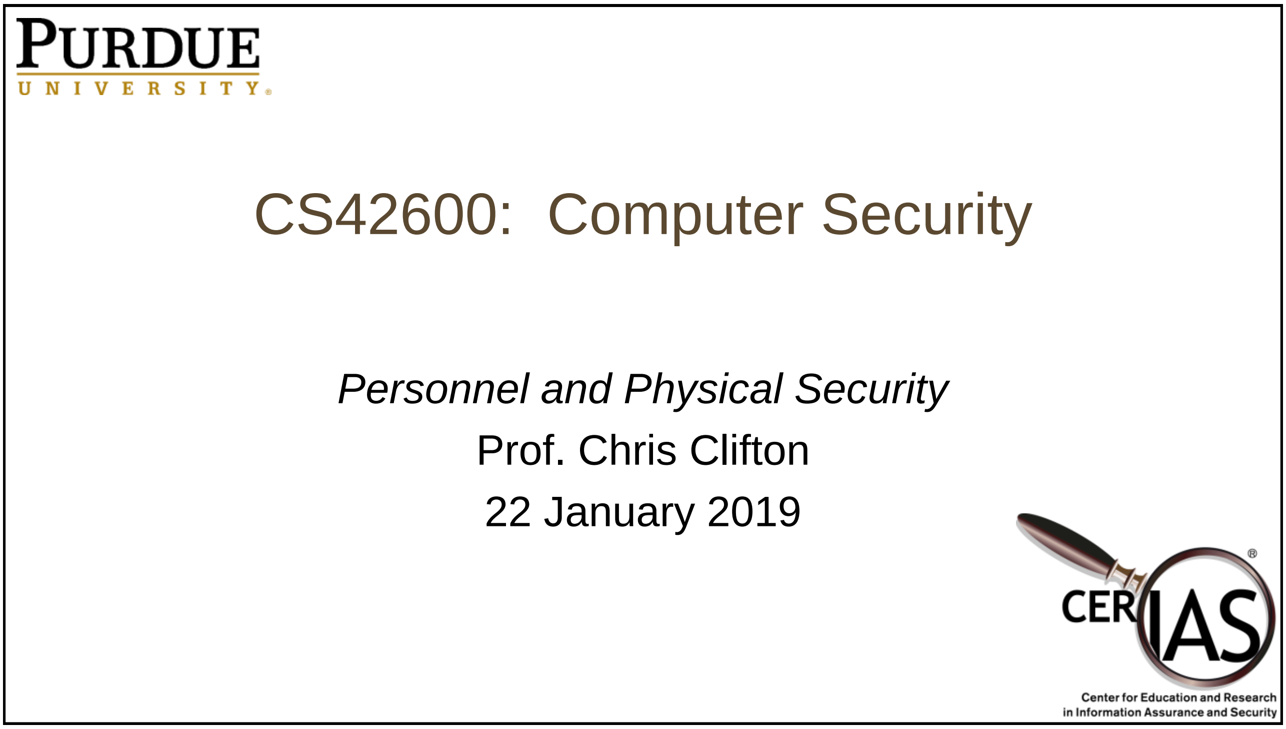


PURDUE UNIVERSITY

CS42600: Computer Security

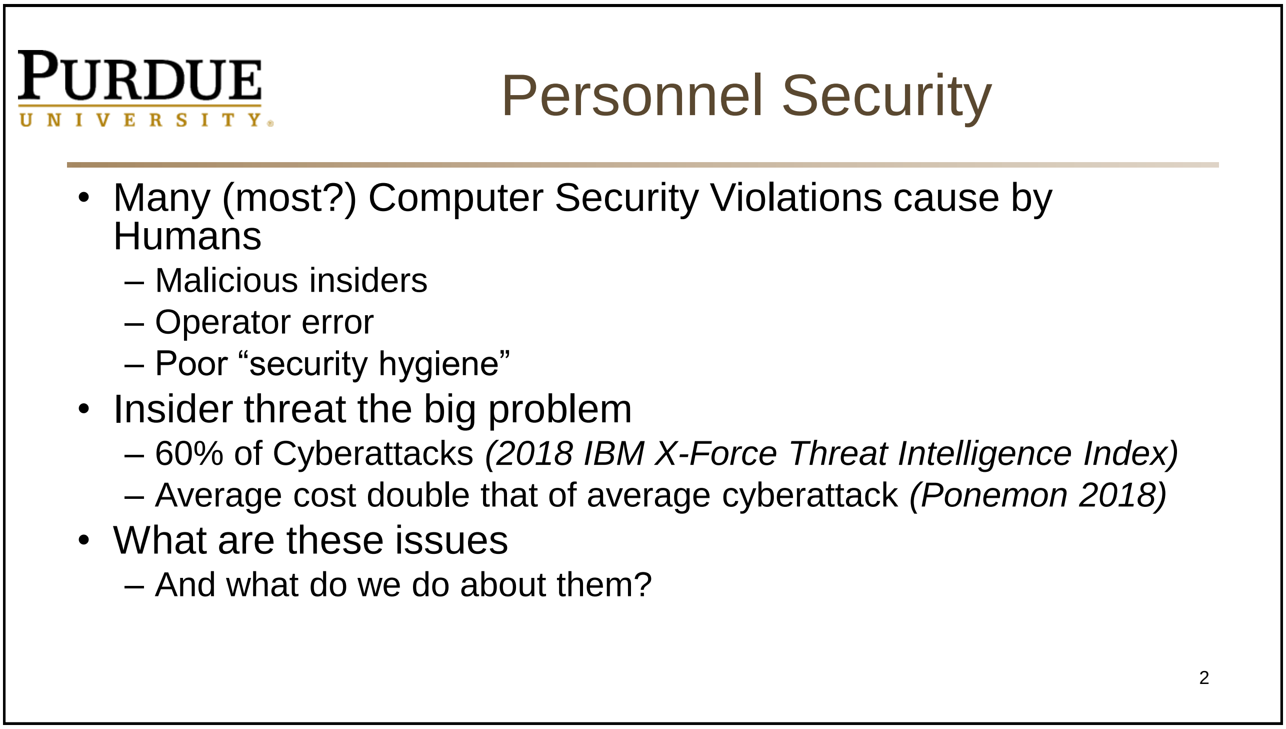
Personnel and Physical Security

Prof. Chris Clifton

22 January 2019

CERIAS

Center for Education and Research in Information Assurance and Security



PURDUE UNIVERSITY

Personnel Security

- Many (most?) Computer Security Violations cause by Humans
  - – Malicious insiders
  - – Operator error
  - – Poor “security hygiene”
- Insider threat the big problem
  - – 60% of Cyberattacks *(2018 IBM X-Force Threat Intelligence Index)*
  - – Average cost double that of average cyberattack *(Ponemon 2018)*
- What are these issues
  - – And what do we do about them?

2

PURDUE
UNIVERSITY

Insider Threat: Types

- Motivations
  - Persistent Malicious
    - “Mole”
  - Disgruntled Employees
  - Collusion
    - “Opportunist”
  - Inadvertent
    - 2/3 of data records compromised in 2017 *(IBM)*
  - Nonresponders
- Category
  - Trusted Unwitting
  - Trusted Witting
  - Untrusted

PURDUE
UNIVERSITY

Insider Threat: Mole

Intentionally embeds themselves to compromise security

- Attacks
  - Steal confidential information
  - Plant misleading information
  - Bring down systems
- Motivations
  - Money, ideology, …
  - Goal: Benefit some other entity

Insider Threat: Mole

Prevention / Remediation

- Background checks
- Access control
  - – Complete mediation
  - – Principle of Least Privilege
- Audit behavior
  - – Detect unusual (although authorized) access

Insider Threat: Disgruntled Employee

Previous non-threat decides to become a threat

- Attacks
  - – Expose confidential information
  - – Destroy critical information
  - – Bring down systems
- Motivations
  - – Revenge, ideology
  - – Goal: Damage the entity

