PURDUE UNIVERSITY

CERIAS Center for Education and Research in Information Assurance and Security

CS62600: Advance Information Assurance

Prof. Chris Clifton

8 January, 2013

What do we know?

- Tools
  - Cryptography
  - Access control
  - …
- Formal Models
  - HRU
  - Bell-LaPadula

This Course: The Rest of the Story

- How does this play in the real world?
  - What tools to use
  - When
  - and How.
- Physical Security
- Insider Threat
- Attack models
- Red teams
- …

Purdue IT Policies: Authentication and Authorization

- **Reason for Policy**
- Controlled access to IT Resources is essential for Purdue University to continue its mission of learning, discovery, and engagement. This policy describes a comprehensive approach to Authentication and Authorization that can support current needs for electronic access and accommodate future services and technologies by employing standardized mechanisms for Identification, Authentication, and Authorization.
- This policy is guided by the following objectives:
  1. To ensure that Purdue can, without limitation, operate and maintain its IT Resources;
  2. To ensure that Purdue can, without limitation, protect the security and functionality of University IT Resources and the data stored on those resources;
  3. To protect the University's other property, rights, and resources;
  4. To preserve the integrity and reputation of the University;
  5. To safeguard the privacy, property, rights, and data of users of University IT Resources;
  6. To comply with applicable existing federal, state, and local laws; and
  7. To comply with existing University policies, standards, guidelines, and procedures.

Purdue IT Policies: Authentication and Authorization

- **Statement of Policy**
- **Access Control**. Identification, Authentication, and Authorization are controls that facilitate access to and protect University IT Resources and data. Access to non-public IT Resources will be achieved by unique User Credentials and will require Authentication.
- Purdue University will assign a Purdue University Identifier (PUID) and User Credentials for Identification and Authentication purposes to each individual that has a business, research, or educational need to access University IT Resources.
- Authorization for University IT Resources depends on the individual's relationship, or relationships, to the University and the requirements associated with that relationship. In all cases, only the minimum privileges necessary to complete required tasks are assigned to that individual. Privileges assigned to each individual will be reviewed on a periodic basis and modified or revoked upon a change in status with the University.
- **No Unencrypted Authentication.** Unencrypted Authentication and Authorization mechanisms are only as secure as the network they use. Traffic across the network may be surreptitiously monitored, rendering these Authentication and Authorization mechanisms vulnerable to compromise. Therefore, all University IT Resources must use only encrypted Authentication and Authorization mechanisms unless otherwise authorized by the director of the Identity and Access Management Office.

Purdue IT Policies: Authentication and Authorization

- **Compliance**
- Users of University IT Resources must comply with this policy and related standards and expiry periods issued by the University in support of this policy.
- Centralized and departmental IT units and IT Resource owners are responsible for ensuring appropriate enforcement of this policy and related standards on University IT Resources within their areas of responsibility. The formal Security Policy/Procedure Exception Form must be filed and approved by the director of the Identity and Access Management Office for any University IT Resource that is unable to comply with these policy requirements.
- Violations of this policy or any other University policy or regulation may result in the revocation or limitation of IT Resource privileges as well as other disciplinary actions, or may be referred to appropriate external authorities.
- **Who Should Know This Policy**
- This policy covers students, faculty, staff, and all individuals or entities using any University IT Resources and all uses of such IT Resources.

Purdue IT Policies: Incident Response

- **Reason for this Policy**
- A formal policy for the reporting of and response to IT Incidents is necessary to ensure the secure operation of IT Resources, to protect the data security and privacy of students, faculty, and staff, and respond appropriately to IT Incidents.
- This policy sets forth a set of general requirements for the efficient response to IT Incidents in order to maintain the security and privacy of IT Resources, data and other assets, as well as satisfy requirements of state and federal law.

Purdue IT Policies: Privacy

- **Procedures**
- Except for monitoring of activity and accounts of individual users of University IT Resources when the user has voluntarily made them accessible to the public, or where the University has reserved the right to do so without notice or by policy, any access to the contents of communications or electronically stored wire and electronic communications and information employing IT Resources permitted under this policy must, in addition to any requirements specified herein, be authorized as follows:

1. A dean, in the case of an academic unit, a vice president in the case of an administrative unit, and/or a chancellor in the case of a regional campus shall have made a written finding prior to such access that the access is reasonably required in order to protect the University's Interests and shall have forwarded such written finding to the Office of the Vice President for Information Technology.
2. The official designee of the Office of the Vice President for Information Technology shall have made a written finding prior to such access that: (a) the access is reasonably required in order to protect the University's Interests, and (b) authorizes the requested access and specifies the scope and conditions of any permitted access. These written findings shall be maintained by the Office of the Vice President for Information Technology.
3. Notwithstanding the foregoing, the Vice President for Information Technology or his or her designee may authorize access in the event that he or she reasonably determines that: (a) there exists an emergency that materially threatens the University's Interests, (b) that emergency access is reasonably required in order to protect the University's Interests, and (c) he or she specifies the scope and conditions of any permitted access. The OVPIT shall, as soon as reasonably possible after such emergency, make a written finding verifying the existence and satisfaction of the foregoing conditions.

- Any access permitted hereunder shall be the minimum access required in order to protect the University's Interests.
- In all cases, technicians and administrators who receive requests from law enforcement or other outside agencies seeking access to computer accounts, files, or network traffic of an IT Resource user shall forward such requests to the appropriate and responsible Purdue department (which may include without limitation the Purdue Police Department, Public Information Officer, Office of the Dean of Students, or the Employee Relations/Human Resource Policy department as appropriate) in accordance with applicable Purdue policy. In all cases, technicians and administrators will obtain written documentation of any requests made before accessing or permitting access to an individual's electronic information resources.

Policy Structure

- Reason for the Policy
- Statement of Policy
  - Scope
  - General requirements
  - Specifics
- *Procedures*
- Who should Know It
- Related Documents
- *Contacts*
- *Definitions*
- *Compliance*
- *Responsibilities*