SimpleRisk: Enterprise Risk Management Simplified

COMMENT?

By Russ McRee – ISSA Senior Member, Puget Sound (Seattle), USA Chapter

Prerequisites/dependencies

LAMP/XAMPP server

Our editorial theme for February's *ISSA Journal* happens to be "Risk, Threats, and Vulnerabilities," which means that Josh Sokol's SimpleRisk as our *toolsmith* topic is bona fide kismet. I am a major advocate for simplicity,[1] and as the occasional practitioner of simpleton arts, SimpleRisk fits my needs perfectly. SimpleRisk is a free and open source web application, released under Mozilla Public License 2.0, and is extremely useful in performing risk management activities. In my new role at Microsoft, I'm building, with a fine team of engineers, a Threat Intelligence and Engineering practice. This effort is intended to be much more robust than what you may currently understand to be threat intelligence. Limiting such activity to monitoring threat feeds, deriving indicators of compromise, and reporting out findings is insufficient to cover the vast realm of risk, threats, and vulnerabilities. As such, we include constant threat assessments of our infrastructure and services in a manner that includes risk analysis and threat modeling, based on SDL principles[2] and the infrastructure threat modeling guidance[3] I wrote some years ago. Keeping in mind that threat modeling can be software-centric, asset-centric, and attacker-centric, recognize that the amount of data you generate can be overwhelming. In addition to embracing the principles of good data science, we've also expanded our tooling to include the likes of SimpleRisk. I asked Josh to provide us with insight on SimpleRisk in his own words:

> "As security professionals, almost every action we take comes down to making a risk-based decision. Web application vulnerabilities, malware infections, physical vulnerabilities, and much more all boil down to some combination of the likelihood of an event happening and the impact of that event. Risk management is a relatively simple concept to grasp, but the place where many practitioners fall down is in the tool set. The lucky security professionals work for companies who can afford expensive GRC tools to aide in managing risk. The unlucky majority out there usually end up spending countless hours managing risk via spreadsheets. It's cumbersome, time consuming, and just plain sucks. After starting a risk management program from scratch at a $1B-a-year company, I ran into these same barriers, and when budget wouldn't allow me the GRC route, I finally decided to do something about it. At Black Hat and BSides Las Vegas 2013, I formally debuted SimpleRisk. A SimpleRisk instance can be stood up in minutes and instantly provides the security professional with the ability to submit risks, plan mitigations, facilitate management reviews, prioritize for project planning, and track regular reviews. It is highly configurable and includes dynamic reporting and the ability to tweak risk formulas on the fly. It is under active development with new features being added all the time and can be downloaded at simplerisk.org.[4] SimpleRisk is truly enterprise risk management simplified."

I can tell you with certainty that a combination of tactics, techniques, and procedures inclusive of threat modeling and analysis, good data science (read *The Field Guide to Data Science*[5]), and risk management with the likes of SimpleRisk will lead to an improved security posture. I'll walk you through a recreation of various real-world scenarios and current events using SimpleRisk after some quick installation pointers.

Quick installation notes

I run SimpleRisk on an Ubuntu 13.10 virtual machine configured with a full LAMP stack. Without question you should read the *SimpleRisk LAMP Installation Guide*,[6] but I'll give you a quick overview of my installation steps, establishing SimpleRisk as the primary application in the Apache web root:

1. `cd /var/www`
2. Download the latest installation bundle, currently (subject to change): `sudo wget http://simplerisk.googlecode.com/files/simplerisk-20131231-001.tgz`
3. `sudo tar zxvf simplerisk-20131231-001.tgz`
4. `sudo mv simplerisk/ * .` (moves all SimpleRisk app files to the web root)
5. `sudo rm simplerisk-20131231-001.tgz` (removes the installation bundle)

1 http://holisticinfosec.org/simplicity-mainmenu-28.
2 http://www.microsoft.com/security/sdl/adopt/threatmodeling.aspx.
3 http://technet.microsoft.com/en-us/library/dd941826.aspx.
4 http://www.simplerisk.org.
5 http://www.boozallen.com/insights/insight-detail/data-science-field-guide.
6 http://simplerisk.googlecode.com/files/SimpleRisk LAMP Installation Guide.pdf.

