CSci 4271W
Development of Secure Software Systems
Day 25: Human factors part 3: warnings and configuration; responsible disclosure

Stephen McCamant (he/him)
University of Minnesota, Computer Science & Engineering

Based in large part on slides originally by Prof. Nick Hopper
Licensed under Creative Commons Attribution-ShareAlike 4.0

Human factors

Ultimately, most computing systems will involve people at some point. How do we design security mechanisms that take the needs, abilities and goals of people into account?



Photo credits via freepik.com: rawpixel.com, wayhomestudio, rawpixel.com

What are we building?

Three primary kinds of interactions occur in user interactions for security:

- Authentications prove that a person can access a computer, application, or resource
- Warnings inform a person that an action will or could have security consequences
- Configurations allow a person to make decisions about the security policy of a system

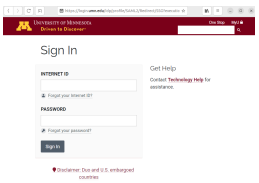
Challenges with users

Challenges with users

Conditioning: people learn to respond to frequent stimuli

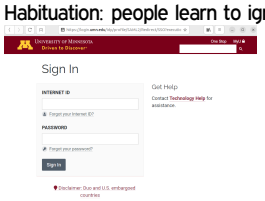
Challenges with users

Conditioning: people learn to respond to frequent stimuli



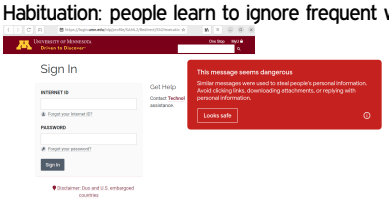
Challenges with users

Conditioning: people learn to respond to frequent stimuli
Habituation: people learn to ignore frequent warnings



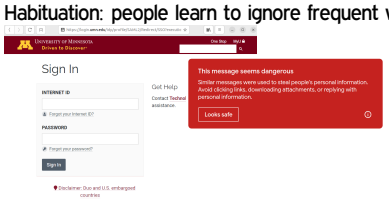
Challenges with users

Conditioning: people learn to respond to frequent stimuli
Habituation: people learn to ignore frequent warnings



Challenges with users

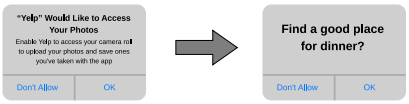
Conditioning: people learn to respond to frequent stimuli
Habituation: people learn to ignore frequent warnings



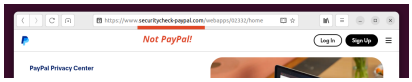
Wicked environment: no way to tell when a decision was bad

User behavior

Goal Orientation: when people are using computers, they are trying to achieve a task.



Confirmation Bias: people look for information that confirms their expectations.



Good decisions: design patterns

- Minimize what you ask of people
- Force people to complete important steps
- Avoid urgency
- Easy path to safety
- No "scamicry"

Outline

Review: what we're building

More detailed suggestions

Announcements intermission

Responsible disclosure

Warnings: NEAT

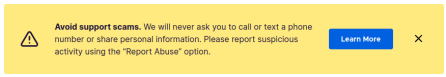
When designing a warning interaction, make sure it is NEAT (Reeder):

- N ecessary — can it be eliminated or deferred?
- E xplained — does it present all info the user needs?
- A ctionable — can the user make a correct decision?
- T ested — effective in benign and malicious settings?

Warnings/explanations: SPRUCE

We can evaluate the warning or explanation using SPRUCE:

- S ource
- P rocess
- R isk
- U nique user knowledge
- C hoices
- E vidence



Configuration design

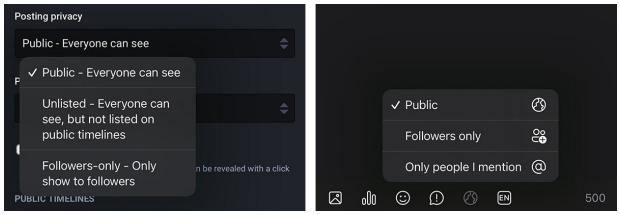
Questions to consider:

Configuration design

Questions to consider:

- Who can perform the configuration? (anyone, admin, parent?)
- What can they configure (and how granular)?
- Why would anyone want to do it? (how can we help them accomplish their goals?)
- When will the configuration happen? (Proactive/reactive? Just in time?)
- Where will users make the change? (How do they find the interface?)
- How will users implement/test their intent?

