CSC309 *Programming on the Web*

week 10: security

Amir H. Chinaei, Spring 2017

Office Hours: M 3:45-5:45 BA4222

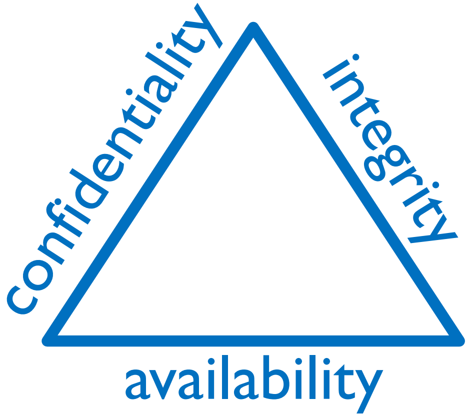
ahchinaei@cs.toronto.edu
http://www.cs.toronto.edu/~ahchinaei/

some contents are from:

- Security in Computing: Pfleeger et al.
- Computer Security: Principles and Practice, Stallings et al.

computer security

- triad architectural requirements



- **computer security definition:** *protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).*

NIST95

all main arch. req's

- **confidentiality**
  - data (& system services) is not accessible to unauthorized parties
- **integrity**
  - data (& system services) are the right ones
- **availability**
  - data (& system services) is accessible to authorized parties

---

- authenticity
  - the triad req's (above) should be verifiable
- accountability
  - all actions in the system should be traceable

preserving security is difficult (1)

- a battle of human vs human!
  - no one is smarter!
  - -∞ to +∞!

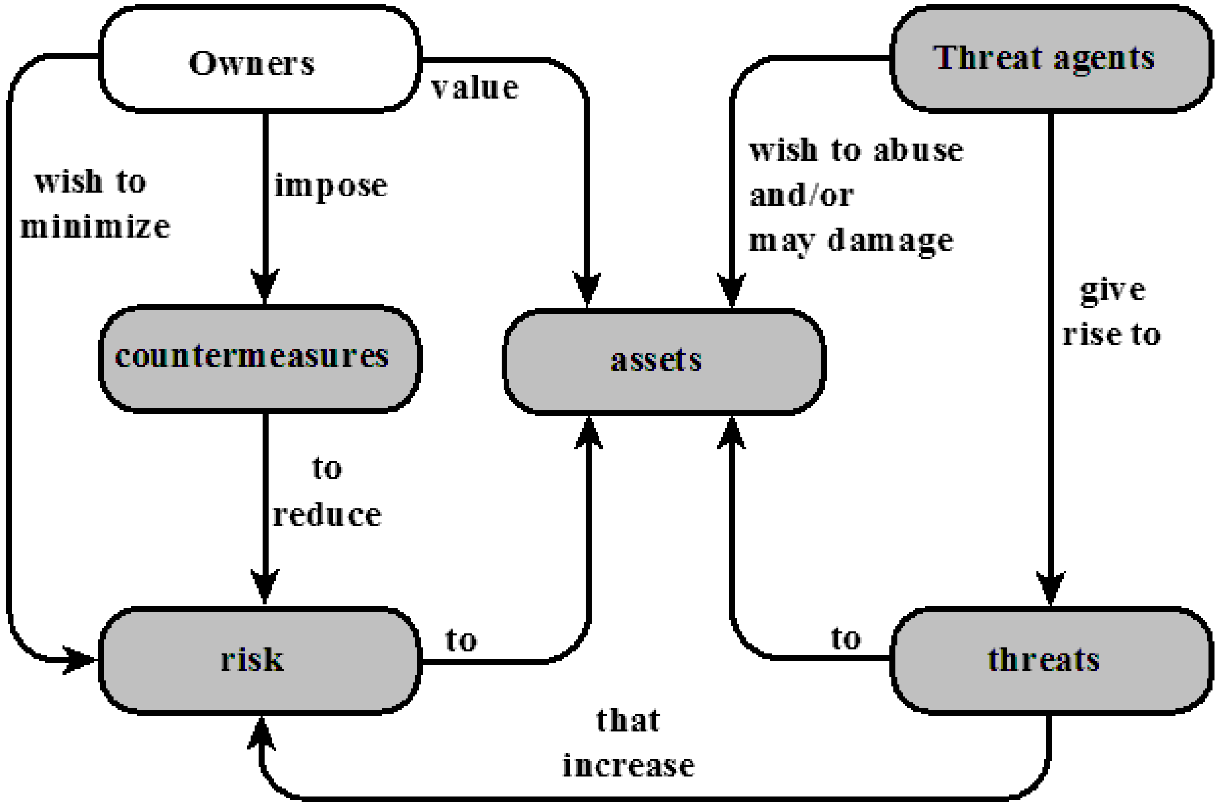
preserving security is difficult (2)

