- Judicial Services has a video for you to watch
- Be careful when consulting with others
- Learn to paraphrase
- Indicate when quoting, and cite all quotes
- When in doubt, ASK!

Administrivia

General Class Structure

- Administrivia
- Questions
- Recent News
- Lecture
- Discussion

Administrivia

- Crash List
 - Name (printed)
 - Email address (valid)
- Unreadable == No Add Code
- If intending to drop, drop early
- Roll

Lecture

Security

rohan% webster security

se.cu.ri.ty \si-'kyu.r-*t-e-\ n 1: the quality or state of being secure :
as 1a: freedom from danger : SAFETY 1b: freedom from fear or anxiety 2a:
something given, deposited, or pledged to make certain the fulfillment of
an obligation 2b: SURETY 3: an evidence of debt or of property (as a stock
certificate or bond) 4a: something that secures : PROTECTION 4b: measures
taken esp. to guard against espionage or sabotage

Context

- You have something you want to protect.
- You have someone or something you want to protect it from.
- You are willing to expend effort and resources in order to protect it.

Pfleeger Definitions

- *Computing System - a collection of hardware, software, storage media, data, and people that an organization uses to perform computing tasks.*
- *Threat - a set of circumstances that has the potential to cause loss or harm.*

Pfleeger Definitions

- Vulnerability - *a weakness in the security system that might be exploited [by a threat] to cause loss or harm.*
- Control - *an action, device, procedure, or technique that removes or reduces a vulnerability.*

Pfleeger Principles

- Principle of Effectiveness - *Controls must be used -- and used properly -- to be effective. They must be efficient, easy to use, and appropriate.*

Historical Overview

- Military first ones to be concerned with computer security
- Terms and thinking in computer security influenced by military history, attitudes, and procedures
- Security needs applied to mainframes, then to minicomputers, then to microcomputers, and then to the network

