Beyond Usable Security: A Matter of Trust An Issue of Risk Management

L. Jean Camp

www.ljean.net

economics of infosec & econ: www.infosecon.net

Objectives

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

Give end users security controls they *WANT* to enable them to *CONTROL* their own dynamic, pervasive computing environments.

- **Risks in process, technology, privacy, security**

Usability on the Surface

Does What we Built Work?

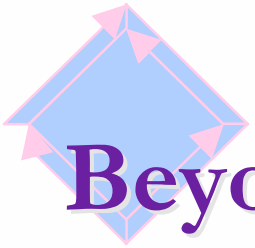
- Toolbars, do people pay attention?
- Signed Email, tor
  - can you install it
  - can you use it
  - can you detect it?
- Seals
  - A triumph of style over substance
- SSL
  - what is that funny lock and what does it mean?
  - economics is NOT the same as business

Dominant Trust Communication

+

=

ADDED VALUE
& CONSUMER TRUST



Beyond Interface Deep

Security people may want
- surveillance as prevention
- information more than privacy provision

Not built for the way people act
- would that be a 7.2 privacy preference?
- do you trust more or les than 17%
- we'll helpfully stop you from lying in any circumstance

With appropriate risk communication, signaling, etc
- examination of how humans evaluate risk
- computer security -- decision-making und er uncertainty

Security and Processes

Business processes

Organizational processes

Security aligned with users and processes

- to the extent that this is possible

Users subvert security when it

- violates privacy
- provides nonrepudiation for all actions (blog, IM)
- prevents use of media
- or it is simply in the way
- human risk behaviours are fairly consistent
  - trust pictures of faces, discount risks

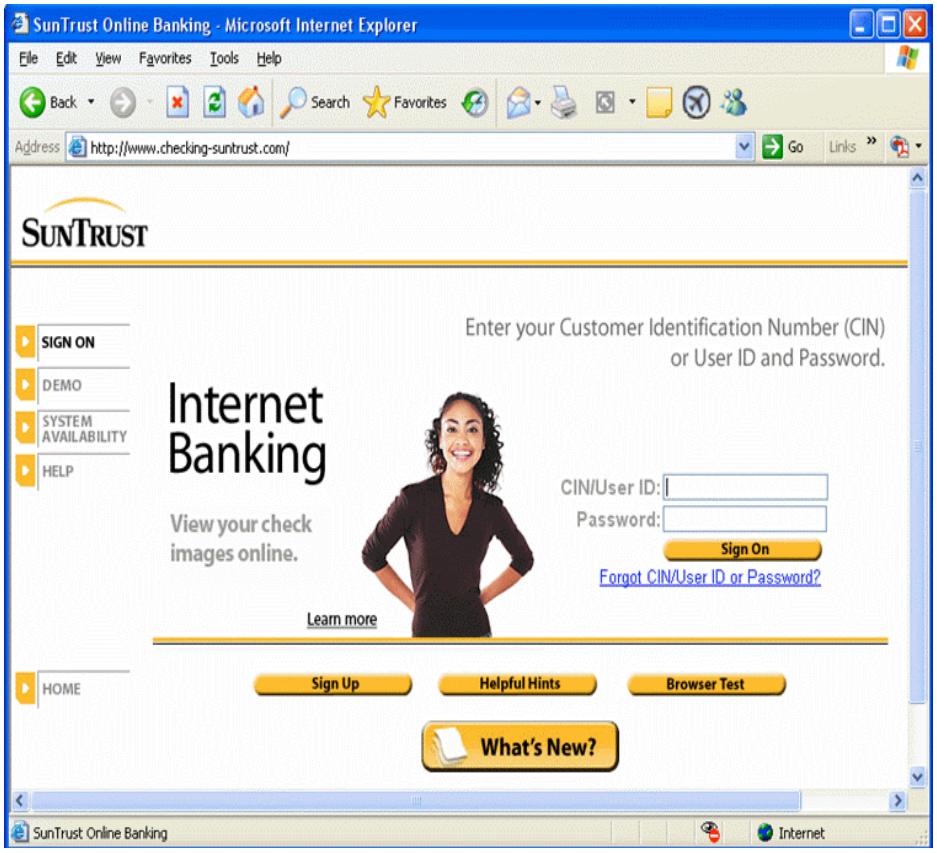
Trust and Context

vs.

