Can AppSec Be Fixed?

Brook S.E. Schoenfield
Author, elder statesman of AppSec
Principal Software Security Strategist, True Positives LLC
Chief Security Architect & Practice Leader, Resilient Software Security, LLC
Advisor, AeroByte, Inc.

Image credit: Publish What You Pay
https://www.pwyp.org/pwyp-resources/ignoring-the-elephant-in-the-room-why-financial-transparency-is-necessary-to-finance-development/

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

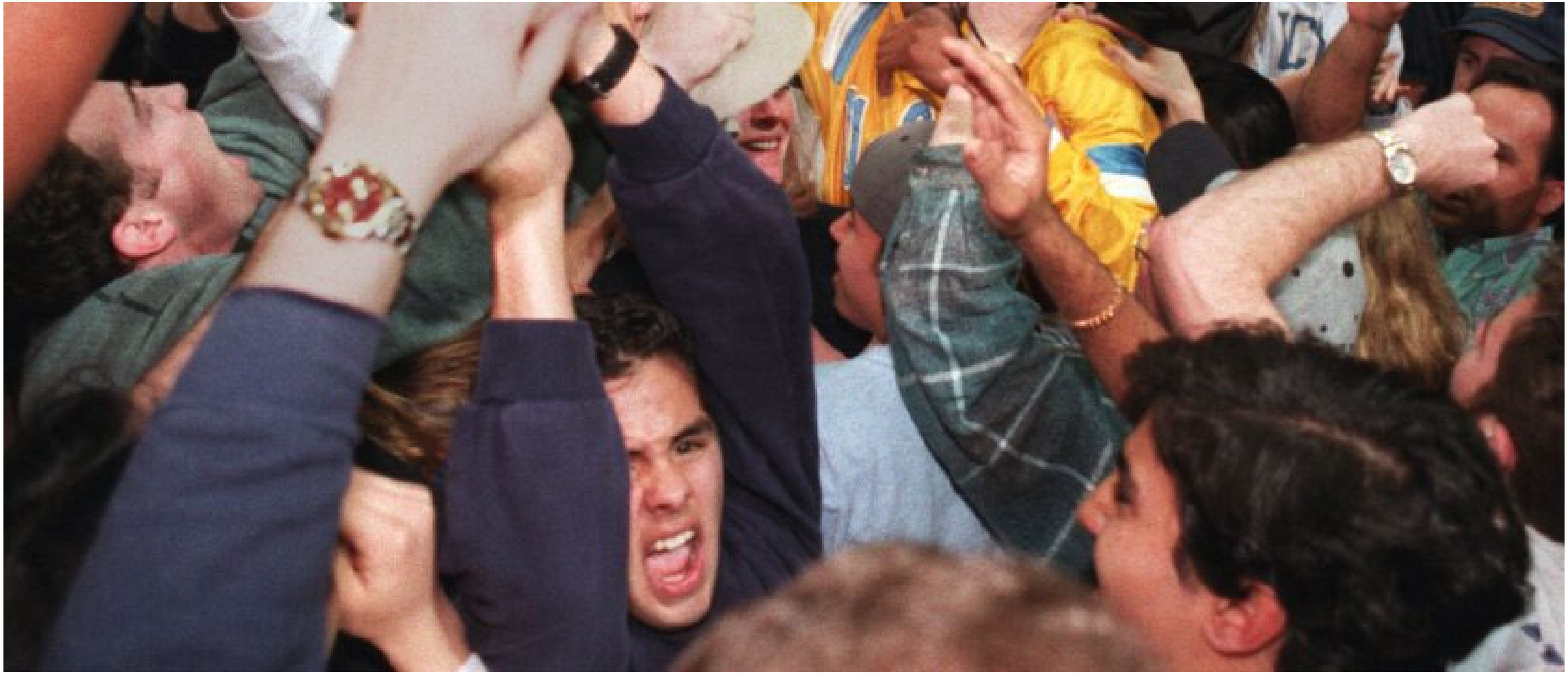
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

27 Million

A Warning!

- Starting 14 years ago
- Vendors focus on enterprise-sized organizations
- Excludes the majority
- The majority produce a lot of software
- ➔ Piles of vulnerability

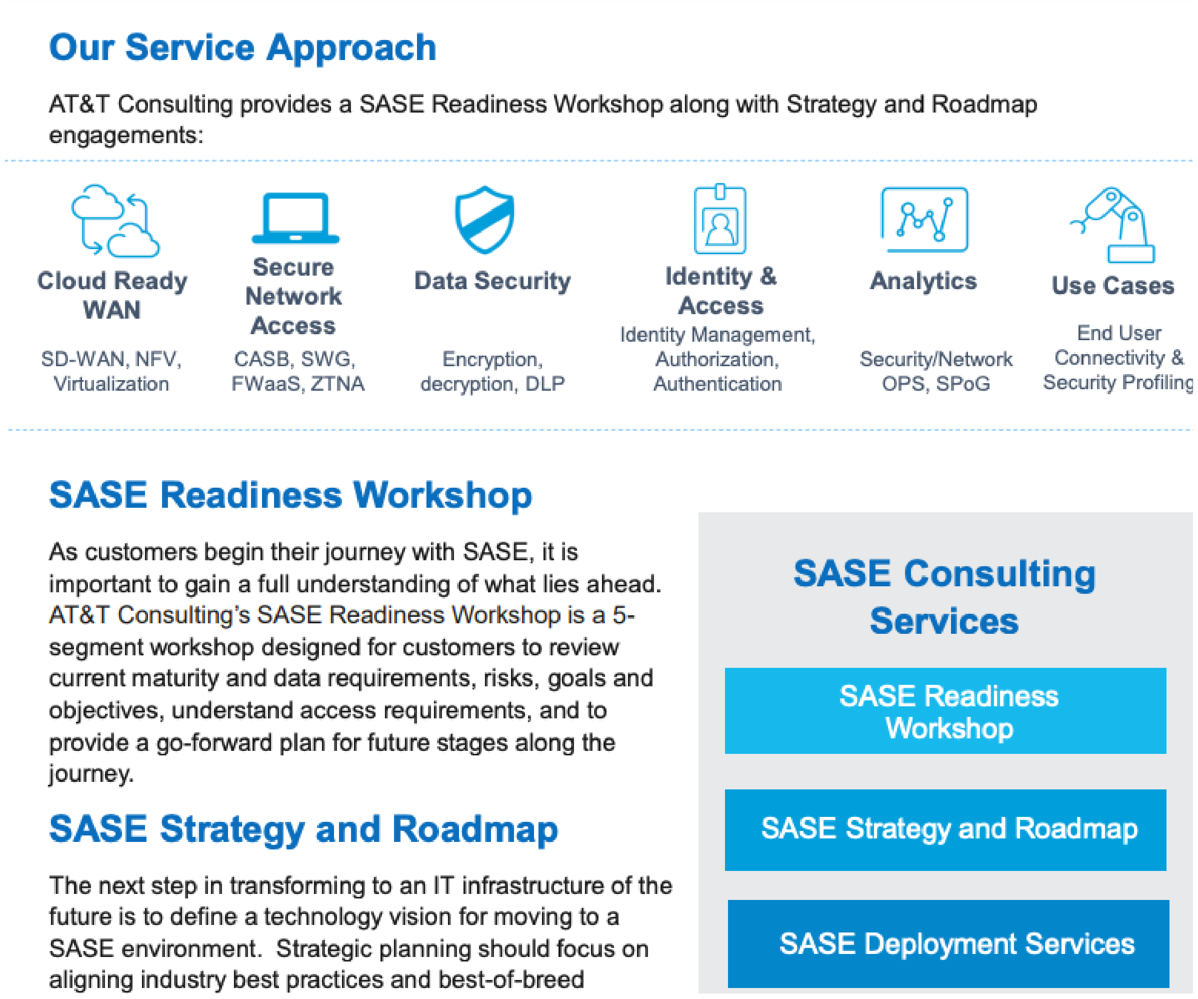
Is RSAC our yearly victory celebration?



