Privacy, Anonynmity, and Security on the Internet

Steven M. Bellovin
smb@research.att.com
http://www.research.att.com/~smb
AT&T Labs Research

One Vision of the Internet

"On the Internet, no one knows you're a dog."

Another Vision of the Internet

It wags its tail, it barks, and it acts the same as last time.

A Third Vision of the Internet

It snarls and bites;
we have to deal
with it.

Three Visions of the Internet

"On the Internet, no one knows you're a dog."

It wags its tail, it barks, and it acts the same as last time.

It snarls and bites; we have to deal with it.

All three perspectives are valid; all three co-exist on the Internet.

Do They Know You're a Dog?

- Your ISP probably knows who you are.
- Your IP address reveals your ISP. It also tends to reveal your geographic location
- Proxies and relays may hide your IP address, but the proxy operator may have logs.
- Anyone with sufficient motive — or power – can ask your ISP. Consider the "subpoena attacks" by the RIAA.

Telling People You're a Dog

- Most purchases require disclosure of identity and location
- That links an IP address to a person
- Voluntary personalization features — for example, a localized weather report — disclose probable location

Enter the Web

- No identification supplied with user queries.
- ☞ Actually, some very early browsers would emit a `User:` line, though that went away very early.
- But — http is stateless; some mechanism was needed to retain state between connections.
- Enter the *cookie* — minimal standardized syntax and semantics.
- Cookies may be retained *across* sessions...

That Bark Sounds Familiar

- When you return to a Web site, stored cookies disclose that fact
- Third-party stored cookies — used by most Internet advertisers — provide cross-site linkages
- Your virtual identity is trackable

Profiling

- Many sites profile your behavior.
- News sites often tailor ads based on the articles you read
- Search engines know a *lot* about you
- ☞ Some search engines link their profile of you to a third-party cookie supplier (i.e., Alta Vista and Doubleclick, years ago)
- Net result: you have a behaviorally-defined online identity

Even More Linkages

- If you buy something from an cookie user, you've established a linkage
- Who gets that information?
- How many sites know who you are?

Big Brother versus Little Brother

- Most of these threats are from corporations, no governments
- The U.S. has *very* few restrictions on private sector collection, use, and sharing of private data.
- Big Brother can and does purchase data from Little Brother if and as needed.

Fighting Back

- Free hotspots
- Rejecting third-party cookies
- Anonymizers
- Sharing site logins (web sites with such lists)

Who Pays?

- Someone has to pay to provide all these nice facilities
- For better or worse, the coin we're using is our privacy
- The money has to come from somewhere. . .

Steady State

- Empirically, most people don’t take active measures to protect their privacy
- The avoidance behaviors don’t scale
- Result: enough people “pay” that some can ride free
- Some linkages are possible, but aren’t instantiated

Ouch! You Bit Me!

- Bad guys strain the social contract
- Deterring misbehavior creates pressure for identification
- The alternative is often reduced functionality

Security and Identification

- If you've misbehaved badly enough, legal mechanisms can be used to learn your identity
- Example: the police vs. hackers
- Example: the RIAA vs. file-sharers
- Example: many large companies vs. people who have "defamed" them

Proactive Identification

- When the threat is serious enough — or perceived to be serious enough — requirements for identification spring up
- Example: Internet cafe regulations in Vietnam and China. (The new Los Angeles rules don't appear to be connected to cyberspace behavior.)
- Some people want to mandate attribute identification, i.e., age, geographic location, etc.
- Repeated calls to “fix” the Internet so that every packet is tagged with its owner's identity

Loss of Functionality

- Have you sent to port 25 lately?
- Demands that ISPs block — somehow — peer-to-peer programs
- (Disney asked for a “copyright” flag in all packets.)
- Login requirements at free hotspots

Identification, Authorization, and Spam

- Spam (and hacking) are not identification problems — the bad guys use many identities
- Spam (and hacking) are not authorization issues — anyone is allowed to send email. (Most breakins don't occur because of bad authentication.)
- It's behavioral — but methods to detect such misbehavior are proving insufficient, so there is pressure to fall back on identification and authorization

Fighting Spyware

- A lot of spyware/hackware exploits buggy, insecure operating systems. We know what to do about that...
- But much of it is voluntarily downloaded by users who don't read the (deliberately?) confusing license agreements.
- We need a way to permit such downloads — but to isolate them during execution to protect privacy

Achieving Privacy

- The best way to achieve privacy is to avoid linkages
- Do not permit cross-site or cross-application communication
- Don't use hard-to-change authentication data (biometrics are generally the wrong answer to the wrong question)
- Watch for common data — the same user-chosen login or password from a related IP address
- Site-issued, per-site certificates are a better way to do authentication, because they avoid some common data
- Change IP addresses frequently

Status

- We have a delicate 3-way balance between privacy, payment, and proper behavior
- People who want privacy can usually get it — but it takes a lot of knowledge
- Financial pressures or behavioral pressures can disrupt this balance

The Challenge

- Someone has to find a financially sound footing for the Web that doesn't violate privacy
- We need a financially and technologically sound solution to the file-sharing issue — one that doesn't involve the new crime of "felony interference with a business model"
- We need a way to prevent or block misbehavior
- This last one may be achievable by technical means — and that's our task