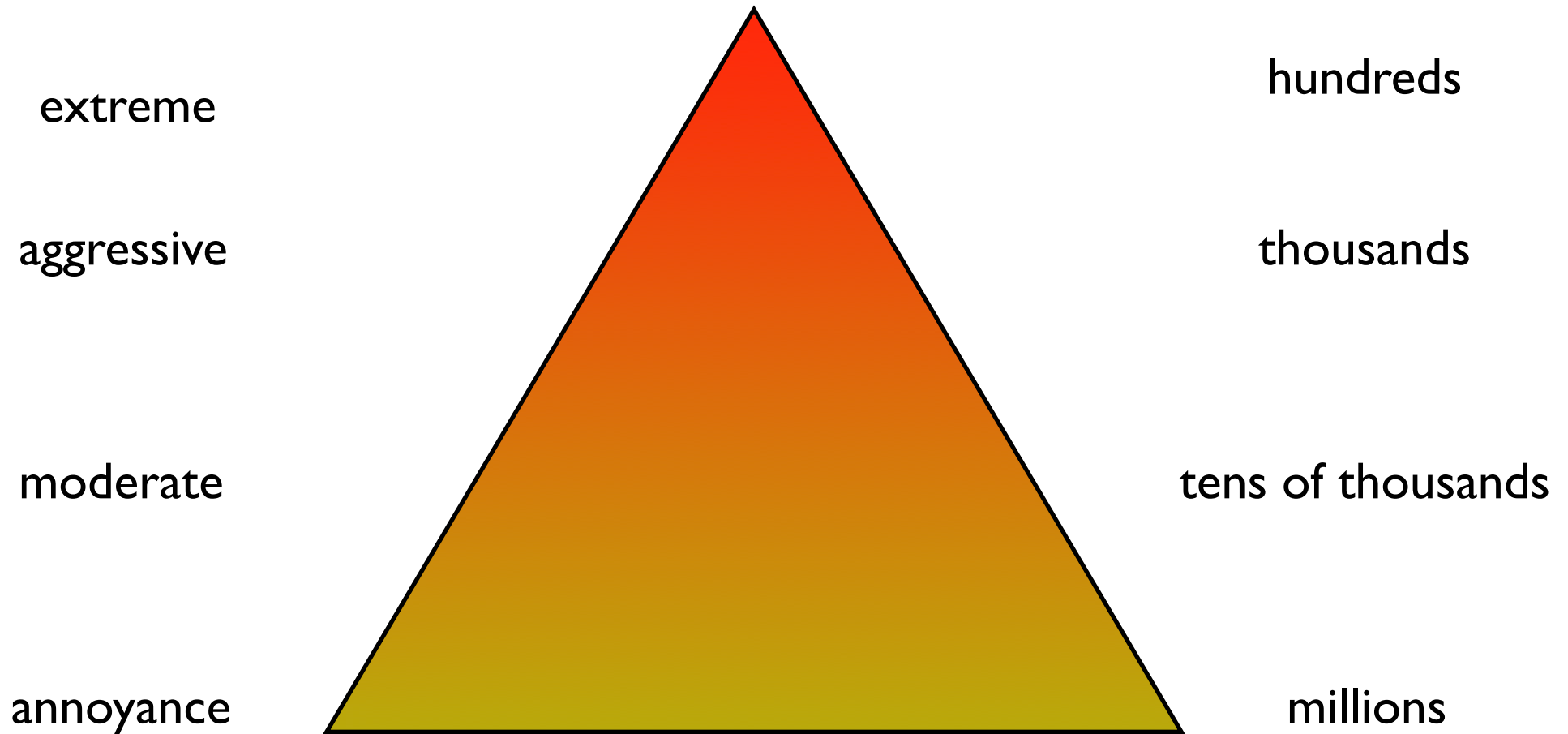
Military vs. Private Sector

- At stake: lives / money
- Ability: guns / lawyers
- Attitude: desire / cost

Threats

- Snooping
- Modification / alteration
- Masquarading / spoofing
- Repudiation
- Denial or Delay of Service
- Others ...

Tom Perrine's Threat Pyramid



Tom Perrine, (*Unpublished*)

