usable security: introduction

EECE 571B “Computer Security”

Konstantin Beznosov

human in the security loop

- security managers attribute about 60% of security breaches to human error (2006 Computing Technology Industry Association survey)
- SANS Top 20 Internet Security Vulnerabilities report began lists human vulnerabilities
- increasing security concerns
  - social engineering attacks
  - lack of compliance with organizational security policies
-

when humans are necessary

- knowledge difficult for a computer to reason about or process
  - recognizing faces in crowds
  - noticing other humans who are acting suspiciously
- knowledge about context
  - whether an email attachment is suspicious in a particular context
- make some security-related configuration decisions
- apply policies when
  - difficult to encode all of the nuances of a policy
  - program a computer to handle special cases
- a completely automated system might be too restrictive, inconvenient, expensive, or slow
- manipulate or protect physical components
  - insert a smartcard into a reader and remove it before walking away
- participating in authentication process

Security in the wild: user strategies for managing security as an everyday, practical problem

Dourish, P., Grinter, E., Delgado de la Flor, J., and Joseph, M., “Security in the wild: user strategies for managing security as an everyday, practical problem,” Personal Ubiquitous Computing v8, n6 (Nov. 2004), pp. 391-401

experience of security: **as a barrier**

"Security systems typically attempt to introduce barriers to action while HCI designers attempt to remove such barriers."

akin to a gate or a locked door

various threats become co-constructed as the common entities against which security protects

- security and spam are two aspects of the same problem
- imagine and seek unitary solutions
- so what?
  - solutions that solve only one problem could be rejected as "partial"
  - technology deployed to solve one problem can be interpreted as protection against others
  - expectation failures
  - mistaken assumptions
  - focus on one aspect of the problem blinding to others

experience of security: **online and offline**

- leakage of information between online and offline
  - inadvertent information disclosure online could create a threat offline
    - personal security: stalkers
- physical manifestation of their computing environment
  - networked printer troubleshooting

attitudes towards security

- frustration
  - younger participants more likely to report encountering situations in which security services proved problematic, hindering rather than helping their activities
    - circumvent security technologies in order to get their work done
    - talk of security in terms of its costs and benefits
    - security measures can interfere with the work
  - study of teen use of SMS (Grinter and Eldridge, 2003)
    - never turned their phones off
    - rarely used their password to log back onto the phone after a reboot
    - need to take their mobile phone to the nearest service center to get the password reset
    - frustration with missing out on SMS' and other activities without the phone
  - persistence of security in interrupting user in order to insist that something be done
    - security is either something unmentioned, or it is something to be dealt with suddenly and immediately
- pragmatism
  - use known insecure technologies where they felt that the risks were justified
- futility
  - reference to the unknown others (hackers, stalkers, etc.) who will "always be one step ahead"
  - always new attacks to be diverted
  - security lying not so much in technology as in vigilance
  - frustration: one is continually "running to stay in the same place"; "due diligence" in organizations

practice of security: **delegating security**

1. delegate to technology: SSL, SSH, switched Ethernet, etc.
   - least common way of delegation
     - if could turn a technically working security system into an individually workable solution
   - depends on visible presence of technology to be trusted
2. delegate to another individual: e.g., colleague, family member, roommate
   - for personally owned devices
   - “technical friend”grounded in a series of positive experiences
3. delegate to an organization
   - skills and especially the vigilance of the organization in which people place their trust
   - more trust may be accorded to external organizations
4. delegate to institutions
   - trust that certain types of institutions, would take appropriate security measures
   - impressions formed about institutions are carried over to online security

- temporal aspect
  - delegates were still invoked as the guarantor of security, even if they were not there any more
  - work practices of groups often “grow over” the underlying security, with no-one concerned

practice of security: **secure actions**

- institutional means to secure communications
  - signature file that states the legal and illegal uses of the contents of the message
    - mitigate the risks of information leaks by securing the consequences of those leaks by marking the messages
    - migration of email to a formal means of corporate communications
- “I took the actions you requested”
  - Using “cryptic” email was a easier to do than using a security tool to encrypt the information
- media switching as a security measure
  - from email to the telephone when the most sensitive of topics came up
  - teenagers switching from SMS to telephone for most confidential of conversations
  - why telephone?
    - less vulnerable medium than email
    - ephemeral
    - privacy and confidentiality
- security incorporated into working practices
  - legal staff use of the access control settings for shared directories as a means of communications
  - did not have to know specifically to whom they had to send the files (unlike email)

practice of security: **holistic security management**

physical arrangement of space: separating confidential data from interactions with visitors

