CS361C: Information Assurance and Security

Introduction to IA

Bill Young
Department of Computer Science
University of Texas at Austin

Last updated: February 2, 2015 at 06:38

Some Sources

- Andrew Blyth and Gerald L. Kovacich, *Information Assurance: Surviving in the Information Environment*: Springer, 2001.
- Debra S. Herrmann, *Complete Guide to Security and Privacy Metrics*: Auerbach, 2007.
- Douglas J. Landoll, *The Security Risk Assessment Handbook*: Auerbach, 2006.
- Michael E. Whitman and Herbert J. Mattord, *Principles of Information Security*: Thomson, 2009.
- Bel G. Raggad, *Information Security Management: Concepts and Practice*: CRC Press, 2010.

Thought Experiment

Suppose you visit an e-commerce website such as your bank, stock broker, etc.

Before you type in highly sensitive information, you'd like to have some assurance that your information will be protected. Do you (have such assurance)? How can you know?

What security-relevant things do you want to happen, or not happen when you use such a website?

Thought Experiment

You might want:

- Privacy of your data
- Protection against phishing
- Integrity of your data
- Authentication
- Authorization
- Confidentiality
- Non-repudiation
- Availability
- What else?

Which of these do you think fall under Information Assurance?

System Quality

According to ISO/IEC Standard 9126-1 (Software Engineering—Product Quality), the following are all aspects of system quality:

- functionality
  - adequacy
  - interoperability
  - correctness
  - security
- reliability
- usability
- efficiency
- maintainability
- portability

Which of these do you think apply to IA?

What is Information?

This class is about *Information Assurance*; so what is "information"? How does information differ from data?

What is Information?

This class is about *Information Assurance*; so what is "information"? How does information differ from data?

"Information is data endowed with relevance and purpose. Converting data into information thus requires knowledge. Knowledge by definition is specialized." (Blyth and Kovacich, p. 17)

And what characteristics should information possess to be useful? It should be: accurate, timely, complete, verifiable, consistent, available.

What is Information?

According to Raggad (pp. 14ff), the following are all distinct conceptual resources:

Noise: raw facts with an unknown coding system

Data: raw facts with a known coding system

Information: processed data

Knowledge: accepted facts, principles, or rules of thumb that are useful for specific domains. Knowledge can be the result of inferences and implications produced from simple information facts.

What is Information Assurance?

What about "assurance"? What does that mean? Assurance from what or to do what? Is it context-dependent?

What is Information Assurance?

What about "assurance"? What does that mean? Assurance from what or to do what? Is it context-dependent?

According to the U.S. Department of Defense, IA involves:

> *Actions taken that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities.*

Information Assurance (IA) is the study of how to protect your information assets from destruction, degradation, manipulation and exploitation. But also, how to recover should any of those happen. *Notice that it is both proactive and reactive.*

What is IA? (cont)

According to the DoD definition, these are some aspects of information needing protection:

- **Availability:** timely, reliable access to data and information services for authorized users;
- **Integrity:** protection against unauthorized modification or destruction of information;
- **Confidentiality:** assurance that information is not disclosed to unauthorized persons;
- **Authentication:** security measures to establish the validity of a transmission, message, or originator.
- **Non-repudiation:** assurance that the sender is provided with proof of a data delivery and recipient is provided with proof of the sender's identity, so that neither can later deny having processed the data.

Is this specifically a military view? Which of these are the most important? How would you decide?

What is IA?

Information Assurance is such a broad field that there is no universally accepted definition. Researchers often give their own spin to IA, usually reflecting their own concerns.

In these slides, are several different views of IA, including the DoD view (above), Herrmann's view (below), and Blyth and Kovacich's view (below). Be able to compare and contrast these views.

A Different View of IA

According to Debra Herrmann (*Complete Guide to Security and Privacy Metrics*), IA should be viewed as spanning four security engineering domains:

- physical security
- personnel security
- IT security
- operational security

> *The simple truth is that IT security cannot be accomplished in a vacuum, because there are a multitude of dependencies and interactions among all four security engineering domains.* (Herrmann, p. 10)

So threats/risks to IA should be considered along these dimensions as well.