Brook S.E. Schoenfield
Author,
Passionate security architect
Teacher, mentor, curious questioner
brookschoenfield.com

70M stolen AT&T records advertised for sale by well-known hacker

Assume AT&T Security deliver
“Industry best practice”



Our Service Approach

AT&T Consulting provides a SASE Readiness Workshop along with Strategy and Roadmap engagements:

Cloud Ready WAN	Secure Network Access	Data Security	Identity & Access	Analytics	Use Cases
SD-WAN, NFV, Virtualization	CASB, SWG, FWaaS, ZTNA	Encryption, decryption, DLP	Identity Management, Authorization, Authentication	Security/Network OPS, SPoG	End User Connectivity & Security Profiling

SASE Readiness Workshop

As customers begin their journey with SASE, it is important to gain a full understanding of what lies ahead. AT&T Consulting’s SASE Readiness Workshop is a 5-segment workshop designed for customers to review current maturity and data requirements, risks, goals and objectives, understand access requirements, and to provide a go-forward plan for future stages along the journey.

SASE Strategy and Roadmap

The next step in transforming to an IT infrastructure of the future is to define a technology vision for moving to a SASE environment. Strategic planning should focus on aligning industry best practices and best-of-breed

SASE Consulting Services

SASE Readiness Workshop

SASE Strategy and Roadmap

SASE Deployment Services

For real?

leading cybersecurity company protecting customers from all cyber threats

strategic security solution that covers all your security gaps

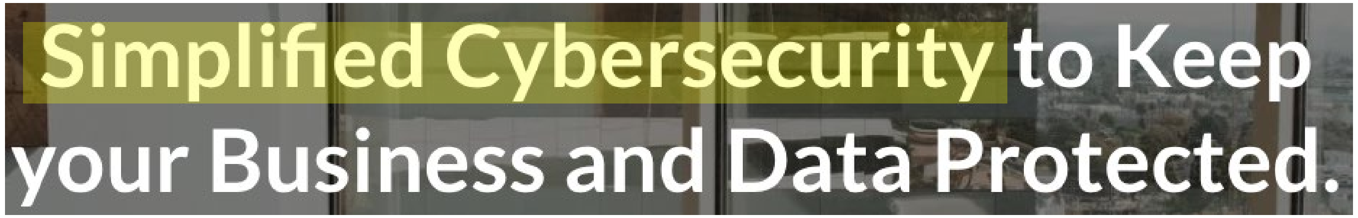
Help contain risk, embrace change, and elevate trust

Deploy Tech
Expand Scope
Reduce Cost
Reduce Security Risk
Improve Performance
Respond to Issues

It’s about securing the code as fast as you write it

Secure your sites, apps, APIs & infrastructure

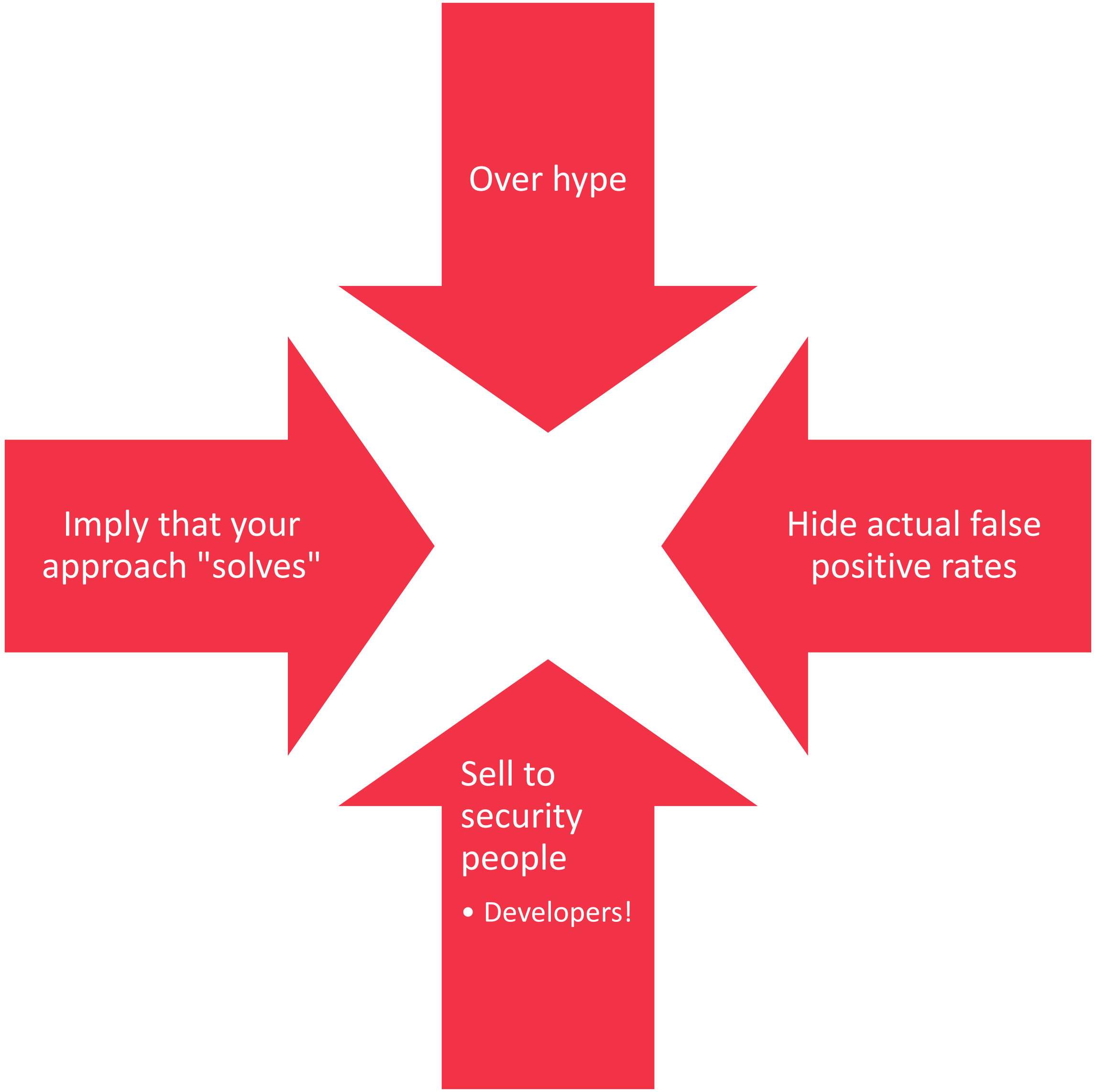
Make every part of your business more resilient


Simplified Cybersecurity to Keep your Business and Data Protected.

Emphases, mine

Tool Vendors, We Need You!

But please



Over hype

Imply that your approach "solves"

Hide actual false positive rates

Sell to security people

- Developers!

