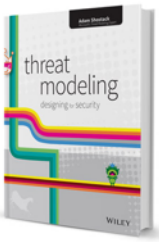
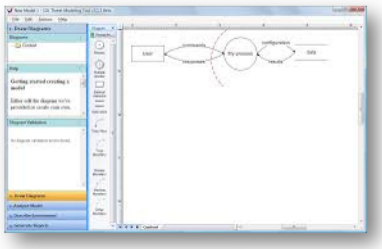
Threat Modeling in 2018

Adam Shostack

The PDF is in ‘notes’ view because there are lots of URLS in the 2nd half.

About Me





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

2

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'

IoT Robot Vacuum Vulnerabilities Let Hackers Spy on Victims

NEW YORK POST

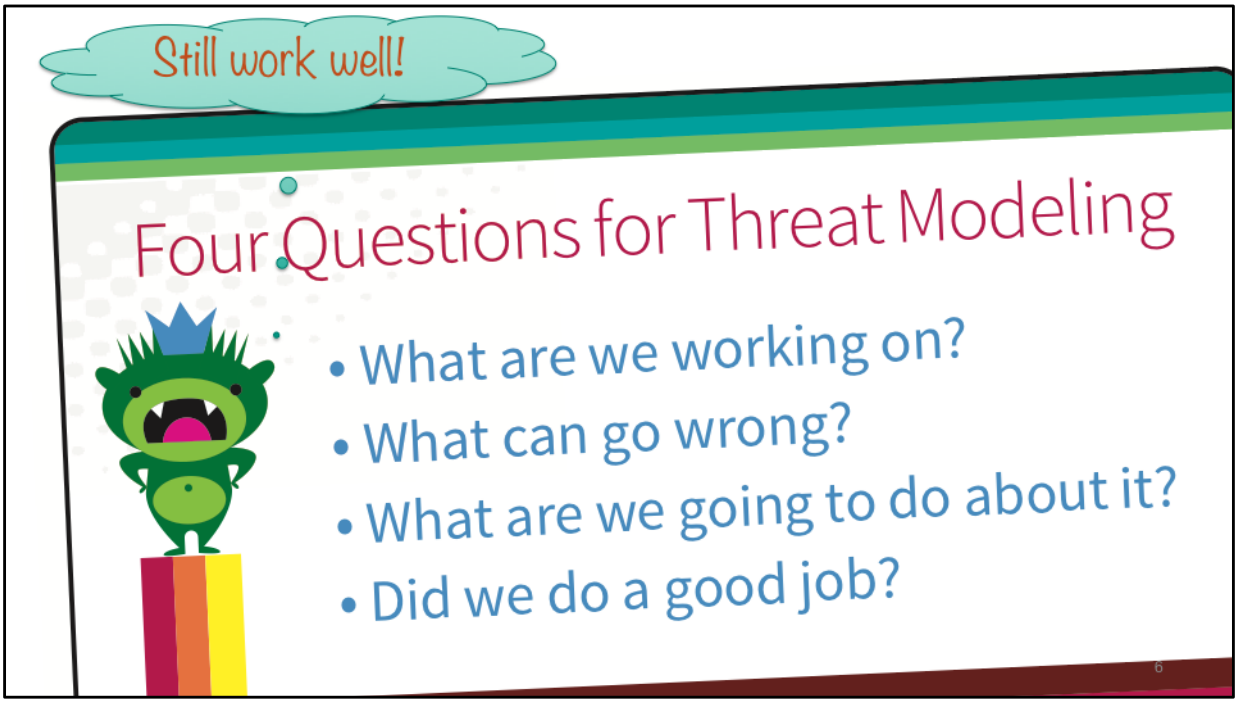
Dutch spies reportedly caught Russian hackers on video

By Associated Press

3

Kim Yong Chol, former NK military intel chief, FBI has publicly attributed break in to NK https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

https://www.youtube.com/watch?v=EmBneh0oy7E


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?
  - The fast moving world of cyber
  - The agile world
  - Models are scary
- What can go wrong? Threats evolve!
  - STRIDE
  - Machine Learning
  - Conflict Modeling

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?)

9

* Now if you include IoT which fails to compile with modern defenses.

