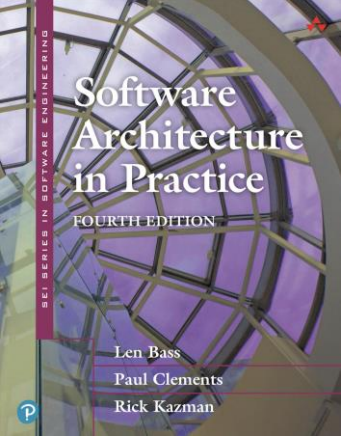
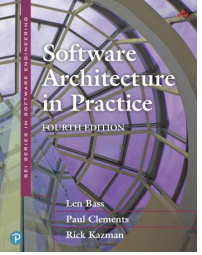


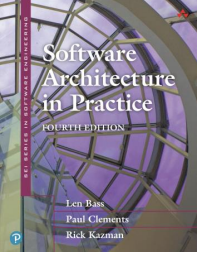
Chapter 11: Security

If you reveal your secrets to the wind, you should not blame the wind for revealing them to the trees.
—Kahlil Gibran



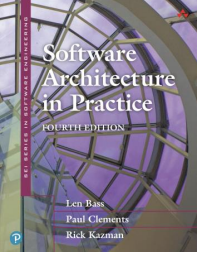
Chapter Outline

- What is Security?
- Security General Scenario
- Tactics for Security
- Tactics-Based Questionnaire for Security
- Patterns for Security
- Summary



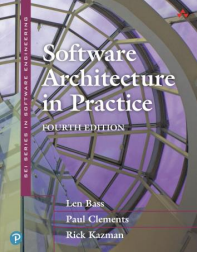
What is Security?

- Security is a measure of the system's ability to protect data and information from unauthorized access while still providing access to people and systems that are authorized.
- The simplest approach to characterizing security focuses on three characteristics: confidentiality, integrity, and availability (CIA):
  - *Confidentiality* is the property that data or services are protected from unauthorized access.
  - *Integrity* is the property that data or services are not subject to unauthorized manipulation.
  - *Availability* is the property that the system will be available for legitimate use.



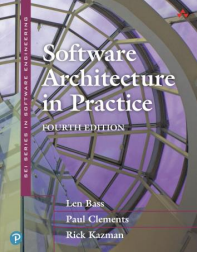
Security General Scenario

Portion of Scenario	Description	Possible Values
Source	The attack may be from outside the organization or from inside the organization. The source of the attack may be either a human or another system. It may have been previously identified (either correctly or incorrectly) or may be currently unknown.	▪ Human ▪ Another system which is: ▪ Inside the organization ▪ Outside the organization ▪ Previously identified ▪ Unknown
Stimulus	The stimulus is an attack.	An unauthorized attempt to: ▪ Display data ▪ Capture data ▪ Change or delete data ▪ Access system services ▪ Change the system's behavior ▪ Reduce availability
Artifact	What is the target of the attack?	▪ System services ▪ Data within the system ▪ A component or resources of the system ▪ Data produced or consumed by the system



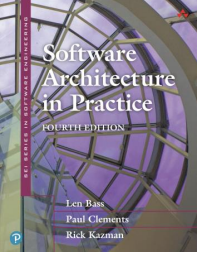
Security General Scenario

Environment	What is the state of the system when the attack occurs?	The system is: ▪ Online or offline ▪ Connected to or disconnected from a network ▪ Behind a firewall or open to a network ▪ Fully operational ▪ Partially operational ▪ Not operational
Response	The system ensures that confidentiality, integrity, and availability are maintained.	Transactions are carried out in a fashion such that ▪ Data or services are protected from unauthorized access ▪ Data or services are not being manipulated without authorization ▪ Parties to a transaction are identified with assurance ▪ The parties to the transaction cannot repudiate their involvements ▪ The data, resources, and system services will be available for legitimate use The system tracks activities within it by ▪ Recording access or modification ▪ Recording attempts to access data, resources, or services ▪ Notifying appropriate entities (people or systems) when an apparent attack is occurring
Response measure	Measures of a system's response are related to the frequency of successful attacks, the time and cost to resist and repair attacks, and the consequential damage of those attacks.	One or more of the following: ▪ How much of a resource is compromised or ensured ▪ Accuracy of attack detection ▪ How much time passed before an attack was detected ▪ How many attacks were resisted ▪ How long it takes to recover from a successful attack ▪ How much data is vulnerable to a particular attack

