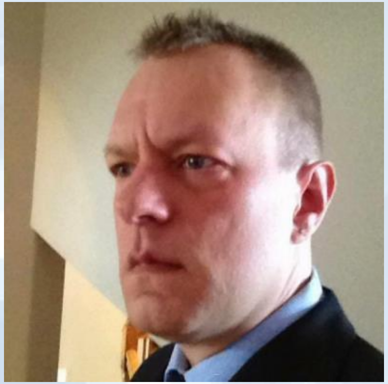
Application Security Maturity: DAST, SAST, or IAST?

Adrien de Beaupré
Consultant and instructor

Intru-Shun.ca Inc
PRACTICING THE ART AND SCIENCE OF INTRUSION SECURITY

Instructor



Consultant

InfoSec full time since 2000

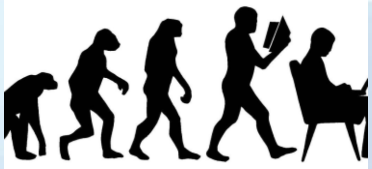
Black Belt &
Martial Arts Enthusiast

CoAuthor of SANS SEC 460 and 642

Introduction

- Why this presentation?
- That cyber word
- A little bit of history
- Visibility is one problem
- The future of InfoSec is AppSec
- Application behaviour modeling
- Solutions

WHY?



This discussion will focus on how modern information security has evolved and what we will need to move into the 21st century.

We need a new paradigm in security with a workforce that understands application security; the new frontier.

I liked it better when we could tell someone did not know what they were talking about by counting the use of the word 'cyber'

It is all about risk to the organization

Maybe just call it security?

Everything keeps changing…

- The industry re-invents itself every 5 years
- Which means that we have to do the same, evolve
- Security must be multi-disciplinary
- We must solve risk problems with common sense, science, and technology
- Massive implications of interconnection

Cloud

- We are still playing catch up with cloud
- It can be a business enabler
- Can also be a disaster
- Not just outsourcing
- Not just virtualization
- Architecting security in cloud has changed

We have to stop saying no

- We did so for far too long
- The business routes around roadblocks
- Users go direct to cloud, and route around IT
- 'Yes, and let me help you with that'
- Get the requirements to design security from the beginning, not as an afterthought

History

- Firewalls - late 1980's early 1990's
- Patching - 1990's
- Anti-virus - early 2000
- End point security - now
- Agents
- What about those applications?

Attacks evolved

- Server side attacks -> firewalls
- Service exploits -> patching
- Worms and bots -> anti-virus and anti-malware
- Client side attacks -> patching and end point
- Phishing -> user awareness training
- Attackers/users logging into the application?

Network security

- Network security has matured
- More and more operationalized
- Firewalls have moved from being a speciality to mostly being a networking role
- Intrusion Detection/Prevention IDS and IPS do not give us visibility into applications
- Encryption makes it even more difficult

End point security

- We are maturing security at the end point
- Also gaining more visibility into user activities
- A plethora of agents
- We can do forensics on disk and memory
- What about those applications?

Application security

- We have limited visibility
- Encryption is an increasing problem
- Logging is an ongoing problem
- Attackers use the applications with malicious intent, which can be difficult to differentiate from normal user behaviour

Applications

- Almost everything involves applications
- Mobile, web, containers, toasters…
- The state of security in IoT and embedded systems is not good
- Every day there is a new dev framework!
- New and old vulnerabilities keep coming

Application security issues

- Security is not always integrated into the development lifecycle
- Companies are not investing enough in secure architecture and coding training
- Application Security programs often lack structure and a systematic approach
- We need to provide metrics to management

Application security program maturity

- There is not a common and consistent way to measure the maturity level of an application security program either between organizations or between industries
- This is problematic, how do we know how well we are doing? Or not doing.

Requirements?

- The business needs to help us help them
- Both functional and business requirements
- What does the application do?
- Who will be using it?
- Sensitivity of the data?
- How does it process, store, transmit data?

Threat model

- Asset inventory
- Data categorization and classification
- Who are the most likely threat sources/actors?
- Identify and prioritize likely threats
- What are their most likely targets
- Probability and vectors?

Threat model to roadmap

- Model attack and defense; broad or granular
- How effective are the existing controls?
- Level of sophistication and resourcing?
- Now you have a threat model, develop a roadmap to mitigate

Behaviour

- We need to model user behaviour
- We need to have the applications log user actions so that we can study behaviour
- This is both a visibility problem and a lack of tools that help us baseline users

DevSecOps.org

- 'Everyone is responsible for security' www.devsecops.org
- DevOps
- Agile development
- Cloud adoption
- Security must be part of the solution with automation as much as possible

SAST, DAST, IAST

- Looking at static source code gives you one perspective: time consuming and expensive
- Dynamic testing is a different view: Can be of limited value depending on testers and tools
- Interactive testing involves installing an agent server side, probably in DEV, QA, or TEST. Runtime testing.
- So, which one(s) to choose?

Solutions

- Stop saying no
- Threat modeling
- SecDevOps
- Security in the development life cycle
- We will adapt to new technologies and adopt strategies that make sense in the future

Questions?

Thanks!

Adrien de Beaupré
Instructor and Author
Consultant
613 797-3912
adrien@intru-shun.ca
@adriendb