Security Officers Management & Analysis Project (SOMAP)

By Russ McRee

Prerequisites

Java

Similar Projects

OCTAVE http://www.cert.org/octave/methodintro.html
CORAS http://www2.nr.no/coras/

The Security Officers Management & Analysis Project (SOMAP) and its offerings represent a strengthening trend in the information security space: risk assessment and risk management as the core of the enterprise security framework. You have likely encountered this well studied and documented formula: Risk = Threat x Vulnerability, and perhaps variations inclusive of cost or asset value. This rather fundamental formula is the basis for SOMAP methodology, but only just begins to shape the process. Algorithmic science, applied by bright academicians, can further the study of risk and calculating the value of assets. Read Dantu and Kolan's *Risk Management Using Behavior Based Bayesian Networks*. ISSA members should be familiar with ISSA Hall of Fame member Thomas Peltier's work regarding the Facilitated Risk Analysis Process (FRAP), best illustrated in his book *Information Security Risk Analysis*.

What CISSP, or those studying for it, is not painfully familiar with Annualized Rate of Occurrence (ARO), Business Impact Analysis (BIA), or Exposure Factor (EF), and Single Loss Expectancy (SLE)? OMG, I'm losing my MIND (Multiple Initialisms Noted Disorder).

Consider the burgeoning Common Vulnerability Scoring System (CVSS): *"CVSS helps organizations prioritize and coordinate a joint response to security vulnerabilities by communicating the base, temporal and environmental properties of vulnerability."* [1] This approach will allow a business to more precisely manage risk based on their specific environments. Imagine the difference between two businesses, one that exposes known Oracle vulnerabilities to the Internet and one that carefully isolates their Oracle installation behind multiple protective layers, such that even if vulnerable, their data base is at no where near the same level of risk as its internet-exposed counterpart. The resulting "grades" these disparate systems would receive in a well conducted risk assessment would obviously be quite different, as would their environmental CVSS score. But, I digress.

Project highlights

I spoke with Adrian Wiesmann from SOMAP and he offered some project highlights you may find interesting.

- As a small team, there is much to do, and every helping hand is welcome. There is the possibility for CISSPs to earn CPEs helping the SOMAP project.
- SOMAP is currently finishing version 1 of the SOBF Tool which contains basic functionality to do risk assessments. They are already working on version 2 which will enhance the features finalized in version 1. Their intent has always been to design the SOBF Tool as a shell or framework where users can change and extend the many features of the SOBF Tool, such as parts of the UI, the assessment workflow, calculations, etc. They took the liberty to test different UIs and ideas and now that the preferences are finalized, they will work towards a new, clean architecture and source. Consider it as a prototype first (v1) and a clean implementation later (v2).
- Version 1 of their *Handbook* and *Guide* were published some time ago and both documents need some further attention. Some topics are not covered yet and the text will be significantly updated in pending versions.
- They are currently concentrating on the Reports for version 1 of the SOBF Tool. This is taking some time because they not only need to define what kind of reports to offer, but formatting details as well. The project would appreciate feedback here.
- While they have a roadmap, they do not currently have any communicated release dates. As a small team working on SOMAP in their spare time, it is difficult to commit to specific dates.

Consider the SOMAP Project one to be watched closely for further development, well worthy of bookmarking and visiting regularly.

1 http://www.first.org/cvss/

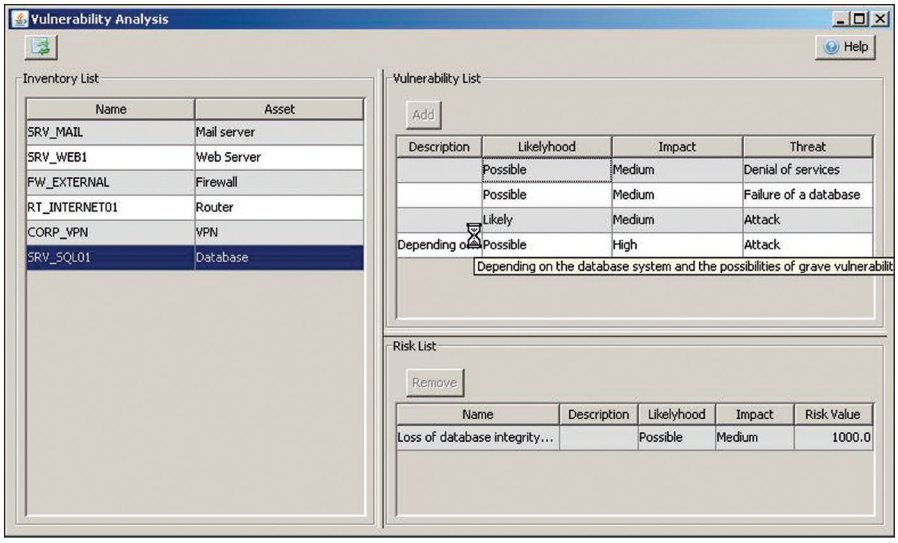

Figure 1 – Context Establishment – Vulnerability Analysis

Security Officers Best Friend (SOBF)

