Zabezpečená data

Radek Hranický
Lukáš Zobal
Vojtěch Večeřa

5. 6. 2016

Cíle skupiny

Vytvořit řešení pro obnovu hesel, které bude:

- Podporovat GPU akceleraci (NVIDIA + AMD)
- Bude fungovat distribuovaně
- Nabídne dostatečný výkon
- Efektivně využívat výpočetní prostředky
- Škálovatelnost se bude blížit lineární
- Dokáže se přizpůsobit změnám v síti i za běhu
- Bude dostatečně bezpečné vůči útokům
- Bude jednoduše ovladatelné pomocí GUI

Řešení z projektu Sec6Net

Nástroj Wrathion

- Windows / Linux
- Podpora formátů MS Office, PDF, ZIP, 7z, RAR
- GPU akcelerace (OpenCL)
- Podpora Unicode

Nevýhody:

- Nelze používat distribuovaně
- Neintuitivní ovládání
- Nedosahuje rychlosti nástroje Hashcat

Systém Fitcrack

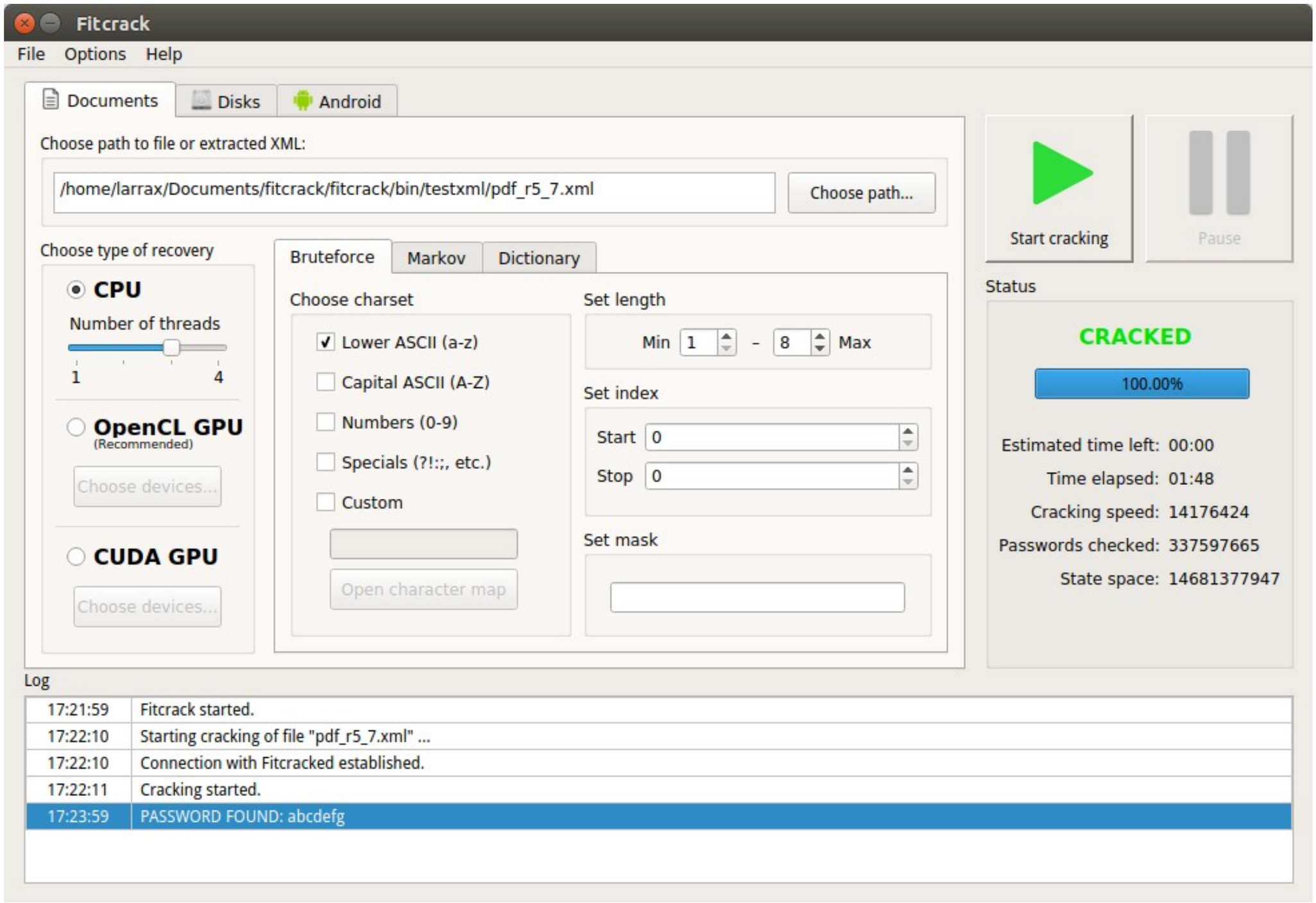
- Využívá platformy BOINC
- Schopen fungovat samostatně i distribuovaně
- Princip klient-server
- Lze provozovat v síti LAN nebo v Internetu
- Lze provozovat více výpočtů současně
- Je možno připojovat / odpojovat uzly za běhu výpočtu
- Odolnost vůči výpakům v síti, změně výkonu, apod.

