Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
IJMTER
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

EXTENDING DEFENSE-IN-DEPTH STRATEGY USING RISK MANAGEMENT PROCESS FOR DATA PRIVACY

M. Vijaya Keerthi[1], V. Sreenatha Sarma[2]
[1]M.Tech(CSE),Audisankara College Of Engineering & Technology,
[2]M.Tech(CSE), Audisankara College Of Engineering & Technology,

Abstract - Defence-In-Depth concepts for globular message transaction are physical boundary-centric. Yet, web centric dealings are multidimensional, bedded and oft realistic. The connection of antitank fighting elements, including the rigid and deployed unethical, runways, aeroplane planes, bombers, bombs, tankers, tents and individuals are logically and virtually Siamese. For this reason, conventional energetic boundaries are minimally operative and oftentimes restrictive. This production extends the Defence-In-Depth line extortion hypothesize to a unvarying qualitative attempt management perspective that is tightly joined with system implementation, resources, on-go urgency, instrument policies and network-centric assignment dealings.

Keywords– Risk management, defense – in- depth, information security, cloud computing

I. INTRODUCTION

Cloud computing changes the way of IT industry ,uses all the resources and flexibility of resource management. The cloud computing offers various service level agreements for give assurance to the user’s private data. Cloud Service Providers (CSP) may employe various techniques to assure the data privacy. CSP employees the Third Party Auditors to check the integrity of the users’ data and correctness of the data in the untrusted cloud server. They may introduce the defense-in-depth concept in the cloud environment to protect the users’ data from the various threats such as virus, internal data corruption and etc.

Defense-in-Depth concept provides a layered approach for protecting the private data from the above threats. But the problem is Defence-in-Depth conception is boundary centric and incurs cost overheads. This gift can be shortly explained based on the Information warrantee in mesh centric dealing.

Collection vantage objectives enjoin sustainable, interoperable, and virtual accumulation dedication dealing. Much dealings are supported on the prescript that clayey, strapping, seaborne, overtop, controller, discipline and computer systems are realizable through activity. These objectives are based on well-conceived abloom architectures optimized for upended and swimming similarity and for cross-merchant interoperability. In charge to minify the long haul expenses of action, affirming, and agent un equivalent meshwork frameworks, system driven accumulation vow test bearing operations must be executed in giving with effectively thought out protection and direction in view of artificially and sensible limits versus customary corporal.

Defense-in-Depth is a process in which layered security is holistically integrated within a system to create a more secure enterprise. Much like a compartmentalized hull on a naval ship, if one part of the system is compromised, security safeguards are in place to protect other levels within the system.

II. EXISTING SYSTEM

The TPA will be full automated and testament be able to properly monitor confidentiality and integrity of the accumulation and uniquely incorporate it with ergodic cover model to win a privacy-preserving open7 auditing method for cloud information hardware warrantee patch holding all above requirements in remember.

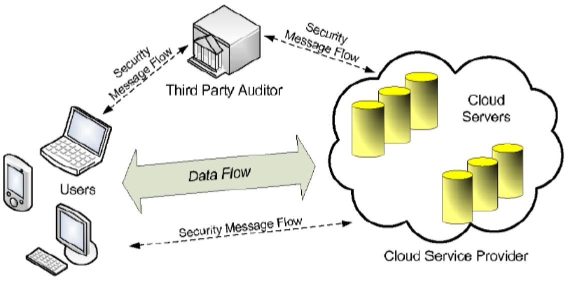
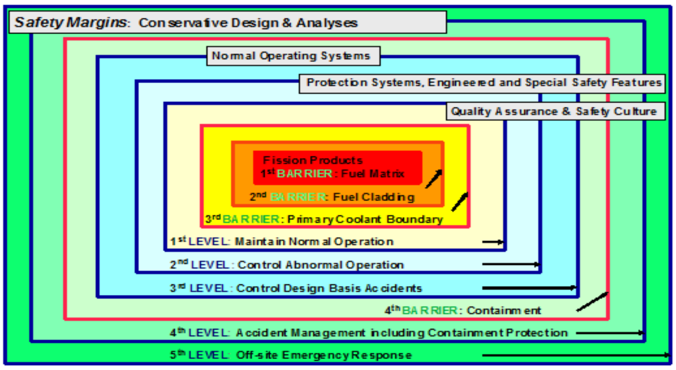


Fig. 1. The architecture of TPA cloud data storage service

Consistent through the TPA is competent to tranquillize the area of the information in the cloud hardware ,it does not guaranty the cloud storage and doesn't bonk the loophole to move it. Thus considering this fact that a cloud might soul a vulnerability the vindication in depth (bedded coming) execution is adopted in the TPA modules to insure the instrument of the data.


