RESEARCH ARTICLE OPEN ACCESS

Conceptural Oriented Analysis On The Industrial Standard Cyber Security

Dr.K.Sai Manoj, Ms. K. Mrudula, Mrs. G.Maanasa, Prof.K.Phani Srinivas
CEO, Innogeecks Technologies and Amrita Sai Institute of Science and Technology/Reviewer, Vijayawada, AP, India
Director, Innogeecks technologies, Vijayawada, AP, India
Research Scholar, Acharya Nagarjuna University, Guntur Dist, AP, India
Editor and Reviewer, Director R&D, Innogeecks Technologies and Amrita Sai Institute of Science and Technology, Vijayawada, AP, India

ABSTRACT

Digital computers have been chosen as a safety system in newly constructed nuclear facilities. Owing to digitalization, cyber threats to nuclear facilities have increased and the integrity of the digital safety systems has been threatened. To cope with such threats, the nuclear regulatory agency has published guidelines for digital safety systems. This paper suggests an implementation method of cyber security for the safety system in the development phase. It introduces specific security activities based on a practice in a nuclear facility construction project. It also explains experiences resolving security vulnerabilities of the system and gives lessons learned about considerations in a real construction.

Keywords : **-** 0jjSoftware Verification and Validation, Cyber security.

I. INTRODUCTION

Nowadays, the cyber-security media are very concerned about people being exposed to all sorts of abuse on Social Media Platforms (SMPs). The malicious intent of humans deceiving other humans constitutes a cyber threat that is one of the most difficult to contend. More importantly, these cyber threats are aggravated by the sheer number of vulnerabilities present in SMPs, the number of available and different types of SMPs (Chaffey, 2016), the poor design and construction of SMPs (Haimson and Hoffmann, 2016), the large volumes of unstructured content (Assunção et al., 2015), and the opportunities that SMPs provide to humans acting in malicious ways (Fire et al., 2014). These factors all contribute to SMPs being extremely vulnerable to cyber threats caused by malicious users. Furthermore, as a result of these cyber threats and SMP vulnerabilities we witness an alarming increase in the prevalence of cyber bullying (Smit, 2015), identity theft (Kabay et al., 2014), identity impersonation (Galán-GarcÍa et al., 2015), dissemination of pornography (Benevenuto et al., 2010), fraud (Gurajala et al., 2015), and the like. As an example, consider a recent cyber-security case reported on in South Africa where, as in any other country in the world, an alarming increase has been noted in cyber threats related to abuse against women (Bliss, 2017). The cyber threat in this case manifested itself in the form of identity impersonation by two malicious users who exploited the "ease-of-opening-a-deceptive-account" vulnerability on Face book and were arrested for luring, raping, and killing women (de Villiers, 2017). This and other cyber security cases (Peterson, 2016); (Digital, 2016) point to a common thread in exploiting SMP vulnerabilities, namely the ease of creating fake or deceptive identities (Tsikerdekis and Zeadally, 2014). In the case of identity deception, a deceptive account is either created with malicious intent or to preserve anonymity. This paper is concerned with the detection of deceptive accounts created with malicious intent, as these pose a cyber threat to other humans at large. A deceptive account with malicious intent could for example be used to defame someone's character (Galán-GarcÍa et al., 2015) or conduct online bullying (Smit, 2015). These deceptive accounts are generated by humans or bots (Chu et al., 2010). Much research (Oentaryo et al., 2016); (Dickerson et al., 2014); (Cresci et al., 2015) has been done to detect bot

accounts that require no human involvement for the actions they perform. These deceptive bot accounts are known to target groups, as opposed to specific individuals (Oentaryo et al., 2016). However, to date, very little research has focused on detecting deceptive human accounts on SMPs.
The research reported on in this paper is a first attempt at minimising the cyber risk of identity deception as exploited by malicious users on SMPs through the intelligent detection of deceptive identities. The aims of the research reported on in this paper are summarised as follows:

- To identify and describe the different types of information

available on SMPs – also referred to as attributes (e.g. the date on which the account is created) – that can potentially be used to detect user identity deception.

- To experiment with SMP attributes to detect, in an intelligent way, user identity deception by using various machine learning models.
- To enhance the SMP attributes for improving identity deception detection by using engineered features derived from two fields: Firstly, the field of psychology where we focus specifically on discovering why people lie, and secondly, from the field of detecting bot accounts where we

intend to determine how these solutions can be leveraged for detecting human identity deception.

