

- Security must be balanced against the needs of privacy.
- Security is important yes, but it must be done cognizant of Privacy needs.

Don't Ever Say Things Like  
That!

# Reject the Security/Privacy Dichotomy

- Law enforcement depends heavily on anonymity (only works if anonymity is trusted)
- Anonymizer.com set up link to FBI anonymous tip line from their homepage on Sept. 12, 2001
- Identity theft costs businesses, govt., and individuals a fortune
- Whistleblowers can make managers aware of security problems without fear of reprisal from immediate superiors

# Privacy Enhancing Technologies Workshop

- Here at University of Toronto
- May 26–28, 2004
- Submissions due January 26<sup>th</sup>
- More info at <http://petworkshop.org>

# Understanding Privacy Enhancing Technologies: Do More With Less

Paul Syverson

Naval Research Lab

Roger Dingledine

The Free Haven Project

# PETs and *Beyond*

- Why should you care about magic technology?
  - It won't solve your immediate (currently foreseeable) problems
- Don't push for legislation that is responsive to some currently hot technology  
By the first court case, it will be outdated
- You need to know what is possible.
  - You need to change your expectation so you can change that of the public and the policy makers.

# It's hard to manage privacy information

- Worry about regulatory compliance
- Human and technology costs of protecting information

# What if you don't have any information to protect?

- Answer: Then you don't have to protect that information
- Subject Access Request (SAR) debate this morning
  - If you have not collected anything . . .
  - (perhaps can even prove that you *could not* have collected anything),  
then you are home free.
- Our theme: You can do more with less

- Michael Geist listed reasons why privacy is decreasing
  - workplace monitoring
  - cell phone locational data
  - wireless internet applications
  - copyright
  - lawful access
- Technology already exists to do most of these things without hurting privacy.
- Caller ID example (Bank customer called for general info)
  - shows the immediate relevance of anonymous communication technology (but it's OK Mike, I won't talk about mixes or Onion Routing).

# Example: Identity management

- Microsoft Passport.
- Helps you manage all those passwords, etc.
- Microsoft is carefully protecting that information
- Microsoft is not going to use or sell your usage profile (trust them)

# Lucent Personal Web Assistant (LPWA)

- Invented at Lucent in the mid nineties
- Generates usernames and passwords for all Web sites from a single username and password
- Proven cryptographically robust generation
- Stateless: Nothing is stored
- Provides single sign-on without storing any private information

# Problem: Intended to Make Money

- Had alot of press when developed and then spun off in late nineties
- Used as portal, not on desktop
- Sold, died with Navipath in the Internet bust
- Is patented and languishing
- Great bit of technology that is lost to us for now.

# Making Money is Hard for Decentralized Privacy Systems

- ZKS Freedom, etc. (Cf. Economics of Anonymity, FC 2003)
- Costs are lower if no centralization
- Funded by public sector (Java Anon Proxy, Onion Routing) or volunteers (Onion Routing, MixMinion, Privoxy)?

# Who is *Really* Participating in your System

- Need attributes, reputation, real-world checks, credentials
- There are technologies that allow you to have these
- **But** no identification
- It's not who you are, it's what you can do.

# Just collect the data you need

- A certificate that says bearer is old enough to drink rather than a drivers license
- A zero knowledge proof that you earn enough to carry a mortgage, have done so for five years, etc. rather than submitting copy of your income tax records

# How do you decide when to issue a credential?

- What attributes, reputations, are needed?
- How do you measure the trust on each factor?
- – This does not need to involve identification at all

# How do you protect credentials? Hardware?

- Problem for *all* credentials (not just private ones).
- Better to prove you have the private credential for “allowed to buy alcohol” than trust that the bouncer won’t remember your address from your license.
  - Again, enhancing privacy enhances security

# Function Creep

- Shopping mall owner decides is-a-citizen card should get you into his stores / get you a discount.
- If an issuer's *employee* thinks you should get into the mall, may be willing to bend the rules to get you a credential
- Increased protection  $\Rightarrow$  increased value  $\Rightarrow$  Decreased security

# Function creep can be subtle

- Airlines did not balk at requiring ID
  - not because they believed it did anything for security, but because it helped them control resale of nonrefundable discounted tickets

# What is the Value of Privacy?

-

# Starting Questions

- Are people rational in reasoning about privacy?
- What about corporate valuation of privacy?
- What about governmental valuation of privacy?

# A Classic Scenario

- Check off your favorite soft drinks and restaurants
  - and give your name, address, phone number, DoB, . . .
- Receive a free hamburger
  
- Usual conclusion: consumers are irrational
  - Claim to value privacy in surveys\*
  - Seem willing to trade it for a free hamburger

\*Huh?

