SESSION ID: AIR-W02

Threat Modeling From The Trenches To The Clouds

Brook S.E. Schoenfield

Passionate security architect
Curious questioner
Principal Engineer, Intel Security

“TM” == Threat Modeling!



TM == Wizardry?



Based Upon What?

- Trained 100's of security architects over 15+ years
- 51 Intel Security TM training sessions
  - TM every type of architecture
    - Below OS to global clouds
- 300+ people trained throughout Intel + 3 teachers



From What Exprience Is This Drawn?

- Trained 100's of security architects over 15 years
- 51 Intel Security TM training sessions
  - TM every type of architecture
    - Below OS to global clouds
- 300+ people trained throughout Intel +3 teachers

Technical lead for 4 security architecture programs at 4 organizations (9th technical lead role)



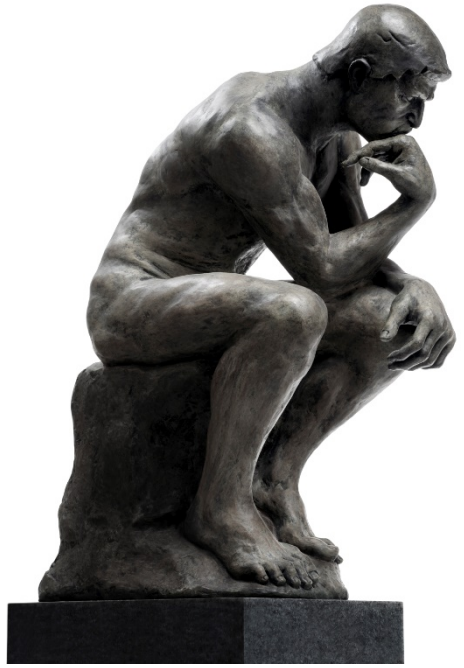
Working Definition

Threat modeling is a technique to identify the attacks a system[1] must resist and the defenses that will bring the system to a desired defensive state

1. “system” is defined inclusively

Our Collective Challenge == Secure Design

- Little progress in 20+ years!
  - Early standard = NIST 800-14, 1996!
- Is it simply that “developers don’t care”?
  - Or, “developers are dumb”?
  - Or, “Developers have no training”



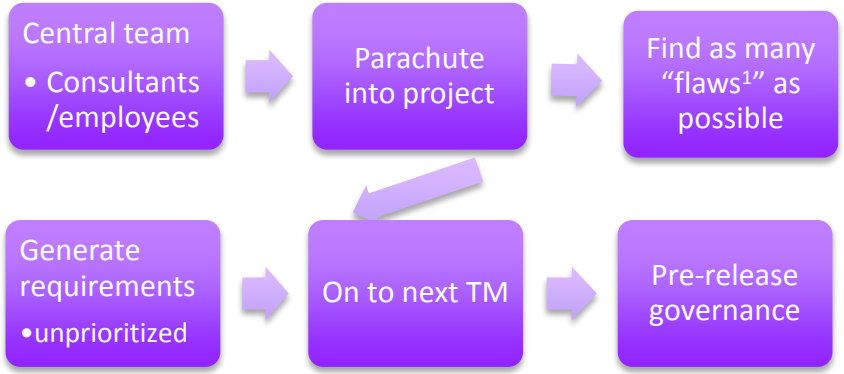
Consider Recent Design Misses

- That Jeep Wrangler
- Open WiFi Pacemaker
- The Target breach was a system design failure





Old Guard





1. Gary McGraw's term

Old Guard



- Balky, defensive developers
- Resistant project managers
- Escalations & exceptions

1. Gary McGraw's term

Are These Your Challenges?



- Only staff critical apps
- Fight between “creativity” & “security”
- Security requirements don’t can’t be built
- Business always trumps security
- Threat model treated as irrelevant or bureaucratic
- Security are synonymous with ”No”

Be Different!

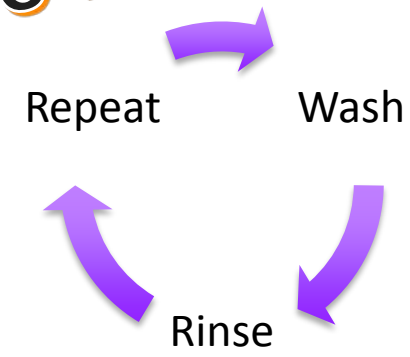
- Decentralize
- Fully empower
- Skill can be built, difficult to buy
  - 1-2 highly skilled hires who both execute and teach
- Play a long game, sometimes a very long game
- Teach, coach, mentor, let go



Be Different!