Pfleeger's Categories of Threats

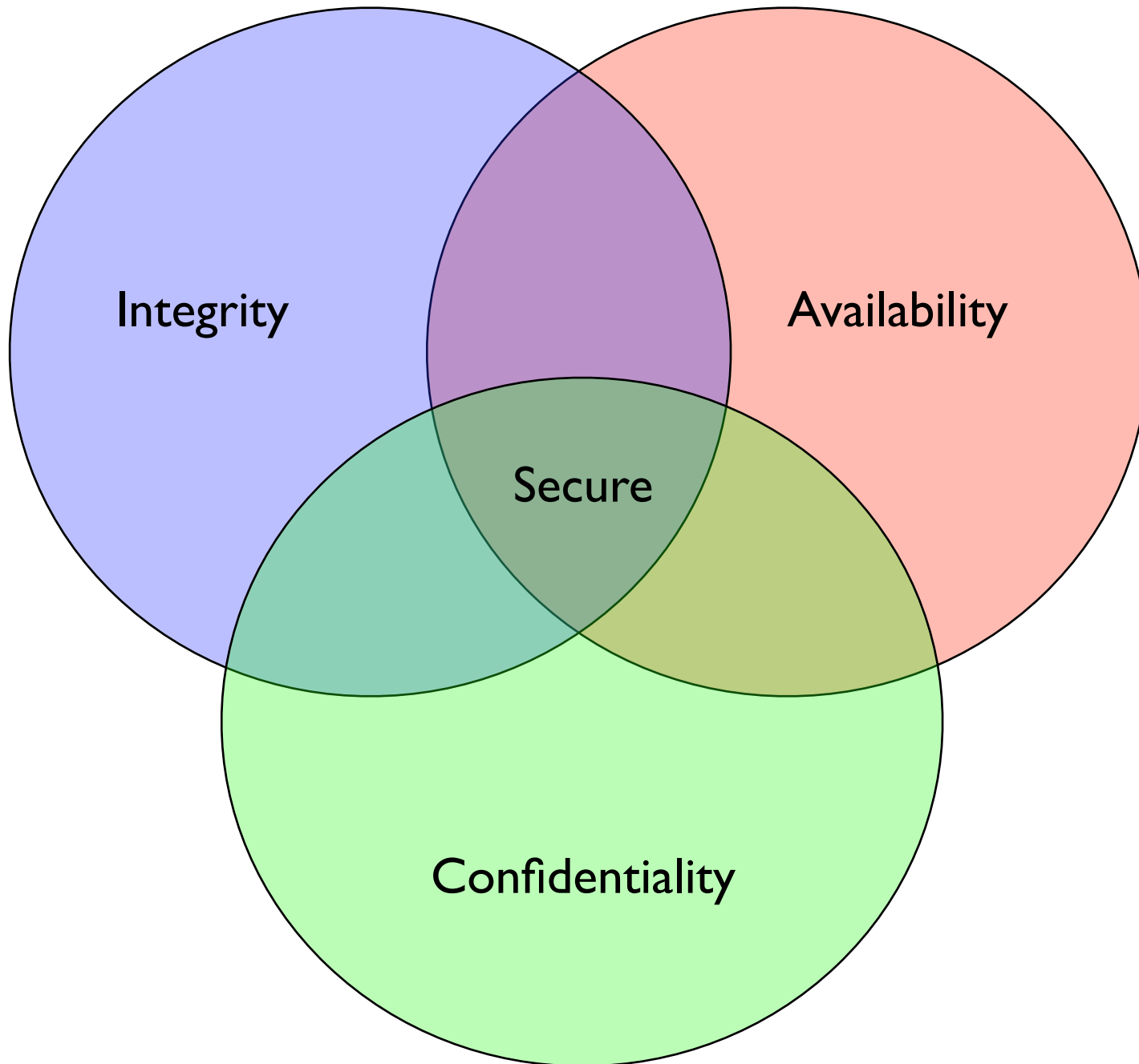
- Interception - *unauthorized party has gained access to an asset.*
- Interruption - *an asset of the system becomes lost, unavailable, or unusable.*
- Modification - *an unauthorized party tampers with an asset.*
- Fabrication - *an unauthorized party creates counterfeit objects on a computing system.*

Shirey Categorizations

- Disclosure - *unauthorized access to information.*
- Deception - *acceptance of false data.*
- Disruption - *interruption or prevention of correct operation.*
- Usurpation - *unauthorized control over some part of a system.*

Goals of Security

- Confidentiality
- Integrity
- Availability



Goals of Security

(another viewpoint)

- Prevention - *an attack will fail*
- Detection - *know that an attack is occurring or has occurred*
- Recovery - *assess and repair damage from an attack, perhaps even while the attack is underway.*

Pfleeger Definitions

- *Attack - an exploitation of a vulnerability or the realization of a threat.*
- *Security Policy - a rule for describing behavior that is or is not allowed.*
- *Security Mechanism - a means for enforcing a security policy.*