Fitcrack na jednom stroji

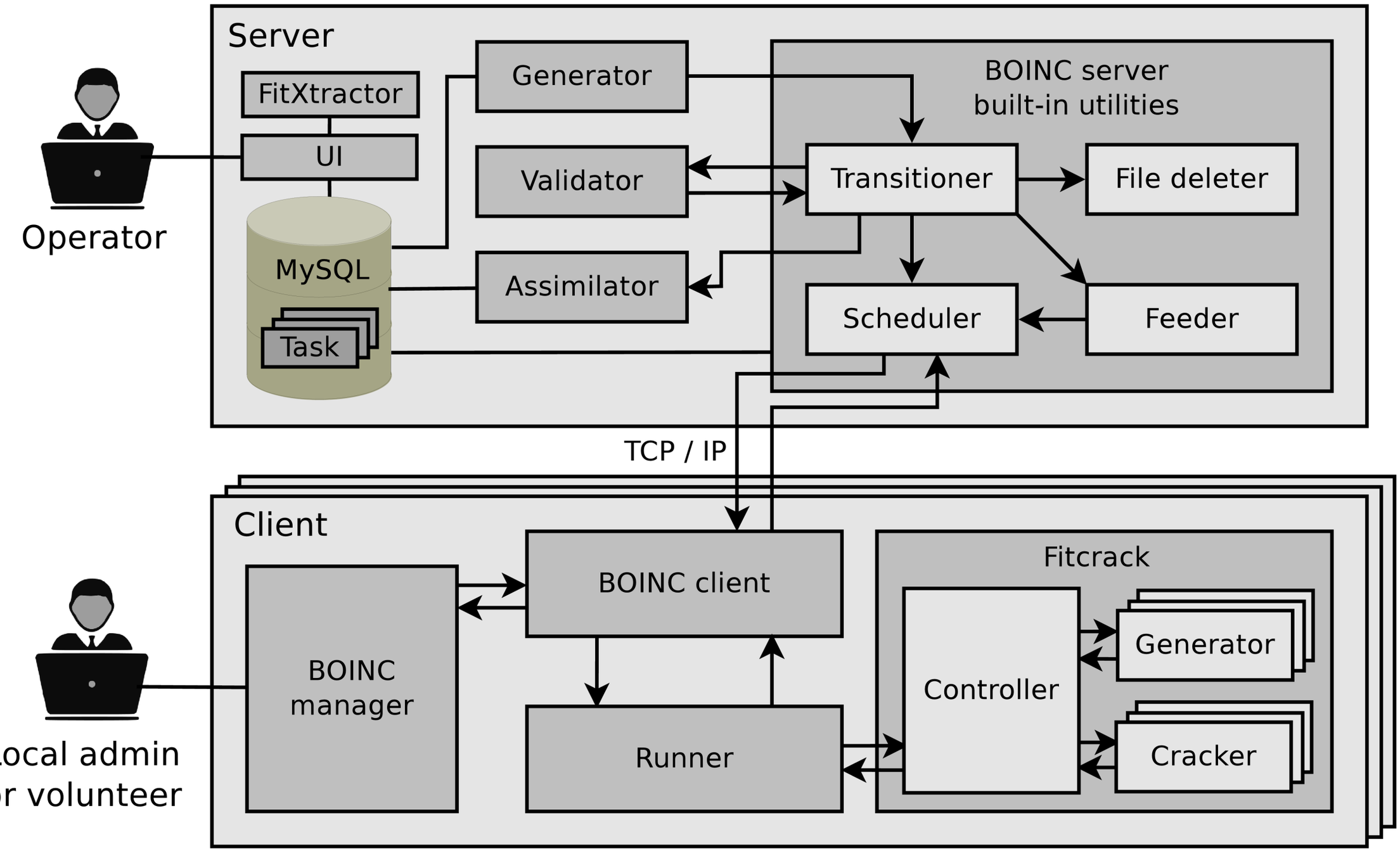
- Podobně jako Wrathion lze použít na jedné stanici jako samostatný nástroj
- Ovládání přes příkazový řádek nebo uživatelsky přívětivější GUI

```
Done: 3.39% | 282959951 of 8353082581 | Speed: 37146478 p/s
Done: 3.41% | 284945261 of 8353082581 | Speed: 38898221 p/s
Done: 3.55% | 296276628 of 8353082581 | Speed: 33367267 p/s
Done: 3.59% | 299880183 of 8353082581 | Speed: 37660435 p/s
Done: 3.68% | 307590572 of 8353082581 | Speed: 34626096 p/s
Done: 3.71% | 310172479 of 8353082581 | Speed: 30248046 p/s
Done: 3.82% | 318885501 of 8353082581 | Speed: 35955734 p/s
Done: 3.82% | 318885501 of 8353082581 | Speed: 27045164 p/s
Done: 3.92% | 327596029 of 8353082581 | Speed: 28070569 p/s
Done: 3.95% | 330228055 of 8353082581 | Speed: 32362294 p/s
Done: 4.01% | 335315792 of 8353082581 | Speed: 35144308 p/s
Done: 4.07% | 340385452 of 8353082581 | Speed: 27910864 p/s
Total time spent by cracking: 70.01 s
Password found: abcdefg
ihranicky@pchranicky:~/fitcrack/bin$
```