- To propose a model that intelligently detects and interprets the perceived deceptiveness of a SMP user, given the results from the aforementioned experiments.

This will be the first time that features derived from the field of psychology will be applied towards the detection of human identity deception on SMPs.

II. CYBER SECURITY FOR SAFETY SYSTEM

Safety-grade digital computers are used for the reliable protective functions of nuclear facilities. This section introduces a planning for cyber security of the safety systems. Shortly, the cyber security considerations have been incorporated into the safety system development process.

A. Relationship between V&V activities and cyber security activities

A well-known industrial standard, IEEE, 2004, endorsed by the nuclear regulatory body gives specific activities for software verification and validation (V&V) of digital safety systems. The security analysis mentioned in the standard has been interpreted as the concept of physical security only. Considering recent regulatory positions, it is acceptable that the security analysis should be conducted for the cyber security of digital systems. Thus, this study decomposes the standard requirements into three major parts, software V&V, safety analysis, and cyber security analysis. The analysis results for each part through the development phases are published independently. Fig. 2 shows the cyber security plan within the V&V plan of the system.

Generally, system developers use qualified commercial-off-the shelf (COTS) products as the platform of safety systems. Software V&V and a safety analysis only focus on logic source codes that are newly developed within the products. In the case of a security analysis, the security capability in the past does not ensure the same effectiveness currently due to continuously evolving cyber threats. Therefore, this paper recommends that the hardware and software of the COTS are included as review items in the security analysis.

B. A cyber security plan

This section proposes a cyber security plan including a cyber security team (CST) organization and security activities implementation. The cyber security team consists of a team leader and team members. The major missions of the team are as follows:

- supervision of the secure development environment,
- analysis of the system vulnerability and penetration test to the system,
- introducing cyber security requirements,
- tracking and resolving security issues,

- assessing security impact on the system integrity, and
- reviewing the results of development phases

The system development model for the digital system is a well known waterfall design model, which consists of the concept, requirement, design, implementation, and test phases. This paper adds security activities to the design model to perform the security team missions. Fig. 3 shows the security activities defined in the plan.

- Attack Path Analysis: Used to identify accessible pathways to the system cabinet physically and logically. Non-accessible pathways by existing security controls are found in this activity. It is used as evidence for justification that the security controls used to eliminate vulnerabilities at the pathways can be excluded in the system. Detailed information about the accessible pathways is utilized as input to the penetration test of the system.
- Penetration Test: Used to test whether attackers can jeopardize the system through the identified pathways or not. If the cyber attacks actually impact the system functioning, then security controls used to block the attacks are proposed in this activity.
- Security Requirements V&V: Hardware and software requirements for the cyber security are defined as part of the overall system requirements. If potential vulnerabilities of the system are induced by the functional requirements, the results are fed back to the developers, and the design problems are resolved directly in the same phase.
- Security Design V&V: It is checked that the security requirements are mapped into specific design items as part of the systems. For example, the password, session lock, and isolation devices become design items for the control of the access requirements.

To decide whether the design is acceptable, a security assessment used to identify potential vulnerabilities to the system is performed using detailed design documents.

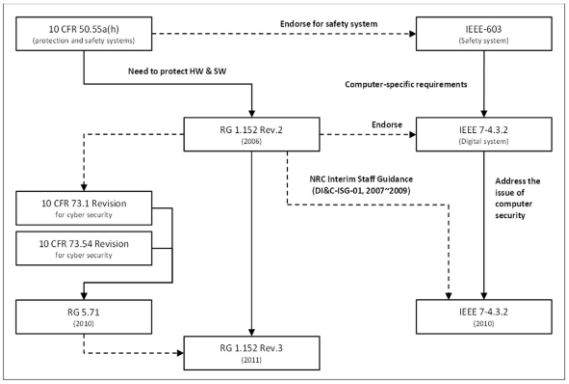

Fig. 1. Codes and standards for cyber security.

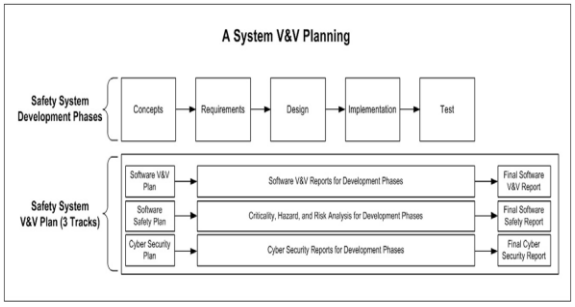

Fig. 2. Cyber security incorporated into system V&V plan.