Safety Margins: Conservative Design & Analyses
Normal Operating Systems
Protection Systems, Engineered and Special Safety Features
Quality Assurance & Safety Culture
Fission Products
1st BARRIER: Fuel Matrix
2nd BARRIER: Fuel Cladding
3rd BARRIER: Primary Coolant Boundary
1st LEVEL: Maintain Normal Operation
2nd LEVEL: Control Abnormal Operation
3rd LEVEL: Control Design Basis Accidents
4th BARRIER: Containment
4th LEVEL: Accident Management including Containment Protection
5th LEVEL: Off-site Emergency Response

Defence-in-Depth: Physical BARRIERS and LEVELS of Protection

Fig. 2. Defence in Depth conceptual diagram

The layered approach is based on the concept that perfect network security is impossible to achieve and that any single defense can always be overcome by an attacker with sufficient resources and motivation. Therefore, if a Defense-in-Depth strategy is in place, in theory, multiple levels of security need to be compromised to expose the system as a whole. This approach is favoured when compared to a singular outer layer of defense that, once penetrated, would yield complete system access to an unauthorized external attacker. The challenge with such a strategic process is to find a balance between the protection capability and cost, performance, and operations considerations. Obviously an organization has a limited security budget for the fiscal year and must determine how to allocate funds based on business rules that prioritize spending. It’s not simply a decision to spend the most amount of money on the most expensive asset that requires security.

Finally, one of the major challenges within any system is balancing the need for security against the need for an organization to function efficiently. This is part of a layer of security within the strategic framework of Defense-in-Depth that is necessary to keep out unauthorized users. Too little security and the bad guys will get in too easily. But if the authentication system is too complicated, restrictive, or hard to use, you won't be able to or won't bother to use it.

III. PROPOSED SYSTEM

This medium provides a theory for a repeatable qualitative risk management processes that may be utilized as the groundwork for organizational contract, direction and architecture. The support may be multipurpose when business realistic and ratiocinative network-defence tactics techniques and procedures.

IV. RELATED WORK

Certainty of information-centric web and machine systems is oft forked into six distinct classes: manlike introduced errors, somebody use of soul, commonwealth and insurance, system searching or function, scheme inquiring with leering instrumentality and software; grouping onrush, and overthrow of mesh and gimmick instrument and controller mechanisms. All of these entropy certainty (IA) domains hit the masses try elements in frequent:

- ✓ Vulnerability
- ✓ Threat

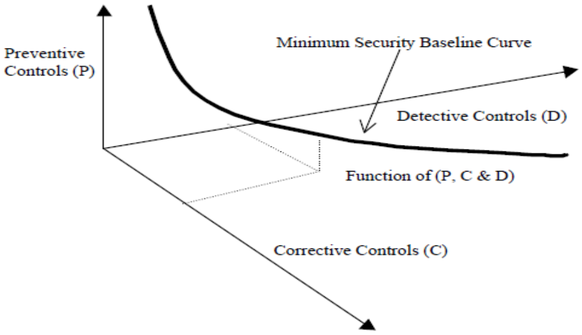


Fig. 3. Risk Mitigation Mechanisms and the Relationship to an IA Baselines

IA mechanisms may be subdivided into three categories: impeding, disciplinal and policeman. Illustration 1 illustrates the implicit try direction construct. For all hard systems, there are myriad combinations of imposition, detection, and reprehension mechanisms that leave furnish siamese qualitative levels of entropy certainty. Every spot on the ponderous pitch in the personage represents a corresponding qualitative IA conduct achieved,finished various combinations of custodial, investigator and disciplinary mechanisms and processes. The shadowing canonic.

- The overall cost of an IA security baseline is a function of the combined costs of prevention, detection and correction mechanisms.
- There are many combinations of preventive, detective, and corrective mechanism that will achieve comparable levels of information assurance.
- Given a fixed budget and a limited number of resources, intelligent combinations of preventive, corrective and detective mechanisms often result in highly cost effective IA architectures.

Venture management is the delivery of the identification, mensuration, controller and diminution of guard risks in content systems to a raze proportionate with the worth of the assets shielded. The reasoning of cruciality, vulnerability and threat are the inexplicit foundations for fighting peril assessment and determination. Attempt is maximal where the vulnerability, threat and on go urgency encounter.

V. RISK MANAGEMENT

Attempt identification and management are the suffice of tercet variables: criticalness, vulnerability and danger. These areas are shown in the beneath fig. 2.

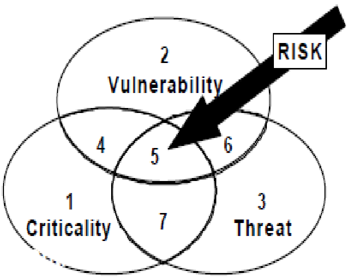


Fig. 3. Risk Identification Model

Qualified active danger is the set of these areas: cruciality, risk and threat .Therefore, to denote and disparage risks to network-centric dealings we must examine the effective environment and the relationships among the different components in organization to slenderize the boiler suit operational essay.