A Different View of IA

According to Debra Herrmann, IA has four major categories:

- physical security
- personnel security
- IT security
- operational security

Into which of these would you put the following?

- enforcing hard-to-guess passwords
- encrypting your hard drive
- locking sensitive documents in a safe
- stationing a marine guard outside an embassy
- assigning security clearances to staffers
- using SSL for data transfers
- having off-site backup of documents

Four Security Domains

Quotes from Debra Herrmann, *Complete Guide to Security and Privacy Metrics*:

"*Physical security* refers to the protection of hardware, software, and data against physical threats to reduce or prevent disruptions to operations and services and loss of assets."

"*Personnel security* is a variety of ongoing measures taken to reduce the likelihood and severity of accidental and intentional alteration, destruction, misappropriation, misuse, misconfiguration, unauthorized distribution, and unavailability of an organization's logical and physical assets, as the result of action or inaction by insiders and known outsiders, such as business partners."

Four Security Domains

"*IT security* is the inherent technical features and functions that collectively contribute to an IT infrastructure achieving and sustaining confidentiality, integrity, availability, accountability, authenticity, and reliability."

"*Operational security* involves the implementation of standard operational security procedures that define the nature and frequency of the interaction between users, systems, and system resources, the purpose of which is to

1. achieve and sustain a known secure system state at all times, and
2. prevent accidental or intentional theft, release, destruction, alteration, misuse, or sabotage of system resources."

Are these domains purely defensive, or might they be offensive? Compare and contrast Herrmann's view of IA with the government view outlined before.

Yet Another Perspective

According to Raggad's taxonomy of information security, a computing environment is made up of five continuously interacting components:

- activities,
- people,
- data,
- technology,
- networks.

A comprehensive security plan must take all of these into account. How do these map onto the previous scheme?

Does protecting a computing environment merely mean protecting these five components?

Yet Another View: Components of IA

IA includes computer and information security, but more besides. According to Blyth and Kovacich, IA can be thought of as protecting information at three distinct levels:

physical: data and data processing activities in physical space;

information infrastructure: information and data manipulation abilities in cyberspace;

perceptual: knowledge and understanding in human decision space.

IA Levels: the Physical

The lowest level focus of IA is the physical level: computers, physical networks, telecommunications and supporting systems such as power, facilities and environmental controls. Also at this level are the people who manage the systems.

Desired Effects: to affect the technical performance and the capability of physical systems, to disrupt the capabilities of the defender.

Attacker's Operations: physical attack and destruction, including: electromagnetic attack, visual spying, intrusion, scavenging and removal, wiretapping, interference, and eavesdropping.

Defender's Operations: physical security, OPSEC, TEMPEST.

IA Levels: Infrastructure

The second level focus of IA is the information structure level. This covers information and data manipulation ability maintained in cyberspace, including: data structures, processes and programs, protocols, data content and databases.

Desired Effects: to influence the effectiveness and performance of information functions supporting perception, decision making, and control of physical processes.

Attacker's Operations: impersonation, piggybacking, spoofing, network attacks, malware, authorization attacks, active misuse, and denial of service attacks.

Defender's Operations: information security technical measures such as: encryption and key management, intrusion detection, anti-virus software, auditing, redundancy, firewalls, policies and standards.

IA Levels: Perceptual

The third level focus of IA is the perceptual level, also called *social engineering*. This is abstract and concerned with the management of perceptions of the target, particularly those persons making security decisions.

Desired Effects: to influence decisions and behaviors.

Attacker's Operations: psychological operations such as: deception, blackmail, bribery and corruption, social engineering, trademark and copyright infringement, defamation, diplomacy, creating distrust.

Defender's Operations: personnel security including psychological testing, education, and screening such as biometrics, watermarks, keys, passwords.

IA Overview

Thus, IA includes aspects of:

- COMPSEC: computer security;
- COMSEC: communications and network security;
- ITSEC: (which includes both COMPSEC and COMSEC);
- OPSEC: operations security.

Compare Blyth and Kovacich's view of IA with the government view and Herrmann's views described previously.

IA Overview

If you entrench yourself behind strong fortifications, you compel the enemy to seek a solution elsewhere. –Carl von Clausewitz

A recent headline in the AAS read: "The Biggest Threat to Computer Security? Carelessness"

Principle of Easiest Penetration: An attacker on any information system will use the simplest means of subverting system security.