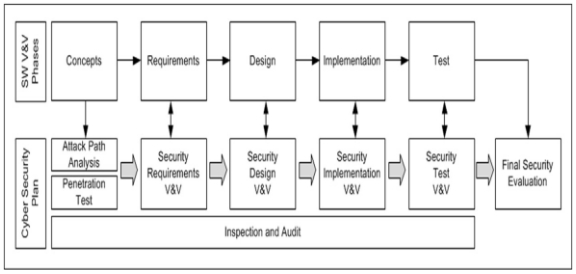

Fig. 3. Cyber security plan and activities.

_ Security Implementation V&V: Checks whether the security design items are appropriately transformed into specific hardware and software representations. The security team forces system developers to keep a secure development environment to minimize any inadvertent or

inappropriate alterations of the system. In addition, the V&V team performs the code level analysis between the requirements and source codes of the system, and the security team confirms no inclusion of undocumented codes or functions within the system by reviewing the code analysis results.

_ Security Test V&V: During the test phase, it is verified that the implementation results meet the security design requirements completely. Through security tests on the system hardware, software, and communication devices, it is validated that the security functions of the system are implemented appropriately.

_ Final Security Evaluation: After testing, the security team publishes a cyber security report for the system. It includes a summary of the security activities and conformance analysis about the regulatory positions (USNRC, 2006).

Configuration management ensures that the security objectives remain satisfied by controlling the changes made to the safety system. The configuration management team should assess the impacts of the changes on the security posture of the system when making a configuration change. The security impact analysis focuses on potential vulnerabilities, weakness, and risks introduced by changes in the system. Evaluations on logical and physical connectivity pathways, equipment interdependencies, and effectiveness of related documents are included in the analysis. The impact analysis is performed as part of the change approval process.

The proposed plan is featured by (1) the harmonization of the security activities with the legacy V&V activities, (2) the security analysis including penetration testing about the platform in the initial phase to address technical security problems that are hard to be mitigated at the system level, and (3) security V&V activities for tracking the security design, maintaining the secure development environment, and conforming the completeness of the source codes.

III. RESULTS AND DISCUSSIONS

This section introduces an implementation practice of the proposed security plan in a construction project. Instrumentation and control system package includes a safety-grade digital protection system. Thus, cyber security consideration is taken in the development process of the safety system to meet the regulatory guide (USNRC, 2006). This section explains the implementation results of security activities. In addition, it discusses the lessons learned through detecting and resolving the security issues.

A. Attack path analysis and penetration test

Even if developers have not added source codes to the system yet, internal vulnerabilities of the system platform should be addressed early in the project. Generally, technical support of the platform manufacturer takes a long time. For this reason, the cyber security team performs an attack path analysis to identify internal vulnerabilities in the concept phase of the V&V process. The attack paths are revealed by reviewing the design documents such as the system configuration diagram, system hardware configuration, and system interface description. Through the analysis, the security team has built up logically possible attack scenarios to a digital safety system. Fig. 4 shows the channel-A (Ch-A) system cabinet configuration composed of signal controllers, a maintenance computer, and a development kit. It has been found that the attack scenarios are initiated at the development tool kit computer and the connection interface to other digital system as shown in (1) and (2). For each attack scenario, a penetration test prepared by independent specialists, such as white hackers, has been made. They summarized the detailed access steps and the security team evaluated the impact on the system integrity.

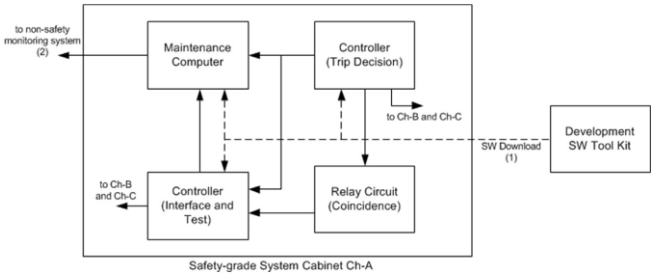

Fig. 4. Internal and external interfaces of a safety system cabinet.

