Rapid Risk Assessments

a lightweight approach
to measuring risks
and modeling threats

Julien Vehent - Sec4Dev 2021

Sam and Mark are building a file sharing app

They want everyone to share stuff easily and securely.

They have a few ideas on wireframe and a very early webapp prototype.

They want Android and iPhone apps as well.

And monetization for heavy sharing.

But they’re concerned about security...

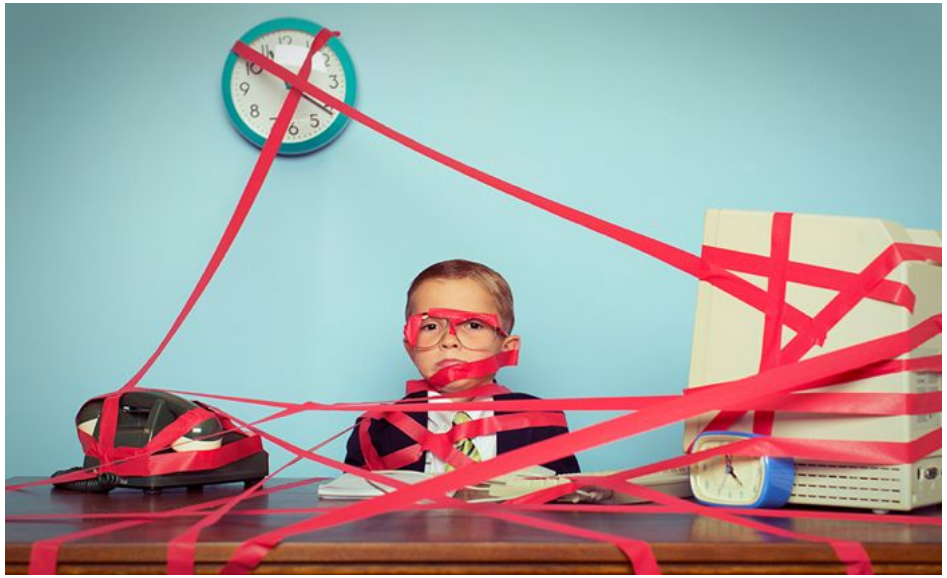
Sam and Mark work for a software company

And lately, internal processes have become more and more painful.

They've heard that review can take weeks. And that launching "prototypes" is getting harder and harder.

So they are a bit worried about asking for a security review.

But they could really use the help, so they try anyway.



They meet Jim, a security engineer

He’s mumbling something about “PGP”.

Doesn’t get why people don’t use “Age”.

Rants about something called “memory unsafe languages”.

He looks like he could use a vacation.

But he’s friendly enough.

Sam, Mark and Jim schedule a 1h meeting to discuss the file sharing project.

Jim says he'll use something called "Rapid Risk Assessment", or RRA.

Not ARR, that's for pirates. RRA.

Phase 1: Information Gathering

Jim asks for an overview of the project:

- Who owns, developers and operate the service?
- Who is the audience? Internal? Public?
- What are the user stories?
  - *Moana wants to share a large PDF with her Dad who doesn't know anything about computers. She uploads the PDF to the service and sends a link and a password to her dad.*
- How is it built? Is there a design doc? Diagrams?
  - *Python backend hosted in a container. Object storage in AWS S3. Postgres database. Frontend in React.*

Phase 1: Information Gathering

- High-level understanding
- **DON’T** go into details
- Assess investment level

  (prototype/experiment vs major effort)
- Ask relevant questions
- Take good notes
- Capture all links
- **Listen** more than you speak
- Foster a pleasant conversation

Phase 2: Data Dictionary

Jim the prototype. Now he wants to know what data it'll be manipulating.

Designation	Classification	Description
User Account	Internal	Associated user account.
User Data	Restricted	User-submitted data.
Data Id	Internal	ID of data in DB.
Password	Secret	Password that protects the submitted data and is not stored or seen by the service.
Data Telemetry	Internal	Statistics on user data, such as download count, access logs, etc.

Data Classification

Sam and Mark don’t understand those data classification levels. Jim explains that they represent data access level for the entire company:

- **Public**: everyone inside and outside the company
- **Internal**: everyone inside the company
- **Restricted**: small groups or teams within the company
- **Secret**: data owner and specific individuals

Phase 3: Threat Scenarios

Jim understands context and data. Know it’s time to model threats.