Designed to be the management portal and data repository for your risk assessment, the Security Officers Best Friend (SOBF) is a Java-based tool, currently still beta, which divides your effort into three stages:

1. Context establishment
2. Risk retention
3. Risk treatment

Context establishment

In this phase you will Collect Data (asset inventory and classification) or apply a Rapid Risk Assessment if you do not inventory item descriptions and details. You can then pull an Inventory Report, conduct a Threat Analysis, review the Threat Analysis Report, conduct a Vulnerability Analysis, and finally review the Vulnerability Analysis Report.

Collect Data will offer you an Asset List to assign to your qualitative inventory items, including routers, firewalls, mail servers, web servers, etc.

When carrying out your Threat Analysis, you will choose from a list of Potential Threats including items like Failure of a Database, Intrusion, Insufficient Monitoring of IT Security Measures, and Denial of Services. Once complete, you can then begin the Vulnerability Analysis and apply Likelihood, Impact, and Threat to each of your assets.

Remember, you can execute rudimentary reports after the Inventory, Threat Analysis, and Vulnerability Analysis phases.

Risk retention

The Risk Retention phase includes Risk Identification, Estimation, Evaluation, as well as a simple report page.

Risk Estimation includes qualitative values assigned to your assets, based on the likelihood and impact of threats realized against assets. You will note a Risk Financing feature that will be available in the next release.

Risk treatment

During Risk Treatment you will render the Controls Report, which offers mitigation safeguards discovered during the Context Establishment and Risk Retention phases. Pending the release of version 1, you will also find a checklist feature intended to "produce checklists for owners and custodians of Inventory Items. These checklists are used to manage the implementation and maintenance of Controls."

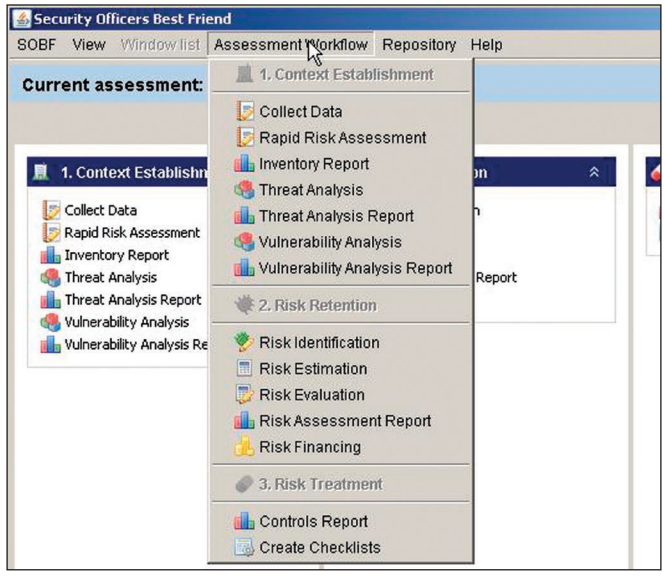

Figure 3 – Assessment Workflow

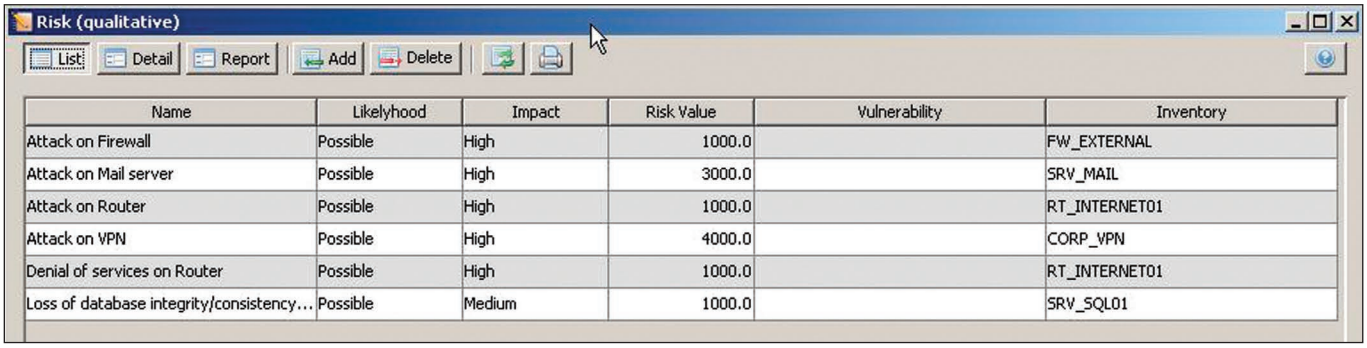

Figure 2 – Risk Retention, Risk Estimation

SOMAP Open Information Security Risk Management Handbook

This 26 page text was published in September 2006, and as indicated earlier, can use some attention. To be fair, the English translation is a bit rough in places (the active project leads are Swiss) but they get an A+ for effort and the intent is excellent. This text is geared towards upper management, and is thoughtfully and concisely laid out. The SOMAP project docs might benefit from an editor to help tidy up a bit.