- defense vs offense
  - defender needs to close **all** holes
  - attacker needs only **one** open hole
    - one bad component in defense side is sufficient enough to fail

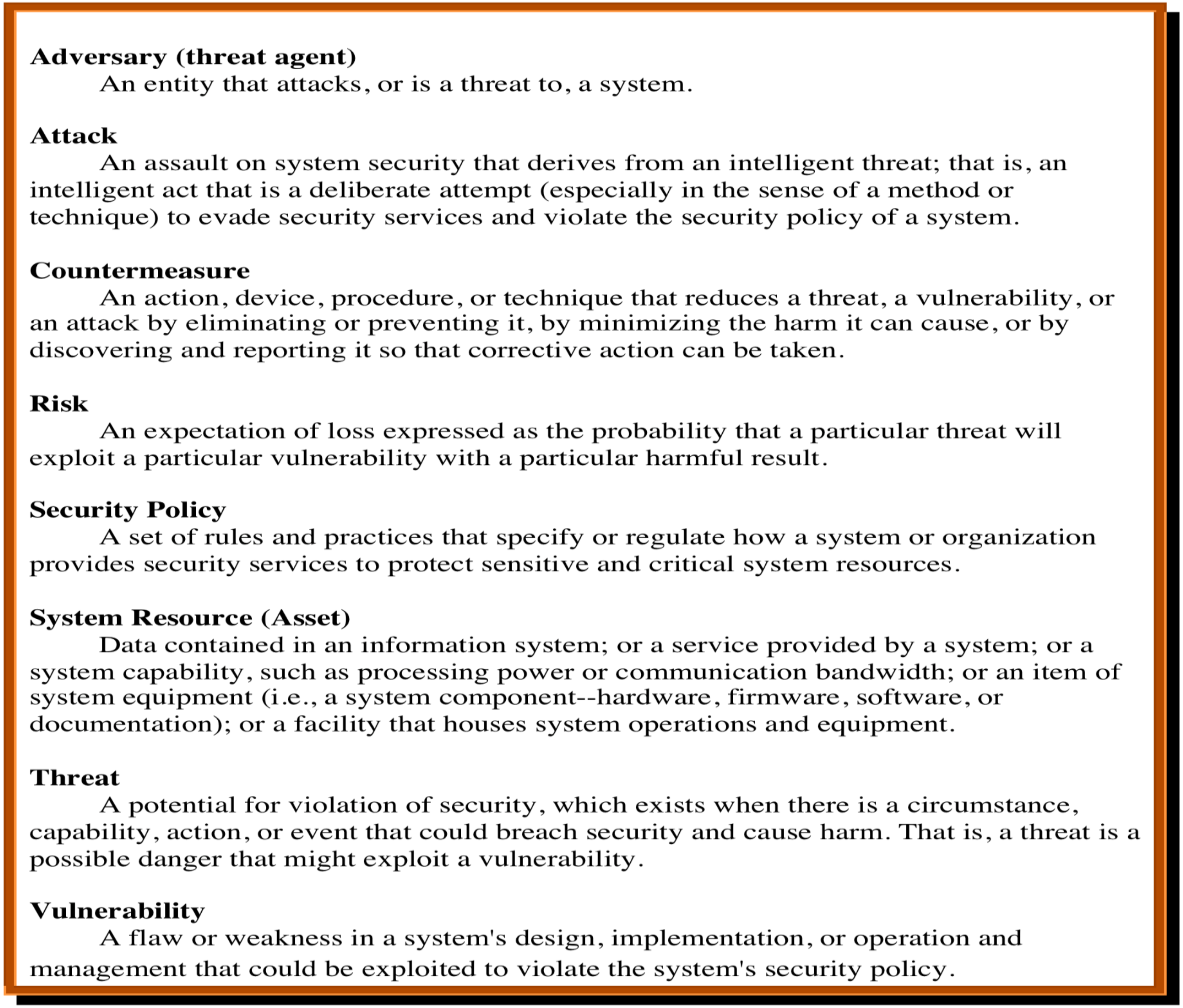
preserving security is difficult (3)

