humu

Building for Trust:

Because we don't *all* have to learn lessons the hard way

Lea Kissner
Chief Privacy Officer, Humu

@LeaKissner
leak@humu.com

Why am I here?

Why am I here?

Failure.

Why am I here?

Failure.

No, really.

Why am I here?

Failure.

No, really.

Framework on how to help teams build with respect.

Tested, practical in the face of edges.

Edges

- **The world is made of edges.**
  - Systems are large enough that “edge cases” aren’t
  - There are so many humans and so many types of human

- **“If something happens to 1/1,000,000 users once per year, at Google that’s best expressed as *‘six times per day’*.” -Andy Schou**

Outline

1. *Why build for trust, build with respect*
2. *Framework*
3. *Collaboration: technical*
4. *Collaboration: public policy/regulation*

Outline

1. ***Why build for trust, build with respect***
2. *Framework*
3. *Collaboration: technical*
4. *Collaboration: public policy/regulation*

Building for trust

- **Our goal is to build for trust**
  - Willingness to engage with us
  - Willingness to believe in our reliability
  - Willingness to believe we speak the truth
  - Willingness to believe we act with respect

Building for trust

- **Our goal is to build for trust**
  - Willingness to engage with us
  - Willingness to believe in our reliability
  - Willingness to believe we speak the truth
  - Willingness to believe we act with respect

- “Respect is a **positive feeling or action shown towards someone or something considered important, or held in high esteem or regard**; it conveys a sense of admiration for good or valuable qualities; and it is also the **process of honoring someone by exhibiting care, concern, or consideration for their needs or feelings**.” – Wikipedia

Building for trust

- Why build for trust?

Building for trust

- Why build for trust?

Building for trust

- Why build for trust?
- Would you like to buy a Pinto?

Building for trust

- Why build for trust?

- Would you like to buy a Pinto?

Building for trust

- Why build for trust?
- Would you like to buy a Pinto?
- The Pinto was about average for subcompact car safety.*

* Schwartz, Gary T. (1991). “The Myth of the Ford Pinto Case.” *Rutgers Law Review*. 43: 1013–1068.

Outline

1. *Why build for trust, build with respect*
2. ***Framework***
3. *Collaboration: technical*
4. *Collaboration: public policy/regulation*

Building with respect

Building with respect

- Product teams want to build a great product.

Building with respect

- Product teams want to build a great product.

- No one is an expert in everything.

Building with respect

- Product teams want to build a great product.
- No one is an expert in everything.

Building with respect

- Product teams want to build a great product.
- No one is an expert in everything.
- Start at the beginning.

Building with respect

- Product teams want to build a great product.
- No one is an expert in everything.
- Start at the beginning.
- If you can’t, don’t despair.

Steps for respect review

1. *Find all the parts.*
2. *Check the invariants.*
3. *Model the threats.*
4. *Triage and correct issues.*
5. *Document, document, document.*

Steps for respect review

1. ***Find all the parts.***
2. *Check the invariants.*
3. *Model the threats.*
4. *Triage and correct issues.*
5. *Document, document, document.*

Steps for respect review

1. *Find all the parts.*
2. ***Check the invariants.***
3. *Model the threats.*
4. *Triage and correct issues.*
5. *Document, document, document.*

Check the invariants

- **Invariants are the baseline promises that you have made to yourself or others.**
  - Driven by regulations or contracts
  - Promises you have made to your users
  - Promises you have made to yourself to protect affected parties

Check the invariants

- **Invariants are the baseline promises that you have made to yourself or others.**
  - Driven by regulations or contracts
  - Promises you have made to your users
  - Promises you have made to yourself to protect affected parties

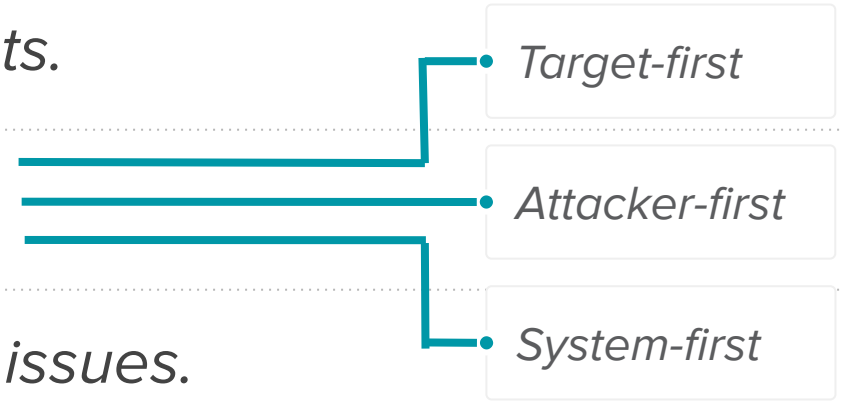
- **Start by checking invariants**
  - Faster than the more in-depth analysis
  - No point in further work until the invariants are satisfied