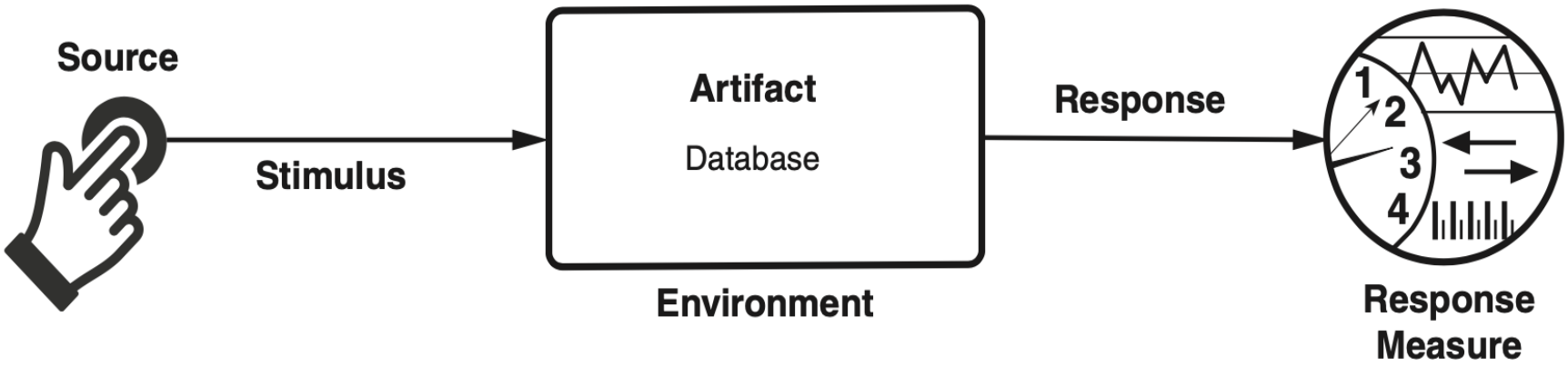


Sample Concrete Security Scenario

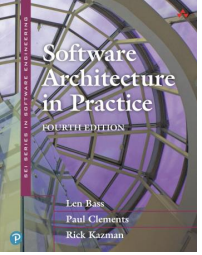
- *A disgruntled employee at a remote location attempts to improperly modify the pay rate table during normal operations. The unauthorized access is detected, the system maintains an audit trail, and the correct data is restored within one day.*



Sample Concrete Security Scenario

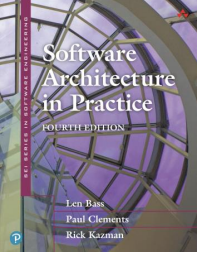


A disgruntled employee at a remote location	Attempts to improperly modify the pay rate table	Normal operations	The unauthorized access is detected and the system maintains an audit trail	Correct data is restored within one day

