Introduction to Usable Security
Reasoning About the Human in the Loop

Lorrie Faith Cranor

September 2011

Carnegie Mellon

CyLab Usable Privacy and Security Laboratory
http://cups.cs.cmu.edu/

Outline

- Why should we make secure systems more usable?
- How can we make secure systems more usable
- The human in the loop

Why should we make secure systems more usable?

Unusable security & privacy

- Unpatched Windows machines compromised in minutes
- Phishing web sites costing $billions
- Most PCs infected with spyware
- Users have more passwords than they can remember and practice poor password security
- Enterprises store confidential information on laptops and mobile devices that are frequently lost or stolen

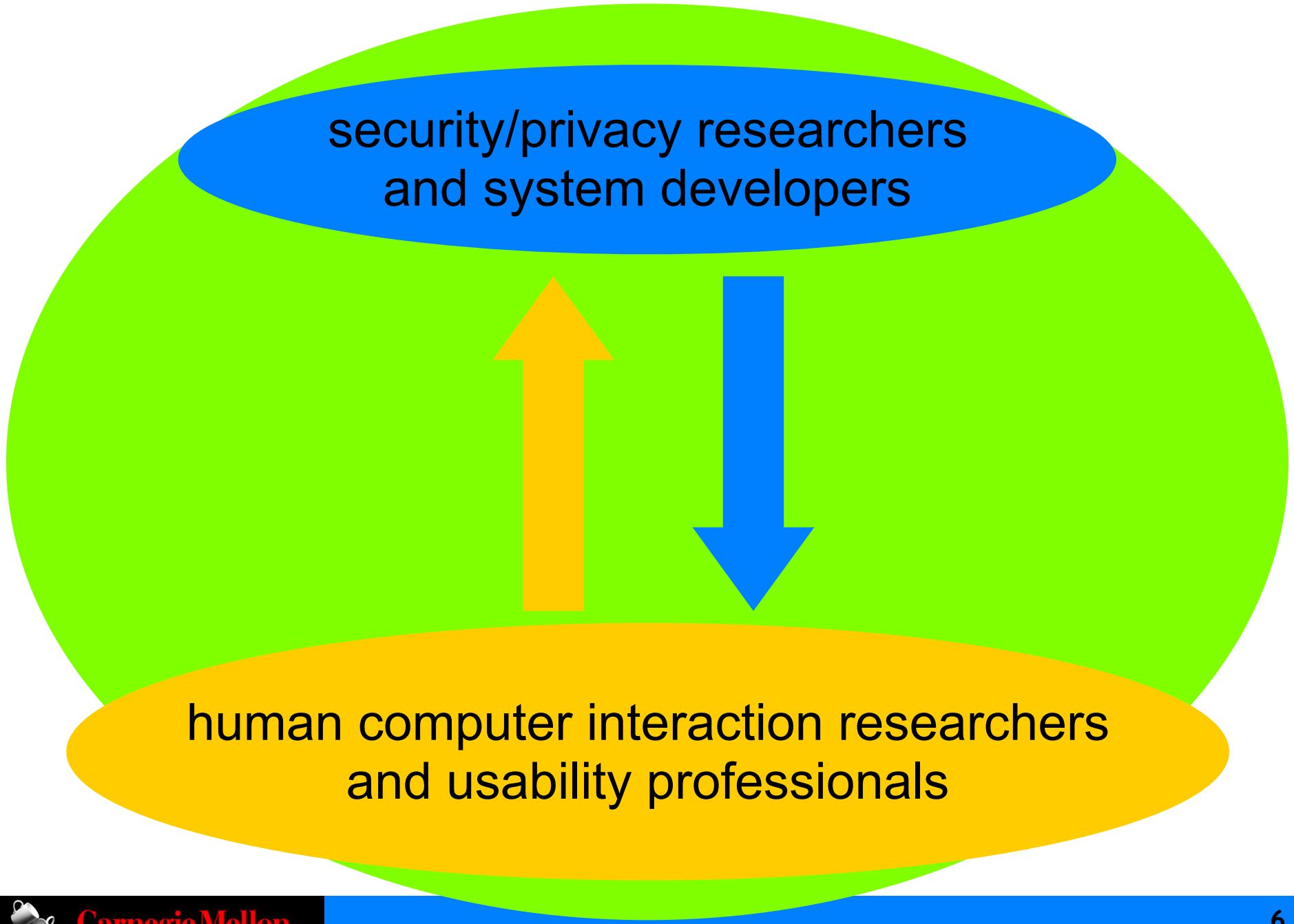
Grand Challenge

"Give end-users security controls they can understand and privacy they can control for the dynamic, pervasive computing environments of the future."

- Computing Research Association 2003

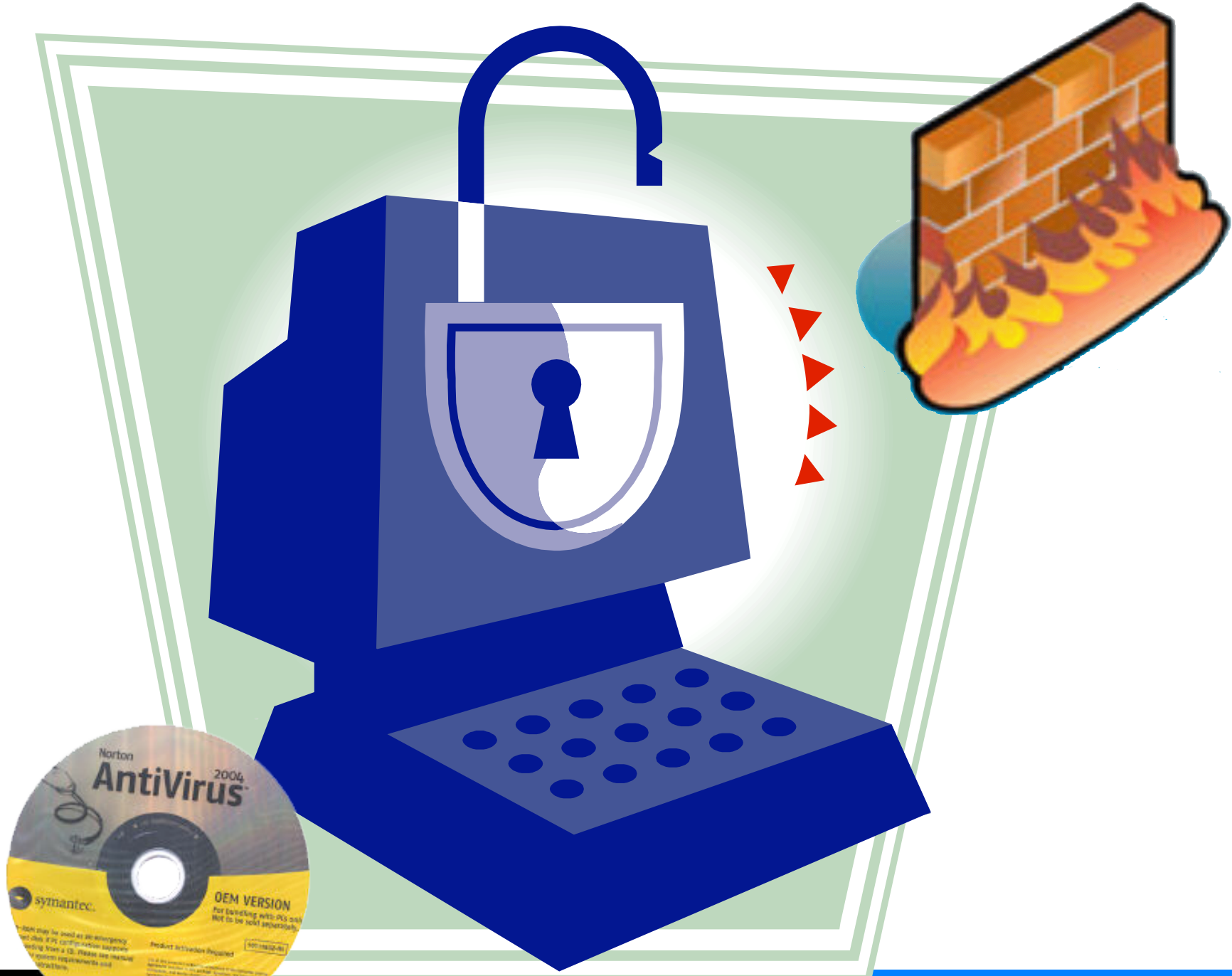
security/privacy researchers
and system developers

human computer interaction researchers
and usability professionals

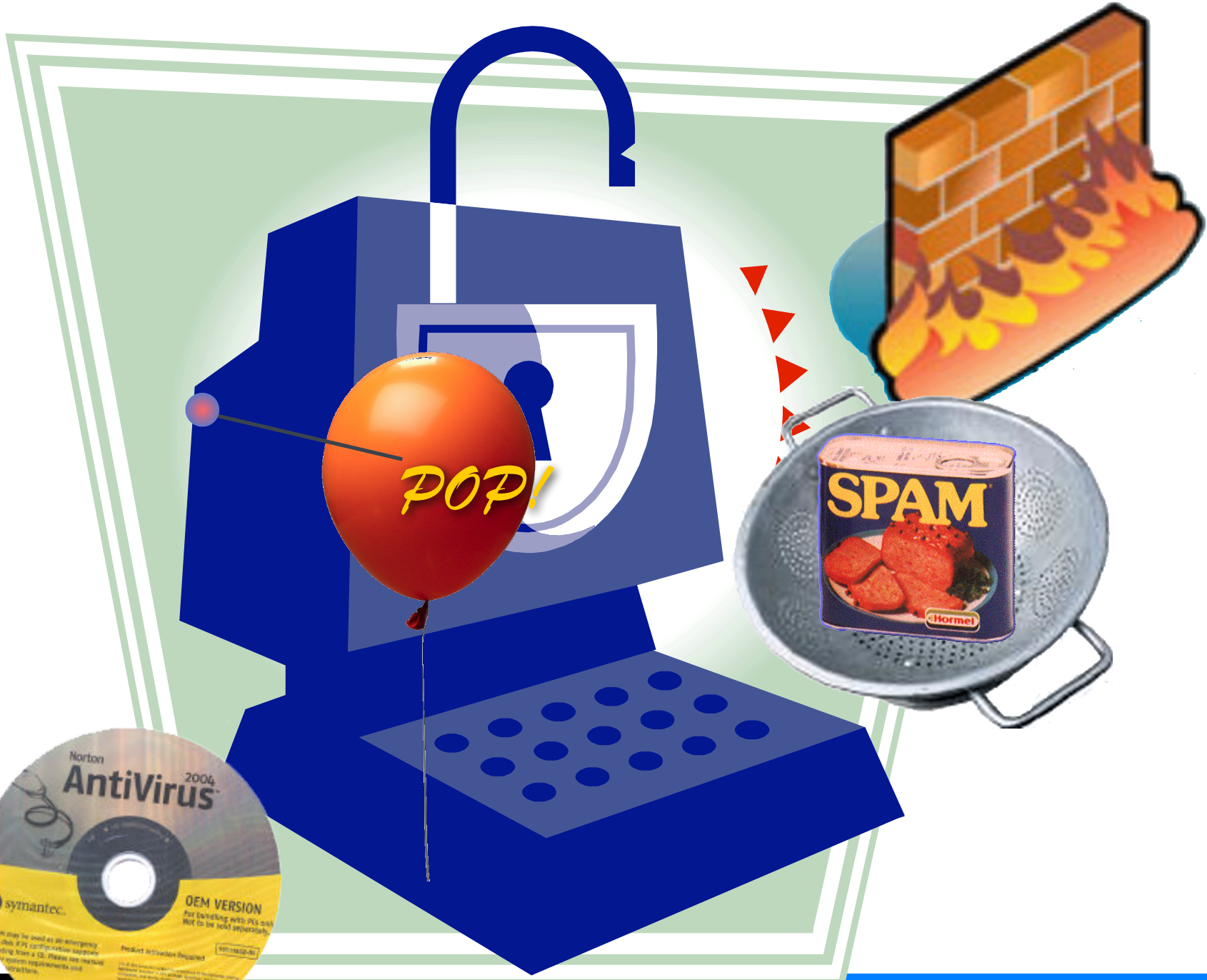

security/privacy researchers
and system developers
human computer interaction researchers
and usability professionals

The user experience

How do users stay safe online?


Norton
AntiVirus
2004
symantec.
OEM VERSION


Norton
AntiVirus
2004
symantec.
OEM VERSION
SPAM
Hormel


POP!
SPAM
Hormel
Norton
AntiVirus
2004
symantec.
OEM VERSION


COOKIES
POP!
SPAM
Hormel
Norton
AntiVirus
2004
symantec.
OEM VERSION

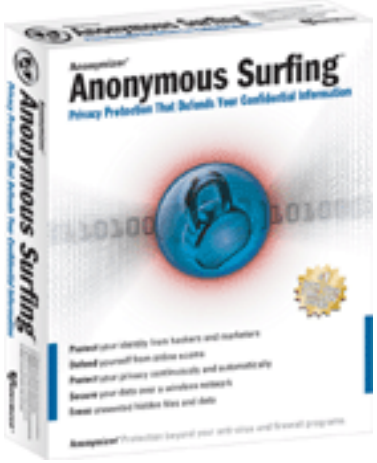

PAL Spyware
Spy Sweeper
webroot
Spy Sweeper
2004
Spyware
Eliminator
COOKIES
POP!
SPAM
Hormel
Norton
AntiVirus
2004
symantec.
OEM VERSION

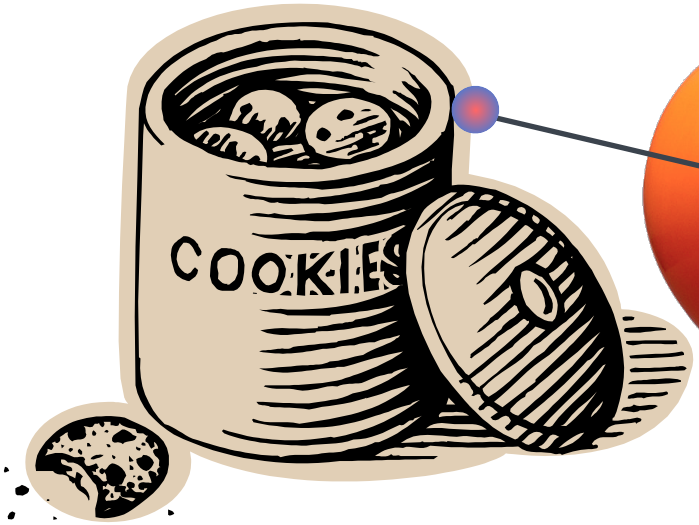

2004
Spyware
Eliminator
Spy Sweeper
COOKIES
POP!
SPAM
Hormel
Norton
AntiVirus
2004
symantec.
OEM VERSION
Encryption for Everyone
PGP
Pretty Good Privacy
HARDENED
PGP
Simson Garfinkel
O'Reilly & Associates, Inc.


2004
Spyware
Eliminator
Spy Sweeper
COOKIES
POP!
SPAM
Hormel
Norton
AntiVirus
2004
symantec.
OEM VERSION
Net Nanny
Encryption for Everyone
PGP
Pretty Good Privacy
HARDENED
PGP
Simson Garfinkel
O'Reilly & Associates, Inc.


PAL Spyware
webroot
Spy Sweeper
2004
Spyware
Eliminator
Anonymous Surfing
Privacy Protection That Unleash Your Confidential Information
COOKIES
POP!
SPAM
Hormel
Norton
AntiVirus
2004
symantec.
OEM VERSION
Net Nanny
3
Encryption for Everyone
PGP
Pretty Good Privacy
HARDENED
PGP
Simson Garfinkel
O'Reilly & Associates, Inc.

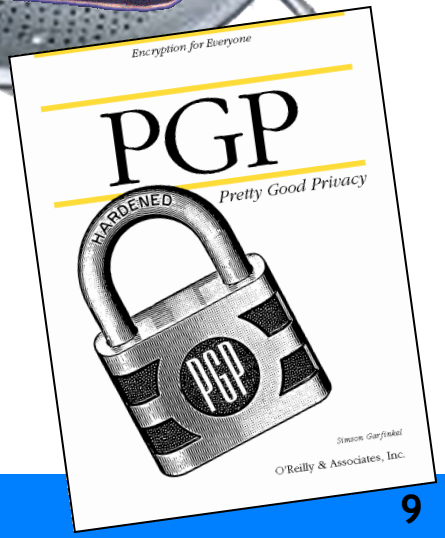

2004
Spyware
Eliminator
Spy Sweeper


Anonymous Surfing

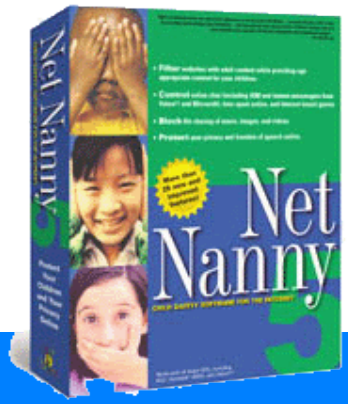

COOKIES


POP!


SPAM
Hormel


Encryption for Everyone
PGP
Pretty Good Privacy
HARDENED
PGP
Simson Garfinkel
O'Reilly & Associates, Inc.