Steps for respect review

1. *Find all the parts.*
2. *Check the invariants.*
3. ***Model the threats.***
4. *Triage and correct issues.*
5. *Document, document, document.*

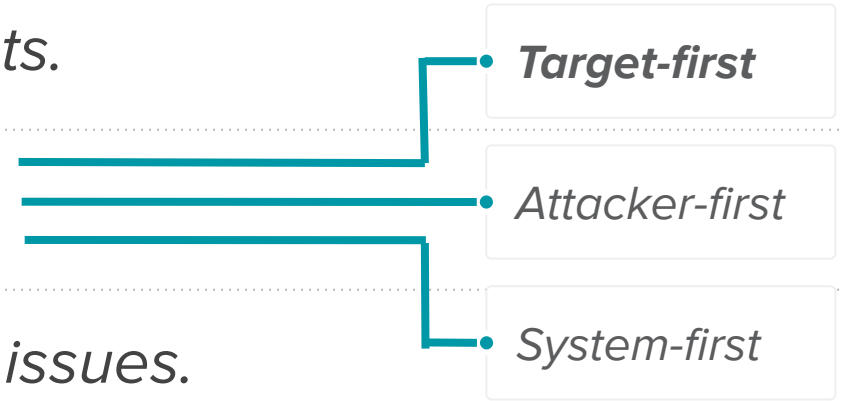
Steps for respect review

1. *Find all the parts.*
2. *Check the invariants.*
3. ***Model the threats.***
4. *Triage and correct issues.*
5. *Document, document, document.*



Steps for respect review

1. *Find all the parts.*
2. *Check the invariants.*
3. ***Model the threats.***
4. *Triage and correct issues.*
5. *Document, document, document.*



Target-first

- Identify all groups affected: directly and indirectly.

Target-first

- Identify all groups affected: directly and indirectly.
- Consider the vulnerabilities of those groups.

Target-first

- Identify all groups affected: directly and indirectly.
- Consider the vulnerabilities of those groups.
- Warning: you will miss something.

Target-first

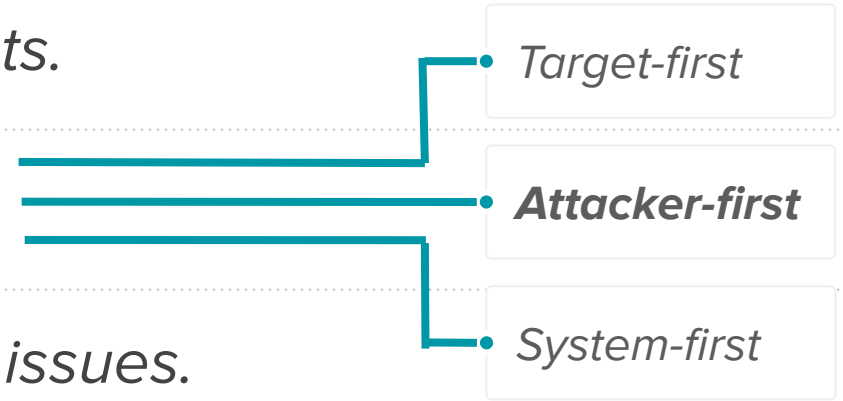
- Identify all groups affected: directly and indirectly.
- Consider the vulnerabilities of those groups.
- Warning: you will miss something.
  - Team diversity helps
  - User research helps

Example vulnerability factors

- Visible minority
- Invisible minority
- Gender
- Age
- Other identities
- Disability
- Poverty
- Abuse
- Target of generalized government action
- Target of specific government action
- Person with a secret

Steps for respect review

1. *Find all the parts.*
2. *Check the invariants.*
3. ***Model the threats.***
4. *Triage and correct issues.*
5. *Document, document, document.*



Example attacker factors

- Objective: commercial
- Objective: criminal
- Objective: political
- Objective: malicious
- Objective: chaos
- Personal vs. impersonal
- Primary vs. secondary