- Decentralize
- Fully empower
- Skill can be built, difficult to buy
  - 1-2 highly skilled hires who both execute and teach
- Play a long game, sometimes a rebuilding game
- Teach, coach, mentor, let go

Mistakes will be made: prepare!
There is always churn



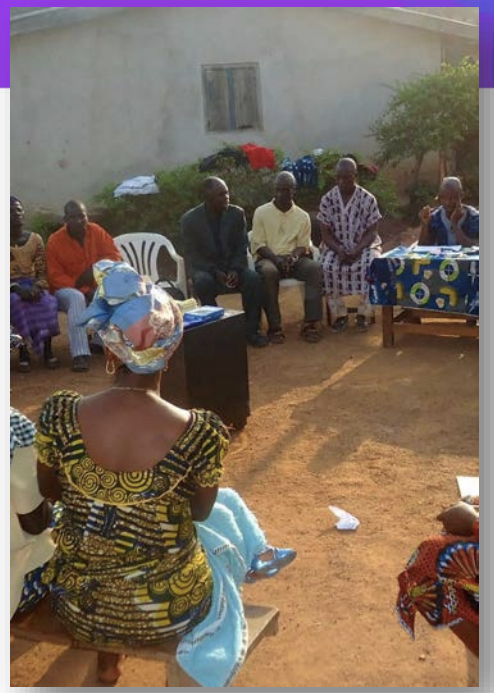


Grassroots

- TM is part of the ”woodwork”, the “expected” flow
- Go viral: build generations of teachers
- Leverage each level of skill



Involve Everyone



- Team sport
  - Everyone! Really!

• Product managers	• Designers
• Quality people	• Architects
• Devops	• Security experts
• SDETs	• Facilitator
• Developers	• Project management

  - It takes a village to build a complete threat model
- Prioritization is hard. All the stakeholders must be involved
- It’s fun! (yeah, it really is)

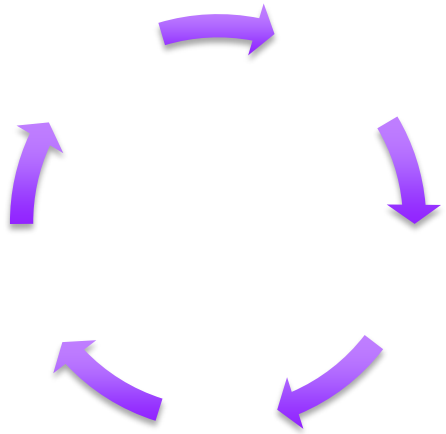


A threat model is a crossroads of knowledge from architecture experts, domain experts, and security experts

Absence of one or more stakeholders cripples the model and its usefulness

Iteration Is Your Friend

- Let the threat model breathe
- Security implementation can improve through iteration
- Changes of structure trigger review of model
- Changes to security trigger re-evaluation
  - Especially of the design



Prioritizing

- Risk is the way!
  - Calculating risk is difficult
- Adopt an easy risk analysis methodology
  - Just Good Enough Risk Rating (JGERR)[1] or similar
- Work towards the intended posture
  - Particular system
  - Relevant threat agents
  - Impactful assets
  - User expectations
  - System Owners
  - Organization's risk tolerance

1. co-author, Vinay Bansal, 2008, based upon Factor Analysis of Information Risk, Jack Jones, Open Group Standard

Prioritizing

- Risk is the way!
  - But that's hard
- Adopt an easy risk analysis methodology
  - Just Good Enough Risk Rating[1] or similar
- Must understand the intended posture
  - Particular system
  - User expectations
  - System Owners
  - Organization's risk tolerance

We don't sweat the small stuff!