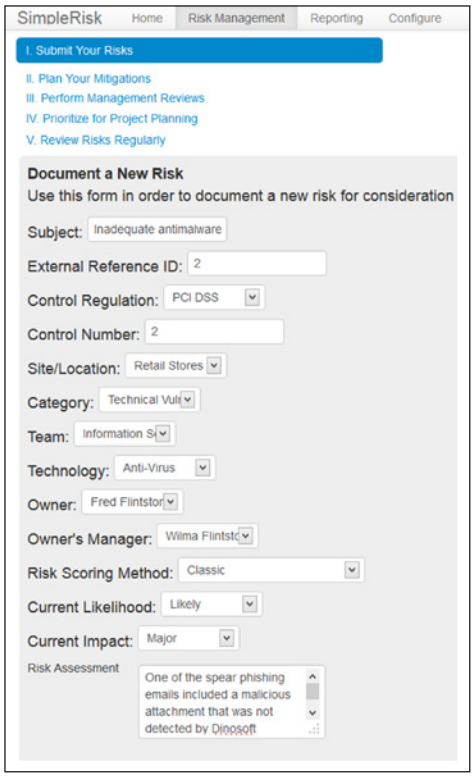

Figure 1 – Fred submits risk for SimpleRisk documentation

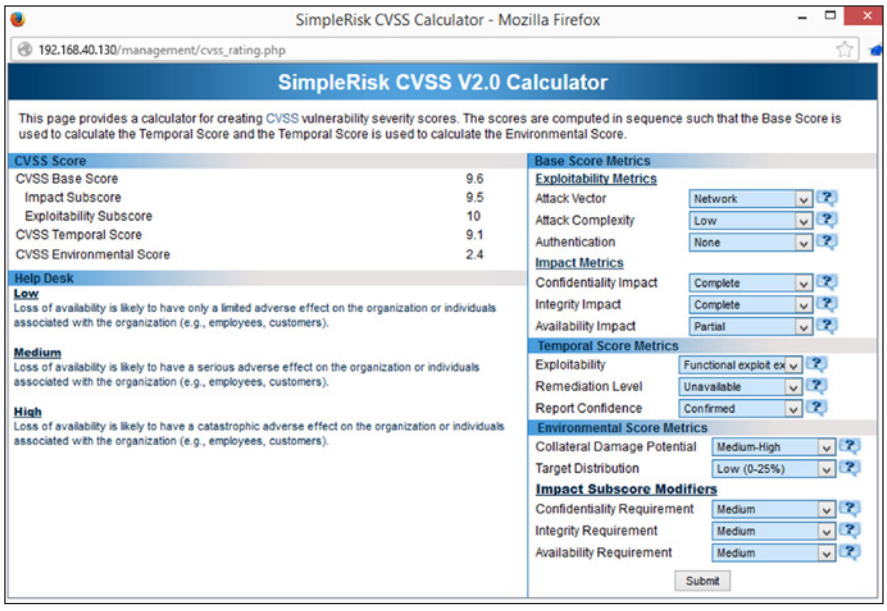

Figure 2 – Fred calculates a CVSS score with SimpleRisk CVSS calculator

6. `sudo rm simplerisk` (removes the now empty simplerisk directory)
7. `cd ~`
8. Download the SimpleRisk database import: `wget http://simplerisk.googlecode.com/files/simplerisk-20131231-001.sql`
9. `mysql –u root -p`
10. create database simplerisk;
11. use simplerisk;
12. source ~/simplerisk-20131231-001.sql (populates the SimpleRisk database)
13. GRANT SELECT, INSERT, UPDATE, DELETE ON simplerisk.* TO 'simplerisk'@'localhost' IDENTIFIED BY 'CHANGEME'; (creates the SimpleRisk database user, change CHANGEME to your preferred password)
14. exit
15. `sudo gedit /var/www/includes/config.php`
16. Edit line 16 with the database password you set in step 13 (you can also change your timezone in config.php)
17. Browse to your web server's root and login as admin with password admin
18. Click the *Admin* button in the upper right of the UI then click *My Profile*
19. Change the admin password!

SimpleRisk and the Flintstones

Flintstone, Inc., a prehistoric cave retailer with a strong online presence, has been hacked by the Bedrock Electronic Militia. In one breach, 40 million clams had been stolen, and soon thereafter it was revealed that 70 million additional clams were compromised. Additionally, the attackers used social engineering to gain access to the Flintstone, Inc. social media accounts, including Critter and Cavebook, as well as the Flintstone, Inc. blog. Even the Bedrock news media outlet, *Cave News Network*, is not immune to Bedrock Electronic Militia's attacks. Fred and Wilma, the CISO and CEO, are very concerned that their next PCI audit is going to be very difficult, given the breach, and they want to use SimpleRisk to track and manage the risks they need to mitigate, as well as the related projects necessary to fulfill the mitigations.