Example attacker factors

- Objective: commercial
- Objective: criminal
- Objective: political
- Objective: malicious
- Objective: chaos
- Personal vs. impersonal
- Primary vs. secondary

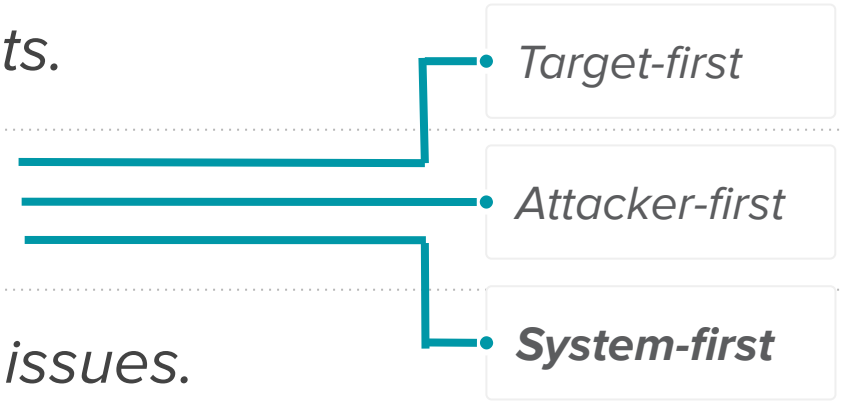
- Bonus features:
  - Advanced
  - Insider
  - Intimate
  - Power figure
  - Persistent

Example attackers

- Intimate persistent threats
- Advanced intimate persistent threats
- Untrusted roommate
- Employer
- Angry online attack mob
- Impersonal manipulator
- Suppressing political dissidence (targeted)
- Suppressing political dissidence (untargeted)

Steps for respect review

1. *Find all the parts.*
2. *Check the invariants.*
3. ***Model the threats.***
4. *Triage and correct issues.*
5. *Document, document, document.*

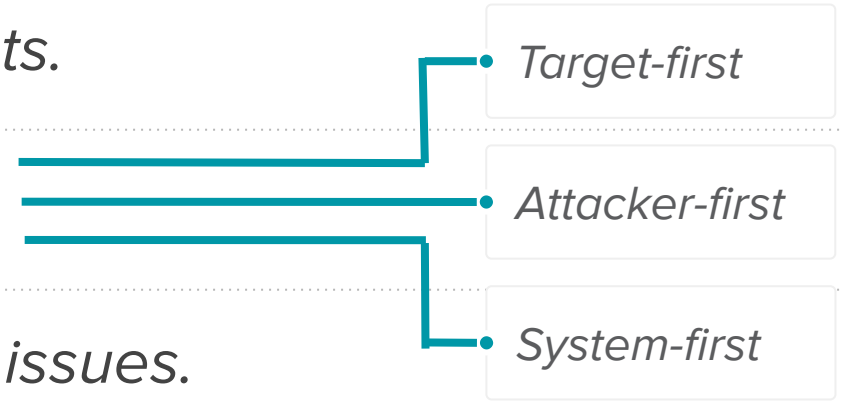


Example system areas

- Information sharing
- Authentication (and un-authentication)
- Authorization (system and models)
- Automated decision-making (correct and incorrect)
- Anti-abuse systems and their failures
- Where two systems meet
- System turndown

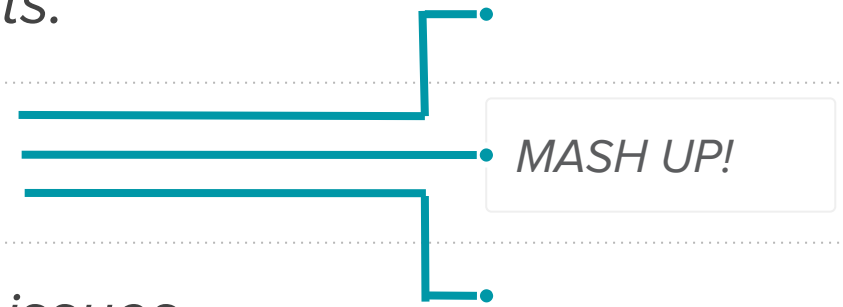
Steps for respect review

1. *Find all the parts.*
2. *Check the invariants.*
3. ***Model the threats.***
4. *Triage and correct issues.*
5. *Document, document, document.*



Steps for respect review

1. *Find all the parts.*
2. *Check the invariants.*
3. ***Model the threats.***
4. *Triage and correct issues.*
5. *Document, document, document.*



Mash up!

