

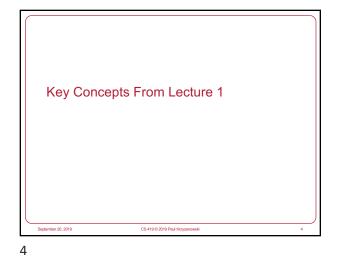
 Recitation Topics

 Recitations will cover:

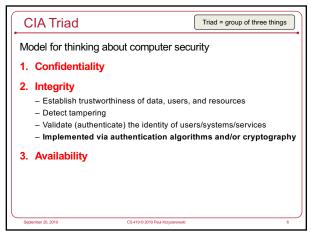
 • Homework review & project guidance

 • Extended coverage of course material

 • Exam preparation

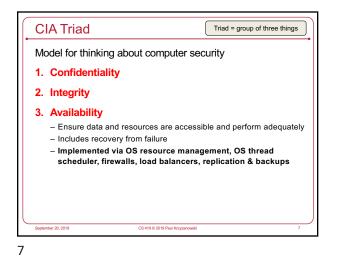


Triad = group of three things CIA Triad Model for thinking about computer security 1. Confidentiality - Restrict access to data and resources (e.g., computing, network) to only those who need to know Authentication establishes - This access is defined by a policy e<u>arity</u> of the user the inte Requires • Identification: who is the user (or computer or application)? • <u>Authentication:</u> verify the user (or computer or application) · Authorization; check the policy to see if the user is has access - Implemented via access control mechanisms or cryptography 2. Integrity 3. Availability



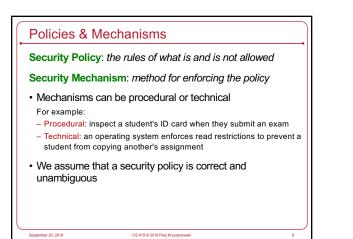


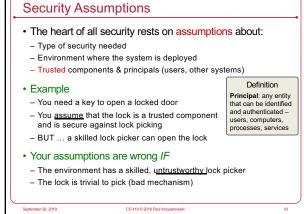
5



## Security Engineering Combination of 1. Policy (rules) 2. Mechanisms (implementation) 3. Assurance (integrity of the mechanisms and policy) 4. Incentives (the human factor) Engineering = not just the design of the system but understanding the trade-offs (time, money, complexity, features, ...)

8









 A trustworthy CPU will correctly enforce memory protections and not allow a user to read regions of memory disallowed by the operating system

Examples

9

 A trustworthy operating system will not allow you to read or modify files to which you do not have access permissions

- A trustworthy lock picker will not bypass security unless properly authorized

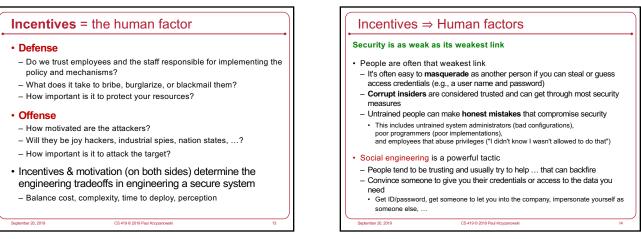
Trust: Trustworthy components

May have the capabilities to break security policies ... but will not do so: they will follow the policy

- If a core component turns out to be <u>not trustworthy</u> then the security of the **entire** system may be in jeopardy
- Example: a malicious boot loader can patch the code of the operating system that, in turn, can run a malicious program or change the behavior of programs

11

ber 20, 2019



14

13