Fast Changing World: IoT

- 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

10

New attackers are covered in Tampering, EoP and Conflict

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

11

Explicitly not "the way to threat model is"

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*

13

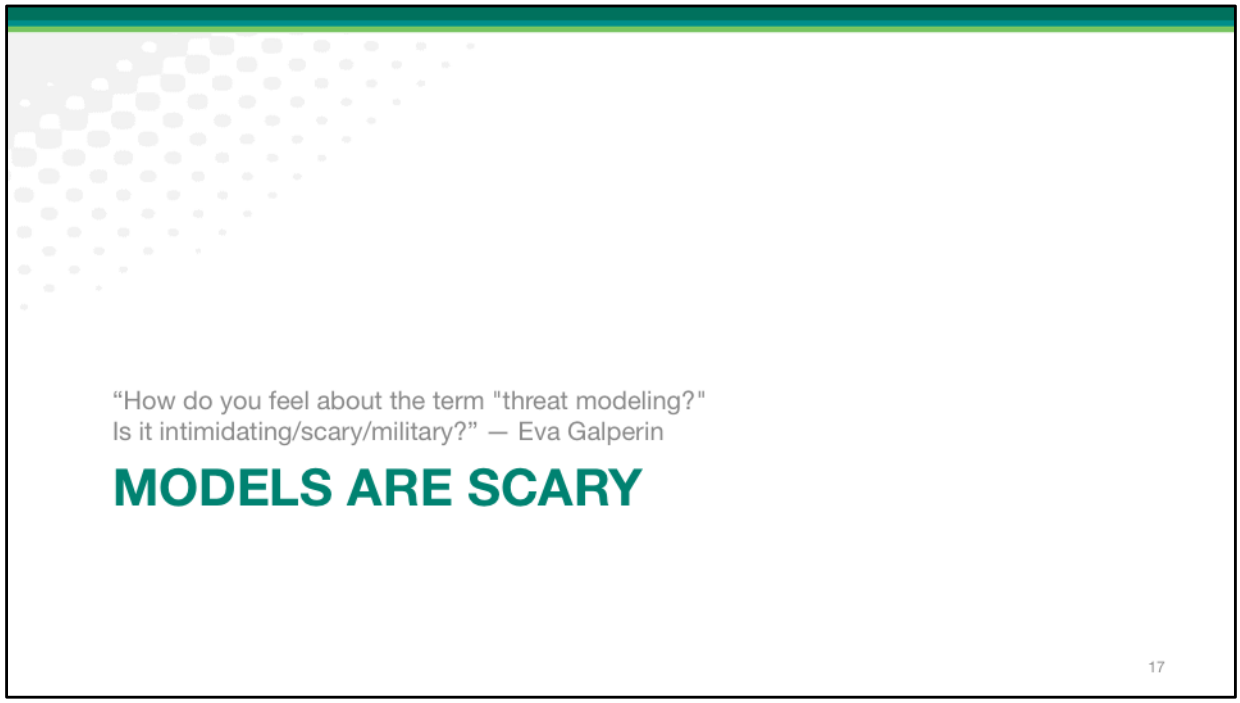
	Waterfall: "Threat Model Documents"	Agile: "Bugs and conversations"
System Model	• Big complex scope • System diagrams & essays • Gates, dependencies	• Scope tiny: this sprint's change • Big picture as security debt
Finding Threats	• Brainstorm • STRIDE • Kill Chain	• Same, aim at in-sprint code
Fixes	• Controls • Mitigations • Test cases	• Spikes to understand • Sec-focused stories in sprint, backlog or epic • Sec. acceptance criteria
Quality	• Test plans	• Test automation

14

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)

15



https://twitter.com/evacide/status/878695077085708288

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

18

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

19

Which Model Is Better?

“All models are wrong, some models are useful”