Brook S.E. Schoenfield
Author,
Passionate security architect
Teacher, mentor, curious questioner
brookschoenfield.com

“Pen test all code before release”

Impossible

Old chestnut,
"Fix all vulnerabilities"

"Using CVSS base score is statistically equivalent to choosing at random" – Alloddi & Massacci, 2014 “no computing machine exists that can decide whether or not an arbitrary computing machine is circle-free” – Alan Turing, 1936

The solution approaches infinity

The essential AppSec problem derives from the Turing Proof & Turing Complete Languages

Bugs' Hard Truths

- There will be bugs
- All security coding errors are bugs
- Not all bugs are vulnerabilities
- All weaknesses aren't coding errors
  - Not all weaknesses (readily) found in code

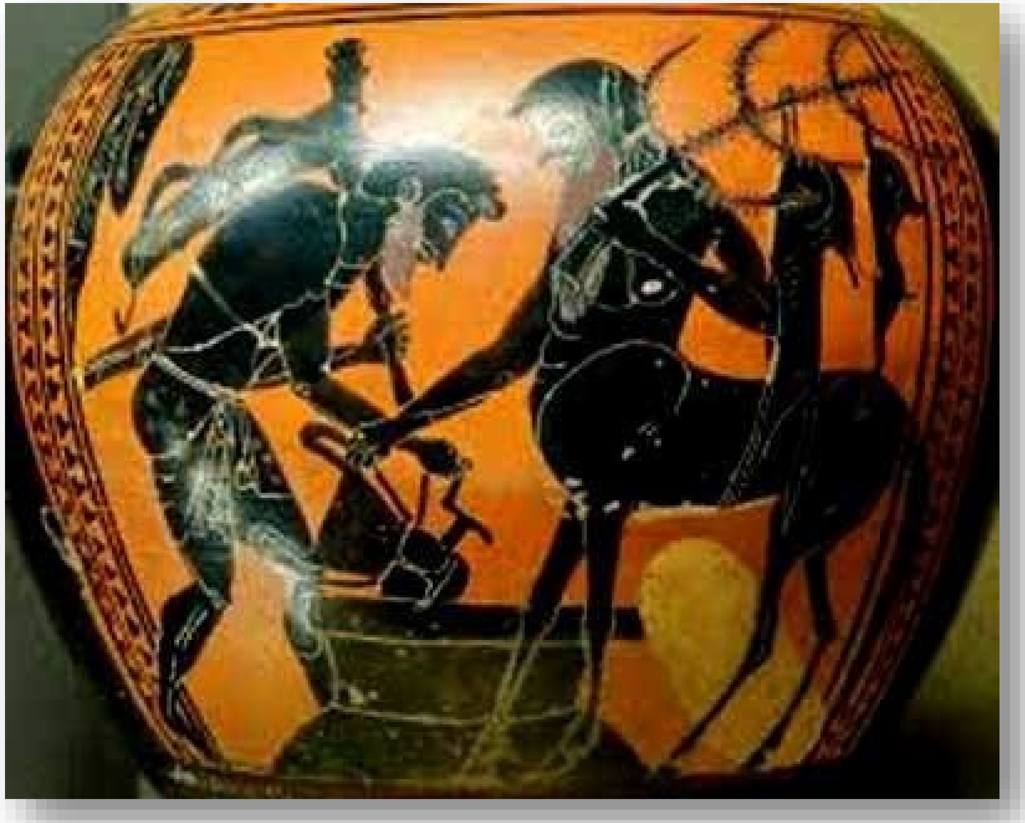
Brook S.E. Schoenfield
Author,
Passionate security architect
Teacher, mentor, curious questioner
brookschoenfield.com

Buried deep

> …software is complex and flexible…it's assembled from components in unique ways. The patterns involved in effective operation are unclear and rapidly changing.

Adam Shostack, “Ransomware Is Not the Problem”, DarkReading, 6/9/2021
https://www.darkreading.com/attacks-breaches/ransomware-is-not-the-problem/a/d-id/1341171

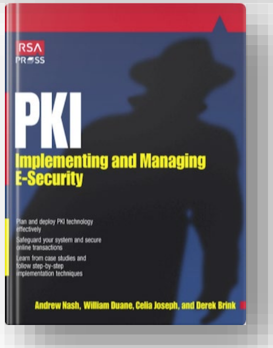
Myths, Misconceptions, Folklore



- Open source is “free”
- Cloud takes care of security
- Security review ➔ “secured”
- Threat Model == STRIDE == DFD → Point-in-time

[our digital world is] "…a house of *cards* during a *tornado* warning"

Bill Duane quoted by Andy Greenberg in
"The Full Story Of The Stunning RSA Hack Can (Finally) Be Told",
Wired, July/Aug 2021
My emphasis



RSA PRESS

PKI

Implementing and Managing
E-Security

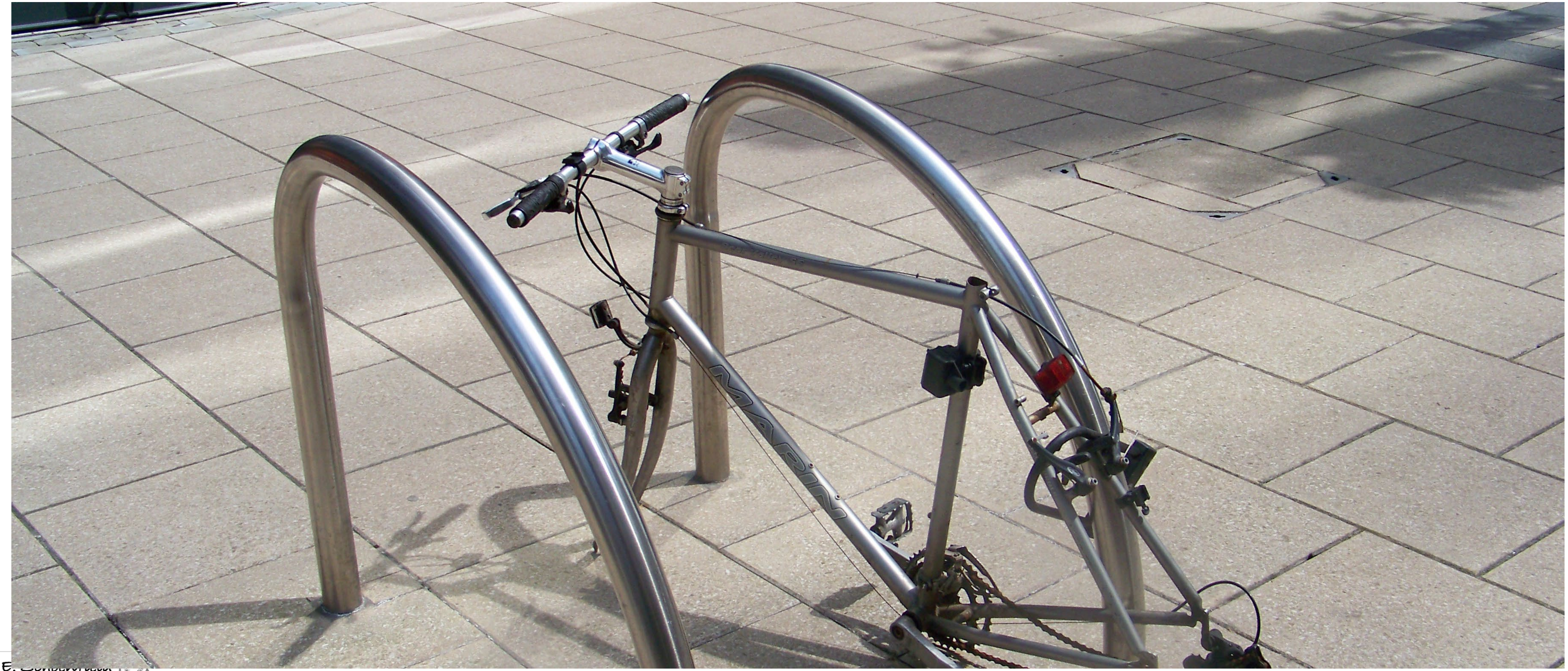
Plan and deploy PKI technology effectively

Safeguard your system and secure online transactions

Learn from case studies and follow step-by-step implementation techniques

Andrew Nash, William Duane, Celia Joseph, and Derek Brink

Fix?