PURDUE
UNIVERSITY

Insider Threat: Disgruntled Employee

Prevention / Remediation

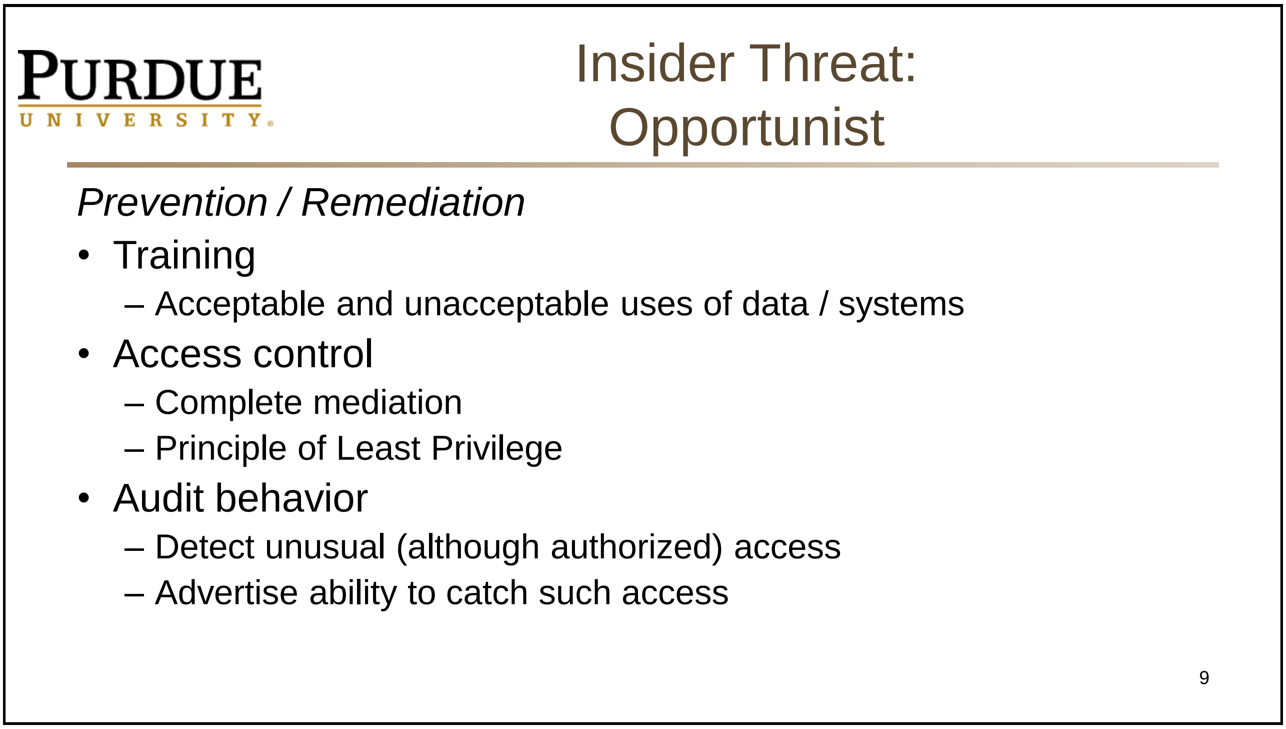
- Awareness/training
  - Recognize potentially dangerous situations
- Access control
  - Complete mediation
  - Principle of Least Privilege
- Revocation
  - Ability to immediately revoke access

PURDUE
UNIVERSITY

Insider Threat: Opportunist

Attack based on current situation, immediate gain

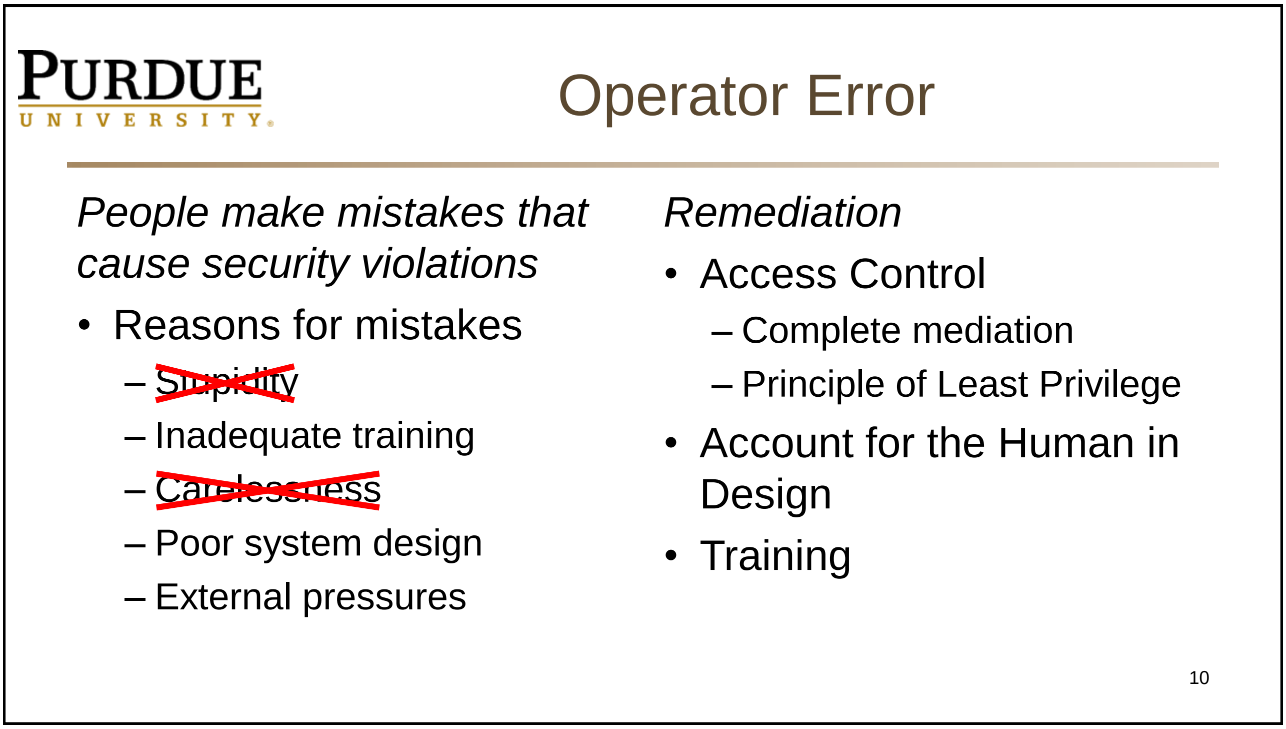
- Attacks
  - Steal confidential information
- Motivations
  - Money
    - Fraud, IP Theft
  - Curiosity
  - Goal: Benefit to attacker



