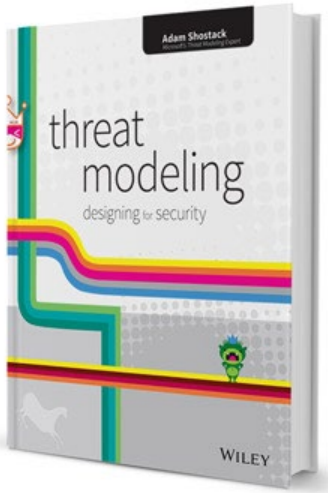
RSAConference2019
San Francisco | March 4–8 | Moscone Center

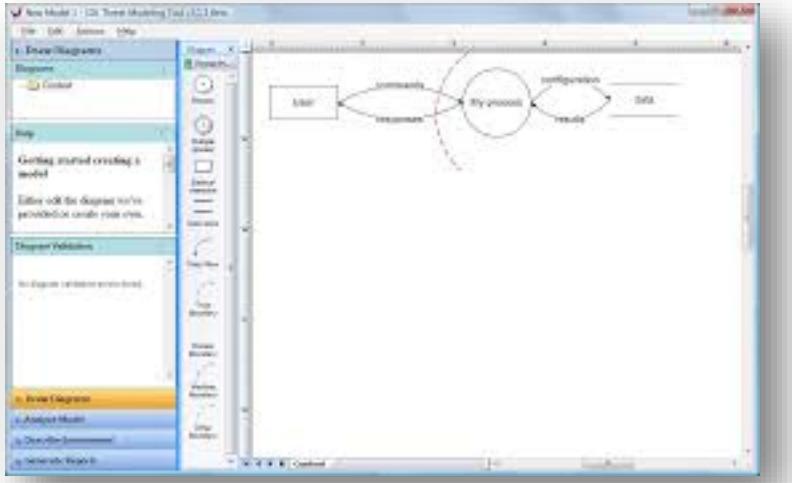
SESSION ID: ASD-F01

Threat Modeling in 2019

Adam Shostack
Shostack & Associates

About Me





Disclaimer: all products and companies mentioned for illustration. No endorsement or criticism implied.

What's Changing in Threat Modeling?

What's changing in the world?

IoT Robot Vacuum Vulnerabilities Let Hackers Spy on Victims

Still work well!

Four Questions for Threat Modeling

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

Agenda

- What are we working on? How are we working on it?
  - The fast moving world of cyber
  - The agile world
- What can go wrong? Threats evolve!

Agenda

- **What are we working on? How are we working on it?**
  - **The fast moving world of cyber**
  - The agile world
- What can go wrong? Threats evolve!

Everything's Changing So Fast!…?

- Models help us see similarities & understand change
- Example: Morris worm (1988)
  - Stack smashing (~1970-now*)
  - Common passwords (epoch – end of days)
  - Mis-configured daemons (1988-200?)

Fast Changing World: IoT

- More sensors and actuators
  - Look like cars and door-opening dogs
- Run Linux like it's 1999
- Cost: lightbulbs to jet engines
- Impact: water sensors to medical devices
- New attackers

The Ways To Threat Model Are … Evolving and Responding

- Many building blocks
  - Tooling: Was MS TM Tool/OWASP Threat Dragon (IDEs)
  - New: Tutamantic (discrete), PyTM (code), IriusRisk (enterprise)*
  - Approaches: STRIDE, Kill Chain
  - Deliverables: documents, bugs, backlogs…
- Building block frame helps understand change

* Disclosure: I'm on the advisory board of Continuum Security, makers of IriusRisk