Resource Verification

Resources are often fairly easy to identify as "good" or "bad" in physical realms

Trust and Context



Fewer signals in economic terms
Less usable in design terms

Standing on the Toenails of Giants?

- Other disciplines and methods
- Management and marketing
  - trust indicators
  - advanced survey methods
- Organizational theory
  - benevolence
  - competence
  - trust, confidence
- Philosophy
  - trust, privacy as cultural
  - conceptual arguments of trust behaviors
- Social Science
  - survey expertise
  - qualitative methods
  - trust behaviors
  - payment as dis-incentive

More central Disciplines

Economics

- behavioral
  - adversaries prefer to limit conflict scope
  - credible commitment
  - the advantage of closing off options
  - tipping
  - small incentives

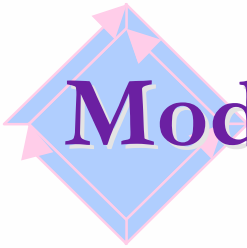
- rational
  - **CENTRALIZED PLANNED ECONOMIES DON'T WORK**
  - **distributed mechanisms, coordination at the low level**

Usability, HCI & Design

- usability studies
- involving designers at an earlier level
- what do users understand?, from yesterday:
  - wireless: *wide spread deployment by non-experts*
  - *botnets, e.g., home users, major tier 1 threat*
  - what can the network do for me today
- Usability in Depth
  - Interface
  - Interactions
  - Incentives
    - is it rational to design for humans as if they were machines?
  - Social context
  - Human and Organizational requirements

Ex. 1: Net Trust Building from Theory

Creating Social Context



Model and Theory

Simulation suggests

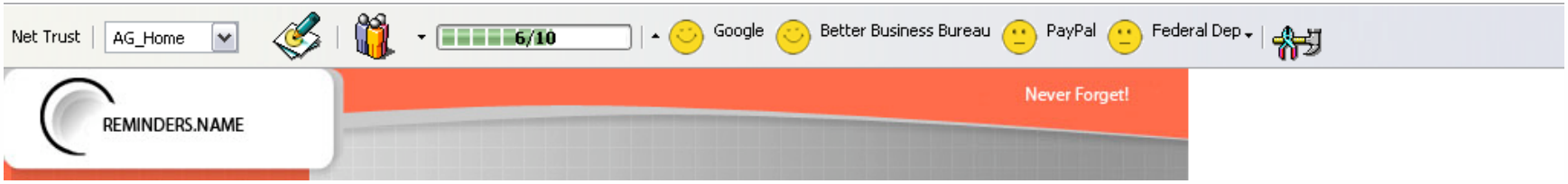
- under basic conditions, networked actors are very good at rejecting bad resources without avoiding good resources.
- a mechanism is needed to seed the network with good information.
- the network amplifies the power of individual detection abilities.
- temporal signatures of bad resources (phishing) can be detected.

BUT: non-savvy actors cannot achieve perfect (95%+) results without exogenous information sources.

beyond trusted third parties

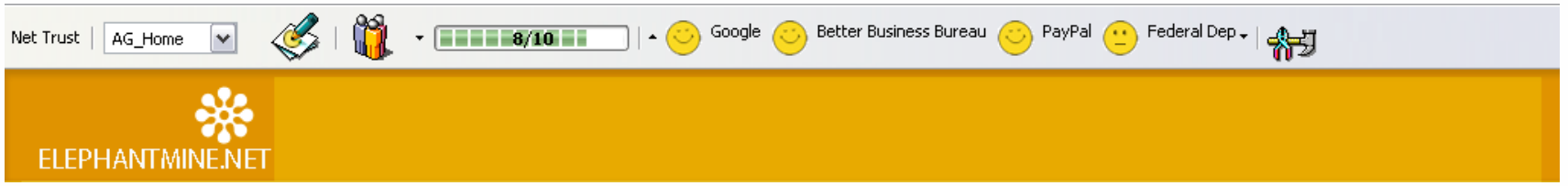
- giving users their own histories
  - » Verisign has not approved this certification
  - » This is a new site you have never visited
  - » This site has no domain name, just a IP address
    - in a more meaningful manner

First Results: Reminders.name



Without Toolbar: 60% say they do not trust the first site With Toolbar: 42% say they do not trust the second site (n=26)