Configuration example



Who, what, when, where, why and how?

Configuration metrics

Metrics for configuration interactions:

- Discoverability (can people find the interface?)
- Accuracy (can people complete a given task?)
- Time to completion (can they do it quickly, before giving up?)
- Side effects (can they do it without messing other things up?)
- Satisfaction (easy to do, or frustrating?)

Usability testing principles

Cognitive Walkthroughs — Developers should use the security interaction, narrating (and recording) the task.
Benign and Malicious Testing — Test every feature both when there is a security risk and when there is not.
Ecological Validity — Will users respond the same way in testing as "in the wild?" (this can go both ways: "it's only a study" or "it's a security study, I will be more careful")

Outline

Review: what we're building

More detailed suggestions

Announcements intermission

Responsible disclosure

Upcoming activities

- Homework 6 is due tonight by 11:59pm
- Project part 3 coming up
  - One section draft due this Thursday
  - Final report due Monday 5/5, no extensions
- Final exam Saturday 5/10 4–6pm

SRTs and completion incentive

- Student Ratings of Teaching are important feedback for me and the department
- Available now and through Monday May 5th
  - `srt.umn.edu/blue` or via Canvas
- Collective completion incentive if at least 6 (resp. 7) students complete evaluations
  - Equivalent to 1 (resp. 2) points on the final exam
- Will have reminder and time to complete on Thursday

Outline

Review: what we're building

More detailed suggestions

Announcements intermission

Responsible disclosure

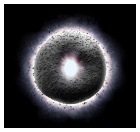
Vulnerability disclosure

So you've found (and confirmed) a vulnerability. Do you…

Vulnerability disclosure

So you've found (and confirmed) a vulnerability. Do you…

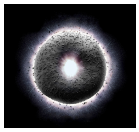
Tell everyone, everywhere all at once?



Vulnerability disclosure

So you've found (and confirmed) a vulnerability. Do you…

Tell everyone, everywhere all at once?



Never speak of this again.

Image sources: Everything Everywhere All at Once soundtrack "This Is A Life" single cover art; The Simpsons S06E04

Responsible disclosure

Is a process that looks for a middle ground, balancing interests among the parties:

- Finder
- Reporter
- Vendor/developer
- Downstream vendors/maintainers
- Users/customers
- The public

Disclosure process principles

- Reduce harm
  - Publish information
  - Reduce days of risk
  - Ensure high patch quality
- Presume benevolence
- Avoid surprise
- Incentivize desired behavior
- Process improvement

Ethics (CS perspective)

From the ACM Code of Ethics:

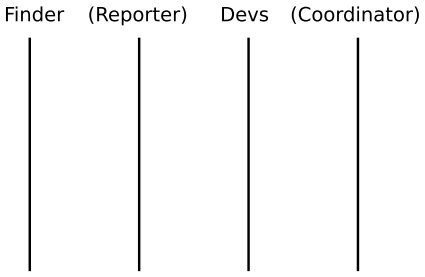
- Contribute to society and human well-being.
- Avoid harm to others.
- Be honest and trustworthy.
- Be fair and take action not to discriminate.
- Honor property rights including copyrights and patent.
- Give proper credit for intellectual property.
- Respect the privacy of others.
- Honor confidentiality.

