CS 194-1 (CS 161) Computer Security

Lecture 2

Threat models, security goals, access control

August 30, 2006 Prof. Anthony D. Joseph http://cs161.org/

Review: What is Computer Security Today?

- Computing in the presence of an adversary!
 An adversary is the security field's defining characteristic
- · Reliability, robustness, & FT: random failures
- Security

 Dealing with/surviving actions of knowledgeable attacker dedicated to causing harm

8/30/06

• Wherever there is an adversary, there is a computer security problem!

Joseph CS161 ©UCB Fall 2006

Lec 2.2

 Review: Analyze to Learn!

 • Study attackers and think about how to break into systems to learn attack tactics

 • Analyze previous successful attacks

 • Analyze previous successful attacks

 • Arms race for solutions...

 - (Some) attackers are intelligent

 • Attacks will change and get better with time

 • Deploy a new defense, they respond, you build a better defense, they respond, you...

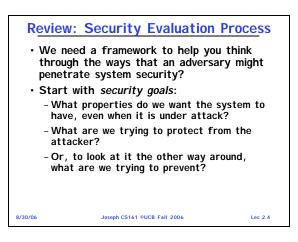
 • Try to anticipate future attacks

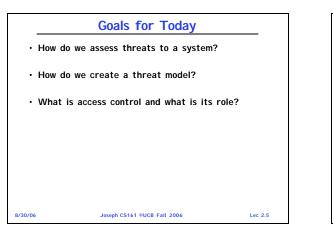
 • Security is like a game of chess

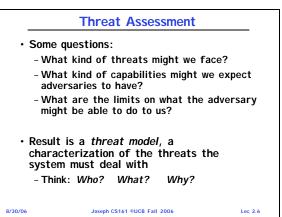
 • Except the attackers often get the last movel

Joseph CS161 ©UCB Fall 2006

8/30/06







Developing a Threat Model First decide how much we can predict about kinds of adversaries we will face Sometimes, know very well who the adversary is, and even their capabilities, motivations, and limitations Sold War: US military oriented towards main enemy (Soviets) and focused on understanding USSR's military capabilities/effectiveness/responsiveness If we know potential adversary, can craft a threat model that reflects adversary's abilities and options and nothing more However, often adversary is unknown

8/30/06

Joseph CS161 ©UCB Fall 2006

Lec 2.7

Lec 2.9

Thinking Generically Must reason more generically about unavoidable limitations of the adversary - Silly ex: physics means adversary can't exceed speed of light Can usually look at system design and identify what an adversary might do - Ex: If system never sends secret info over wireless nets, then don't need to worry about threat of wireless eavesdropping - Ex: If system design means people might discuss secrets by phone, then threat model needs to include possible phone co. insider threats: eavesdrop/re-route/impersonate 8/30/06 Joseph CS161 ©UCB Fall 2006 Lec 2.8

What to Ignore?

- Good threat model also specifies threats we don't care to defend against
 - Ex: home security I don't worry about a team of burglars flying a helicopter over my house and rappelling down my chimney
- Why not?
- · Many easier ways to break into my house...
- Can classify adversaries by their motivation - Ex: financial gain motivation means won't
 - spend more money on attack than they'll gain
 - Burglar won't spend 1,000's to steal car radio
- Motives are as varied as human nature

 Have to prepare for all eventualities...

8/30/06

8/30/06

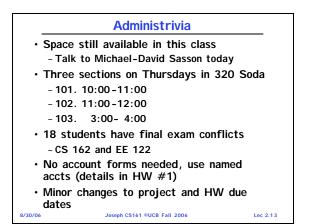
Joseph CS161 ©UCB Fall 2006

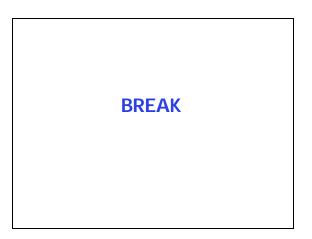
Helpful to Examine Incentives · Ex: Do fast food places make more profit on soft drinks than on food? - Would expect some places to try to boost drink sales (e.g., salting french fries heavily) • Ex: Do customer svc reps earn bonuses for handling more than X calls per hour? - Would expect some reps to cut long calls short, or to transfer trouble customers to other depts. when possible Ex: Do spammers make money from those who respond, while losing nothing from those who don't? - Would expect that spammers send their emails as widely as possible, no matter how unpopular it makes them Joseph CS161 ©UCB Fall 2006 8/30/06 Lec 2.10

Incentives

- As a rule of thumb, organizations tend not to act against their own self-interest (at least not often...)
- Incentives (frequently) influence behavior
 Exposes the motivations of potential adversaries
- Incentives are particularly relevant when two parties have opposing interests
 - When incentives clash, conflict often follows.
 - In this case it is worth looking deeply at the potential for attacks by one such party against the other

Thr	eat Assessment Summa	ary
Rememb	er the three W's:	
- Who a	re the adversaries we might	t face?
	ight they try to attack us, eir capabilities?	and what
	hight they be motivated to a distributed to a distributed what are their incentives?	
	curity goals and threat m is performing a security	
/30/06	Joseph CS161 ©UCB Fall 2006	Lec 2.12





