Threat Modeling in 2018

Adam Shostack

About Me
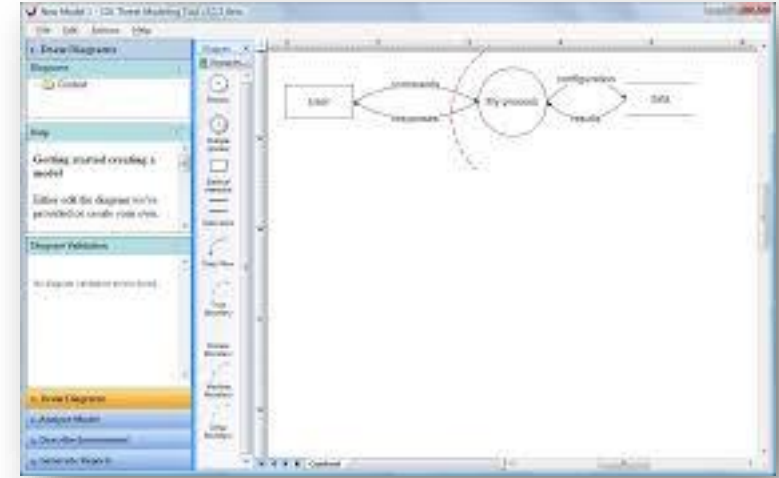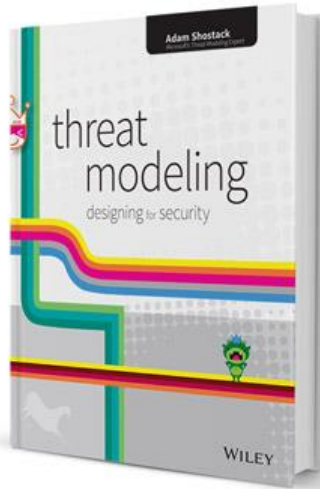
What's Changing in Threat Modeling?

What's changing in the world?

Tyler Barriss, accused of making hoax call, regrets death of 'swatting' victim

• Andrew Finch shot dead on his doorstep by armed police
• Barriss: 'I feel a little remorse for what happened'

TEMPE | DEADLY CRASH WITH SELF-DRIVING UBER

GDPR

Data Protection Officer (DPO) | Compliance | 25 May 2018 | Data Breaches | Personal Data

IoT Robot Vacuum Vulnerabilities Let Hackers Spy on Victims

SECTIONS   SEARCH   NEW YORK POST

Dutch spies reportedly caught Russian hackers on video

By Associated Press   January 26, 2018 | 6:19am

2018 in a Nutshell

Thanks to John of Vordio.net

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
  - Models are scary
- What can go wrong? Threats evolve!
  - STRIDE
  - Machine Learning
  - Conflict Modeling

Four Questions for Threat Modeling

- What are we working on?
- What can go wrong?

THE FAST MOVING WORLD OF CYBER

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

Boston Dynamics

- More sensors and actuators
  - Run Linux like it's 1999
  - Look like cars and door-opening dogs
- 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
  - Tools: MS TM (IDE), Tutamantic (discrete), IriusRisk (enterprise)*
  - Approaches: STRIDE, Kill Chain
  - Deliverables: bugs, backlogs, documents…
- Building block frame helps contextualize change

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

AGILE

Fast Moving World of Development

- Threat modeling is no more inherently waterfall than Ruby
- 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"
System Model	• Big complex scope • System diagrams & essays • Gates, dependencies	• Scope tiny: this sprint's change • Big picture as security debt
Finding Threats	• Brainstorm • STRIDE • Kill Chain	• Same, aim at in-sprint code
Fixes	• Controls • Mitigations • Test cases	• Spikes to understand • Sec-focused stories in sprint, backlog or epic • Sec. acceptance criteria
Quality	• Test plans	• Test automation

Starting Threat Modeling When Agile

- Start agile: 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)

GDPR

- Expensive projects to comply by May, 2018
- Compliance required data flows
  - Useful to threat modeling
- Ongoing programs to remain current
  - Using data flows widely amortizes cost
  - Value from compliance! ☺

"How do you feel about the term "threat modeling?" Is it intimidating/scary/military?" — Eva Galperin

MODELS ARE SCARY

As Easy As Possible, But No Easier

- We should respect the concern
- We should make threat modeling easier

— and —

- People model all the time
- Some things are hard

In a World of Automated Code Generation…

- Models require thought
- Thoughts might be wrong
- Quality requires judgement, not just "it compiles"

- So, models are scary

Which Model Is Better?