Many IA Failures Don't Involve Technology

In 1996, news of possible signs of life in a Martian meteorite called ALH84001 leaked out ahead of a press conference that had been scheduled by NASA.

This was partly because a high-ranking White House official told a prostitute about the meteorite, who then sold the information to a tabloid.

NASA had to scramble to reschedule its press conference to an earlier date to satisfy the growing demand for information from the press and the public.

The Information Warfare Spin on IA

The flip side of Information Assurance is Information Warfare (IW). In fact, one can think of the offensive part of IW as "information operations," and the defensive part as information assurance.

- *Type I* involves managing an opponent's perception through deception and psychological operations. In military circles, this is called *Truth Projection*.
- *Type II* involves denying, destroying, degrading, or distorting the opponent's information flows to disrupt their ability to carry out or co-ordinate operations.
- *Type III* gathers intelligence by exploiting the opponent's use of information systems.

IW can be carried out against individuals, corporations, or nations. Is hacking IW?

Nature of the Threat

Necessary for IW, as for any related activity, are *motive*, *means*, and *opportunity*.

In general, the offensive players in the world of IW come in six types:

Insiders: consists of employees, former employees and contractors.

Hackers: one who gains unauthorized access to or breaks into information systems for thrills, challenge, power, or profit.

Criminals: target information that may be of value to them: bank accounts, credit card information, intellectual property, etc.

Nature of the Threat (cont.)

Corporations: actively seek intelligence about competitors or steal trade secrets.

Governments and agencies: seek the military, diplomatic, and economic secrets of foreign governments, foreign corporations, and adversaries. May also target domestic adversaries.

Terrorists: usually politically motivated and may seek to cause maximal damage to information infrastructure as well as endanger lives and property.

Is there overlap among these categories of actors? Which do you think is the biggest threat? Does it depend on the target?

Why Does it Matter?

It's a dangerous world out there.

> *While experts may disagree on the definition of cyber war, there is significant evidence that nations around the world are developing, testing and in some cases using or encouraging cyber means as a method of obtaining political advantage.* –McAfee *Virtual Criminology Report 2009*

> *A plausible worst-case worm could cause $50 billion or more in direct economic damage by attacking widely used services in Microsoft Windows and carrying a highly destructive payload."* –Nicholas Weaver and Vern Paxson, 6/14/04

Why Does it Matter?

America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration that will take office in January 2009. ... It is a battle we are losing. Losing this struggle will wreak serious damage on the economic health and national security of the United States. –CSIS report on *Securing Cyberspace for the 44th Presidency*, Dec. 2008

IA Functional Components

Note that IA is both proactive and reactive involving: *protection, detection, capability restoration, and response.*

- *IA environment protection pillars:* "ensure the availability, integrity, authenticity, confidentiality, and non-repudiation of information"
- *Attack detection:* "timely attack detection and reporting is key to initiating the restoration and response processes."

IA Functional Components (2)

- *Capability restoration:*
  - "relies on established procedures and mechanisms for prioritizing restoration of essential functions. Capability restoration may rely on backup or redundant links, information system components, or alternative means of information transfer."
  - "A post-attack analysis should be conducted to determine the command vulnerabilities and recommended security improvements."
- *Attack response:* "involves determining actors and their motives, establishing cause and complicity, and may involve appropriate action against perpetrators... contributes ... by removing threats and enhancing deterrence."

IA Applies to Info Infrastructure

If adversaries intended to attack nations in cyber space, they would select targets which would cause the largest impacts and losses to their opponents with the least effort. It is therefore a very reasonable assumption that adversaries would attack critical infrastructure systems via the Internet. –McAfee Virtual Criminology Report 2009, p. 16

- *Global Information Infrastructure:* "worldwide interconnection of communication networks, computers, databases, and consumer electronics that make vast amounts of information available to users."
- *National Information Infrastructure:* those within or serving the U.S., for government, commerce and research.
- *Defense Information Infrastructure:* those within or serving the DoD (e.g. nodes on SIPRNET and NIPRNET).

