Information Assurance with special reference to the Security Content Automation Protocol (SCAP)—*An Overview*

P. K. Paul[1]&P. S. Aithal[2]
[1]Executive Director, MCIS, Department of CIS, Raiganj University (RGU), West Bengal, India
[2]Vice Chancellor, Srinivas University, Karnataka, India
E-mail:pkpaul.infotech@gmail.com

Type of the Paper: Explorative Research.
Subject Area: Information Science.
Type of Review: Peer Reviewed.
Indexed In: OpenAIRE.
DOI: http://doi.org/10.5281/zenodo.3514575.
Google Scholar Citation: IJCSBE

How to Cite this Paper:
Paul, P. K., & Aithal, P. S. (2019). Information Assurance with special reference to the Security Content Automation Protocol (SCAP)—An Overview. *International Journal of Case Studies in Business, IT, and Education (IJCSBE), 3*(2), 52-58.
DOI: http://doi.org/10.5281/zenodo.3514575.

International Journal of Case Studies in Business, IT and Education (IJCSBE)
A Refereed International Journal of Srinivas University, India.
IFSIJ Journal Impact Factor for 2019-20= 4.252

Information Assurance with special reference to the Security Content Automation Protocol (SCAP)—*An Overview*

P. K. Paul[1] & P. S. Aithal[2]
[1]Executive Director, MCIS, Department of CIS, Raiganj University (RGU), West Bengal, India
[2]Vice Chancellor, Srinivas University, Karnataka, India
E-mail:pkpaul.infotech@gmail.com

ABSTRACT

Information Assurance, in short, is called as IA. This is responsible for securing information systems and computing. The term holds the highest degree of security related affairs. In generally Computer Security considered as a branch and area of security but now apart from this, Information Security, IT Security, and Information Assurance considered as important. And among these, security related domain Information Assurance treated as broader and interdisciplinary. Moreover, this Information Assurance holds all the areas and dealing of IT Security and Information Security but additionally, it is responsible for the designing, development of policies, regulation and guidelines of security related projects /proposal, etc. And among the administrative and protocol related affairs Security Content Automation Protocol treated as important. In short, it is called as SCAP. It is a kind of method for using specific standards for the purpose of enabling vulnerability management systems in an automated way for the measurement as well as policy compliance assessment regarding the systems inbuilt in a company or institutions; that may include IT company or may not be. This is a conceptual paper, initially, it has discussed with the areas of Information Assurance but gradually it has described about the Security Content Automation Protocol; including its aim and objectives, versions, etc. paper mentioned all the areas in short and simple sense.

Keywords: Information Assurance, SCAP, IT Security, IT Policies, Security Content Automation Protocol, IT Management.

1. INTRODUCTION :

Information Assurance in short called as IA. This is a major name in Information Science and Computing as far as Security and allied technologies are concerned. Information Assurance is a broad field and containing all the areas of security viz. IT Security, Information Security, and sub areas viz. Network Security, Web Security, Database Security etc. It is important to note that, while other security fields are concerned about the technologies and technicalities, Information Assurance is additionally focused with managerial, social and legal areas of security. And that includes about the tools, products, rules and framework etc [1], [12]. In Information Assurance, content play a major role and as far as various and noted protocol is concerned among them one important is Security Content Automation Protocol (SCAP). The SCAP is required for the automated vulnerability measurement, policies etc. OpenSCAP is a kind of example of open marketable method. NIST stated SCAP as "…a suite of specifications that standardize the format and nomenclature by which security software products communicate software flaw and security configuration information". The SCAP is basically consist with two major element first one is protocol and second one is Software flaw. It is important to note that, various security activities as well as disciplines is able to get benefit from standardized expression including reporting and, in this regard, SCAP is important one [5], [7], [12].