Norton
AntiVirus
2004
symantec.
OEM VERSION


Net Nanny
Net Nanny

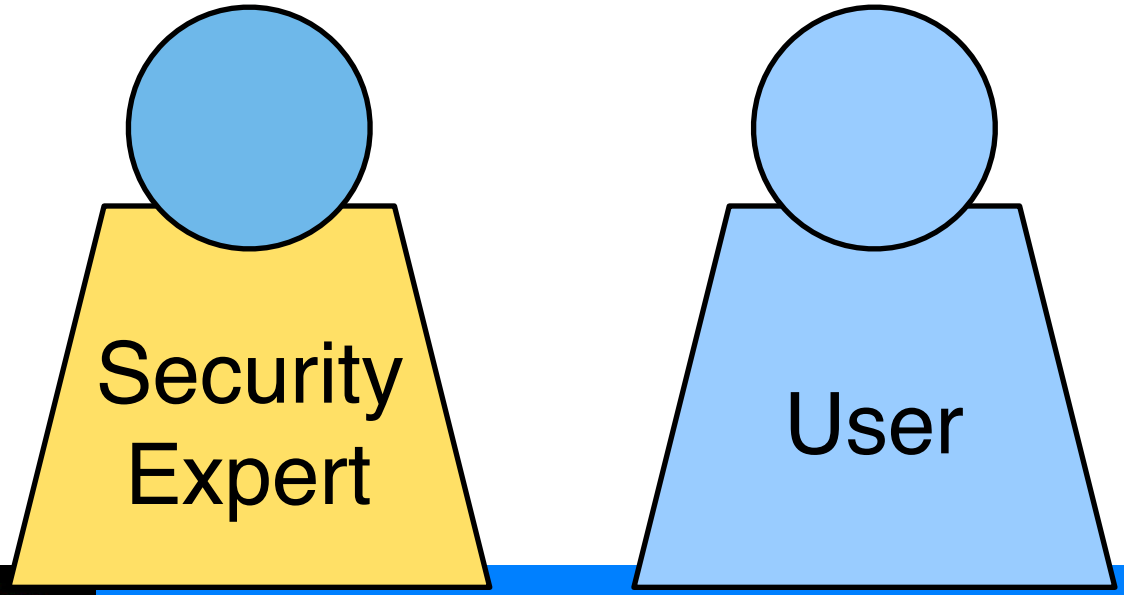
After installing all that security and privacy software do you have any time left to get any work done?

Security is a secondary task

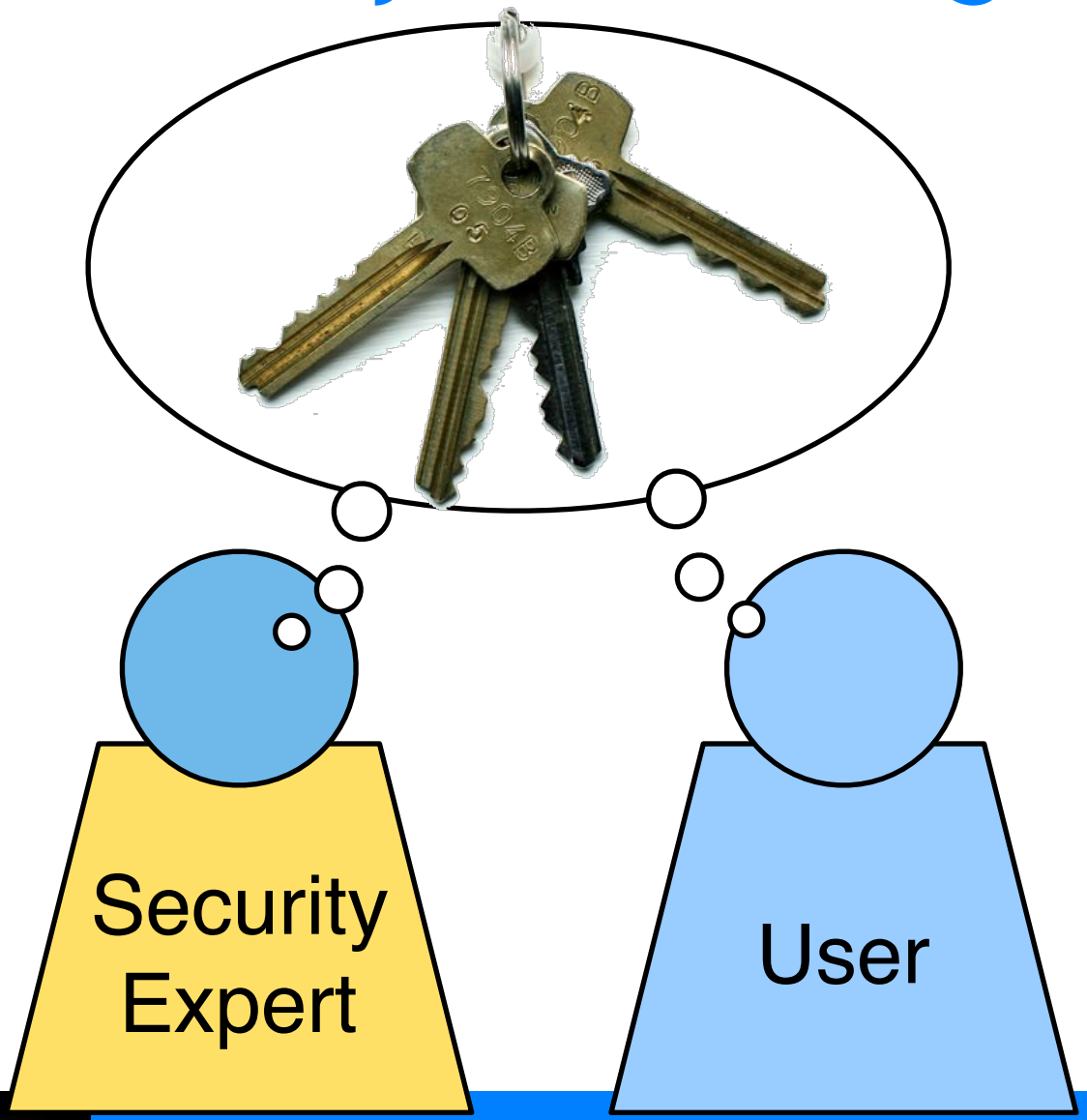
"Users do not want to be responsible for, nor concern themselves with, their own security."

- Blake Ross 

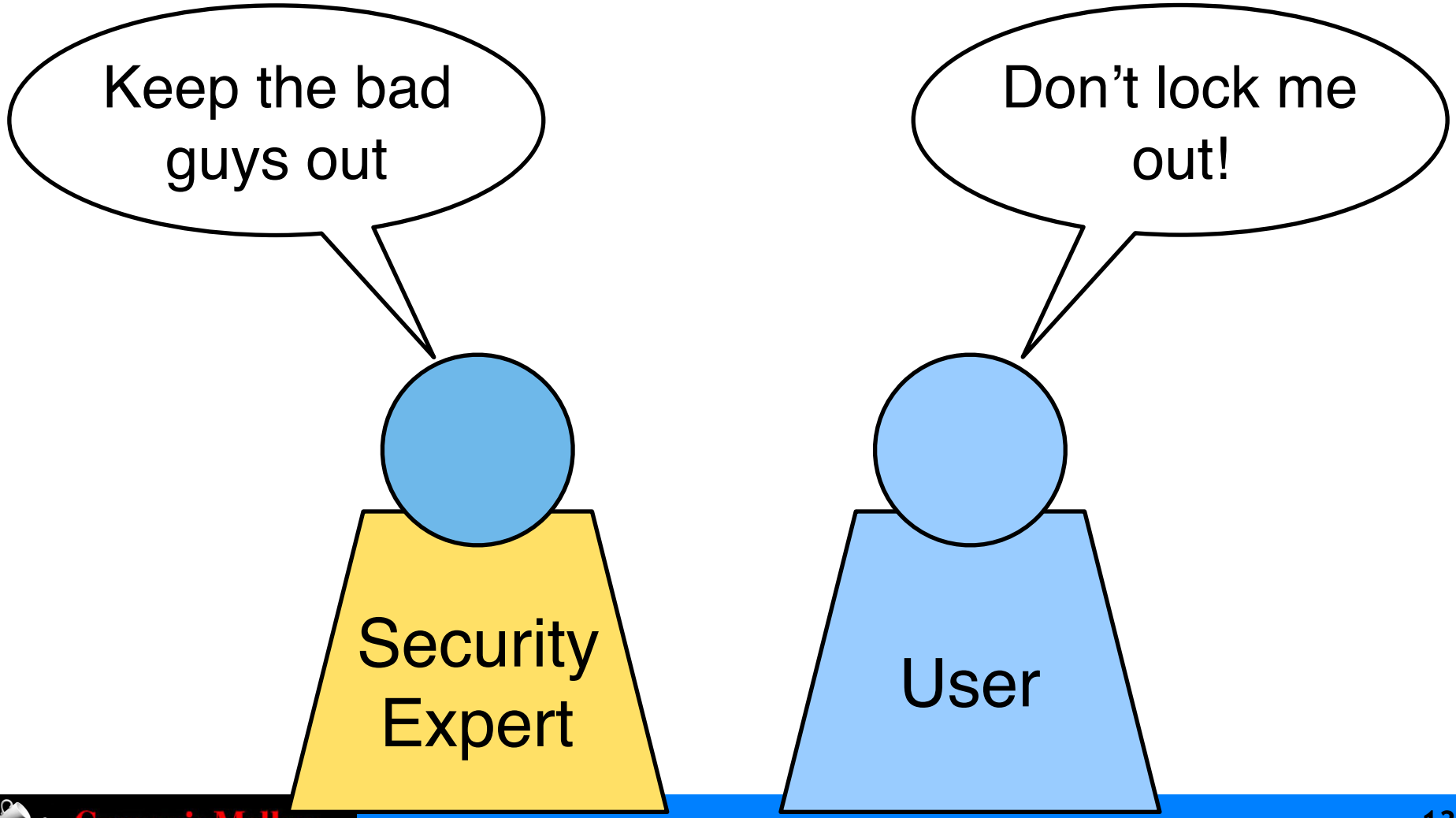
Concerns may not be aligned



Concerns may not be aligned



Concerns may not be aligned



Grey

- Smartphone based access-control system
- Used to open doors in the Carnegie Mellon CIC building
- Allows users to grant access to their doors remotely

L. Bauer, L.F. Cranor, R.W. Reeder, M.K. Reiter, and K. Vaniea. **A User Study of Policy Creation in a Flexible Access-Control System.** CHI 2008. http://www.robreeder.com/pubs/greyCHI2008.pdf

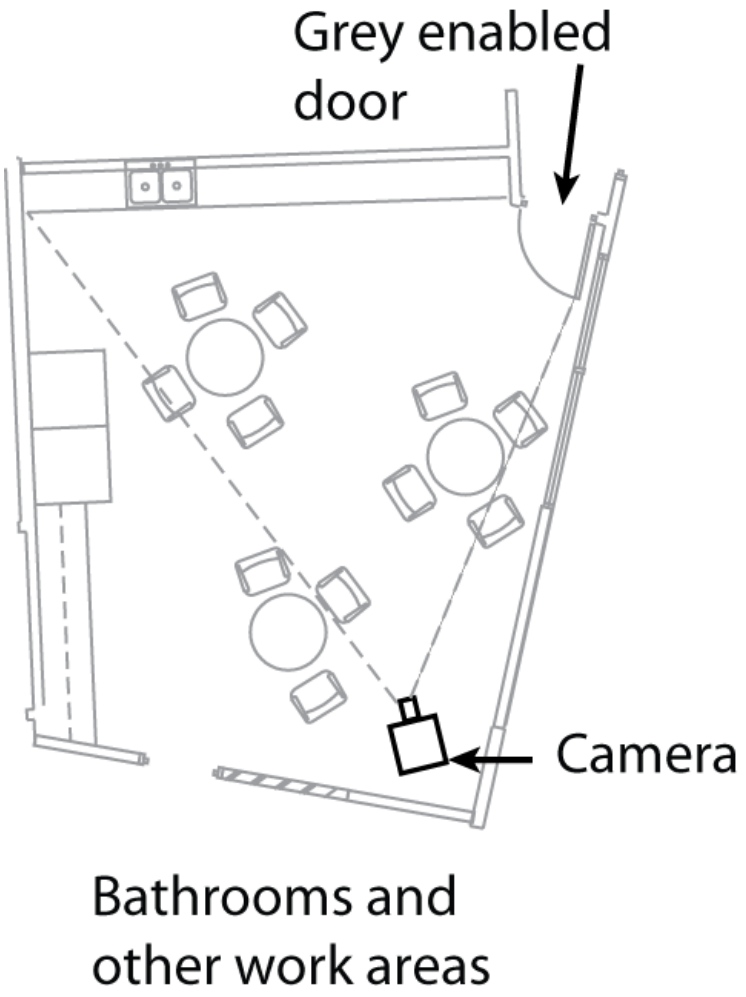
L. Bauer, L. F. Cranor, M. K. Reiter, and K. Vaniea. **Lessons Learned from the Deployment of a Smartphone-Based Access-Control System.** SOUPS 2007. http://cups.cs.cmu.edu/soups/2007/proceedings/p64_bauer.pdf

Data collection

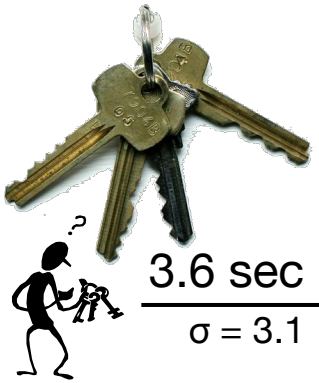
- Year long interview study
- Recorded 30 hours of interviews with Grey users
- System was actively used: 29 users x 12 access per week

Users complained about speed

- Users said Grey was slow
- But Grey was as fast as keys
- Videotaped a door to better understand how doors are opened differently with Grey and keys



Average access times



Getting keys

3.6 sec
σ = 3.1

Stop in front of door

5.4 sec
σ = 3.1

Door opened

5.7 sec
σ = 3.6

Door Closed

Total 14.7 sec

σ = 5.6

Average access times

3.6 sec
σ = 3.1

5.4 sec
σ = 3.1

5.7 sec
σ = 3.6

Getting keys

Stop in front of door

Door opened

Door Closed

Total 14.7 sec

σ = 5.6

8.4 sec
σ = 2.8

2.9 sec
σ = 1.5

3.8 sec
σ = 1.1

Getting phone

Stop in front of door

Door opened

Door Closed

Total 15.1 sec

σ = 3.9

Average access times

3.6 sec
σ = 3.1

5.4 sec
σ = 3.1

5.7 sec
σ = 3.6

Getting keys

Stop in front of door

Door opened

Door Closed

Total 14.7 sec

σ = 5.6

8.4 sec
σ = 2.8

2.9 sec
σ = 1.5

3.8 sec
σ = 1.1

Getting phone

Stop in front of door

Door opened

Door Closed

Total 15.1 sec

σ = 3.9

“I find myself standing outside and everybody inside is looking at me standing outside while I am trying to futz with my phone and open the stupid door.”

Nobody wants to have to reboot their door

Unanticipated uses can bolster acceptance


Convenience
always wins

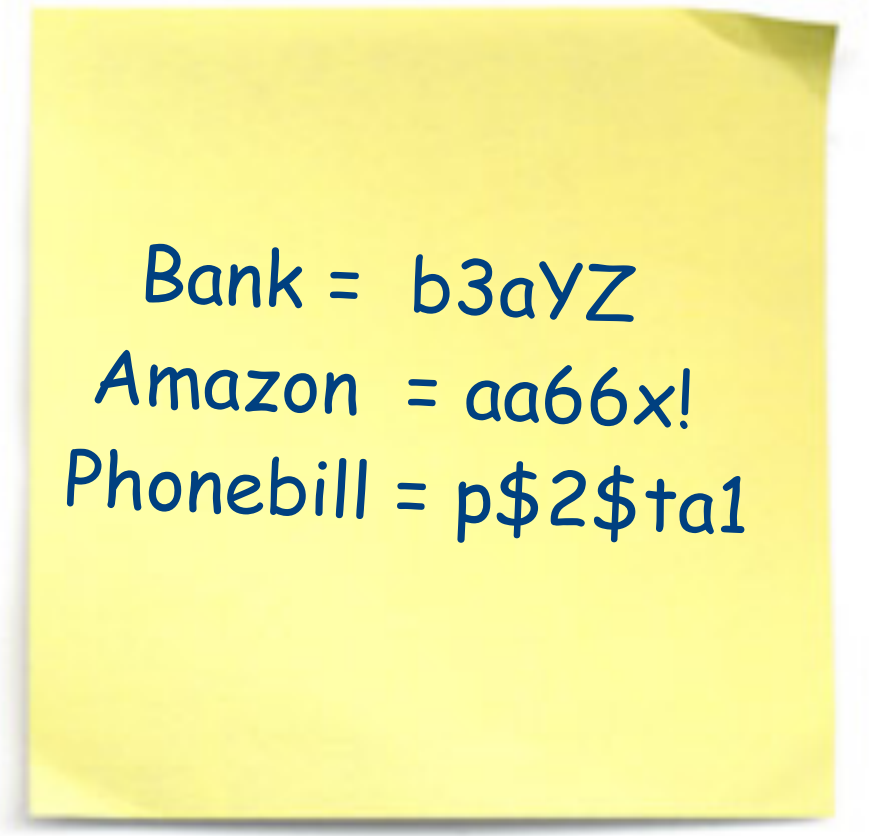
Secure, but usable?

Unusable security frustrates users

Typical password advice

- Pick a hard to guess password
- Don’t use it anywhere else
- Change it often
- Don’t write it down

What do users do when every web site wants a password?


Bank = b3aYZ
Amazon = aa66x!
Phonebill = p2ta1

How can we make secure systems more usable?

How can we make secure systems more usable?

