securiCAD by foreseeti

A CAD tool for enterprise cyber security management

Mathias Ekstedt, Pontus Johnson, and Robert Lagerström
KTH Royal Institute of Technology
Osquldas väg 12
Stockholm, Sweden
robertl@kth.se

Dan Gorton, Joakim Nydrén, and Khurram Shahzad
foreseeti AB
Valhallavägen 79
Stockholm, Sweden
joakim.nydren@foreseeti.com

***Abstract*—This paper presents a CAD tool for enterprise cyber security management called securiCAD. It is a software developed during ten years of research at KTH Royal Institute of Technology, and it is now being commercialized by foreseeti (a KTH spin-off company). The idea of the tool is similar to CAD tools used when engineers design and test cars, buildings, etc. Specifically, the securiCAD user first models the IT environment, an existing one or one under development, and then securiCAD, using attack graphs, calculates and highlights potential weaknesses and avenues of attacks. The main benefits with securiCAD are; 1) built in security expertise, 2) visualization, 3) holistic security assessments, and 4) scenario comparison (decision-making) capabilities.**

Keywords—cyber security; enterprise architecture; modeling; analysis

I. INTRODUCTION

The digital development where everything is getting connected makes cyber security vital. Global cost of cyber-crime amounts to 300-1.000 BUSD [1], increasing at ~45% CAGR (Compound Annual Growth Rate) [2], same trend appears in [3].

These trends have also been observed by different authorities which have stepped up their minimum security requirements, for example, the Federal Financial Institutions Examinations Council (FFIEC) in the US, and the European Central Bank (ECB) in Europe, including requirements for risk management of online banking [4][5].

Risk management of cybersecurity is however challenging; it requires a holistic perspective in a world of details, expertise in several different security domains, and ability to conduct complex analyses across large-scale architectures with integrated systems-of-systems. Today, this work is typically done through manual expertise, which is scarce, expensive and subjective, leading to risks, and inconstancies.

foreseeti has developed a CAD tool for enterprise cyber security management called securiCAD. The user either models the architecture by drag-and-drop functionality and/or by importing data from other tools, such as vulnerability and network scanners. securiCAD then simulates hacker attacks and provides a "heat map" of where the architecture is likely to be more or less vulnerable, based on security research and expertise combined with sophisticated network analysis (cf. Fig. 1).

securiCAD helps its users to:

- Understand current cyber security levels across complex architectures.
- Prioritize areas to address and cyber security investments to pursue.
- Proactively manage cyber security e.g. when building or modifying to-be scenarios.

The value provided to users of securiCAD is:

- **Access to expertise**. The tool provides users with access to large amounts of research & expertise within the area of cyber security management. Expertise that is scarce in the market today [6]. Thus, the tool empowers it users, which is especially valuable for organizations that do not have the resources to attract and hire the best experts.
- **Improved cyber security management efficiency**. The tool enables or improves the efficiency in conducting the complex analyses needed to get the overview understanding of vulnerability levels across the enterprise architecture. The insights can be used to improve prioritization of resources for detailed analyses such as e.g. penetration tests.
- **Improved visualization**. As the importance of cyber security increases, the topic is moving upwards in companies' agendas. This increases the importance of getting and providing an overview picture of the area for common understanding and prioritization and management reporting.
- **Improved cyber security ROI**. In the end the target is to get an improved cyber security level and/or return on investment. Each 1% reduction in cybercrime = typically ~150.000-200.000 € for a company in foreseeti's priority 1 industries (critical infrastructure, banking et cetera).

978-1-4673-9331-7/15 $31.00 © 2015 IEEE
DOI 10.1109/EDOCW.2015.40

The last two bullets have been highlighted in a report from World Economic Forum [7] where the authors argue for a cyber value-at-risk model.