Highlights include definitions of risk, risk management, and risk mitigation, as well as clarifications of the proactive versus reactive approach and prioritization.

SOMAP Open Information Security Risk Assessment Guide

The *Assessment Guide* is longer, more detailed, and while suffering from the same issues as the *Handbook*, offers some great methodology for the assessor. This document is really the workflow that you will find built into the SOBF Tool and works well as a companion piece.

The *Guide* includes lots of discussion about ISO standards, current and pending, risk calculation formulas (both qualitative and quantitative), and all the common elements of a complete risk assessment.

ORIMOR

The SOMAP project believes that a comprehensive repository of best practice rules and guidelines is critical to the assessment and management of information security. To that end they have built and maintain an open database of these rules and guidelines. They refer to it as the Open Risk Model Repository (ORIMOR) and it is made available under their unique ORIMOR License. Additionally, the SOMAP team embraces the "garbage in, garbage out" mindset with regard to risk assessment. The assessor makes assumptions about likelihood, impact, asset values, etc., often based on instinct. One of the team goals is to populate ORIMOR with values which are "known good" and which are "validated by peers."

There is also the prospect of investigating the use of third party data like the OSVDB,[2] to prepare better default values for a risk assessment. Better, in this case, means "closer to reality" and therefore reduces the "garbage-in" factor. The ORIMOR database is included in the SOBF Tool and can be queried under Repository.

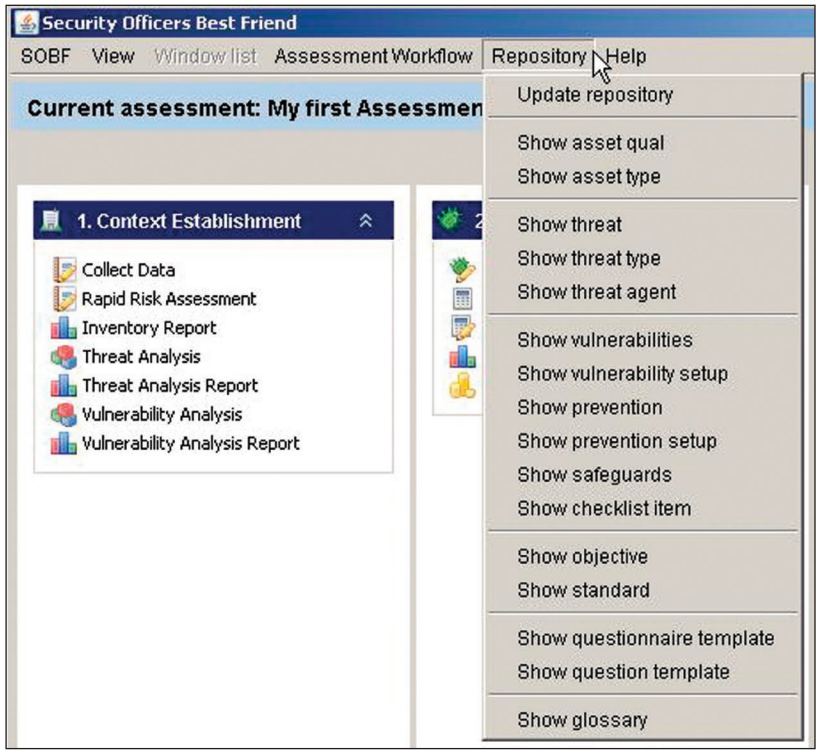

Figure 4 – ORIMOR Repository

Benefits and drawbacks

The benefits of a well-conducted risk assessment are immediate, including better understanding of your assets, your risk posture, and identification of ways to improve your exposure. The process can be daunting, requires commitment, and can lead to debate over methodology, particularly when faced with qualitative or quantitative approaches. Time is your biggest cost; you do not need expensive tools to execute a sound risk assessment.

In conclusion

Clearly denoted as an open source project, and release under the GNU GPL v2, SOMAP wants to "*define and freely distribute a Repository of Best Practices in Risk Management. We therefore chose the Open Source way as our method of operation.*" Far be it from me to argue with that logic. This is a great start on a project with great potential, focused on a discipline in its ascension to its rightful place in the larger framework of information assurance. Cheers…until next month.

Acknowledgments

Adrian Wiesmann of SOMAP for his feedback and insight.

About the Author

Russ McRee, GCIH, CISSP, is a security analyst working for Expedia. He is a member of numerous security organizations and maintains holisticinfosec.org. Contact him at russ@holisticinfosec.org.

2 Open Source Vulnerability DataBase – http://osvdb.org/

