CSci 4271W
Development of Secure Software Systems
Day 23: Human factors part 1: functionality and attacks

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

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? (1)

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

What are we building? (1)

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

- Authentications prove that a person can access a computer, application, or resource

What are we building? (1)

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

What are we building? (1)

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

What are we building? (2)

Configurations can include:

- Configuration of software settings
- Consenting to terms
- Authorization of permission settings
- Verification of settings or claims
- Auditing the state of the system

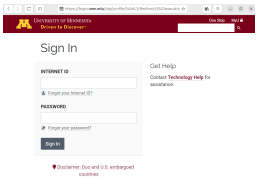
Challenges with users

Challenges with users

Conditioning: people learn to respond to frequent stimuli

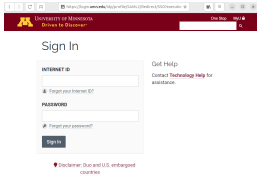
Challenges with users

Conditioning: people learn to respond to frequent stimuli



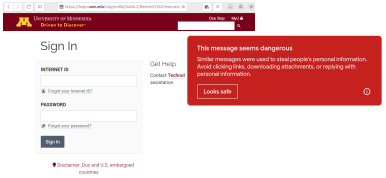
Challenges with users

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



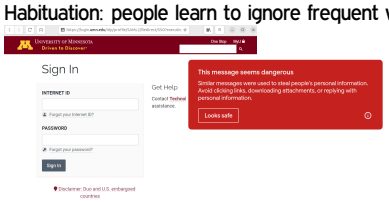
Challenges with users

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

Interacting with users

Kahneman notes four important ways people deviate from "rationality":

Interacting with users

Kahneman notes four important ways people deviate from "rationality":

- What You See Is All There Is (WYSIATI): excluded context is forgotten. (Why you see an "unlock" icon on a non-TLS site)

Interacting with users

Kahneman notes four important ways people deviate from "rationality":

- What You See Is All There Is (WYSIATI): excluded context is forgotten. (Why you see an "unlock" icon on a non-TLS site)
- System 1 vs System 2: practiced skills don't engage "rational" thought.

Interacting with users

Kahneman notes four important ways people deviate from "rationality":

- What You See Is All There Is (WYSIATI): excluded context is forgotten. (Why you see an "unlock" icon on a non-TLS site)
- System 1 vs System 2: practiced skills don't engage "rational" thought.
- Anchoring: comparing numbers across contexts.

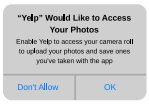
Interacting with users

Kahneman notes four important ways people deviate from "rationality":

- What You See Is All There Is (WYSIATI): excluded context is forgotten. (Why you see an "unlock" icon on a non-TLS site)
- System 1 vs System 2: practiced skills don't engage "rational" thought.
- Anchoring: comparing numbers across contexts.
- Satisficing: people make "good enough" decisions when a "good" decision is hard to make.

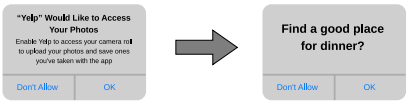
User behavior

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



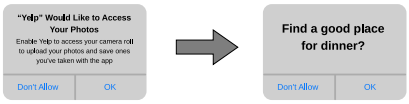
User behavior

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



User behavior

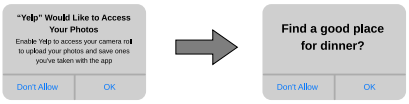
Goal Orientation: when people are using computers, they are trying to achieve a task.



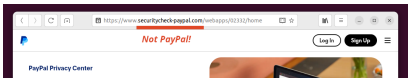
Confirmation Bias: people look for information that confirms their expectations.

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.



Outline

What are we building?

Announcements intermission

What can go wrong?

Upcoming activities

- Homework 6 was posted yesterday, due in a week on 4/29
- Expect project part 3 to be posted tonight
  - One section draft due Thursday 5/1
  - Final report due Monday 5/5, no extensions
- Final exam Saturday 5/10

Outline

What are we building?

Announcements intermission

What can go wrong?

What can go wrong (1)

Channel of contact	Thing spoofed	Persuasion to interact	Human act exploited	Technical spoofing
Email	UI element	Greed	Open doc	System dialog
Website	Product or service	Fear	Click link	Filename
Social Network	Person you know	Social relationship	Attach device	File type
IM	Organization	Business relationship	Run program	Icon
Physical	Person you don't know	Curiosity	Enter credentials	Filename (multilingual)
	An authority	Lust	Establish relationship	

What can go wrong (2)

Online fraud

What can go wrong (2)

Online fraud

- Browser extensions that replace ads, mine cryptocurrency, hijack passwords.

What can go wrong (2)

Online fraud

- Browser extensions that replace ads, mine cryptocurrency, hijack passwords.
- Fake Antivirus software informs users they have malware, then does nothing (or installs malware/spyware)

What can go wrong (2)

Online fraud

- Browser extensions that replace ads, mine cryptocurrency, hijack passwords.
- Fake Antivirus software informs users they have malware, then does nothing (or installs malware/spyware)
- Fraudulent retailers using SEO or "privacy certificates" to convince users they're safe

What can go wrong (3)

Social engineering

What can go wrong (3)

Social engineering

- Pretexting: asking for information while pretending to have a legitimate reason to need it.

What can go wrong (3)

Social engineering

- Pretexting: asking for information while pretending to have a legitimate reason to need it.
- Distraction: convince employees that something is true because they are distracted/busy.

What can go wrong (3)

Social engineering

- Pretexting: asking for information while pretending to have a legitimate reason to need it.
- Distraction: convince employees that something is true because they are distracted/busy.
- Sock Puppets: spread information through multiple sources to make it appear legitimate

What can go wrong (4)

- Phishing: Using spoofed emails to steal user credentials or install malware (to steal credentials, send spam, click on ads...)
- Spear-Phishing: Targeting specific individuals, by spoofing known contacts (collected from other campaigns, social networks, etc...)
- Extortion: (I know what you did on the web last night...)

What can go wrong (5)

Operational security (opsec) failures

What can go wrong (5)

Operational security (opsec) failures

- Tailgating: ask someone with a badge to hold the door.

What can go wrong (5)

Operational security (opsec) failures

- Tailgating: ask someone with a badge to hold the door.
- Dumpster diving: finding confidential materials in the trash.

What can go wrong (5)

Operational security (opsec) failures

- Tailgating: ask someone with a badge to hold the door.
- Dumpster diving: finding confidential materials in the trash.
- USB drop: leave a USB stick in the parking lot.

Frauds and Phishers

Stajano-Wilson model:
Distraction Principle: Distracted people won't notice missing details.
Social Compliance Principle: Society trains people to not question authority.
Herd Principle: People let their guard down if many others share the risk.

Stajano-Wilson, cont'd

Dishonesty Principle: Our own inner larceny is what hooks us initially.
Kindness Principle: People are fundamentally nice and willing to help.
Need and Greed Principle: Once hustlers know what someone wants, they can easily manipulate them.
Time Principle: Time pressure causes people to make "easier" decisions.