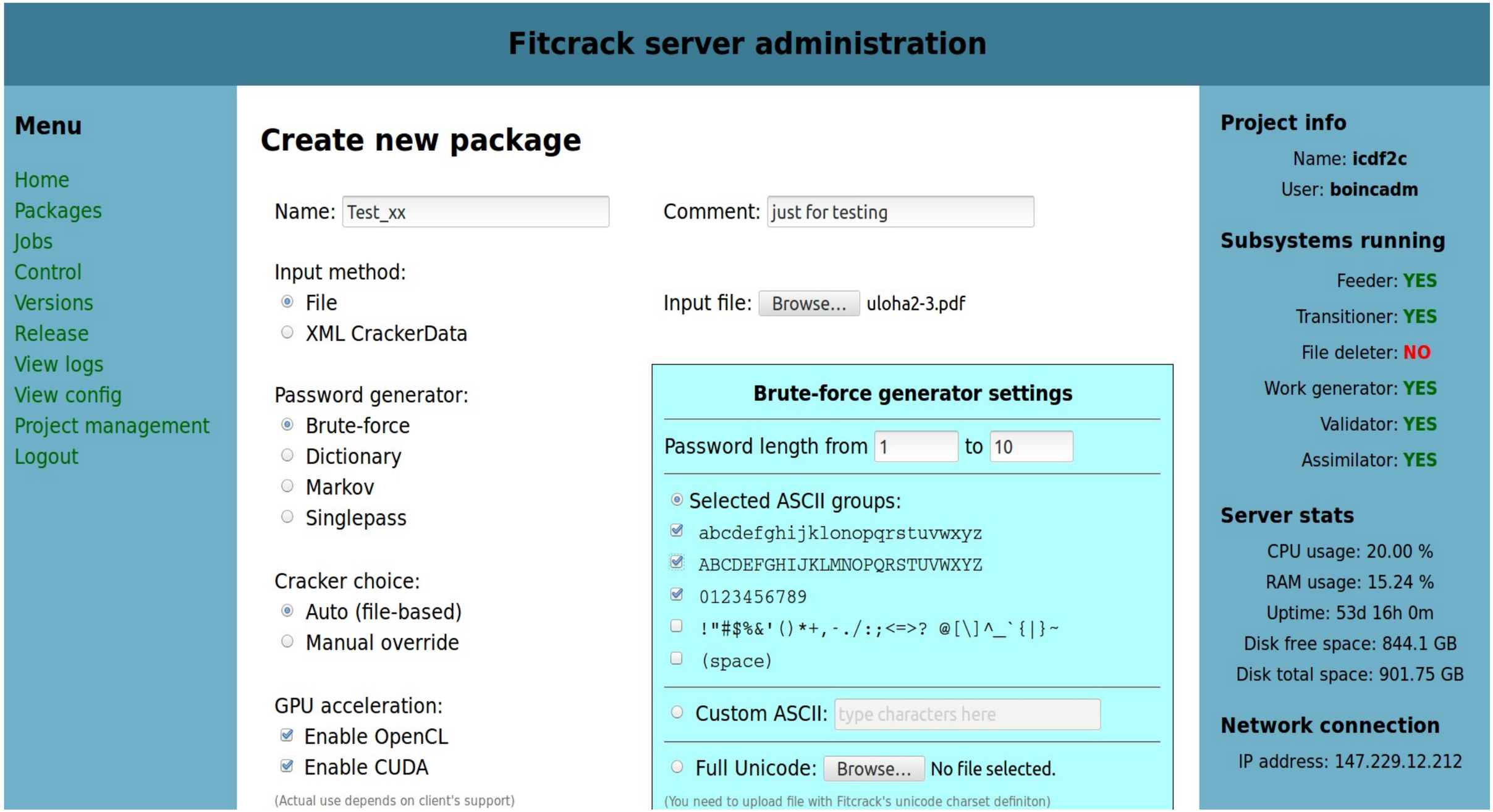
Fitcrack na jednom stroji



Fitcrack – distribuované řešení



Fitcrack – strana serveru



Fitcrack – strana serveru

host ID	IP address	name	RAC	total credit	CPU	OS
3	127.0.1.1	martin-HP	10.56	112.0	GenuineIntel Intel(R) Core(TM) i5-2410M CPU @ 2.30GHz [Family 6 Model 42 Stepping 7]	Linux 3.19.0-56-generic
4	127.0.1.1	p311	23.46	266.4	GenuineIntel Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz [Family 6 Model 26 Stepping 5]	Linux 4.2.0-42-generic
5	127.0.1.1	radek-ntb	0.08	34.2	GenuineIntel Intel(R) Core(TM) i7-4700MQ CPU @ 2.40GHz [Family 6 Model 60 Stepping 3]	Linux 3.13.0-86-generic
6	127.0.1.1	pchranicky	0.54	5.4	GenuineIntel Intel(R) Core(TM) i3-4330 CPU @ 3.50GHz [Family 6 Model 60 Stepping 3]	Linux 3.13.0-57-generic
10	10.10.10.102	h02	86.95	969.9	GenuineIntel Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz [Family 6 Model 23 Stepping 10]	Linux 2.6.32-504.8.1.el6.x86_64
11	10.10.10.103	h03	79.84	999.7	GenuineIntel Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz [Family 6 Model 23 Stepping 10]	Linux 2.6.32-504.8.1.el6.x86_64
12	127.0.0.1	localhost.localdomain	175.36	3275.5	GenuineIntel Intel(R) Core(TM) i5-4460 CPU @ 3.20GHz [Family 6 Model 60 Stepping 3]	Linux 2.6.32-573.3.1.el6.x86_64
13	10.10.10.104	h04	88.16	996.5	GenuineIntel Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz [Family 6 Model 23 Stepping 10]	Linux 2.6.32-504.8.1.el6.x86_64