II. Background

When engineers design e.g. bridges or cars, they leverage computer aided design tools for designing and testing their constructions. In the area of enterprise architecture and IT such tools are largely lacking. This was the main insight that led a group of KTH Royal Institute of Technology researchers to start develop such a tool for IT about 10 years ago. The research has now produced a well-functioning and proven research prototype of this tool, consisting of an enterprise architecture analysis tool and modules containing expertise in different areas such as e.g. cyber security [8]-[18], interoperability, modifiability, et cetera [19]-[24].[1] The enterprise architecture analysis tool together with the module for cyber security is now being developed into a market ready product and taken to the commercial market by the startup company foreseeti. The main commercialization activities are funded by KIC InnoEnergy[2].

There are other tools designed for comparable purposes, however these are often very limited in scope, for instance NetSPA [25], MulVAL [26][27], and the TVA-tool [28], or imprecise, and therefore also too subjective [29], like OCTAVE [30], CORAS [31], Common Criteria [32], and work by Breu et al. [33].

III. System Overview

The analysis (simulation) run with securiCAD is based on probabilistic simulation in attack graphs similar to Bayesian networks, combined with security research and expertise. The actual analysis is done on an attack/defense type level. I.e. this means that for each asset in the users model (e.g. an application), the average time to compromise the asset is determined for each type of attack (e.g. Memory corruption exploitation or Code injection) based on what defenses has been implemented with respect to that asset (e.g. Anti-malware, Encryption etc.). The parameters, relationships, and dependency-structure have been determined through research incorporating standards and scientific articles, reviewed and prioritized by experts. Vulnerability probabilities are based on: 1) Logical necessities, e.g.: if the firewalls allow you to connect to A from B and you have access to B, then you can connect to A. 2) Others' scientific studies, e.g. time-to-compromise for authentication codes and patch level vs. patching procedures. 3) Experts' judgments, own surveys to researchers and security professionals. 4) Own experiments, lab and cyber defense exercises.

securiCAD contains 23 asset types, including protocol, data store, dataflow, application client, web application, web application firewall, application server, network zone, firewall, network interface, operating system, software product, intrusion prevention system (IPS), intrusion detection system (IDS) sensor, zone management process, network vulnerability scanner, social zone, physical zone, person, security awareness program, access control point, password account, and password authentication mechanism, as well as 51 system relations types.

Each asset contains a number of attacks and defenses. E.g. the software product class which has the defenses; source code secret, binary secret, improved with static code analysis, written only in safe languages, has been scrutinized, has no unpatchable vulnerability, and has no patchable vulnerability, as well as the attach steps; get product information, find public patchable critical vulnerability, find public unpatchable critical vulnerability, find public exploit for patchable critical vulnerability, develop exploit for patchable critical vulnerability, find public exploit for unpatchable critical vulnerability, develop exploit for unpatchable critical vulnerability, and develop zero day exploit. Another example asset is data flow that has no defenses but six attack types namely; disrupt, replay, eavesdrop, main in the middle, produce request, and produce response. While the asset called protocol instead has no attacks but three defenses namely; freshness indicator, cryptographic authentication, and cryptographic obfuscation.

In total securiCAD contains 59 attacks / malicious activities, other examples are;

- zero-day discovery,
- memory corruption exploitation,
- web application exploitation (XSS, RFI, SQLi, Command injection),
- social engineering,
- code injection using removable media,
- password guessing (online/offline),
- denial of service,
- man-in-the-middle,
- …

and 58 defense types, including;

- network intrusion detection (both detection and prevention-based),
- host intrusion detection systems,
- web application firewalls,
- anti-malware,
- firewalls,
- security training,
- encryption,
- software development best practice methods,
- network management (e.g., scanning, USB policy, etc),
- ...