Critical Infrastructure Protection

Presidential Decision Directive (PDD-63) of 1998

- Civilian systems are "essential to the minimum operations of the economy and government"
- Examples: telecommunications, energy, banking, transportation and emergency services

Increased vulnerability as:

- information systems have become automated and interlinked;
- information systems are using COTS technology, subject to viruses, worms, etc.

Every federal department CIO is responsible for information assurance.

Federal Orgs Defining IA

Committee on National Security Systems (CNSS)

- Designation of the National Security Telecommunications and Information Systems Security Committee (NSTISSC), chaired by DoD.
- Establishes federal policy directives on network security.
- Sanctions universities to offer security certification.

National Security Agency (NSA)

- Lead cryptographic organization
- Builds and tests secure systems for classified applications
- Coordinates with industry on security development

National Institute of Standards and Technology (NIST)

- Formerly National Bureau of Standards (NBS)
- Leverages NSA's experience in standardizing cryptosystems for civilian use. E.g. DES, SHA, AES.

IA Relationship to Computer Security

- IA includes considerations for non-security threats to information systems, such as acts of nature and the process of recovery from incidents.
- IA *emphasizes management, process, and human involvement*, and not merely technology.
- IA deployments may involve multiple disciplines of security:
  - COMPUSEC (Computer security)
  - COMSEC (Communications security), SIGSEC (Signals security) and TRANSEC (transmission security)
  - EMSEC (Emanations security) denying access to informatoin from unintended emanations such as radio and electrical signals
  - OPSEC (Operations security) the processes involved in protecting information

Some Basic IA Terms

A complete IA glossary can be found at: *National Information Assurance Glossary*, `www.cnss.gov/Assets/pdf/cnssi_4009.pdf`.

Assets

An *asset* is the resource being protected, including:

- **physical assets**: devices, computers, people;
- **logical assets**: information, data (in transmission, storage, or processing), and intellectual property;
- **system assets**: any software, hardware, data, administrative, physical, communications, or personnel resource within an information system.

Assets have value so are worth protecting.

Subjects and Objects

Often a security solution/policy is phrased in terms of the following three categories:

Objects: the items being protected by the system (documents, files, directories, databases, transactions, etc.)

Subjects: entities (users, processes, etc.) that execute activities and request access to objects.

Actions: operations, primitive or complex, that can operate on objects and must be controlled.

For example, in the Unix operating system, processes (subjects) may have permission to perform read, write or execute (actions) on files (objects). In addition, processes can create other processes, create and delete files, etc. Certain processes (running with `root` permission) can do almost anything. That is one approach to the security problem.

Can an entity be both a subject and an object?

Attributes

Both subjects and objects have associated *attributes*. The security mechanisms may operate in terms on the attributes and manipulation of the attributes can be used to subvert security.

What are some attributes associated with subjects? With objects? How are attributes established/changed?

Critical Aspects

Information assets (objects) may have critical aspects:

availability: authorized users are able to access it;

accuracy: the information is free of error and has the value expected;

authenticity: the information is genuine;

confidentiality: the information has not been disclosed to unauthorized parties;

integrity: the information is whole, complete and uncorrupted;

utility: the information has value for the intended purpose;

possession: the data is under authorized ownership and control.

Terms: Threat and Threat Actors

A *threat* is a *category* of entities, or a circumstance, that poses a potential danger to an asset (through unauthorized access, destruction, disclosure, modification or denial of service).

- Threats can be categorized by intent: accidental or purposeful (error, fraud, hostile intelligence);
- Threats can be categorized by the kind of entity involved: human (hackers, someone flipping a switch), processing (malicious code, sniffers), natural (flood, earthquake);
- Threats can be categorized by impact: type of asset, consequences.

A *threat actor* is a specific instance of a threat, e.g. a specific hacker, a particular storm, etc.

Examples of Threats

Interruption: an asset becomes unusable, unavailable, or lost.

Interception: an unauthorized party gains access to an information asset.

Modification: an unauthorized party tampers with an asset.

Fabrication: an asset has been counterfeit.

Give examples of each of these.

Examples of Threats

Interruption: an asset becomes unusable, unavailable, or lost.

Interception: an unauthorized party gains access to an information asset.

Modification: an unauthorized party tampers with an asset.