14	10.10.10.105	h05	86.92	968.0	GenuineIntel Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz [Family 6 Model 23 Stepping 10]	Linux 2.6.32-504.8.1.el6.x86_64
15	10.10.10.106	h06	85.19	946.7	GenuineIntel Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz [Family 6 Model 23 Stepping 10]	Linux 2.6.32-504.8.1.el6.x86_64
16	10.10.10.101	h01	87.89	1003.3	GenuineIntel Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz [Family 6 Model 23 Stepping 10]	Linux 2.6.32-504.8.1.el6.x86_64
17	10.10.10.101	h01	6.51	66.9	GenuineIntel Intel(R) Core(TM) i5-4460 CPU @ 3.20GHz [Family 6 Model 60 Stepping 3]	Linux 2.6.32-573.3.1.el6.x86_64
18	10.10.10.102	h02	187.98	3223.7	GenuineIntel Intel(R) Core(TM) i5-4460 CPU @ 3.20GHz [Family 6 Model 60 Stepping 3]	Linux 2.6.32-573.3.1.el6.x86_64
						Linux 2.6.32-573.3.1.el6.x86_64
						Linux 2.6.32-573.3.1.el6.x86_64
						Linux 2.6.32-573.3.1.el6.x86_64
						Linux 2.6.32-573.3.1.el6.x86_64
						Linux 2.6.32-573.3.1.el6.x86_64
						Linux 2.6.32-573.3.1.el6.x86_64
						Linux 2.6.32-573.3.1.el6.x86_64
						Linux 2.6.32-573.3.1.el6.x86_64
						Linux 2.6.32-573.3.1.el6.x86_64
						Linux 2.6.32-573.3.1.el6.x86_64
						Linux 2.6.32-573.3.1.el6.x86_64
						Linux 2.6.32-573.3.1.el6.x86_64
						Linux 2.6.32-573.3.1.el6.x86_64
						Linux 2.6.32-573.3.1.el6.x86_64
						Linux 2.6.32-573.3.1.el6.x86_64