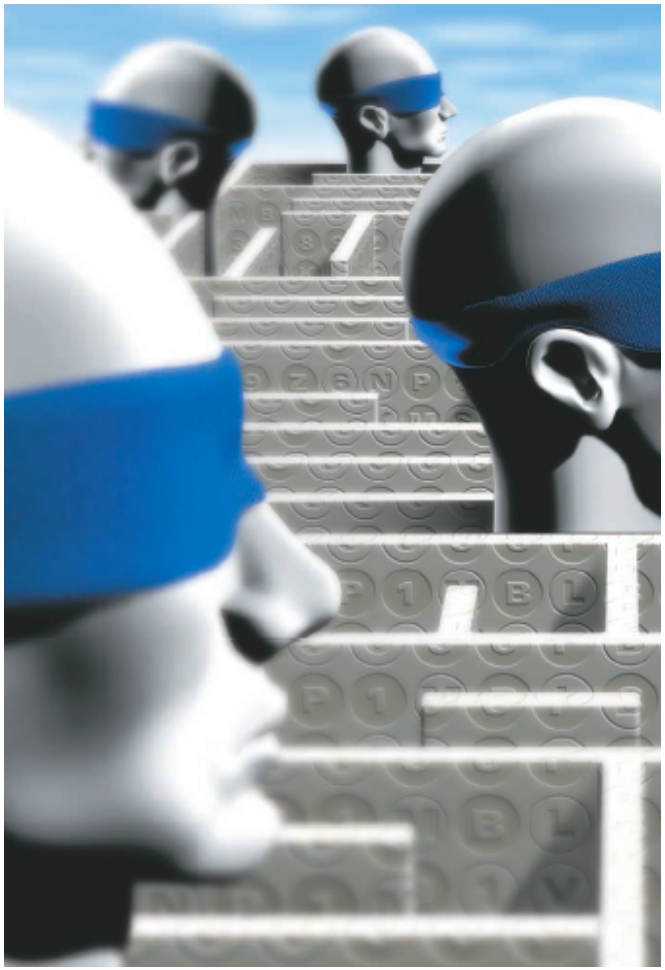
- Make it “just work”
  - Invisible security
- Make security/privacy understandable
  - Make it visible
  - Make it intuitive
  - Use metaphors that users can relate to
- Train the user

Make it “just work”

This makes users very happy

(but it's not that easy)

One way to make it work: make decisions

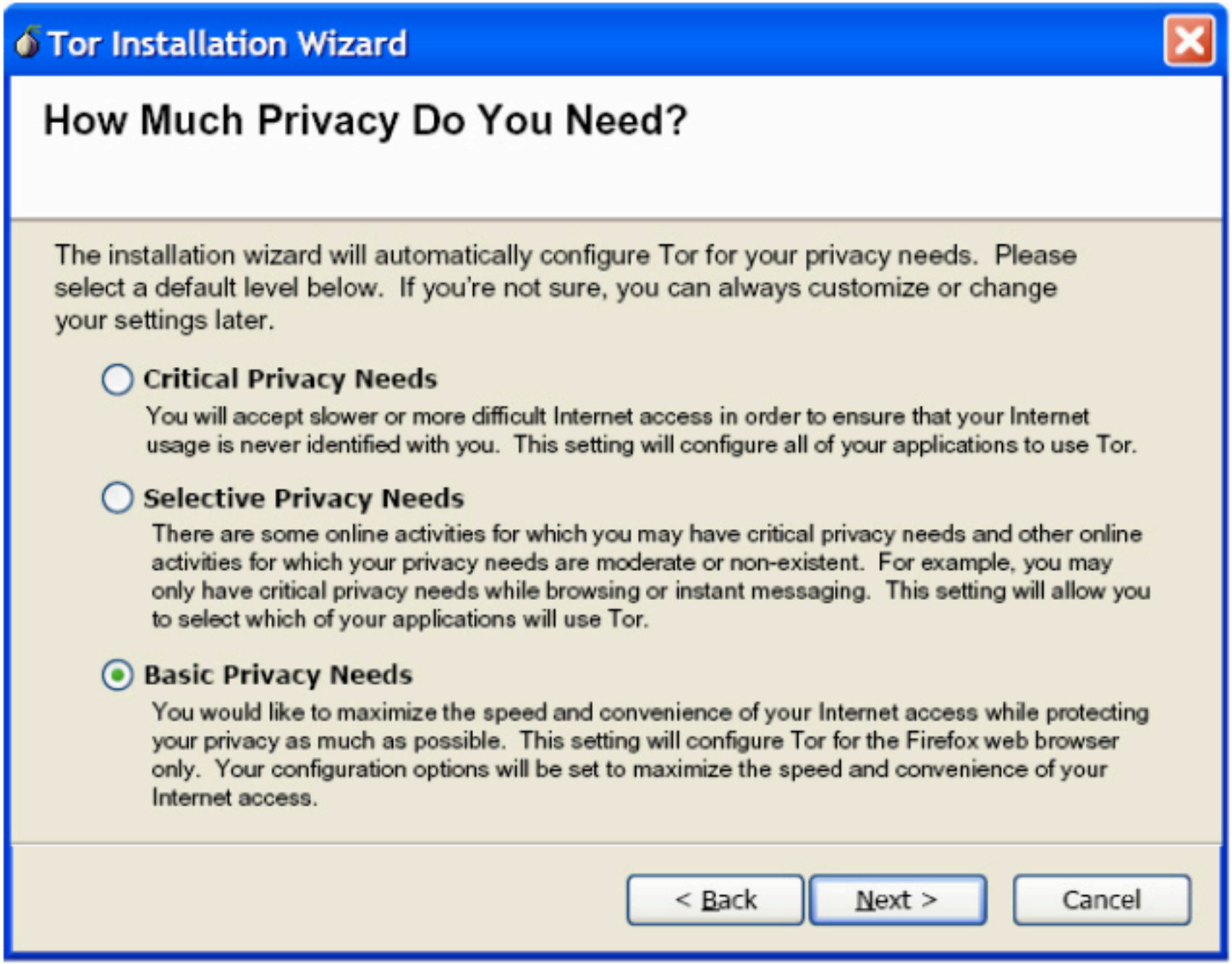


- Developers should not expect users to make decisions they themselves can't make

Make security understandable

"Present choices, not dilemmas"

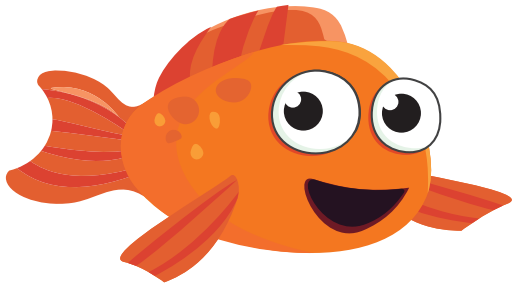
- Chris Nodder
(in charge of user experience for Windows XP SP2)


Tor Installation Wizard
How Much Privacy Do You Need?
The installation wizard will automatically configure Tor for your privacy needs. Please select a default level below. If you're not sure, you can always customize or change your settings later.
Critical Privacy Needs
You will accept slower or more difficult Internet access in order to ensure that your Internet usage is never identified with you. This setting will configure all of your applications to use Tor.
Selective Privacy Needs
There are some online activities for which you may have critical privacy needs and other online activities for which your privacy needs are moderate or non-existent. For example, you may only have critical privacy needs while browsing or instant messaging. This setting will allow you to select which of your applications will use Tor.
Basic Privacy Needs
You would like to maximize the speed and convenience of your Internet access while protecting your privacy as much as possible. This setting will configure Tor for the Firefox web browser only. Your configuration options will be set to maximize the speed and convenience of your Internet access.
< Back
Next >
Cancel

Train the user

Why do humans fall for phish?

- Not motivated to pay attention to training
  - "Security is not my problem"
- Mental models inconsistent with reality
  - "If site looks professional it must be legitimate"
- Need actionable advice they can understand
  - Difficult to be alert if you don't know what you're looking for



How do we get people trained?

Learning science principles

+

Teachable moments

+

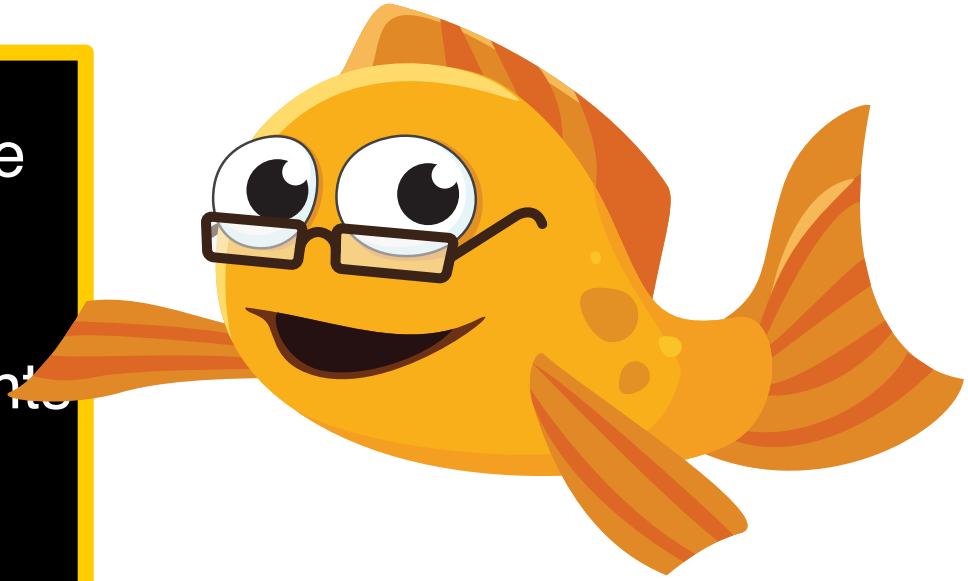
Fun

P. Kumaraguru, S. Sheng, A. Acquisti, L. Cranor, and J. Hong. Teaching Johnny Not to Fall for Phish. *ACM Trans. Internet* [illegible] 31.

PhishGuru embedded training

- Send email that look like phish
- If recipient falls for it, train in succinct and engaging format
- Study demonstrated effectiveness of PhishGuru and found that same training was not effective sent as regular email

Learning science principles
+
Teachable moments
+
Fun



School of phish

Carnegie Mellon University

- 28-day study
- 515 CMU students, faculty, and staff
- Conditions: No training, 1 training message, 2 training messages
- 7 simulated phishing emails and 3 legitimate emails sent to each participant

P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M.A. Blair, and T. Pham. **School of Phish: A Real-Word Evaluation of Anti-Phishing Training.** SOUPS 2009. http://www.cylab.cmu.edu/research/techreports/tr_cylab09002.html

Simulated spear phishing message

From: Help Desk <alert-password@cmu.edu>
Subject: **Your Andrew password alert**
Date: November 17, 2008 11:08:19 AM EST
To: Ponnurangam Kumaraguru (PK)

Dear Student/Faculty/Staff,

Our records indicate that you have not changed your Andrew password in the last 90 days, if you do not change your password in the next 5 days, your access to the Andrew email system will be terminated. Click the link below to update your password.

http://andrewwebmail.org/password/change.htm?ID=9009

Sincerely,
Andrew Help Desk

Simulated spear phishing message

From: Help Desk <alert-password@cmu.edu>
Subject: **Your Andrew password alert**
Date: November 17, 2008 11:08:19 AM EST
To: Ponnurangam Kumaraguru (PK)

Plain text email without graphics

Dear Student/Faculty/Staff,

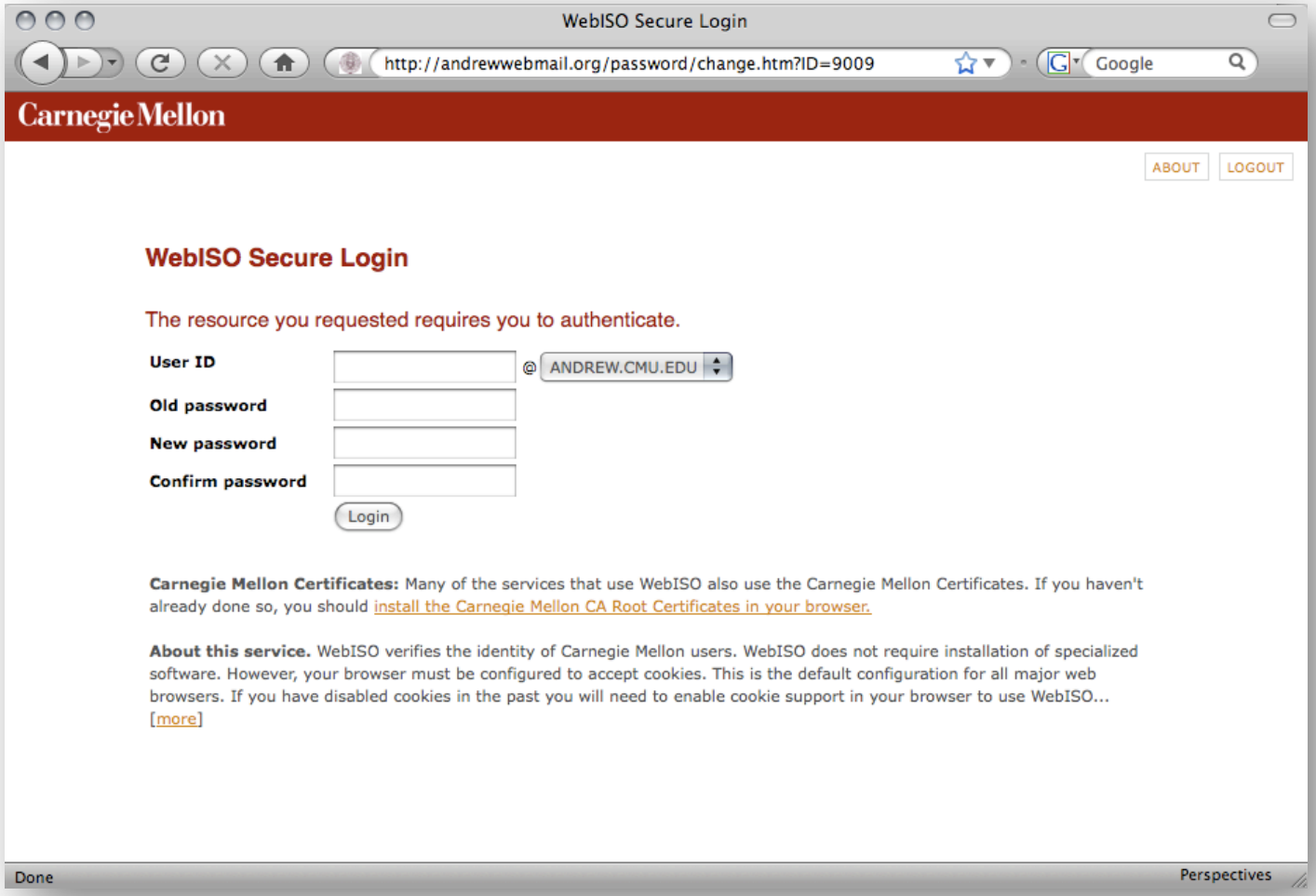
Our records indicate that you have not changed your Andrew password in the last 90 days, if you do not change your password in the next 5 days, your access to the Andrew email system will be terminated. Click the link below to update your password.