Second: Elephantmine.net



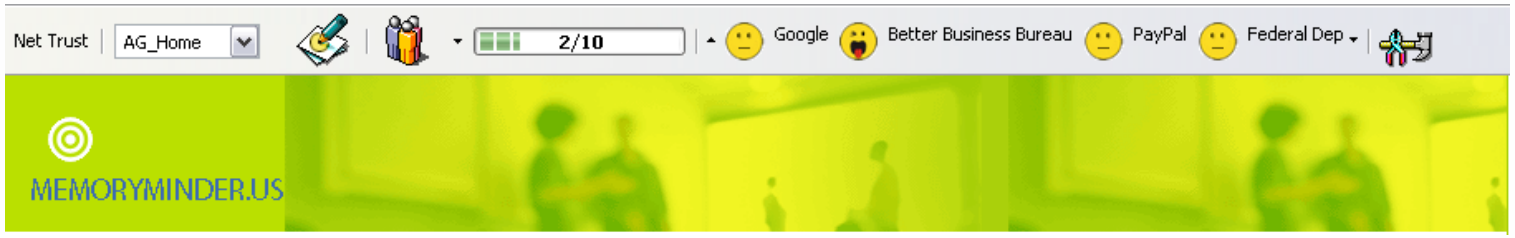
Without Toolbar: 52% say they do not trust this site

With Toolbar: 24% say they do not trust this site

Third: MemoryMinders.us

Without Toolbar: 80% say they do not trust this site

With Toolbar: 76% say they do not trust this site



Mixed signals produce statistically insignificant result.

Example 2: Design for Humans

- Hypotheses about human trust behavior developed from social science
- Compared with implicit assumptions in common technical mechanisms
- Test computer-human trust behaviors
- Two "Betrayal" Types
  - One group faced a *technical* betrayal
    - Another person's data is displayed
    - "John Q. Wilson"
    - DoB, Credit Card Number, social network data
  - One group faced a *moral* betrayal
    - Change in privacy policy announced
    - Collection of third party information correlated with compiled data
      - very common policy
      - eBay, Face Book, mySpace

Three Step Process

- Users introduced to first site
  - Sites in the same order
- Users experience betrayal
  - Half the users have technical failure
  - Half had privacy change
  - Both sets of users experience a failure upon departure of first site
- Then users go to second site

Findings: Differentiation

Users respond to first site betrayal with significant change in behavior wrt second site

- users had on average seven years experience with Internet
- computer experience not at all significant
- second site not seen as “new” entity

Cannot support the hypothesis that users differentiate

- users do not enter each transaction with a new calculation of risk

Findings: Betrayal Type

Stronger reaction to privacy change

- Yet technical failure indicated an inability to protect privacy
- People are not rational in risk behavior
- So is designing for rational people irrational?

	"Malevolence"		"Incompetence"	
	Privacy Before	Privacy After	Security Before	Security After
Your IM Buddy List	22%	09% p<.001	16%	13% p<.001
Coworkers' Names & Contact	44%	31% p<.01	42%	52%
Friends' Names & Contact	53%	34% p<.001	65%	68%

Example 3: DDos

Goals:

- Stop abuse of resources from the edges

Solutions

- identity systems
  - » perfect knowledge & perfect enforcement across jurisdictions
  - » or increase of cost in terms of risks
- economics
  - » proof of work
  - » incentive-aware protocols
- lock-down
  - » rate limit end points
  - » MS detects and repairs zombies
- policy
  - » make ISPs or end user liable for zombie behavior

Events & resources

- OPEN
  - » DIMACS on Economics of Security
    - http://dimacs.rutgers.edu/Workshops/InformationSecurity/
  - » Financial Cryptography
    - http://www.ifca.ai/fc07
- PAST
  - » Workshop on Economics of Information Security
    - http://www.infosecon.net
  - » Past workshops, bibliography, future calls
    - http://www.infosecon.net/workshop/bilbiography.php

Usability

OPEN

- Usable Security
- http://www.ifca.ai/

PAST

- Symposium on Usable Privacy and Security
  - » cups.cs.cmu.edu/soups
- CHI
  - » has had affiliated workshops on security, measuring privacy
    - some questionable security assumptions
- Oakland
  - » accepted usability papers
    - some questionable research methods

My Questions

Beyond simple usability

- output so programmers can read it; making formal tools usable by programmers; improving usability for programmers as well as end users

Research teams

- methods, disciplines, problem scale

Research agendas

- identification of challenges beyond phishing
- emerging risks
  - identity assumptions
  - pervasive systems
  - detailed data aggregation

Venues and outreach

- new venues. reaching a broader audience, connecting with other communities