[1] www.ics.kth.se/cysemol ----and--- www.ics.kth.se/eaat

[2] http://www.kic-innoenergy.com

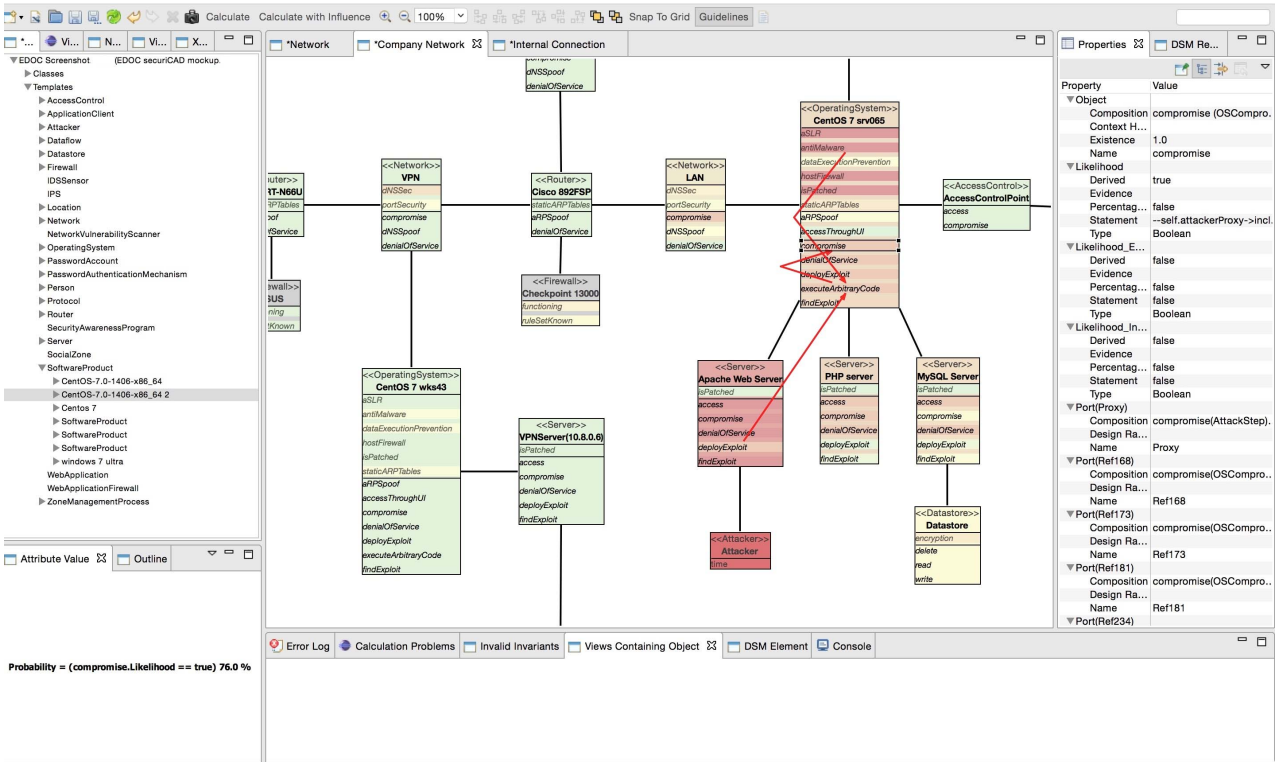

Figure 1. A screenshot from securiCAD showing an example model.

Some attacks, defenses, assets, and relations can be seen in the example model in Fig. 1.

Additional features of securiCAD are e.g. import of data, templates, and influence visualization.

Users of securiCAD can chose to import data from other tools in order to ease the modeling effort. Thus, instead of manually dragging and dropping objects and relationships, or setting values to different countermeasures, this information can be feed into securiCAD in XML format. This functionality has so far been tested and used in both various research setups and currently in a case with a large Nordic bank. Typical tools that can contain valuable information reusable for securiCAD are; network scanners, vulnerability scanners, firewall configuration tools, enterprise architecture tools, application databases et cetera.

