

# Burning Your Security At Three Ends



Security, Privacy and Trust  
In the Age of Disclosure

Steven P. Crain  
Georgia Institute of Technology

April 17, 2008

# Outline

- Definitions: Security; Trust; Privacy
- Security Theory: A A A
- A A A Case Studies
- What is Consuming Security?
  - Enhancing Security
  - Enhancing Profit
  - Enhancing Community
- Appropriate Solutions

# Definitions

- Security

# Definitions

- **Security**
  - Controls to limit risk that “stuff” will be stolen, damaged or used without permission.

Stuff: You, your family, belongings, information, creative works, activities, . . . .

# Definitions

- **Security**
  - Controls to limit risk that “stuff” will be stolen, damaged or used without permission.
- **Trust**

Stuff: You, your family, belongings, information, creative works, activities, . . . .

# Definitions

- **Security**
  - Controls to limit risk that “stuff” will be stolen, damaged or used without permission.
- **Trust**
  - Belief that the benefit of allowing someone access to your “stuff” is greater than the risk they will misuse it.

Stuff: You, your family, belongings, information, creative works, activities, . . . .

# Definitions

- **Security**
  - Controls to limit risk that “stuff” will be stolen, damaged or used without permission.
- **Trust**
  - Belief that the benefit of allowing someone access to your “stuff” is greater than the risk they will misuse it.
- **Privacy**

Stuff: You, your family, belongings, information, creative works, activities, . . . .

# Definitions

- **Security**
  - Controls to limit risk that “stuff” will be stolen, damaged or used without permission.
- **Trust**
  - Belief that the benefit of allowing someone access to your “stuff” is greater than the risk they will misuse it.
- **Privacy**
  - The ability to limit what others know about your “stuff.”

Stuff: You, your family, belongings, information, creative works, activities, . . . .

# Security Theory: A A A

- **Authentication**
  - How you identify who someone is.
    - private information
    - shared secret
    - difficult to forge features
    - independent confirmation
    - zero-knowledge proof
- **Authorization**
  - What someone is trusted to do.
- **Accounting**
  - Records and other safeguards to ensure the authorization is not abused.

# Outline

- Definitions: Security; Trust; Privacy
- Security Theory: A A A
- A A A Case Studies
- What is Consuming Security?
  - Enhancing Security
  - Enhancing Profit
  - Enhancing Community
- Appropriate Solutions

# A A A Case Study: Personal Acquaintance

- Authentication
  - As we interact with someone, we remember what they look like, how they sound, how they act, . . . .
  - We use that information to identify people.
- Authorization
  - We trust people based on:
    - Our experience of the person.
    - What trusted people have told us about the person.
    - Our experience of other people who seem similar.
- Accounting
  - Rarely applied in personal relationships, because it communicates mistrust.
  - Examples: prenuptial agreements; gossip.

# A A A Case Study: Banking

- Authentication
  - Liability for mistakes makes banks cautious.
    - Private information
    - Government documents
    - Signature
- Authorization
  - Each person is only authorized to access their own money.
  - Notarization
- Accounting
  - Detailed record keeping of each transaction.
  - Archived video.

# AAA Case Study: Websites

- Authentication
  - Care used depends on website risks.
    - Simple identity claims
    - Ability to receive email
    - Password
    - Cookie
    - IP Address
    - Access to bank account, credit card
- Authorization
  - Usually fixed by website policy.
  - May be influenced by cookies from 3<sup>rd</sup> parties.
- Accounting
  - Typically based on web log files.
  - Intrusion detection systems.

# Outline

- Definitions: Security; Trust; Privacy
- Security Theory: A A A
- A A A Case Studies
- What is Consuming Security?
  - Enhancing Security
  - Enhancing Profit
  - Enhancing Community
- Appropriate Solutions

# Consuming Security by Enhancing Security

## ➤ Causes:

- Large rise in fraud
- Sites needing increased security
- Sites wanting to look like they have great security
- Increased logging required by VISA and SOX.

## ➤ Results:

- Greatly increased use of private information for authorization.
- That is, greatly increased disclosure of private information.
- Very analogous to energy crisis.
- More information collected increases risk of improper disclosure.

# Consuming Security by Enhancing Profit

- Information is of tremendous value to marketers.
- Traditional websites are doing more to mine existing logs.
- 3<sup>rd</sup> party cookies to identify anonymous users based on interactions with affiliated sites.
- Move to web-based applications.
- Inappropriate access and use of private information for profit.

# Consuming Security by Enhancing Community

- Privacy means that we decide what private information we want to disclose.
- To enhance community, we often choose to share that private information.
- Little regard for the public nature of the Internet.
- Facebook and similar applications make it possible to reconnect with friends from very long ago.
- This all ends up disclosing the very same information that businesses want us to use for authentication.

# Outline

- Definitions: Security; Trust; Privacy
- Security Theory: A A A
- A A A Case Studies
- What is Consuming Security?
  - Enhancing Security
  - Enhancing Profit
  - Enhancing Community
- Appropriate Solutions

# Appropriate Solutions

# Appropriate Solutions

- To avoid inappropriate use of private information by infrastructure providers:
  - Discourage web-based applications.
  - Encourage end-to-end encryption of information exchanges like email.
  - There are technologies to make it impossible to tell the real destination of an encrypted transmission.

# Appropriate Solutions

- To minimize use of private information for security:
  - Trusted 3<sup>rd</sup> party authentication.
  - Electronic notarization.
  - Public Key cryptography.

Thank You!

Slides are available on my web page:  
<http://www.cc.gatech.edu/~scrain6>