Query: **select * from result limit 20**

56128 records match the query. Displaying 1 to 20.

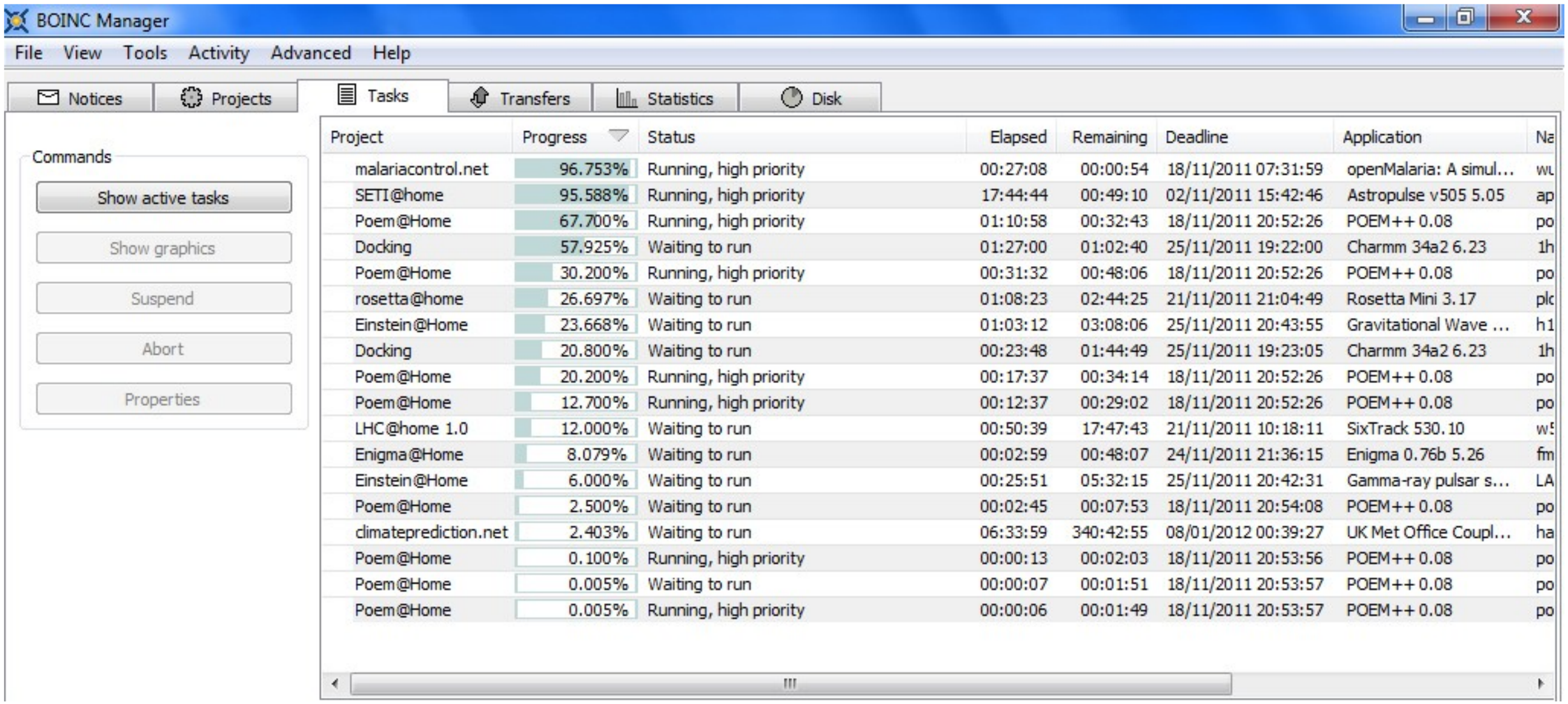
Next 20

Summary | More detail | Return to main admin page

result ID	WU ID	server state	outcome	client state	validate state	delete state	exit status	host (user)	app ver	received *or* deadline *or* created	CPU hours	granted credit
1	16	Pozdě [5]	Úspěšně dokončeno [1]	Hotovo [5]	Validní [1]	Deleted	0 (0x0)	31 (l307)	ICDF2C v0.26 x86_64-pc-linux-gnu (25)	7 Apr 2016, 2:43:44 UTC	0.0	0.063
2	13	Pozdě [5]	Úspěšně dokončeno [1]	Hotovo [5]	Validní [1]	Deleted	0 (0x0)	28 (l307)	ICDF2C v0.26 x86_64-pc-linux-gnu (25)	7 Apr 2016, 2:43:53 UTC	0.0	0.045
3	2	Pozdě [5]	Úspěšně dokončeno [1]	Hotovo [5]	Validní [1]	Deleted	0 (0x0)	17 (disabled)	ICDF2C v0.26 x86_64-pc-linux-gnu (25)	7 Apr 2016, 2:44:00 UTC	0.0	0.052
4	11	Pozdě [5]	Úspěšně dokončeno [1]	Hotovo [5]	Validní [1]	Deleted	0 (0x0)	26 (l307)	ICDF2C v0.26 x86_64-pc-linux-gnu (25)	7 Apr 2016, 2:44:04 UTC	0.0	0.052
5	17	Pozdě [5]	Úspěšně dokončeno [1]	Hotovo [5]	Validní [1]	Deleted	0 (0x0)	32 (l307)	ICDF2C v0.26 x86_64-pc-linux-gnu (25)	7 Apr 2016, 2:44:10 UTC	0.0	0.051
6	5	Pozdě [5]	Úspěšně dokončeno [1]	Hotovo [5]	Validní [1]	Deleted	0 (0x0)	20 (l307)	ICDF2C v0.26 x86_64-pc-linux-gnu (25)	7 Apr 2016, 2:44:12 UTC	0.0	0.049
7	10	Pozdě [5]	Úspěšně dokončeno [1]	Hotovo [5]	Validní [1]	Deleted	0 (0x0)	25 (l307)	ICDF2C v0.26 x86_64-pc-linux-gnu (25)	7 Apr 2016, 2:44:14 UTC	0.0	0.052