"All models are wrong, some models are useful"

—George Box

Dialogue before discussion

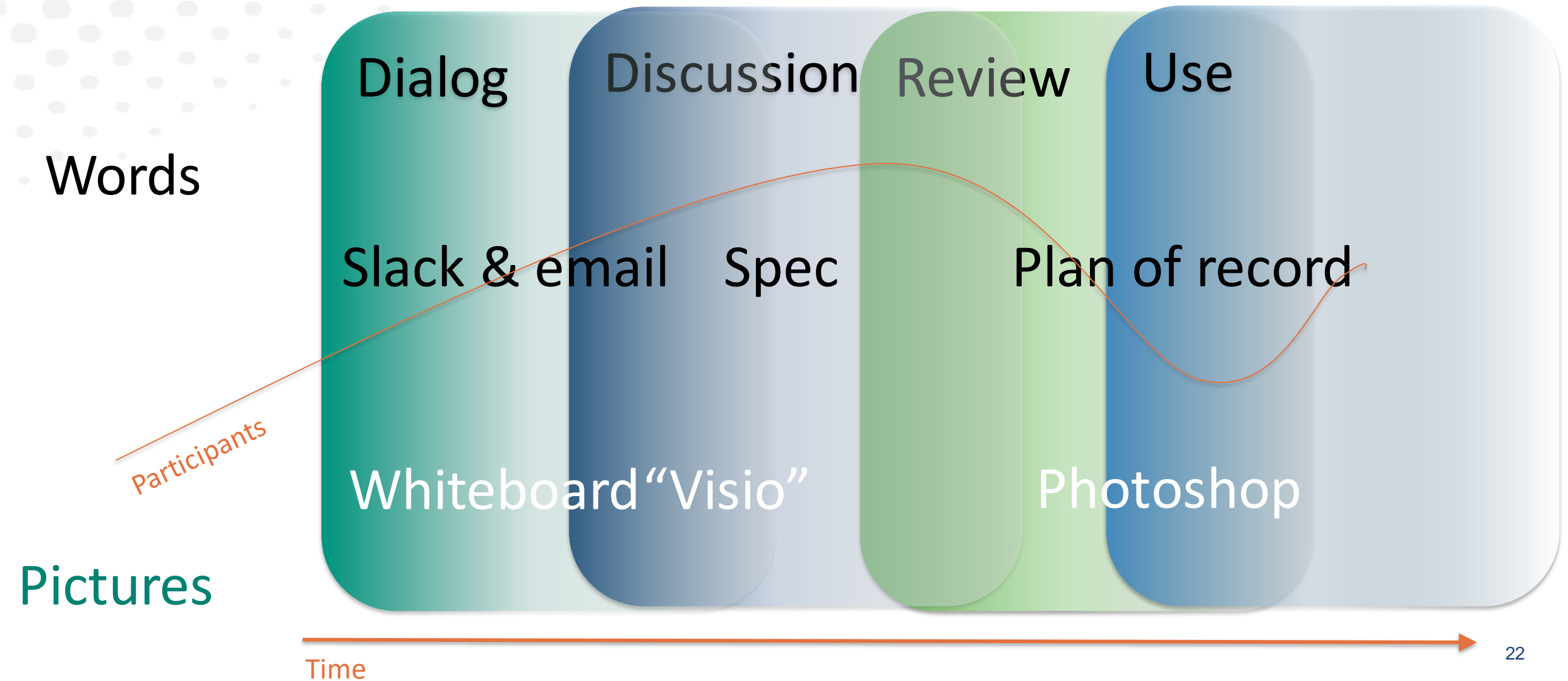**Dialogue**
- Explore ideas and consequences
  - "What if?"
  - "How about"
- Prototypes & experiments
- Fluid not fixed

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

Borrowing from John Allspaw (Etsy, kitchensoap.com)

System Models Serve Different Goals

Dialog

Discussion

Review

Use

Words

Slack & email

Spec

Plan of record

Participants

Whiteboard "Visio"

Photoshop

Pictures

Time

Different Goals

- 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?

WHAT CAN GO WRONG?

"What Can Go Wrong" Agenda

- STRIDE
- Adversarial Machine Learning
- Operations: Kill Chain/Threat Genomics/Att&CK
- Conflict

Why Would Anyone Do That?