Agenda

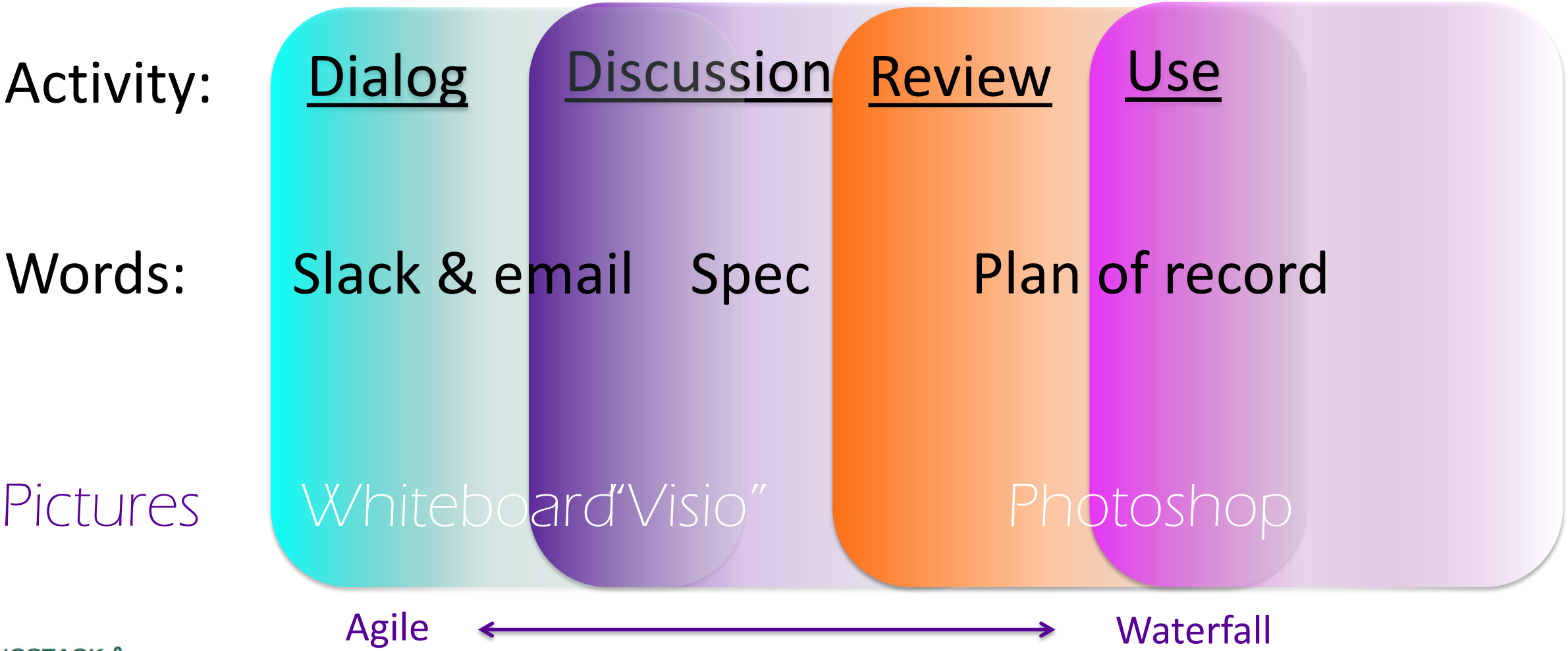
- **What are we working on? How are we working on it?**
  - The fast moving world of cyber
  - **The agile world**
- What can go wrong? Threats evolve!

Fast Moving World of Development

- Threat modeling in agile, CI/CD
- Waterfall vs agile
  - Skills, tasks, frameworks are similar
  - Deliverables and scoping are very different
- Benefits of fast cycles
  - Controls, quality to address threats in the backlog

	Waterfall: “Threat Model Documents”	Agile: “Bugs and conversations”
Working On	• Big complex scope • System diagrams & essays • Gates, dependencies	• Scope tiny: this sprint’s change • Big picture as security debt
Go Wrong	• Brainstorm • STRIDE • Kill Chain	• Same, aim at in-sprint code
Do About It	• Controls • Mitigations • Test cases	• Spikes to understand • Sec-focused stories in sprint, backlog or epic • Sec. acceptance criteria
Quality	• Test plans	• Test automation

Different Deliverables Serve Different Goals



Dialogue Before Discussion

Dialogue

- Explore ideas & consequences
  - "What if?"
  - "How about?"
- Prototypes & experiments
- Fluid not fixed

Discussion

- Commit to one idea
- Production code
- Fixed not fluid

Different Goals of Threat Modeling Work

- Different goals, different deliverables
  - Dialogue: whiteboard
  - Inform: fancy documents
- Implicit goals generate conflict
  - If you want dialogue, don't ask team to bring a diagram
  - "Oh, you want a review and sign off, not new choices!"
- Implicit goals generate work
  - Who needs a fancy document and why?