8	29	Pozdě [5]	Úspěšně dokončeno [1]	Hotovo [5]	Validní [1]	Ready to delete	0 (0x0)	31 (l307)	ICDF2C v0.26 x86_64-pc-linux-gnu (25)	7 Apr 2016, 2:44:28 UTC	0.0	0.029
9	4	Pozdě [5]	Chyba při validaci [6]	Hotovo [5]	Neplatné [2]	Deleted	0 (0x0)	19 (l307)	ICDF2C v0.26 x86_64-pc-linux-gnu (25)	7 Apr 2016, 2:44:49 UTC	0.0	---
10	46	Pozdě [5]	Úspěšně dokončeno [1]	Hotovo [5]	Validní [1]	Deleted	0 (0x0)	32 (l307)	ICDF2C v0.26 x86_64-pc-linux-gnu (25)	7 Apr 2016, 2:45:17 UTC	0.0	0.051
11	31	Pozdě [5]	Úspěšně dokončeno [1]	Hotovo [5]	Validní [1]	Deleted	0 (0x0)	17 (disabled)	ICDF2C v0.26 x86_64-pc-linux-gnu (25)	7 Apr 2016, 2:45:19 UTC	0.0	0.056
12	39	Pozdě [5]	Úspěšně dokončeno [1]	Hotovo [5]	Validní [1]	Deleted	0 (0x0)	25 (l307)	ICDF2C v0.26 x86_64-pc-linux-gnu (25)	7 Apr 2016, 2:45:21 UTC	0.0	0.052
13	34	Pozdě [5]	Úspěšně dokončeno [1]	Hotovo [5]	Validní [1]	Deleted	0 (0x0)	20 (l307)	ICDF2C v0.26 x86_64-pc-linux-gnu (25)	7 Apr 2016, 2:45:21 UTC	0.0	0.051
14	42	Pozdě [5]	Úspěšně dokončeno [1]	Hotovo [5]	Validní [1]	Deleted	0 (0x0)	28 (l307)	ICDF2C v0.26 x86_64-pc-linux-gnu (25)	7 Apr 2016, 2:45:23 UTC	0.0	0.046
15	40	Pozdě [5]	Úspěšně dokončeno [1]	Hotovo [5]	Validní [1]	Deleted	0 (0x0)	26 (l307)	ICDF2C v0.26 x86_64-pc-linux-gnu (25)	7 Apr 2016, 2:45:23 UTC	0.0	0.052
16	33	Pozdě [5]	Úspěšně dokončeno [1]	Hotovo [5]	Validní [1]	Deleted	0 (0x0)	19 (l307)	ICDF2C v0.26 x86_64-pc-linux-gnu (25)	7 Apr 2016, 2:45:24 UTC	0.0	0.047
17	45	Pozdě [5]	Úspěšně dokončeno [1]	Hotovo [5]	Validní [1]	Deleted	0 (0x0)	31 (l307)	ICDF2C v0.26 x86_64-pc-linux-gnu (25)	7 Apr 2016, 2:45:24 UTC	0.0	0.064