- Dockless bikes: cable cuts and vandalism

STRIDE

- **Still helpful mnemonic**
  - Spoofing, Tampering, Repudiation, Info Disclosure, DoS, Elevation of Privilege
  - Not taxonomy
  - Wide range of system types
  - New details for various threats
- **STRIDE-LM** ⍰

Spoofing

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

Spoofing and 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

Spoofing Audio

- Voice cloning as a service!
    - Startups, open source: CandyVoice, Festvox, Vivotext, Lyrebird…
- Formal or background authentication
- 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?"

Spoofing Video

- "Deepfake" video democratizes, improves video fakery
- Machine learning to imitate a victim
- Create new video
- Overlay new faces onto existing
- Warning: lots of disturbing examples

Deepfake Example (SFW)

Tampering

- "AirBNB attacker" can tamper with each device
  - (Thanks to Roy D'Souza for the evocative term)

- Tapplock vs screwdriver

Repudiation

Migrating Stork Racks Up $2,700 On Researchers' Cell Phone Bill

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

Tue, January 07, 2014
My $500 Cloud Security Screwup—
UPDATED

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

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
  - Rowhammer and RAMPage EoP from app
  - We'll see more, and responses are mostly at the platform
- 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
  - Lateral movement ≠ spoofing?
- Only Microsoft can fix LM via asymmetric authN
  - Windows auth vs SSH & keys
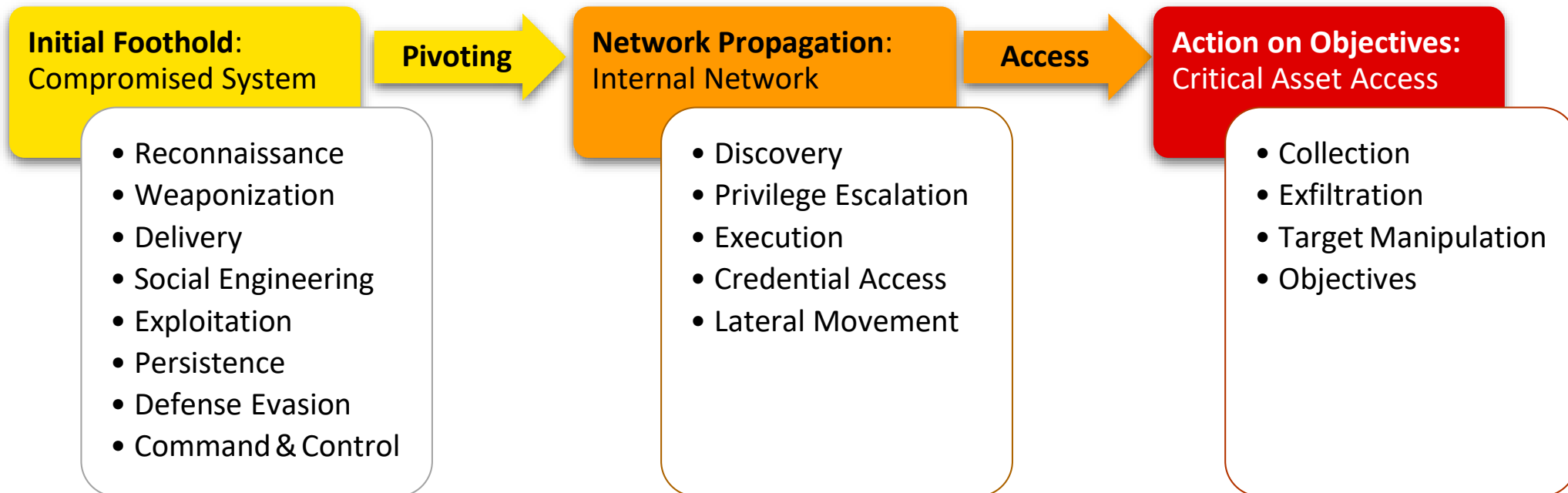- But if it helps you, use it

Machine Learning

Kill Chains

Conflict modeling

THREATS EVOLVE: STRIDE IS ONE OF MANY APPROACHES

Kill Chain as Alternative to STRIDE

- Kill Chain & variants for operational threat models
- Unifiedkillchain.com for analysis & comparison
  - Doesn't yet include threat genomics

Initial Foothold: Compromised System

Pivoting

Network Propagation: Internal Network

Access

Action on Objectives: Critical Asset Access

- Reconnaissance
- Weaponization
- Delivery
- Social Engineering
- Exploitation
- Persistence
- Defense Evasion
- Command & Control

- Discovery
- Privilege Escalation
- Execution
- Credential Access
- Lateral Movement

- Collection
- Exfiltration
- Target Manipulation
- Objectives

Adversarial Machine Learning

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

More on AML, See "Protecting the Protector", by Holly Stewart, Jugal Parikh & Randy Treit, Thurs Noon, South Seas CDF

What goes wrong isn't just sploits

CONFLICT & THREAT 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!

