Trust: A Collision of Paradigms

As Presented at Financial Cryptography 2001

Grand Cayman, February 19

L. Jean Camp, Catherine McGrath, Helen Nissenbaum

Human and Computer Trust

- **Trust is approached differently by different disciplines**
  - **Social sciences**
    - **Experiments designed to evaluate how people extend trust**
    - **Game theory**
    - **Common assumption: information exposure == trust**
  - **Philosophy**
    - **Macro approach**
    - **Examine societies and cultural practices**
  - **Computer Security**
    - **Build devices to enable trust**

An Interdisciplinary Approach

- Informed by philosophy
- Examine social science theory
  - Developed three hypotheses
- Apply to computer security
- Search for inconsistencies between the disciplines

Philosophy Suggests

- **Trust is necessary to simplify life**
  - **People have an innate desire or need to trust**
  - **People will default to extending trust**

Research on Humans Suggest...

- Humans may not differentiate between machines
- Humans become more trusting of ‘the network’
- Humans begin with too much trust for computers
  - Confirmed by philosophical macro observation
  - Confirmed by computer security incidents
    - E-mail based
      - Scams
      - Viruses
      - Hoaxes

Three Hypotheses

- **Do humans respond differently to human or computer "betrayals" in terms of forgiveness?**
- **People interacting with a computer do not distinguish between computers as individuals but rather respond to their experience with "computers”**
- **The tendency to differentiate between remote machines increases with computer experience**

So What?

H1: Response to Failure

- **Do humans respond differently to human or computer "betrayals" in terms of forgiveness?**
  - **Attacks which are viewed as failures as 'ignored' or forgiven**
  - **Technical failures as seen as accidents rather than design decisions**
    - **May explain why people tolerate repeated security failures**
  - **May inform the balance between false positives and negatives in intrusion detection**
    - **Rarely identified malicious behavior taken more seriously**
    - **Technical failures easily forgiven**

H2: Individiation

- **People interacting with a computer do not distinguish between computers as individuals but rather respond to their experience with "computers”**
  - **People become more trusting**
  - **People differentiate less**
  - **Do people learn to differentiate or trust**

H3: Differentiation

- **The tendency to differentiate between remote machines decreases with computer experience**
  - **Explicit implication of second hypothesis**
  - **Will either confirm or undermine the second hypothesis**

If Hypotheses are Correct

- **Users may bad security managers**
  - **PGP, P3P,….**
- **Security should necessarily be a default**
- **Does end-to-end security maximize autonomy without end-to-end human abilities and tendencies?**
- **At the least security mechanisms should be designed to address hypotheses**

Computer security is built for machines

- **Passwords**
  - **Humans are a bad source of entropy**
- **SSL**
  - **Two categories: secure and not secure**
  - **Does not encourage differentiation**
  - **Every site should include a unique graphic with the lock**
  - **Computer security should seek to differentiate machines**

Privacy standards are built for machines

- **P3P assumes**
  - **All merchants trustworthy w.r.t. their own policies**
  - **Assumes increasingly sophisticated user**
  - **One standard for all transactions**
- **PGP**
  - **Monotonic increase in trust**
  - **No reset**
  - **No decrease in rate of trust extension**
    - **To compensate for increasing trust**
  - **No global or local reset**
    - **E.g. change in status**

Key revocation is built for Machines

- CRL tend to be single level
- Different levels of key revocation are needed
  - Falsified initial credential
    - All past transactions suspect
  - Change in status
    - Future transactions prohibited
  - Refusal of renewal
    - Current systems adequate
- CRL should reflect the entire systems in which they work, including the social system

WHAT TO CONCLUDE?

Computer security must be designed with social science in mind

- OR -

Assuming the human will act like the computer is the core design problem, remove assumptions about humans

Hopes for Future Research

- **Test the hypotheses**
  - **Using traditional social science practices**
  - **Evaluate data for different cultural setting**
    - **Start with US (MA then S. CA.) then UK, India due to language similarities**
- **Examine computer security mechanisms**
  - **How to minimize assumptions about human behavior**
    - **End to end enabling autonomy vs. limiting risk exposure**
    - **Not unlike a timeless government question?**