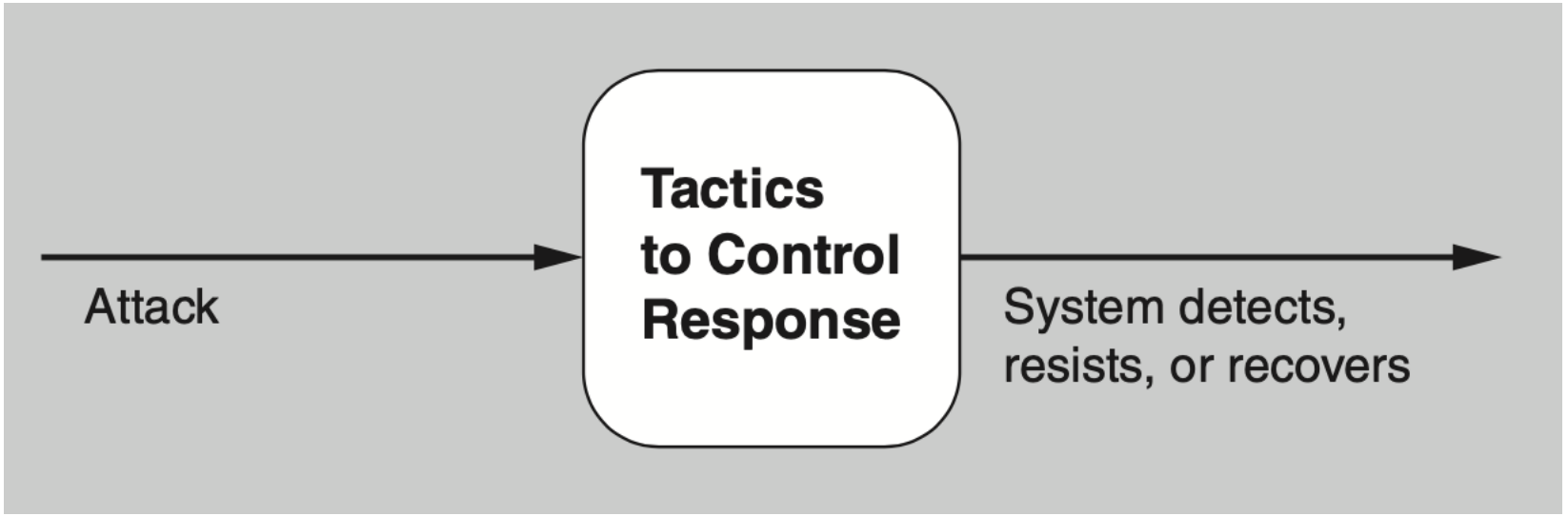


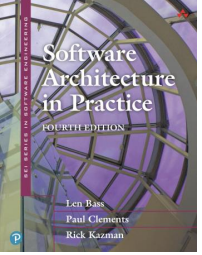
Goal of Security Tactics

- Secure facilities in the real world permit only limited access to them (e.g., fences and security checkpoints), have means of detecting intruders (e.g., requiring visitors to wear badges), have deterrence mechanisms (e.g., armed guards), have reaction mechanisms (e.g., automatic locking of doors), and have recovery mechanisms (e.g., off-site backup).
- These lead to our four categories of tactics: detect, resist, react, and recover.