- computer screen to point away from the first point of entry into the office
- sensitive paper documents by monitor but not for visitors
  - colored folders balance security and information access
- desk separating office into front (visitors) and back (documents) parts
  - social conventions prevent breaches
- examples: admin assistants to executives, managers
- relationship between online and offline security

practice of security: **managing identity**

- production of identity
  - conscious of presenting themselves online
    - maintain many virtual identities as a way of controlling their visibility
  - partial identities for controlling identifiability and track-ability

- interpretation of identity
  - individuals manage their own security but not always their own identity
    - executives and secretaries
    - mismatch between the e-mail address (bob@company.com) and its type
  - pressures on the mechanisms that allow people to control information disclosure
  - people act continually and simultaneously in multiple capacities
    - conventional “roles” fail to capture the fluid and especially the simultaneous nature of these capacities

reframing security (for ubiquitous computing)

- "what sorts of mathematical and technical guarantees can be made about the interaction between these components and channels?"
- "is this computer system secure enough for what I want to do now?"
- inherently implausible to specify, in advance of particular circumstances, what their security needs might be
  - needs arise only as a result of specific encounters between people, information, and activities.
- place security decision-making back within the context in which it makes sense as a practical matter

implications for design

- protection and sharing of information are two aspects of the same task
  - e.g., switching media from email to the telephone during a discussion or using cryptic email
  - should use the same mechanisms to share information as to protect it
- extent to which people are able to monitor and understand the potential consequences of their actions
  - e.g., installing a firewall and then running an unencrypted wireless network
  - visibility of system behavior on users' terms
  - security implications of the current configuration of technologies at their disposal
  - security highly visible, rather than transparent
    - visibility expression should fit users' activities and needs at the time
- security is a mutual achievement of multiple parties
  - scope of security is collaborative