http://andrewwebmail.org/password/change.htm?ID=9009

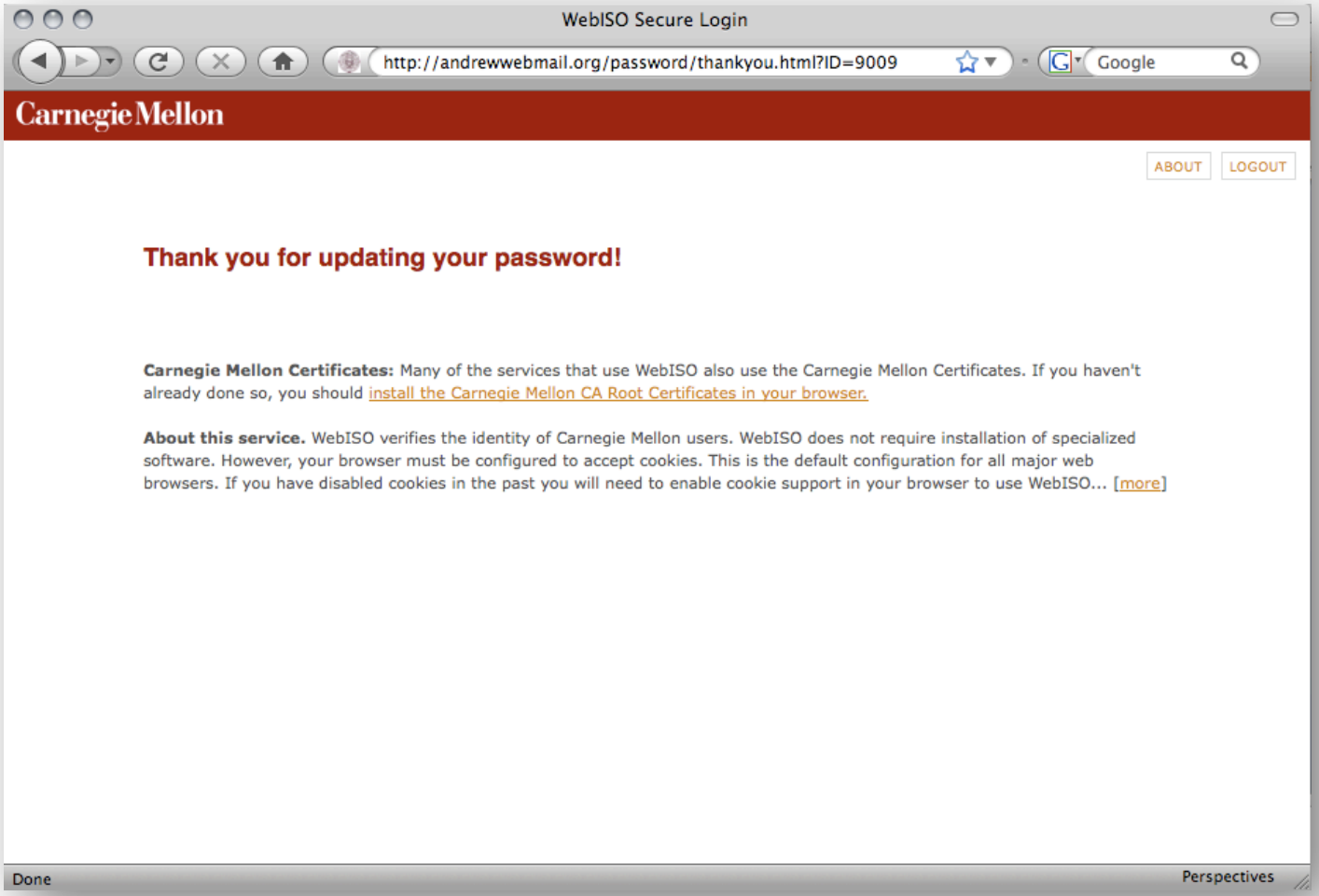
URL is not hidden

Sincerely,
Andrew Help Desk

Simulated phishing website

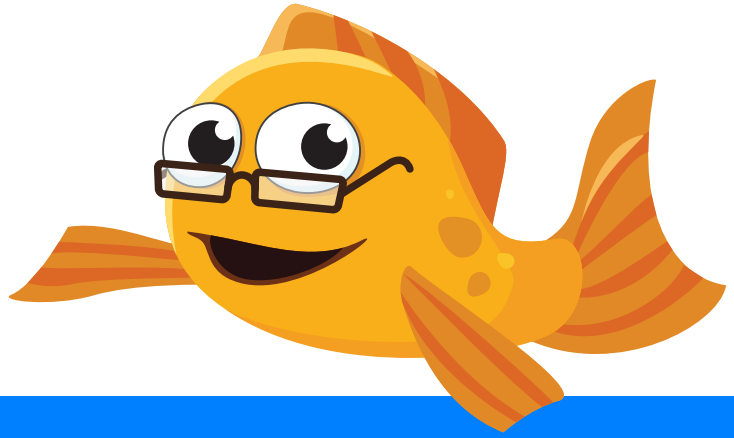


Simulated phishing website

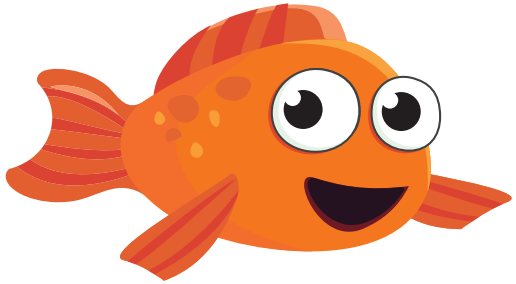


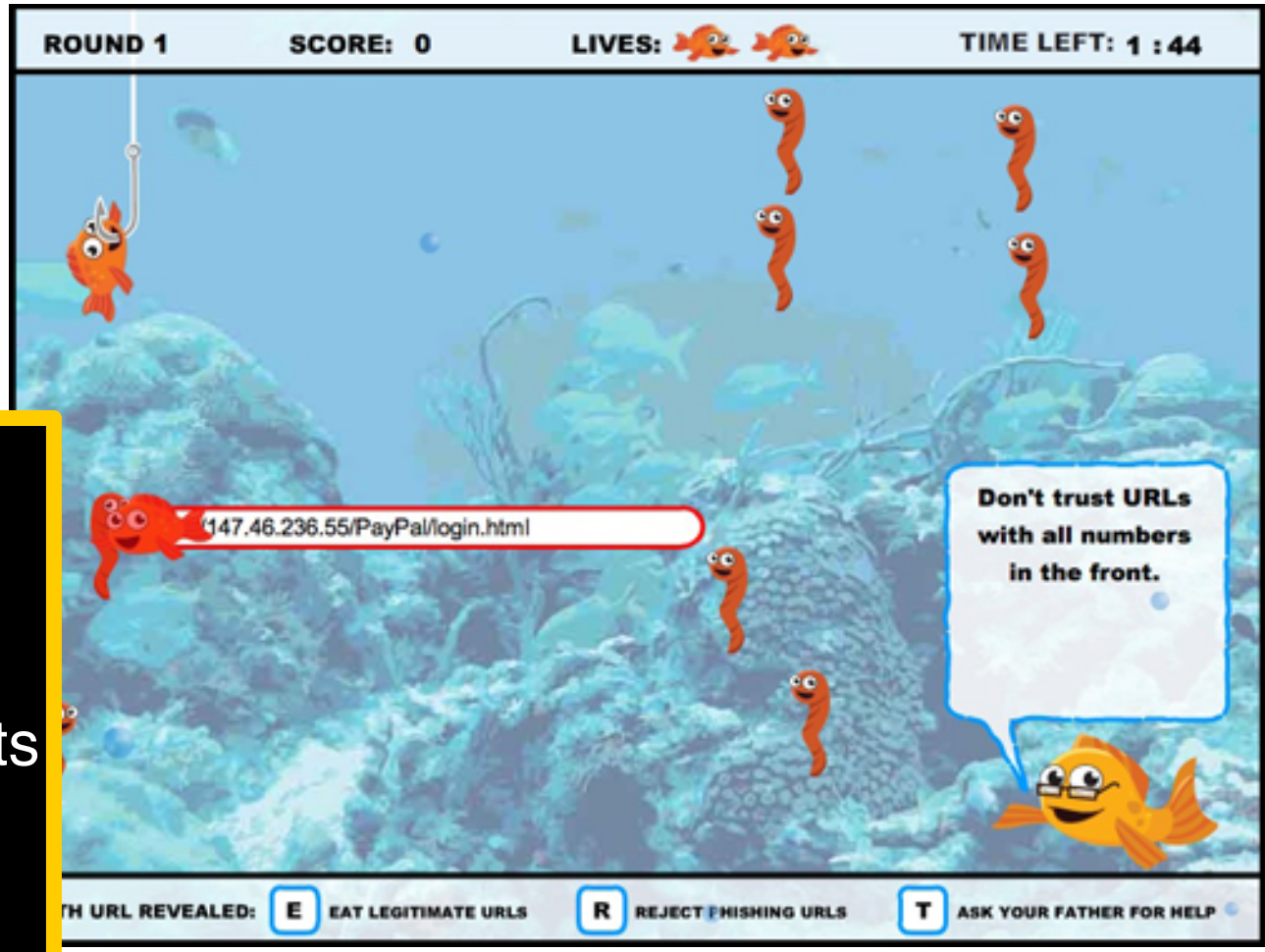
Results

- PhishGuru training taught people to distinguish phishing and legitimate emails
  - Those trained with PhishGuru still clicked on legitimate links
  - But those trained with PhishGuru were less likely to click on phishing links, even 28 days after training



Training games: Anti-phishing Phil





Learning science principles
+
Teachable moments
+
Fun

From research to reality

- Started as student thesis projects
- Studied how experts, novices respond to phish
- Iterated on PhishGuru and Phil implementations
  - Lab studies, focus groups, field studies
- PhishGuru training, Anti-Phishing Phil, and more now offered by Wombat Security Technologies

The human in the loop

Humans

"Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. (They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations.)"

-- C. Kaufman, R. Perlman, and M. Speciner. *Network Security: PRIVATE Communication in a PUBLIC World*. 2nd edition. Prentice Hall, page 237, 2002.

Humans are weakest link

- Most security breaches attributed to “human error”
- Social engineering attacks proliferate
- Frequent security policy compliance failures
- Automated systems are generally more predictable and accurate than humans

Why are humans in the loop at all?

Why are humans in the loop at all?

- Don’t know how or too expensive to automate
- Human judgments or policy decisions needed
- Need to authenticate humans

The human threat

The human threat

- Malicious humans who will attack system

The human threat

- Malicious humans who will attack system
- Humans who are unmotivated to perform security-critical tasks properly or comply with policies

The human threat

- Malicious humans who will attack system
- Humans who are unmotivated to perform security-critical tasks properly or comply with policies
- Humans who don't know when or how to perform security-critical tasks

The human threat

- Malicious humans who will attack system
- Humans who are unmotivated to perform security-critical tasks properly or comply with policies
- Humans who don't know when or how to perform security-critical tasks
- Humans who are incapable of performing security-critical tasks

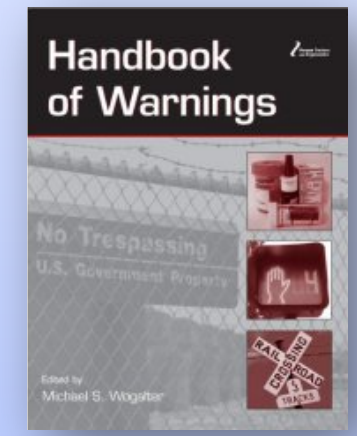
Need to better understand humans in the loop

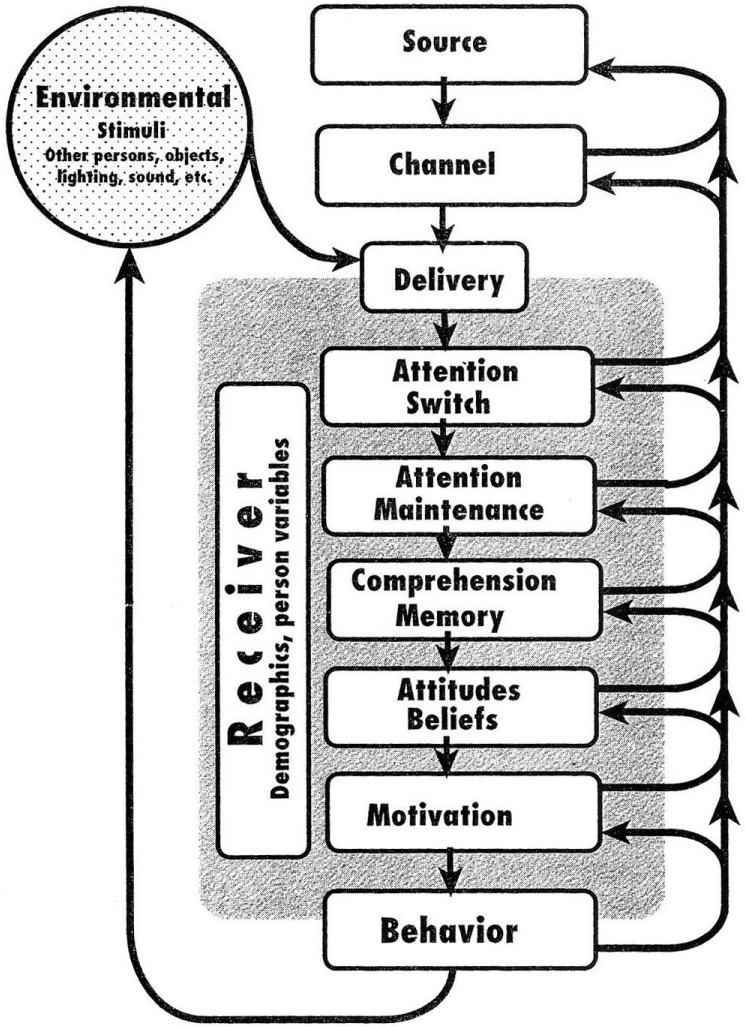
- Do they know they are supposed to be doing something?
- Do they understand what they are supposed to do?
- Do they know how to do it?
- Are they motivated to do it?
- Are they capable of doing it?
- Will they actually do it?

C-HIP Model

Communication-Human Information Processing Model

Wogalter, M. 2006. Communication-Human Information Processing (C-HIP) Model. In Wogalter, M., ed., *Handbook of Warnings*. Lawrence Erlbaum Associates, 51-61.



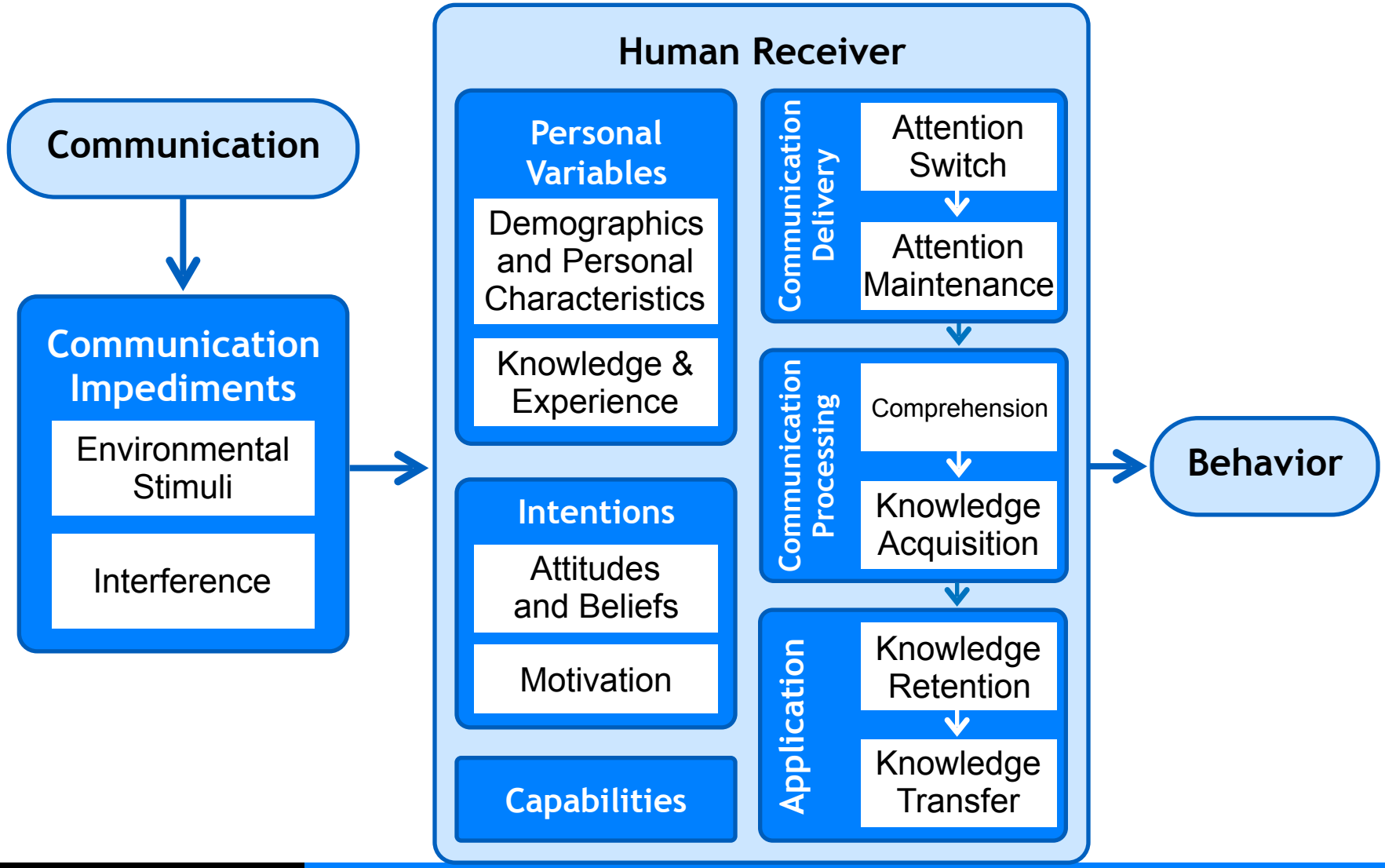


Human-in-the-loop security framework

- Applied C-HIP to security indicators
- Expanded to model other types of human interaction with secure systems
  - Password policies
  - Online trust decisions
- Developed human threat identification and mitigation process

L. Cranor. A Framework for Reasoning About the Human In the Loop. Usability, Psychology and Security 2008. http://www.usenix.org/events/upsec08/tech/full_papers/cranor/cranor.pdf

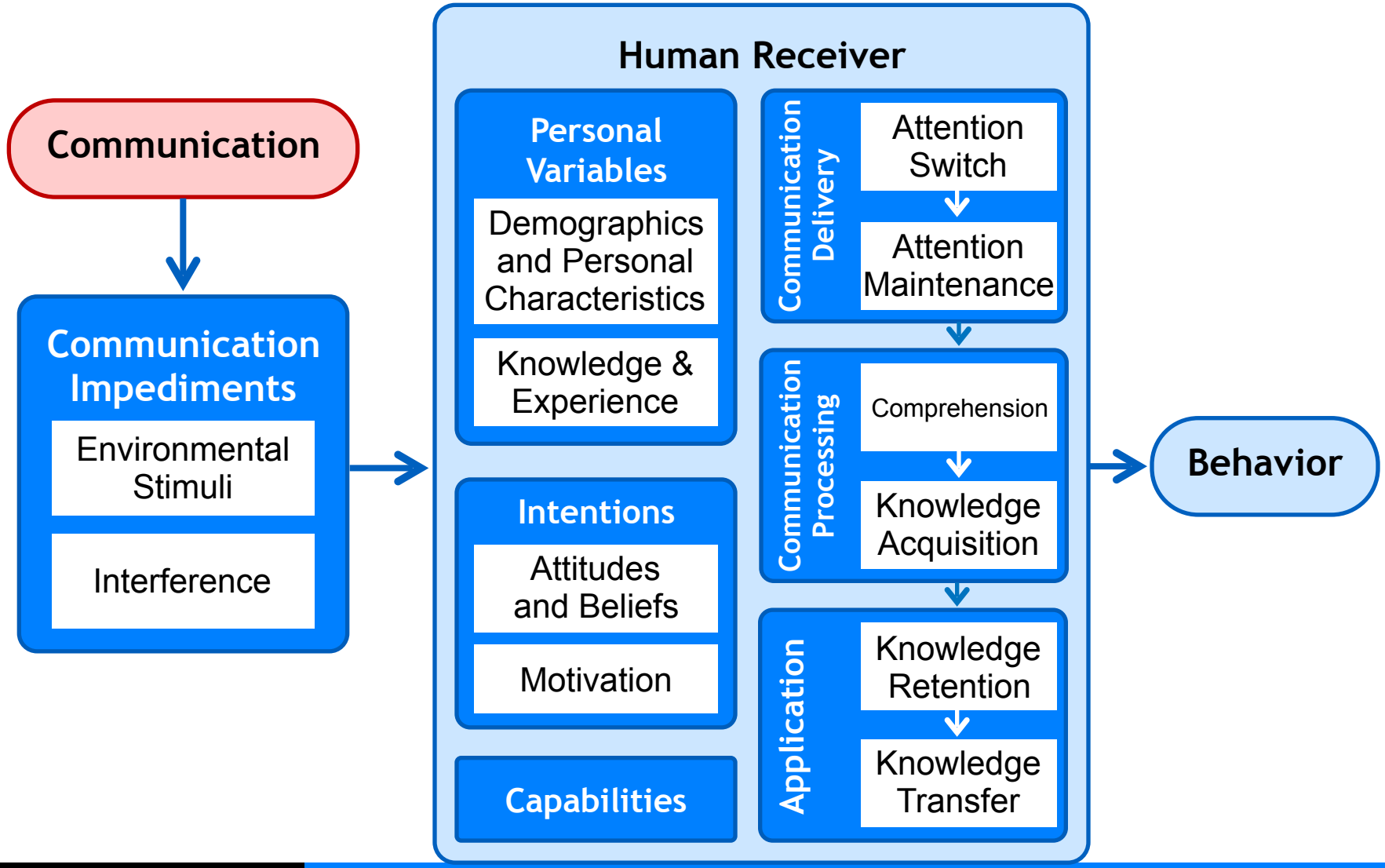
Human-in-the-loop framework



Communication processing model

- Framework is based on communication processing model
  - Many models in the literature
  - Used to model all sorts of communications
- Most end-user security actions are triggered by some form of communication
  - Pop-up alert, email, manual, etc.
- Expert self-discovery of a security process can be modeled as communication to oneself

Communication



Types of security communications

Types of security communications

- Warnings
  - Alert users to take immediate action to avoid hazard

Types of security communications

- Warnings
  - Alert users to take immediate action to avoid hazard
- Notices
  - Inform users about characteristics of entity or object