Combining assets and relationships with pre-defined values can be saved as templates in order to support reuse, decrease modeling effort, and increase data accuracy. Also as a future feature we aim to provide a community based template sharing function, where users of the tool can upload their templates, download templates created by others, and iteratively enhance the templates. This sharing function can be used both internally within an enterprise using securiCAD and publicly for all to share. Templates can hold anything from lower level combinations of assets together representing e.g. a Windows 7 operating systems or higher level combinations describing an industrial SCADA system.

As a baseline securiCAD provides the user with a heat map using different colors representing the likelihood of an attacker reaching that asset using a certain attack type, e.g. red means very likely to succeed and green not very likely, and then various nuances/shades of red, yellow, and green. The user can also decide to investigate what the attack step(s) that are influencing a specific attack step. This is shown using red arrows. Thus, stepping through the model the user can follow how an attacker could travel through out the architecture to reach a certain point. In Fig. 1 you find four red arrows pointing to the **attack** *Compromise* of the **asset** named *CentOS 7 srv065* that is of the type <<Operating System>>. Succeeding with a compromise of this operating system, following the red arrows one step back, can be done through an *executeArbitraryCode* on the same operating system. Which in turn can be reached through *deployExploit* on the *Apache Web Server* <<Server>>. It is also influenced by the existence of the **defense** labeled *antiMalware.*

IV. Case Studies

During our ten years of research we have been doing case studies with numerous Swedish and international companies, such as Vattenfall, ABB, E.on, Fortum, Volvo, Scania, and Swedbank.

In the current innovation phase of foreseeti we are currently working with ABB, Eandis, Infrax, and Atos in two KIC InnoEnergy innovation projects, as well as with our first customer – a large Nordic bank.

REFERENCES

[1] McAfee, report center for strategic & international studies and Symantec, Norton Study, 2012

[2] Ponemon Institute, Cost of Cyber Crime reports, 2010-2013

[3] Verizon, Data breach investigations report, 2014

[4] Council, Federal Financial Institutions Examination, "Authentication in an internet banking environment," Financial Institution Letter, FIL-103-2005. Washington, DC: Federal Deposit Insurance Corp.(FDIC), 2005

[5] ECB, Recommendations for the Security of Internet Payments, 2013

[6] RAND, report H4cker5 wanted, 2014

[7] World Economic Forum, Partnering for Cyber Resilience Towards the Quantification of Cyber Threats, Industry Agenda, January 2015. http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf

[8] H. Holm, T. Sommestad, M. Ekstedt, and L. Nordström, "CySeMoL: A tool for cyber security analysis of enterprises," 22nd International Conference and Exhibition on Electricity Distribution (CIRED), 2013

[9] H. Holm, K. Shahzad, M. Buschle, and M. Ekstedt, "P2CySeMoL: Predictive, Probabilistic Cyber Security Modeling Language," IEEE Transactions on Dependable and Secure Computing, IEEE Computer Society, 2014

[10] M. Buschle, H. Holm, T. Sommestad, M. Ekstedt, and K. Shahzad, "A tool for automatic enterprise architecture modeling," IS Olympics: Information Systems in a Diverse World, 2012, pp. 1-15

[11] H. Holm, T. Sommestad, J. Almroth, and M. Persson, "A quantitative evaluation of vulnerability scanning," Information Management & Computer Security, 19(4), 2011, pp. 231-247

[12] T. Sommestad, "A framework and theory for cyber security assessments," PhD Thesis, Industrial Information and Control Systems, KTH Royal Institute of Technology, Stockholm, Sweden, 2012

[13] H. Holm, "A framework and calculation engine for modeling and predicting the cyber security of enterprise architectures," PhD Thesis, Industrial Information and Control Systems, KTH Royal Institute of Technology, Stockholm, Sweden, 2014

[14] M. Buschle, "Tool Support for Enterprise Architecture Analysis: with application in cyber security," PhD Thesis, Industrial Information and Control Systems, KTH Royal Institute of Technology, Stockholm, Sweden, 2014

[15] M. Välja, M. Korman, K. Shahzad, and P. Johnson, "Integrated metamodel for security analysis," 48th Hawaii International Conference on System Sciences (HICSS), 2015

[16] T. Sommestad, M. Ekstedt, and H. Holm, "The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures," Systems Journal, IEEE, 7(3), 2013, pp- 363-373

[17] H. Holm, M. Korman, and M. Ekstedt, "A bayesian network model for likelihood estimations of acquirement of critical software vulnerabilities and exploits," Information and Software Technology, vol. 58, 2015, pp. 304-318.

