Usable Security and Privacy
Class notes
February 21, 2006

Trust and semantic attacks I

Presented by Jason Chalecki

Not much trust in the online community

- Consumer Report Webwatch survey of 2002
    - For ecommerce sites
        - Only 29% always trust
- Trust is an online problem, other sections have higher ratings of trust

Issues of losing trust

- Napster
    - Poor performance ed to the lost of trust. Use of program stopped.
- Other examples – Jakob Nielsen (Alertbox 1999)
    - Did not sign up for the eFax service because of reluctance to be "locked in" to service
- Amazon.com
    - Favorable reviews paid for = loss of trust in system and recommendations
    - But, Amazon instituted a policy to refund purchases if they were made based on a faulty recommendation

Questions: How does reputation affect the ability of users to trust the company (i.e. a big name corporation vs a smaller less recognized company)?

- Steve feels like there is a different between what people do and what they say they do.
- Mike Reiter: Trust and satisfaction equated?

Fundamental Questions:

- How to represent trust in interactions and interfaces?
- What are the building blocks?
- Fallibility of trust
    - Without risk – no need for trust
- How to transform trust-based decisions into security decisions while maintaining the meaning of trust–based decisions
    - What does this mean?
        - When people made decisions, many factors come into play. It is difficult to get those interactions into the computer. It is difficult to allow the computer to do those interactions for the people.
        - Example: Open attachment?
            - Consequence – security decision
            - Personal contacts/relationship known by person and not computer
            -

Definitions given in class

- Kami – likes pulling out risk

- Kami's sister forwarded the "Bill Gates pay-for-ever email forwarded" chain letter
    - While her sister had a lack of trust, she did not see the risk in forwarding the email (i.e. virus in email)
- Jason – disagrees w/ the term "assured"
- When there's an expectation, is there always risk?

Layers of trust:
- Dispositional trust – Psychological disposition or personality train to be trusting
- Learned trust – Learned through experience
- Situational trust – Basic tendencies adjusted in response to situational cues

Are there layers or not?
- Yes to dispositional (Rachel)
- Overlap, but not layers (Mike)
- Yes, with overlapping layers (PK)
- Layers in time (Jason)

Granularity of trust
- I trust you
- I trust you ... this much
- I trust you this much to do this thing

Another Axis
- Hard trust
    - Technology (i.e. encryption)
- Soft
    - Social

People can be accountable if they betray your trust. Technology is not accountable.

How is credibility different than trust?

Credibility is believability
Trust is dependability

Trust may not be an issue if you find the information credible or not.
- Medical info: Can I depend on this info:
    - Was this really written by a doctor?

Whether or not you decide to depend on it, you still need to decide it is credible.
You may decide it is credible but decide not to depend on the info.

4 types of credibility
- presumed credibility (Dispositional trust)
    - based on general assumptions
- reputed credibility (situational? trust)
    - 3rd party reports

- surface credibility (situational)
    - based on inspection
- experienced credibility (Learned trust)
    - based on one's own experience

Trust a component of credibility

How doe the types of credibility relate to the layers of trust?

Judgments of credibility
Prominence (experienced)

Interpretation (presumed and experience)

How does Time play a factor?
- Initial trust
- Interactions
- Long-term trusted relationship

Trust industry – Trust models
1. Trustworthiness
2. Bhattacherjee's model
    a. Willingness to transaction even w/o trust
3. Lee, Kim & Moon's Model
    a. Views reflected by the community at large
    b. Less complexities = increase in transaction cost
    c. Large number of competitors also increases transaction cost

What is specificity?
– It is the inability of customers to transfer the skills/knowledge/value from one store to another store.

There was a recent book looking at how the number of competitors for things increases transaction costs (experiment w/ cereals) - *Paradox of Choice*

A problem not addressed – actually studying what people actually do (vs. what they say they do)

Corritor's Model
- Perceptions are not objective
- Ease of Use is a crucial building block

Egger's Mode
McKnight's Model
- Diff b/x intensions and actual behavior
- Made into a big list of questions

Riegelsberger's Model

Models Comparison

- Modes have been operationalized as questionnaires

Components of trust

- Ability
- Integrity
- Benevolence

Many factors affect trust

What's important is what trust enables you to do. It, alone, is not the important aspect.

Trust Design Guidelines

Stanford Guidelines for Web Credibility

Restaurants raising money for schools? - Giving site connection to the physical world
Making it part of the virtual community

Jakob Nielsen's Guidelines

- Design quality
- Up-front disclosure
- Comprehensive, correct, and current
- Connected to the rest of the web

Keep your information current

Guidelines comparison

- Professional appearance and ease of use are important
- Be correct and verifiable
- Be a part of a larger community

Group activity

- Scenarios
- Each group has 2 different scenarios where each group analyzes the risk, and how these risks can be mitigated.

An online electronic store is selling a large HDTV. The brand is an unfamiliar one, and cheaper than the name brands. Shipping is free with the first purchase. It has all the features you want and the store accepts all major credit cards.

Risks:

- Not a real store. Takes your money and disappears
- No brand reputation, no reviews of products.
- No security of the site – credit card theft/loss
- Unintentional security problems due to new site
- Might sell your information

Mitigate

- Privacy policy
- Check w/ BBB online
- Verify company information
- Check to see if the company is an actual registered company
- Check for comments on the web or forums
- Examine website

Heath care scenario:

Risks:

- Incorrect diagnosis
- Bad recommendations
- Prevent from going to a real doctor

Mitigate

- Check other sites (that are credible)