2. OBJECTIVE AND AGENDA :

This current paper is theoretical in nature and basic type. It is provided bellow an overview on Information Assurance but with additional focus on Security Content Automation Protocol (SCAP) viz.—

- To know about the basics of Information Assurance and its nature or characteristics in simple sense.
- To learn about the importance, function and role of Information Assurance in current age of security systems.
- To learn about the basics of SCAP i.e. Security Content Automation Protocol including its basic need and aim.
- To learn about the basics of SCAP i.e. Security Content Automation Protocol with reference to the components and other related affairs.
- To know about the increasing importance of Security Content Automation Protocol (SCAP) in automated information security etc.

3. INFORMATION ASSURANCE: THE WAY :

Information Assurance is a broader field within security related areas and there are different areas within this viz. IT Security, Information Security, Computer Security and Cyber Security as it is deals with following features, functions and aims—

- Information Assurance is dedicated to information solutions of security related affairs viz. IT Security, Information Security etc.
- Information Assurance is also care about the manual as well as technological securities.
- The policies, framework, guidelines of security related services and products are the jurisdiction of the field Information Assurance.
- Information Assurance is cares about manual content security as well as privacy related issues and this is increasing day by day.
- Information Assurance today not only a way for the security management but also become a field of study and the field/ term/ applications growing internationally [12], [22].

4. SCAP: AN OVERVIEW :

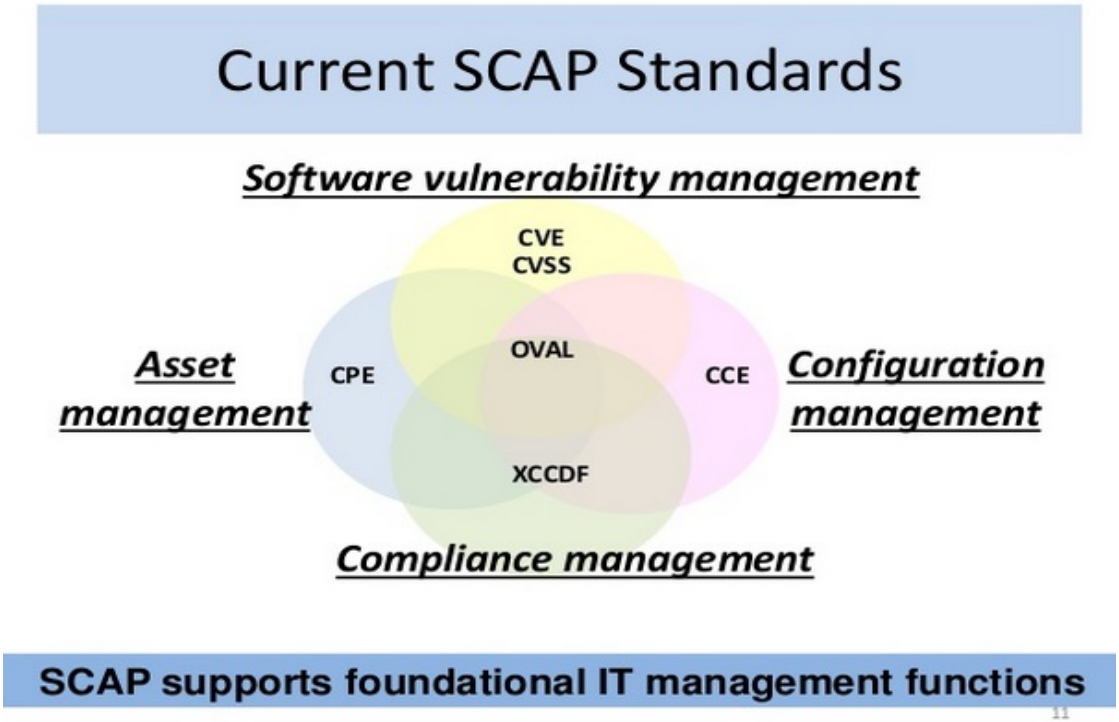

Fig. 1 : Current SCAP Standard (Source: GILIGAN, 2009)