B. Security V&V activities

Technical issues caused by a lack of security functions in the platform can be covered by the manufacturer. However, potential vulnerabilities in the logic source codes made by system developers should be found and resolved by the V&V activities. The regulatory body also emphasizes the correctness of the source codes in (USNRC, 2006) through following statement: 'ensure that the safety system does not contain unwanted and undocumented functions or codes'. Thus, both the implementation of security features and the correctness of the source codes should be reviewed by the V&V team. The security team has concentrated directly on the system design life cycle (SDLC) to determine whether the security requirements have been completely transformed into specific design features. The correctness of the source codes and functions has been verified in the traceability activity by the V&V team. Thus, the security team has joined and reviewed the traceability from the perspective of security. As the review results, some source codes for the module tests and temporary functions have been found and removed in the implementation phase.

IV. CONCLUSION

One of the emerging issues related to the digital safety system of a nuclear facility is computer security. To address this issue, security considerations in the development process should be made as described in the industrial standards. This paper suggests an implementation method of cyber security of a nuclear safety system. It explains four main activities, a cyber security team organization, security assessment including penetration test, security V&V during software development, and security evaluation. It also presents the harmonization of the security activities with the legacy V&V activities. This paper also introduces a practice of the cyber security implementation in a real construction project. It explains the detailed results of the security activities and introduces a process in the finding and resolving of security vulnerabilities. Finally, some lessons learned in the experience are also introduced. It is expected to be useful so that system designers and developers can understand the overall security activities of the safety system.

DECLARATIONS

Availability of data and material
Not applicable.

Competing interests

Not applicable.

Funding
No funding was applicable.

Authors' contributions
The other of the paper do all the work, the environment for research work is done by my best of my knowledge and supporting my family members.

Acknowledgements
First of all, I am thankful to Honorable Amrita Sai Management for giving me this opportunity and to complete my work. It gives me an immense pleasure and pride to express my deep sense of gratitude to the Innogeecks technologies for their technical support in all the aspects.

REFERENCES

[1]. MANN, H. B. & WHITNEY, D. R. 1947. On a test of whether one of two random variables is stochastically larger than the other. *The annals of mathematical statistics*, 50-60.

[2]. MCDONALD, J. H. 2009. *Handbook of biological statistics*, Sparky House Publishing Baltimore, MD.

[3]. MENARDI, G. & TORELLI, N. 2014. Training and assessing classification rules with imbalanced data. *Data Mining and Knowledge Discovery*, 1-31.

[4]. OENTARYO, R. J., MURDOPO, A., PRASETYO, P. K. & LIM, E.- P. On Profiling Bots in Social Media. InternationalConference on Social Informatics, 2016. Springer, 92-109.

[5]. PEDDINTI, S. T., ROSS, K. W. & CAPPOS, J. 2017. Mining Anonymity: Identifying Sensitive Accounts on

Twitter. *arXiv preprint arXiv:1702.00164*.

[6]. PETERSON, T. 2016. Rapist who used social media to lure child victims sentenced to 20 years. *News24*, 15 Jun 2016.

[7]. PINTEREST. 2017. Pinterest API. Available: https://developers.pinterest.com/ [Accessed 8 Jan 2018].

[8]. RÉNYI, A. On measures of entropy and information. Proceedings of the fourth Berkeley symposium on mathematical statistics and probability, 1961. 547-561.

[9]. RIBEIRO, M. T., SINGH, S. & GUESTRIN, C. Why should i trust you?: Explaining the predictions of any classifier.

[10]. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2016. ACM, 1135-1144.

[11]. RONG, R., HOUSER, D. & DAI, A. Y. 2016. Money or friends: Social identity and deception in networks. *European Economic Review*, 90**,** 56-66.

[12]. RUBIN, V. L. 2017. Deception Detection and Rumor Debunking for Social Media. *The SAGE Handbook of Social Media Research Methods***,** 342.

[13]. SAABAS, A. 2018. Contribute to treeinterpreter development by creating an account on GitHub.

[14]. SCHWARTZ, H. A., EICHSTAEDT, J. C., KERN, M. L.,DZIURZYNSKI, L., RAMONES, S. M., AGRAWAL, M., SHAH, A., KOSINSKI, M., STILLWELL, D. & SELIGMAN, M. E. 2013. Personality, gender, and age in the language of social media: The open-vocabulary approach. *PloS one*, 8**,** e73791.

[15]. SEDHAI, S. & SUN, A. 2017. Semi-Supervised Spam Detection in Twitter Stream. *arXiv preprint arXiv:1702.01032*.

