Principles of Information Security

Target Course

CS1

Learning Goals

A student shall be able to:

1. Describe foundational security concepts in securing networks and systems.
2. Describe security design principles and identify security issues associated with common threats and attacks.

IAS Outcomes

The CS2013 Information Assurance and Security outcomes addressed by this module are:

IAS Knowledge Topic	Outcome
Foundational Concepts in Security	1. Analyze the tradeoffs of balancing key security properties (Confidentiality, Integrity, and Availability). [Usage] 2. Describe the concepts of risk, threats, vulnerabilities and attack vectors (including the fact that there is no such thing as perfect security). [Familiarity] 3. Explain the concepts of authentication, authorization, access control. [Familiarity] 4. Explain the concept of trust and trustworthiness. [Familiarity]
Threats and Attacks	1. Describe likely attacker types against a particular system. [Familiarity]

Dependencies

- Assumes no pre-requisite knowledge.

Summary

Introduce foundational concepts in security from a top down perspective.

Estimated Time

[Provide the estimated amount of lecture time to cover this module, using the notion of time as defined in CS2013.]

Materials

What is information security?

Information security can be thought of as a discipline that studies ways to make systems trustworthy. Trust is the act of placing your confidence in something and trustworthiness means that the placement of confidence is well-founded. In the context of information security trust is the belief that a system or a component will operate in an expected manner and that attacks on the system will either not succeed or will cause minimal damage. Trustworthiness means that evidence exists that allows us to have trust in a component/system; we have evidence that a component/system meets a set of (functional and security) requirements.

An example of having trust is when a consumer trusts that a credit card reader will not divulge their credit card information to an unknown third party. In the case of the attack on Target (the large retail company) in December, 2013, attackers were able to inject malicious code into the credit card readers [5], allowing the information for any credit card swiped to be sent to a malicious third party. This is an example where a consumer has trust in the credit card system,

but the credit card readers at Target during this attack were not trustworthy (i.e., these devices, at this point in time, did not deserve our trust).

Due to society's increasing reliance of computer systems it is a necessity to place trust on computer systems and web services and it is done so pervasively. To ensure the trustworthiness of information systems the latest NIST cybersecurity framework advocates that organizations think of security as a continuous process and lists five key functions:

- Identification of vulnerabilities and risks.
- Defending systems user errors and malicious attacks.
- Detecting when a system has been misused or attacked.
- Responding to attacks.
- Planning for recovery.

Information security at a high level includes all of these functions.

We list some definitions related to the first step of the NIST framework: identification of ***vulnerabilities*** *and* ***risks*** . A vulnerability is a susceptibility or weakness in the system that can expose it to an attack. For example, a vulnerability might allow a malicious user to gain access to private data. The people or adversaries who may violate a systems security by exploiting vulnerabilities are called ***threats*** or ***attackers.*** The list of possible threats include incompetent or unintentional blunders, hackers, disgruntled employees, organized crime, market competitors, foreign nations etc. The list of potential threats will vary based on the given system. For example a system storing student records is probably not going to be targeted by a foreign nation or organized crime. ***Risk*** is the expected damage of vulnerability. Thus risk considers the likelihood of a vulnerability being exploited and the cost of the damage. For example a web service running on a server may have a vulnerability, but if it's not connected to the network, the risk is zero. An ***attack vector*** describes how an attacker was able to gain access to the system and carried out the attack and is typically used to describe malicious attacks rather than unintentional errors. Attack vectors could include malicious email attachments, a sql code injection, and even social engineering attacks where a human operator is tricked to weaken system defenses.

What are the goals of information security?

The goals of information security are often described by the acronym C.I.A which stands for *confidentiality, integrity* and *availability* (not central intelligence agency!).

In the context of information security, *confidentiality* is the protection of data from unauthorized disclosure. *Integrity* is the assurance that data has not been altered with in an unauthorized way. *Availability* is the assurance that the data/service is accessible in a reliable way by those authorized to access it.

What are some examples of breaches of C.I.A?

Ensuring confidentiality means to prevent sensitive information from reaching unauthorized persons. Examples of breaches in confidentiality are:

- A student finds a spreadsheet containing the test scores of all the students in the class
- A student's private discussions with his/her counselor is revealed to his/her teacher. (For example if the teacher and guidance counselor are friends)
- A student's records are released by the school without obtaining the student's permission

Integrity is the assurance that data has not been changed inappropriately, whether by accident or by a malicious attacker. It also includes the assurance that the data actually came from the expected person or entity rather than an imposter. Examples of breaches include

- You receive an email that looks like it is from your bank but in fact is a phishing attack
- You request to transfer $100 from your account but an attacker changes the value to $10,000

Availability measures make data/service accessible to those who are authorized. Examples of breeches of availability:

- Not being able to access a web site if it is under a denial of service attack
- A malicious attacker gains access to administrative privileges to a website and changes the passwords of valid users, preventing them from accessing the site

Balancing C.I.A

The C.I.A goals are often at odds with one another. When designing security controls for a particular system, one needs to determine the right balance between these goals. For example, an application may lockout a user's account after several failed password attempts. This design intentionally compromises availability (i.e., locking out the user) to ensure the confidentiality and integrity of data. This tradeoff may be suitable for some applications (e.g. email, bank accounts, etc.), but not for others (e.g. emergency applications where it would be unacceptable to lock out a user). Often it is the case that whenever availability is increased, confidentiality and integrity decreases because of prolonged exposure.