The SimpleRisk admin has created two accounts for Fred and Wilma; they're impressed with the fact that the *User Management* options under *Configure* are so granular specific to *User Responsibilities*, including the ability to *Submit New Risks*, *Modify Existing Risks*, *Close Risks, Plan Mitigations, Review Low Risks, Review Medium Risks, Review High Risks*, and *Allow Access to "Configure" Menu*.

Fred and Wilma are also quite happy that the SimpleRisk user interface is so…simple. Fred first uses the *Configure* | *Add* and *Remove Values* menu to add Online and Retail Stores as Site/Location values, given the variety and location of risks identified. He also adds Identity Management under *Team*, as well as POS and Proxy under *Technology*. Fred notes that the *Configure* menu also offers significant flexibility in establishing risk formula preferences, review (high, medium, low) settings, and the ability to redefine naming conventions for impact, likelihood, and mitigation efforts. He and Wilma then immediately proceed to the *Risk Management* menu to, you guessed it, begin to manage risks exposed during the breach root-cause analysis and after-action report.

To get started the Flintstones immediately identify five risks to document:

1. **Account compromise via social engineering**

Below is the list of submitted risks that require mitigation planning.

ID	Status	Subject	Risk	Submitted	Mitigation Planned	Management Review
1004	New	Flintstone.com web application vulnerable to cross-site scripting (XSS)	10	2014-01-27 22:42:03	No	No
1001	New	Account compromise via social engineering	6.4	2014-01-27 22:16:03	No	No
1002	New	Inadequate antimalware detection	6.4	2014-01-27 22:19:25	No	No
1005	New	Flintstone, Inc. Point Of Sale (POS) compromised with Frack POS malware	5	2014-01-27 22:44:20	No	No
1003	New	Flintstone, Inc. users compromised via watering hole attacks	2.4	2014-01-27 22:33:17	No	No

Figure 3 – SimpleRisk risk ranking allows mitigation prioritization

   a. The Flintstone.net Critter and Cavebook accounts were compromised when one of their social media management personnel was spearphished

2. **Inadequate antimalware detection**
   a. One of the spearphishing emails included a malicious attachment that was not detected by Dinosoft Security Essentials
3. **Flintstone, Inc. users compromised via watering hole attacks**[7]
   a. A lack of egress traffic analysis, detection, and prevention from Flintstone, Inc. corporate networks meant that users were compromised when enticed to visit a known good website that had been compromised with the Blackrock Exploit Kit
4. **Flintstone.com web application vulnerable to cross-site scripting (XSS)**
   a. Attackers can use XSS vulnerabilities to deliver malicious payloads in a more trusted manner, given that they execute in the context of the vulnerable site
5. **Flintstone, Inc. point of sale (POS) compromised with Frack POS malware**
   a. All POS devices must be scanned with the SecureSlate's Frack POS Malware Scan

As seen in figure 1, Fred can be very specific in his risk documentation.

As Fred works on the watering hole risk, he decides he'd rather use CVSS risk scoring than classic and is overjoyed to discover that SimpleRisk includes a CVSS calculator as seen in figure 2. There is also an OWASP calculator the Fred uses when populating the XSS risk, and a DREAD calculator he uses for the POS risk.

When Fred and Wilma move to the *Plan Your Mitigations* phase, they are a bit taken aback to find that SimpleRisk has stack ranked the XSS risk as the highest, as seen in figure 3, but they recognize that risk calculations can be somewhat subjective and that each scoring calculator (CVSS, DREAD, OWASP) derives scores differently. SimpleRisk does include links to references for how each is calculated.

Fred and Wilma believe that the XSS vulnerability happens to be one they can have mitigated rather quickly and at a low cost, so they choose to focus there first. Clicking *No* under *Mitigation Planned* for ID 1004 leads them to the *Submit Risk Mitigation* page. They submit their planned mitigation as seen in figure 4.

After SimpleRisk accepts the mitigation, Fred and Wilma are sent promptly to the *Perform Management Reviews* phase where they choose to review ID 1001 Account Compromised via social engineering by clicking *No* in the related row under the *Management Review* column. Under *Submit Management Review* they choose to *Approve Risk* (versus reject), *Consider for Project* as the Next Step and add Deploy two-factor authentication under *Comments*.