# A Consumer Measure of Privacy: Identity Theft

Hamburger	=	\$2
E(ID theft from survey)	=	$\$100K \times 10^{-9}$
E(transaction)	$\approx$	\$2

- Overlooks other values of identity/privacy
- Overlooks cumulative effects on value (myopic)

# Corporate Measure of Privacy

- Information economy favors bundling, price discrimination
  - High fixed costs, low marginal costs
- Both approaches enhanced personalized preference information
  - Varian, Odlyzko
- Not if consumers are strategic
  - Acquisti and Varian (2001,2003)

# Consumer *Cost* of Privacy

- Gellman (March 2002) consumer cost of privacy: \$ 277.90 US per year
- Included: Credit reports, caller ID, Unlisted number, Anonymizer, Junk Mail opt outs
- Not included
  - Time: Downloading Spam, Deleting Spam, Sorting Junkmail, Shredding Junkmail
  - Expected ID theft costs
  - Business overhead ID theft costs
  - Service overhead, outage, reduction from spam and DoS

All of these are about the value of privacy and/or the value of personal information

- None include intangible values (hard to model)
- Ignore dynamic nature of identity theft

# Identity Theft is the Killer App of Privacy Enhancing Technology

- ID theft is not the real crime in ID theft
- Propagating ID theft is the primary problem
- It's not a secrecy compromise, it's an authentication failure
- Recognizing this we can better cope with dynamics

# Cost, Prevalence of ID Theft Both Growing

(GAO Report, March 2002)

- With consumers
- In the financial services industry
- Law enforcement:
  - Agencies could give no meaningful average of either costs or number of cases
- Rough Estimates of Average
  - Investigation, Prosecution: \$10K - \$15K each per case
  - Incarceration: \$17400/inmate/year
  - Parole: \$2900/person/year

# Where Are We Now?

- Some legal protections started
- Consumers should do things outlined above (careful with data, get credit reports, etc.)
- But this is analogous to telling people to watch for suspicious email attachments and not open them
  - Immediately practical, but not addressing the basic problems

# Analogy: Credit Reporting Agency as Pawn Shop

- Check your report twice a year, good advice but ...
  - Like requiring you to
    1. Deposit valuables as cost of doing business
    2. Check the local pawnshops to see if your valuables were stolen/misused
- Not Fair? Credit Agencies centralized, mandated to help you correct problems, etc.

# Better Analogy: Criminal Justice System as Pawn Shop

- There is no central place to check (*correct*) your record
- Little focus on reporting of false information as the problem
- Maybe unfair to pawn shops under current regulations
- Criminal identity theft: the darkest side

# Get The Model Right?

- Allocate cost of ID Theft  $\Rightarrow$  knowing vulnerabilities source
- 72% of 2002 victims: no idea how thief obtained information
- Could survey convicted ID thieves
  - But these are the ones who got caught
  - They're criminals
- Situation is just too dynamic for predictive use of data

# Get the Crime Right

- ID theft is integrity/authentication/reputation violation  
NOT a secrecy violation
- We can better allocate cost if the libel is addressed,  
not just the slander that led to the libel

# Discussion

- Current allocation of costs causes us to focus on identity theft as the central crime
- Likewise squishy authentication infrastructure via nonsecrets (SIN/SSN)
- Current focus is on better handling of PII (personally identifiable information)
- Could strengthen this to, e.g., make use of SIN/SSN illegal outside govt.
- Still focused on containing information, not assigning reputation

# Financial Scenario

1. I give credit to you (as Bob),
2. You default,
3. I say Bob defaulted.
  - Giving you credit was my choice not Bob's
  - If you're Bob, you should incur liability as in credit report
  - If not, I should incur liability of reporting Bob;  
I'm the one who screwed up, affected Bob's reputation integrity
  - Advantage: My choice/risk to authenticate you or limit your credit
  - If I screw up, I should pay a fine
  - Insurance actuarial data gives us the cost of ID theft
  - Who should get the fine/award? The "victim"? The government?

# Criminal Scenario

1. You are arrested for a crime,
2. I (e.g., local court) assign arrest to you (as Bob),
3. You abscond,
4. I say Bob absconded.
  - My report of arrest and/or absconding should be subject to penalties of wrongful arrest
  - Similarly for any agency propagating my report

# Reprise: Do more with less

- This shift in understanding on ID theft means
  - Put the value/cost/incentives of transactions in right place
  - Stop sanctioning use of identifiers as authenticators
  - Whole category of privacy data drops out (SSN/SIN, driver's license, etc.)
  - It won't matter that we all know Steve Adler's Passport number is (omitted for distribution)

# Reprise: Do more with less

- Technologies already exist that allow you to provide service, even highly personalized without capturing private information.
- Financial transactions, location, amazon purchase records, all can be personalized without identification using already invented technologies
- Who cares if your Tivo thinks you're gay, if it doesn't know who you are.  
(Thanks to Lorrie Cranor for the example.)
- We've built it.
- We're not saying you have to come; just know what's there.

# Privacy Enhancing Technologies Workshop

- Here at University of Toronto
- May 26–28, 2004
- Submissions due January 26<sup>th</sup>
- More info at <http://petworkshop.org>