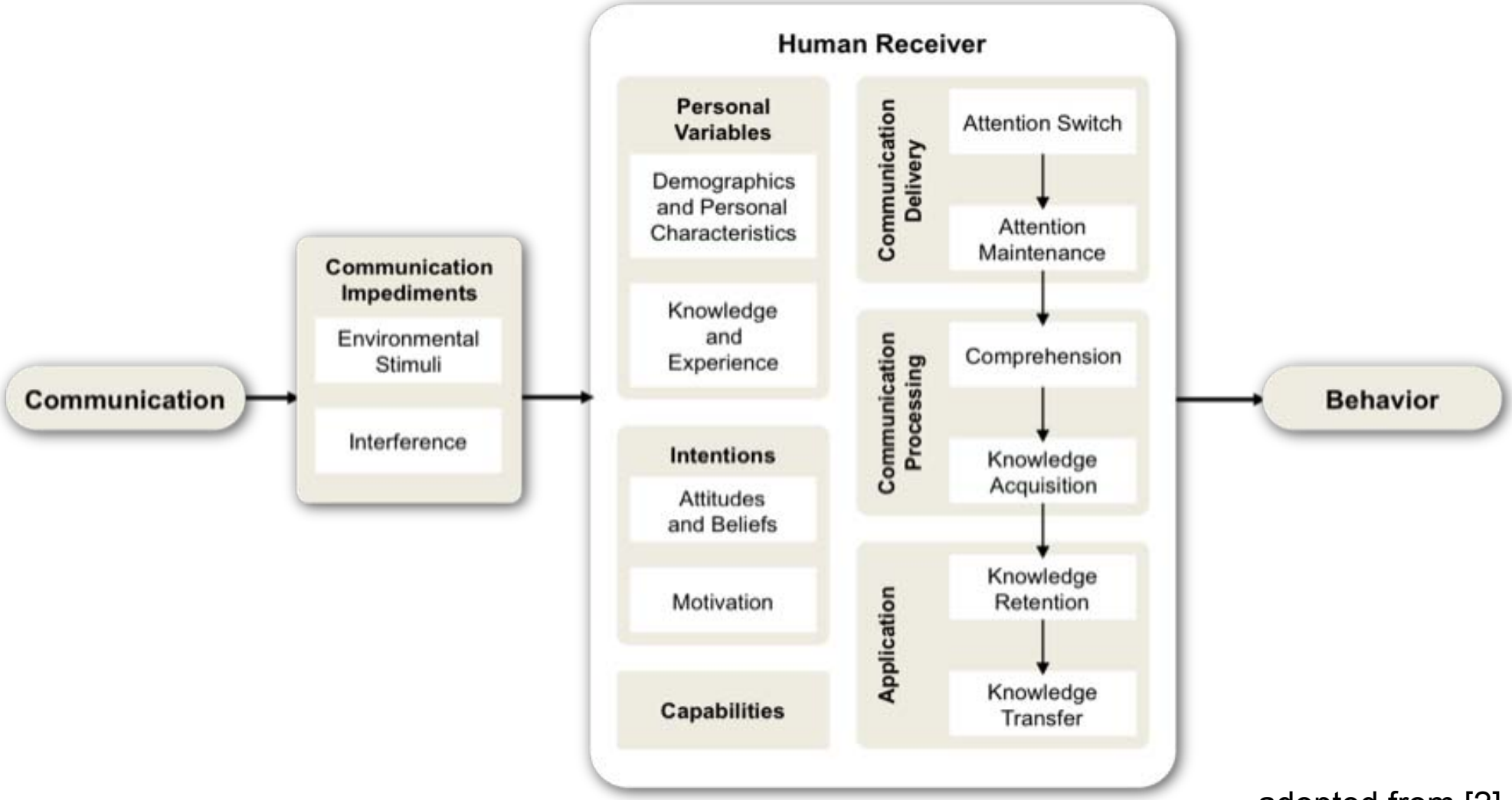
modelling humans in security

Lorrie Faith Cranor, 2008, “A framework for reasoning about the human in the loop,” In Proceedings of the 1st Conference on Usability, Psychology, and Security (UPSEC'08), Elizabeth Churchill and Rachna Dhamija (Eds.). USENIX Association, Berkeley, CA, USA, 15 pages.

human threats

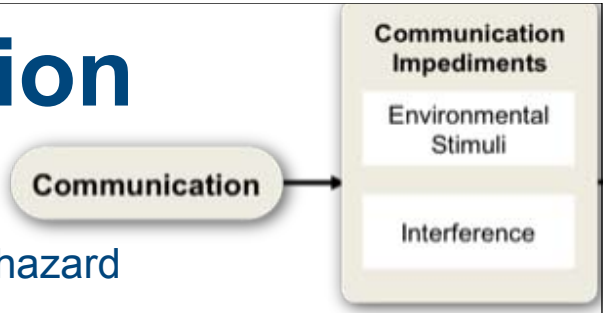
- adversaries
- non-malicious humans
  - don’t understand when or how to perform security-related tasks
  - unmotivated to perform security-related tasks or comply with security policies
  - not capable of making sound security decisions

human-in-the-loop security framework



adopted from [2]

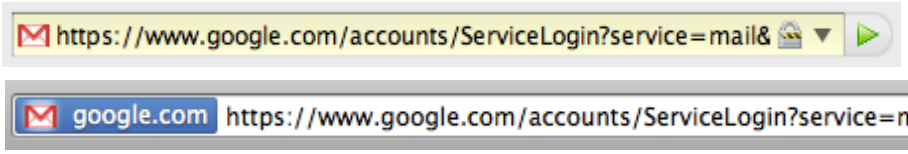
types of communication



- warnings alert users to take immediate action to avoid a hazard
  - active or passive, used only when impossible to protect user from a hazard
  - should: get user attention, provide clear instructions how to avoid the hazard
- notices inform users about characteristics of an entity or object
  - examples: privacy policies, SSL certificates
  - used by users to evaluate an entity and decide whether to interact or not
- status indicators inform users about system status information
  - examples: taskbar and menu bar indicators that show whether Bluetooth has been enabled or whether anti-virus software is up to date, file permissions
- training teach users about security threats and how to respond to them
  - examples: tutorials, games, instruction manuals, web sites, emails, seminars, courses, and videos
  - users learn concepts and procedures, remember what they learned, and recognize situations where they need to apply them
- policies: documents that inform users about system or organizational policies that they are expected to comply with
  - examples: password policies, information/document protection policies
  - users must recognize situations where the policy is applicable, understand how to apply the policy, and have the capability and motivation to comply.