Confidentiality and integrity may also conflict with each other. For example, consider an application that allows you to query for averages or other statistical information over a population. Enforcing integrity means that the outputs of these queries should be related to the underlying population data *x*. It might seem that since the queries are over a whole population information of a single individual is still kept confidential. However, this may not be the case. For example, the average salary over a sub-population of 1 person yields the salary of the sole individual. And creating a sub-population of size 1 is surprisingly easy: gender, date of birth, and zip code (i.e., well known attributes for an individual) together uniquely identify 99% of the people in Cambridge, Massachusetts.

Since the C.I.A goals are often at odds with one another it is impossible to design systems which have perfect security. Hence the goal is rather to design system security to minimize risk and to be aware (as much as is possible) of the risks which still remain.

What are some important concepts in information security?

Authenticity, assurance, anonymity and non-repudiation are important concepts.

- Assurance "refers to how trust is provided and managed in computer systems". Trust involves the interaction of:

  - Policies (i.e., behavioral expectations).
  - Permissions (i.e., behaviors allowed by agents).
  - Protections (i.e., mechanisms that enforce policies and permissions).
- Authenticity is the ability to determine whether credentials issued by a person or system are genuine. For example when you go to the bank teller or an ATM you present your bank card and a pin. These items are used to authenticate that you have the right to make a withdrawal from your account. Authentication can be done based on:
  - Something you know: things such as a PIN, a password, or your mother's maiden name.
  - Something you have: a driver's license or a magnetic swipe card.
  - Something you are: biometrics, e.g. fingerprints, retina scans, etc.
- Anonymity is a “property that certain records or transactions (are) not … attributable to any individual”.
- Non-repudiation is the assurance that someone cannot deny something; a user should be responsible for their actions and should not be able to deny what they have done.

How are ethical issues relevant in information security?

Information security is a discipline that requires more than just technical solutions. Often security designers must make policy choices and consider ethical issues. For example, consider the choice of whether or not to disclose a newly discovered vulnerability in a deployed system. On one hand revealing the vulnerability can make an attacker’s job easier and open current users to attacks. On the other hand, not disclosing the vulnerability is equivalent to misrepresenting the system's security which may be bad for business, and might even have legal consequences. Furthermore, keeping a vulnerability secret in no way guarantees that the vulnerability will stay secret from attackers.

Assessment Methods

Multiple Choice Questions (answers are in bold)

1. With respect to cybersecurity, what does CIA stand for?
   a. Central intelligence agency.
   b. Confidential internal audit.
   c. Confidentiality, integrity, and availability.
   d. Cyber information asset.

2. Which of the following statements are true?
   a. Trust is the user’s belief that a system will operate in an expected manner and that attacks will either not succeed or cause minimal damage.
   b. The most popular web services (e.g. bank web sites, facebook, twitter) are trustworthy.
   c. All of the above.
   d. None of the above.

3. What does anonymity mean from an information security perspective?
   a. Anonymity is a property that certain records or transactions are not attributable to any individual.
   b. Anonymity is a property that certain records or transactions are not authenticated to any individual.
   c. Anonymity is a property that certain records or transactions are not available to any individual.
   d. None of the above.

4. Information security is a broad subject area that encompasses many aspects of information technology and organizational processes. According to NIST (the U.S. National Institute of Standards and Technology), the five functions that make up information security are:
   a. Establish, protect, discover, reply, and recover.
   b. Establish, protect, detect, reply, and recover.
   c. Establish, protect, detect, respond, and recover.
   d. Identify, protect, detect, respond, and recover.
   e. Identify, protect, discover, reply, and recover.

5. Which of the following is the best description for information security?
   a. Information security is the practice of defending information from unauthorized access and misuse.
   b. Information security is the practice of defending information from unintentional errors by trusted users and from attacks from malicious users.
   c. Information security is the practice of defending systems from unauthorized access and misuse.
   d. Information security is the practice of defending systems from unintentional errors by trusted users and from attacks from malicious users.
   e. All of the above.
   f. None of the above.

6. Which of the following is an accurate description of an information security goal?
   a. Confidentiality is the protection of data from unauthorized disclosure.
   b. Confidentiality is the protection of systems from unauthorized access.
   c. All of the above.
   d. None of the above.

7. Which of the following is an accurate description of an information security goal?
   a. Integrity is the assurance that data has not been altered in an unauthorized way.
   b. Integrity is the assurance that systems have not not altered in an unauthorized way.
   c. All of the above.
   d. None of the above.

8. Which of the following is an accurate description of an information security goal?
   a. Availability is the assurance that the data/service is accessible in a reliable way by those authorized to access it.
   b. Availability is the assurance that a system is accessible to authorized users.
   c. All of the above.
   d. None of the above.