Based the CIA model: Confidentiality, Integrity and Availability.

For each area, they evaluate:

- How would an attacker abuse or break into the service?
- How would it affect the company’s reputation? finance? overall ability to conduct business?
- How likely is it to happen?

Ships are safe in harbor.
But that's not what
ships are for.

Phase 3: Threat Scenarios

Confidentiality

- Threat: *Insecure storage exposes user data.*
- Impact: **HIGH** *Service is advertised as secure file sharing. Leaking data could put users at risk, would break trust and damage reputation. Password mitigates but perhaps not sufficiently.*

Integrity

- Threat: *Attacker replaces legitimate files with ransomware.*
- **HIGH** *Break the security guarantee to end users. Would put users at risk. Perhaps even create legal risk to company.*

Availability

- **Threat:** *Attacker targets the service with a denial of service.*
- **MEDIUM** *Would impact reputation and long term goal to monetize.*

What are those impact levels?

Sam and Mark don’t really understand those levels. Jim explains that an impact scale has been defined by executives for the entire company:

- **Low**: Loss <$100k, up to 10k users impacted, no media coverage
- **Medium**: Loss <$1M, up to 100k users, media coverage in tech news
- **High**: Loss <$10M, up to 1M users, broad media coverage
- **Critical**: Loss >$10M, over 1M users, sustained reputational damage, potential legal risks.

What are those impact levels?

Most engineers / managers underestimate the amount of risk an organization is willing to take. They tend to categorize low impact as high, and medium impact as critical.

Only way to avoid this is to define impact levels that are specific to your organization.

Ideally, get the executive team to dictate them. At a minimum, have them review and sign-off.

Phase 4: Recommendations

Based on the threats ranked by impact, how could the design be changed to mitigate at the lowest possible cost?

This is where Jim makes design recommendations that are appropriate and realistic. Sam & Mark happily contribute to the brainstorming.

Recommendation

- **High** *Encrypt data client-side in the browser using a symmetric AES GCM 256 bits key stored in URL anchor.*

  `https://share.foo.com/myfile123#c2VjcmV0a2V5Cg==`

And that’s the end of the RRA

Sam & Mark leaves the meeting with a solid set of recommendations and a plan to move forward. They’re pretty satisfied.

But Jim’s work isn’t yet done.

