GNET - A fully anonymous distributed networking infrastructure

by

GNET - A fully anonymous distributed networking infrastructure

by

— not disclosed due to DMCA —

User Experience

- search for “mp3” AND “Metallica” AND “DMCA”
- *GNet* returns list of files with description
- user selects interesting file
- *GNet* returns the file

Applications

- anonymous sharing of medical histories
- distributed backups of important data
- ad-hoc communication between small devices

Applications

- anonymous sharing of medical histories
- distributed backups of important data
- ad-hoc communication between small devices
- and others

Requirements

- Anonymity
- Confidentiality
- Deniability

Requirements

- Anonymity
- Confidentiality
- Deniability
- Accountability
- Efficiency

Related Work (1/2)

- Napster:
  - ⋆ centralized, outlawed
  - ⋆ no confidentiality or anonymity
  - ⋆ no authentication
- GNutella:
  - ⋆ distributed (breadth first), legally challenged
  - ⋆ no confidentiality or anonymity
  - ⋆ no authentication, no accounting

Related Work (2/2)

- Freenet:
  - ⋆ distributed (depth first)
  - ⋆ anonymity, confidentiality and deniability
  - ⋆ no accountability
  - ⋆ can not handle large files
- Mojo Nation:
  - ⋆ centralized
  - ⋆ no confidentiality or anonymity
  - ⋆ accounting (micro payments)

The GNet Framework

GNet is layered:

1. UDP

The GNet Framework

GNet is layered:

1. UDP
2. Networking Layer

The GNet Framework

GNet is layered:

1. UDP
2. Networking Layer
3. Application Layer

The GNet Framework

GNet is layered:

1. UDP
2. Networking Layer
3. Application Layer

The Networking Layer

GNet's networking layer provides:

- authentication $\Rightarrow$ accountability
- confidentiality
- routing of queries and content
- host evaluation based on earlier behavior

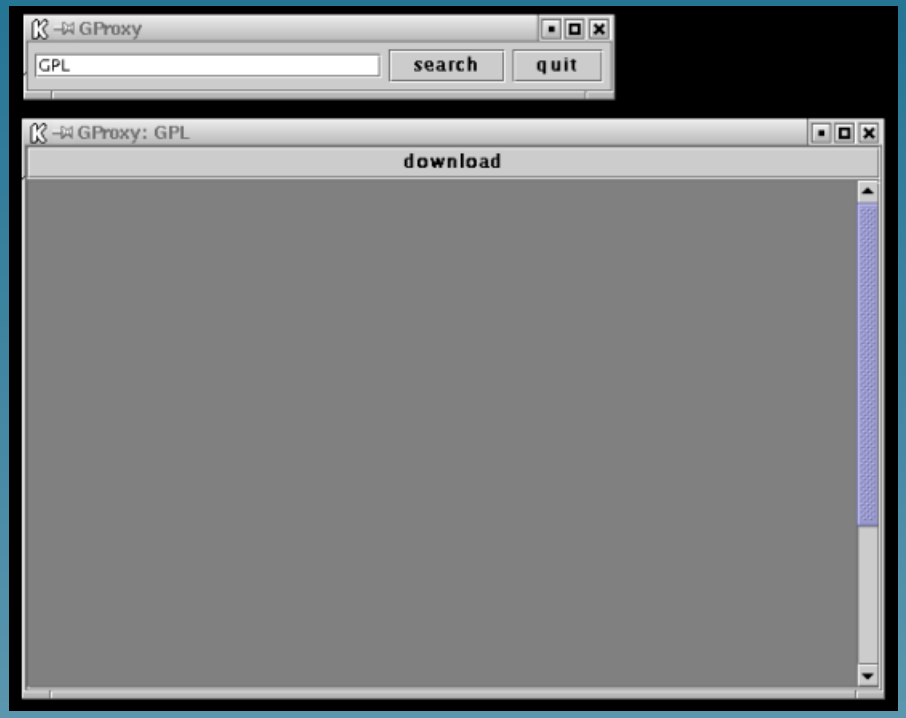
The Application Layer

Currently, the only application implemented is *GProxy*. *GProxy* provides:

- content encoding and decoding
- query encoding
- user interface

GProxy communicates with the networking layer via TCP (loopback).

How does it look like?



Java!?

- *GProxy* is written in Java.

Java!?

- *GProxy* is written in Java.
- *GNet*'s authors did realize that a JVM is too big for a server process.

Java!?

- *GProxy* is written in Java.
- *GNet*'s authors did realize that a JVM is too big for a server process.
- The networking layer is written in C.

Focus: Content encryption

- intermediaries can not find out the content transmitted or be plausably be expected to
- intermediaries can not find out the content of queries
- hosts can deny being originator of a query as long as not all other hosts conspire
- retrieve content with simple keyword
- keep storage requirements minimal

Encoding Content

- split content into 1k blocks B (UDP packet size!)
- compute H(B) and H(H(B))
- encrypt B with H(B), with Blowfish
- store under H(H(B))
- build inner blocks containing H(B)
- root node R contains description

Limitiations

- if the keywords can be guessed...

Limitiations

- if the keywords can be guessed...participating hosts can decrypt the query
- if the exact data can be guessed...

Limitiations

- if the keywords can be guessed...participating hosts can decrypt the query
- if the exact data can be guessed...participating hosts can match the content

Limitiations

- if the keywords can be guessed...participating hosts can decrypt the query
- if the exact data can be guessed...participating hosts can match the content

  this is intended to reduce storage costs!

System Requirements

- At the moment: Linux

System Requirements

- At the moment: Linux
- Java JDK 1.3 for GProxy.
- OpenSSL for encryption
- gcc, autoconf, automake for compilation
- libz (CRC32), pthreads

What do I download?