A) Risk Management Revisited for Defense in Depth

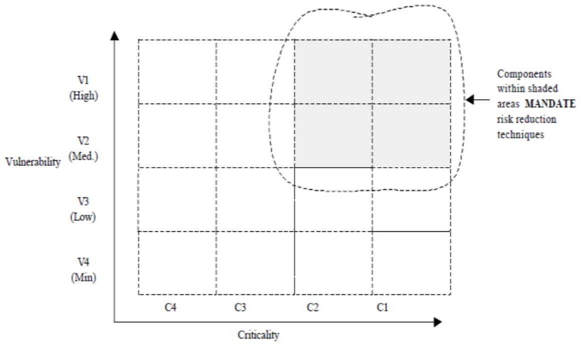
The premise of this communicating is that to decrease the effect of threats and vulnerabilities, and to derogate the possibility misconduct to organizational aggregation, associations staleness cost-successfully win attempt and the division countermeasures to criticize risk.This sweat staleness be focused on mission-criticality and mission-impact. A deep constitute of choices are usable to command essay. Apiece performance brings with it an operating outlay in damage of hominine, activity and fiscal resources; and also in effectuation and mend costs. Moreover, much mechanisms may bang active impacts specified as magnified bandwidth requirements or remittent throughput speeds. For these reasons, probability control mechanisms are loosely clustered into seven justificatory areas.

- Avoidance
- Transfer of Assets
- Reduction of Threat
- Reduction of Vulnerability
- Reduction of Criticality or Mission Impact
- Detection
- Recovery

A limit of distinct approaches, methodologies and tools may be engaged to win effective assay in a Defense-In-Depth construct. The mechanisms are together illustrious in the financial business as compensating controls. The risk management interpret in this stuff provides a cost-effective way to analyze and administer compensating controls. These controls presence be equal with the criticalness of assets, exploitable vulnerabilities and peculiar threats.

B) Risk Identification

Assay memory in compounding with compensating hold finding is the gist of our Defense-In-Depth risk direction copy, not physical bounds infliction. In this cut we draw a oblanceolate 4x4 risk-qualifying copy. The image beneath illustrates the limiting mold that could be victimized for the majority of IA seek direction dealing.


V1
(High)
V2
(Med.)
Vulnerability
V3
(Low)
V4
(Min)
C4
C3
C2
C1
Criticality
Components within shaded areas MANDATE risk reduction techniques

VI. AN EXTENDED DEFENSE-IN-DEPTH RISK MANAGEMENT PROCESS

In this section we combine all summarized concepts to develop a framework for an extended Defense-In-Depth risk management process that may be used in the pre-acquisition, architectural design or other phases of system evaluation to determine risk level. Our goal is a practical, cost-effective risk reduction and management process:

Step 1: Identify System Components and Elements
Step 2: Define Scope and Boundary of the Problem
Step 3: Identify Subsystems and Components in the Dotted Boundary
Step 4: Determine Mission Criticality Qualifier
Step 5: Identify Known Vulnerabilities of Each Subsystem in Step 3.
Step 6: Identify Existing Compensating Controls Mechanisms, Policies and Processes

Step 7: Qualify Vulnerabilities Based on Existing Controls
Step 8: Complete the 4x4 Risk Qualifying Matrix
Step 9: The Process of Risk Reduction

VII. CONCLUSION

This paper applies traditional risk management techniques in a uniform network-centric information assurance construct. In particular, the Defense-In-Depth model is extended to logical, layered and virtual "boundaries" beyond more traditional physical and geographic boundaries. This approach provides a baseline framework for understanding how Defense-In-Depth could be extended to increasingly complex operational environments. High levels of cost-effective information assurance may be achieved by consistently applying a uniform risk management methodology to systems and processes.

REFERENCES

[1] "Information Assurance through Defense-in-Depth," Directorate for Command, Control, Communications, and Computer Systems, U.S. Department of Defense Joint Staff, February 2000.

[2] Rochin, Gene, "Trapped in the Net: The Unanticipated Consequences Computerization," Princeton University Press, Princeton, NY, 1997.

[3] Abrams, M., Jajodia, S., and Podell, Editors," Information Security: An Integrated Collection of Essays," IEEE Computer Society Press, Los Alamitos, CA, 1995.

[4] Mollema, K., "Audit of Information Processing," Elsevier Advanced Technology, Oxford, United Kingdom, 1989.

[5] Jackson, K., Hruska, J., and Parker, D., editors, "Computer Security Reference Book," CRC Press, Butterworth-Heinemann, Ltd., Boca Raton, FL, 1992.