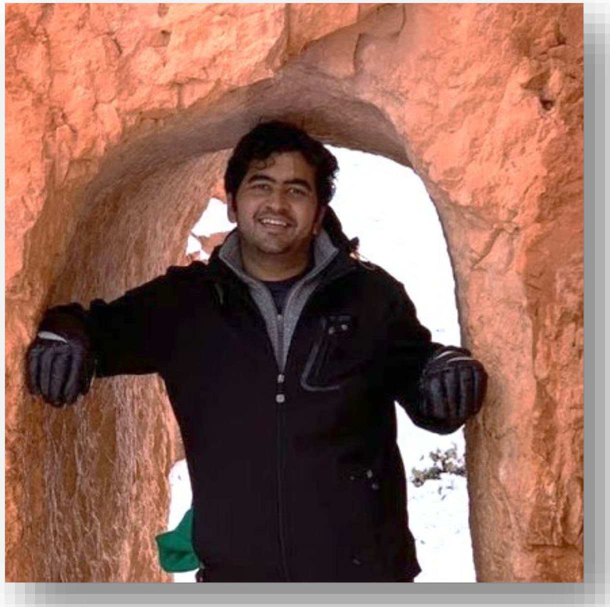
“Am *I* ***enabling*** *creativity* and ***innovation*** to be ***secure enough****?*”

Developer-centric security

(see the manifesto: https://brookschoenfield.com/?page_id=256)

Brook S.E. Schoenfield
Author,
Passionate security architect
Teacher, mentor, curious questioner
brookschoenfield.com

“[*Developers!*]…need tools that are fast, customizable to our codebases, can easily be added to any part of the SDLC, and are effective at enforcing secure coding patterns
to prevent vulnerabilities”

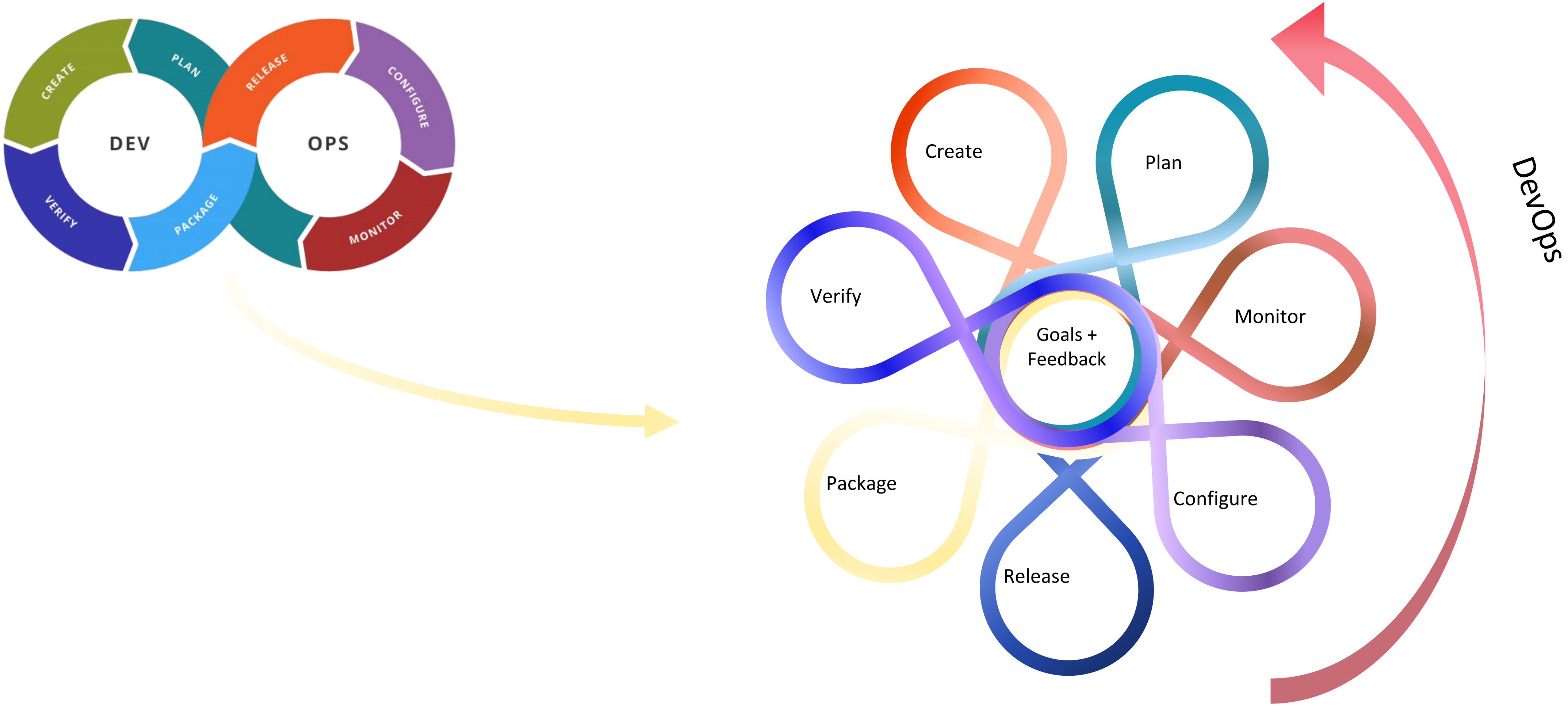


Devdatta Akhawe, “Modern Static Analysis: how the best tools empower creativity”