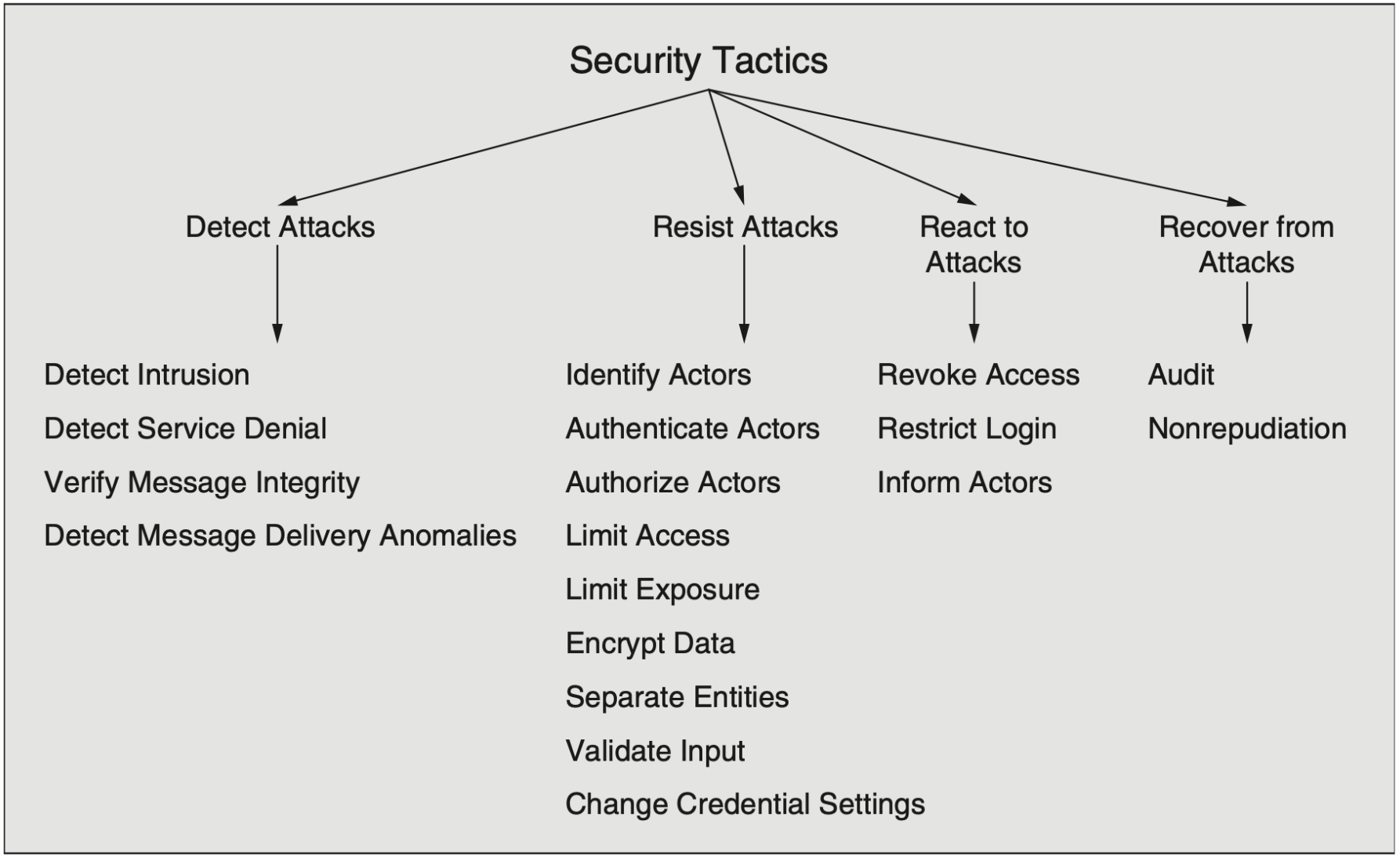


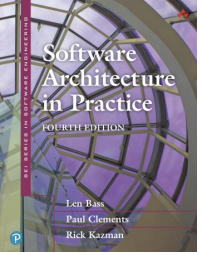
Goal of Security Tactics





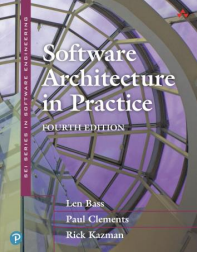
Security Tactics





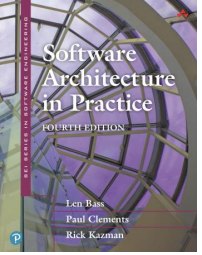
Detect Attacks

- *Detect intrusion.* This tactic compares network traffic or service request patterns within a system to a set of signatures or known patterns of malicious behavior stored in a database.
- *Detect service denial.* This tactic compares the pattern or signature of network traffic coming into a system to historical profiles of known denial-of-service (DoS) attacks.



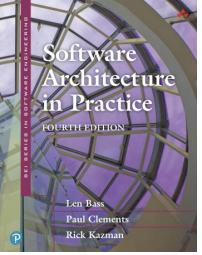
Detect Attacks

- *Verify message integrity.* This tactic employs techniques such as checksums or hash values to verify the integrity of messages, resource files, deployment files, and configuration files.
- *Detect message delivery anomalies.* This tactic seeks to detect man-in-the-middle attacks. If message delivery times are normally stable, then by checking the time that it takes to deliver or receive a message, it becomes possible to detect suspicious timing behavior. Similarly, abnormal numbers of connections and disconnections may indicate such an attack.



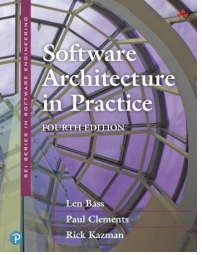
Resist Attacks

- *Identify actors*. Identifying actors (users or remote computers) focuses on identifying the source of any external input to the system. Users are typically identified through user IDs. Other systems may be "identified" through access codes, IP addresses, protocols, ports, or some other means.
- *Authenticate actors*. Authentication means ensuring that an actor is actually who or what it purports to be. Passwords, one-time passwords, digital certificates, two-factor authentication, and biometric identification provide means for authentication.
- *Authorize actors*. Authorization means ensuring that an authenticated actor has the rights to access and modify either data or services. This mechanism is usually enabled by providing some access control mechanisms within a system.



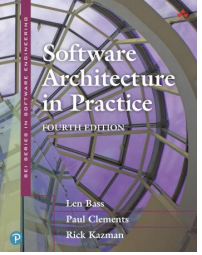
Resist Attacks

- *Limit access*. This tactic involves limiting access to computer resources. Limiting access might mean restricting the number of access points to resources, or restricting the type of traffic that can go through the access points. Both kinds of limits minimize the attack surface of a system.
- *Limit exposure.* This tactic focuses on minimizing the effects of damage caused by a hostile action. It is a passive defense since it does not proactively prevent attackers from doing harm. Limiting exposure is typically realized by reducing the amount of data or services that can be accessed through a single access point, and hence compromised in a single attack.
- *Encrypt data*. Confidentiality is usually achieved by applying some form of encryption to data and to communication. Encryption provides extra protection to persistently maintained data beyond that available from authorization.