The Security Content Automation Protocol (SCAP) may be treated as a type of method accountable for the applications in definite and specific standards and responsible for managing vulnerability and among these important are—

- Measurement;
- Policy compliance (like FISMA Compliance);
- Evaluation of systems [2], [3], [4]

The Security Content Automation Protocol in short SCAP basically pronounced as S (ESS) CAP. And sometime individually as S.C.A.P. The NIST definition we already learned it is worthy to note that, according to the NIST guidelines three major ways of maintaining security of the organizations are includes—

1. Verifying as well as installation of the patches, automatically.
2. Checking and continuing configuration of the system security.
3. Examining the systems for the signs of the compromise [6], [9], [10], [12].

5. SECURITY CONTENT AUTOMATION PROTOCOL AND FEW CONCERNS :

The NVD i.e. National Vulnerability Database is established in United States and responsible to content and data repository for the SCAP. Security Content Automation Protocol (SCAP) is responsible for the following—

- Organizing
- Expressing
- Measuring

Security information having automated approach for security management of the entire enterprise systems. OpenSCAP is a kind of example of open marketable method. FDCC i.e. Federal Desktop Core Configurations well as United States Government Configuration Baseline initiative i.e. USGCB i.e., it was evolved from the Federal Desktop Core Configuration authorized as well as mandate the requirements of the SCAP/Security Content Automation Protocol [8], [11].

The SCAP or Security Content Automation Protocol required for the purpose of guard against security threats of the institutions, organizations etc for continuous monitoring to the computer systems; it includes the applications they have deployed, upgrade to configurations. It is worthy to note that, various open standards which are applicable to enumerate software flaws including configuration issues related to security fall under the SCAP. Some of the applications which is required to conduct security monitoring as well as measuring vulnerabilities basically comes under the SCAP i.e. Security Content Automation Protocol (Refer Fig: 1 & Fig: 2 for further).

6. SCAP COMPONENTS:

Security Content Automation Protocol has two major concern/ elements and among these few important are—

- **First,** it is a protocol **(**It is a kind of four open specifications which is dedicated to the standardize the format as well as nomenclature and specification; and each is known as SCAP Specification.
- **Second,** Security Content Automation Protocol is also about the software flaw as wellas few security configuration standard reference data, and this is also referred as SCAP content [13], [14], [15].

The following table (table 1) shows the **Security Content Automation Protocol** Version and components herewith.

Table 1 :SCAP Various Versions

SCAP Version 1.0	SCAP Version 1.0 and 1.2
• Common Vulnerabilities and Exposures • Common Configuration Enumeration • Description Format • Open Vulnerability and Assessment Language • Common Platform Enumeration • Common Vulnerability Scoring System • Extensible Configuration Checklist	• Open Checklist Interactive (1.1) • Language (OCIL) Version 2.0 • Trust Model for Security Automation Data • Asset Identification • Asset Reporting Format • Common Configuration Scoring System

It is worthy to note that Security Content Automation Protocol version 1.0 was released on July, 2010 and SCAP 1.1 in the year February, 2011 while SCAP 1.2 in September, 2011.