Insider Threat: Opportunist

Prevention / Remediation

- Training
  - Acceptable and unacceptable uses of data / systems
- Access control
  - Complete mediation
  - Principle of Least Privilege
- Audit behavior
  - Detect unusual (although authorized) access
  - Advertise ability to catch such access



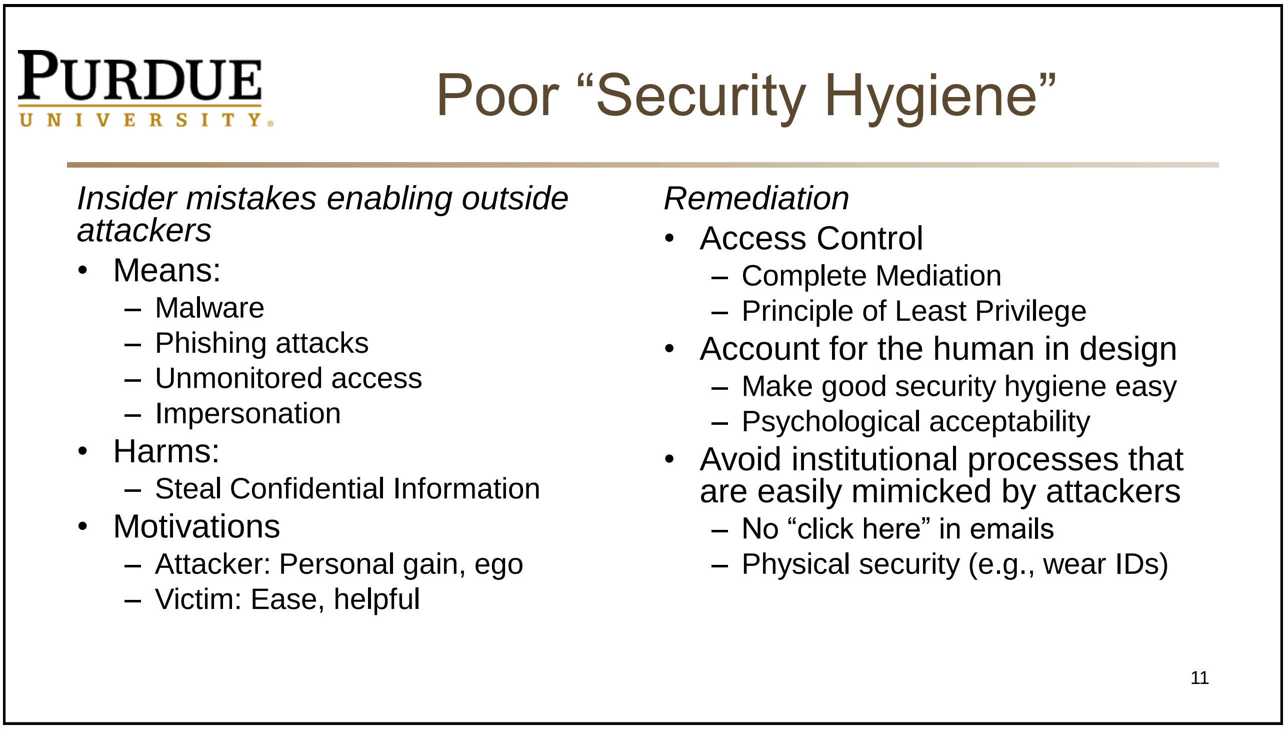
Operator Error

People make mistakes that cause security violations

- Reasons for mistakes
  - ~~Stupidity~~
  - Inadequate training
  - ~~Carelessness~~
  - Poor system design
  - External pressures

Remediation

- Access Control
  - Complete mediation
  - Principle of Least Privilege
- Account for the Human in Design
- Training



PURDUE UNIVERSITY

Poor “Security Hygiene”

Insider mistakes enabling outside attackers

- Means:
  - Malware
  - Phishing attacks
  - Unmonitored access
  - Impersonation
- Harms:
  - Steal Confidential Information
- Motivations
  - Attacker: Personal gain, ego
  - Victim: Ease, helpful

Remediation

- Access Control
  - Complete Mediation
  - Principle of Least Privilege
- Account for the human in design
  - Make good security hygiene easy
  - Psychological acceptability
- Avoid institutional processes that are easily mimicked by attackers
  - No “click here” in emails
  - Physical security (e.g., wear IDs)