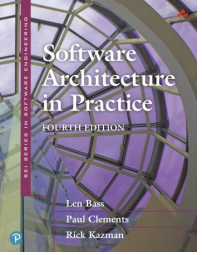
Resist Attacks

- *Separate entities*. Separating different entities limits the scope of an attack. Separation within the system can be done through physical separation on different servers attached to different networks, the use of virtual machines, or an “air gap”—that is, by having no electronic connection between different portions of a system.
- *Validate input*. Cleaning and checking input as it is received by a system, or portion of a system, is an important early line of defense in resisting attacks. This is often implemented by using a security framework or validation class to perform actions such as filtering, canonicalization, and sanitization of input.
- *Change credential settings*. Many systems have default security settings assigned when the system is delivered. Forcing the user to change those settings will prevent attackers from gaining access to the system through settings that may be publicly available.



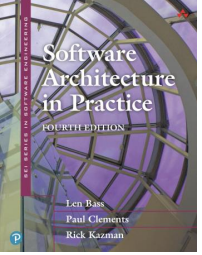
React to Attacks

- *Revoke access.* If the system or an administrator believes that an attack is under way, then access can be limited to sensitive resources, even for normally legitimate users and uses.
- *Restrict login*. Repeated failed login attempts may indicate a potential attack. Many systems limit access from a particular computer if there are repeated failed attempts to access an account from that computer.
- *Inform actors*. Ongoing attacks may require action by operators, other personnel, or cooperating systems. Such personnel or systems—the set of relevant actors—must be notified when the system has detected an attack.



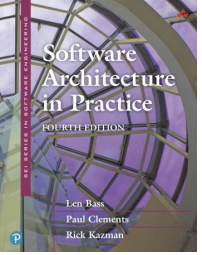
Recover from Attacks

- *Audit.* We audit systems—that is, keep a record of user and system actions and their effects—to help trace the actions of, and to identify, an attacker. We may analyze audit trails to attempt to prosecute attackers or to create better defenses in the future.
- *Nonrepudiation.* This tactic guarantees that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.
- In addition, all of the Availability tactics (chapter 4) aid in recovering from attacks.



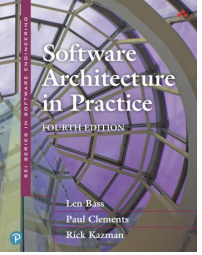
Tactics-Based Questionnaire for Security

Tactics Group	Tactics Question	Supported? (Y/N)	Risk	Design Decisions and Location	Rationale and Assumptions
Detecting Attacks	Does the system support the **detection of intrusions** by, for example, comparing network traffic or service request patterns within a system to a set of signatures or known patterns of malicious behavior stored in a database?				
	Does the system support the **detection of denial-of-service attacks** by, for example, comparing the pattern or signature of network traffic coming into a system to historical profiles of known DoS attacks?				
	Does the system support the **verification of message integrity** via techniques such as checksums or hash values?				
	Does the system support the **detection of message delays** by, for example, checking the time that it takes to deliver a message?				



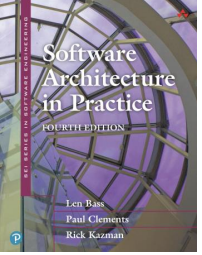
Tactics-Based Questionnaire for Security

Resisting Attacks	Does the system support the **identification of actors** through user IDs, access codes, IP addresses, protocols, ports, etc.?
	Does the system support the **authentication of actors** via, for example, passwords, digital certificates, two-factor authentication, or biometrics?
	Does the system support the **authorization of actors**, ensuring that an authenticated actor has the rights to access and modify either data or services?
	Does the system support **limiting access** to computer resources via restricting the number of access points to the resources, or restricting the type of traffic that can go through the access points?
	Does the system support **limiting exposure** by reducing the amount of data or services that can be accessed through a single access point?



