

Password security

First of all thank you to

- OpenBSD project for producing a nice OS with amd64 support
- Alec Muffet for writing crack
- Solar Designer for John the Ripper

Anyone else that have contributed to those projects :-)

John the Ripper for fun and profit

I have used the famous Alec Muffet Crack program for years and with great pleasure helped people see how bad passwords make security crumble. Since then I have been wanting to try out John the Ripper, but only recently found the time to try out John on my machines.

I bought a new machine for OpenBSD/amd64 work and I have my old OpenBSD/i386 build server - but they are quite comparable and below you will find some interesting things to note about John the Ripper running on them.

Hardware - Fluffy and Sylvester

The two servers used are small amd64 based systems using hardware found in ordinary office systems - note that they are not specialized in any way, not overclocked, not even high-end systems! Dmesg output from the two systems:

```
hlk@fluffy:hlk$ dmesg | head
OpenBSD 3.9-current (RAID) #0: Mon May 29 19:54:13 CEST 2006
root@fluffy.kramse.dk:/sys/arch/i386/compile/RAID
cpu0: AMD Athlon(tm) 64 Processor 3200+ ("AuthenticAMD" 686-class,
1024KB L2 cache) 2.01 GHz
cpu0: FPU,V86,DE,PSE,TSC,MSR,PAE,MCE,CX8,APIC,SEP,MTRR,PGE,MCA,CMOV,PAT,
PSE36,CFLUSH,MMX,FXSR,SSE,SSE2
real mem = 804024320 (785180K)
avail mem = 725032960 (708040K)
using 4256 buffers containing 40304640 bytes (39360K) of memory
mainbus0 (root)
bios0 at mainbus0: AT/286+(00) BIOS, date 11/27/03, BIOS32 rev. 0 @
0xf0010,
SMBIOS rev. 2.3 @ 0xf0520 (65 entries)
bios0: To Be Filled By O.E.M. To Be Filled By O.E.M.
hlk@sylvester:hlk$ dmesg | head
OpenBSD 3.9-current (GENERIC) #583: Mon Jun 12 01:20:37 MDT 2006
deraadt@amd64.openbsd.org:/usr/src/sys/arch/amd64/compile/GENERIC
real mem = 536408064 (523836K)
avail mem = 447954944 (437456K)
using 13147 buffers containing 53850112 bytes (52588K) of memory
mainbus0 (root)
bios0 at mainbus0: SMBIOS rev. 2.2 @ 0xf0000 (30 entries)
```

Default Publication

```
bios0: Shuttle Inc SN95V30
cpu0 at mainbus0: (uniprocessor)
cpu0: AMD Athlon(tm) 64 Processor 3500+, 2211.01 MHz
```

The newest one is Sylvester with 2.2GHz and it is a nice little shuttle system - perfect for a home server. The biggest difference from these two systems - with regards to raw CPU power and password cracking is that Fluffy is used as an OpenBSD/i386 build server while Sylvester is running as an OpenBSD/amd64 build server.

Introducing John the Ripper

John the Ripper is an extremely fast password cracker which is famous for being able to crack passwords. It can be found at the address: <http://www.openwall.com/john/> I decided to install john from the OpenBSD ports, as the ports maintainer has chosen two nice targets, namely openbsd-x86-mmxx and openbsd-x86-64 both which seem to run well.

Speed comparison

Without further delay - here is the output from john -test runs from Fluffy and Sylvester with the above OpenBSD versions.

```
hlk@fluffy:hlk$ john -test
Benchmarking: Traditional DES [64/64 BS MMX]... DONE
Many salts: 780736 c/s real, 780736 c/s virtual
Only one salt: 704843 c/s real, 704843 c/s virtual
Benchmarking: BSDI DES (x725) [64/64 BS MMX]... DONE
Many salts: 26086 c/s real, 26086 c/s virtual
Only one salt: 25612 c/s real, 25612 c/s virtual
Benchmarking: FreeBSD MD5 [32/32]... DONE
Raw: 5921 c/s real, 5933 c/s virtual
Benchmarking: OpenBSD Blowfish (x32) [32/32]... DONE
Raw: 303 c/s real, 303 c/s virtual
Benchmarking: Kerberos AFS DES [48/64 4K MMX]... DONE
Short: 147723 c/s real, 147723 c/s virtual
Long: 504130 c/s real, 504130 c/s virtual
Benchmarking: NT LM DES [64/64 BS MMX]... DONE
Raw: 5779K c/s real, 5779K c/s virtual
```

and Sylvester running john -test

```
hlk@sylvester:hlk$ john -test
Benchmarking: Traditional DES [64/64 BS]... DONE
Many salts: 735653 c/s real, 740103 c/s virtual
Only one salt: 678335 c/s real, 676979 c/s virtual
Benchmarking: BSDI DES (x725) [64/64 BS]... DONE
Many salts: 23134 c/s real, 23367 c/s virtual
Only one salt: 22623 c/s real, 22668 c/s virtual
Benchmarking: FreeBSD MD5 [32/64 X2]... DONE
Raw: 5297 c/s real, 5351 c/s virtual
Benchmarking: OpenBSD Blowfish (x32) [32/64]... DONE
Raw: 357 c/s real, 358 c/s virtual
Benchmarking: Kerberos AFS DES [48/64 4K]... DONE
```

Default Publication

```
Short: 305207 c/s real, 307045 c/s virtual
Long: 825536 c/s real, 830509 c/s virtual
Benchmarking: NT LM DES [64/64 BS]... DONE
Raw: 6232K c/s real, 6245K c/s virtual
```

It seems that even though Fluffy has a weaker CPU the software is better tuned to some algorithms like DES, while the newer 2.2GHz CPU is faster on other algorithms. I have no explanation - but I would recommend running OpenBSD/amd64 if you have that athlons. I decided that the difference is so small and the number of cracks per second is good enough for now.

Make it easy

Being lazy is a virtue and I dont want to spend time remembering how to start John from time to time and I made this small Makefile:

```
h1k@sylvester:pwd$ cat Makefile
JOHN=/usr/local/share/john/
single:
john -single passwd
word:
john -rules -wordlist:openwall-wordlists-all.lst passwd
long:
john -incremental:all passwd
show:
john -show passwd | less
```

Then I just concatenate password files into passwd and run make single, make word and then make long - if I really need those last 3% of the passwords that aren't cracked by the first two make targets :-)

Practical use

Yes, there is a practical use for passwords crackers and you should try running John on password files on systems you administer. When you are sufficiently scared then go on and implement some password rules - like cracklib. Without enforced rules to enforce the selection of strong passwords most people will choose bad passwords.