1. co-author, Vinay Bansal, 2008, based upon Factor Analysis of Information Risk, Jack Jones, Open Group Standard

Get Out And See The Architectural World

- Analyze unfamiliar architectures and unfamiliar structural types
- Build skill; attend analysis with others
  - Across organizational boundaries
  - Across projects



“Keystone” activity
Participation results:

- Why security is crucial
- What to worry about and what not
  - Sense of the risk posture for their system
  - Priorities
- How each role contributes
- SDL tasks, Security Definition of Done





Governance



- Central boards are a bottleneck
- The best don't have to "approve" everything

Peer Review ➔ Governance



- Central boards are a bottleneck
- The best don't have to "approve" every model

Learn By Doing

- Experience -> Reflection -> Integration[1]
  - Let participants find personal learning
- Active participation
- Solve problems
- Keep didactic to a minimum
- Problems highlight concepts
- Exercises increase in difficulty and scope
- Every analysis holds validity (even if off-base)



1. Empowered learning model – Eric Bear, Mary Klein, et al, based on Pedagogy of the Oppressed – Paulo Freire, 1968

The Downside

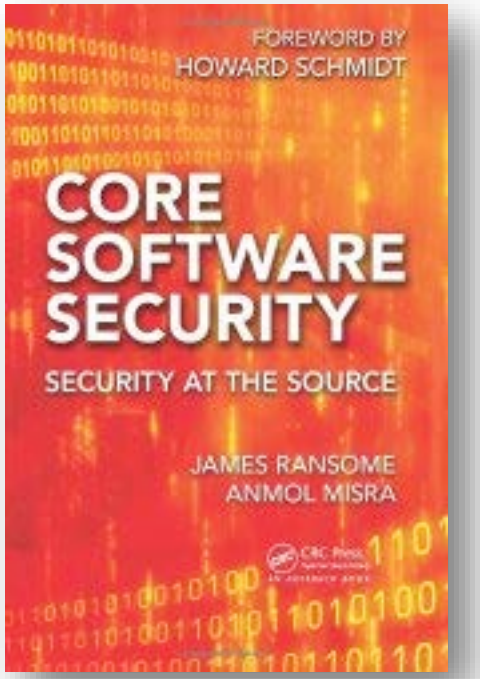
- Trees for the forest analyses
- Accepting component threat models w/o analysis
- Lose the centre
- Poor visibility of errors

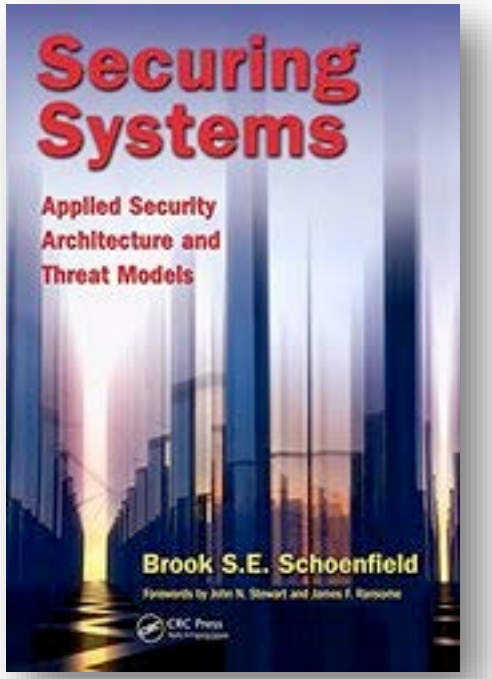


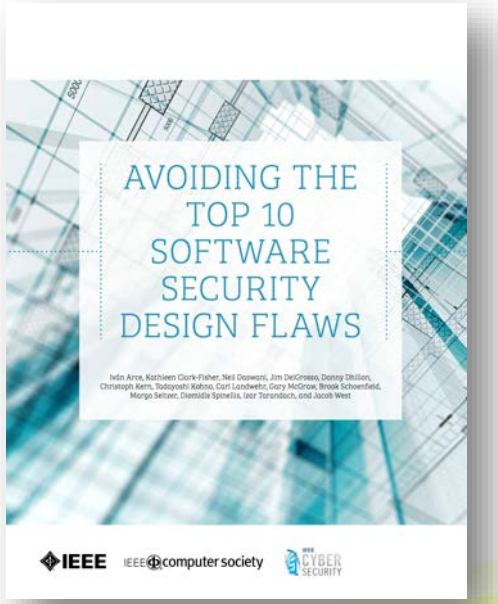
Take Aways

- Build, because we couldn't buy/hire
  - Grassroots + management + executives
  - Train & mentor as though our lives depend upon it
- Don't sweat the small stuff!
  - Exceptions are my friends
- Involve everyone
- Iterate to stay in sync and for improvement
- Peer review => governance
- Threat modeling is The Keystone activity
- Continual care and feeding