Fabrication: an asset has been counterfeit.

Give examples of each of these.

Examples:

Interruption: a denial of service attack on a website

Interception: compromise of confidential data, e.g., but packet sniffing

Modification: hacking to deface a website

Fabrication: spoofing attacks in a network

Terms: Environments, Enclaves

A *hostile environment* for assets is one that has known threats. Example: locating an asset in a war zone or a flood zone, or placing an unprotected machine on the Internet.

A *benign environment* is a nonhostile environment that may be protected from external hostile elements by physical, personnel, and procedural countermeasures.

An *enclave* is a collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security.
Describe a local enclave here at UT?

Terms: Vulnerabilities and Exploits

A *vulnerability* is a weakness or fault in a system that exposes information to attack.

- A bug in a computer program is a very common vulnerability in computer security (e.g. buffer overflow situation).
- A procedural failing can subvert technology controls (e.g. a core dump of secure information upon a failure).
- A lack of controls can result in vulnerabilities, if controls are subverted (e.g. Enron financials).

An *exploit* is a method for taking advantage of a known vulnerability.

What's the difference between an exploit and an attack?

Terms: Vulnerabilities and Exploits

A *dangling vulnerability* is one for which there is no known threat (vulnerability is there but not exploitable).

A *dangling threat* is one that does not pose a danger as there is no vulnerability to exploit (threat is there, but can't do damage).

Can you give examples of these or situations in which they might occur?

Terms: Attacks, etc.

An *attack* is an attempt to gain access, cause damage to or otherwise compromise information and/or systems that support it.

Passive attack: an attack in which the attacker observes interaction with the system.

Active attack: at attack in which the attacker directly interacts with the system.

Unintentional attack: an attack where there is not a deliberate goal of misuse

Terms: Attacks, etc. (2)

Attacks have a subject and object.

Attack subject: the active entity, usually a threat actor, that interacts with the system.

Attack object: the targeted information system asset.

The *attack surface* of an organization/entity is the set of ways in which an adversary can enter the system and potentially cause damage. For example:

> *The attack surface of a software environment is the code within a computer system that can be run by unauthenticated users. This includes, but is not limited to: user input fields, protocols, interfaces, and services. (Wikipedia)*

Mention some ways in which the attack surface can be reduced.

Terms: Exposure, Compromise

Exposure is an instance when the system is vulnerable to attack.

A *compromise* is a situation in which the attacker has succeeded.

An *indicator* is a recognized action—specific, generalized or theoretical—that an adversary (threat actor) might be expected to take in preparation for an attack.

Give an example of an indicator.

Terms: Consequences

A *consequence* is the outcome of an attack. In a purposeful threat, the threat actor has typically chosen a desired consequence for the attack, and selects the IA objective to target to achieve this.

- Disruption: targets availability
- Corruption: targets integrity
- Exploitation: targets confidentiality

A consequence may cause the information system to lose effectiveness, and may have other costs.

Inadvertant disclosure is a type of consequence, involving accidental exposure of information to an agent not authorized access.

Terms: Countermeasures

Controls, *safeguards* and *countermeasures* are any actions, devices, procedures, techniques and other measures that reduce the vulnerability of an information system. There are many kinds:

- technical
- policy, procedures and practices
- education, training and awareness
- cover and deception (camouflage)
- human intelligence (HUMINT), e.g. disinformation
- monitoring of data and transmissions
- surveillance countermeasures that detect or neutralize sensors, e.g. TEMPEST
- assessments and inspections.

A *security posture* or security profile is the implementation (policy, procedures, technology) of the security effort within an organization.

Terms: Risk

Viega and McGraw, *Building Secure Software* assert that software and system security is "all about managing risk." Do you agree? Why or why not?

Risk is the possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability. The assessment of risk must take into account the consequences of an exploit.

Risk management is a process for an organization to identify and address the risks in their environment. There are several *risk management frameworks*, and each defines a procedure for an organization to follow.

Risk Management Framework

One particular risk management procedure (from Viega and McGraw) consists of six steps:

1. Assess assets
2. Assess threats
3. Assess vulnerabilities
4. Assess risks
5. Prioritize countermeasure options
6. Make risk management decisions

Thought experiment: try to follow this procedure to manage risks to your material possessions stored at your home or apartment.

