Jan 21, 2005 -- Lecture 2

22C:169
Computer Security

Douglas W. Jones

Department of Computer Science

Attacker

identifies

Vulnerability

designs

Attack

Our Job

identify

Vulnerabilities

design

Defenses

Defenses

block

Attackers

Defense types:

Eliminate Vulnerability (redesign)

Block Vulnerability (add layers)

Distract from Vulnerability

Detect Exploitation of Vulnerability

Cost of Defense

should not exceed

Value of Assets to Owner

Cost of Attack

unlikely to exceed

Value of Assets to Attacker

Most likely attack?

that with lowest **Cost of Attack** *among those* **Identified**

Best defenses?

those with lowest

Cost of Defense

Sources of Surprise?

mistaken estimates of

asset value

cost of attack

vulnerability identification

Example: Time and Temp Web Site

vulnerabilities?

asset value to attacker?

who might attack?

Example: On-line web-based store

vulnerabilities?

asset value to attacker?

who might attack?

Example: Small law firm's E-mail Server

vulnerabilities?

asset value to attacker?

who might attack?