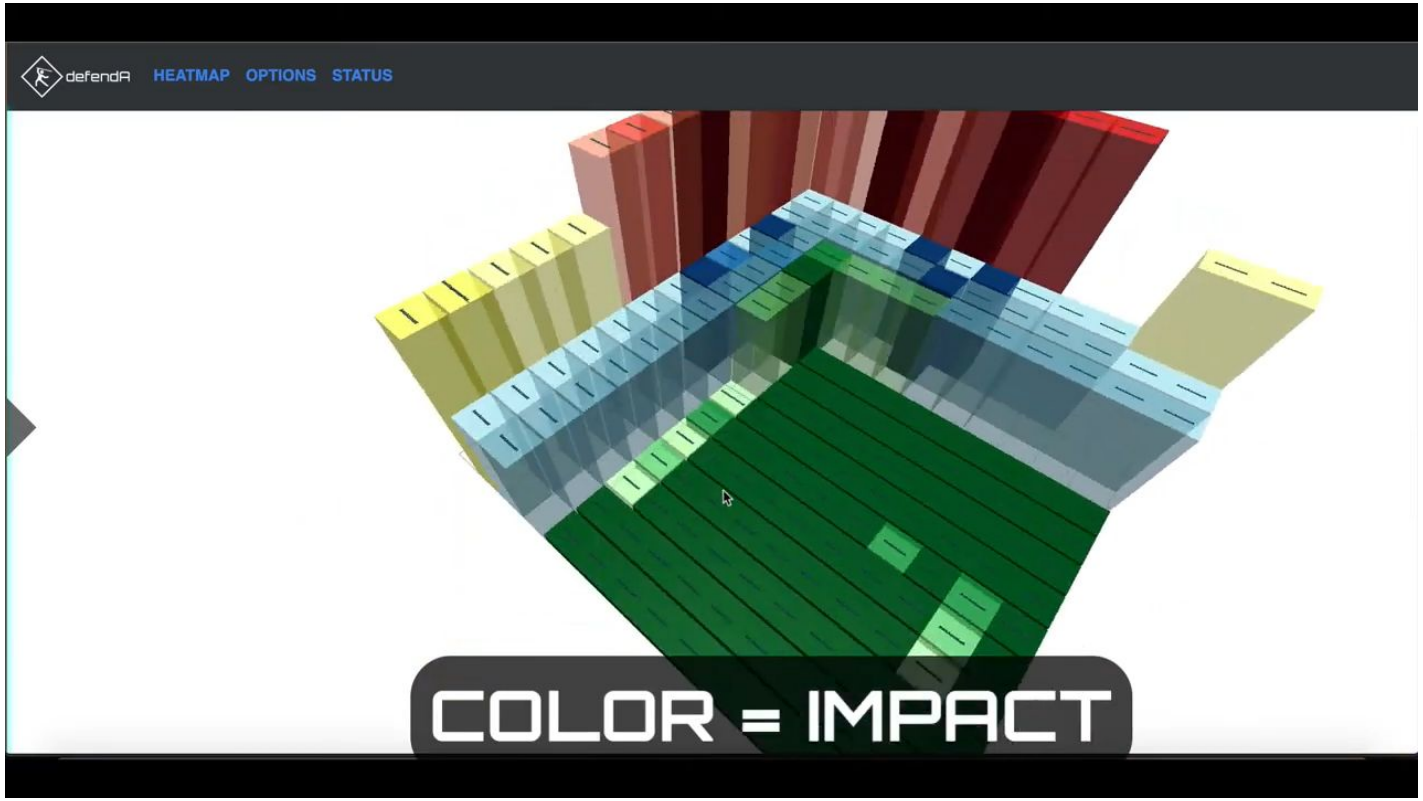
Bonus: Risk Register

RRAs are great to create a culture of security within an organization. But all those assessments need to be followed-up on. Risks categorized. Recommendations tracked.