- complex mechanisms, although simple req's
- requires considering potential attacks
  - requires avoiding counterintuitive procedures
- developing error-free software is challenging
  - recursive nature (developing software to protect software)
- requires deciding where to deploy mechanisms
- requires possession of secret info
- requires constant teamwork and cooperation
  - hence, good training becomes even more critical
- battle of wits between attacker / admin
- not perceived on benefit until fails
- requires regular monitoring
- too often an afterthought
- regarded as impediment to using system

security terminology (1)



security terminology (2)



Adversary (threat agent)

An entity that attacks, or is a threat to, a system.

Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Countermeasure

An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Risk

An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Security Policy

A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

System Resource (Asset)

Data contained in an information system; or a service provided by a system; or a system capability, such as processing power or communication bandwidth; or an item of system equipment (i.e., a system component--hardware, firmware, software, or documentation); or a facility that houses system operations and equipment.

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Vulnerability

A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

attacks

- attacks are threats carried out and may be
  - passive: attempt to learn or make use of information from the system that does not affect system resources
    - Eavesdropping on, or monitoring of, transmissions
    - Goal of attacker is to obtain information that is being transmitted
    - Two types:
      - Release of message contents
      - Traffic analysis
    - are hard to detect, so aim to prevent them
  - active: attempt to alter system resources or affect their operation
    - Involve some modification of the data stream or the creation of a false stream
    - Four categories:
      - Replay
      - Masquerade
      - Modification of messages
      - Denial of service
    - are hard to prevent, so aim to detect them

defense methods (countermeasures)

- means used to deal with security attacks
  - prevent it
  - deter it (make attacks harder)
  - deflect it (make attacks look not worthy)
  - detect it
  - recover from it
- may result in new vulnerabilities
- will have residual vulnerability

- the goal is to minimize risk given constraints
- depth defense (layering)

some countermeasure mechanisms (1)

- for data
  - cryptography
- for systems
  - authentication
  - access control
  - os security measures
  - anti virus scanner
  - firewalls