Under *Prioritize for Project Planning*, Fred and Wilma then add a new project called Two Factor Authentication Deployment. They can add other projects and prioritize them later. They also set a schedule to review risks regularly after plan-

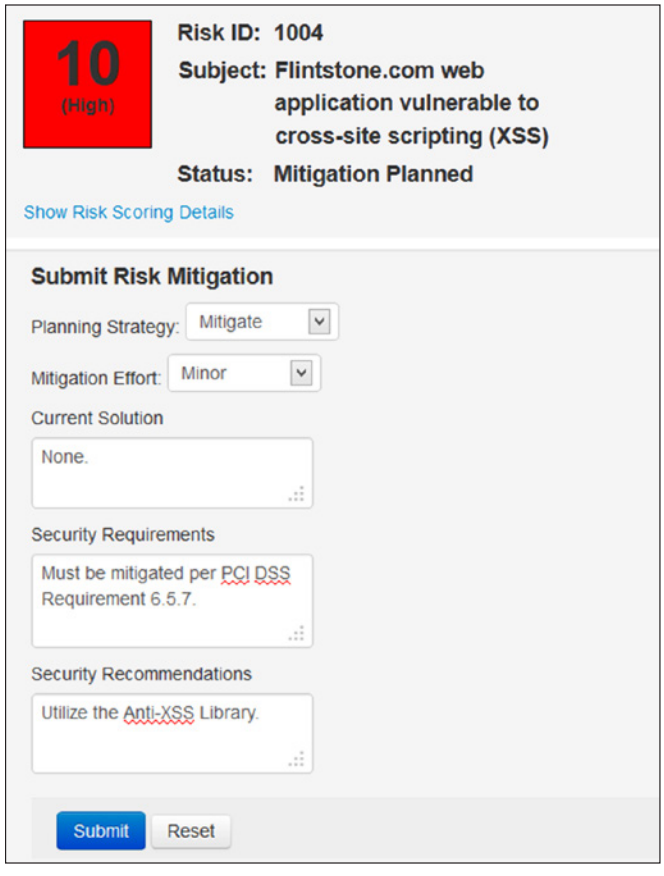

Figure 4 – SimpleRisk XSS mitigations submittal

7 http://about-threats.trendmicro.com/RelatedThreats.aspx?language=au&name=Watering+Hole+101.