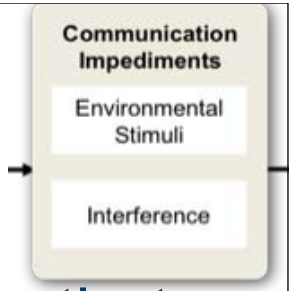
active vs. passive communications

- active -- interrupt the user's primary task and force them to pay attention
- passive -- available but easily ignored



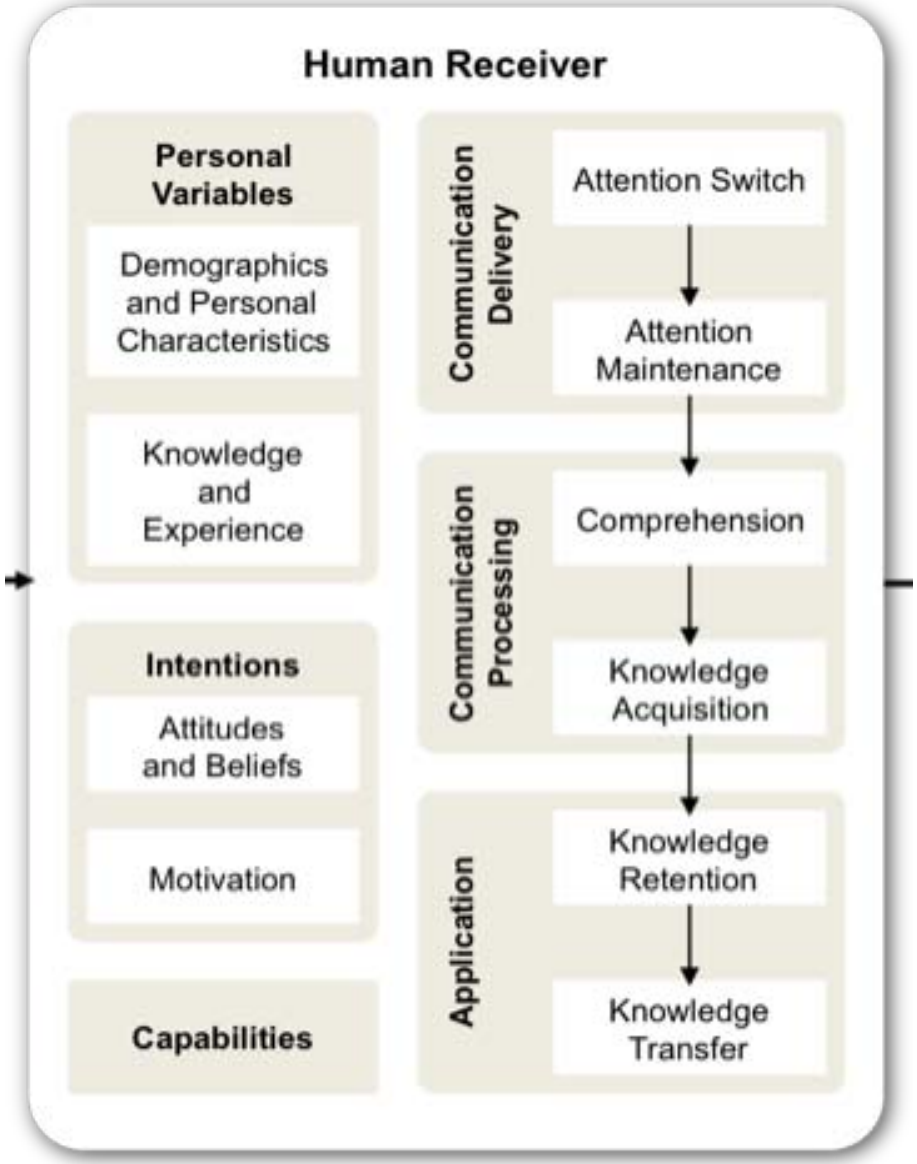
- design considerations
  - severity of the risks
  - need for user's action(s)
  - frequency

communication impediments



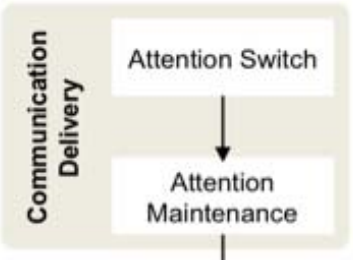
- environmental stimuli -- communications and activities that may divert the user's attention away from the security communication
  - examples: other communications, ambient light and noise, primary task
  - interplay between passivity of the communication and the environmental stimuli
- interference -- anything that may prevent a communication from being received as the sender intended
  - examples: malicious attackers, technology failures, or environmental stimuli that obscure the communication.