Security Analysis

- Seeing whether there attacks (within threat model) that successfully violate security goals
 - Often highly technical and dependent on system details
 We'll show you many security analysis methods
- One analogy:
 - Threat model defines set of moves an adversary is allowed to make
 - System design defines how defender plays game
 - Security goals define success condition: if adversary violates any goal, he wins; otherwise, the defender wins
- Security analysis is examining all moves and counter-moves to see who has a winning strategy 8/30/06 Joseph CS161 CUCB Fall 2006 Lec 2.15

Another Analogy

- Mystery writers like to talk about means, motive, and opportunity
 - Security evaluation is similar way of thinking
- Threat assessment examines the means and motive
- Security analysis examines what opportunity the adversary might have to do harm

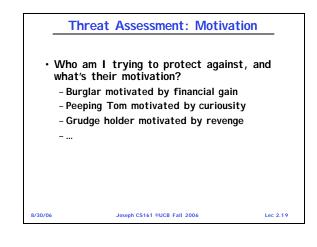
8/30/06

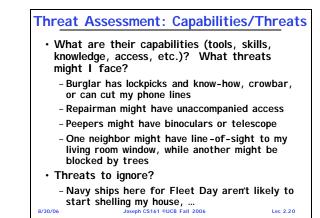
Joseph CS161 ©UCB Fall 2006

Lec 2.16

Security Evaluation Summary · Identify the security goals - What are we trying to protect? · Perform a threat assessment - What threats does the system need to protect against? · Do a security analysis - Can we envision any feasible attack that would violate the security goals? - May be very technical · Use same process for new system design - Easier to ensure security when you know the security goals you and threats - Security analysis helps refine system design Joseph CS161 ©UCB Fall 2006 8/30/06 Lec 2.17

Hor	me Security Analysis Examp	le
• What	at are my security goals?	
	rotecting assets from theft or tamper integrity)	ing
– Pi	rotecting my personal safety	
	» Ex: if someone does break in to steal money, I'd much prefer to know, so tha don't surprise them and get shot	at I
f	insuring my house and contents remain ull working order whenever I want the availability)	
	roviding a certain measure of privacy confidentiality)	
8/30/06	Joseph CS161 ©UCB Fall 2006	Lec 2.18



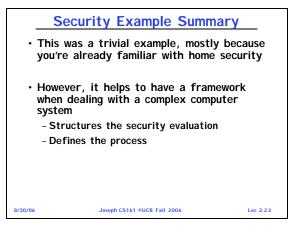


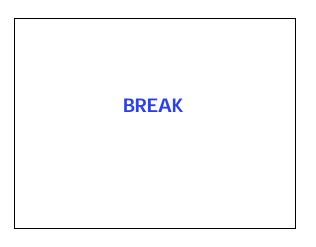
Security Analysis: Possible Attacks All sorts of crazy scenarios! A burglar breaks window, grabs stuff, leaves I secure the windows, but determined burglar takes chainsaw to the walls and breaks in Slightly smarter burglar might look under the flowerpot and find the spare house key, ... Sneaky burglar throws pebble against window at 3am each morning, setting off alarm and bringing the police, each morning until police decide to ignore obviously unreliable burglar alarm, then burglar is free to break in...

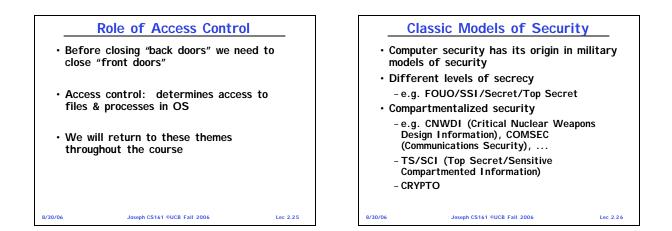
8/30/06

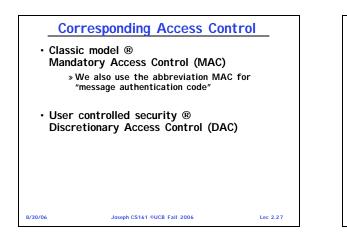
Joseph CS161 ©UCB Fall 2006

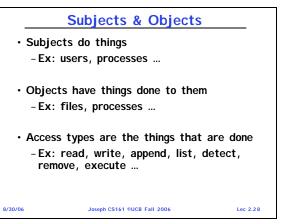
More Possible A	ttacks		
 Neighbor with line-of-sigh uses telescope to peer in v 	,		
 Someone intent on revenge unpleasant items on my law depending on my home's so might be able to smash my 	n, or - ecurity system -		
 Unscrupulous competitor knows I have an important early morning business meeting, so they cut my house's power at night to make my alarm clock fail 			
8/30/06 Joseph CS161 ©UCB Fall 200	6 Lec 2.22		