Ethics (another perspective)

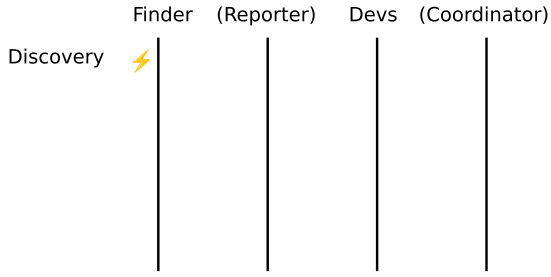
Society of Professional Journalists:

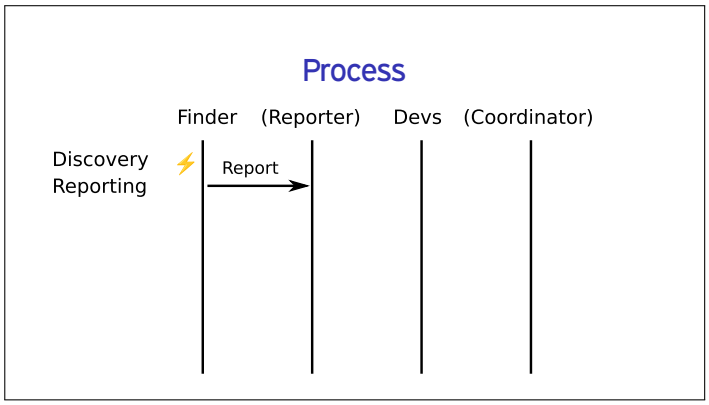
- Seek truth and report it — be accurate and fair
- Minimize harm — treat sources, subjects, colleagues and members of the public as human beings deserving of respect
- Act independently — highest and primary obligation is to serve the public
- Be accountable and transparent