[16]. SHANNON, C. E. 2001. A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review*, 5**,** 3-55.

[17]. SHAPLEY, L. S. 1953. A value for n-person games. *Contributions to the Theory of Games*, 2**,** 307-317.

[18]. A Survey on Protection of Multimedia Content in Cloud Computing, Dr. K.Sai Manoj, Mrudula Kudaravalli,International Journal of Computer Science and Mobile Computing - Vol.6 Issue.11, November-2017, pg. 7-11

[19]. INVESTIGATION ON THE DATA SECURITY IN CLOUD COMPUTING USING BIOMETRICS Dr.Sai Manoj.K International Journal of Current Advanced Research Volume 7; Issue 12(B), December 2018; Page No: 16473-16475

[20]. Conceptual oriented study on the cloud computing architecture for the full-security Dr.K.Sai Manoj International journal of Engineering and Technology, Volume 7,Issue 4,2018,Scinence Publishing Corporation.

Authors' information

Dr K Sai Manoj, Founder and Executive Director of Innogeecks Global Services Pvt Ltd, Founder and CEO of Innogeecks Technologies and Founder of 3 start-ups based on IOT and Cloud Computing, is an Enthusiastic learner, Excellent Financial Advisor, Innovative and Visionary Leader, Insightful team builder and strategic planner, who has 10+ years of experience in Financial Services, Equity Research and IT- ITeS services to his credit. He has worked in Reputed Companies like WIPRO Technologies, Fidelity Inverstments.etc.,

He is Proud of achieving many laurels in the field of Computers and Research. He is a Certified Ethical hacker, Certified Computer hacking forensics Investigator, Certified Security Analyst, Charted Engineer from IEI (India), Certified Blockchain Expert, Microsoft Certified Technology Specialist, AWS Certified Solutions Architect-Associate, Google Analytics Individual Qualification, IBM Block chain Certification, Certified EC Council Instructor and so on.

He has a proven record of having 10+ certifications from the most sought after software giants such as Microsoft, IBM, Google, Face book, EC Council & Amazon besides this he has

acted as a reviewer for the Journal of Super Computing (Springer) , Journal of Big Data (Springer) and Journal of the Institution of Engineers (India) – Series B (Springer). And also with his solid financial advice 21 start-ups of Kochi, Bangalore and Vijayawada have tread the success track.

Talking about his research excellence, it is exciting to know that he has filed 3 patents and 4 more are in pipeline and has Published more than 25 research papers in reputed journals like Thomas Reuters, IEEE, Scopus etc., and shows keenness in researching on Cyber Security, Cloud Computing, Big Data / Hadoop, Block chain and Data Analytics

Ms. K.Mrudula working as a Director for the Innogeecks Technologies. She was completed M.Tech from IIIT Hyderabad .She got more than 6 years of experience in Teaching. She published more than 5 research papers in various International and national research journals. She attended 2 FDP, and 1 workshop.

Mrs.G.Maanasa worked as HR manager in Jaya lakshmi Powercorp Ltd for a Period of 6 years after completing her M.B.A from RVR&JC college of Engineering. She is currently pursuing her doctorate (PhD) in Development of Framework for Tourism Promotion in AP and ICT Integration from Nagarjuna University.

K.PHANI SRINIVAS working as a Director for the Research and Development and He Had Five Years of Industrial Experience as a team Leader in the research areas of Embedded Systems and telecommunications and also He is Having 13 Years of Experience in Academics, Research and Administrative reports. He received so many awards such as a Best Engineer, Best Teacher and also as a Best Researcher. Also He is acting as an Editor/Reviewer for so many top international Journals.

The Focus of His research work is Design of Patch antennas which are Suitable for Defence and Space Based Applications. He received appreciation award in various National and International Conferences. He received Best Coordinator Certificates from IUCEE, IIT ROORKEE, IIT Bhubneswar, NCAT, ELAT and INTEL. He attended WIPRO training Program. He completed one Joint research Program with IIT Kharagpur.He Organized various student level Competitions, workshops, Faculty Development Programs, Guest lectures, Orientation Programs, and Subject Based Seminars with scientists and Academicians. He is doing research work under the valuable Directions of Eminent Scientists. He had done technical Discussions with experts at Space Station, Antenna Research Lab, and Radar station. He Published research articles in Various Scientific Journals. He is an active Editor/Reviewer for the so many top most international journals.