45

Attackers Adjust

Bella Sophia W.
Thousand Oaks, CA
0 friends
3 reviews

★☆☆☆☆ 6/24/2018

I was very disappointed in the quality of my food. Server was very unpleasant.
I would not recommend this restaurant .

Was this review ...?

Useful   Funny   Cool

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-state Conflict

- "Fake news"
- Computational propaganda
- Election interference (Facebook's breakdown)
  - Attacks on knowledge including fake messages
  - Safety of elections: harassment, account takeover, threats of violence against voters, candidates, election officials
  - Disenfranchise/reduce turnout
- Armies of trolls

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
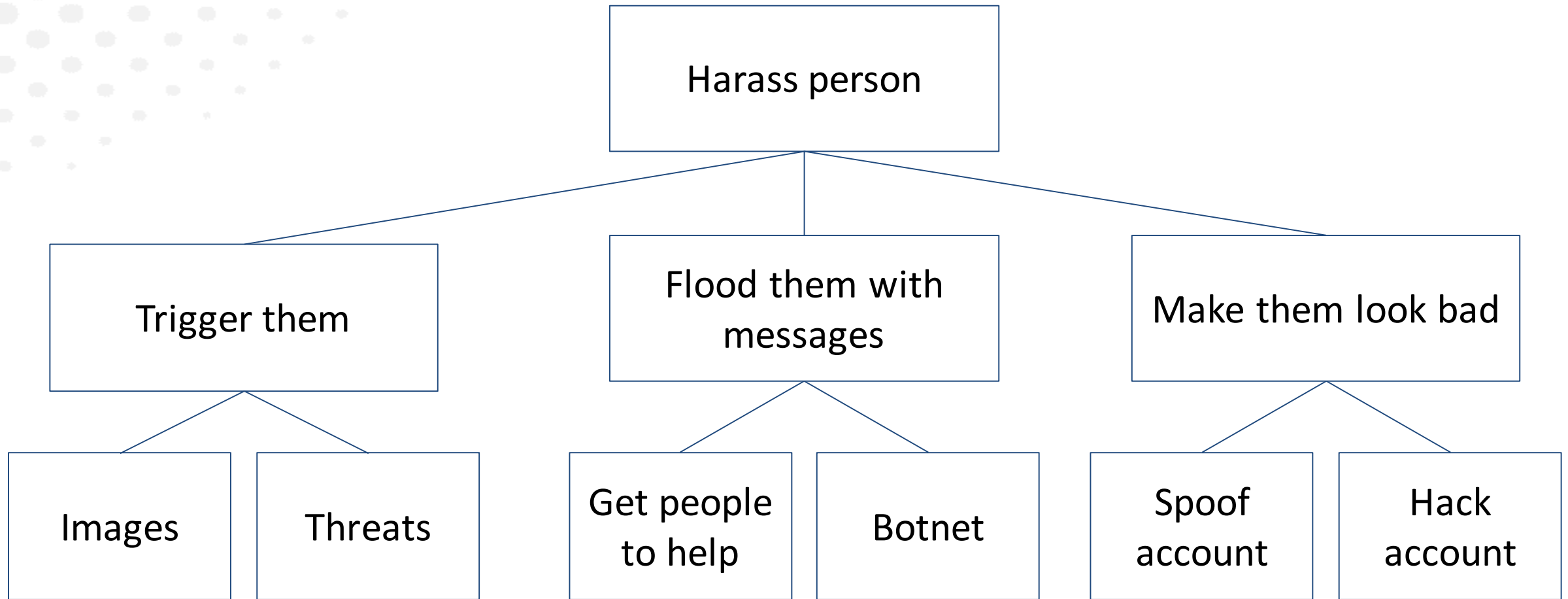
What to do?
Obvious Fixes Fail or Exacerbate

QUARTZ

POPULAR

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

Summary: Threats

- 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

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