What I Found When Modelling Threats

In The Open (Source)

Dan Conn
Developer Advocate, Sonatype

About Me

- Developer Advocate for Sonatype
- Worked as a developer for 10 years, mainly writing Java, PHP, Python and Ruby
- Interested in cybersecurity for just as long
- Postgrad Certificate in Advanced Security and Digital Forensics from Edinburgh Napier.
- Not an Australian rugby player, that's another Dan Conn!

Twitter: @danjconn
Mastodon: https://defcon.social/@danjconn
Instagram: @dan_j_conn
GitHub: @danjconn
LinkedIn: danconn
Website: danconn.dev

sonatype

My OWASP Journey


HOW DO YOU DO,
MUSIC BAND
FELLOW APPSEC KIDS?

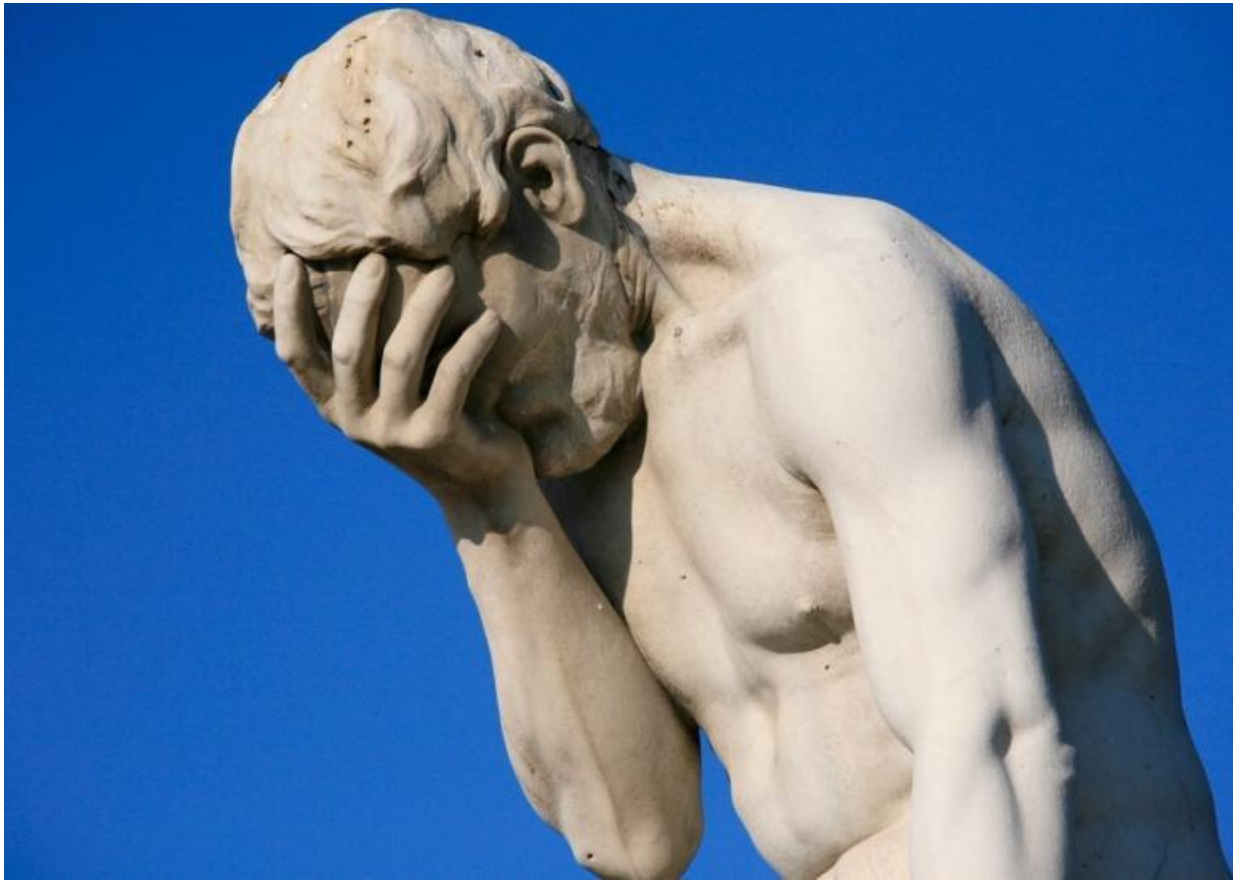


Photo credit: Alex E. Proimos, Creative Commons

OWASP Top Ten

Main | Translation Efforts | Sponsors | Data 2020

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

> Globally recognized by developers as the first step towards more secure coding.