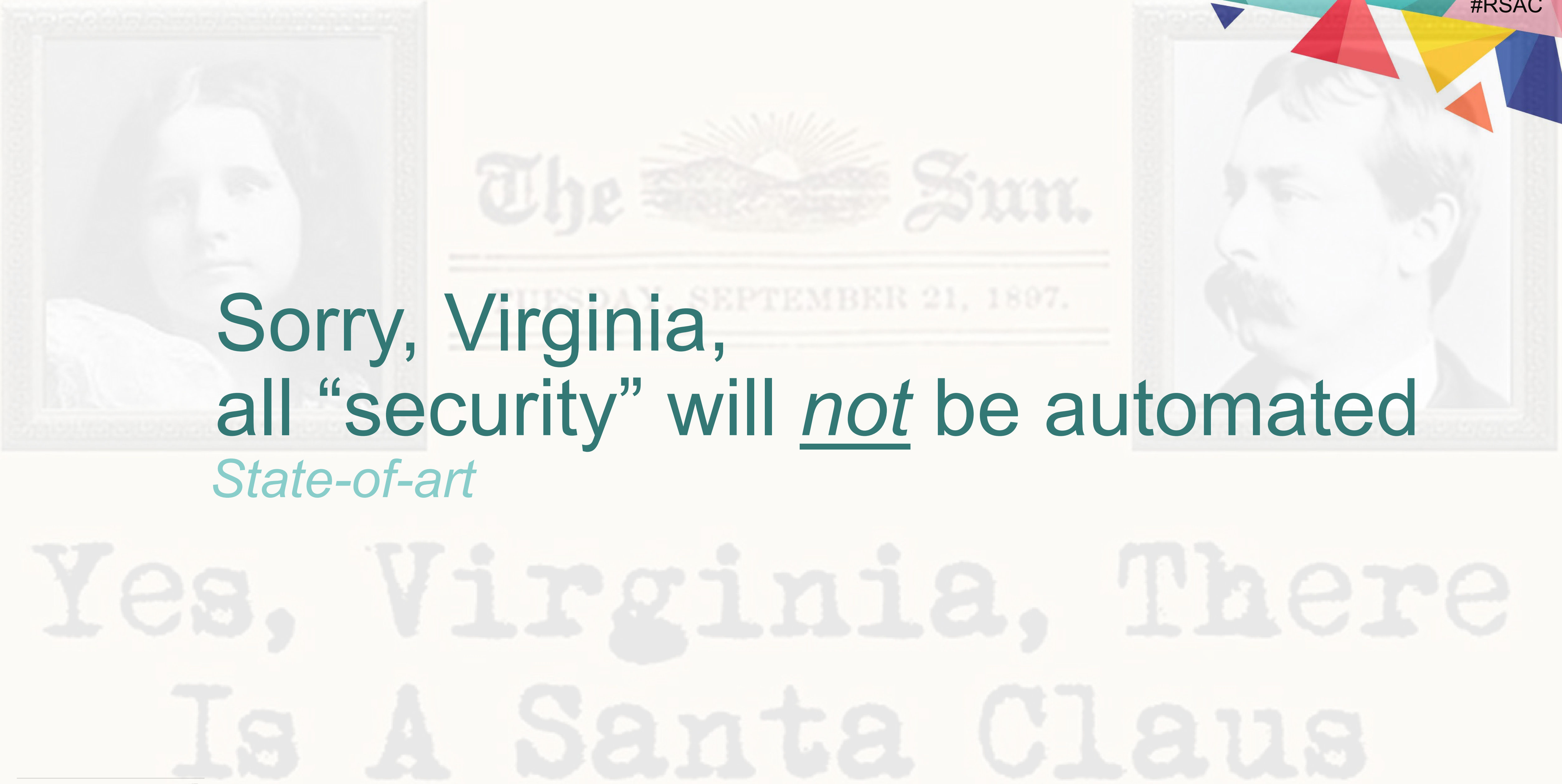
https://devd.me/log//posts/static-analysis/

Edits and emphasis, mine

DevOps Infinite Loop



Interdependent infinite loops of continuous activity

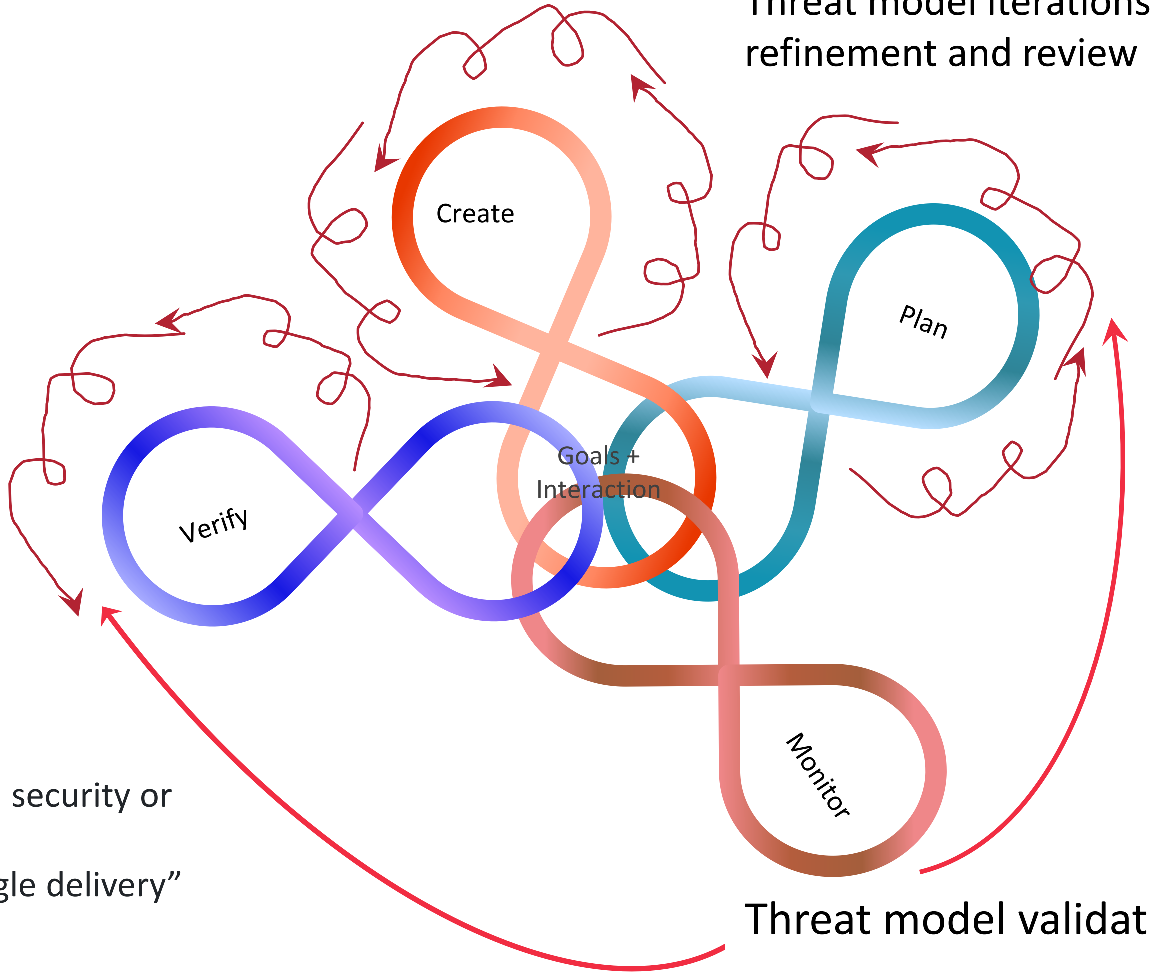


Sorry, Virginia,
all “security” will *not* be automated

State-of-art

Brook S.E. Schoenfield
Author,
Passionate security architect
Teacher, mentor, curious questioner
brookschoenfield.com