First, you need the sources:

http://gecko.cs.purdue.edu/gnet/download.php3

In addition to this, you need an initial set of hosts. You can find their keys under:

http://gecko.cs.purdue.edu/gnet/hosts/

It is usually a good idea to download as many hostkeys as possible.

How to install?

```
# tar xvfz gnet-VERSION.tar.gz
# cd gnet-VERSION
# bin/build.sh /tmp
# cp gnet.conf ~/.gnet
# /tmp/bin/gnet &
# cd ../hosts
# cp * ~/.gnet_/data/hosts
# /tmp/bin/gproxy &
# sleep 60
```

Search for “Microsoft” to test.

How to insert content?

```
# /tmp/bin/insertfile FILENAME KEYWORD DESCR
```

Repeat for multiple keywords. If you want to share files that you are still using in plaintext on your drive, *GNet* will allow in the next version to share directly from the drive.

Is that safe?

Short answer: NO. Long answer:

- This is new software. There will be bugs and important features are missing.
- The TCP port 2086 (default) should be firewalled as the node "trusts" that connection.
- If nobody *guesses* your keywords, nobody will be able to know what you asked for or what you got.

GNet resources

- FAQ
- Mailinglist
- Mantis
- README
- Sources
- WWW page

Conclusion

- *GNet* could be a cool system for privacy.

Conclusion

- *GNet* could be a cool system for privacy.
- *GNet* can already be used.

Conclusion

- *GNet* could be a cool system for privacy.
- *GNet* can already be used.
- *GNet* can get alot better.

Conclusion

- *GNet* could be a cool system for privacy.
- *GNet* can already be used.
- *GNet* can get alot better.
- *GNet* needs your help, participate!

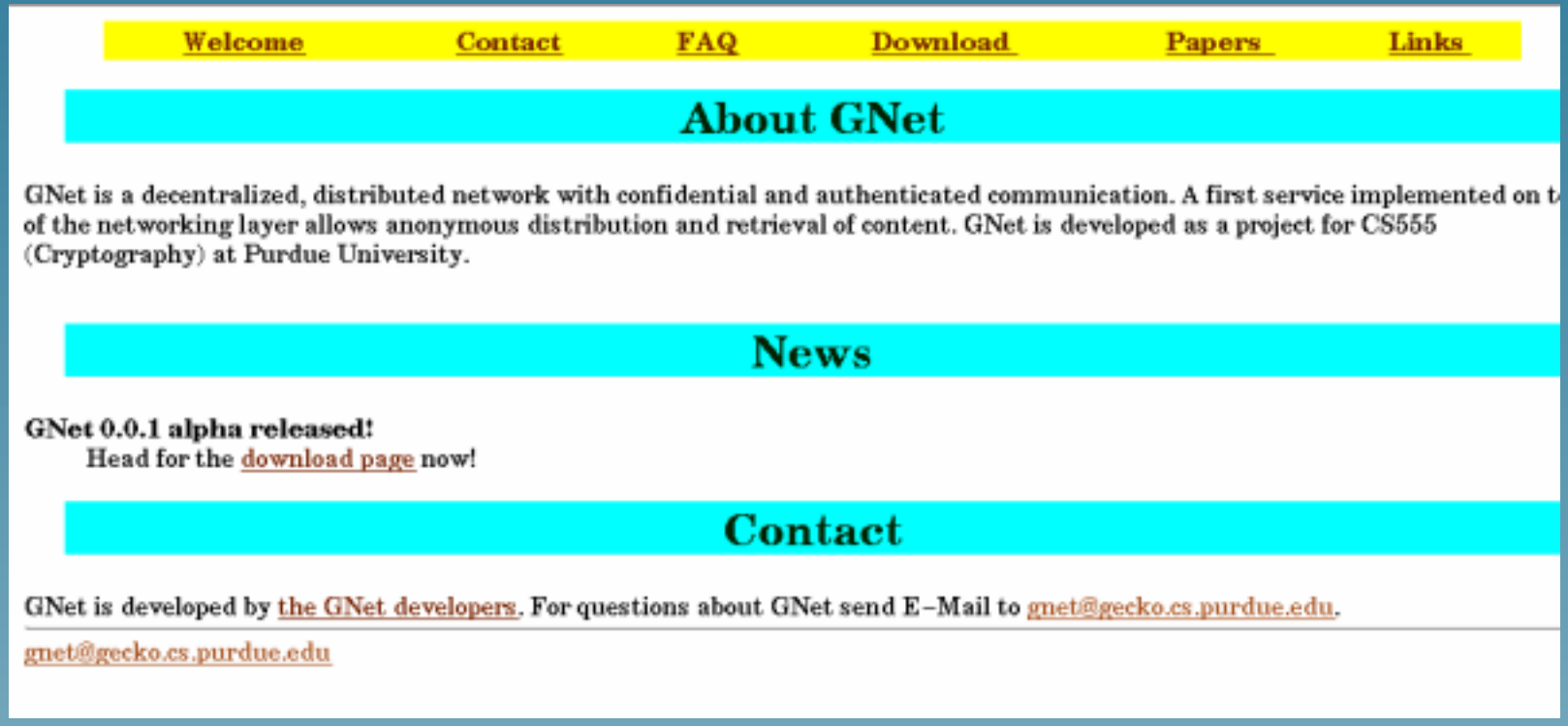
Conclusion

- *GNet* could be a cool system for privacy.
- *GNet* can already be used.
- *GNet* can get alot better.
- *GNet* needs your help, participate!
- *Linux* rules.

GNET Online

GNET can be obtained from our web-page:

http://gecko.cs.purdue.edu/gnet/



Famous last words...

Famous last words...

RTFM