Companies should adopt this document and start the process of ensuring that their web applications minimize these risks. Using the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces more secure code.

Photo credit: KVDP, Shokunin, Aungkarns, CC BY-SA 3.0


THE
BEER
FARMERS

My AppSec Village!

- Mike Thompson
- Sean Wright
- Daniel Ward
- Brett Crawley
- Zuhal Vargun
- Dan Card
- Ian Thornton Trump
- Zoë Rose

What Is Threat Modelling

“Threat modelling works to identify, communicate, and understand threats and mitigations within the context of protecting something of value”

Victoria Drake, OWASP

sonatype

The Four Questions of Threat Modelling:

- What are we working on?
- What can go wrong?
- What are we going to do about it?
- Did we do a good enough job?

The Threat Modeling Manifesto, 2020

Threat Modelling is best done with a group as diverse in thought as possible.

Security is for EVERYONE!

Modelling Threats In The Open (Source)

Open Source Has Many Threats

- Global open source consumption will surge to an estimated 3.1 trillion total requests.
- 742% average yearly increase in software supply chain attacks since 2019.
- 6 out of every 7 vulnerabilities affecting open source projects are due to transitive dependencies.
- Legislation in US (Executive Order) and coming soon in EU (Cyber Resilience Act).

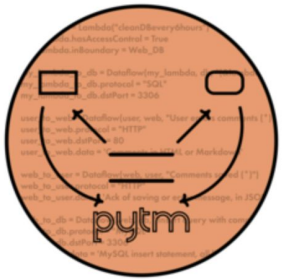
Open Source Is Difficult To Model

- Users of software may use things differently to how you expect
- Especially in the case of libraries, you may not know the state of the code your library has been put into.
- You can not know the hardware architecture a user has chosen (Kubernetes, Serverless, Simple Bare Metal).

Tools

Threagile

Agile Threat Modeling



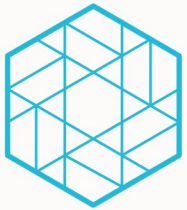
Tools

- We wanted a diagram that looked like arch diagram for data flows
- Wanted an update mechanism that felt comfortable for developers
- We wanted the data flow diagram to show a level of risk and to be flexible