Risk Treatments

Once the risk has been identified and assessed, managing the risk can be done through one of four techniques:

Risk acceptance: risks not avoided or transferred are retained by the organization. E.g. sometimes the cost of insurance is greater than the potential loss. Sometimes the loss is improbable, though catastrophic.

Risk avoidance: not performing an activity that would incur risk. E.g. disallow remote login.

Risk mitigation: taking actions to reduce the losses due to a risk; many technical countermeasures fall into this category.

Risk transfer: shift the risk to someone else. E.g. most insurance contracts, home security systems.

Risk Management

The risk treatments—acceptance, avoidance, mitigation, transfer—are with respect to a *specific risk for a specific pary.*

E.g., buying insurance is risk transfer for you, not for the insurance company. For the insurance company, it's risk acceptance. But they may require you to take measures to avoid or mitigate their risk.

There is generally more money in a bank than in a convenience store; but which is more likely to be robbed? Why? Of which risk management technique(s) is this an instance?

Mitigation versus Avoidance

There is often a confusion about the difference between *risk avoidance* and *risk mitigation.*

Risk avoidance is about preventing the risk from being actualized. E.g., not parking in a high crime area.

Risk mitigation is about limiting the damage should the risk be actualized. E.g., having a LoJack or cheap car stereo.

Note the risk in this case is that your car will be broken into.

Terms: Trust and Assurance

Trust is a generic term that implies a mechanism in place to provide a basis for confidence in the reliability/security of the system. Failure of the mechanism may destroy the basis for trust.

Trust mechanisms are the security features of a system that provide enforcement of a security policy.

The *trusted computing base* (TCB) is a collection of all the trust mechanisms of a computer system which collectively enforce the policy.

Assurance is a measure of confidence that the security features, practices, procedures, and architecture of a system accurately mediates and enforces the security policy.

Trust Management

The concept of *trust management* provides a unified approach to conceptualizing (parts of) IA. That is, a big part of IA is about controlling interactions among:

- actions
- principals
- policies
- credentials

Various policy management systems have been built with the goal of formalizing and describing these relationships: KeyNote (1999) and Extensible Access Control Markup Language (XACML) (2009).

These provide formal mechanisms for defining policy languages.

Why do you think that trust is a vital component of IA?

Lifecycle

A *lifecycle* is the process by which an asset is managed from its arrival or creation to its termination or destruction.

Software engineering defines several lifecycle models for the development or acquisition of computer software. in a *waterfall model*, the process is divided into stages performed sequentially:

- Requirements
- Design
- Coding
- Testing
- Deployment
- Production
- Decommission

Security Systems Lifecycle Management

Security systems lifecycle management is a process by which the project managers for a system will ensure that appropriate information assurance safeguards are incorporated into a system.

The stages leading to acquisition by the government of a secured system might be:

1. evaluation of sensitivity of the application based on risk analysis
2. determination of security specifications
3. design review and perform system tests to ensure safeguards are adequate, through testing and validation that the product meets specifications
4. system certification and accreditation, issuance of a certificate that the system meets the need and can be procured.

Assurance Requirements

Some indication of various types of lifecycle concerns appear in the Common Criteria "Assurance requirements", including:

Class APE, ASE: *System Evaluation*.

Class ACM: *Configuration Management*, includes CM automation, capabilities, and scope.

Class ADO: *Delivery and Operations*, includes delivery and installation, and generation and set-up.

Class ADV: *Development*, includes functional specification, low-level design, implementation representation, TSF internals, high-level design, representation correspondence, and security policy modeling.

Assurance Requirements (2)

Class AGC: *Guidance Documentation*, includes administrator guidance, and user guidance.

Class ALC: *Life Cycle*, includes development security, flaw remediation, tools and techniques, and life cycle definition.

Class ATE: *Tests*, includes test coverage, test depth, functional tests, and independent testing.

Class AVA: *Vulnerability Assessment*, includes covert channel analysis, misuses, strength of functions, and vulnerability analysis.

Class AMA: *Maintenance of Assurance*, includes assurance maintenance plan, component categorization, evidence of assurance maintenance, and security impact analysis.