human receiver



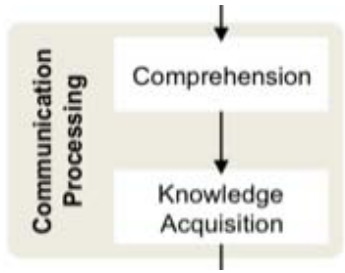
adopted from [2]

communication delivery



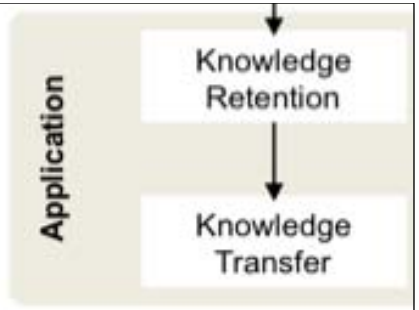
- attention switch -- the user has to notice the communication
- attention maintenance -- pay attention long enough to process the communication
  - examples: recognize an indicator, read/watch/listen tutorial/policy/warning
- impacted by
  - environmental stimuli
  - interference
  - communication characteristics
  - habituation -- the tendency for the impact of a stimulus to decrease over time as people become more accustomed to it
- most users don't notice security indicators in software they use regularly

communication processing



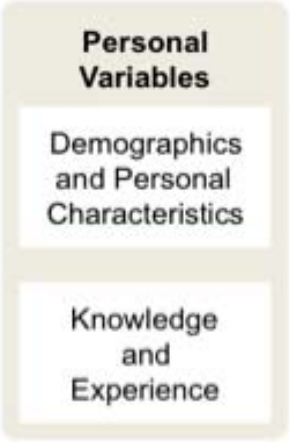
- comprehension --- ability to understand the communication
  - contributing factors: familiarity with indicator symbols, their similarity to related symbols, conceptual complexity, vocabulary and sentence structure
  - short, jargon-free sentences, use of familiar symbols, and unambiguous statements about risk
- knowledge acquisition --- ability to learn what to do in response to the communication
  - what specific steps to take to avoid the hazard?
  - unless users have received previous training they are unlikely to know what they are supposed to do when they see the warning
  - specific instructions on how to avoid the hazard
- challenges
  - difficult to write about computer security concepts without technical jargon
  - security-related concepts are difficult to represent clearly with icons.

application



- **knowledge retention** --- ability to remember the communication when a situation arises in which the user needs to apply it, and to recognize and recall the meaning of symbols or instructions
  - factors: frequency and familiarity of the communication, long-term memory abilities, and the level of interactivity of training activities.
- **knowledge transfer** --- ability to recognize situations where the communication is applicable and figure out how to apply it
  - factors: level of interactivity of training activities, the degree of similarity between training examples and situations where knowledge should be applied
  - may be unnecessary if there is no need to figure out on their own when a warning is applicable

personal variables



- **demographics and personal characteristics**: age, gender, culture, education, occupation, and disabilities.
  - Who these humans are likely to be and what their personal characteristics suggest about how they are likely to behave?
- **knowledge and experience**: education, occupation, and prior experience
- impact a user's ability to comprehend and apply communications, and their intention and capability to act

- example: experts
  - understand complicated instructions
  - second-guess security warnings and, perhaps erroneously, conclude that the situation is less risky than it actually is

intentions

- behavioral compliance models
- **attitudes and beliefs**
  - beliefs about the accuracy of the communication
  - whether the user should pay attention to the communication
  - user's ability to complete recommended actions successfully (self-efficacy)
  - whether recommended actions will be effective (response-efficacy)
  - how long it will take to complete recommended actions
  - user's general attitude towards the communication (trust, annoyance, etc.)
- **Motivation** --- the incentives users have to take the appropriate action and to do it carefully or properly
- relevant considerations
  - conflict with primary task & goals
  - security delays in the primary task
  - past experience with security communications (FPs)
  - organizational incentives

motivating users in security tasks

- easy to perform
- minimize disruption of user's workflow
- taught to appreciate the consequences of security failures
- address cultural norms resulting in disincentives
- rewards and punishments in organizations

capabilities

- specific knowledge, or cognitive or physical skills
- special software or devices required in specific cases
- example
  - remembering random-looking strings for password