Shameless Self-promotion

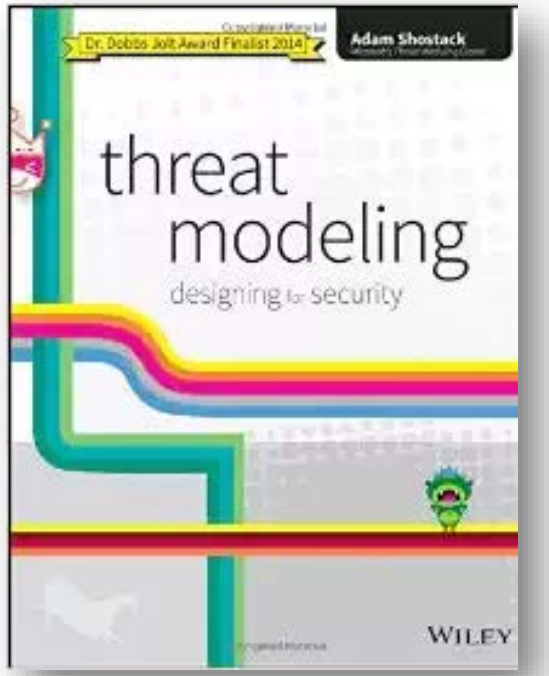


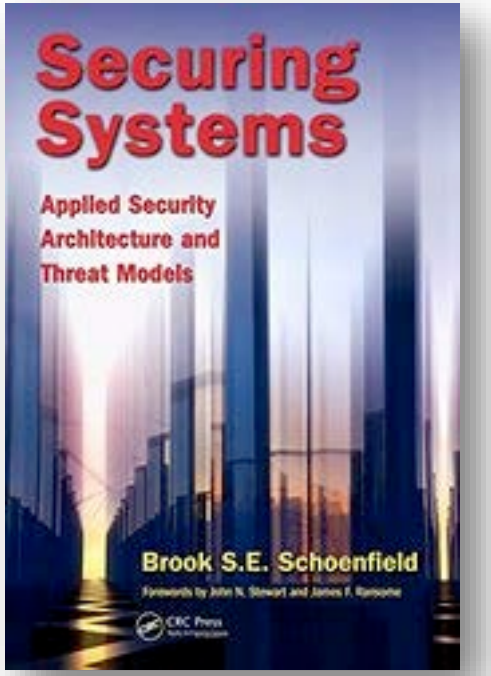


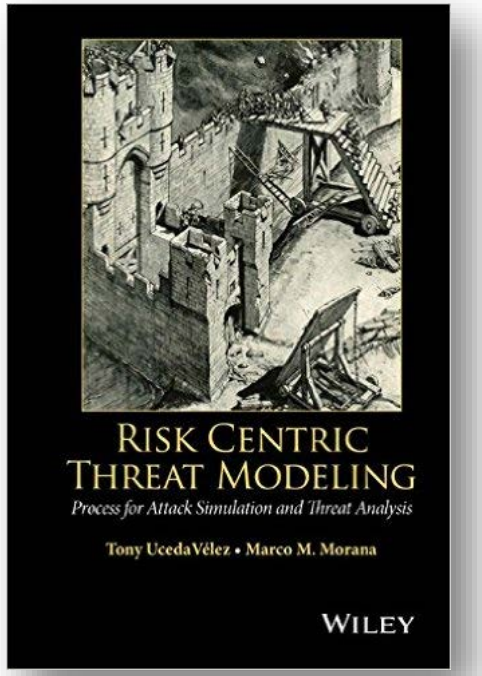


https://www.facebook.com/securingsystems

A Threat Modeling Library







https://www.facebook.com/securingsystems

Developer-centric Security

- Enable creativity and innovation
- Secure innovation
- Let’s start a movement!

Some Resources

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
http://www.intel.com/Assets/en_US/PDF/whitepaper/wp_IT_Security_RiskAssessment.pdf
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

Where To Find Me

Brook.e.schoenfield@intel.com

http://www.brookschoenfield.com

brook@brookschoenfield.com

@BrkSchoenfield

1. I apologize in advance. I only Linkedin with people with whom I've had meaningful interaction. Thanks.

Brook's Social Networking

- https://www.linkedin.com/in/brookschoenfield [1]
- http://www.amazon.com/Brook-S.-E.-Schoenfield/e/B00XQFZLSW

1. I apologize in advance. I only Linkedin with people with whom I've had meaningful interaction. Thanks.

Q & A



www.brookschoenfield.com

