11.4 Intrusion Detection Requirements

An intrusion detection system (IDS) must satisfy a set of requirements for both the service and the quality of service. IDS is a security service that automates the monitoring of events occurring in a computer system or network, and analyzes these events for any indication of security violations. While each situation that calls for intrusion detection is unique, there are common generic requirements that apply to all intrusion detection situations. This pattern provides a common generic set of intrusion detection requirements. The pattern also helps you to apply the general requirements to your specific situation, and helps you to determine the relative importance of conflicting requirements.

Example

The museum's research department has a network that they use for messaging and collaboration with various universities around the world. Among the information exchanged and stored are details about the location of various natural gemstone mines. Samuel the museum system engineer wants the museum immediately to detect unauthorized and successful attempts to gain access to the network and to any hosts that contain sensitive information. Once alerted, Samuel would like information that can be used to hold accountable the individual(s) that have breached their perimeter. In addition, Samuel would like to have information recorded and available on unsuccessful attempts to gain access. Samuel understands that trade-offs are involved, because stopping intruders and capturing information about attempted intrusions can require significant resources that degrade system performance, and which may make legitimate access more difficult. Privacy considerations are also a constraint on intrusion detection efforts. Samuel needs to identify requirements for an IDS service that will help the museum achieve the goals while balancing the constraints.

Context

Accounting requirements and their relative importance are understood. The requirements might have been selected by applying SECURITY ACCOUNTING REQUIREMENTS (360). The planned uses of IDS are understood.

Problem

IDS is a security service that automates the monitoring of events occurring in a computer system or network. It analyzes these events for any indication of security violations. You need a clear set of requirements to ensure that the intrusion detection strategy employed actually satisfies the needs of the organization or system. Requirements for intrusion detection often conflict with each other, and trade-offs among them are often necessary. The conflict stated in the example is that the need to detect intrusion must be balanced with resource and privacy constraints.

What types of information are appropriate or required for an IDS to analyze? How can you determine a balanced set of specific requirements for an IDS service, and their relative importance?

The process of selecting and prioritizing intrusion detection requirements needs to balance the following forces:

- Applying intrusion detection increases the likelihood of achieving the desired security properties, especially accountability and integrity.
- Applying intrusion detection has associated costs, such as software, additional processing time and resources, and risks, such as privacy violations.
- Intrusion detection errors can result in two different types of problems. First, if an intrusion occurs that violates security, and the IDS service does not detect it or prevent it, then damage can occur, and it might not be discovered until a later time. Second, if no intrusion occurs but the IDS incorrectly believes an intrusion has occurred, then resources are wasted trying to respond to a problem that does not exist.

Solution

Specify a set of intrusion detection requirements for a specific domain such as a system or network, and determine the relative importance of each requirement. The solution has two aspects: a requirements process and a common set of generic requirements.

Requirements Specification and Prioritization Process

The requirements process is typically performed by a system requirements engineer in conjunction with an enterprise architect, and includes several activities. An important first step is explicitly to define the domain for which IDS requirements are to be specified, such as a specific system or facility. Factors that affect specialization and importance of requirements are also defined, such as organization constraints. IDS requirements for the target domain are then specified, using the generic requirements provided below. The final activity is to define the relative importance of the specified requirements.

Generic Requirements Description

The following are general requirements that drive the design of an IDS Service:

- Detect intrusion events.

  An IDS service must detect intrusion attempts. This information is used to determine organization vulnerabilities. By its very need to provide immediate information, IDS services will only be able to provide information about security events as it is received. While some IDS services can provide a degree of correlation between events, there is an inherent time delay before such information can be reported.

- Report on successful intrusions and thwarted intrusion events.

  Reported information includes actor identities and any distinguishing characteristics of the events. The information should also include, but not be limited to: the location of the actor, software or hardware used in the attack, discussion of whether or not any elements of the attack were detected in advance, and the responses that ensued.

- Provide countermeasures against intrusions.