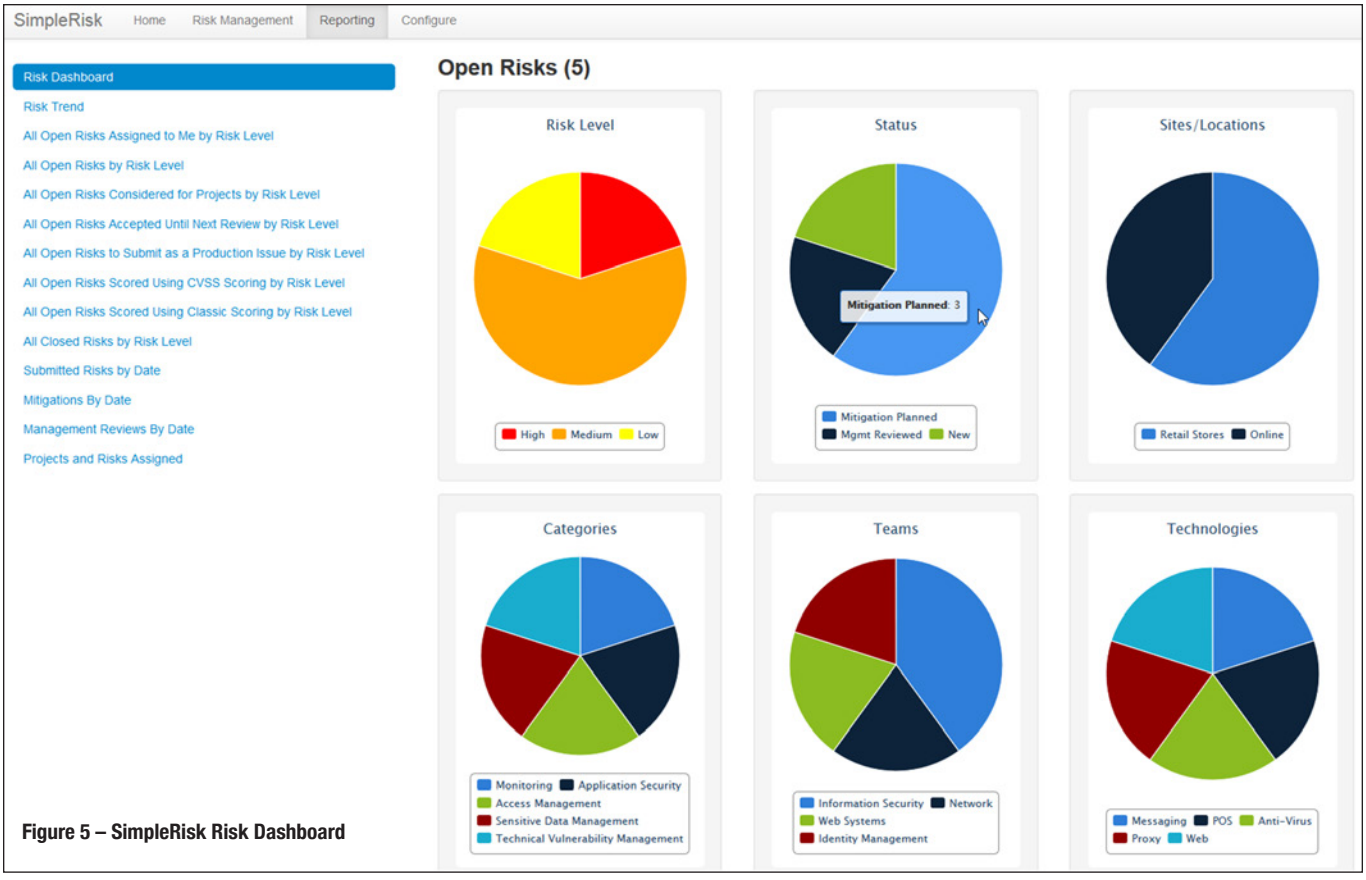

Figure 5 – SimpleRisk Risk Dashboard

ning mitigations for, and a conducting reviews of, their remaining risks.

As the CISO and CEO of Flintstone, Inc., Fred and Wilma love their executive dashboards. They check the SimpleRisk Risk Dashboard under *Reporting*, as seen in figure 5.

They also really appreciate that SimpleRisk maintains an audit trail for all changes and updates made.

Finally, Fred and Wilma decide to take advantage of some SimpleRisk "extras" that cost a bit but are offered under a perpetual license:

- **Custom authentication extra:** Currently provides support for Active Directory Authentication and Duo Security multi-factor authentication, but will have other custom authentication types in the future.
- **Team-based separation extra:** Restriction of risk viewing to team members the risk is categorized as.
- **Notification extra:** Email notifications when risks are updated or due for action.
- **Encrypted database extra:** Encryption of sensitive text fields in the database.

In conclusion

Josh has devised a great platform in SimpleRisk; I'm really glad to have caught mention of it rolling by in Twitter reads. It fits really nicely in any threat/risk management program. On a related note, as I write this Adam Shostack's new book, *Threat Modeling: Designing for Security*,[8] is nearing its publication date (17 FEB 2014, Wiley). Be sure to grab a copy and incorporate its guidance into your risk, threat, and vulnerability management practice along with the use of SimpleRisk.

Ping me via email if you have questions or suggestions for topic via russ at holisticinfosec dot org or hit me on Twitter @holisticinfosec.

Cheers…until next month.

Acknowledgements

—Josh Sokol, SimpleRisk developer and project lead

About the Author

Russ McRee manages the Threat Intelligence & Engineering team for Microsoft's Online Services Security & Compliance organization. In addition to toolsmith, he's written for numerous other publications, speaks regularly at events such as DEFCON, Black Hat, and RSA, and is a SANS Internet Storm Center handler. As an advocate for a holistic approach to the practice of information assurance Russ maintains holisticinfosec.org. He serves in the Washington State Guard as the Cybersecurity Advisor to the Washington Military Department. Reach him at russ at holisticinfosec dot org or @holisticinfosec.

8 http://www.amazon.com/Threat-Modeling-Designing-Adam-Shostack/dp/1118809998/ref=sr_1_1?ie=UTF8&qid=1390788711&sr=8-1&keywords=Threat+Modeling%3A+Designing+for+Security.