ANY OF THESE TOOLS WOULD HAVE BEEN GOOD TO USE

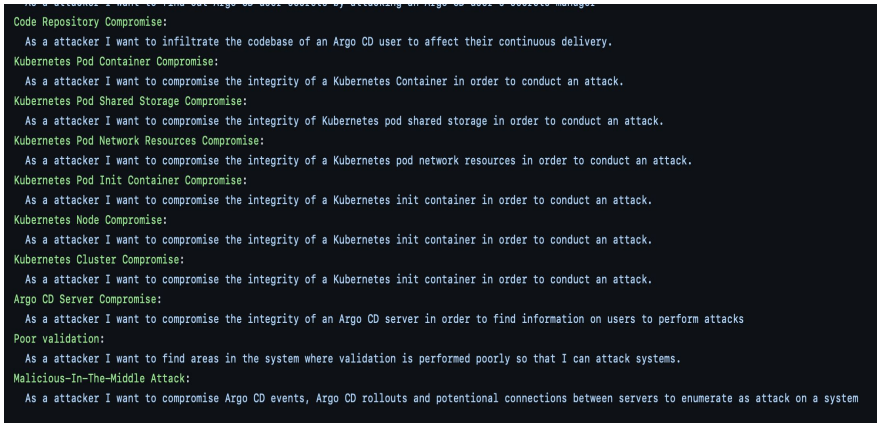
Threagile – Agile Threat Modelling

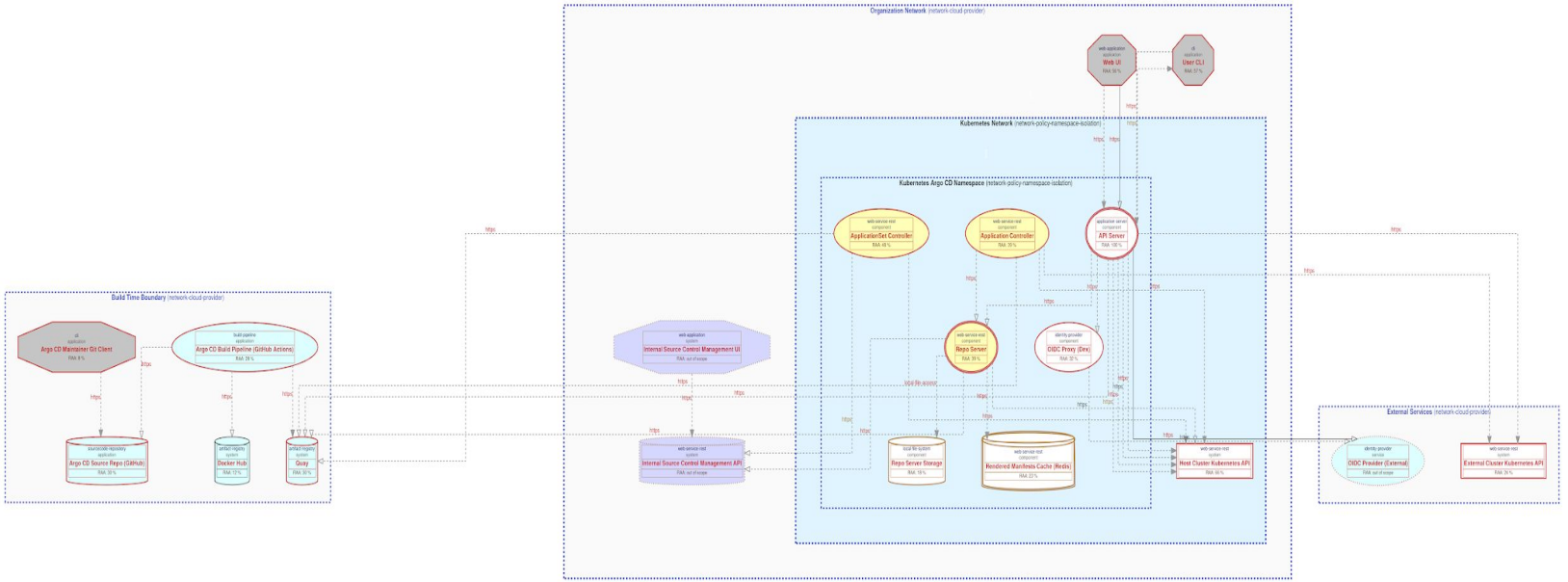
- Released in 2020 by Christian Schneider
- Open Source
- Uses YAML to model architecture.
- Generates data-flow diagrams, based on calculated RAA (Relative Attacker Attractiveness)
- The higher the RAA, the more interesting it is to compromise an asset.



Threagile – Agile Threat Modelling

- Written in Go
- Can run on command line, REST server of Docker container.
- Due to YAML you can create a base template.
- This may be then used for similar projects.

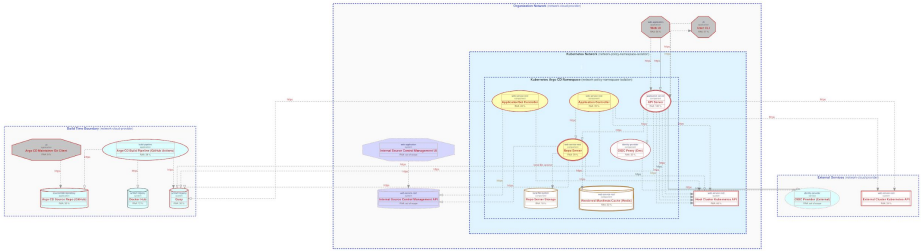




Argo CD Data Flow Diagram, 2023

Threagile – Agile Threat Modelling

- Outputs data model as png
- Also can output risks identified and mitigated as a pdf
- These could be stored in a .security folder for open source projects.
- We can create YAML standard templates which can be leveraged by security focussed organisations



Are We Doing A Good Enough Job?


NIST
NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE


bcs
The
Chartered
Institute
for IT


OWASP
®


National Cyber
Security Centre


CLOUD NATIVE
COMPUTING FOUNDATION


OpenSSF
OPEN SOURCE SECURITY FOUNDATION


sonatype

Threat Modelling is really a security code review.

Code reviews are the most effective way of reducing errors to a code base.

Having defined threat model templates backed by open source organisations are important to speed up adoption.

Beyond Modelling

Actions

- Use tools to manage threats – there are many free ones that open source can use.
- Rapid threat templates of known infrastructure to help developers
- More complex projects and deployments will need more help
- Question your open source projects
- Security is for EVERYONE!

Thanks for listening!