—George Box

21

Dialogue before discussion

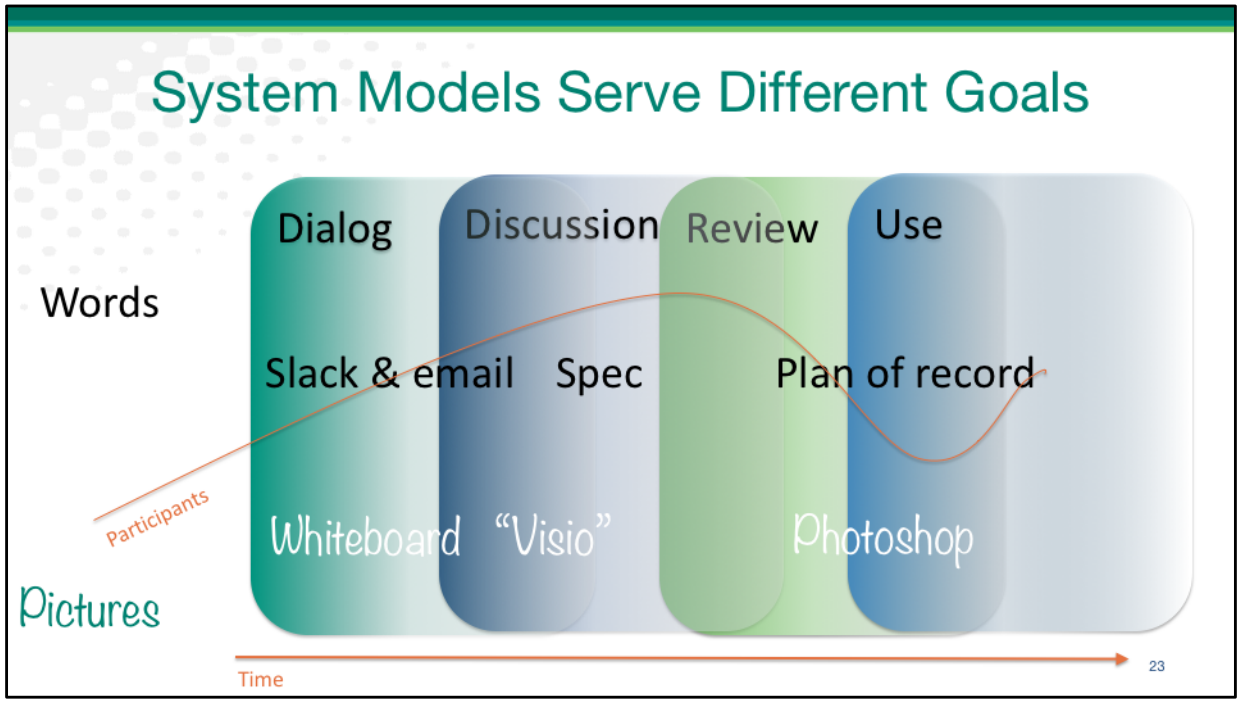
Dialogue

- 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)



Discussion and dialog, Allspaw's Kitchen Soap blog

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

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 

28

Spoofing

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

29

Spoofing and Phone Authentication

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

30

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

31

https://techcrunch.com/2016/10/04/mastercard-launches-its-selfie-pay-biometric-authentication-app-in-europe/
https://darkwebnews.com/dark-web/selfie-darknet-sale/
https://arxiv.org/pdf/1803.04683.pdf

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?”

32

https://www.theverge.com/tldr/2018/4/17/17247334/ai-fake-news-video-barack-obama-jordan-peele-buzzfeed

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

33

https://www.theverge.com/tldr/2018/4/17/17247334/ai-fake-news-video-barack-obama-jordan-peele-buzzfeed

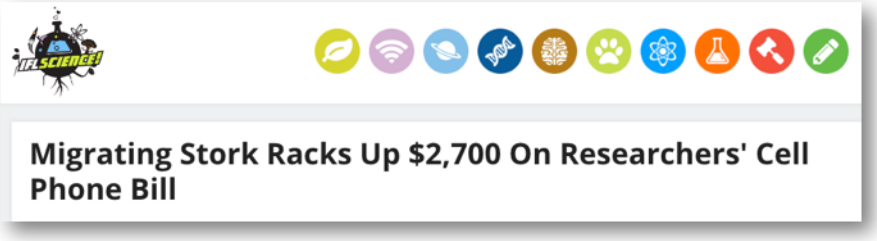
Tampering

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

35

https://www.theregister.co.uk/2018/06/15/taplock_broken_screwdriver/

Repudiation



36

http://www.iflscience.com/plants-and-animals/migrating-stork-racks-up-2700-on-researchers-cell-phone-bill/

Information Disclosure

- Location
- 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/

37

https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases
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

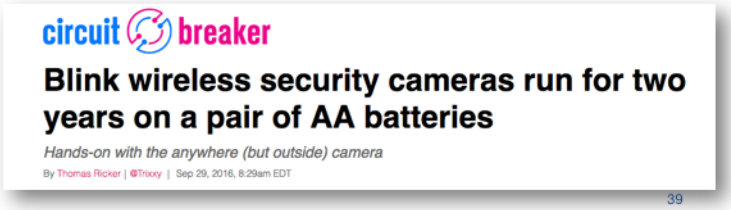
38

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



39

https://www.eetimes.com/document.asp?doc_id=1333308

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

40

Stress how usability again becomes a security property, and how hard configuration can be to understand.