Fitcrack – strana klienta

- Na cílovou stanici stačí nainstalovat BOINC client
- Automaticky: stažení/aktualizace binárek, úloh, ...



Podpora formátů

Format	Version	Encryption	Verification	CPU	OpenCL	CUDA
PDF	1.1 - 1.4 (Acrobat 5)	RC4 40-bit	MD5, RC4	YES	YES	YES
	1.4 (Acrobat 5)	RC4 128-bit	MD5, RC4	YES	YES	YES
	1.6 (Acrobat 6)	AES 128-bit	MD5, RC4	YES	YES	YES
	1.7 Extension Level 3 (Acrobat 9)	AES 256-bit	SHA-256	YES	YES	YES
	1.7 Extension Level 8 - 2.0	AES 256-bit	SHA-256, SHA-384, SHA-512, AES-128-CBC	in development		
ZIP	ZIP 2.0 Legacy (PKZIP)	PKZIP stream cipher	PKZIP stream cipher, CRC-32	YES	YES	YES
	Strong encryption (WinZIP)	AES 128/192/256-bit	AES 128/192/256-bit, PBKDF2, SHA1	YES	YES	YES
	ZIP 5.2+ (SecureZIP) with AES	AES 128/192/256-bit	AES 128/192/256-bit, CRC-32	YES	YES	YES
7z	7-Zip	7zAES 256-bit	7zAES 256-bit, SHA-256, LZMA for decompression	YES	YES	NO
RAR	Version 3	AES-128-CBC	SHA1, CRC	YES	YES	NO
	Version 3 - uncompressed	AES-128-CBC	SHA1, CRC	YES	YES	NO
	Version 3 - encrypted header	AES-128-CBC	SHA1	YES	YES	NO
	Version 5	AES-256-CBC	BKPDF2-HMAC-SHA-256	YES	YES	NO
DOC, XLS	97-2000	RC4 40-bit	MD5, RC4	YES	YES	YES
	XP	RC4 128-bit	SHA1, RC4	YES	YES	YES
	2003	RC4 128-bit	SHA1, RC4	YES	YES	YES
PPT	XP	RC4 128-bit	SHA1, CRC	YES	YES	YES
	2003	RC4 128-bit	SHA1, CRC	YES	YES	YES
DOCX, XLS, PPTX	2007	AES 128/192/256-bit	SHA1, AES	YES	YES	YES
	2010	AES 128/192/256-bit	SHA1, SHA256, SHA512, AES	YES	YES	YES
	2013	AES 128/192/256-bit	SHA1, SHA256, SHA512, AES	YES	YES	YES
	2016	AES 128/192/256-bit	SHA1, SHA256, SHA512, AES	YES	YES	YES