Effective threat modelling



Threat model iterations:
refinement and review

Threat model validation/feedback

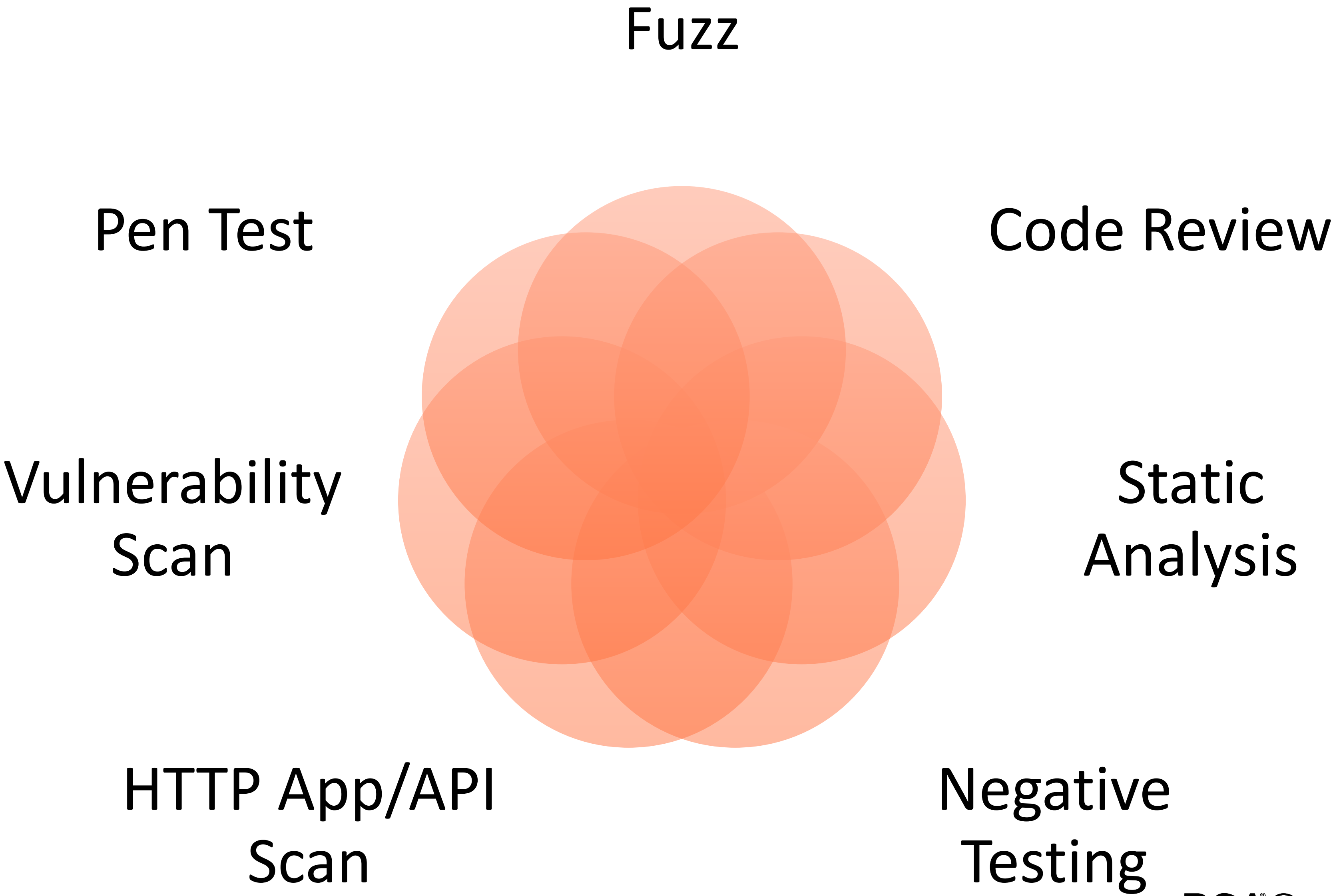
“A journey of understanding over a security or privacy snapshot.”
“Continuous refinement over a single delivery”
--Threat Modeling Manifesto

James Ransome & Brook S.E. Schoenfield,
Building In Security At Agile Speed, © 2020

Refine, Revisit, Review

- Structural (architecture) change
  - new/changed components
  - Flow/data exchange changes
- Security items
- New attack methods
- (No existing threat model)

Overlap, Redundancy, Coverage



Fuzz

Pen Test

Code Review

Vulnerability Scan

Static Analysis

HTTP App/API Scan

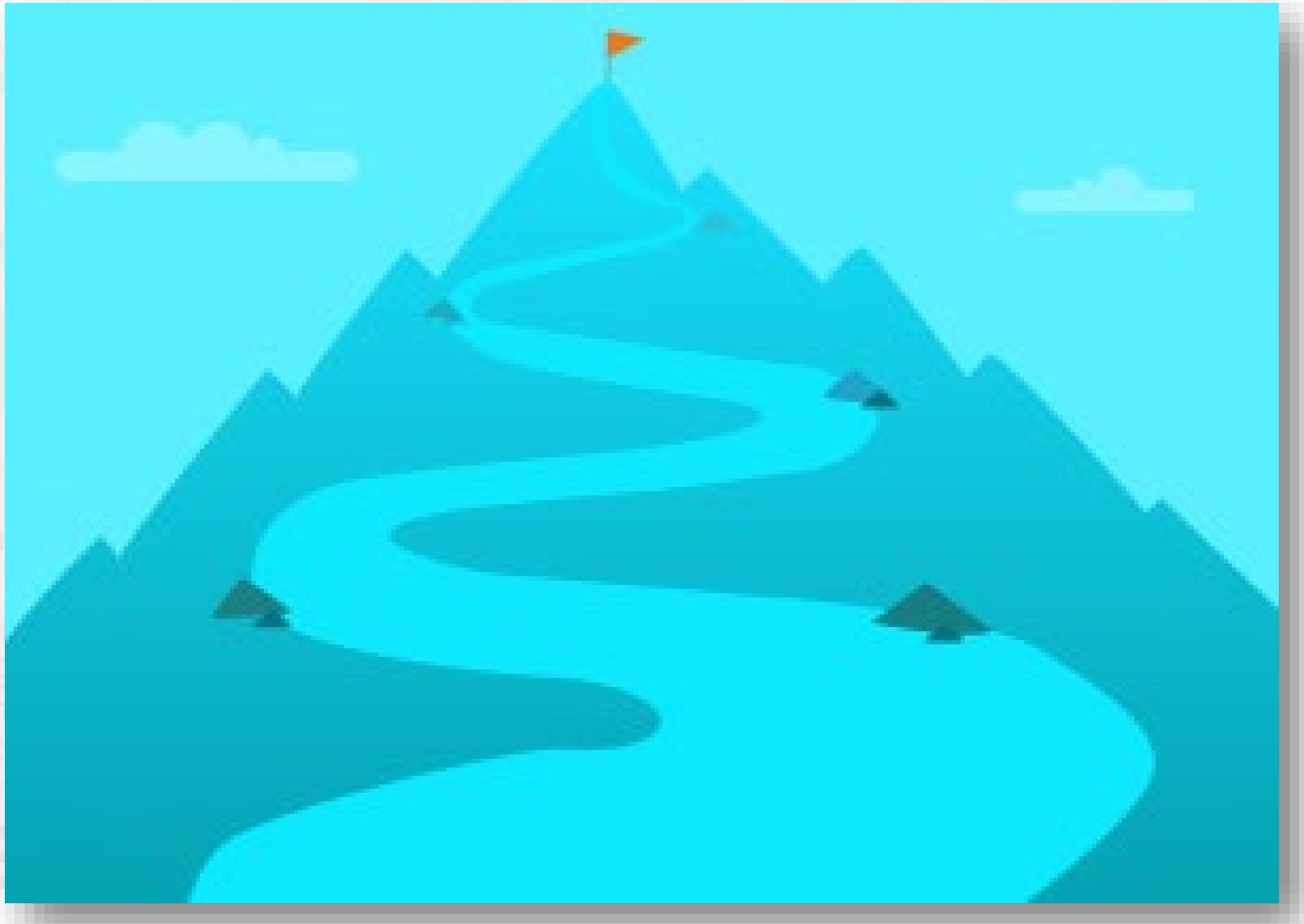
Negative Testing

Why Isn’t *Everyone* Fuzzing?