https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html
https://threatpost.com/rowhammer-variant-rampage-targets-android-devices-all-over-again/133198/

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

41

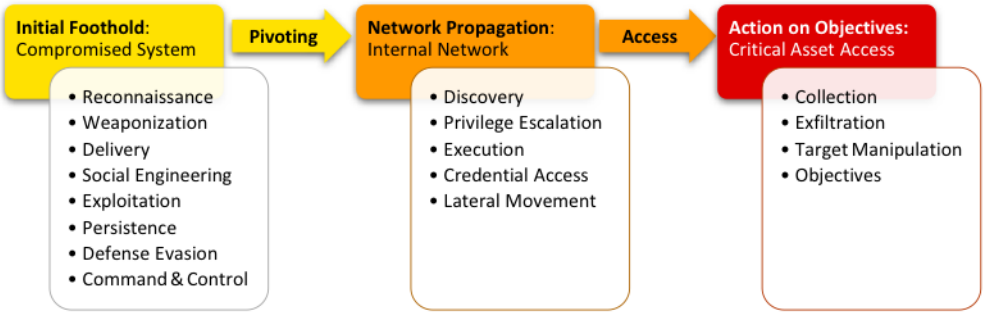
SSH auth forwarding still rocks by default ☺

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



43

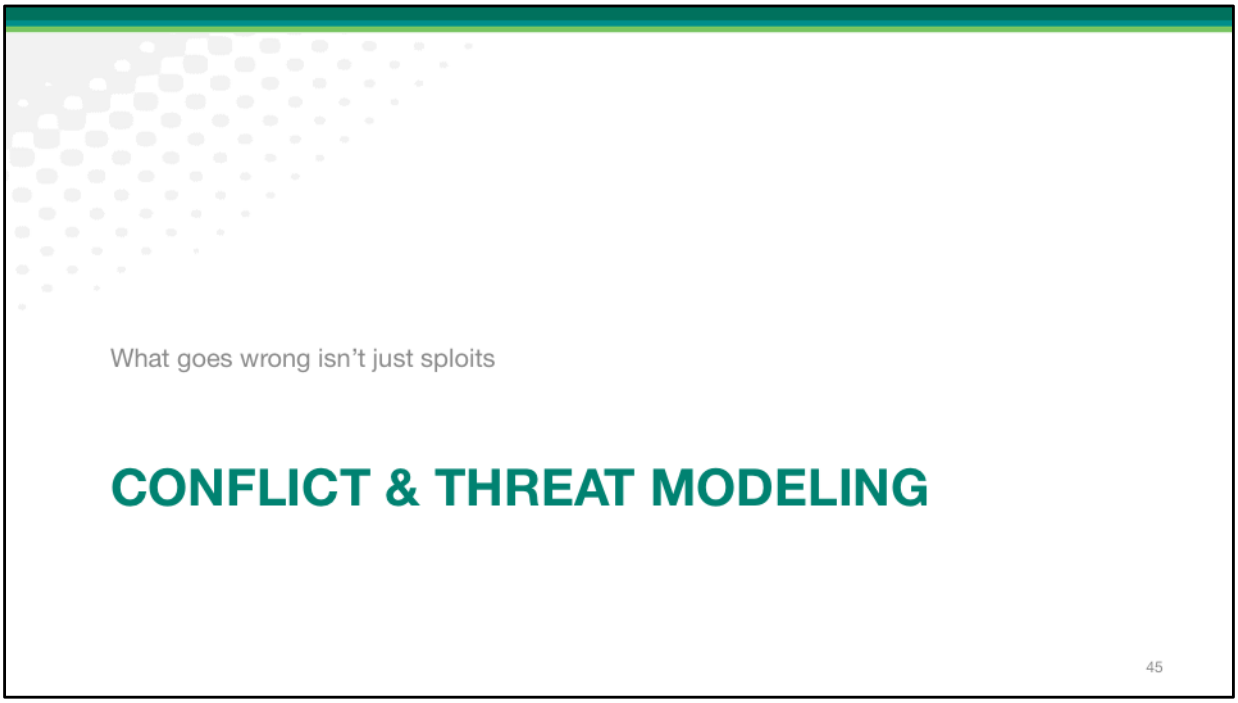
Paul Pols

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

44

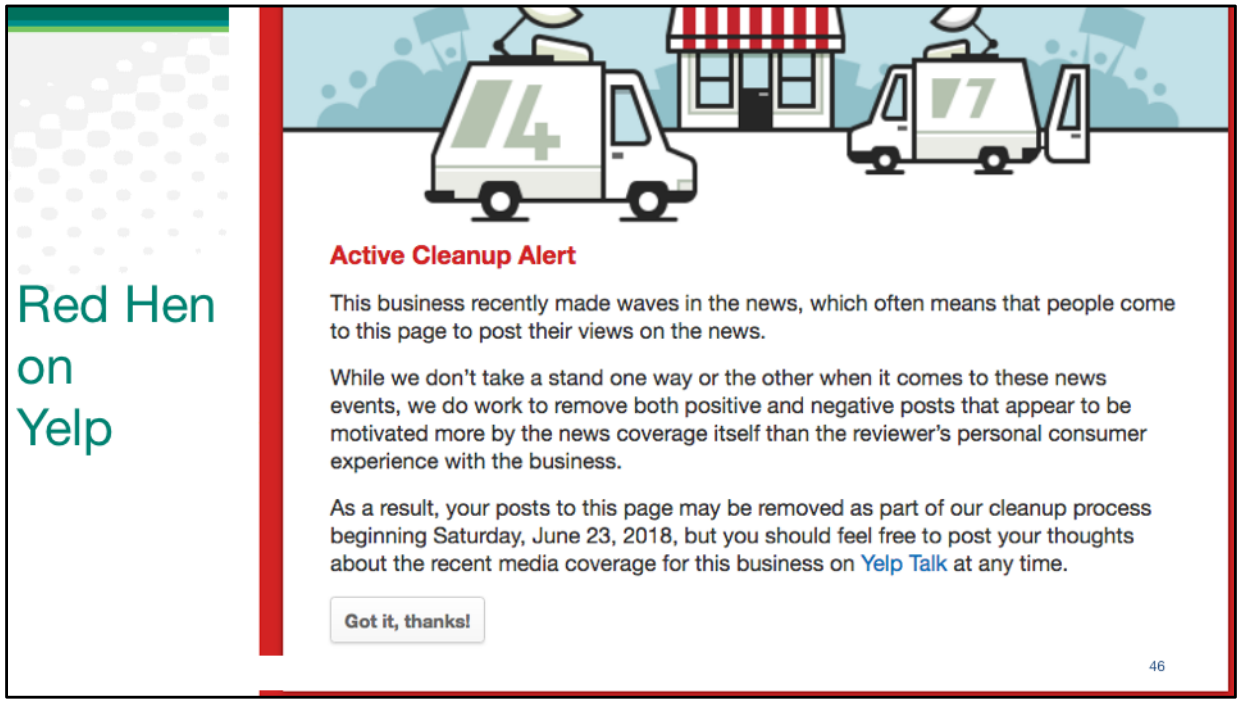
More complex code, more bugs goes back to the intro to the 1st ed of firewalls & Internet security by Cheswick & Bellovin



Conflict

- Countries & “Non-state actors” with geopolitical goals
- Between groups
- Between people

”non-state actors” like ISIS



Note the technical choices: create an interstitial; review (rather than delay) reviews; explain what a good review is
https://www.yelp.com/biz/the-red-hen-lexington-3

https://www.nbcwashington.com/news/local/Wrong-Red-Hen-DC-Restaurant-Getting-Death-Threats-After-Spot-With-Same-Name-Booted-Sarah-Huckabee-Sanders-486500061.html

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?	

