Defense in Depth

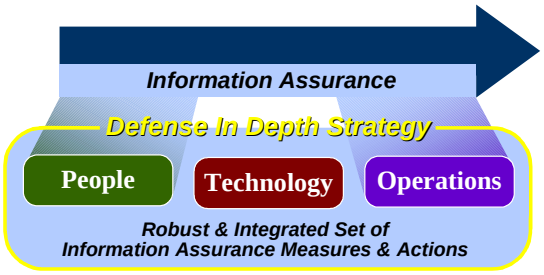
A practical strategy for achieving Information Assurance in today's highly networked environments.

Introduction. Defense in Depth is practical strategy for achieving Information Assurance in today's highly networked environments. It is a "best practices" strategy in that it relies on the intelligent application of techniques and technologies that exist today. The strategy recommends a balance between the protection capability and cost, performance, and operational considerations. This paper provides an overview of the major elements of the strategy and provides links to resources that provide additional insight.

Adversaries, Motivations, Classes of Attack. To effectively resist attacks against its information and information systems, an organization needs to characterize its adversaries, their potential motivations, and their classes of attack. Potential adversaries might include: Nation States, Terrorists, Criminal Elements, Hackers, or Corporate Competitors. Their motivations may include: intelligence gathering, theft of intellectual property, denial of service, embarrassment, or just pride in exploiting a notable target. Their classes of attack may include: passive monitoring of communications, active network attacks, close-in attacks, exploitation of insiders, and attacks through the industry providers of one's Information Technology resources.

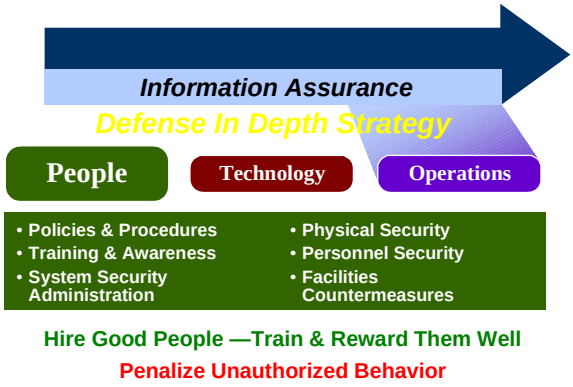
It's also important to resist detrimental effects from non-malicious events such as fire, flood, power outages and user error.

Information Assurance. Information Assurance is achieved when information and information systems are protected against such attacks through the application of security services such as: Availability, Integrity, Authentication, Confidentiality, and Non-Repudiation. The application of these services should be based on the Protect, Detect, and React paradigm. This means that in addition to incorporating protection mechanisms, organizations need to expect attacks and include attack detection tools and procedures that allow them to react to and recover from these attacks.



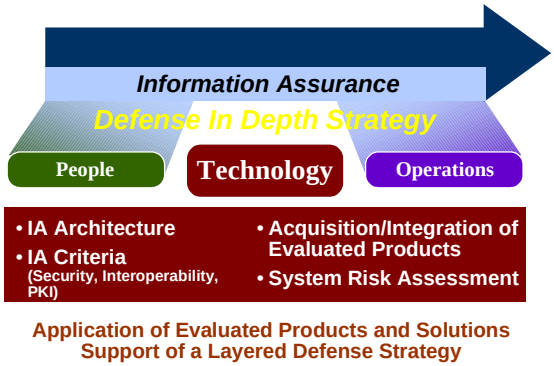
An important principle of the Defense in Depth strategy is that achieving Information Assurance requires a balanced focus on three primary elements: People, Technology and Operations.

People. Achieving Information Assurance begins with a senior level management commitment (typically at the Chief Information Officer level) based on a clear understanding of the perceived threat. This must be followed through with effective Information Assurance policies and procedures,



assignment of roles and responsibilities, commitment of resources, training of critical personnel (e.g. users and system administrators), and personal accountability. This includes the establishment of physical security and personnel security measures to control and monitor access to facilities and critical elements of the Information Technology environment.

Technology. Today, a wide range of technologies are available for providing Information Assurance services and for detecting intrusions. To insure that the right technologies are procured and deployed, an organization should establish effective policy and processes



for technology acquisition. These should include: security policy, Information Assurance principles, system level Information Assurance architectures and standards, criteria for needed Information Assurance products, acquisition of products that have been validated by a reputable third party, configuration guidance, and processes for assessing the risk of the integrated systems. The Defense in Depth strategy recommends several Information Assurance principles. These include:

a) Defense in Multiple Places. Given that adversaries can attack a target from multiple points using either insiders or outsiders, an organization needs to deploy protection mechanisms at multiple locations to resist all classes of attacks. As a minimum, these defensive "focus areas" should include:

- Defend the Networks and Infrastructure
  - Protect the local and wide area communications networks (e.g. from Denial of Service Attacks)
  - Provide confidentiality and integrity protection for data transmitted over these networks (e.g. use encryption and traffic flow security measures to resist passive monitoring)
- Defend the Enclave Boundaries (e.g. deploy Firewalls and Intrusion Detection to resist active network attacks)