- Used as intended
- Used as intended (adjacent group)
- Used by someone well-meaning & misguided
- Used by attacker
- Used by (nearly) everyone
- Social & financial pressures
- Feelings

Steps for respect review

1. *Find all the parts.*
2. *Check the invariants.*
3. *Model the threats.*
4. ***Triage and correct issues.***
5. *Document, document, document.*

Triage and correct

Triage and correct

- Building consensus around respectful decisions.

Triage and correct

- **Building consensus around respectful decisions.**
- **Weigh the tradeoffs.**
  - Probability
  - Degree of impact
  - Ability to avoid bad outcomes

Triage and correct

- **Building consensus around respectful decisions.**
- **Weigh the tradeoffs.**
  - Probability
  - Degree of impact
  - Ability to avoid bad outcomes
- **Some problems don’t have correct answers.**
  - Privacy and security are not the only benefits in play
  - Different perspectives lead to non-parallel metrics
  - If we always choose to avoid risk, that choice is not free

Triage and correct

- **Building consensus around respectful decisions.**
- **Weigh the tradeoffs.**
  - Probability
  - Degree of impact
  - Ability to avoid bad outcomes
- **Some problems don’t have correct answers.**
  - Privacy and security are not the only benefits in play
  - Different perspectives lead to *non-parallel* metrics
  - If we always choose to avoid risk, that choice is not free
- **Goal: respectful, well-reasoned decisions in a reasonable amount of time.**

Steps for respect review

1. *Find all the parts.*
2. *Check the invariants.*
3. *Model the threats.*
4. *Triage and correct issues.*
5. ***Document, document, document.***

Now... you have a design

Now... you have a design

- Automated assurance
  - Make failures **logically** impossible
  - Make failures **practically** impossible
  - **Monitor** for failures (and fix them)

Now... you have a design

- Automated assurance
  - Make failures **logically** impossible
  - Make failures **practically** impossible
  - **Monitor** for failures (and fix them)

- Human assurance
  - **Audit** “load-bearing code”
  - **Decision support**: right information, right place, right time
  - **Process**: avoid forgetfulness and procrastination
  - **UX research**

Now... you have a design

- Automated assurance
  - Make failures **logically** impossible
  - Make failures **practically** impossible
  - **Monitor** for failures (and fix them)

- Human assurance
  - **Audit** “load-bearing code”
  - **Decision support**: right information, right place, right time
  - **Process**: avoid forgetfulness and procrastination
  - **UX research**

... now do it again for every change

Outline

1. *Why build for trust, build with respect*
2. *Framework*
3. ***Collaboration: technical***
4. *Collaboration: public policy/regulation*

Technical collaboration

Technical collaboration

- So many open questions.

Technical collaboration

- So many open questions.
- This framework as the start of a community resource.
- Please add to it; help those of us in industry who ask these questions every day.

Technical collaboration

- So many open questions.
- This framework as the start of a community resource.
- Please add to it; help those of us in industry who ask these questions every day.
- Would you like to join the curation committee? Let me know.

Outline

1. *Why build for trust, build with respect*
2. *Framework*
3. *Collaboration: technical*
4. ***Collaboration: public policy/regulation***

Public policy/regulation

Public policy/regulation

- Work with the practitioners to make costs clear.

Public policy/regulation

- Work with the practitioners to make costs clear.
- Don’t anticipate the research (too much).

Public policy/regulation

- Work with the practitioners to make costs clear.
- Don’t anticipate the research (too much).
- Regulate in concert with systemization.

Public policy/regulation

- Work with the practitioners to make costs clear.
- Don’t anticipate the research (too much).
- Regulate in concert with systemization.
- Account for human diversity.

Public policy/regulation

- Work with the practitioners to make costs clear.
- Don’t anticipate the research (too much).
- Regulate in concert with systemization.
- Account for human diversity.
- Let the profession learn.

Public policy/regulation

- Work with the practitioners to make costs clear.
- Don’t anticipate the research (too much).
- Regulate in concert with systemization.
- Account for human diversity.
- Let the profession learn.

humu

Building for Trust:

Because we don't all have to learn lessons the hard way

Lea Kissner
Chief Privacy Officer, Humu

@LeaKissner
leak@humu.com