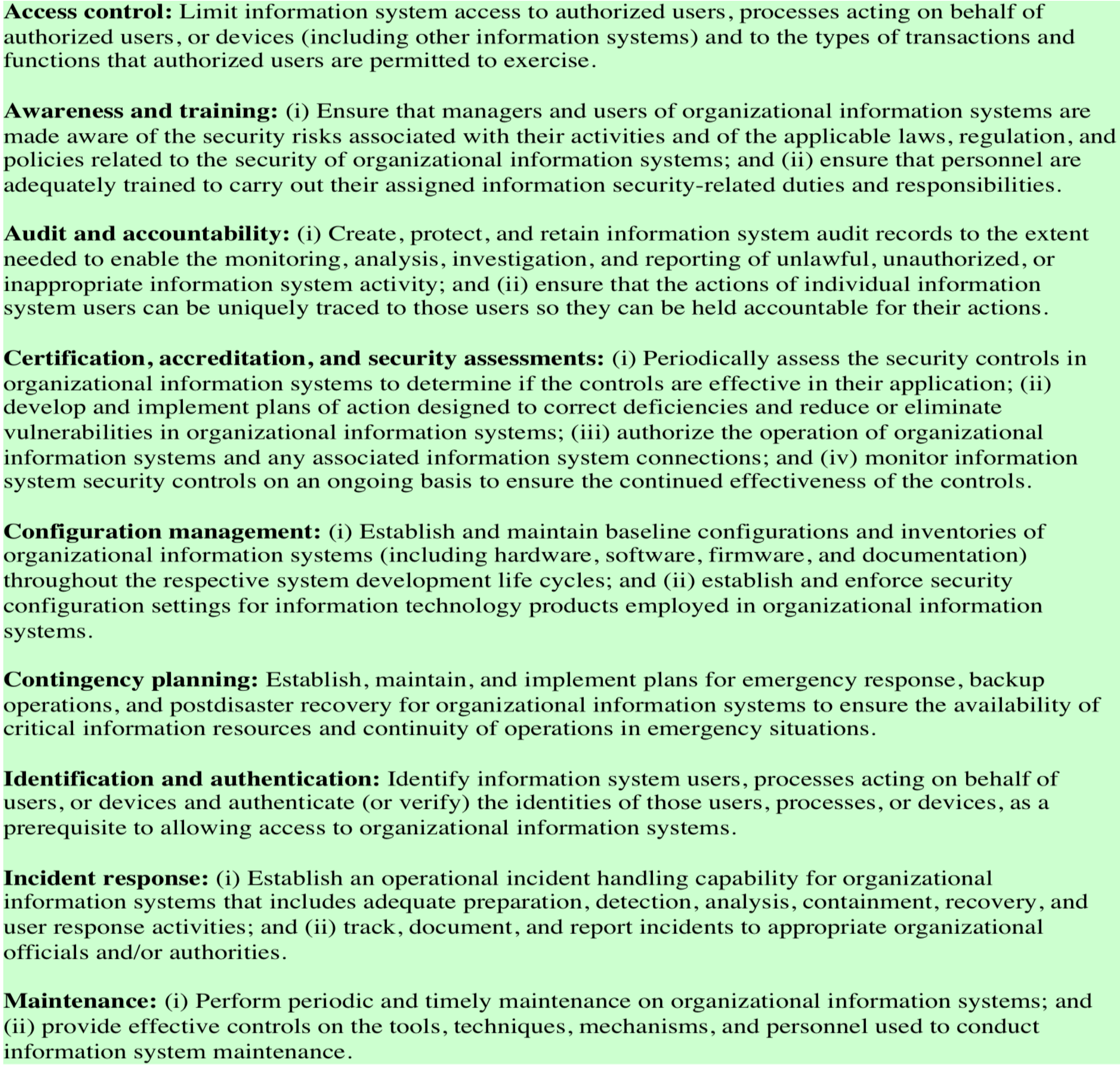
some countermeasure mechanisms (2)

- physical countermeasures
  - physical protection of hardware
  - locks
  - guards
  - surveillance systems
  - off-site backup
- policies and procedures
  - covers data, systems, and physical controls

threat consequences

- disclosure
  - data/system is accessed by an unauthorized entity
- deception
  - authorized entity accesses wrong (falsified) data/system, and believe it
- disruption
  - the data/system is not available to authorized entity
- usurpation
  - an unauthorized entity gets the control of the data/system

security functional requirements (1)



Access control: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Awareness and training: (i) Ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, regulation, and policies related to the security of organizational information systems; and (ii) ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Audit and accountability: (i) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Certification, accreditation, and security assessments: (i) Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Configuration management: (i) Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