- Difficult
- Expensive
- Wrong targets
- Ad hoc

Ideal

- Straightforward
- Natural SDLC/IDE
- Obvious automation
- Understandable, reliable results
- Indicate faulty code
- Affordable!

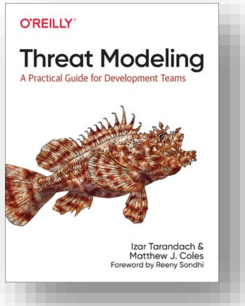


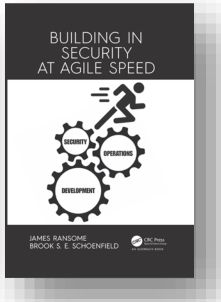
Brook S.E. Schoenfield
Author,
Passionate security architect
Teacher, mentor, curious questioner
brookschoenfield.com

Worth Considering?

“Is it time to pay bounty hunters for their threat models?”
-- Izar Tarandach

“A Tech & Architecture searchable ontology into Mitre ATT@CK+D3FEND”
-- Brook S.E. Schoenfield





Take Away

- Common myths and faulty assumptions hold us back
- There will be vulnerabilities
- Overlapping, complimentary techniques
- Threat models and fuzzing are critical
- An ideal tool

Q & A

brook@brookschoenfield.com

http://www.brookschoenfield.com

brook@brookschoenfield.com

@BrkSchoenfield

https://www.linkedin.com/in/brookschoenfield [1]

http://www.amazon.com/Brook-S.-E.-Schoenfield/e/B00XQFZLSW

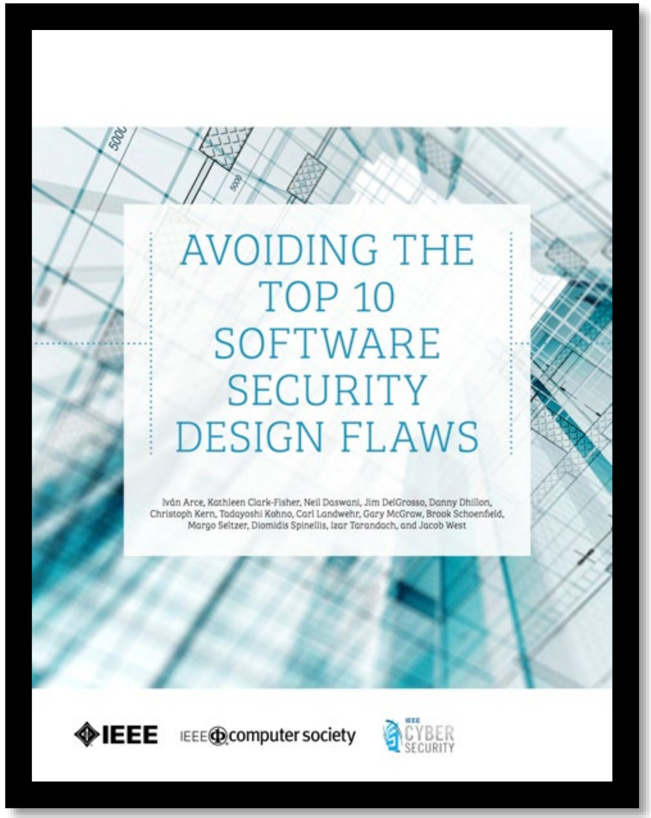
https://www.facebook.com/brookseschoenfield/

[1] I apologize in advance. Please note that you were at this presentation in your LinkedIn invitation. Thanks.

Resources

IEEE
CENTER FOR
SECURE DESIGN

A secure design primer



AVOIDING THE TOP 10 SOFTWARE SECURITY DESIGN FLAWS

Iván Arce, Kathleen Clark-Fisher, Neil Daswani, Jim DelGrosso, Danny Dhillon, Christoph Kern, Tadayoshi Kohno, Carl Landwehr, Gary McGraw, Brook Schoenfield, Margo Seltzer, Diomidis Spinellis, Izar Tarandach, and Jacob West

IEEE IEEE computer society IEEE CYBER SECURITY

https://www.computer.org/cms/CYBSI/docs/Top-10-Flaws.pdf

THREAT MODELING MANIFESTO

We have come to value:

- **A culture of finding and fixing design issues** over checkbox compliance.
- **People and collaboration** over processes, methodologies, and tools.
- **A journey of understanding** over a security or privacy snapshot.
- **Doing threat modeling** over talking about it.
- **Continuous refinement** over a single delivery.

We follow these principles:

- The best use of threat modeling is to improve the security and privacy of a system through early and frequent analysis.
- Threat modeling must align with an organization's development practices and follow design changes in iterations that are each scoped to manageable portions of the system.
- The outcomes of threat modeling are meaningful when they are of value to stakeholders.
- Dialog is key to establishing the common understandings that lead to value, while documents record those understandings, and enable measurement.

https://www.threatmodelingmanifesto.org/

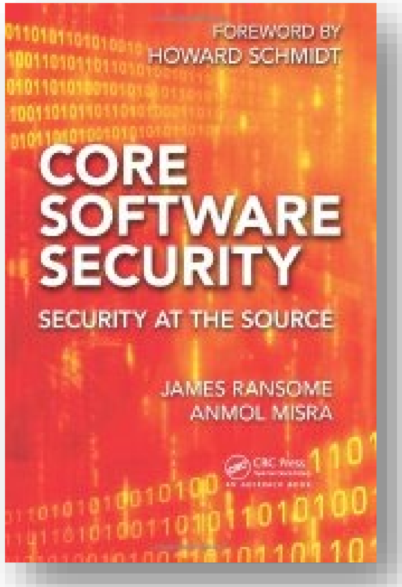
Brook S.E. Schoenfield
Author,
Passionate security architect
Teacher, mentor, curious questioner
brookschoenfield.com