Types of security communications

- Warnings
  - Alert users to take immediate action to avoid hazard
- Notices
  - Inform users about characteristics of entity or object
- Status indicators
  - Inform users about system status information

Types of security communications

- Warnings
  - Alert users to take immediate action to avoid hazard
- Notices
  - Inform users about characteristics of entity or object
- Status indicators
  - Inform users about system status information
- Training
  - Teach users about threat and how to respond

Types of security communications

- Warnings
  - Alert users to take immediate action to avoid hazard
- Notices
  - Inform users about characteristics of entity or object
- Status indicators
  - Inform users about system status information
- Training
  - Teach users about threat and how to respond
- Policy
  - Inform users about policies

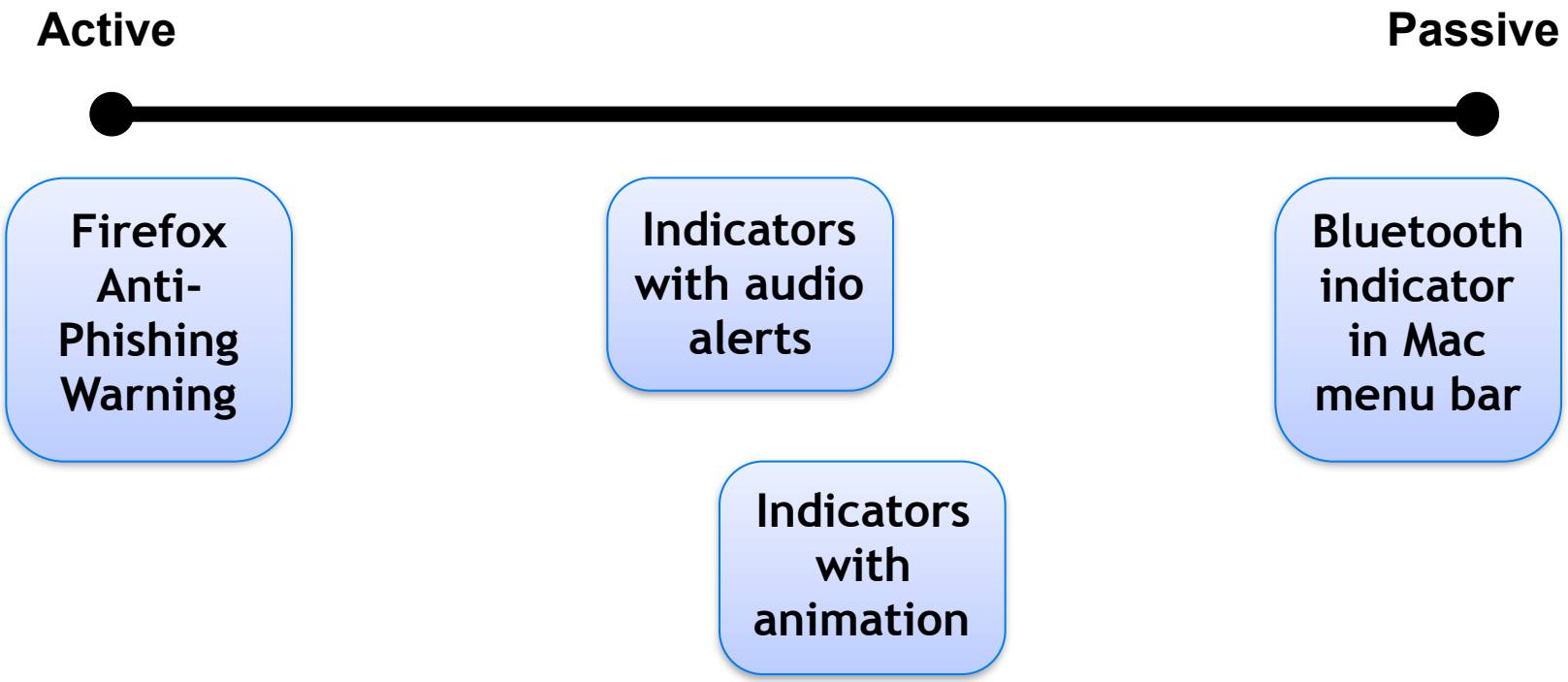
Active versus passive communications

Active versus passive communications

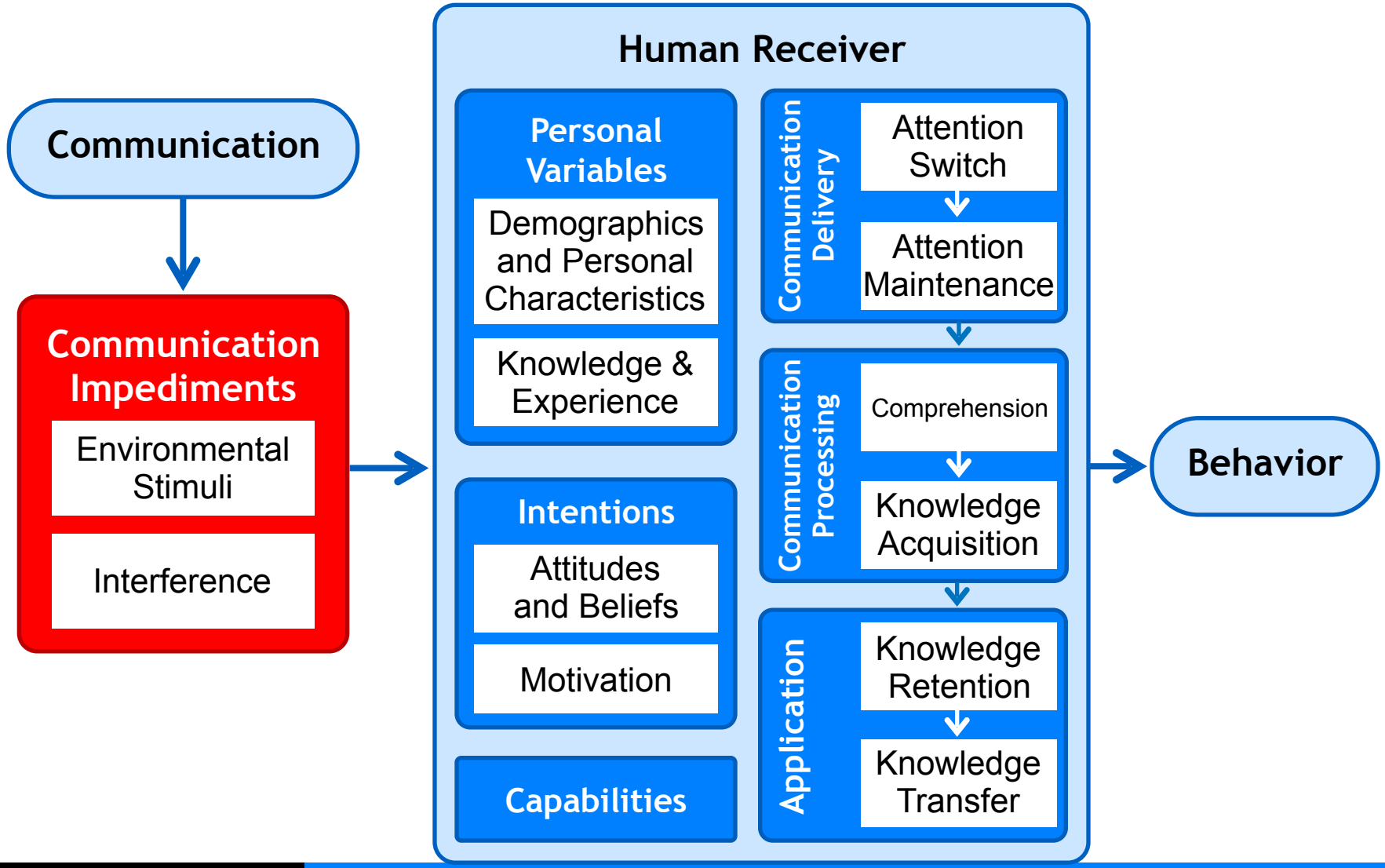
Active versus passive communications

Active versus passive communications

Active versus passive communications

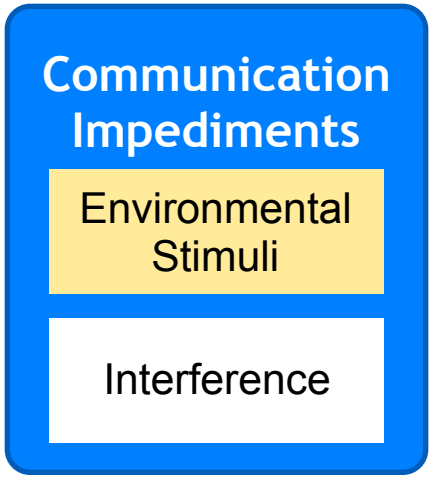


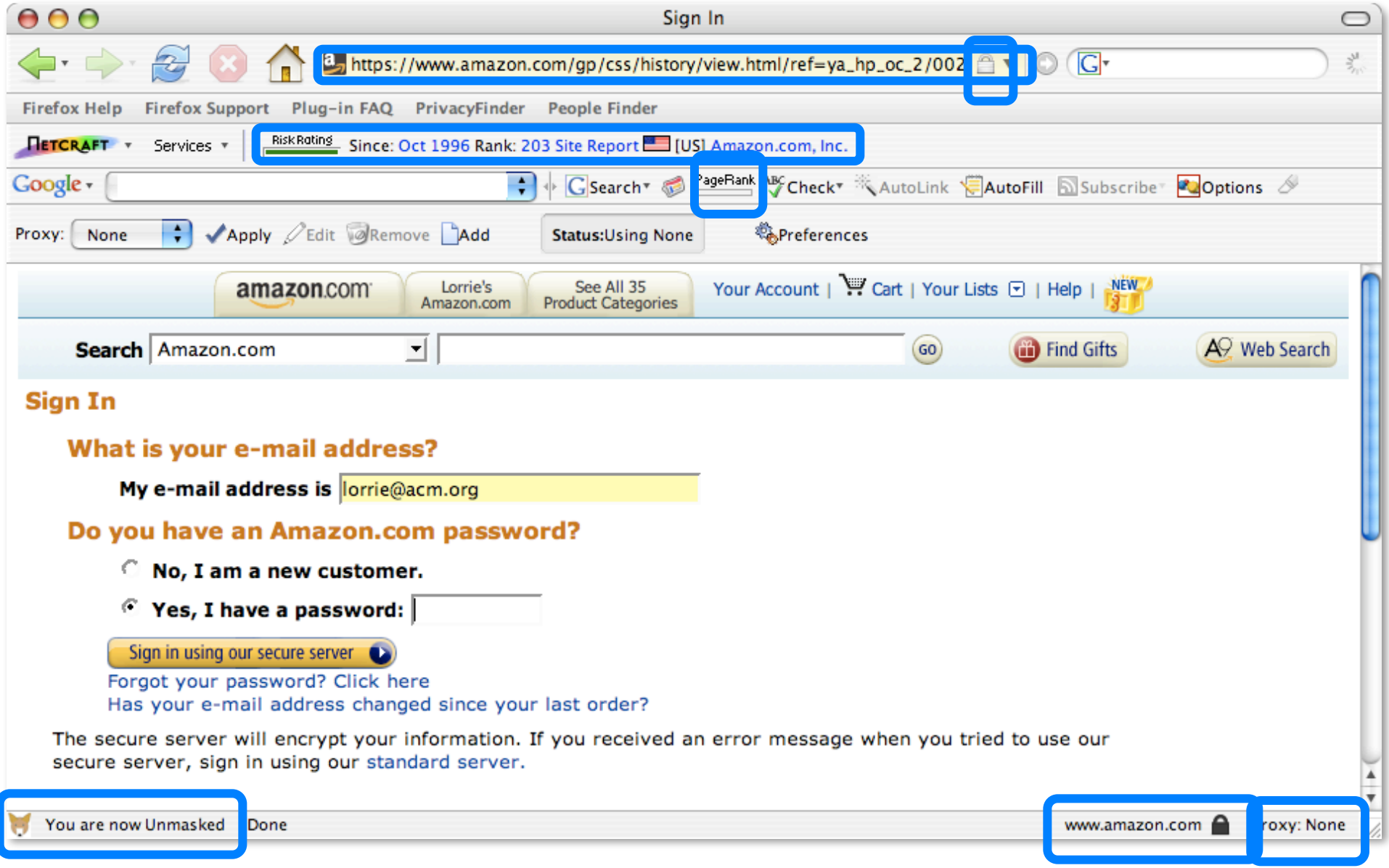
Communication impediments



Environmental stimuli

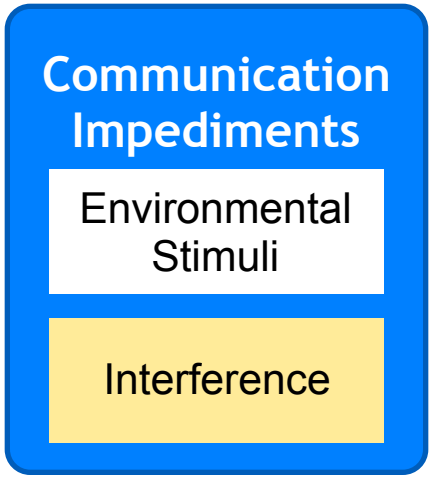
- Divert user's attention
- Greatest impact on passive communication
- Examples
  - Other communications
  - Ambient light and noise
  - User's primary task



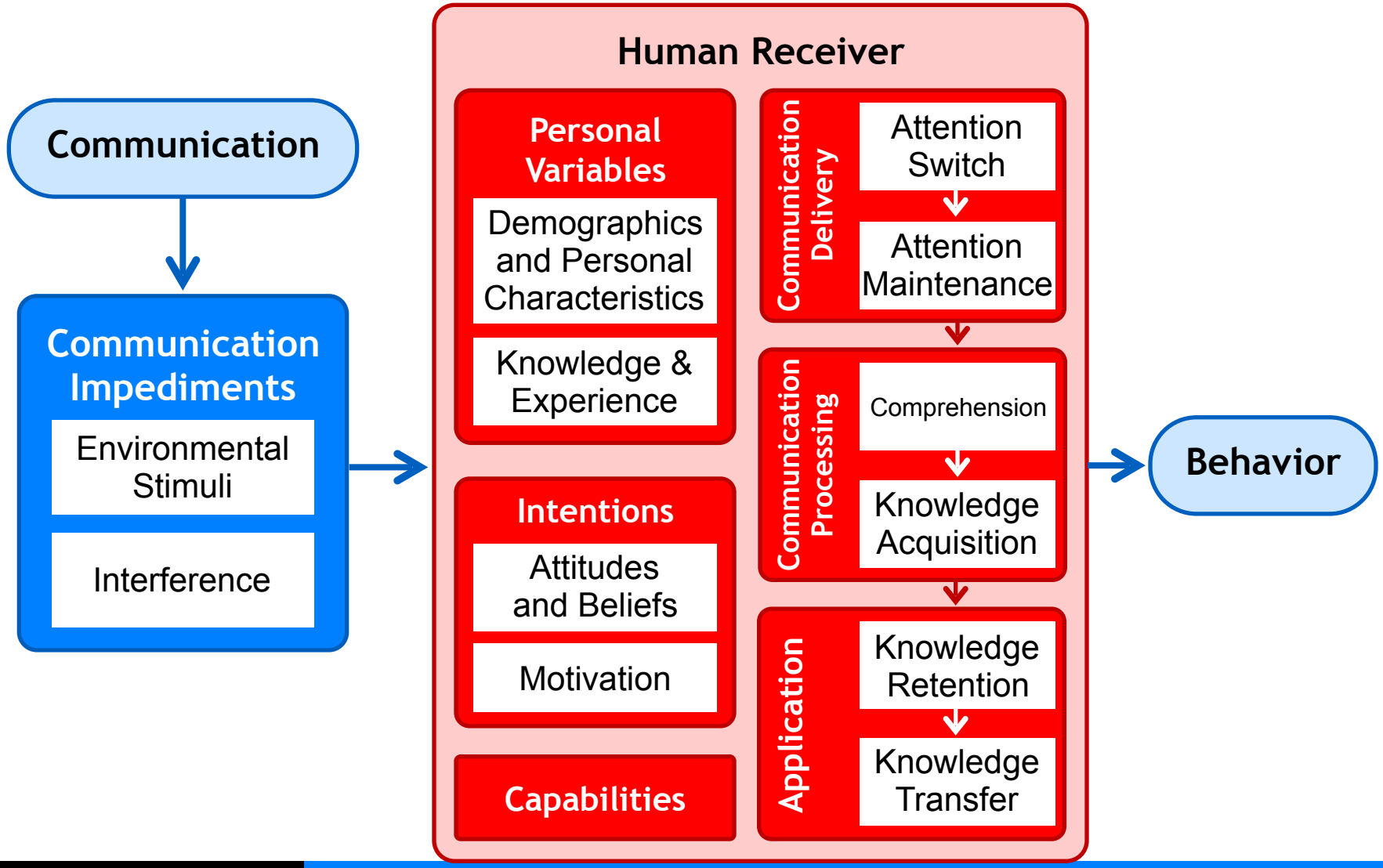

Sign In
https://www.amazon.com/gp/css/history/view.html/ref=ya_hp_oc_2/002
Firefox Help
Firefox Support
Plug-in FAQ
PrivacyFinder
People Finder
NETCRAFT
Services
Risk Rating
Since: Oct 1996 Rank: 203 Site Report
[US] Amazon.com, Inc.
Google
Search
PageRank
Check
AutoLink
AutoFill
Subscribe
Options
Proxy:
None
Apply
Edit
Remove
Add
Status:Using None
Preferences
amazon.com
Lorrie's Amazon.com
See All 35 Product Categories
Your Account | Cart | Your Lists | Help |
NEW
Search
Amazon.com
GO
Find Gifts
Web Search
Sign In
What is your e-mail address?
My e-mail address is
lorrie@acm.org
Do you have an Amazon.com password?
No, I am a new customer.
Yes, I have a password:
Sign in using our secure server
Forgot your password? Click here
Has your e-mail address changed since your last order?
The secure server will encrypt your information. If you received an error message when you tried to use our secure server, sign in using our standard server.
You are now Unmasked
Done
www.amazon.com
roxy: None

Interference

- Anything that may prevent a communication from being received as the sender intended
- Caused by
  - Malicious attackers
  - Technology failures
  - Environmental stimuli that obscure the communication
- Focus of traditional secure systems analysis