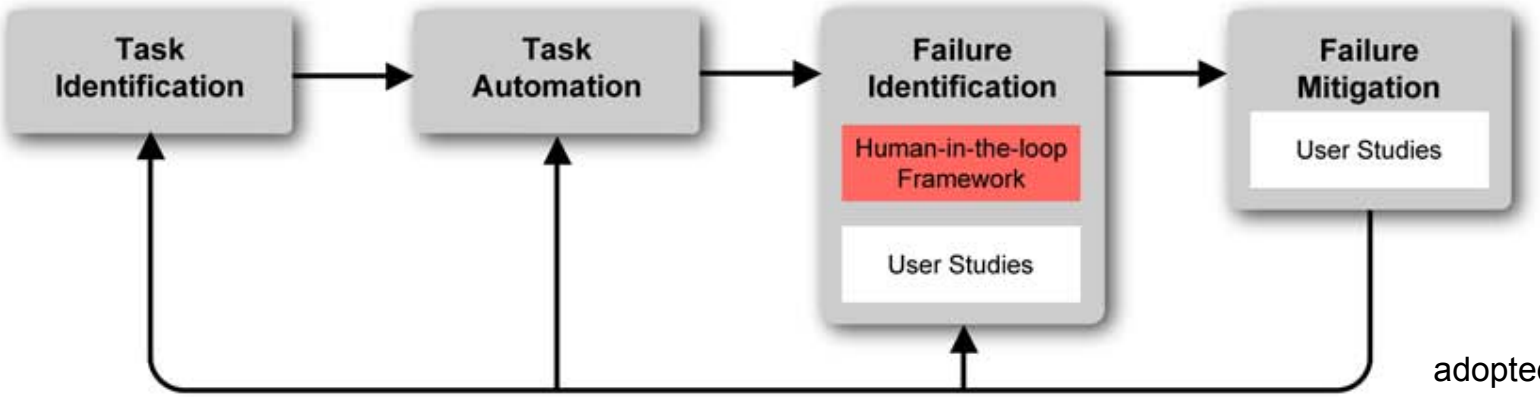
behavior

- Gulf of Execution
  - example: updating AV
  - security communications should include clear instructions about how to execute the desired actions
  - proper use should be readily apparent
- Gulf of Evaluation
  - examples: state of the personal firewall, file permissions, inserting smart card into a reader
  - relevant feedback for determining the outcome of the actions

designing for better behavior

- types of error (Generic Error-Modeling System)
  - **mistake** -- action plan that won't achieve the desired goal
    - example: trusting an attachment based on the sender
  - **lapse** -- forgetting to perform a planned action
    - example: skipping a step
  - **slip** -- perform an action incorrectly
    - examples: press a wrong button, select a wrong menu item
- design considerations
  - minimize the number of steps necessary to complete the task
  - provide cues to guide users through the sequence of steps and prevent lapses
  - locate the necessary controls where they are accessible and arrange and label them so that they will not be mistaken for one another
  - consider whether an attacker might be able to exploit predictable user behavior,
    - if so, find ways to encourage less predictable behavior or prevent users from behaving in ways that fit known patterns

applying the framework



adopted from [2]

- **identify** all of the points where the system relies on humans to perform security-critical functions
- find ways to (partially) **automate** some of the security-critical human tasks
- **identify** potential **failure** modes for the remaining security- critical human tasks
- find ways to **prevent failures** by determining how humans might be better supported in performing these tasks

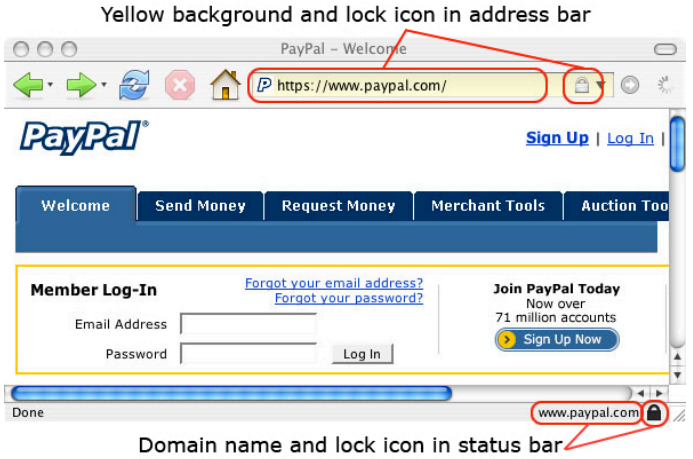
Why Phishing Works

Rachna Dhamija, J. D. Tygar, and Marti Hearst, "Why phishing works," In Proceedings of the SIGCHI conference on Human Factors in computing systems (CHI '06), ACM, pp. 581-590.

analysis of past phishing attacks

- lack of knowledge
  - lack of computer system knowledge
    - www.ebay-members-security.com and www.ebay.com
    - e-mail headers
  - lack of knowledge of security and security indicators
    - padlock & HTTPS