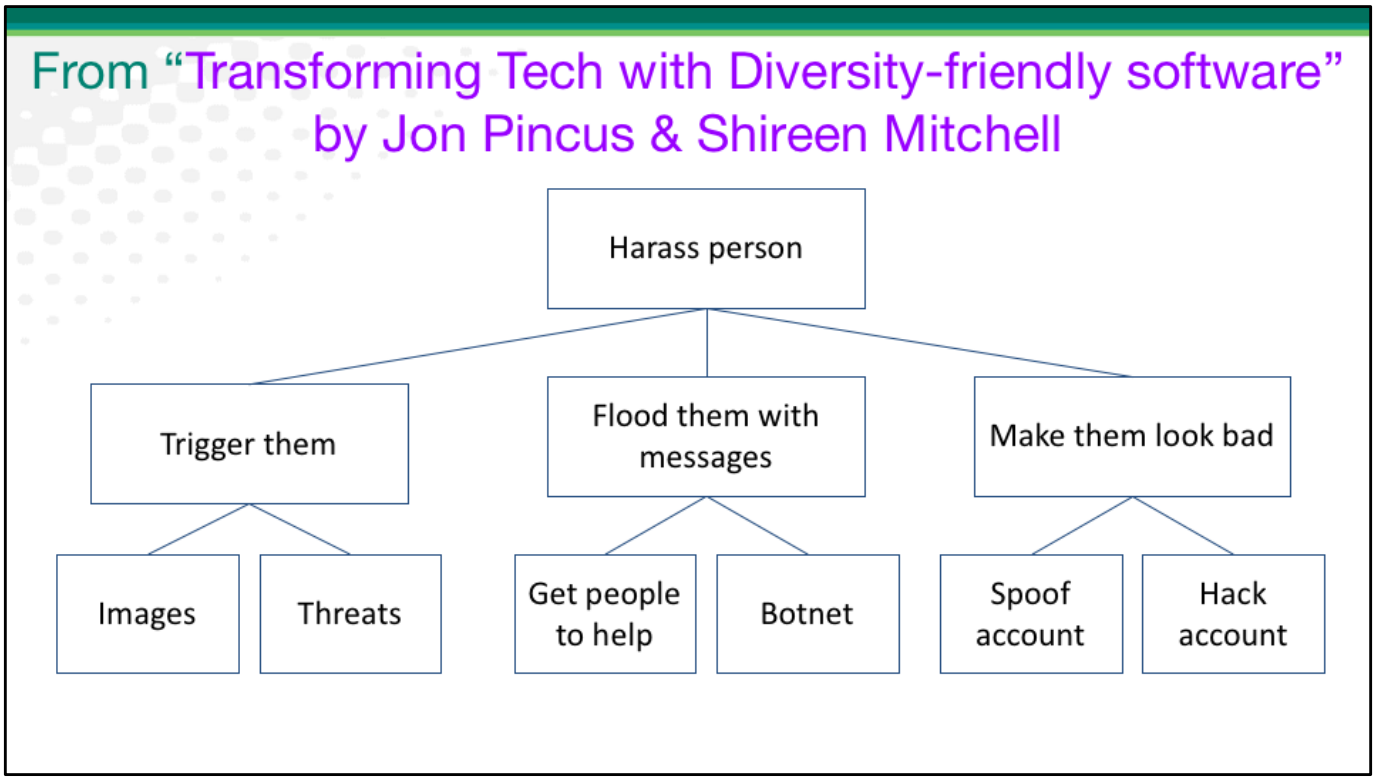
48

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!

50

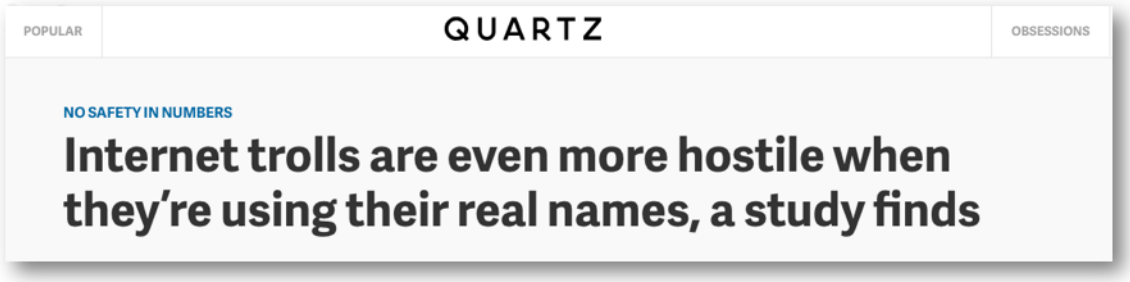
https://www.levendowski.net/conflict-modeling
http://achangeiscoming.net/2017/04/15/transforming-tech-diversity-friendly-software/



Here's a more structured example. What are some of the ways an harasser could attack somebody?

Original: https://docs.google.com/presentation/d/1JB3bTbJvjEypKlPu1JKV20Oz9YlF5zRCl3vLIPdDTrA/edit#slide=id.g2073602466_0_0

What to do?
Obvious Fixes Fail or Exacerbate



52

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%...”

53

https://splinternews.com/how-nextdoor-reduced-racist-posts-by-75-1793861389
https://blog.nextdoor.com/2016/08/24/reducing-racial-profiling-on-nextdoor/

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

56

Key Takeaways

- Fundamental skills of threat modeling still work
- 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