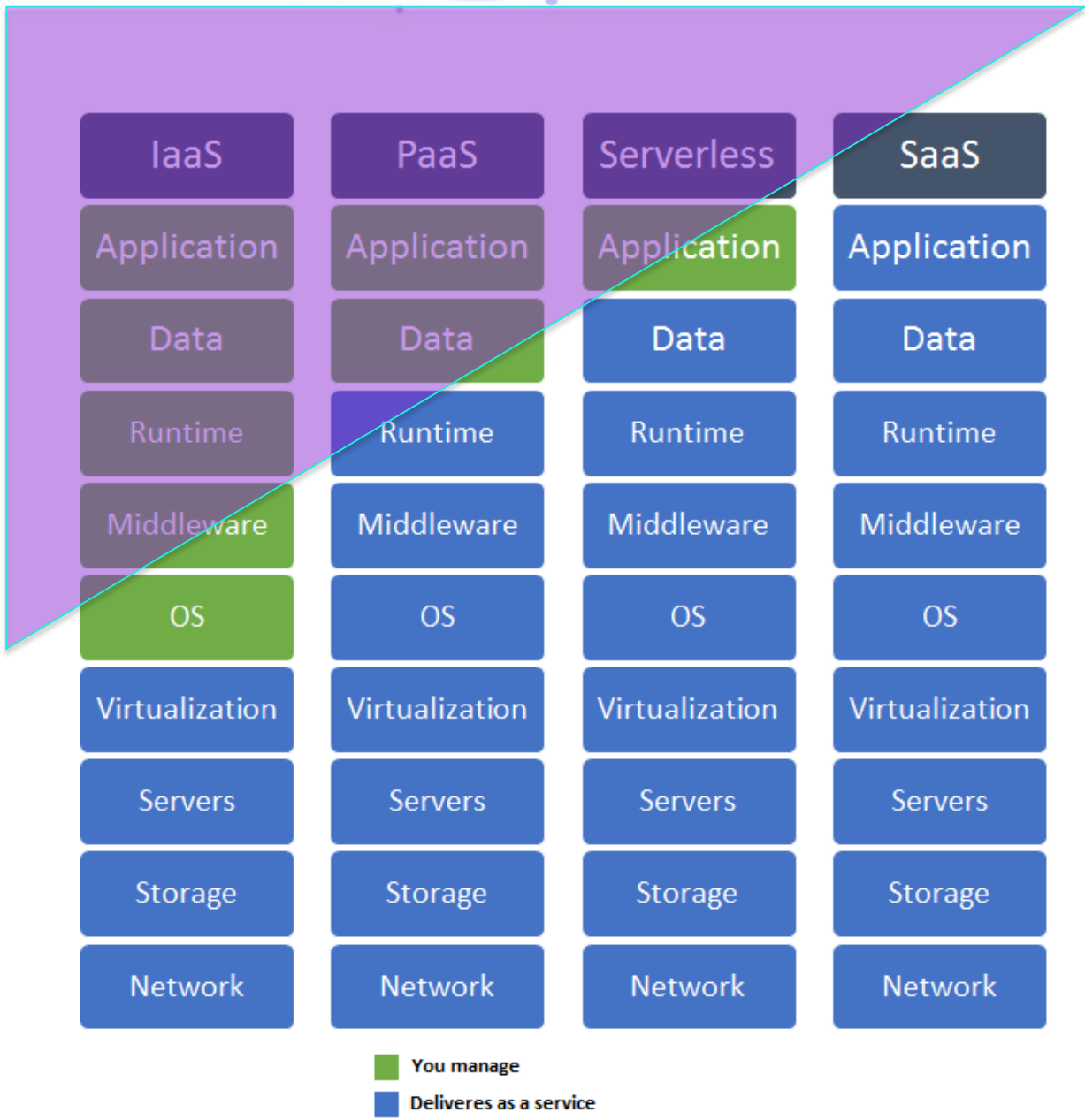
Which Model Is Better?

