

Speed Up Your Cracker “Distributed Password Cracking!”

Presented By DaemonFox
IDSECCONF 2008

Issue???

- Autentikasi
- Username / Password
- Hash password
 - ✓ MD5 (Message Digest 5)
 - ✓ SHA1 (Secure Hash Algorithm 1)
 - ✓ ??
- Kesalahan umum
 - ✓ Kualitas password
 - ✓ Lupa password

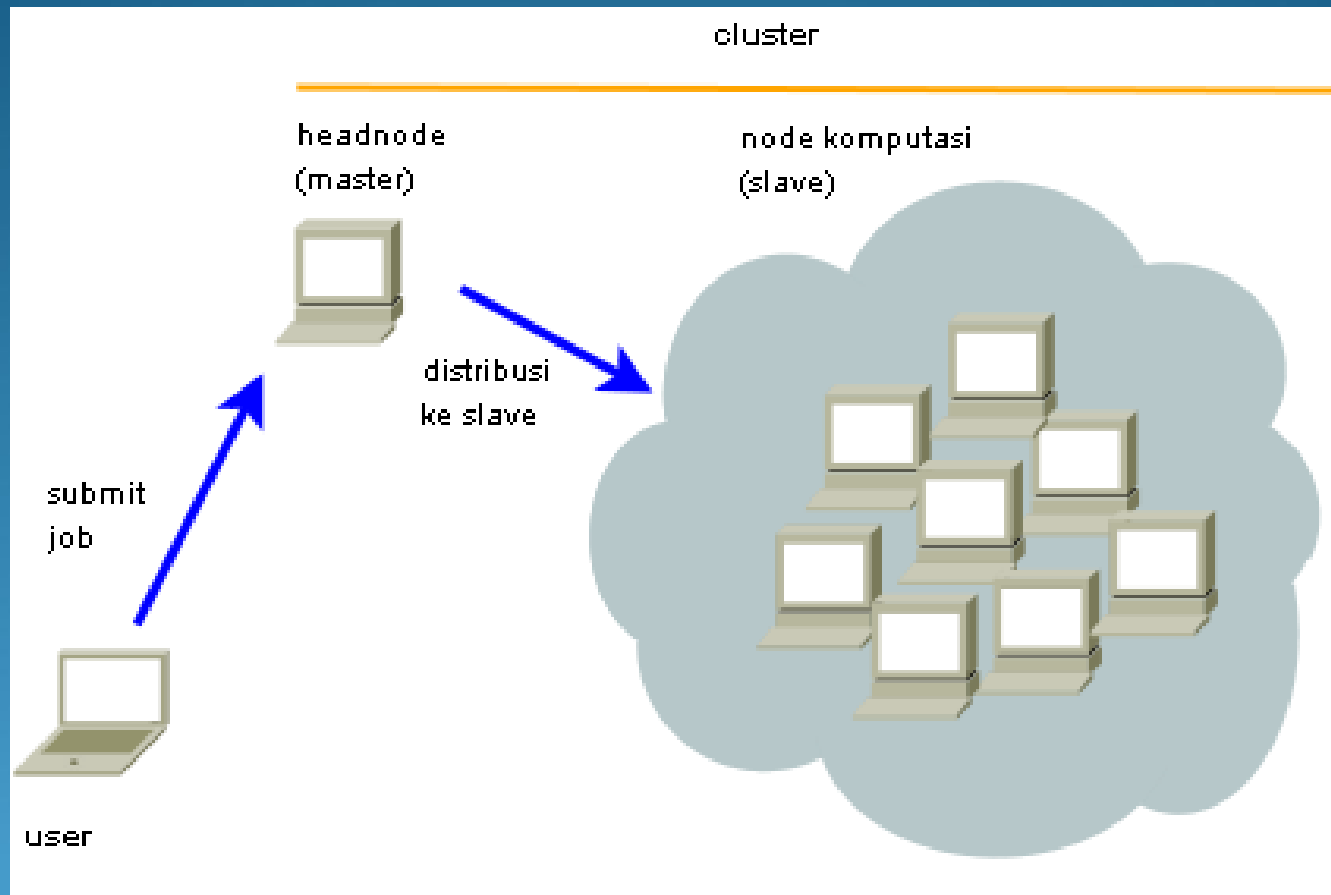
Password Cracking???