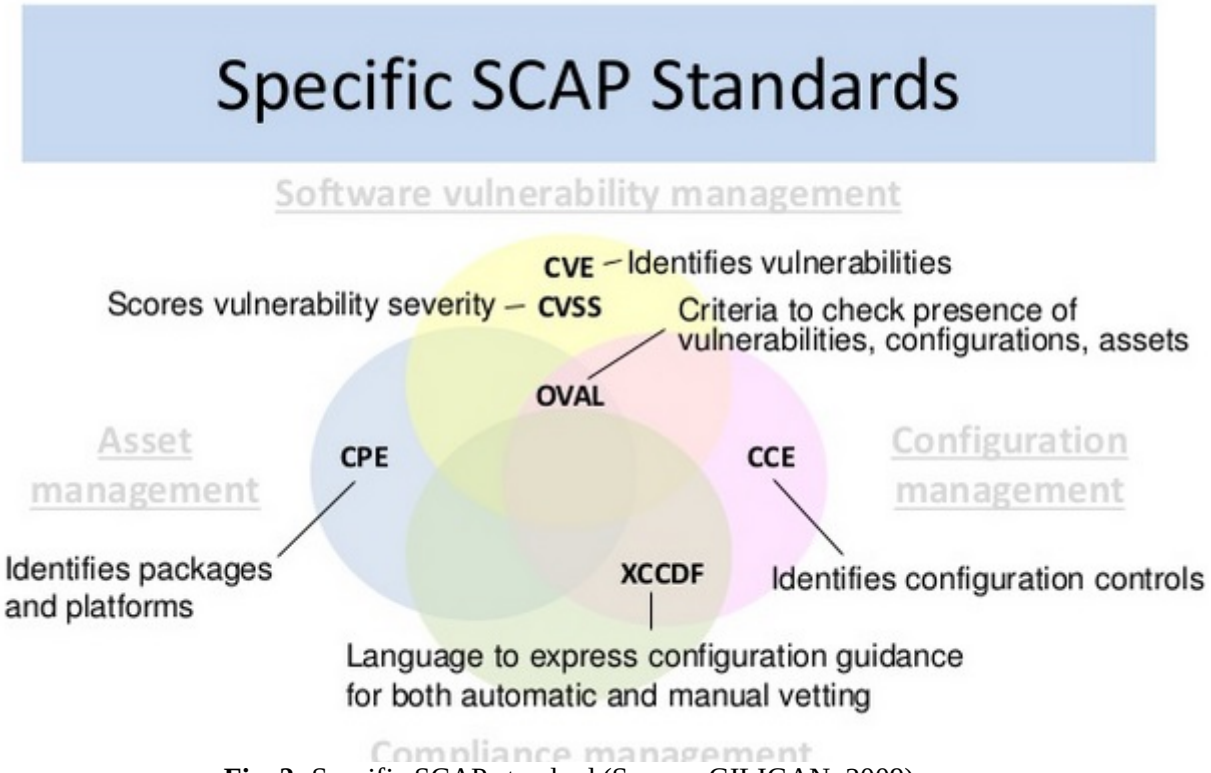

Fig. 2 : Specific SCAP standard (Source: GILIGAN, 2009)

7. SCAP CHECKLISTS :

Security Content Automation Protocol (SCAP) checklist is responsible for the automation ad also the linkage between the configuration of the computer security and with SP 800-53 framework. Running Security Content Automation Protocol (SCAP) version is dedicated to the initial measurement and also continuous monitoring [4], [16], [17].

Additionally, this way, Security Content Automation Protocol (SCAP) is dedicated to the implementation, evaluation as well as monitoring steps of the NIST Risk Management Framework. And here SCAP Validation Program is responsible for checking the ability of products to employ SCAP standards [18], [19]. It is also important to note that Community participation is required for healthy Security Content Automation Protocol (SCAP) implementation. It is important to note that security automation agenda of the NIST is currently broader and weakness management application.

8. CONCLUSION :

The world is changing rapidly, security is an important concern as far as Information Technology and Computing field. Privacy is very important concern in various respects. Information Assurance is a great name in respect of combining both. Additionally, Information Assurance is also responsible for the managing manual contents and it deals managerial affairs leading to rules, regulation, framework etc [12], [20], [21]. Hence as far as SCAP is concerned it is needed for better and healthy security policies designing and development. Every big organizations these days are using IT products and services and it is important if they are interested to employ SCAP for further enhancement.

REFERENCES:

[1] Al-Shaer, E. (2011). Security automation research: Challenges and future directions. *IAnewsletter*, *14*(4), 14-18.

[2] Aslam, M., Gehrmann, C., & Björkman, M. (2013). Continuous security evaluation and auditing of remote platforms by combining trusted computing and security automation techniques. In *Proceedings of the 6th International Conference on Security of Information and Networks* (pp. 136-143). ACM.