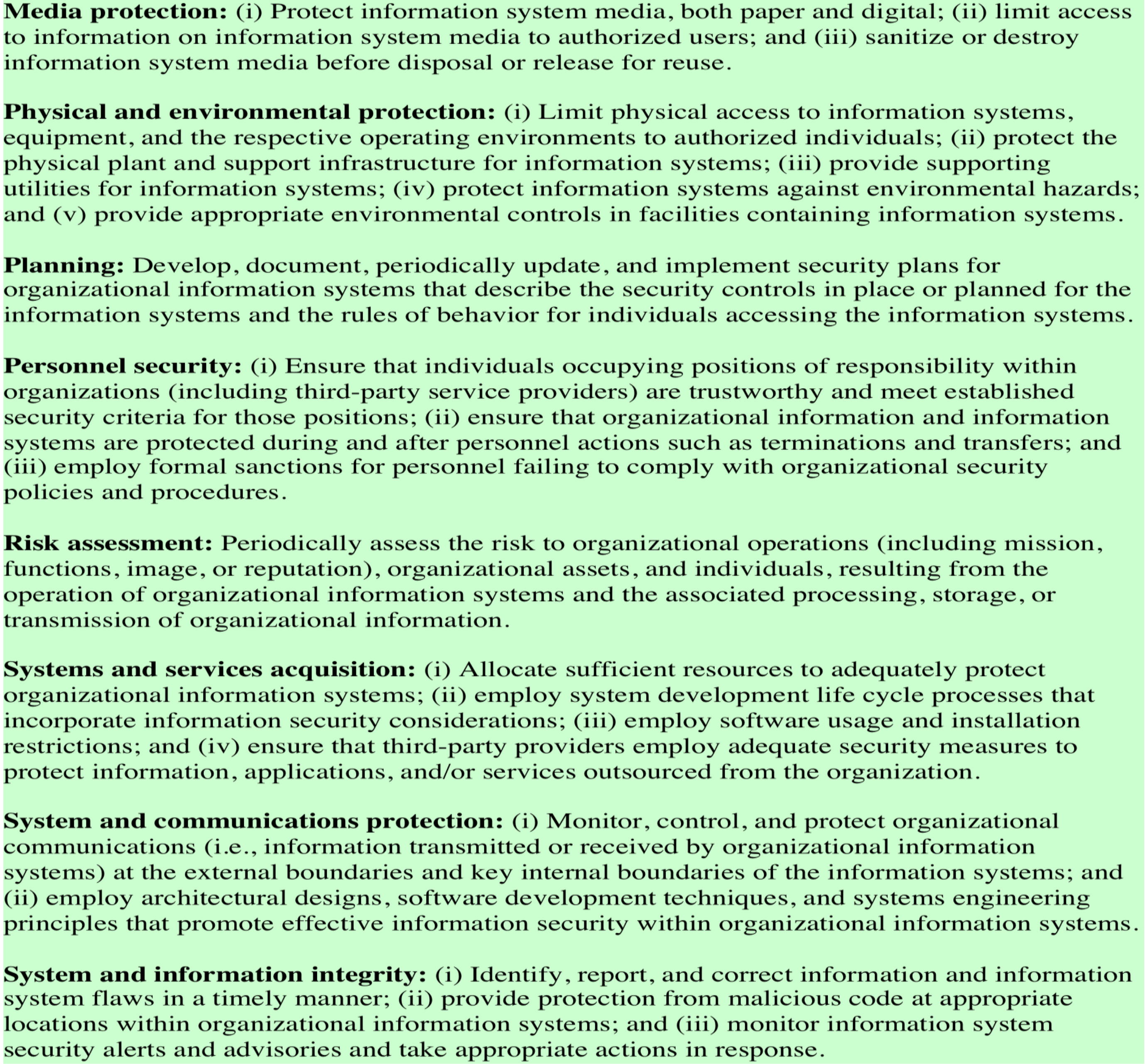
Contingency planning: Establish, maintain, and implement plans for emergency response, backup operations, and postdisaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Identification and authentication: Identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Incident response: (i) Establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