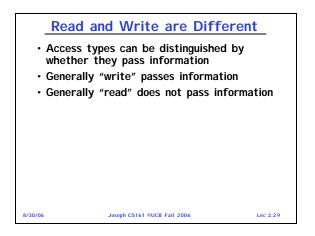




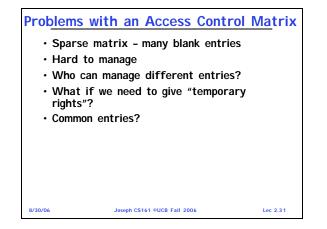


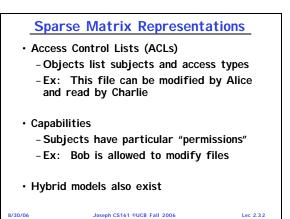






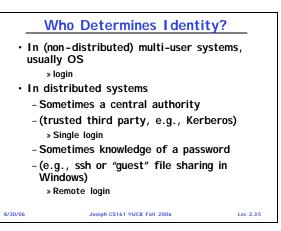
/	Access C	ontrol Ma	trix
	File 1	File 2	File 3
Alice	read		read/write
Bob		execute	
Charlie			read
10/06	Joseph CS16	o1 ©UCB Fall 2006	Lec 2.30





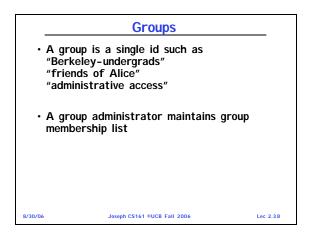
Are ACLs & Capabilities Equivalent?	
 In representative power, yes Both are sparse matrix representations of the Access Matrix 	
• In philosophy, no	
- Often come with particular features & OS philosophy	
- Capabilities often appeal to researchers	
 But capability systems often work poorly 	
 Perennial claim: Capability lists are coming back! 	
8/30/06 Joseph CS161 ©UCB Fall 2006 Lec 2.3.3	

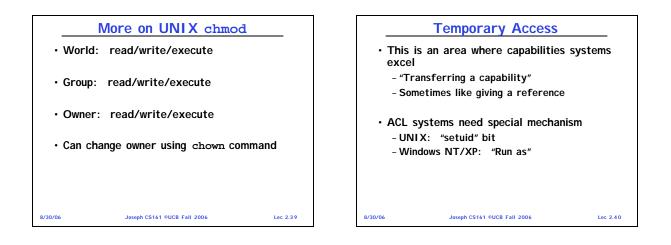
Where is an ACL Applied? • In some systems: on the file • In some systems: on the directory • In some systems: a combination

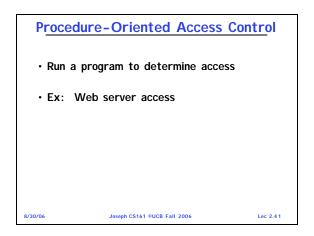


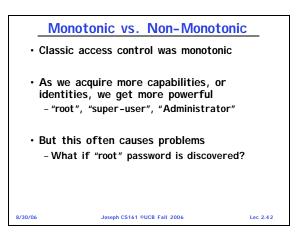
Who is A	llowed to Modify a	n ACL?
	ystems, the "owner" of ss/directory	the
 Example: chmod command in UNIX World access: read/write/execute » For directories: read = list items; » execute = "enter" directory Owner access: read/write/execute 		
8/30/06	Joseph CS161 ©UCB Fall 2006	Lec 2.36

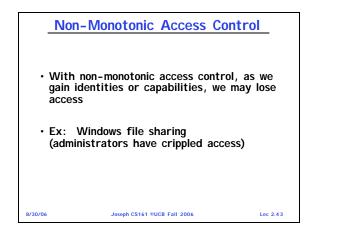


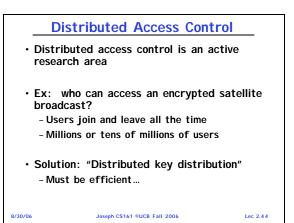


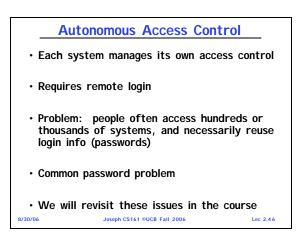












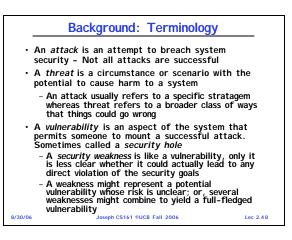
Summary

- Access Control is Central to Security
 - We'll return to access control repeatedly in the course
 - Old area of security, but not well understood
 - Often poorly implemented
 - And we haven't even begun to look at "backdoors"!

Joseph CS161 ©UCB Fall 2006

- Security analysis framework for a complex computer system
 - Structures the security evaluation
 - Defines the process

8/30/06



Background: Terminology (cont'd)

- A security goal is a goal that is supposed to be achieved by the system; if it fails, the system will be considered insecure
- A threat assessment is an attempt to assess the set of all possible threats
- A threat model is a characterization of the possible threats, usually produced during a threat assessment
- 24 by 7 refers to the window of time in which systems are most vulnerable to attack
 - (Ok, this one is a joke from http://www.csoonline.com/read/080105/debrief.html)

Joseph CS161 ©UCB Fall 2006