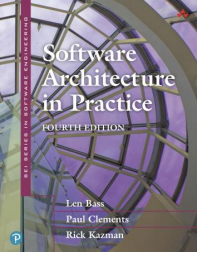
Tactics-Based Questionnaire for Security

Resisting Attacks	Does the system support **data encryption**, for data in transit or data at rest?
	Does the system design consider the **separation of entities** via physical separation on different servers attached to different networks, virtual machines, or an "air gap"?
	Does the system support **changing credential settings**, forcing the user to change those settings periodically or at critical events?
	Does the system **validate input** in a consistent, system-wide way—for example, using a security framework or validation class to perform actions such as filtering, canonicalization, and sanitization of external input?



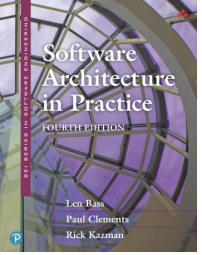
Tactics-Based Questionnaire for Security

Reacting to Attacks	Does the system support **revoking access** by limiting access to sensitive resources, even for normally legitimate users and uses if an attack is under way?
	Does the system support **restricting login** in instances such as multiple failed login attempts?
	Does the system support **informing actors** such as operators, other personnel, or cooperating systems when the system has detected an attack?
Recovering from Attacks	Does the system support maintaining an **audit** trail to help trace the actions of, and to identify, an attacker?
	Does the system guarantee the property of **nonrepudiation**, which guarantees that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message?
	Have you checked the “recover from faults” category of tactics from Chapter 4?



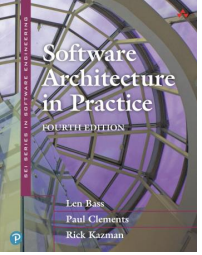
Intercepting Validator Pattern for Security

- This pattern inserts a software element—a wrapper—between the source and the destination of messages.
- This approach assumes greater importance when the source of the messages is outside the system.
- The most common responsibility of this pattern is to implement the verify message integrity tactic, but it can also incorporate tactics such as detect intrusion and detect service denial, or detect message delivery anomalies.



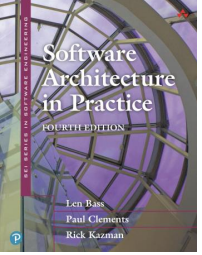
Intercepting Validator Pattern Benefits

- Benefits:
  - Depending on the specific validator that you create and deploy, this pattern can cover most of the waterfront of the “detect attack” category of tactics, all in one package.



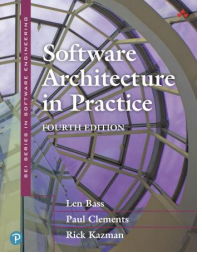
Intercepting Validator Pattern Tradeoffs

- Tradeoffs:
  - As always, introducing an intermediary exacts a performance price.
  - Intrusion patterns change and evolve over time, so this component must be kept up-to-date so that it maintains its effectiveness. This imposes a maintenance obligation on the organization responsible for the system.



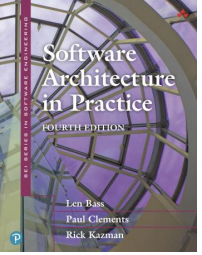
Intrusion Prevention System Pattern

- An intrusion prevention system (IPS) is a standalone element whose main purpose is to identify and analyze any suspicious activity.
- If the activity is deemed acceptable, it is allowed. Conversely, if it is suspicious, the activity is prevented and reported.



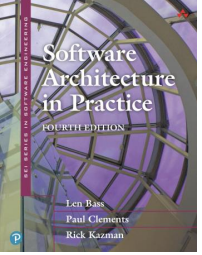
Intrusion Prevention System Pattern Benefits

- These systems often encompass most of the "detect attacks" and "react to attacks" tactics.



Intrusion Prevention System Pattern Tradeoffs

- The patterns of activity that an IPS looks for change and evolve over time, so the patterns database must be constantly updated.
- Systems employing an IPS incur a performance cost.
- IPSs are available as commercial off-the-shelf components, which makes them unnecessary to develop but perhaps not entirely suited to a specific application.



Summary

- Attacks against a system can be characterized as attacks against the confidentiality, integrity, or availability of a system or its data.
- This leads to many of the tactics used to achieve security. Identifying, authenticating, and authorizing actors are tactics intended to determine which users or systems are entitled to what kind of access to a system.
- No security tactic is foolproof and systems *will* be compromised. Hence, tactics exist to detect an attack, limit the spread of any attack, and to react and recover from an attack.