Maintenance: (i) Perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

security functional requirements (2)



Media protection: (i) Protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

Physical and environmental protection: (i) Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

Planning: Develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

Personnel security: (i) Ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

Risk assessment: Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

Systems and services acquisition: (i) Allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

System and communications protection: (i) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

System and information integrity: (i) Identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

3 paradigm principles

- principle of easiest penetration
  - a system is only as strong as its weakest link
- principle of effectiveness
  - countermeasures must be efficient, easy, and appropriate
    - awareness of problem
    - likelihood of use
    - overlapping countermeasures
    - periodic review
- principle of adequate protection
  - security is economics

13 design principles (1)

- principle of simplicity
  - the design must be as small and simple as possible
- principle of closed-world assumption
  - fail-safe default (false negative is better than false positive in this context)
- principle of complete mediation
  - access should be controlled not only at arrival also throughout the system
    - rarely used

13 design principles (2)

- principle of open design
  - cannot assume the adversary does not know your design
- principle of separation of privileges
  - inspired by separation of duties (multistepping)
  - more than one privilege is needed to access a critical data/system
- principle of least privilege
  - minimize privileges given to entities

13 design principles (3)

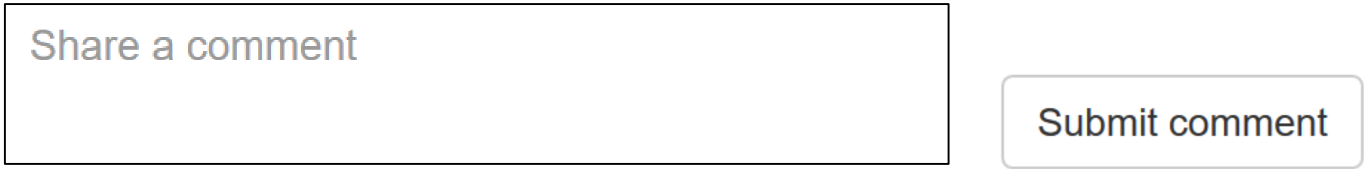
- principle of least common mechanism
  - minimize the functions shared by different end-users
- principle of psychological acceptability
  - do not interfere unduly with normal work of end-users
- principle of isolation
  - public components should be isolated from critical ones;
  - critical ones should be isolated from one another if can
  - isolations should be both logically and physically
- principle of encapsulation
  - object oriented form of isolation

13 design principles (4)

- principle of modularity
  - develop security modules that are shared by all other modules
- principle of layering
  - depth defense
- principle of least astonishment
  - use transparent methods
    - minimize surprising approach

threat examples: **sql injection**

- if the front-end does not sanitize the input:



- back-end code:

```
var query = “INSERT INTO comments (comment) VALUES (‘$c’)”;
```

normal input:

nice website!

malicious input:

‘); drop table users;--

```
var query = “INSERT INTO
comments (comment) VALUES
(‘nice website’)”;
```

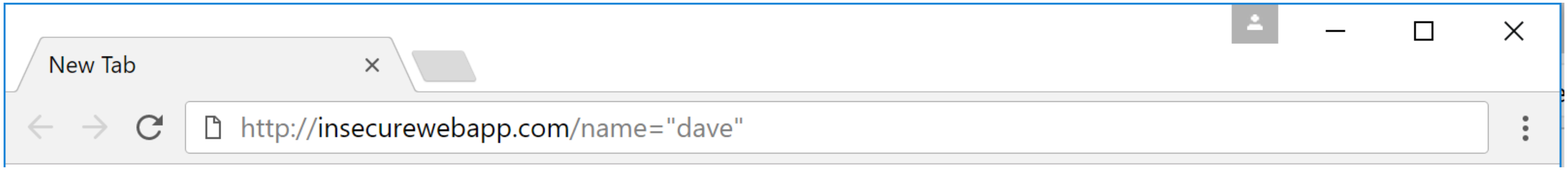
```
var query = “INSERT INTO
comments (comment) VALUES
(‘’); drop table users;--‘)”;
```

threat examples: **sql injection**

- how to prevent sql injection?