  An IDS service has the responsibility to try to thwart intrusion attempts. An IDS service will need to perform some event correlation so that it will be able to recognize attack patterns and warn security officers and system administrators. Compiling user profiles based on behavior patterns can also help to recognize and thwart attacks. If reasonable, the IDS service should be permitted to shut down avenues of access when attack patterns indicate that an attack is beginning to happen. In some cases, the known presence of an IDS may in itself deter actors from engaging in malicious activity.

- Support the capability for repeated examination of information derived from an event.

  The IDS service needs to provide the security events and information it detects to the normal audit trail and logging mechanisms for capture and storage for the longer term.

- Perform its service when needed.

  The IDS service will itself require protection. An IDS needs to be available to provide its services when the tracking of events is absolutely important. During operation the IDS should be aware of events that could cause significant damage to the organization, and the IDS service needs to be able to continue functioning during those high-impact events.

- Provide reliable and accurate information.

  Malicious actors should not be able to tamper with information the IDS service obtains or generates: the IDS should protect its own information as far as possible. Decision makers will need to judge how well the IDS information is protected from malicious actors. This requirement is essential to support confidentiality and integrity.

An additional set of requirements applies to all service requirements patterns. Instead of duplicating the discussion of the same set in each requirements pattern, they are simply listed here, because they do need to be considered in each requirements pattern. The requirements are: minimize time and effort to use, minimize mismatch with user characteristics, risks to user safety, costs of per-user set-up, costs of maintenance, management, and overhead, and changes needed to existing system infrastructure. Further discussion of each of these cross-cutting requirements, including implementation factors, is given in I&A REQUIREMENTS (192).

Implementation

This section first provides more detail on the process that was summarized in the Solution section, then discusses factors in determining relative importance of requirements.

Process Guidelines

The requirements process is typically performed by a system requirements engineer in conjunction with an enterprise architect, and includes several steps:

1. Establish the domain for which the intrusion detection service is needed.

   Ensure that the domain has been identified and scoped. Typical intrusion detection domains include [ISG00]:

   - Trespass: gaining unauthorized physical access to sensitive data by circumventing a system's protections
   - Penetration: gaining unauthorized logical access to sensitive data by circumventing a system's protections
   - Reverse engineering: acquiring sensitive data by disassembling and analyzing the design of a system component
   - Cryptanalysis: transforming encrypted data into plaintext without having prior knowledge of encryption parameters or processes

   Other constraints may also bound the domain.
2. Specify a set of factors that affect specialization and importance of requirements.

   The factors include use of IDS, intrusion detection needs, response needs, organization constraints, and priorities. You can find a general candidate set of factors below.
3. Specify the intrusion detection requirements for the target domain.

To do this, specialize the set of generic requirements given in the Solution section.

4. Define the relative importance of specific requirements.

   You can find more details on the association of factors and requirements below.

Factors in Determining Relative Importance

Table 11.7 reiterates the generic requirements described in the Solution section, along with factors for judging their relative importance to the organization. For each requirement, positive and negative impacts of the factors on importance or priority of the requirement are also provided.

Table 11.7 Intrusion detection system service requirements factors

GENERIC REQUIREMENT	FACTOR	RESULTING PRIORITY
Detect intrusion events	Potential intrusions could give access to highly-sensitive or valuable assets, or could cause significant damage.	High
	Intrusions would not cause significant loss or damage, or the loss is covered by insurance.	Low
Report on successful intrusions and thwarted intrusion events	Strong need to assess quality of IDS and patterns of intrusion attempts.	High
	Information needed only for insurance claims.	Medium
Provide countermeasures against intrusions	Potential intrusions could cause loss of or damage to highly-valuable assets that could not be replaced or repaired.	High
	Assets could easily be replaced or repaired.	Low
Support the capability for repeated examination of information derived from an event	IDS is the only accounting service deployed, and understanding of patterns that emerge over time is needed.	High
	An audit trail and logging service is deployed, or the primary need for IDS is to detect and thwart current attacks.	Low
Perform its service when needed	Potential intrusions could give access to highly-sensitive or valuable assets, or could cause significant damage.	High

Table 11.7 Intrusion detection system service requirements factors (*continued*)

GENERIC REQUIREMENT	FACTOR	RESULTING PRIORITY
	Intrusions would not cause significant loss or damage, or the loss is covered by insurance.	Low
Provide reliable and accurate information	Strong need to assess quality of IDS and patterns of intrusion attempts.	High
	Information needed only for insurance claims.	Medium

Example Resolved

Samuel the museum systems engineer defines the museum research network as an IDS domain. Table 11.8 shows the requirements ratings Samuel has specified for this domain.