- Defend the Computing Environment (e.g. provide access controls on hosts and servers to resist insider, close-in, and distribution attacks).

b) Layered Defenses. Even the best available Information Assurance products have inherent weaknesses. So, it is only a matter of time before an adversary will find an exploitable vulnerability. An effective countermeasure is to deploy multiple defense mechanisms between the adversary and his target. Each of these mechanisms must present unique obstacles to the adversary. Further, each should include both "protection" and "detection" measures. These help to increase risk (of detection) for the adversary while reducing his chances of success or making successful penetrations unaffordable. Deploying nested Firewalls (each coupled with Intrusion Detection) at outer and inner network boundaries is an example of a layered defense. The inner Firewalls may support more granular access control and data filtering.

Examples of Layered Defenses

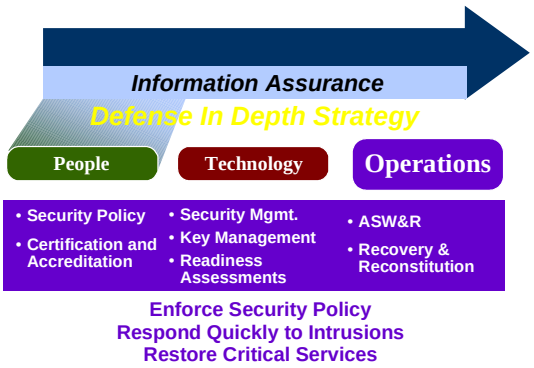
Class of Attack	*First Line of Defense*	*Second Line of Defense*
Passive	Link & Network Layer Encryption and Traffic Flow Security	Security Enabled Applications
Active	Defend the Enclave Boundaries	Defend the Computing Environment
Insider	Physical and Personnel Security	Authenticated Access Controls, Audit
Close-In	Physical and Personnel Security	Technical Surveillance Countermeasures
Distribution	Trusted Software Development and Distribution	Run Time Integrity Controls

c) Specify the security robustness (strength and assurance) of each Information Assurance component as a function of the value of what's it is protecting and the threat at the point of application. For example, it's often more effective and operationally suitable to deploy stronger mechanisms at the network boundaries than at the user desktop.

d) Deploy robust key management and public key infrastructures that support all of the incorporated Information Assurance technologies and that are highly resistant to attack. This latter point recognizes that these infrastructures are lucrative targets.

e) Deploy infrastructures to detect intrusions and to analyze and correlate the results and react accordingly. These infrastructures should help the "Operations" staff to answer questions such as: Am I under attack? Who is the source? What is the target? Who else is under attack? What are my options?

Operations. The operations leg focuses on all the activities required to sustain an organization's security posture on a day to day basis.



These include:

a) Maintaining visible and up to date system security policy

b) Certifying and accrediting changes to the Information Technology baseline. The C&A processes should provide the data to support "Risk Management" based decisions. These processes should also acknowledge that a "risk accepted by one is a risk shared by many" in an interconnected environment.

c) Managing the security posture of the Information Assurance technology (e.g. installing security patches and virus updates, maintaining access control lists)

d) Providing key management services and protecting this lucrative infrastructure

e) Performing system security assessments (e.g. vulnerability scanners, RED teams) to assess the continued "Security Readiness"

f) Monitoring and reacting to current threats

g) Attack sensing, warning, and response

h) Recovery and reconstitution

Additional Resources. The National Security Agency, with support from other U.S. Government Agencies and U.S. Industry, has undertaken a number of initiatives to support the Defense in Depth strategy. These include:

a) The Information Assurance Technical Framework. This document provides detailed Information Assurance guidance for each of the Defense in Depth focus areas. It is available at http://www.iatf.net

b) The National Information Assurance Partnership (NIAP). This is a partnership between NSA and NIST to foster the development of the International Common Criteria (an ISO standard) and to accredit commercial laboratories to validate the security functions in vendor's products. Information on this activity is available at http://niap.nist.gov

c) Common Criteria Protection Profiles. These are documents that recommend security functions and assurance levels using the Common Criteria. They are available for a wide range of commercially available technologies and can be accessed at the IATF or the NIAP web sites listed above.

d) List of Evaluated Products. These are lists of commercial Information Assurance products that have been evaluated against the Common Criteria. The lists are maintained by NIST and are available at the NIAP web site.

e) Configuration Guidance. These documents, being prepared by NSA, contain recommended configurations for a variety of commonly used commercial products.

f) Glossary of Terms. The National Information Systems Security (INFOSEC) Glossary, dated September 2000, can be found at: http://www.nstissc.gov/Assets/pdf/4009.pdf

Feedback. Please address questions or comments on this paper by email to ***deluddy@missi.ncsc.mil*** or by mail to:

National Security Agency
Attention: Information Assurance Solutions Group – STE 6737
9800 Savage Road
Fort Meade, MD 20755-6737