threat examples: **xss** (1)

- cross site scripting
  - many different forms

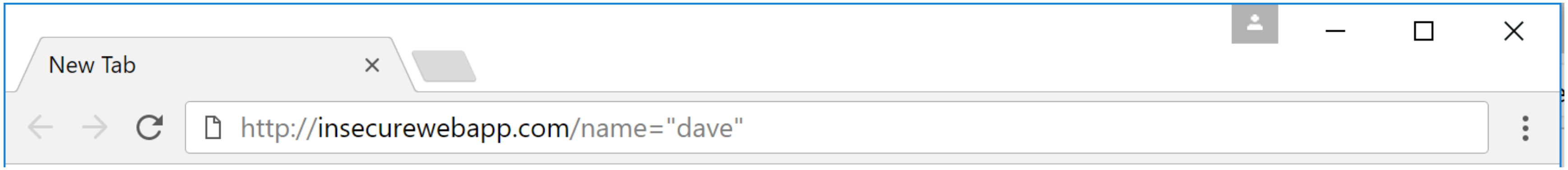


http://insecurewebapp.com/name="dave"

- adversary verifies if scripts run

threat examples: **xss** (1)

- cross site scripting
  - many different forms

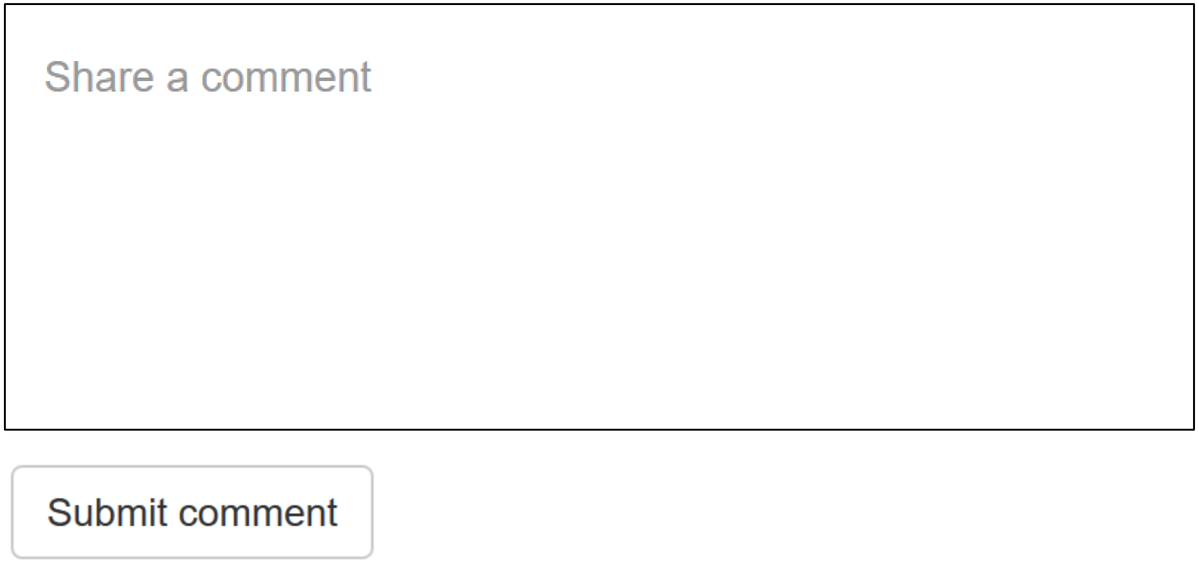


http://insecurewebapp.com/name="dave"

- adversary verifies vulnerability (if scripts run)
  - via url alteration (works for GET method)
  - if yes, then it can send a script to users of the vulnerable web app for malicious purposes

threat examples: **xss** (2)

- if the front-end does not sanitize the input:


Share a comment
Submit comment