Anonymity

Professor Patrick McDaniel
CSE545 - Advanced Network Security
Spring 2011
Anonymity

"On the Internet, nobody knows you're a dog."
The Internet can’t be censored

“The Net treats censorship as damage and routes around it.”

- John Gillmore

(2011 – go ask Libya)
Actually, none of this is true

• It is easy to adopt a pseudonym or a persona on the Internet, but it is difficult to be truly anonymous
  ‣ Identities can usually be revealed with cooperation of ISP, local sys-admins, web logs, phone records, etc.

• The Internet can put up a good fight against censorship, but in the end there is still a lot of Internet censorship
  ‣ Repressive governments and intellectual property lawyers have been pretty successful at getting Internet content removed
  ‣ Case in point, “the great firewall of China”
Why anonymity?

• What about in the real world?
  ‣ Do you want people to know which stores, movies, restaurants, books you make use of?
  ‣ Do you want everything you say to be associated with you (forever)?

• Are there activities that you would not like to share when surfing the net?
  ‣ With whom?
  ‣ What about writings (e.g., blogging), new group postings, …

  “McDaniel’s programming stupidity example”
Degrees of anonymity

More

- **Absolute privacy**: adversary cannot observe communication
- **Beyond suspicion**: no user is more suspicious than any other
- **Probable innocence**: each user is more likely innocent than not
- **Possible innocence**: nontrivial probability that user is innocent
- **Exposed** (default on web): adversary learns responsible user
- **Provably exposed**: adversary can prove your actions to others

Less
Software tools

- Encryption tools – prevent others from listening in on your communications
  - File encryption
  - Email encryption
  - Encrypted network connections

- Anonymity and pseudonymity tools – prevent your actions from being linked to you
  - Anonymizing proxies
  - Mix Networks and similar web anonymity tools
  - Anonymous email

Information and transparency tools - make informed choices about how your information will be used
  ★ Identity management tools
  ★ P3P

Filters
  ★ Cookie cutters
  ★ Child protection software

Other tools
  ★ Computer “cleaners”
  ★ Privacy suites
  ★ Personal firewalls
User view ...

• Problem Statement
  ‣ I want to surf the Internet and view content.
  ‣ … I am concerned that the Websites are going to track me …
  ‣ … or the government or Insurance agency or some other organization is going to associate me with some community.

• This is a reality: many users may be wary of freely surfing sensitive content
  ‣ Especially when societal stigma involved (e.g., looking for information on AIDS)

• Incognito (Chrome): disable caching, history, persistent cookies, etc.
  ‣ Does this lead to anonymous browsing?
Anonymous email

- **Anonymous remailers** allow people to send email anonymously
- Similar to anonymous web proxies
  - Send mail to remailer, which strips out any identifying information (very controversial)
  - Johan (Julf) Helsingius ~ Penet
- Some can be chained and work like mixes

http://anon.efga.org/~rlist
Filters

• Cookie Cutters
  ‣ Block cookies, allow for more fine-grained cookie control, etc.
  ‣ Some also filter ads, referrer header, and browser chatter
    ‣ \url{http://www.junkbusters.com/}

• Child Protection Software
  ‣ Block the transmission of certain information via email, chat rooms, or web forms when child is using computer
  ‣ Limit who a child can email or chat with
    ‣ \url{http://www.getnetwise.org/}
Filters (cont.)

• Pop-up blockers
  ‣ Filters more to reduce annoying, rather than protect privacy
  ‣ Works in similar ways to cookie cutters
  ‣ Built into newer browsers (Safari)
  ‣ New York Times - delay content adds

• Web-Bug detectors (not filters)
  ‣ Highlights invisible .gifs used to track user

http://www.bugnosis.org
Proxy solutions

- Acts as a proxy for users
- Hides information from end servers
- Sees all web traffic
- Adds ads to pages (free service; subscription service also available)

http://www.anonymizer.com
Proxy solutions

- Acts as a proxy for users
- Hides information from end servers
- Sees all web traffic
- Adds ads to pages (free service; subscription service also available)

http://www.anonymizer.com
Proxy solutions

- Acts as a proxy for users
- Hides information from end servers
- Sees all web traffic
- Adds ads to pages (free service; subscription service also available)

http://www.anonymizer.com
Proxy solutions

- Acts as a proxy for users
- Hides information from end servers
- Sees all web traffic
- Adds ads to pages (free service; subscription service also available)

http://www.anonymizer.com
Proxy solutions

- Acts as a proxy for users
- Hides information from end servers
- Sees all web traffic
- Adds ads to pages (free service; subscription service also available)

http://www.anonymizer.com
Mixes [Chaum81]

• Assume a fully connected network of nodes

• Peers want to communicate with each but don’t want people to know that they are talking

• Alternately: the sender might not want the receiver to know who she is

• Assumption: nobody can perform traffic analysis

• Suppose E wants to send to B
1. \( E \) picks a random order of a subset of nodes in the graph. Arbitrarily, she chooses \( FAC \) to send message \( m \).

2. \( E \) creates a message:

\[
E(E(E(P|msg), K_B^+)|B, k_C^+)|C, k_A^+)|A, k_F^+)
\]

where \( P \) is some random padding and sends it to \( F \).

