# distributed.net

Michael Feiri

# distributed.net

- What is it (Stats/History/Motivation)
- Infrastructure (topology/code)
- projects (OGR, crypto, suggestions)
- stories (trojans/lawsuits/fun)
- security

# What is it?

# What is it?

- "...finding new ways for computers connected to the Internet being used during "idle" time." *http://www.distributed.net/pressroom/*
- the first large-scale collaborative computing effort ever
- non-profit organization by volunteers

# The basic idea

Split one huge Problem into millions of small problems

# Statistics

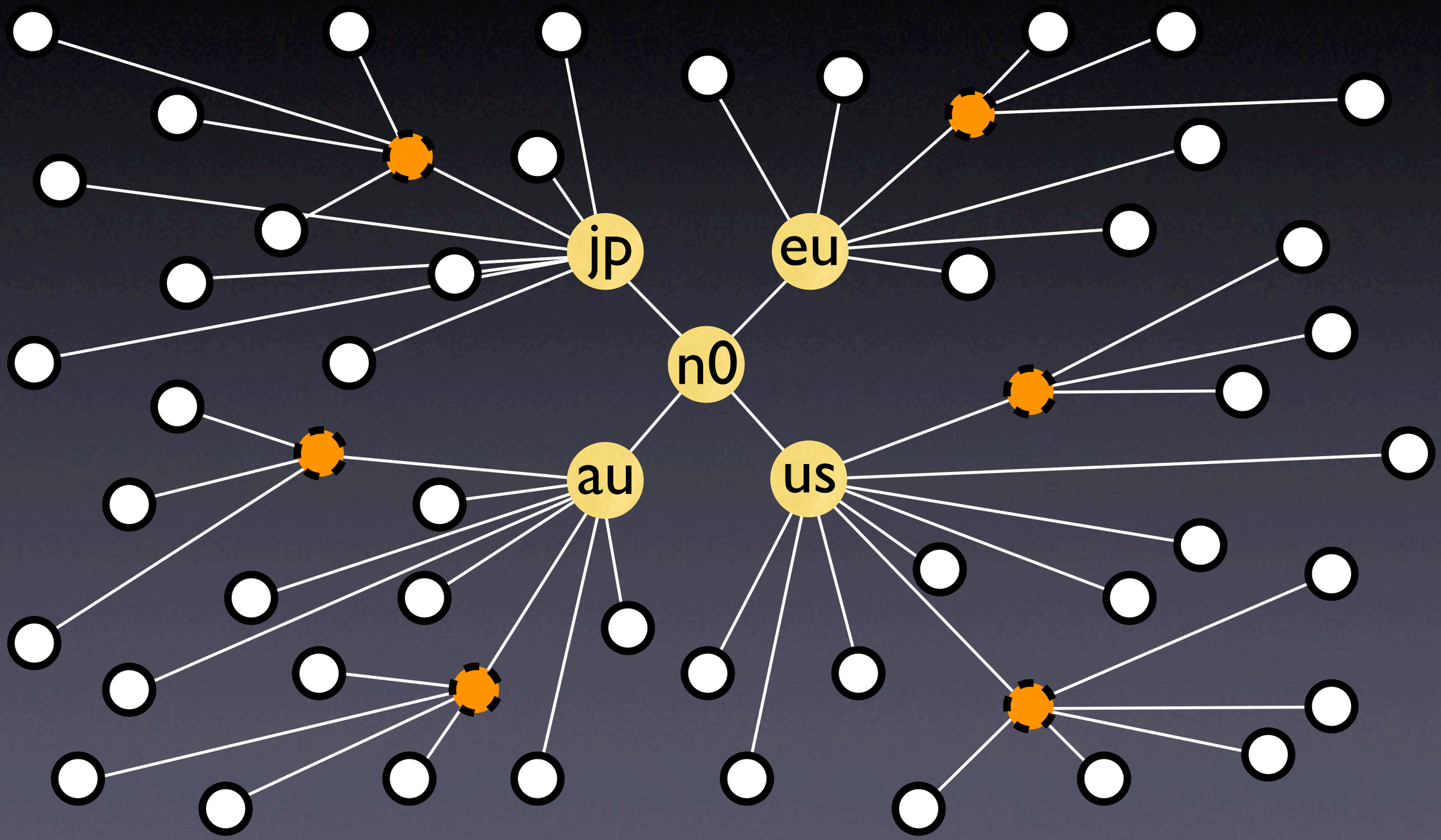
- http://stats.distributed.net/
- http://www.distributed.net/statistics/
- http://www.distributed.net/pressroom/news-20020926.html

# Histroy

- http://www.distributed.net/history.html
- ...
- http://gallery.distributed.net/


# Infrastructure

# Centralized ring with hierarchic extensions



# References

- http://n0cgi.distributed.net/ogr-proxyinfo.html
- http://n0cgi.distributed.net/rc5-proxyinfo.html
- http://www.openp2p.com/pub/a/p2p/2002/01/08/p2p_topologies_pt2.html

# Misc

- Software
  - Client, proxy, keymaster, stats
    - Most of it is open source software
- Communication
  - Proxymessages, .plan, mailinglists, IRC


RSA
SECURITY
COMMUNICATION
& SYSTEMES
Optimal Golomb Rulers
1
3
5
2
NIST
National Institute of
Standards and Technology

# Projects

# DES

- DES-II-1 (Feb 1998)
  - Solved by distributed.net after 40 days
- DES-II-2 (Jun 1998)
  - Solved by EFF within 4 days
- DES-III (Jan 1999)
  - Solved by d.net and EFF in less than 1 day

# CSC/RC5

- CSC (1999/2000)
  - Solved by distributed.net within 61 days
- RC5-56 (1997)
  - Solved by distributed.net after 212 days
  - The unknown message is: It's time to move to a longer key length

# RC5

- RC5-64 (1997-2002)
  - Solved by distributed.net after 1757 days
    - The unknown message is: Some things are better left unread
- RC5-72 (since 2002)
  - Still running

# OGR

- The first non-crypto project at distributed.net
- Launched in February 2000
- Restarted on Friday July 13 2000
- Still running
- more information about OGR.....

# OGR in depth

- Introduction
  - http://library.thinkquest.org/C007645/english/2-golomb-0.htm
  - http://www.research.ibm.com/people/s/shearer/grtab.html
- Algorithms
  - http://www.ee.duke.edu/~wrankin/golomb/golomb.html
- Mathematical background
  - http://www.softnet.tuc.gr/~apdim/diploma/


RC5-64 It's time for a longer key length
distributed.net
cracking made legal
4 Improving encryption by breaking it.
Crack RC5!
Distributed.net
OGR
Join The Search
WATCH OUT RC5-64, THE COWS ARE COMING...
the key - it is out there.
RC5

# Stories

# Stories

- email harvester
- trojans and viruses
- energy waste
- unauthorized installs
- megaflushes
- hacked clients


# Security

# Anti cheat measures

- obfuscate communication with keyserver
- track work assignments to prevent flooding with bogus results (PKI signing)
- report near/false positives and check the distribution
  - http://www.distributed.net/source/specs/opcodeauth.html

# Anti cheat measures

- verify by double/triple checking
- verifiy a distinguished criteria
  - http://crypto.stanford.edu/%7Epgolle/papers/distr.html
- some projects don’t need anti cheat measures

# Outlook

- Anti cheat measures
- 100% Open Source
- New projects
  - ECC
  - OGRng
- Open and extensible protocols and APIs

# Thank You

http://www.distributed.net/download/