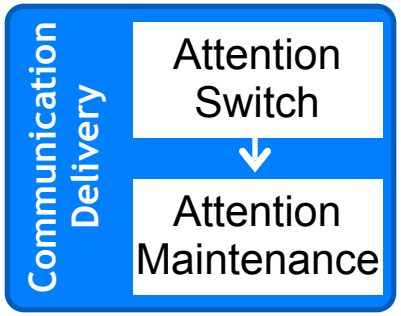
Human receiver – *The human in the loop*



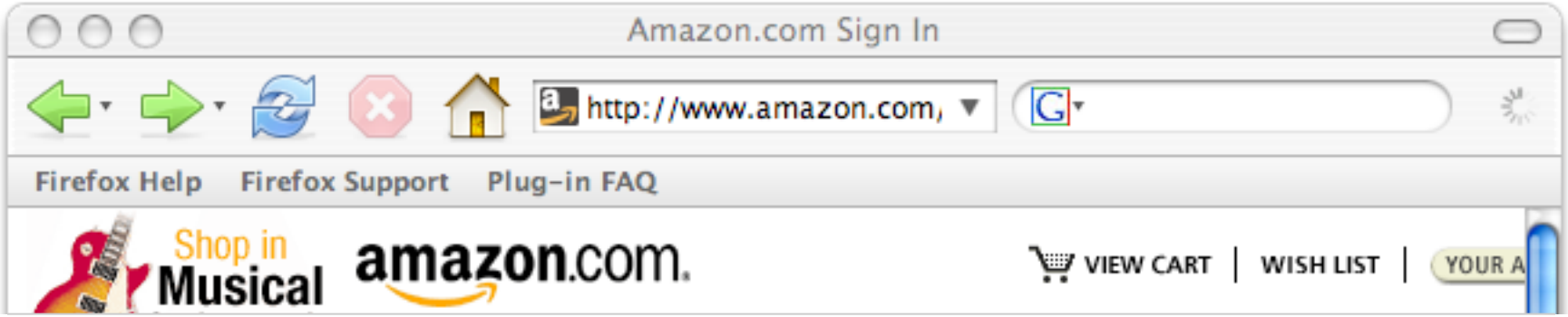
Communication delivery

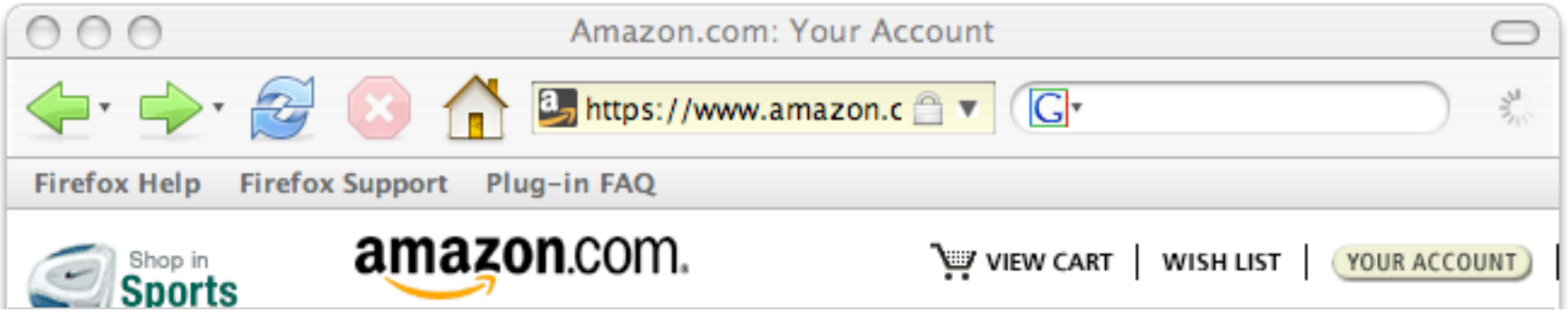
- Attention switch
  - Noticing communication
- Attention maintenance
  - Paying attention long enough to process

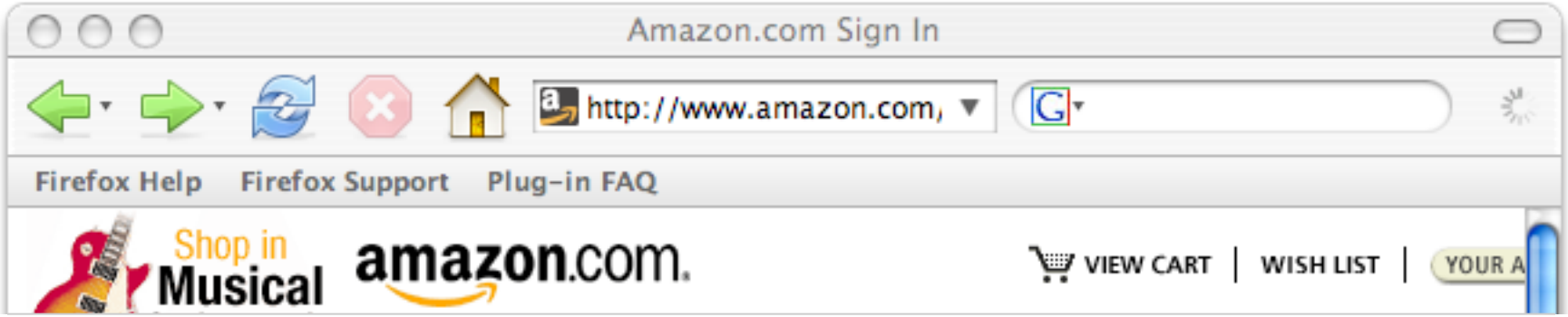
- Breakdowns
  - Environmental stimuli, interference
  - Characteristics of communication
  - Habituation
    - Tendency for the impact of stimuli to decrease over time

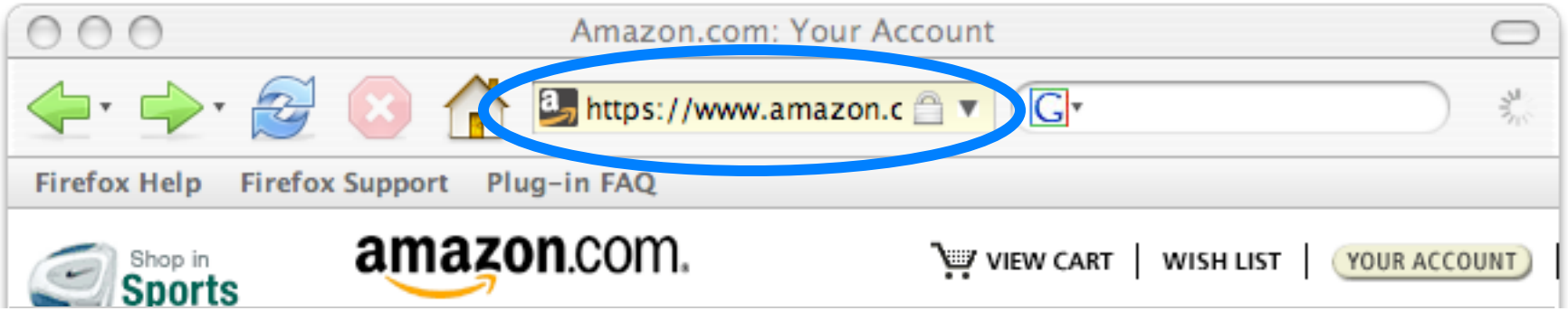


“What lock icon?”


Amazon.com Sign In
http://www.amazon.com/
Firefox Help
Firefox Support
Plug-in FAQ
Shop in
Musical
amazon.com
VIEW CART
WISH LIST
YOUR A


Amazon.com: Your Account
https://www.amazon.c
Firefox Help
Firefox Support
Plug-in FAQ
Shop in
Sports
amazon.com
VIEW CART
WISH LIST
YOUR ACCOUNT

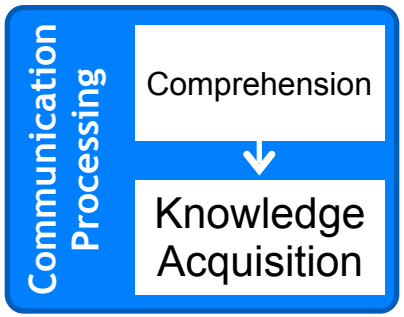

Amazon.com Sign In
http://www.amazon.com/
Firefox Help
Firefox Support
Plug-in FAQ
Shop in
Musical
amazon.com
VIEW CART
WISH LIST
YOUR A

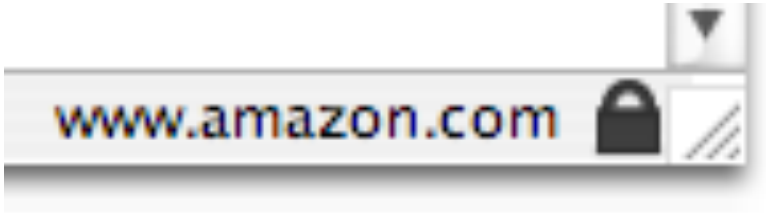

Amazon.com: Your Account
https://www.amazon.c
Firefox Help
Firefox Support
Plug-in FAQ
Shop in
Sports
amazon.com
VIEW CART
WISH LIST
YOUR ACCOUNT

Communication processing

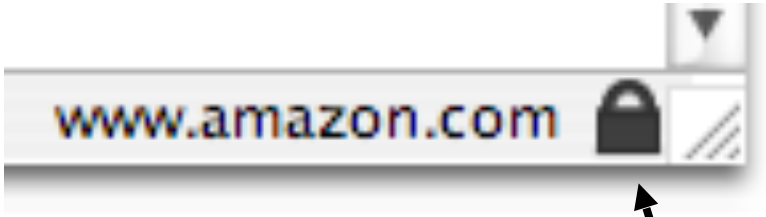
- Comprehension
  - Understand communication
- Knowledge acquisition
  - Learn what to do in response

- Breakdowns
  - Unfamiliar symbols, vocabulary, complex sentences, conceptual complexity

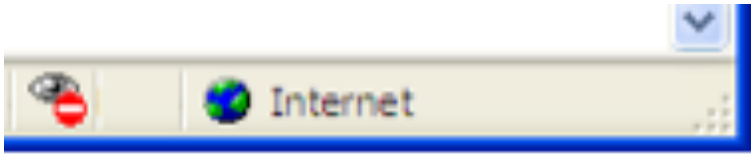


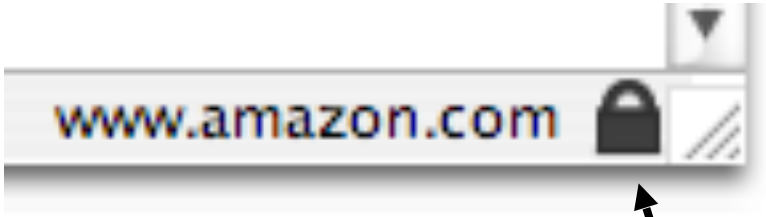

www.amazon.com


www.amazon.com
Firefox SSL icon

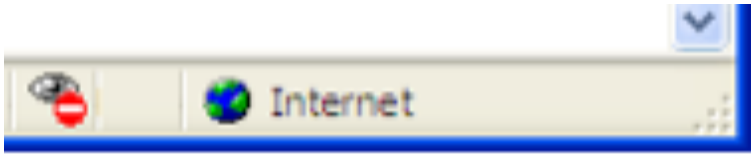


Firefox SSL icon





Firefox SSL icon



Internet Explorer cookie flag

OPERATOR SPECIALTY COMPANY, INC.

⚠ WARNING

Moving Gate Can Cause Serious Injury or Death

KEEP CLEAR! Gate may move at any time without warning.

Do not allow children to operate the gate or play in the gate area.

This gate is for vehicles only. All pedestrians must use a separate entrance.

Read the owner's manual and safety instructions

If entrapment protection is by constant hold control, an automatic closing device shall not be used with this gate operator.

OED-300 7/99

OPERATOR SPECIALTY COMPANY, INC.

WARNING

Moving Gate Can Cause
Serious Injury or Death

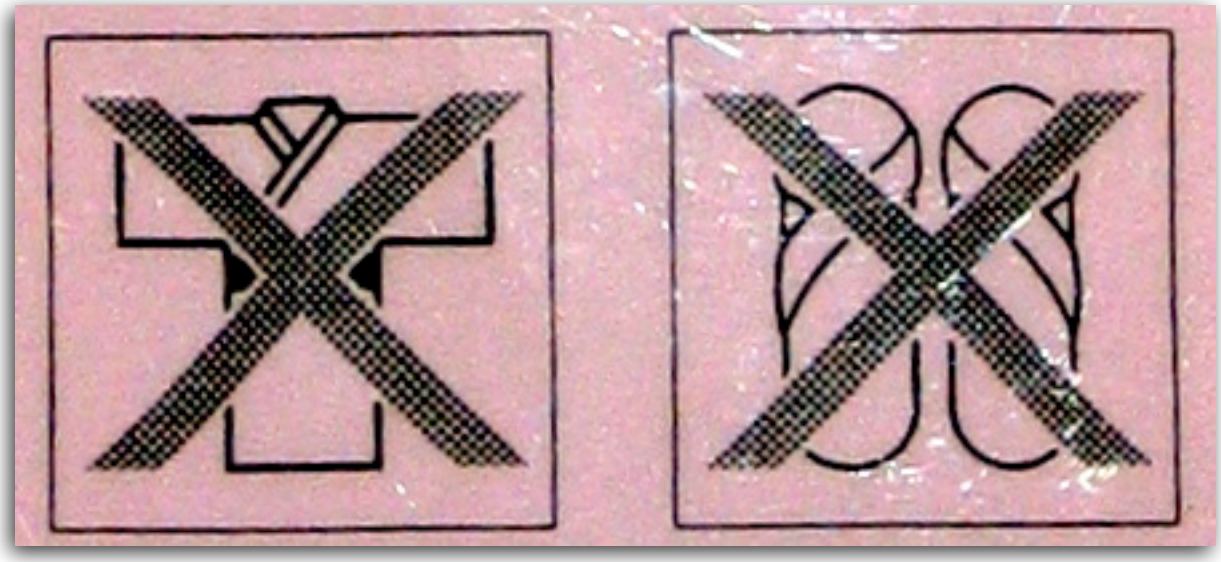
OPERATOR SPECIALTY COMPANY, INC.

ARNING

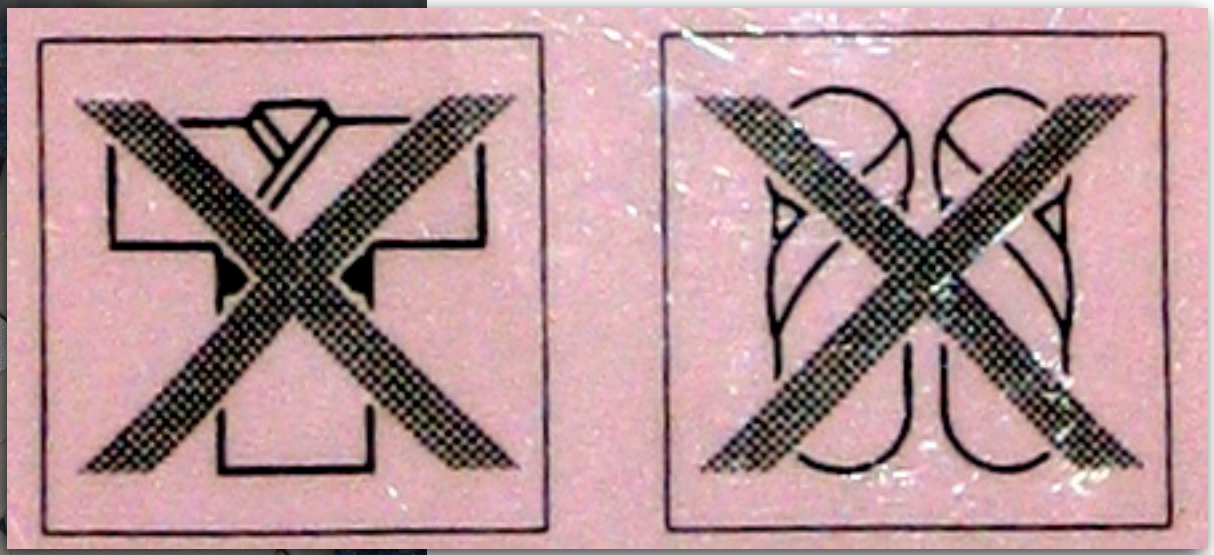
AUTOS ONLY
NO PEDESTRIANS
NO MOTORCYCLES
NO BICYCLES

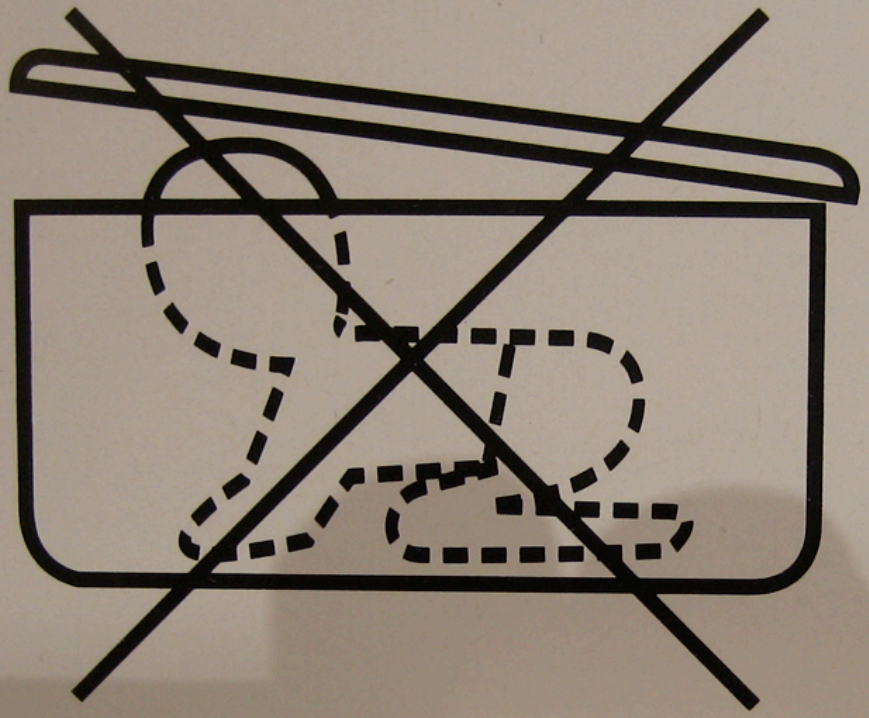
KEEP AWAY FROM GATE ARM
MOVING GATE ARM CAN CAUSE
SERIOUS INJURY OR VEHICLE DAMAGE

Moving Gate Can Cause
Serious Injury or Death




PRINCE HOTELS
浴衣・スリッパのままで、客室フロア（廊下）以外へ
お出になることは、非常時を除き、
ご遠慮ください。



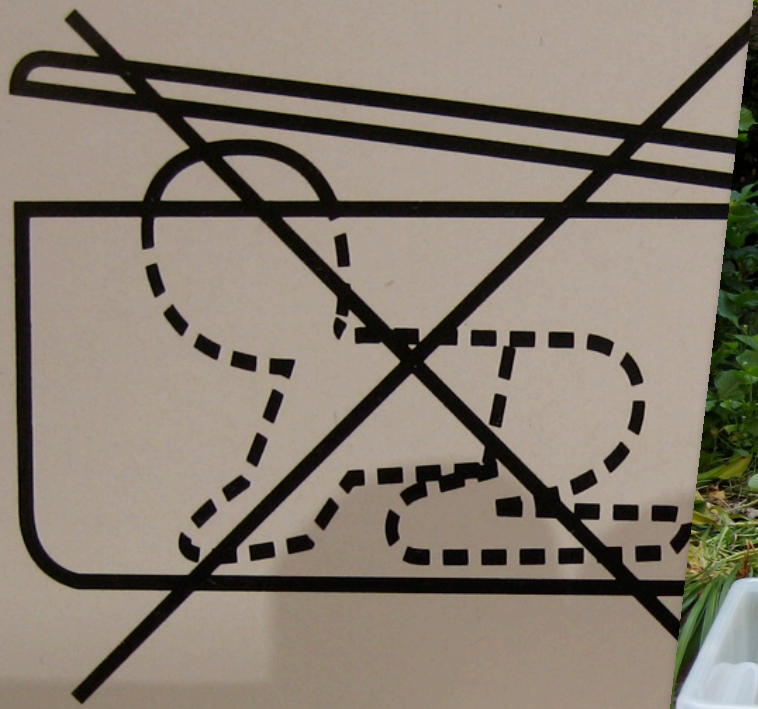


⚠ **WARNING!**
SUFFOCATION HAZARD

⚠ **MISE EN GARDE !**
RISQUE D'ÉTOUFFEMENT.