[3] Borgesius, F. Z., Gray, J., & Van Eechoud, M. (2015). Open data, privacy, and fair information principles: Towards a balancing framework. *Berkeley Technology Law Journal*, *30*(3), 2073-2131.

[4] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), 523-548.

[5] Burr, W., Ferraiolo, H., & Waltermire, D. (2013). NIST and computer security. *IT Professional*, *16*(2), 31-37.

[6] Johnson, C., Quinn, S., Scarfone, K., & Waltermire, D. (2009). The technical specification for the security content automation protocol (SCAP). *NIST Special Publication*, *800*, 126.

[7] Kampanakis, P. (2014). Security automation and threat information-sharing options. *IEEE Security & Privacy*, *12*(5), 42-51.

[8] Kasprzyk, R., & Stachurski, A. (2016). A concept of standard-based vulnerability management automation for IT systems. *Computer Science and Mathematical Modelling*, (3), 33-38.

[9] Kuo, C. L., & Yang, C. H. (2015). Security design for configuration management of Android devices. In *2015 IEEE 39th Annual Computer Software and Applications Conference* (Vol. 3, pp. 249-254). IEEE.

[10] Obrst, L., Chase, P., & Markeloff, R. (2012). Developing an Ontology of the Cyber Security Domain. In *STIDS* (pp. 49-56).

[11] Montesino, R., & Fenz, S. (2011). Information security automation: how far can we go?. In *2011 Sixth International Conference on Availability, Reliability and Security* (pp. 280-285). IEEE.

[11] Paul, Prantosh Kumar, Aithal, P. S., Bhuimali, A., Kalishankar, Tiwary, and Rajesh, R., (2019). FIPPS & Information Assurance: The Root and Foundation (June 15, 2019). *Proceedings of National Conference on Advances in Management, IT, Education, Social Sciences* (MANEGMA 2019), Mangalore. *1*(1) pp. 27-34.

[12]Radack, S., & Kuhn, R. (2011). Managing security: The security content automation protocol. *IT professional*, *13*(1), 9-11.

[13] Rajak, S., & Verma, A. (2012). Secure data storage in the cloud using digital signature mechanism. *International Journal of Advanced Research in Computer Engineering & Technology*, *1*(4), 2278-1323.

[14] Rajamäki, J., Rathod, P., Ahlgren, A., Aho, J., Takari, M., & Ahlgren, S. (2012). Resilience of cyber-physical system: A case study of safe school environment. In *2012 European Intelligence and Security Informatics Conference* (pp. 285-285). IEEE.

[15] Savola, R. (2009). A Security Metrics Taxonomization Model for Software-Intensive Systems. *JIPS*, *5*(4), 197-206.

[16] Savola, R. M., Frühwirth, C., & Pietikäinen, A. (2012). Risk-driven security metrics in agile software development-an industrial pilot study. *J. UCS*, *18*(12), 1679-1702.

[17] Souppaya, M., & Scarfone, K. (2013). Guide to enterprise patch management technologies. *NIST Special Publication*, *800*, 40.

[18] Subramanian, P. (2015). Security Content Metadata Model with an Efficient Search Methodology for Real Time Monitoring and Threat Intelligence. *Retrieved*, *12*(04), 2017.

[19] Sudha, M., Rao, D. B. R. K., & Monica, M. (2010). A comprehensive approach to ensure secure data communication in cloud environment. *International Journal of Computer Applications*, *12*(8), 19-23.

[20] Trček, D. (2009). Security metrics foundations for computer security. *The Computer Journal*, *53*(7), 1106-1112.

[21] Wadkar, H. S., Mishra, A., & Dixit, A. M. (2017). Framework to Secure Browser Using Configuration Analysis. *International Journal of Information Security and Privacy (IJISP)*, *11*(2), 49-63.

****