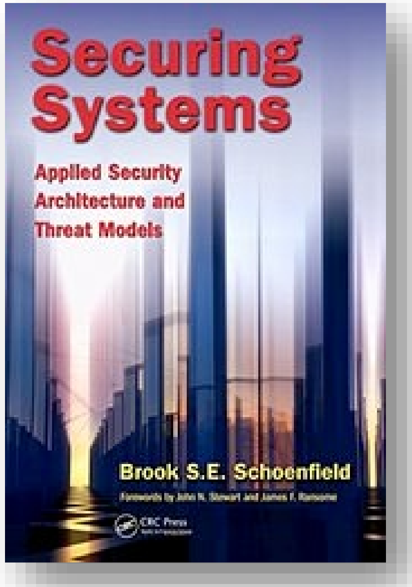
Some Resources

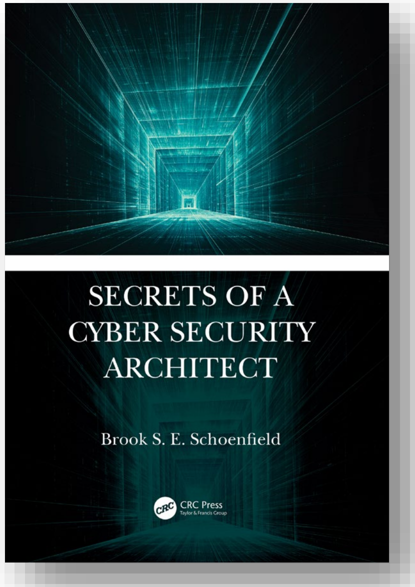
https://www.threatmodelingmanifesto.org/#values
https://safecode.org/wp-content/uploads/2017/05/SAFECode_TM_Whitepaper.pdf
https://www.owasp.org/index.php/Application_Threat_Modeling
https://www.owasp.org/index.php/Threat_Risk_Modeling
https://www.owasp.org/images/a/aa/AppSecEU2012_PASTA.pdf
http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=427321
https://itpeernetwork.intel.com/whitepaper-prioritizing-information-security-risks-with-threat-agent-risk-assessment/
https://ieeecs-media.computer.org/media/technical-activities/CYBSI/docs/Top-10-Flaws.pdf
https://github.com/Autodesk/continuous-threat-modeling/blob/master/Secure_Developer_Checklist.md
https://mitre.github.io/attack-navigator/enterprise/
https://capec.mitre.org/data/definitions/1000.html
https://cwe.mitre.org/data/definitions/1008.html
https://cwe.mitre.org/data/definitions/1000.html
https://cwe.mitre.org/data/definitions/1000.html
https://www.microsoft.com/en-us/download/details.aspx?id=20303
http://securitycards.cs.washington.edu
https://pages.nist.gov/mobile-threat-catalogue/ecosystem.html#page
https://www.facebook.com/securingsystems
http://www.amazon.com/Securing-Systems-Applied-Security-Architecture/dp/1482233975
https://www.facebook.com/softwaresec
www.amazon.com/Core-Software-Security-Source
https://www.amazon.com/Insiders-Guide-Cyber-Security-Architecture-dp-1498741991

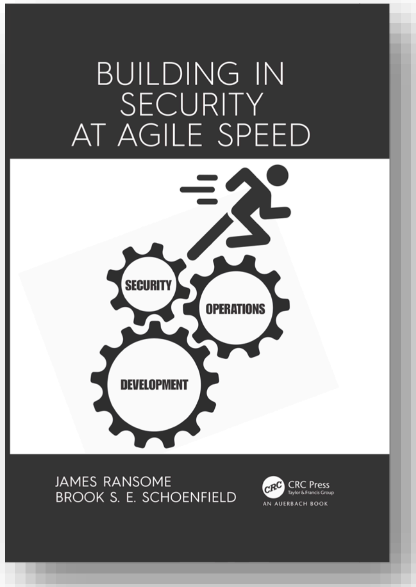
Brook S.E. Schoenfield
Author,
Passionate security architect
Teacher, mentor, curious questioner
brookschoenfield.com

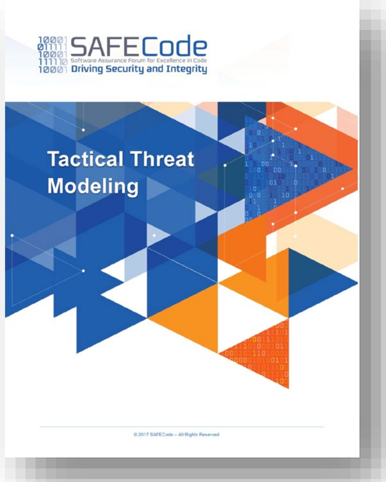
Shameless Self Promotion

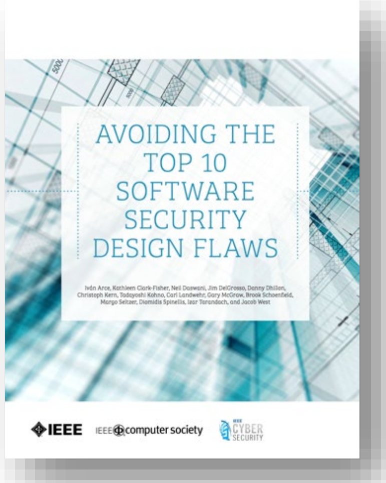



Securing Systems
Applied Security Architecture and Threat Models
Brook S.E. Schoenfield
Forewords by John N. Stewart and James F. Ransome
CRC Press






SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity
Tactical Threat Modeling

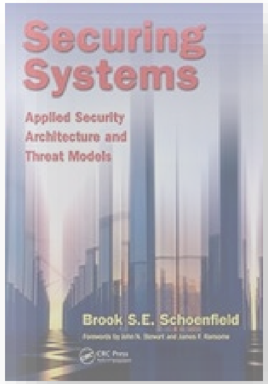

AVOIDING THE TOP 10 SOFTWARE SECURITY DESIGN FLAWS
Iván Arce, Kathleen Clark-Fisher, Neil Daswani, Jim DelGrosso, Danny Dhillon, Christoph Kern, Tadayoshi Kohno, Carl Landwehr, Gary McGraw, Brook Schoenfield, Margo Seltzer, Diomidis Spinellis, Izar Tarandach, and Jacob West
IEEE
IEEE computer society
IEEE CYBER SECURITY

Brook S.E. Schoenfield
Author,
Passionate security architect
Teacher, mentor, curious questioner
brookschoenfield.com

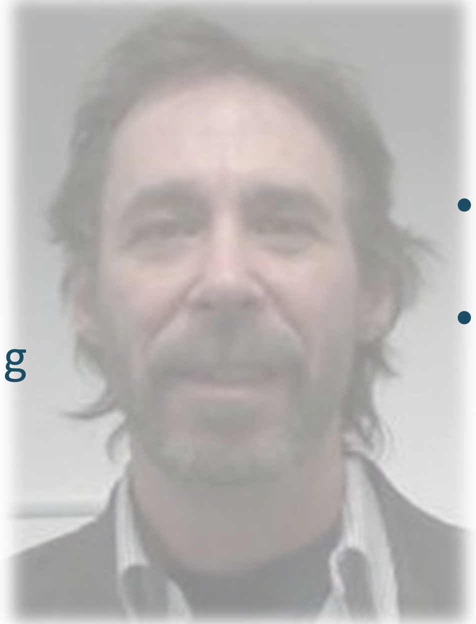
https://www.facebook.com/securingsystems

https://www.facebook.com/brookseschoenfield/

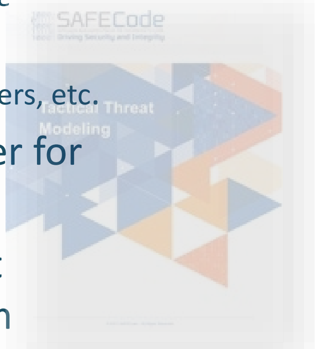
Brook S.E. Schoenfield, MBA
Master Security Architect



- >1000 security reviews
- 22+ years security
- 35+ years software/hi-tech
- Real-time OS, TCP/IP stack down to hardware
- 5 virtual team lead, 10 technical leader roles
- Intel Principal Engineer
- 5 software security lead @ 4 organizations
- Trained 100’s security architects
- 1000’s attended threat modelling classes



- SANS Institute Featured Speaker, contributor GWEB certification
- Author:
  - *Building In Security At Agile Speed*
  - *Secrets Of A Cyber Security Architect Auerbach Press 2019*
  - *Securing Systems*, CRC Press, 2015
  - *Core Software Security*, CRC Press, 2014
  - *Avoiding The Top 10 Security Design Flaws, IEEE*
  - *SAFECode Threat Modeling Guide*
  - *Threat Modeling Manifesto*
  - Various SANS Smart Guides, papers, etc.
- Founding member IEEE Center for Secure Design
- Featured security architect at Bletchley Park Cyber Museum



Brook S.E. Schoenfield
Author,
Passionate security architect
Teacher, mentor, curious questioner
brookschoenfield.com

“Experimentation is key to all engineering”

Aaron Rinehart on Application Security PodCast, April 30, 2021.

Author of *Security Chaos Engineering,* O'Reilly Media, 2020