Starting Threat Modeling When Agile

- Start agily: work the features being built
  - Develop skills
  - Demonstrate value
  - Get buy-in: security properties and assurance
- Then worry about the security debt
  - “What can go wrong” analysis exposes debt
  - All up dataflows (borrow from GDPR)

Cloud and Serverless

- Cloud provider takes over platform issues
  - Platform-level threats are theirs
- Business level threats remain
  - Spoofing an employee of your company to your cloud admin
- Threat model your build, deploy



WHAT CAN GO WRONG?

Agenda

- What are we working on? How are we working on it?
- **What can go wrong? Threats evolve!**
  - **STRIDE**
  - Machine Learning
  - Conflict Modeling

Why Would Anyone Do That?

- Dockless bikes: cable cuts and vandalism

STRIDE

- Turns 20 this year!
- Still helpful mnemonic
  - Spoofing, Tampering, Repudiation, Info Disclosure, DoS, Elevation of Privilege
  - Wide range of system types
  - New details for various threats
- STRIDE-LM

Spoofing

- Phone authentication
- Markets for selfies
- Audio/video spoofing

Spoofing: Phone Authentication

- SMS or calls
  - SMS specifically deprecated by US Gov regulators
- “Phone porting attacks”
- Scamicry: Callers demand authentication from callee

Spoofing Facial Recognition

- Markets for Selfies
  - April 2016: MasterCard announces Identity Check (“Pay with a selfie!”)
  - March 2018: Sixgill reports selfies in darkweb fullz
- Impersonation tools
  - LED Baseball cap allows impersonation

Deepfake Example (SFW)

Deekfake

- Thank you to Nick and Rae of Linkedin Learning
- Part of ”Spoofing in Depth” course (free for now)
- https://www.linkedin.com/learning/threat-modeling-spoofing-in-depth

Spoofing Video

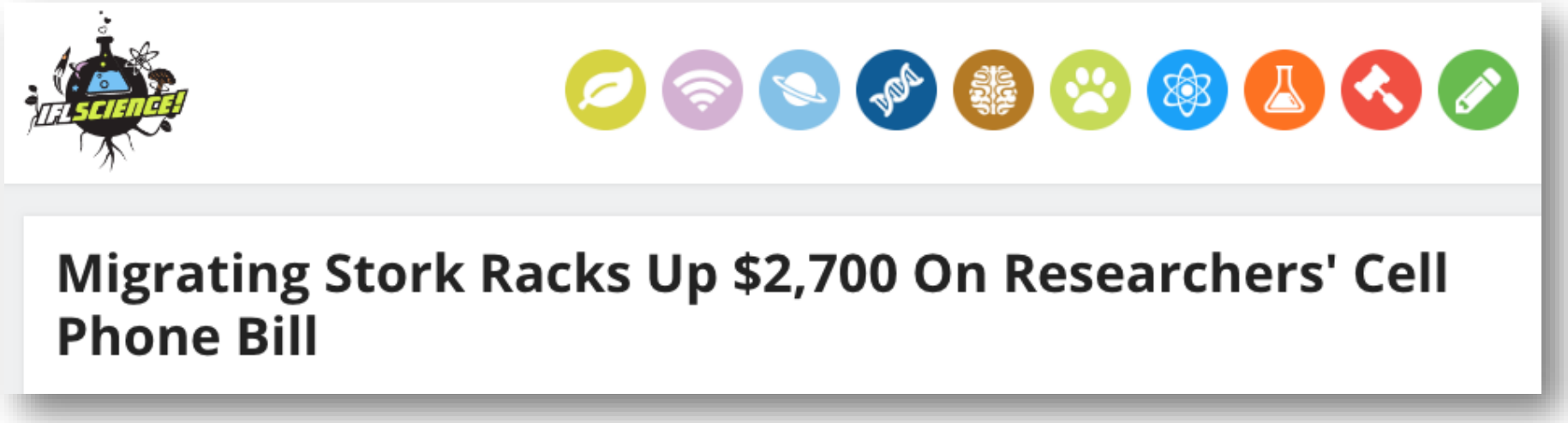
- "Deepfake" video democratizes, improves video fakery
  - Machine learning to imitate a victim
  - Create new video
  - Overlay new faces onto existing
- Google Duplex voice interaction as a service lets you scale
  - BEC 2.0: "This is the CEO, need you to pay …"
  - Phishing 3.0: "Hi honey, just real quick, what's the Netflix pw?"
- Warning: lots of disturbing examples