3. \( F \) uses their private key to decrypt the message and recovers:

\[
E(E(E(P|msg), K_B^+)|B, k_C^+)|C, k_A^+)|A
\]

\( F \) strips off the trailing \( A \) and sends the remainder to \( C \)

4. Repeat until \( B \) receives \( E(P|msg), K_B^+ \), which unwraps the message and returns it.
Simplified Mix

$E(E(E(P|msg), K_B^+)|B, k_C^+)|C, k_A^+)$

$E(E(E(E(P|msg), K_B^+)|B, k_C^+)|C, k_A^+)|A, k_F^+)$

$E(E(P|msg), K_B^+)|B, k_C^+)$

$E(P|msg), K_B^+)$
1. Include a one time key $k_o$ and the following in the original message:
$$E(E(E(E(P|E), K_E^+)|E, k_D^+)|D, k_A^+)|A, k_F^+)|F, k_0$$

2. Encrypt the message to be returned, $m_r$ using $k_o$, then send to $F$:
$$E(E(E(E(P|E), K_E^+)|E, k_D^+)|D, k_A^+)|A, k_F^+)|F, E(m_r, k_o)$$

3. Now follow the reverse routing back to $E$.

This is an imperfect solution, can you guess why?
Tor and Friends

• Circuit-based version of mix-like routing.
  ‣ They use things like SSL/TLS to secure peer communication
  ‣ Build onion circuits that support anonymized communication.

• Challenges:
  ‣ Doing this fast
  ‣ Ensure that traffic analysis is very hard
  ‣ Prevent compromised notes from manipulating the mix to expose the communicating parties
  ‣ Do key security association management
Crowds

• Users join a Crowd of other users
• Web requests from the crowd cannot be linked to any individual
• Protection from
  ‣ end servers
  ‣ other crowd members
  ‣ system administrators
  ‣ eavesdroppers
• First system to hide data shadow on the web without trusting a central authority
Crowds

Crowd members

1  6
2  5
3  4

Web servers

3  5  1
2  6  4
Crowds

Crowd members

1
2
3
4
5
6

Web servers

3
4
5
6
1
2
Crowds

Crowd members

Web servers

1

6

5

2

3

4

5

6

1

2

3

4
Crowds

Crowd members

Web servers
Crowds

Crowd members

Web servers

1 → 2
2 → 3
3 → 4
4 → 5
5 → 1
1 → 6
6 → 2
Crowds

Crowd members

Web servers

Diagram showing the relationships between crowd members and web servers.
Crowds

1. Initiator selects a *jondo* (‘John Doe’), which is another host in crowd
2. *Jondo* either
   (a) forwards traffic to randomly selected next hop or
   (b) forwards requests to end server
Provider view ..

• Problem Statement
  ‣ I want to publish some content
  ‣ ... I am concerned that the Websites are going to track me ...
  ‣ ... or the government or Insurance company or some other organization is going to associate me with some community.

• Some countries are very serious about controlling content on the Internet.
  ‣ Software used to anonymously distribute information to community (political dissident).
Anonymous censorship-resistant publishing

• The printing press and the WWW can be powerful revolutionary tools
  ‣ Political dissent
  ‣ Whistle blowing
  ‣ Radical ideas

• but those who seek to suppress revolutions have powerful tools of their own
  ‣ Stop publication
  ‣ Destroy published materials
  ‣ Prevent distribution
  ‣ Intimidate or physically or financially harm author or publisher
Anonymity increases censorship-resistance

• Reduces ability to force “voluntary” self-censorship

• Allows some authors to have their work taken more seriously
  ‣ Reduces bias due to gender, race, ethnic background, social position, etc.

• Many historical examples of important anonymous publications
  ‣ In the Colonies during Revolutionary War when British law prohibited writings suggesting overthrow of the government
  ‣ Federalist papers
Publius design goals

- Censorship resistant
- Tamper evident
- Source anonymous
- Updateable
- Deniable
- Fault tolerant
- Persistent
- Extensible
- Freely Available
Publius Overview

Publishers - Post Publius content
Servers - Host Publius content
Retrievers - Browse Publius content

- Publius Content - Static content (HTML, images, PDF, etc)
- Publishers - Post Publius content
- Servers - Host Publius content
- Retrievers - Browse Publius content
• Generate secret key and use it to encrypt document
• Use “secret splitting” to split key into n shares
• This technique has special property that only k out of n shares are needed to put the key back together
• Publish encrypted document and 1 share on each of n servers
• Generate special Publius URL that encodes the location of each share and encrypted document — example: http://!publius!/1e6adsg673h0==hgj7889340==345lsafdfg
Publius proxies

- Publius proxies running on a user’s local machine or on the network handle all the publish and retrieve operations.
- Proxies also allow publishers to delete and update content.
Threats and limitations

- Attacks on server resources
  - 100K Content Limit (easy to subvert)
  - Server limits # of files it will store
  - Possibility: use a payment scheme
- Threats to publisher anonymity
- “Rubber-Hose Cryptanalysis”
  - Added “don’t update” and don’t delete bit
- Logging, network segment eavesdropping
- Collaboration of servers to censor content
  - A feature?
Discussion

• Technology that can protect “good” speech also protects “bad” speech

• What if your dog does publish your secrets to the Internet and you can't do anything about it?

• Is building a censorship-resistant publishing system irresponsible?

• If a tree falls in a forest and nobody hears it....