    - browser chrome vs. web page
    - SSL cert verification
- visual deception
  - visually deceptive text: www.paypai.com, www.paypa1.com
    - Unicode characters in domain names
  - images masking underlying text
  - images mimicking windows
  - windows masking underlying windows
  - deceptive look and feel
- bounded attention
  - lack of attention to security indicators
  - lack of attention to the absence of security indicators



adopted from [3]

study methodology

- task
  - presented 19 web sites of financial and e-com. companies
  - task: identify legitimate and fraudulent sites & describe the reasoning behind the decisions
  - primed to look for spoofs
  - 9 representative phishing sites from 200 unique
  - created 3 advanced phishing sites
  - +1 site with self signed cert

"Imagine that you receive an email message that asks you to click on one of the following links. Imagine that you decide to click on the link to see if it is a legitimate web-site or a "spoof" (a fraudulent copy of that website)."

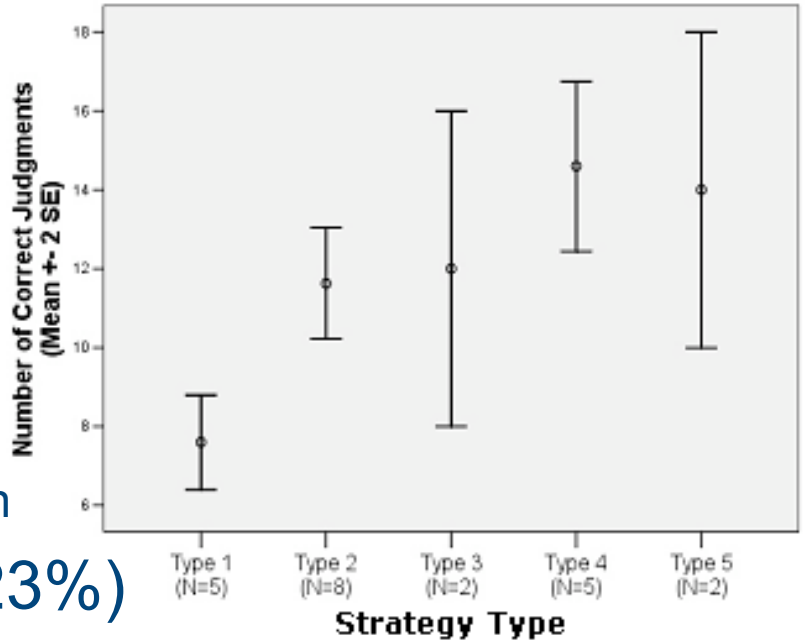
- participants
  - 10 male + 12 female, 18-56 y/o, average 29.9. students and staff
- experiments
  - within-subjects: every participant saw all websites in random order
  - thinking aloud
  - 1-5 Likert scale for confidence of the judgement
  - semi-structured interview about website and phishing experience, SSL certs
  - debriefing

results: stats

- correctness
  - 6-18, mean 11.6
- no statistically significant correlation between age/sex/education/usage/browser/OS/previous_use and correctness