This is what

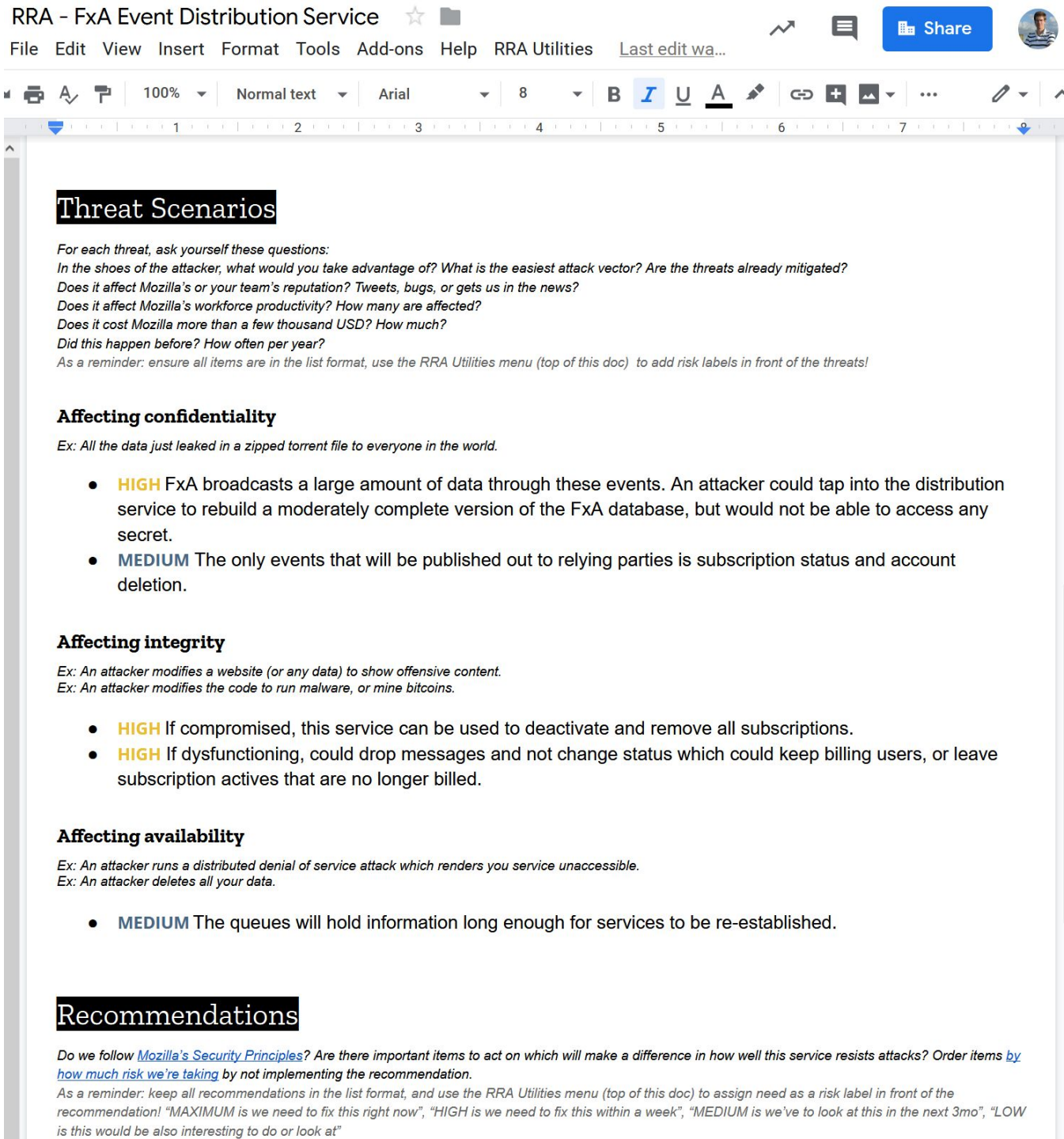
Risk Registers

are for.



Rapid
Risk
Assessments

mzl.la/2mkWN37



RRA - FxA Event Distribution Service

File Edit View Insert Format Tools Add-ons Help RRA Utilities Last edit wa...

Share

100% Normal text Arial 8

Threat Scenarios

For each threat, ask yourself these questions:
In the shoes of the attacker, what would you take advantage of? What is the easiest attack vector? Are the threats already mitigated?
Does it affect Mozilla's or your team's reputation? Tweets, bugs, or gets us in the news?
Does it affect Mozilla's workforce productivity? How many are affected?
Does it cost Mozilla more than a few thousand USD? How much?
Did this happen before? How often per year?
As a reminder: ensure all items are in the list format, use the RRA Utilities menu (top of this doc) to add risk labels in front of the threats!

Affecting confidentiality

Ex: All the data just leaked in a zipped torrent file to everyone in the world.

- HIGH FxA broadcasts a large amount of data through these events. An attacker could tap into the distribution service to rebuild a moderately complete version of the FxA database, but would not be able to access any secret.
- MEDIUM The only events that will be published out to relying parties is subscription status and account deletion.

Affecting integrity

Ex: An attacker modifies a website (or any data) to show offensive content.
Ex: An attacker modifies the code to run malware, or mine bitcoins.

- HIGH If compromised, this service can be used to deactivate and remove all subscriptions.
- HIGH If dysfunctioning, could drop messages and not change status which could keep billing users, or leave subscription actives that are no longer billed.

Affecting availability

Ex: An attacker runs a distributed denial of service attack which renders you service unaccessible.
Ex: An attacker deletes all your data.

- MEDIUM The queues will hold information long enough for services to be re-established.

Recommendations

Do we follow Mozilla's Security Principles? Are there important items to act on which will make a difference in how well this service resists attacks? Order items by how much risk we're taking by not implementing the recommendation.
As a reminder: keep all recommendations in the list format, and use the RRA Utilities menu (top of this doc) to assign need as a risk label in front of the recommendation! "MAXIMUM is we need to fix this right now", "HIGH is we need to fix this within a week", "MEDIUM is we've to look at this in the next 3mo", "LOW is this would be also interesting to do or look at"

Get in Touch

twitter: @jvehent
web: jvehent.org
email: julien@vehent.org