Privacy on the Internet

A help session sponsored by the OCF, CSUA, and XCF

1996-12-18

Contents

Presented by: Sameer Parekh <sameer@c2.org>

President, Community ConneXion: The Internet Privacy Provider.

NOTE: This talk presumes knowledge of PGP. If you don't know PGP you can get it and instructions from:

ftp://ftp.csua.berkeley.edu/pub/cypherpunks/pgp262/

Anonymous Remailers

- Allow for anonymous communication
- No record is kept of originating address
- Uses distributed trust model

To send anonymous mail to spy@kgb.gov, you first compose the message:

> Subject: Stealth bomber plans
>
> Here are the stealth bomber plans:
>
> [...]

Then, using premail, you send it.

```
elm 'spy@kgb.gov^chain=ecafe;mix;hacktic'
```

[etc]

The message will be sent from here to London, San Diego, Holland, and then to the destination. At each step it is encrypted, so each remailer knows only where it came from most recently and where it is going next. It doesn't know about other parts in the chain.

To trace the message back, each remailer would have to be watched and PGP would have to be cracked.

What premail does

Premail is a front end to the remailers. It does all theencryption for you, so that you don't need to hassle yourself with the long process involved in building your encrypted remailing chain:

First you encrypt the message with the key of the final remailer in the chain, with directions to send the message to spy@kgb.gov:

```
::
Anon-Send-To: spy@kgb.gov
##
Subject: Stealth bomber plans
Here are the stealth bomber plans.
```

The above gets encrypted with the key of ‘hacktic’ and then the next step is to encrypt the following with the key for ‘mix’:

```
::
Anon-Send-To: remailer@utopia.hacktic.nl
::
Encrypted: PGP
—–BEGIN PGP MESSAGE—–
[etc]
—–END PGP MESSAGE—–
```

The process continues until you have included as many remailers as you would like on your chain, for the level of privacy that you desire. Premail takes care of all of the above though, so you don’t really need to worry about it. It is good, however, to understand what is going on so that you understand the security issues involved.

Traffic analysis

If all the remailers were being watched and padding and/or reordering wasn’t done, it would be easy to trace. the CIA could see that a message entered ‘ecafe’ from ‘c2.org’, another message left ‘ecafe’ for ‘mix’, another one left ‘mix’ for ‘hacktic’, and another left ‘hacktic’ for ‘kgb.gov’ all at about the same time– then they can suspect c2.org. The remailers reorder messages so they can’t be traced.

Pseudonymity

- persistent identity
- more security than anon.penet.fi
- anonymous message pools

If you had an identity unabomber@alpha.c2.org and the FBI served c2.org with a court order, c2.org would comply with the court order but the FBI would not get the destination address for unabomber@alpha.c2.org. If done well, the FBI would need to obtain court orders in the UK, Holland, US, Canada, and Finland in order to trace the suspect.

Even then, it may not be possible.

Creating identity

Suppose the real address of the unabomber was luddite@aol.com. The Unabomber would build a reply block:

> ::
>
> Anon-Send-To: luddite@aol.com and encrypt it with the key of remail@ecafe.org, and then create the following:
>
> ::
>
> Anon-Send-To: remail@ecafe.org
>
> ::
>
> Encrypted: PGP
>
> —–BEGIN PGP MESSAGE—–
>
> [etc]
>
> —–END PGP MESSAGE—–
>
> And iterate with all the remailers in all the different countries. (Just as though he were sending a null message to himself through the remailers)

Then he would send that to alias@alpha.c2.org to request the creation of the alias unabomber@alpha.c2.org (the following would be encrypted with the key of alias@alpha.c2.org):

> From: unabomber@alpha.c2.org
>
> Password: civilizationsucks
>
> Reply-Block:
>
> ::
>
> Anon-To: remailer@utopia.hacktic.nl
>
> ::
>
> Encrypted: PGP
>
> —–BEGIN PGP MESSAGE—–
>
> [etc]
>
> —–END PGP MESSAGE—–

Sending messages

For the unabomber to send a message from unabomber@alpha.c2.org all he needs to do is send a message to alias@alpha.c2.org (again, encrypted with the key of alias@alpha.c2.org):

> From: unabomber@alpha.c2.org
>
> Password: civilizationsucks
>
> To: Bob_Guccione@penthousemag.com
>
> Subject: you suck
>
> bwhaha, the respected newspapers printed my stuff. You suck.

Bob Guccione would receive an email from unabomber@alpha.c2.org with the message above.

NOTE: A future version of premail will include support for alpha.c2.org aliases.

Anonymous Web Serving

It's possible to serve web pages completely anonymously, as well. Perhaps you want some information disseminated but don't want it linked to your real name. c2.org offers fully anonymous shell accounts which allow five megs of space for webserving..

A court order wouldn't even reveal your name, because we don't even require your real name. See http://www.c2.org/ for more details on anonymous accounts.

Privacy on the Internet
A help session sponsored by the OCF, CSUA, and XCF
1996-12-18

The eXperimental Computing Facility at UC Berkeley - https://xcf.berkeley.edu
This is likely outdated advice and many of the links are dead, but, it's interesting to see early cypherpunks imagining an alternate universe in which the Unabomber sent a mocking email to Bob Guccione of Penthouse magazine.