9. Why is it impossible to design systems which have perfect security?
   a. Designing a system that has perfect security is impossible since the three information security goals, known as CIA, are often at odds with each other. For example, a design that locks out a user account after X failed login attempts compromises availability as a tradeoff for ensuring confidentiality and integrity.
   b. Designing a system that has perfect security is impossible since the three information security goals, known as CIA, are often at odds with each other. For example, a design that queries for averages (or other statistical information) over a population of individuals may leak sensitive data as the size of the population gets closer to 1.

c. All of the above.
d. None of the above.

10. Within the domain of information security, which of the following is the best description for authenticity?
    a. Authenticity is the ability to determine whether an individual has supplied a correct username/password for a system.
    b. Authenticity is the ability to determine whether an individual has supplied credentials that are genuine.
    c. Authenticity is the ability to determine that statements, policies, and permissions issued by persons or systems are genuine.
    d. All of the above.
    e. None of the above.

11. Within the domain of information security, which of the following is the best description for assurance?
    a. Assurance refers to how trust is provided and managed in computer systems.
    b. Assurance refers to the interaction of policies, permissions, and protections that foster trust in a system.
    c. All of the above.
    d. None of the above.

12. Within the domain of information security, which of the following is the best description for anonymity?
    a. Anonymity is a property that certain records or transactions are not attributable to any individual.
    b. Anonymity is a property that certain records or transactions are attributable to any individual.
    c. All of the above.
    d. None of the above.

True/False (answers are in bold)

13. True or false? Keeping the existence of a software vulnerability a secret is always better than publicly revealing that the vulnerability exists.
    a. True.
    b. False.

14. True or false? It is possible to create a software system that has perfect (100%) security (i.e., has no vulnerabilities).
    a. True.
    b. False.

Matching Questions

15. Select the correct description for each term.

    TERMS
    a. Attack vector
    b. Risk
    c. Threat
    d. Vulnerability

DESCRIPTIONS

a. Describes how an attacker was able to gain access to the system and carried out the attack.
b. The expected damage from a violation of a security policy.
c. The people or adversaries who may violate a systems security by exploiting vulnerabilities.
d. A susceptibility or weakness in the system that can expose it to an attack.
e. An intention to inflict damage on a system.
f. The expected damage from a situation involving exposure to danger.

Answers: term a to description a; term b to description b; term c to description c; and term d to description d

Short Answer Questions

16. In each scenario an individual under 21 obtains alcohol. Describe which concept - authentication, authorization and/or access control - is breached.
    a. Scenario: The individual goes into a bar and is asked to wear a green band to indicate that she/he is not allowed to purchase alcohol. The bar is crowded and the bartender misses the green band and allows the individual to purchase alcohol.
    b. Scenario: The individual uses a fake ID to get into a bar and buy alcohol.
    c. Scenario: The individual goes to a party where alcohol is being served.

17. Describe which security properties are being balanced in the following scenarios:
    a. Scenario: Consider the following enhanced security protocol for an application. To login the user first enters their password. If correct the application will text the user a pin. Then the user must type in their password as well as the pin to access the application.
    b. Scenario: Students are only informed of the average grade of a homework assignment only if more than 10 students submitted it.

18. Suppose your company is about to release a new product when a security vulnerability is discovered. What are the ethical implications with fixing or not fixing the vulnerability before releasing the product?

19. Conduct a security review of one of the following scenarios.

    Scenario #1 – At a sit down restaurant you pay with your credit card. The waiter/waitress brings you the bill, you give them your credit card, they take it to the cash register to ring up your order and bring it back to you in approximately 5 minutes.

    Scenario #2 – You and your cousin decide to run in this year's turkey trot (good for you!). Participants can register online up to 3 months prior to the race. On the morning of the race, participants who have pre-registered give the race officer their name, the race officer checks the list of pre-registrants to make sure the name is on a list, and hands out the bib.

    Scenario#3 – Make up a similar type of scenario and analyze it.

    In your security review:
    a. Describe at least one vulnerability that it has.

b. Describe the threats and possible attack vectors for that vulnerability.
c. Describe how risky the vulnerability is.
d. Describe at least one entity we currently trust to not take advantage of the vulnerability.
e. Describe at least one possible way to mitigate the vulnerability even if the entity above is untrustworthy.

References

[1] M.T. Goodrich & R. Tamassia, (2011). *Introduction to Computer Security*. Addison Wesley.

[2]F.B. Schneider - Draft chapters for a textbook on cybersecurity (as yet, untitled) available at Retrieved August, 2016 from https://www.cs.cornell.edu/fbs/fullist.html.

[3] Security Week. Cyberphysical Security: The Next Frontier. Retrieved August, 2016 from http://www.securityweek.com/cyberphysical-security-next-frontier.

[4] National Institute of Standards and Technology. 2014. *Framework for Improving Critical Infrastructure Cybersecurity, Ver. 1.* (Feb. 12, 2014). Retrieved July, 2016 from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

[5] N. Giannopoulos, (2014). Target Identifies Suspects, Security Breaches Become Growing Concern, January 24, 2014. Retrieved August 9, 2017 from https://risnews.com/target-identifies-suspects-security-breaches-become-growing-concern.