[18] H. Holm and M. Ekstedt, "A metamodel for web application injection attacks and countermeasures," Trends in Enterprise Architecture Research and Practice-Driven Research on Enterprise Transformation, 2012, pp. 198-217

[19] P. Johnson, R. Lagerström, P. Närman, and M. Simonsson, "Enterprise Architecture Analysis with Extended Influence Diagrams," Information Systems Frontiers, vol. 9, no. 2-3, 2007, pp. 163-180

[20] R. Lagerström, P. Johnson, and D. Höök, "Architecture Analysis of Enterprise Systems Modifiability: Models, Analysis, and Validation," Journal of Systems and Software, vol. 83, no. 8, 2010, pp. 1387-1403

[21] J. Ullberg, R. Lagerström, P. and Johnson, "A framework for service interoperability analysis using enterprise architecture models," IEEE International Conference on Services Computing (SCC'08), vol. 2, 2008, pp. 99-107

[22] J. Saat, U. Franke, R. Lagerström, and M. Ekstedt, "Enterprise Architecture Meta Models for IT/Business Alignment Situations," EDOC, 2010, pp. 14-23

[23] M. Simonsson, R. Lagerström, and P. Johnson, "A Bayesian network for IT governance performance prediction," Proc. of the 10th International Conference on Electronic Commerce, 2008

[24] R. Lagerström, C. Baldwin, A. MacCormack, and S. Aier, "Visualizing and Measuring Enterprise Application Architecture: An Exploratory Telecom Case," Proc. of the 47th Hawaii International Conference on System Sciences (HICSS), 2014, pp. 3847-3856

[25] K. Ingols, M. Chu, R. Lippmann, S. Webster, and S. Boyer, "Modeling modern network attacks and countermeasures using attack graphs," Annual Computer Security Applications Conference (ACSAC'09), 2009, pp. 117–126

[26] H. Huang, S. Zhang, X. Ou, A. Prakash, and K. Sakallah, "Distilling critical attack graph surface iteratively through minimum-cost sat solving," Proc. of the 27th Annual Computer Security Applications Conference, ACSAC'11, ACM, New York, NY, USA, 2011, pp. 31–40

[27] X. Ou, W. F. Boyer, and M. A. McQueen, "A scalable approach to attack graph generation," Proc. of the 13th ACM conference on Computer and communications security, CCS '06, ACM, New York, NY, USA, 2006, pp. 336–345

[28] S. Jajodia, S. Noel, and B. O'Berry, "Topological analysis of network attack vulnerability," Managing Cyber Threats, Springer, 2005, pp. 247–266

[29] A. J. A. Wang, "Information security models and metrics," Proc. of the 43rd annual Southeast regional conference-Volume 2, ACM, 2005, pp. 178–184

[30] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the octave approach," Pittsburgh, PA, Carnegie Mellon University

[31] F. den Braber, I. Hogganvik, M. S. Lund, K. Stølen, and F. Vraalsen, "Model-based security analysis in seven steps: a guided tour to the coras method," BT Technology Journal 25(1), 2007, pp. 101–117

[32] CCRA, Common Criteria for Information Technology Security Evaluation, Available on http://www.commoncriteriaportal.org/, accessed August 11, 2015 (2012)

[33] R. Breu, F. Innerhofer-Oberperfler, and A. Yautsiukhin, "Quantitative assessment of enterprise security system," Proc. of the Third IEEE International Conference on Availability, Reliability and Security (ARES), 2008, pp. 921–928