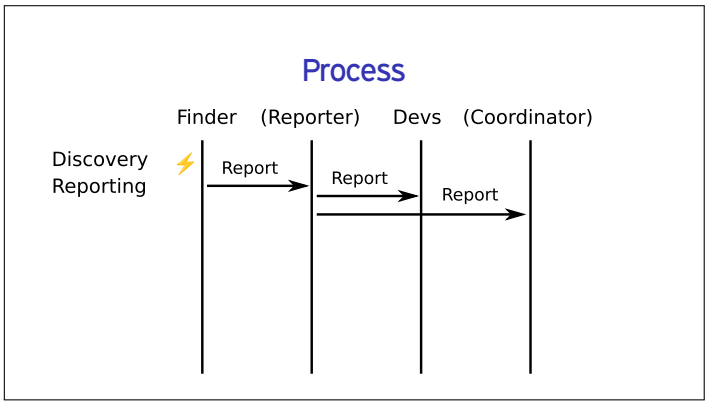
Process

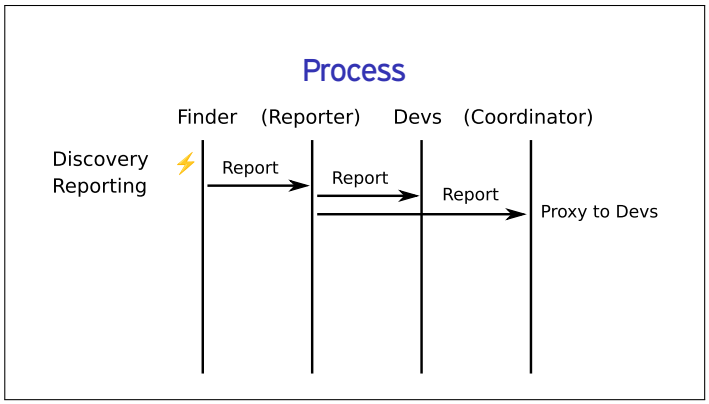


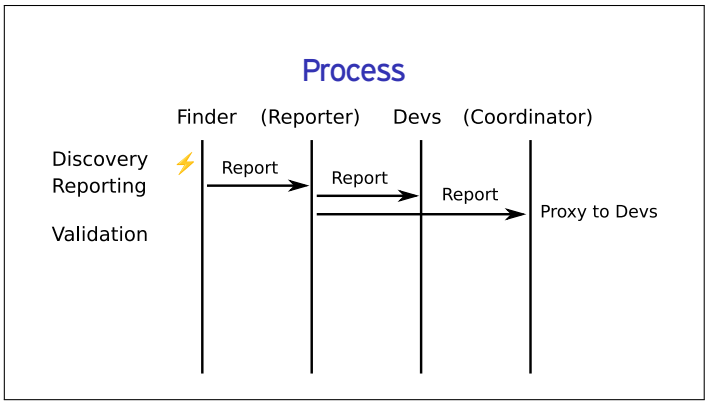
Process

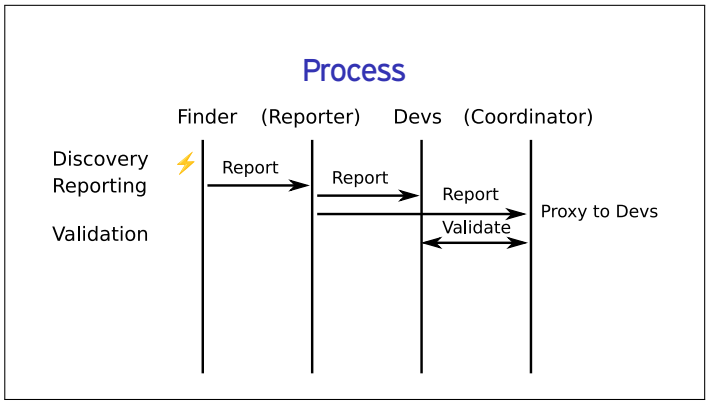


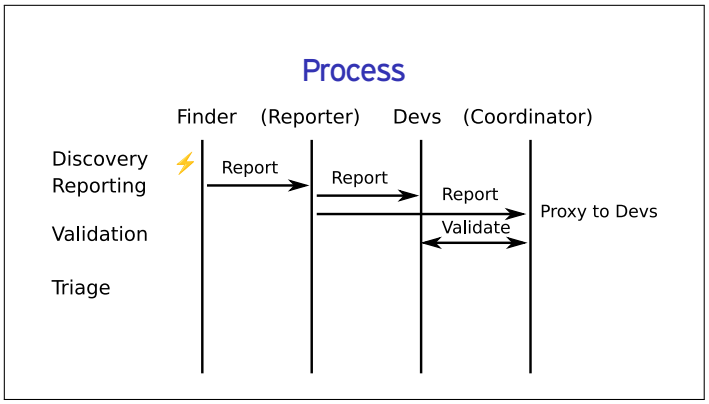

Process
Finder
(Reporter)
Devs
(Coordinator)
Discovery
Reporting
Report

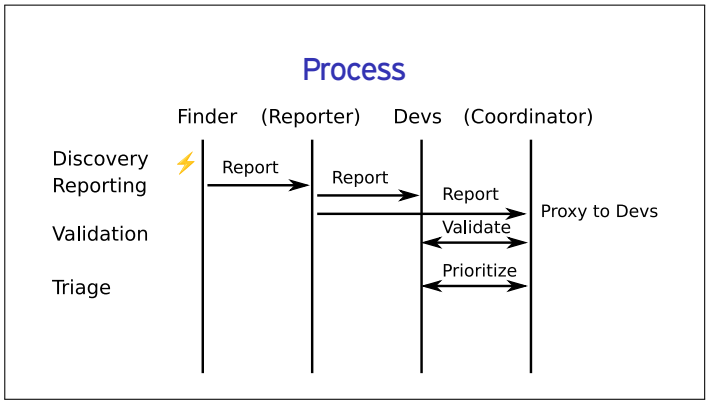

Process
Finder
(Reporter)
Devs
(Coordinator)
Discovery
Reporting
Report
Report
Report