Pfleeger Principles

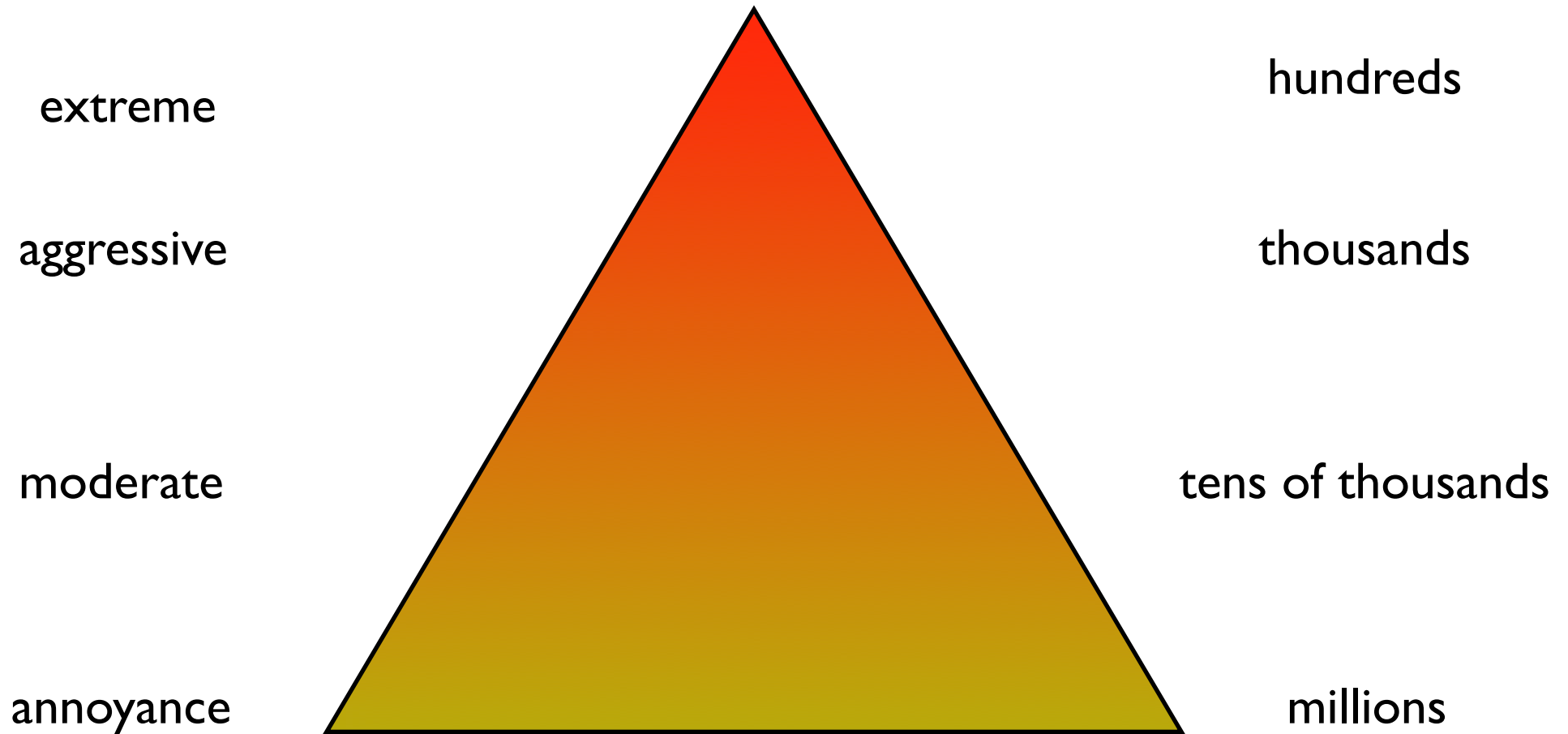
- Principle of Easiest Penetration - *An intruder must be expected to use any available means of penetration. The penetration may not necessarily be by the most obvious means, nor is it necessarily the one against which the most solid defense has been installed.*

Who is Attacking?

- Amateurs
- Script Kiddies
- Disgruntled {Customers,Employees}
- Crackers
- Terrorists
- Professionals

Remember The Threat Pyramid?

Tom Perrine's Threat Pyramid



Tom Perrine, (*Unpublished*)

Appropriate Paranoia

- Is it still paranoia if *they* **are** out to get you?
- Computer can automate the tedious work.
- The other guy may be (assume *is*) smarter.
- Remember Murphy's Law.

Pfleeger Principles

- Principle of Weakest Link - *Security can be no stronger than its weakest link. Whether it is the power supply that powers the firewall or the operating system under the security application or the human who plans, implements, and administers controls, a failure of any control can lead to a security failure.*

Security

- Best considered a process, not a state.
- Risk
 - assessment
 - management
 - mitigation
- Need to identify what's “Good Enough”
- Everything is a tradeoff.

Pfleeger Principles

- Principle of Adequate Protection - *Computer items must be protected only until they lose their value. They must be protected to a degree consistent with their value.*

Reading

- Pfleeger, Chapter 1
- Pfleeger, Chapter 8, section 4

Finis