**Software Assurance and the CIA Triad of Information Security**

Nithish Sunkara

IS 5700 – Information Security and IT Governance

Indiana Institute of Technology  
Changhao Chenli

April 08, 2025

**Introduction**

Data and system security remains the highest priority in the present digital environment where many activities are connected. The processing and storage of critical information by organizations through software platforms necessitates software assurance to be a top organizational priority. Software assurance means having absolute certainty that software maintains its integrity by lacking vulnerabilities and performing correctly while defending itself from threats from beginning to end. Software assurance relies on CIA triad elements as the base framework for information security while implementing its protective measures. This paper examines the relationship between software assurance together with the CIA triad while demonstrating their support for effective security solutions in real-life examples such as the MOVEIT 2023 data breach incident.

**Confidentiality in Software Assurance**

Authorized people have exclusive access to sensitive information through confidentiality parameters. Software assurance uses encryption and strong authentication together with access control protocols to comply with the confidentiality principle. Security features embedded by developers during the software development lifecycle guarantee the protection of confidential data through its whole storage processing and transmission cycle.

The MOVEIT breach during 2023 serves as a warning about the severe effects occurring from the failure to maintain confidentiality. The Cl0p ransomware group exploited the zero-day SQL injection vulnerability present in MOVEIT Transfer version 10.3.1.5 developed by Progress Software. Highly sensitive personally identifiable information (PII) such as Social Security numbers together with financial data ended up being exposed during the breach. The MOVEIT incident proves that system configuration flaws together with inadequate input validation led to breaches in software solutions intended for enterprise use​.

Defense strategies for software assurance programs focus on protected code writing combined with thorough data validation techniques and security examination tools that check for security issues from the beginning of development (Tipton & Nozaki, 2012).

**Integrity in Software Assurance**

The maintenance of data and system consistency along with accuracy and trustworthy attributes represents integrity. The maintenance of software assurance integrity depends on hashing algorithms together with digital signatures while secure version control serves as an additional protection method. The tools assist in finding illegal modifications while verifying that original data and programming code stay unchanged.

The MOVEIT incident introduced breaches to both the data collection and data storage systems. The Clop group could not ensure that the compromised systems maintained their initial setup after unauthorized access because the files might have been modified before they left the network. In Healthcare departments and financial institutions, such failures would trigger serious negative outcomes. The manipulation of medical records may produce incorrect treatment choices because of the modifications.

Software developers protect their systems using thorough testing alongside checksums and changing management procedures to prevent such incidents. According to McGraw (2006), the deployment of security principles needs to begin during design and continue until the end of maintenance cycles to achieve effective integrity assurance.

**Availability in Software Assurance**

The availability principle grants authorized users smooth access to system components as well as data whenever necessary. The attainment of software assurance depends on techniques such as redundancy together with failover systems, load balancing solutions and software patching at the right time. System availability faces three main threats including Distributed Denial of Service (DDoS) attacks, hardware failures alongside unpatched vulnerabilities.

Temporary system outages happened during the MOVEIT breach as organizations performed their breach containment and emergency patch deployment. The service disruption harmed thousands of users together with organizations across many sectors which indicates that CIA triad failures cause rapid availability problems​.

When ensuring availability, the system needs active monitoring of resilient infrastructure and swift response procedures. The validation of system attack resilience depends on recovery testing and system stress testing which software assurance practices combine into their practices.

**Integrating the CIA Triad for Complete Software Assurance**

Any attempt to provide software assurance through attention to one CIA triad element will fail to reach true assurance. The integration of all three principles needs to be pursued as one unified structure. A system with high availability does not become secure because it fails to maintain confidentiality or integrity. A breach of the MOVEIT system illuminates why a confidentiality failure triggered doubts about both system integrity and disrupted its availability.

Security frameworks including the NIST Software Assurance Framework together with the Microsoft Security Development Lifecycle mandate that the CIA triad guidance begin at development's initial stages. These models provide guidance for developers to discover threats while reviewing code, configuring security, and performing ongoing audits for standard compliance verification of the software.

Software structures help organizations establish trustworthy systems and reduce potential dangers from program weaknesses.

**Personal Reflection and Class Connection**

Going through the Information Security and IT Governance program allowed me to grasp why the CIA triad principles form the cornerstone of software assurance and cybersecurity practices. One defective oversight in the MOVEIT incident exposed weaknesses in every segment within the triad. Through this assignment, I gained important knowledge about building software security into code development which should happen initially rather than trying to add it during later development phases. My learning about secure programming and maintaining software patches became essential to me because I want to pursue a career in cybersecurity.

**Conclusion**

Software assurance maintains its fundamental ties with the information security foundation which consists of Confidentiality Integrity and Availability. Software development based on these principles forms the complete framework to produce secure trustworthy and reliable software. A thorough analysis of the MOVEIT 2023 data breach demonstrates that system-wide security compromises result from weaknesses detected in any aspect of the triad framework. Developers together with organizations need to follow secure development practices that integrate information security principles across CIA across all development stages beginning from design through to deployment. Proactive supervision together with standardized assurance systems enables organizations to protect their digital resources throughout changes in the threat environment.

**References**

McGraw, G. (2006). *Software security: Building security in*. Addison-Wesley Professional.

Tipton, H. F., & Nozaki, M. (2012). *Information security management handbook* (6th ed.). Auerbach Publications.

CISA. (2023). *MOVE it Transfer Exploit Advisory*. <https://www.cisa.gov/news-events/alerts/2023/06/01/ongoing-exploitation-moveit-transfer-zero-day>

Progress Software. (2023). *MOVEit Security Bulletin*. <https://www.progress.com/security/moveit-transfer>

BleepingComputer. (2023). *MOVEit Hack Hits Government Agencies*. <https://www.bleepingcomputer.com/news/security/moveit-transfer-hack-hits-us-government-agencies/>