You got your design team in my security team!

You got your security team in my design team!

Eleanor Saitta  @Dymaxion  O’Reilly Velocity Santa Clara 2016
Security Architecture & Design at Etsy

I’m new here
I’m not even supposed to be here today.

Why talk security+design to devops folks?
The Celestial Emporium of Malicious Knowledge

There are four kinds of security issues:

- Those that should not exist
- DDoS
- Those that are math problems
- Those involving people
Are you fighting security problems that shouldn’t exist?
Try Langsec today!

➢ Do your parsers accept things they shouldn’t?
➢ Are your random numbers not random?
➢ Do your buffers overflow?

Dozens* of people like you have found a solution!
Don’t Be That Guy
Yes, We Still Need to Keep Machines Happy

"There are two kinds of people who ponder stories of a machine apocalypse:
Those who fear an error in machine judgment, and those who fear humans being judged."
- Taylor Swift

Langsec doesn’t erase traditional security practices. We’ll never escape from code review, analysis tools, monitoring, incident response, forensics, etc. It’s also important that we don’t think this is all security is.
Security is the set of activities that reduce the likelihood of a set of adversaries successfully frustrating the goals of a set of people we like.
People use systems to act in the world.

No one cares about the system.

They care about the impact the system has in the world.
Your team and your product do not matter.

The only thing that matters is what you enable the humans you care about to do in the world and what they learn along the way.
Worse is Better
Security is Just Another System Property
You think this is a fucking game ?!

Your Responsibility to the Internets
Designing Resilient Security
Do you know what your humans are trying to do?
"Trust does not scale because trust is not reducible to math."

- Taylor Swift
Adversaries are Human Too

I ALSO

LIKE TO LIVE DANGEROUSLY
IN TROUBLE
WE GOT

User Learning & Journeys
Cognitive overhead
OODA loops and operational planning
Stress response
Community and group dynamics
Obstacle and defense patterns
Invariants
Ceremonies
Legibility
Participation frames
Adversary models
Social attacks
Performativity and engagement
Deployability
Security design goals
Playtesting
Threat models
Security objectives
Cognitive overhead
OODA loops and operational planning

NO TIME TO EXPLAIN
GET IN THE CAR

Threat models
Security objectives
Enabling Security Design

"You can eliminate irreducible complexity - just fire everyone who understands it.

Now you have a simple black box."

- Taylor Swift
Sad Panda needs a hug

Be nice
Learn how to talk to each other

IT’S DANGEROUS TO GO ALONE! TAKE THIS.
Measure all of the things
Programming is like any profession where you sit in front of a box and hate yourself for not thinking enough like a machine.

- Taylor Swift

Let engineers engineer and designers design
Three Takeaways
1. Enable collaboration internally between security and everyone else
2. Build holistic security and get design in the security loop
3. Learn what your product does
The two best security books you can buy right now:

**BADASS**
Making Users Awesome

*KATHY SIERRA*

**Engineering a Safer World**
Systems Thinking Applied to Safety

*Nancy G. Leveson*
Thank you!

http://ella@dymaxion.org

twitter

O'Reilly Velocity Santa Clara 2016

You got your design team in my security team!