DEUTSCH
WARNHINWEIS! Erstickungsgefahr.

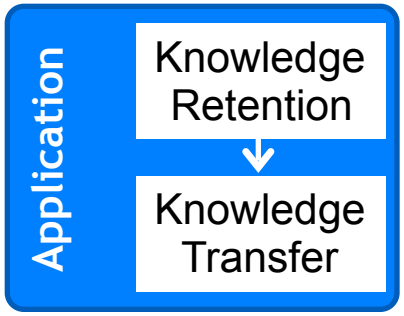
NEDERLANDS
LET OP! Verstikkingsgevaar.



Application

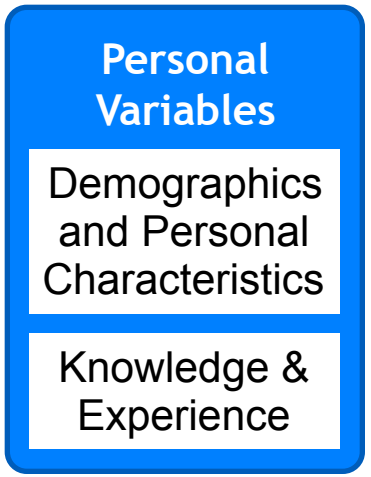
- Knowledge retention
  - Ability to remember communication
- Knowledge transfer
  - Ability to recognize applicable situations and apply knowledge

- May not be necessary if application is immediate (e.g. pop-up warning)



Personal variables

- Demographics and personal characteristics
  - Age, gender, culture, education, occupation, disabilities
- Knowledge and experience
  - Education, occupation, prior experience



Intentions

- Attitudes and beliefs
  - Beliefs about communication accuracy
  - Beliefs about whether they should pay attention
  - Self-efficacy - whether they believe they can complete actions effectively
  - Response-efficacy - whether they believe the actions they take will be effective
  - How long it will take
  - General attitudes - trust, annoyance
- Motivation
  - Incentives, disincentives

Capabilities

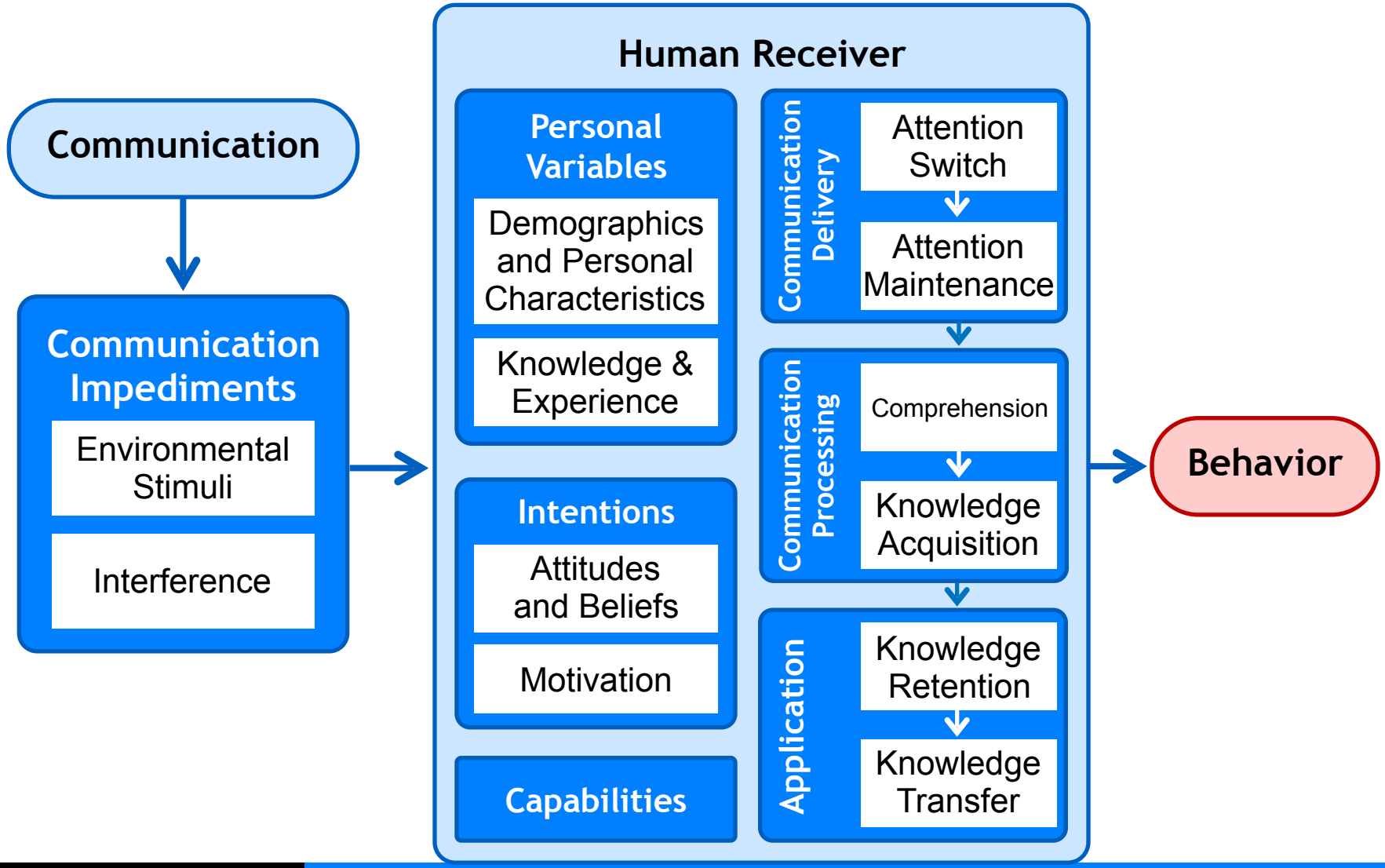
- User's level of ability
  - Cognitive or physical skills
  - Availability of necessary software or devices

Capabilities

Are you capable of remembering a unique strong password for every account you have?

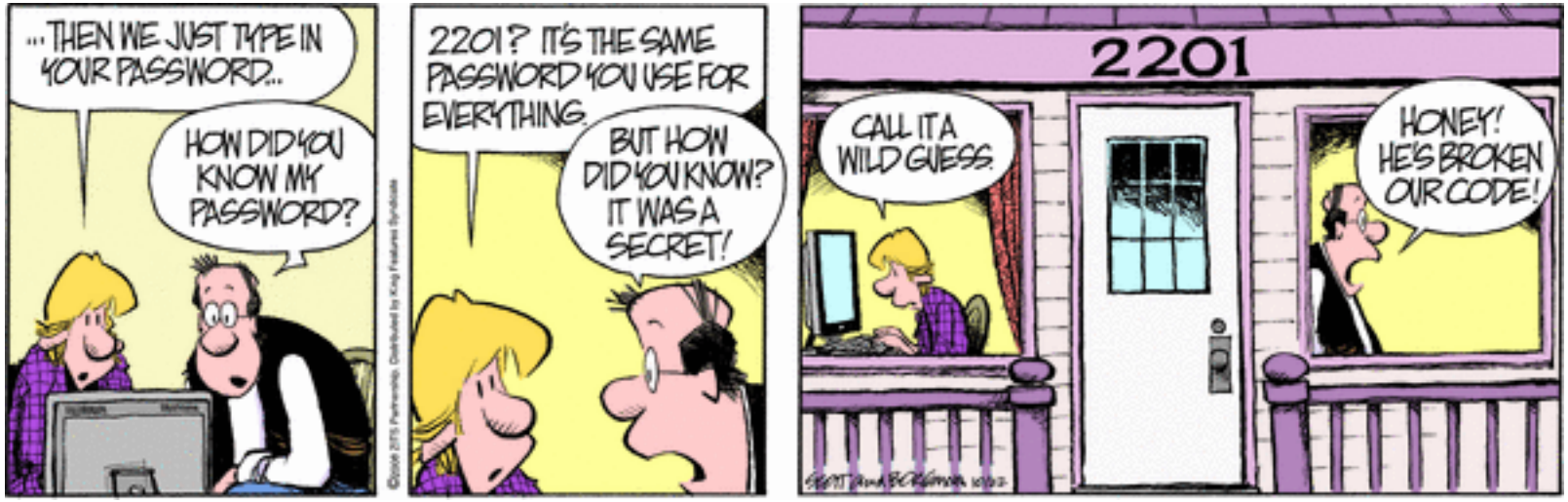
Are you capable of remembering a uniqu strong password for every account you have?

Behavior


Communication
Communication Impediments
Environmental Stimuli
Interference
Human Receiver
Personal Variables
Demographics and Personal Characteristics
Knowledge & Experience
Intentions
Attitudes and Beliefs
Motivation
Capabilities
Communication Delivery
Attention Switch
Attention Maintenance
Communication Processing
Comprehension
Knowledge Acquisition
Application
Knowledge Retention
Knowledge Transfer
Behavior

Behavior

- Users may intend to comply, but may fail to complete necessary action
- Users may complete recommended action, but do so in a way that follows a predictable pattern that can be exploited by attackers
  - Example: password choice



http://www.arcamax.com/zits/s-427369-156783

Zits by Jerry Scott and Jim Borgman, October 22, 2008

Gulfs

- Gulf of Execution
  - Gap between a person's intentions to carry out an action and the mechanisms provided by a system to facilitate that action
    - "I can't figure out how to make it do what I want it to do"
- Gulf of Evaluation
  - When a user completes an action but is unable to interpret the results to determine whether it was successful
    - "I can't figure out whether it worked"

Don Norman. *The Design of Every Day Things*.1988.

Generic Error-Modeling System

- Mistakes
  - When people formulate action plans that will not achieve the desired goal
- Lapses
  - When people formulate suitable action plans, but forget to perform a planned action (for example, skipping a step)
- Slips
  - When people perform actions incorrectly (for example, press the wrong button)

James Reason. *Human Error.* 1990.

Handy tab

Component

Questions to ask

Factors to consider

Appendix A: Components of the human-in-the-loop security framework

Component		Questions to ask	Factors to consider
Communication		What type of communication is it (warning, notice, status indicator, policy, training)? Is communication active or passive? Is this the best type of communication for this situation?	Severity of hazard, frequency with which hazard is encountered, extent to which appropriate user action is necessary to avoid hazard
Communication impediments	Environmental Stimuli	What other environmental stimuli are likely to be present?	Other related and unrelated communications, user's primary task, ambient light, noise
	Interference	Will anything interfere with the communication being delivered as intended?	Malicious attackers, technology failures, environmental stimuli that obscure the communication
Personal variables	Demographics and personal characteristics	Who are the users? What do their personal characteristics suggest about how they are likely to behave?	Age, gender, culture, education, occupation, disabilities
	Knowledge and experience	What relevant knowledge or experience do the users or recipients have?	Education, occupation, prior experience
Intentions	Attitudes and beliefs	Do users believe the communication is accurate? Do they believe they should pay attention to it? Do they have a positive attitude about it?	Reliability, conflicting goals, distraction from primary task, risk perception, self-efficacy, response efficacy
	Motivation	Are users motivated to take the appropriate action? Are thy motivated to do it carefully or properly?	Conflicting goals, distraction from primary task, convenience, risk perception, consequences, incentives/disincentives
Capabilities		Are users capable of taking the appropriate action?	Knowledge, cognitive or physical skills, memorability, required software or devices
Communication delivery	Attention switch	Do users notice the communication? Are they aware of rules, procedures, or training messages?	Environmental stimuli, interference, format, font size, length, delivery channel, habituation
	Attention maintenance	Do users pay attention to the communication long enough to process it? Do they read, watch, or listen to it fully?	Environmental stimuli, format, font size, length, delivery channel, habituation
Communication processing	Comprehension	Do users understand what the communication means?	Symbols, vocabulary and sentence structure, conceptual complexity, personal variables
	Knowledge acquisition	Have users learned how to apply it in practice? Do they know what they are supposed to do?	Exposure or training time, involvement during training, personal characteristics
Application	Knowledge retention	Do users remember the communication when a situation arises in which they need to apply it? Do they recognize and recall the meaning of symbols or instructions?	Frequency, familiarity, long term memory, involvement during training, personal characteristics
	Knowledge transfer	Can users recognize situations where the communication is applicable and figure out how to apply it?	Involvement during training, similarity of training, personal characteristics
Behavior		Does behavior result in successful completion of desired action?	*See Norman's Stages of Action, GEMS*
		Does behavior follow predictable patterns that an attacker might exploit?	Type of behavior, ability of people to act randomly in this context, usefulness of prediction to attacker

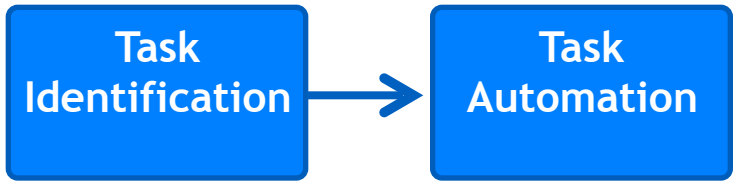
Human threat identification and mitigation process

Human threat identification and mitigation process

Task Identification

Identify points where system relies on humans to perform security-critical functions

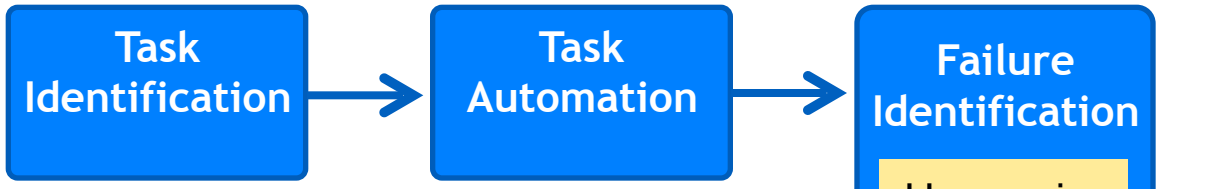
Human threat identification and mitigation process



Identify points where system relies on humans to perform security-critical functions

Find ways to partially or fully automate some of these tasks

Human threat identification and mitigation process

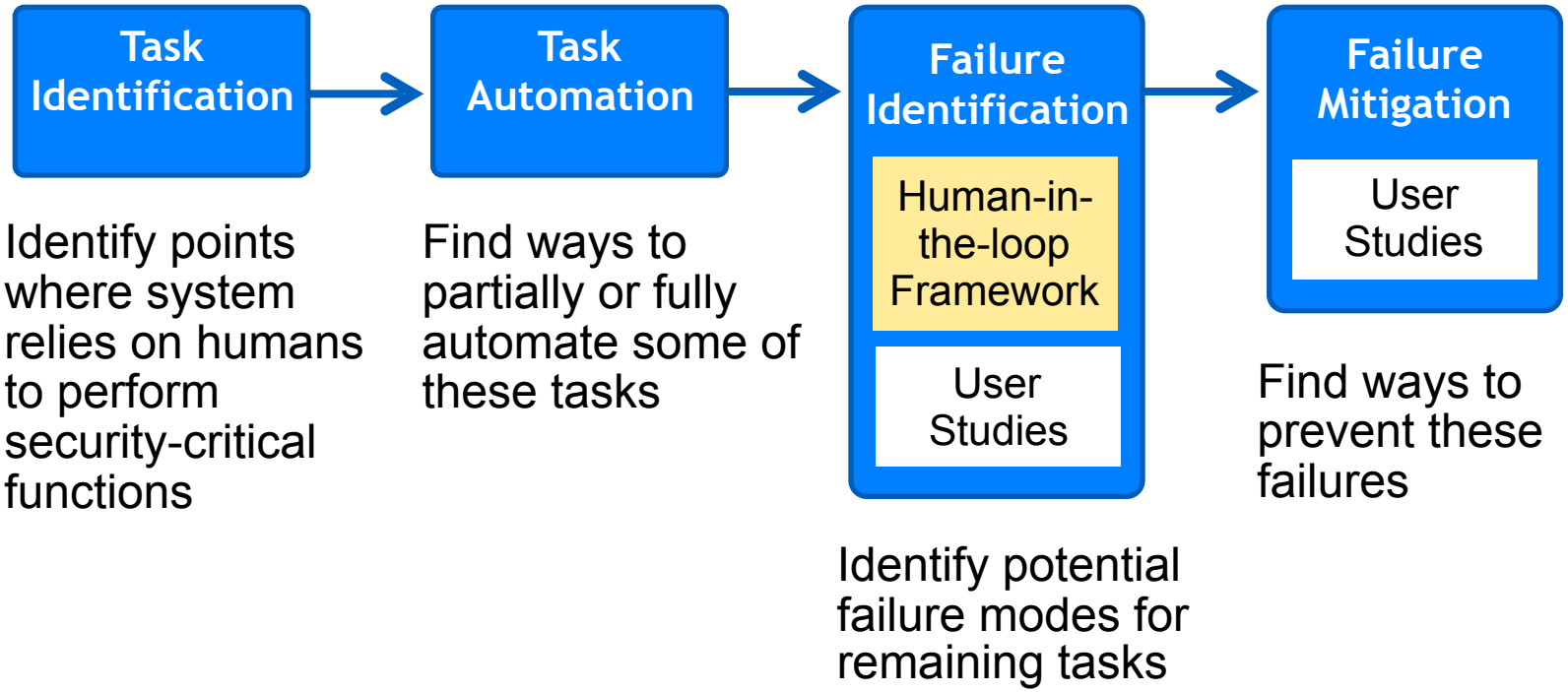


Identify points where system relies on humans to perform security-critical functions