- Proses *recovery* password dari *tempat dan/atau cara* penyimpanan yang aman, dari *chipper/encrypted* menjadi *plaintext*
- Metode cracking
 - ✓ Guessing
 - ✓ Wordlist
 - ✓ Brute Force
- Well known password cracker : John The Ripper (JTR), THC-Hydra, Medusa

Distributed Password Cracking???

- Proses password cracking menggunakan beberapa komputer dalam cluster
- High speed password cracking with high performance computing 😊
- Hemat waktu, lebih efektif dan efisien

Computer Cluster



Distributed Password Cracker

- Well known distributed password cracker
 - ✓ John The Ripper + Condor
 - ✓ John The Ripper + Djohn
 - ✓ John The Ripper With MPI Support
 - ✓ Medussa, Ingat bukan medusa!
 - ✓ ???

Requirement

- Message Passing Interface (MPI)
- Local Area Multicomputer (LAM)
- Password cracker dengan dukungan MPI
- John The Ripper MPI
- Develop your own password cracker!

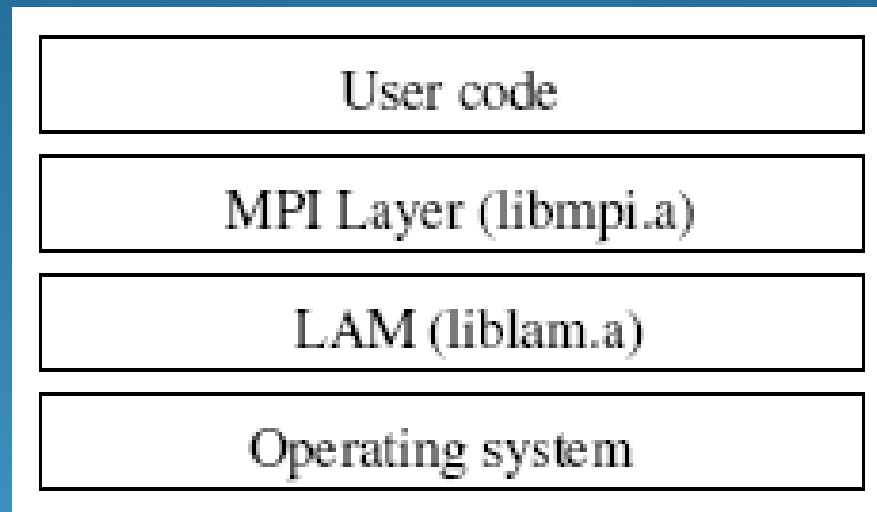
MPI

- Fungsi API yang digunakan untuk pemrograman parallel
- Standar bagi komunikasi antar proses pada pemrograman parallel yang berjalan pada sistem terdistribusi
- MPI telah dikembangkan pada bahasa pemrograman fortran, C, C++, dan Perl
- <http://www.mpi-forum.org>

LAM

- LAM merupakan salah satu aplikasi penyedia library MPI dan kompiler MPI
- Daemon-based process, pada proses distribusi “message” antar node di cluster
- Support untuk kondisi sistem dan jaringan yang heterogen serta bisa diintegrasikan dengan teknologi grid
- <http://www.lam-mpi.org>

Arsitektur LAM/MPI



John With MPI

- John The Ripper dengan dukungan proses cracking paralel pada komputasi terdistribusi
- Proses distribusi oleh MPI disupport oleh OpenMPI, MPICH, dan LAM/MPI
- <http://www.bindshell.net/tools/johntheripper>

Our Cluster

- Equipment
 - ✓ 15 * HP ML 110 Pentium 4 Dual Core CPU 3.00GHz
 - ✓ 15 * Memory 1 GB
 - ✓ OS : Rock Cluster Linux ([http:// www.rockclusters.org](http://www.rockclusters.org))

Hasil Benchmark

- Cracking single processor

```
Benchmarking: FreeBSD MD5 [32/32]... DONE
Raw:      4251 c/s real, 8502 c/s virtual

Benchmarking: OpenBSD Blowfish (x32) [32/32]... DONE
Raw:      216 c/s real, 425 c/s virtual
```

- Cracking 20 processor pada 10 nodes PC

```
Benchmarking: FreeBSD MD5 [32/32]... DONE
Raw:      164359 c/s real, 168574 c/s virtual

Benchmarking: OpenBSD Blowfish (x32) [32/32]... DONE
Raw:      8289 c/s real, 8511 c/s virtual
```

- Speed cracking FreeBSD MD5 ~ 39x lebih cepat
- Speed cracking OpenBSD Blowfish ~ 39x lebih cepat

Demo

Discussion?? Q&A

Thank You