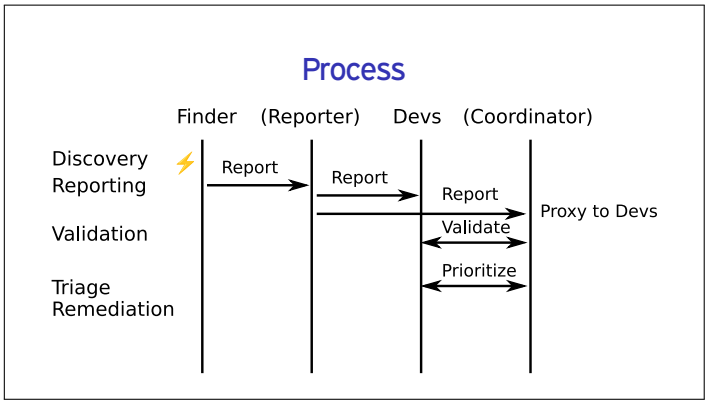

Process
Finder
(Reporter)
Devs
(Coordinator)
Discovery
Reporting
Report
Report
Report
Proxy to Devs


Process
Finder
(Reporter)
Devs
(Coordinator)
Discovery
Reporting
Validation
Report
Report
Report
Proxy to Devs

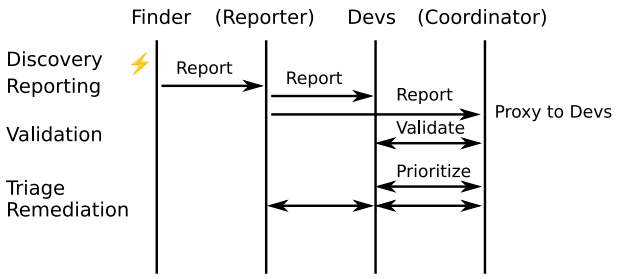

Process
Finder
(Reporter)
Devs
(Coordinator)
Discovery
Reporting
Validation
Report
Report
Report
Validate
Proxy to Devs


Process
Finder
(Reporter)
Devs
(Coordinator)
Discovery
Reporting
Validation
Triage
Report
Report
Report
Validate
Proxy to Devs

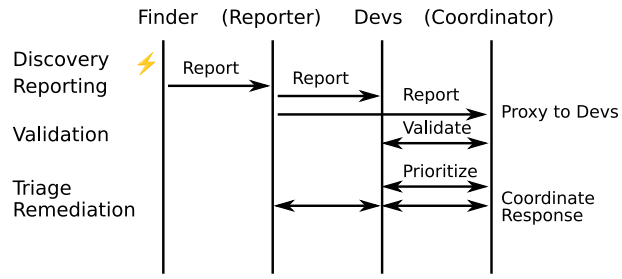

Process
Finder
(Reporter)
Devs
(Coordinator)
Discovery
Reporting
Validation
Triage
Report
Report
Report
Validate
Prioritize
Proxy to Devs


Process
Finder
(Reporter)
Devs
(Coordinator)
Discovery
Reporting
Validation
Triage
Remediation
Report
Report
Report
Validate
Prioritize
Proxy to Devs

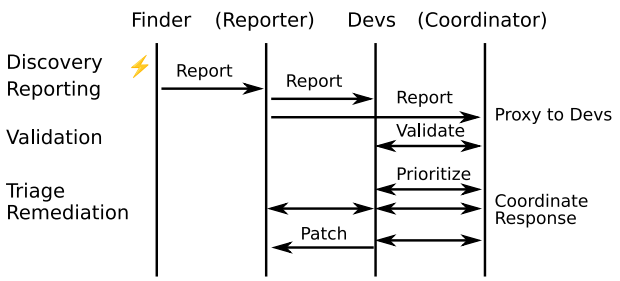
Process



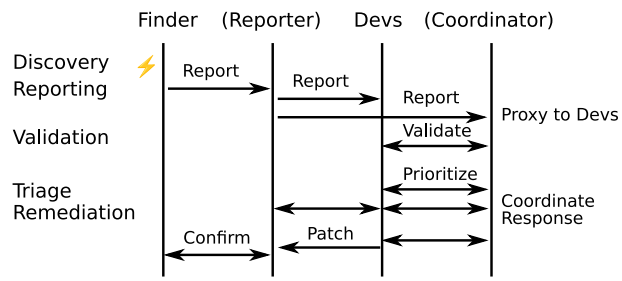
Process



Process



Process



Process