FSEM 1111 Computer Security – from a Free Software Perspective

Christian Grothoff
christian@grothoff.org

http://grothoff.org/christian/

Privacy

- What is Privacy?
- Who cares about Privacy?
- Why value Privacy?
- How to protect Privacy?

I have nothing to hide!

I have nothing to hide?

- Who said it was about hiding illegal things?
- Please post your bank statements on your webpage.
- What are the exact offers you get from our competitors?

Quotes

"Privacy is inherently personal. The right to privacy recognizes the souvereignity of the individual." – Smith v. City of Artesia, 772 P.2d 373, 376 (N.M. Ct. App. 1989)

Quotes

"Privacy is a societal license that excepts a category of acts (including throughts and emotions) from communal, public and governmental scrutiny." – Amitai Etzioni, The Limits of Privacy, 1999

Quotes

"We cannot think of ourselves save as to some extent social beings. Hence we cannot separate the idea of ourselves and our own good from our idea of others and of their good." – John Dewey, Ethics, 1908.

Quotes

"Even when it (privacy) protects the individual, it does so for the sake of society. It should thus not be weighted as an individual right against the greater social good. Privacy issues involve balancing societal interests on both sides of the scale." – Daniel J. Solove, 2007

Case Study (from sfgate, 2004)

For 16 years, California's Cancer Registry has been dutifully logging the names and addresses of all state residents who come down with the dreaded disease, their type of cancer and whether they live or die.

Since April 14, 2003, however, a new federal law designed to protect the privacy of medical records has made it harder for medical researchers in the United States to troll through patient charts.

Citing the privacy rule, at least 17 Bay Area hospitals have imposed restrictions on the state Cancer Registry's accustomed rapid access to patient records.

Case Study (from computer.org, 2007)

In July 2005, Arnold arrived at Los Angeles International Airport. US Customs and Border Patrol (CBP) Officer Peng asked a few routine questions and inspected Arnold's luggage and carry-on bag, which contained a laptop computer. Officer Peng made the customary request that Arnold turn on the computer to verify that it would operate. She then transferred the laptop to a second CBP officer who noticed numerous icons and folders on the display screen, including two folders labeled "Kodak pictures" and "Kodak memories." The CBP officers clicked open the folders to view the contents. Among the images, they found one of two naked adult women.

Case Study (from computer.org, 2007)

With this discovery, Immigration and Customs Enforcement (ICE) special agents interrogated Arnold for several hours about his laptop's contents. They expanded the search and found child pornography. The ICE agents then seized Arnold's computer equipment and released him. Two weeks later, federal agents obtained a warrant to search the laptop and found additional images.

The government indicted Arnold for possession of child pornography. Arnold moved to suppress the evidence, claiming the CBP's search and seizure of his computer equipment violated the Fourth Amendment.

Case Study (from computer.org, 2007)

A further aspect, not before the court in this case, is the plausible scenario of Arnold's having encrypted all data on his hard drive (except for the file folders visible on the desktop). The CBP officers would have seen nothing when they clicked on the desktop icons. Could CBP have attempted, with or without a warrant, to compel Arnold to disclose the password?

Case Study

"Protections for anonymous speech are vital to democratic discourse. Allowing dissenters to shield their identities frees them to express critical, minority views ... Anonymity is a shield from the tyranny of the majority. ... It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation ... at the hand of an intolerant society." – MyEntyre v. Ohio Elections Commission, Supreme Court 1995

Anonymity $\equiv$ Privacy?

What is Anonymity?

Entropy

Entropy is a measure of the uncertainty associated with a random variable.

- Average shortest message length, in bits, that can be sent to communicate the true value of the random variable
- Mathematical limit on the best possible lossless data compression

Entropy: Definition

Let the set Φ be the range of the random variable and p_u the probability for choosing $u \in \Phi$. Then

$$S = -\sum_{u \in \Phi} p_u \cdot \log_2(p_u) \tag{1}$$

is the information in each independent choice.

Anonymity: Definition

1. Attacker computes a **probability distribution** describing the likelyhood of each participant to be the responsible party.

2. Anonymity is the stronger, the larger the anonymity set and the more evenly distributed the subjects within that set are.

Formal Definition

Let $\mathcal{U}$ be the attacker's probability distribution describing the probability that user $u \in \Psi$ is responsible. Define the effective size S of the anonymity distribution $\mathcal{U}$ to be:

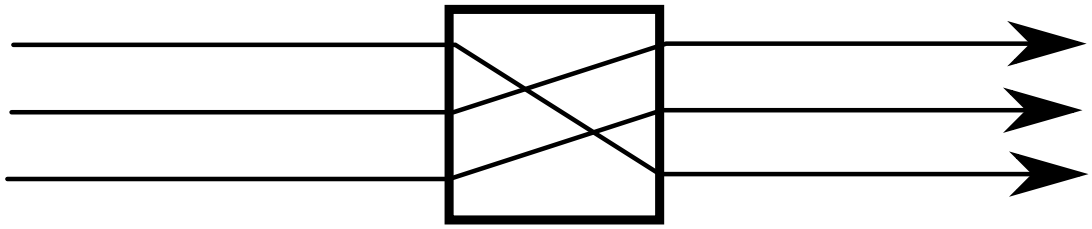
$$S = -\sum_{u \in \Psi} p_u \log_2 p_u \tag{2}$$

where $p_u = \mathcal{U}(u)$.

This is the expected number of bits of additional information that the attacker needs to definitely identify the user!

Mixing

David Chaum's mix (1981) and cascades of mixes are the traditional basis for destroying linkability:



Mixing

David Chaum's mix (1981) and cascades of mixes are the traditional basis for destroying linkability:

Anonymity $\equiv$ Privacy?

- Absolute Anonymity $\Rightarrow$ Privacy
- But: absolute anonymity does not exist!

$\Rightarrow$ Use other means to protect privacy if possible!

Questions

?