Tampering

- "AirBNB attacker" can tamper with each device
  - (Thanks to Roy D'Souza for the evocative term)
- Javascript Libraries
  - Statscounter and /account/withdraw/btc
- Tapplock vs screwdriver

Repudiation

- VM Stores: where did that AMI come from?



Information Disclosure

- Location
  - DOD Ban
- Other sensors

Secretive locations are blurred by Google on satellite imagery, but Polar reveals the invidiuals exercising there.

https://www.bellingcat.com/resources/articles/2018/07/08/strava-polar-revealing-homes-soldiers-spies/

Info Disclose & Fast Moving World of Sensors

- Phones drive sensor tech: quality and cost
- Sensors in everything
- Exceed our intuition
  - Accelerometers measure typing
  - Microphones + ultrasound disclose location

Denial Of Service

- Classically absorb compute, storage or bandwidth
  - Compute transforms into crypto currency
- Money
- Battery

Tue, January 07, 2014

My $500 Cloud Security Screwup—UPDATED

circuit breaker

Blink wireless security cameras run for two years on a pair of AA batteries

Hands-on with the anywhere (but outside) camera

By Thomas Ricker | @Trixxy | Sep 29, 2016, 8:29am EDT

Elevation of Privilege

- Many isolation breaks
  - Spectre/Meltdown EoP from cloud, browser
  - It's worse than we thought: "Spectre Is Here To Stay" paper
  - Docker/Kubernetes escapes
  - Lightning cables
- Disentangling device control can be impossible
  - "Depression of Privilege"


The New York Times

Thermostats, Locks and Lights: Digital Tools of Domestic Abuse

Threats Evolve: STRIDE - LM

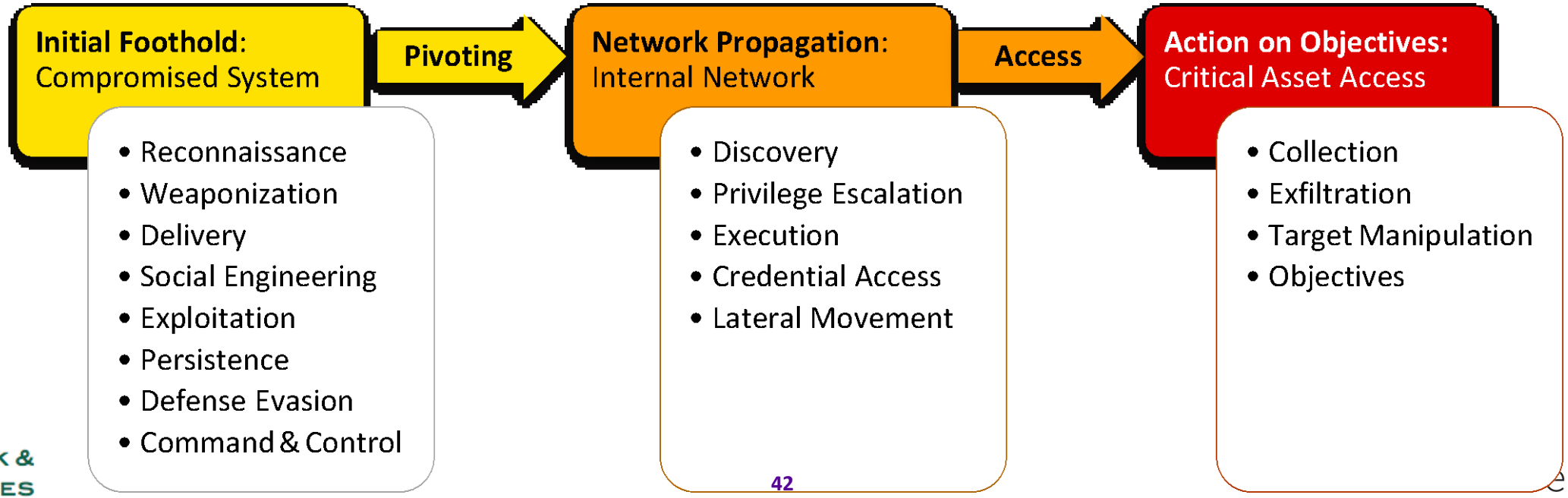
- STRIDE + Lateral Movement
  - Variant that has some momentum for operations threat models
  - Isn't lateral movement a subset of spoofing?
  - Extra ways to find threats can be helpful or annoying
- Only Microsoft can fix LM via asymmetric authN
  - Windows auth vs SSH & keys
- But if -LM helps you, use it