results: strategies

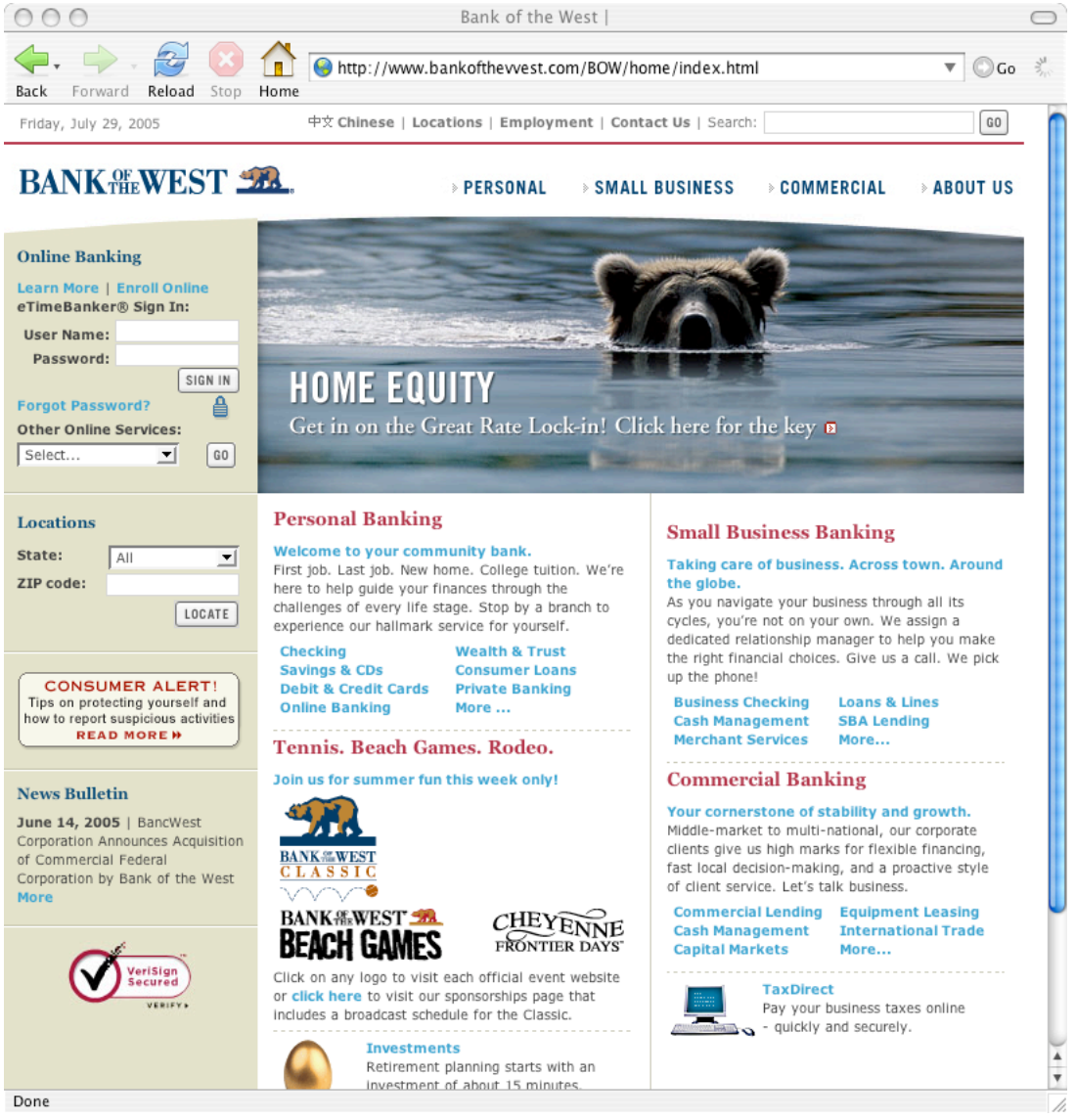
1. security indicators in website content only (23%)
   - logos, layout and graphic design, presence of functioning links and images, types of information presented, language, and accuracy of information
   - “I never look at the letters and numbers up there [in the address bar]. I’m not sure what they are supposed to say”
   - lowest scores
2. #1 + domain name only (36%)
   - address bar and page content
   - distinguish host names from IP addresses
   - no HTTPS indicators
3. #2 + HTTPS (9%)
   - did not notice or look for the SSL padlock icon
4. #3 + padlock icon in the chrome (23%)
   - more credence to padlock in the content
5. #4 + certs (9%)



adopted from [3]

fooled most participants

- 20 misjudged
- 17 -- content
  - cute, level of detail, no much asked, video of the bear
- link to pop-up from Verisign
- Chinese version
  - “fake website could never be this good”
- correctness of the URL
  - only one detected



exit interview

- knowledge and experience with phishing
- knowledge and use of padlock icon and HTTPs
- knowledge and use of Firefox SSL indicators
- knowledge and use of certificates
- new understanding of users
  - lack of knowledge of web fraud
  - erroneous security knowledge

conclusions

- a usable design must take into account what humans do well and what they do not do well.
- it is not sufficient for security indicators to appear only under trusted conditions,
- it is equally, if not more, important to alert users to the untrusted state.

credits

1. Dourish, P., Grinter, E., Delgado de la Flor, J., and Joseph, M. 2004. Security in the wild: user strategies for managing security as an everyday, practical problem. Personal Ubiquitous Computing 8, 6 (Nov. 2004), 391-401.
2. L. F. Cranor, 2008, “A framework for reasoning about the human in the loop,” In Proceedings of the 1st Conference on Usability, Psychology, and Security (UPSEC'08), E. Churchill and R. Dhamija (Eds.). USENIX Association, Berkeley, CA, USA, 15 pages.
3. Rachna Dhamija, J. D. Tygar, and Marti Hearst, “Why phishing works,” In Proceedings of the SIGCHI conference on Human Factors in computing systems (CHI ’06), ACM, pp. 581-590.