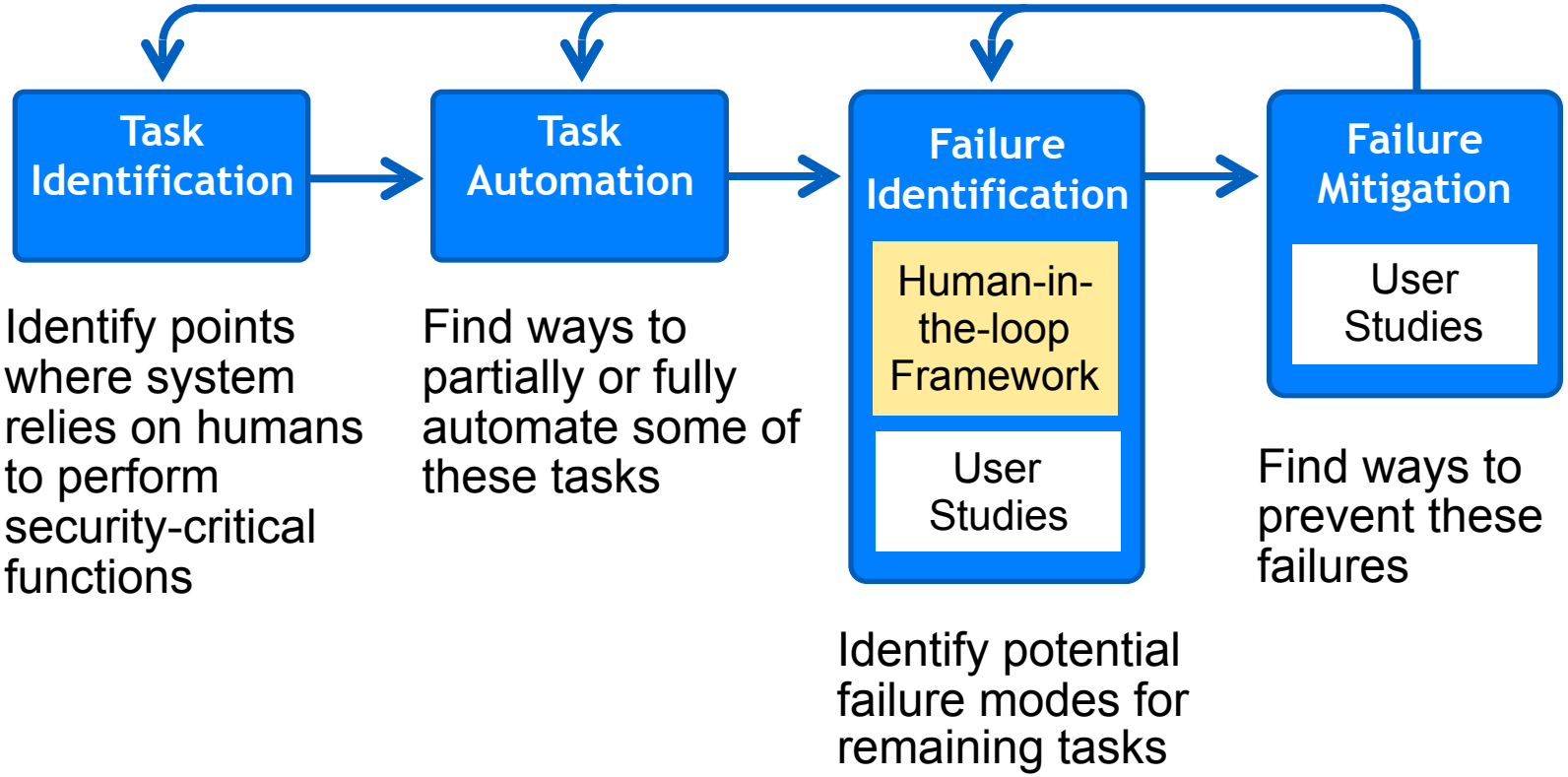
Find ways to partially or fully automate some of these tasks

Identify potential failure modes for remaining tasks

Human threat identification and mitigation process



Human threat identification and mitigation process



Guidelines for automating appropriately

- How accurate is the system?
- How are stakeholder values embodied in the system? What roles do social and environmental contexts have in this particular application?
- Does automation reduce end-user information overload or otherwise simplify the task of security decision making?
- Are there alternatives to automation that are at least as appropriate for end-users?
- If automating, are there mechanisms to "keep the human in the loop"?
- If the automation mechanisms fail, are there user interfaces for gracefully dealing with these situations?

W.K. Edwards, E.S. Poole, and J. Stoll. Security Automation Considered Harmful? NSPW;07.

Applying the framework

- Applied as part of a human threat identification and mitigation process
- Can be applied to understand failures in existing systems and prioritize mitigations
- Can be applied to proposed systems in design phase to inform design decisions

Applying threat identification and mitigation process to warnings

- Task identification
  - Determine whether the task I am trying to complete is sufficiently risky that I should stop
- Often, software asks the user and provides little or no information to help user make this decision

Computer security warnings

- All too often, when software detects a possible security hazard, it warns the user about it
- Often, it turns out not to be a hazard
- But sometimes it really is a hazard and users ignore the warning anyway


Security Error: Domain Name Mismatch
You have attempted to establish a connection with "www.whitehouse.gov". However, the security certificate presented belongs to "a248.e.akamai.net". It is possible, though unlikely, that someone may be trying to intercept your communication with this web site.
If you suspect the certificate shown does not belong to "www.whitehouse.gov", please cancel the connection and notify the site administrator.
View Certificate
Cancel
OK

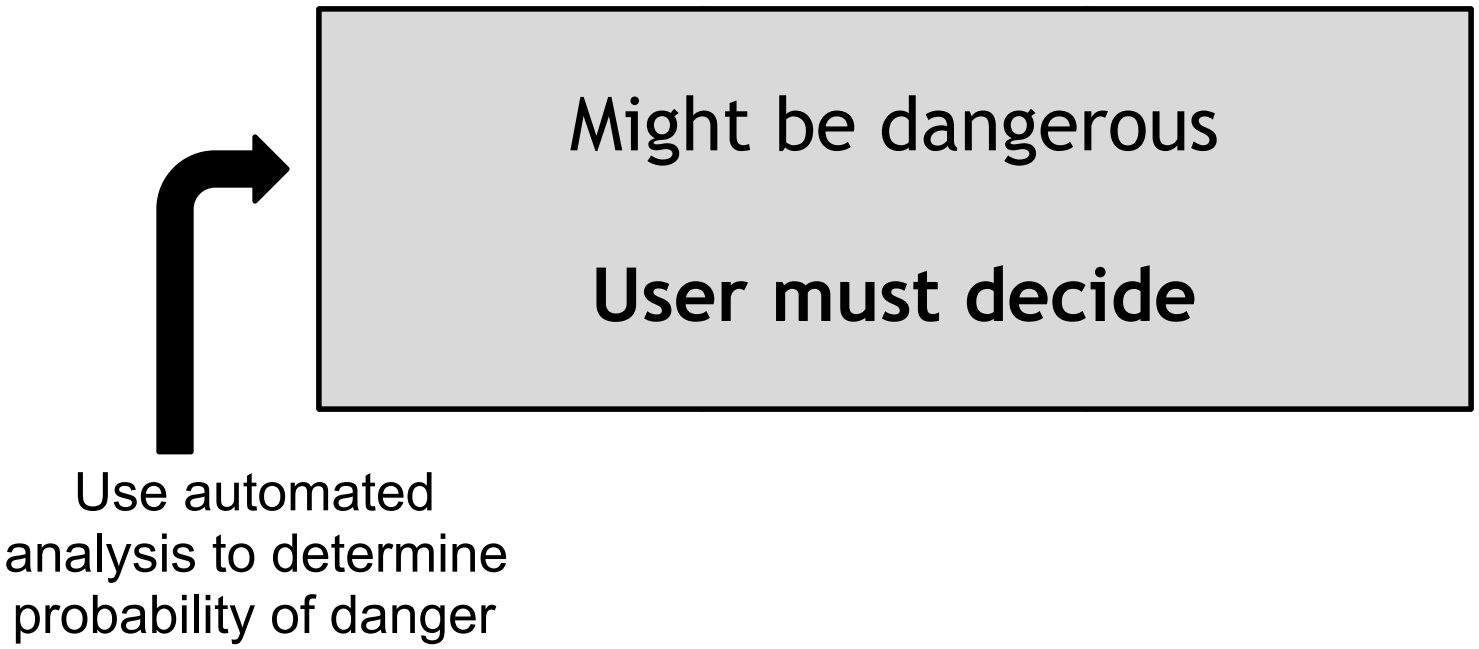
Image courtesy of Jonathan Nightingale

Automate and change tasks to reduce need for user involvement

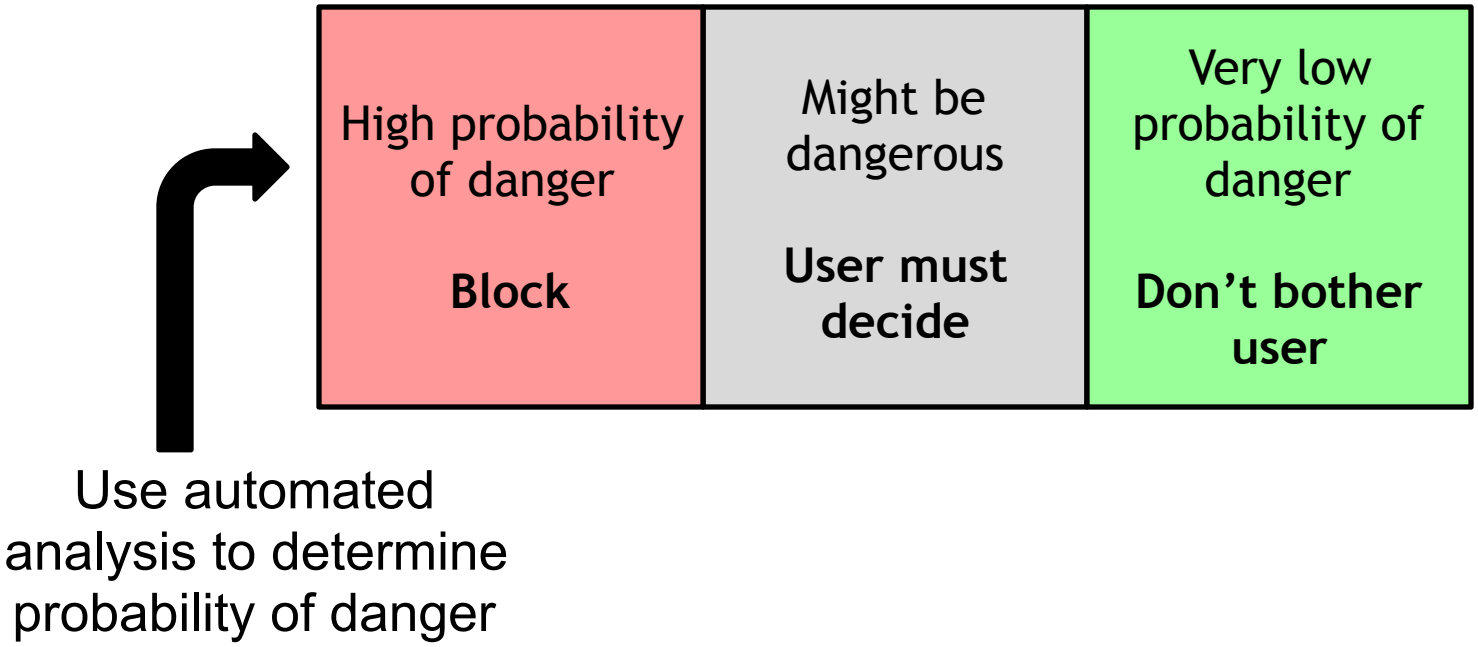
Might be dangerous

User must decide

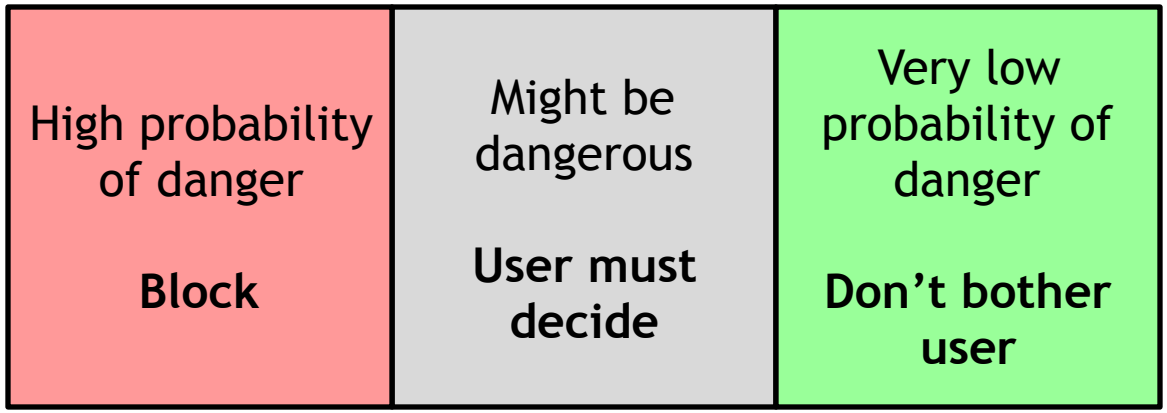
Automate and change tasks to reduce need for user involvement



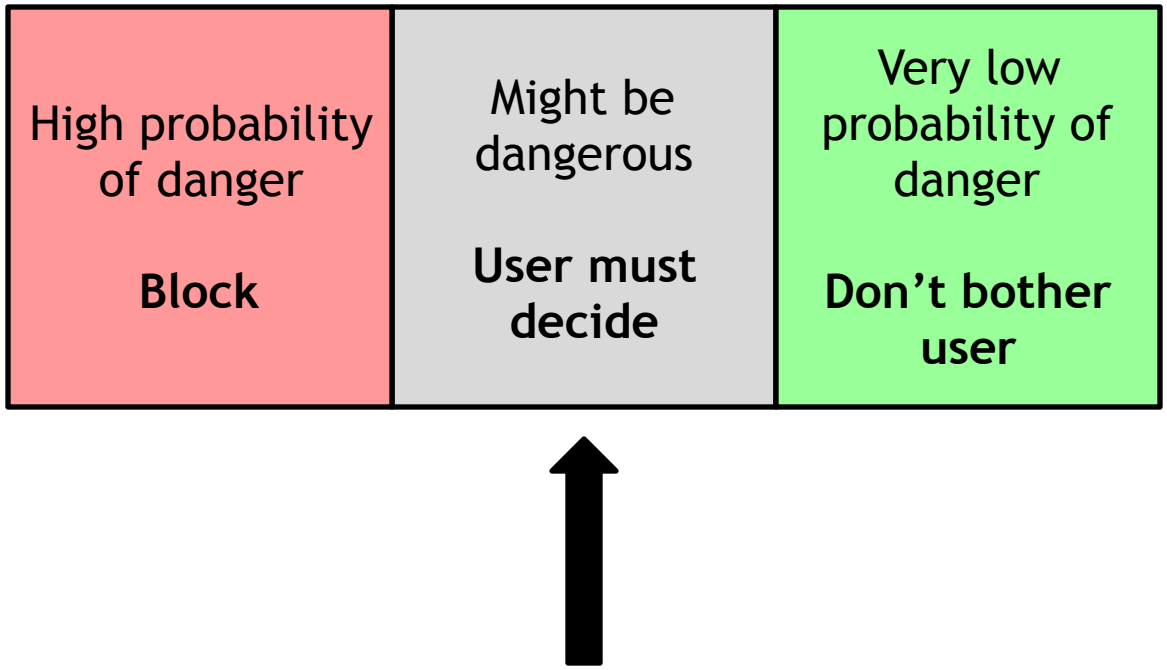
Automate and change tasks to reduce need for user involvement



Support user decision



Support user decision



Help user decide by asking question user is qualified to answer

Bad question

Your web browser thinks this is a phishing web site. Do you want to go there anyway?

Don't go there

Go there anyway

I don't know what a phishing site is.

I really want to go to this site.

Of course I will go there anyway!

Better question

You are trying to go to evilsite.com. Do you really want to go there or would you rather go to yourbank.com?

Go to yourbank.com

Go to evilsite.com

Of course I want to go to yourbank.com!


What to do about hazards?


Best solution: remove hazard


Next best: guard against hazard

If all else fails: warn

CAUTION

CAUTION

Cylab Usable Privacy and Security Laboratory

http://cups.cs.cmu.edu/

Carnegie Mellon