Agenda

- What are we working on? How are we working on it?
- **What can go wrong? Threats evolve!**
  - STRIDE
  - **Machine Learning**
  - Conflict Modeling

Kill Chain as Alternative to STRIDE

- Kill Chain & variants for operational threat models
  - Unifiedkillchain.com for analysis & comparison
  - MITRE ATT&CK



Adversarial Machine Learning

- To violate goals of your ML
- To bend your ML to attacker's goals
  - Attacking code or training data
- Machine learning is code
  - Code has bugs
  - More complex code has more bugs

Agenda

- What are we working on? How are we working on it?
- **What can go wrong? Threats evolve!**
  - STRIDE
  - Machine Learning
  - **Conflict Modeling**

Red Hen on Yelp

Active Cleanup Alert

This business recently made waves in the news, which often means that people come to this page to post their views on the news.

While we don't take a stand one way or the other when it comes to these news events, we do work to remove both positive and negative posts that appear to be motivated more by the news coverage itself than the reviewer's personal consumer experience with the business.

As a result, your posts to this page may be removed as part of our cleanup process beginning Saturday, June 23, 2018, but you should feel free to post your thoughts about the recent media coverage for this business on Yelp Talk at any time.

Got it, thanks!

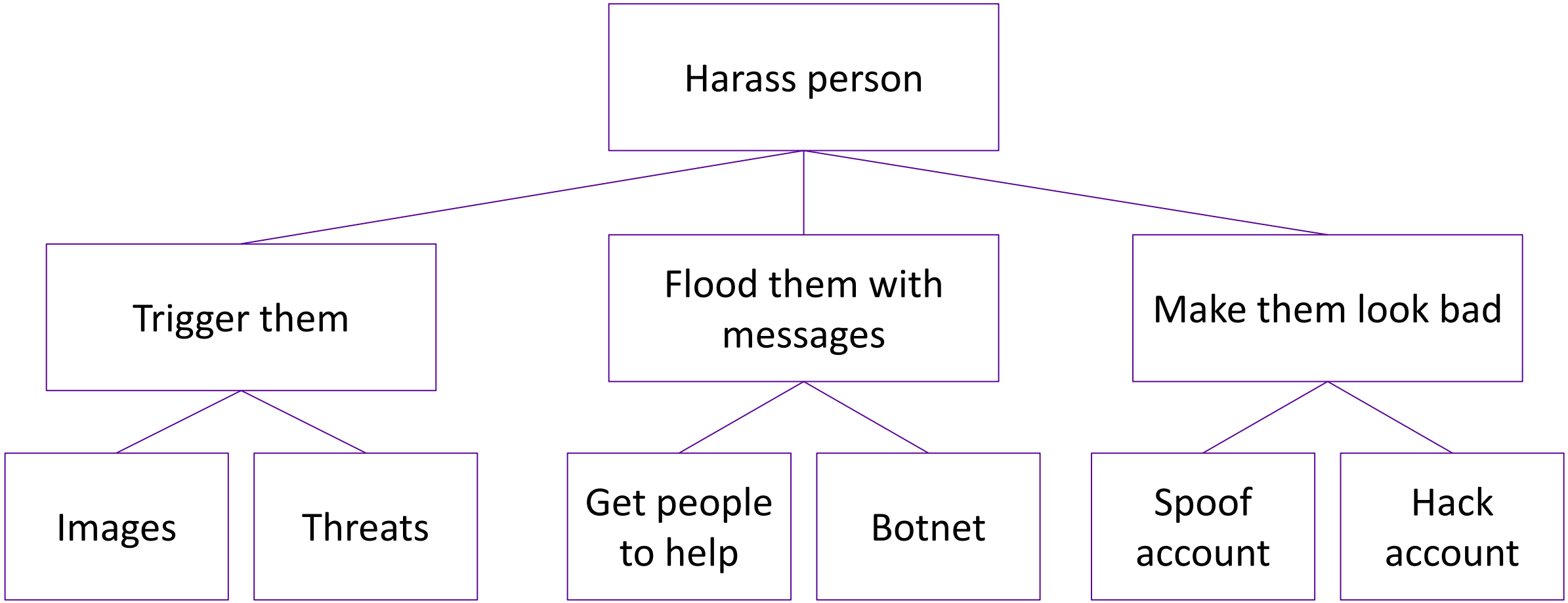
Four Question Frame Works for Conflict

What are we working on?	A system with social aspects or UGC (User Generated Content)
What can go wrong?	Conflict as well as exploit
What are we going to do?	Intuitive measures often fail, we should catalog & study defenses
Did we do a good job?	

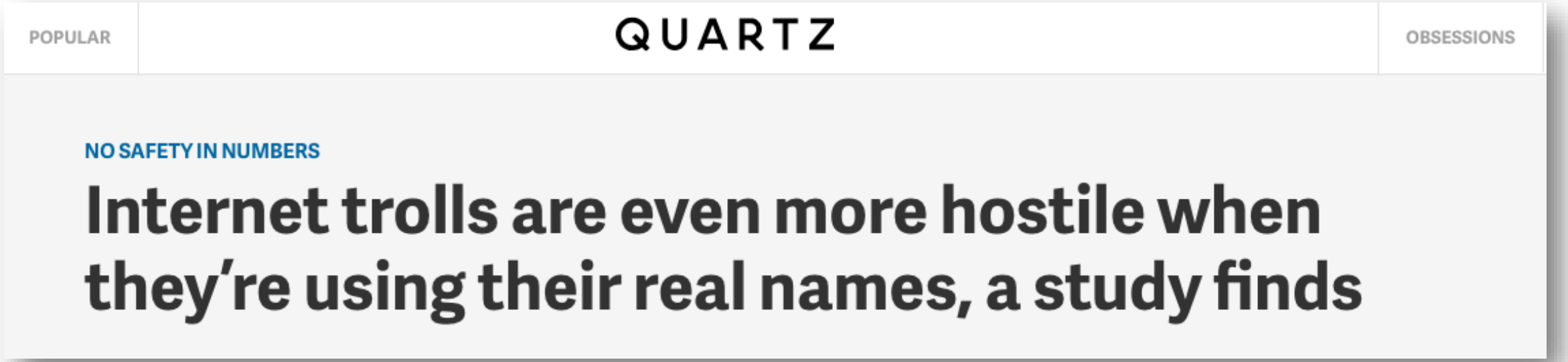
What Goes Wrong: Inter-personal Conflict

- Explicitly adapting threat modeling to conflict
- Shireen Mitchell & Jon Pincus diversity approach
- Amanda Levendowski's SCULPT (in progress)
  - Safety, comfort, usability, legal, privacy, and transparency
  - Focus on mitigation techniques
- Used by nation states!

From “Transforming Tech with Diversity-friendly software” by Jon Pincus & Shireen Mitchell



What to do? Obvious Fixes Fail or Exacerbate


POPULAR

QUARTZ

OBSESSIONS

NO SAFETY IN NUMBERS

Internet trolls are even more hostile when they're using their real names, a study finds

What to Do? Learn from Success

- Nextdoor “private social network for your neighborhood”
- Had a problem with racial profiling in posts
- A/B tested 6 ways to add detail when post mentions race

- Says new forms have “reduced posts containing racial profiling by 75%...”