Table 11.8 Resolution of example problem for IDS requirements

REQUIREMENT	MUSEUM PRIORITY AND CONCERN
Detect intrusion events	HIGH – The museum wants immediately to detect unauthorized and successful attempts to gain access to the network and to any hosts that contain sensitive information.
Report on successful intrusions and thwarted intrusion events	HIGH – Once alerted, the decision makers would like information that can be used to hold the individual(s) that have breached their perimeter accountable.
Provide countermeasures against intrusions	MEDIUM – The museum wants to thwart intrusions, but for this domain, the benefit-to-cost ratio for this capability is less than detection and reporting.
Support the capability for repeated examination of information derived from an event	LOW – The museum is most interested in current attacks rather than long-term analysis.
Perform its service when needed	HIGH – The problem statement clearly states that the museum needs the IDS to capture malicious activity. The museum must have confidence that the IDS can perform this task
Provide reliable and accurate information	MEDIUM – Information on malicious actors is important, but protecting other tracking information is only moderately important.

Known Uses

The general IDS requirements and the process of specifying IDS requirements described in this pattern are widely known, but are generally used informally, as opposed to being codified or published. The requirements as stated here represent a consolidation of MITRE Corporation's experience in working with multiple customers over several decades. However, some publications on intrusion detection and IDS requirements exist. Examples are:

- [ISO13335-4] discusses intrusion detection as one of the primary safeguards.
- [ISO15408] is an international standard that defines evaluation criteria for information technology security. It includes criteria that address IDS requirements, although the discussion is tangential and in the context of audit and system monitoring activities.
- [IDWG02] discusses requirements for IDS message exchange in the context of the Internet.
- [Farshchi03] discusses requirements for wireless IDS.
- [Liesen02] discusses criteria for organization-wide IDS products.

Consequences

The following benefits may be expected from applying this pattern:

- It facilitates conscious selection of IDS requirements, so that decisions about selecting IDS mechanisms have a clear basis, rather than occurring in a vacuum.
- It promotes explicit analysis of trade-offs that encourages balancing and prioritizing of conflicting requirements and forces. This includes balancing the need for accountability with the need for privacy. This helps to avoid stronger than necessary IDS mechanisms that would generate excessive false warnings or cost too much, and at the same time it helps to avoid a weaker than necessary IDS that makes it easy for malicious actors to penetrate.
- It results in documentation of IDS requirements that communicates to all interested parties, and is useful in determining the adequacy of accounting services such as IDS.
- The explicit requirements resulting from the pattern foster a clear connection of requirements to audit and intrusion policies: this also encourages organizations to make their accounting policies more explicit.

The following potential liabilities may arise from applying this pattern:

- It requires an investment of resources to apply the pattern, including time to analyze domains and IDS needs. In some cases the cost of applying the pattern may exceed its benefits.

- It poses a danger of possibly violating privacy rights if extensive actor data is captured and analyzed. You can mitigate this by capturing and analyzing the minimum amount of data, and by working closely with your legal department.
- The formal selection process may be too long and costly and produce too much overhead. You can mitigate this in the same ways as noted above.
- Specific circumstances might not be covered by generic IDS requirements. You can mitigate this by adding specific requirements and including them in the trade-offs.
- Documentation of requirements implies that they must be maintained as they change over time. You can mitigate this by keeping the requirements in a form that is easy to update, integrated with other system documentation.
- Perception of IDS requirements can differ throughout an organization or in a particular domain. This may make it difficult to reach agreement on the relative priorities of requirements. On the other hand, bringing such disagreements to the surface may be a benefit of the pattern, because then they can be properly discussed and resolved.

See Also

AUDIT TRAILS AND LOGGING REQUIREMENTS (378) describes requirements for capturing and storing information that could be passed from an intrusion detection system.