What to do about conflict?

- Fixes for conflict are less obvious
- Need expertise in human behavior to design
- Need a catalog of effective design patterns
- Github.com/adamshostack/conflictmodeling

Summary: What Can Go Wrong?

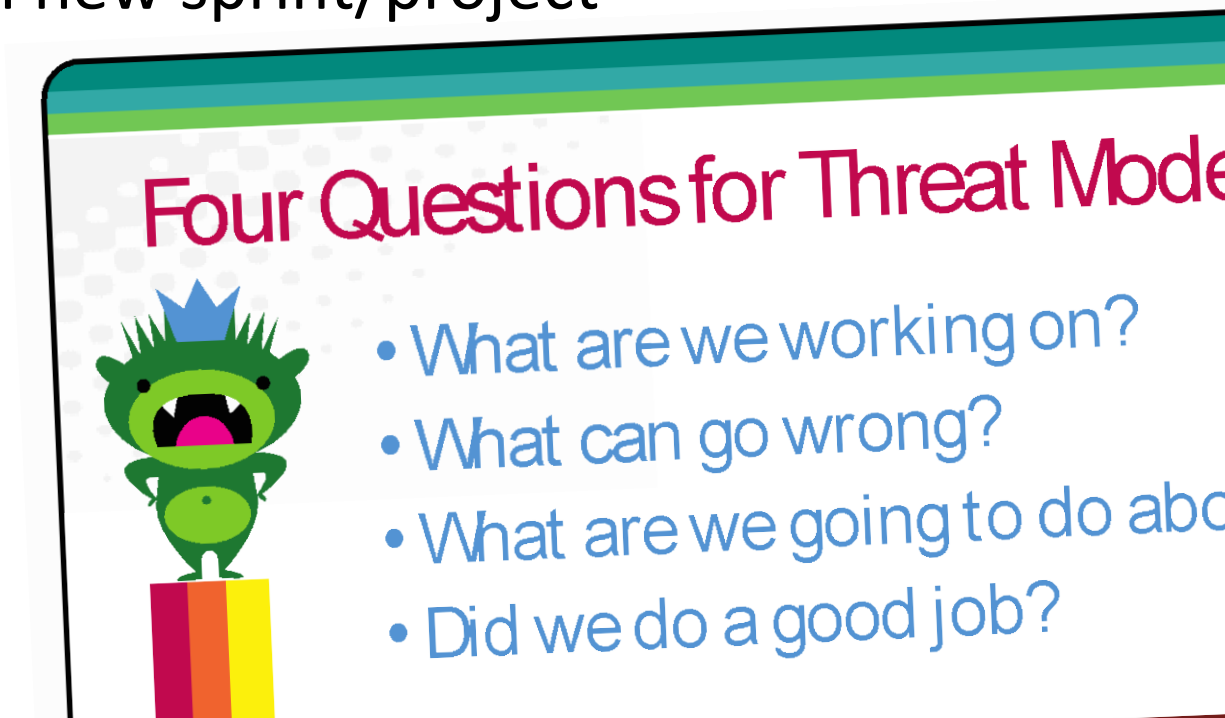
- STRIDE instances evolve
- Adversarial Machine Learning is fun
- Conflict looms

Key Takeaways

- Fundamental skills of threat modeling remain important
- Details of what we're working on, how we work and threats are all changing
- Importance of conflict modeling

Apply What You Have Learned Today

- Next week:
  - Go ask the four threat modeling questions about a project in flight
- Three months:
  - Be asking the four questions in each new sprint/project
  - Learning and adjusting
- Over a year:
  - Start tackling legacy



Thank you!

Also thanks to the team at Continuum, John DiLeo, Jim Gumbley, Shamiq Islam, Jonathan Marcil, Michael Maass, Irene Michlin, Fraser Scott, Izar Tarandach, Steven Wierckx, and many others on the OWASP #threatmodeling slack

(Join us! Owasp.slack.com)

Questions?

adam@shostack.org

associates.shostack.org

Shostack & Associates