+ OpenDocument (OpenOffice, LibreOffice), TrueCrypt, CipherShed

Řešení problému rychlosti

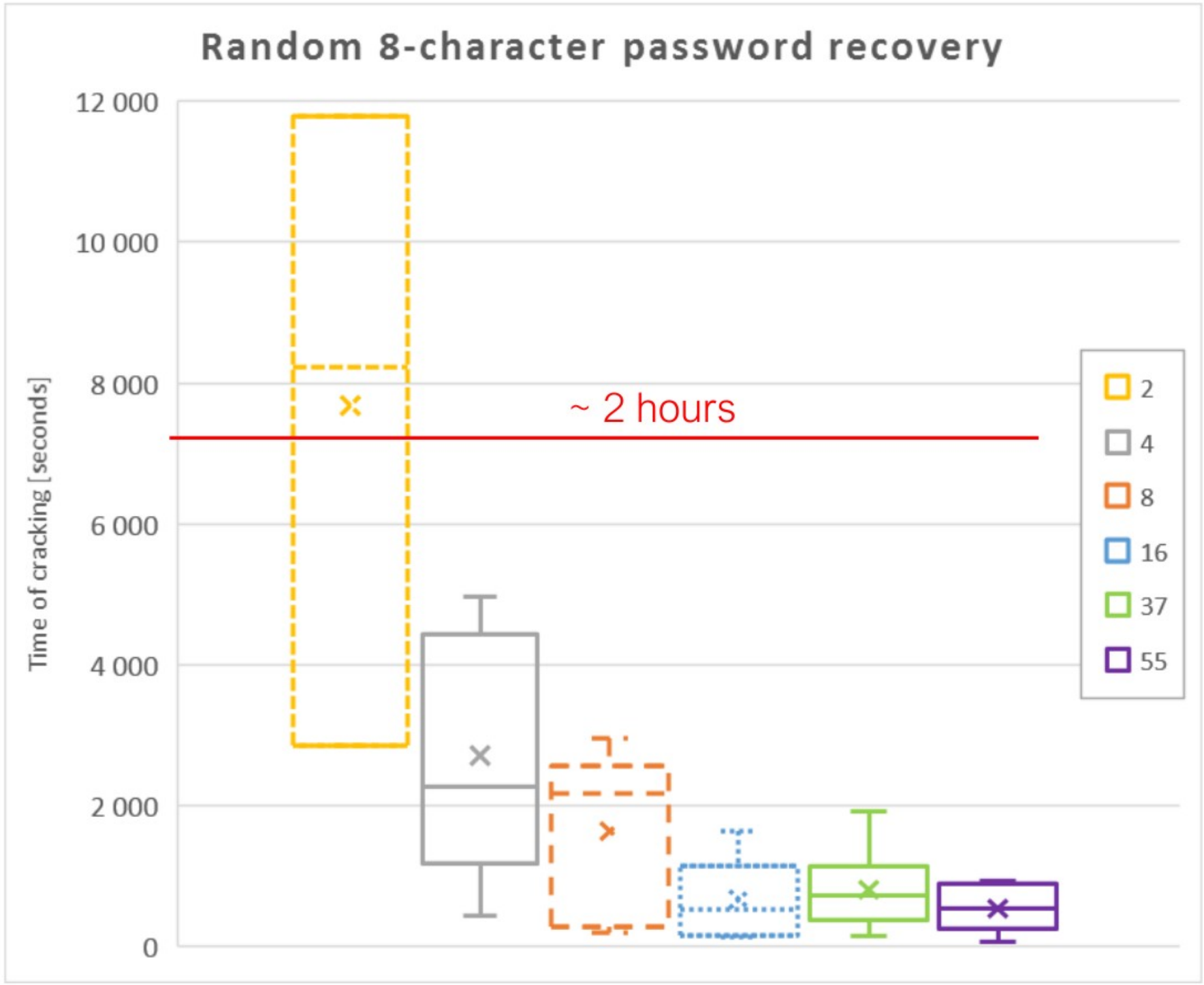
- “Pracovní” podsystém na straně klienta bude nahrazen nástrojem **Hashcat**

→ Výsledek:

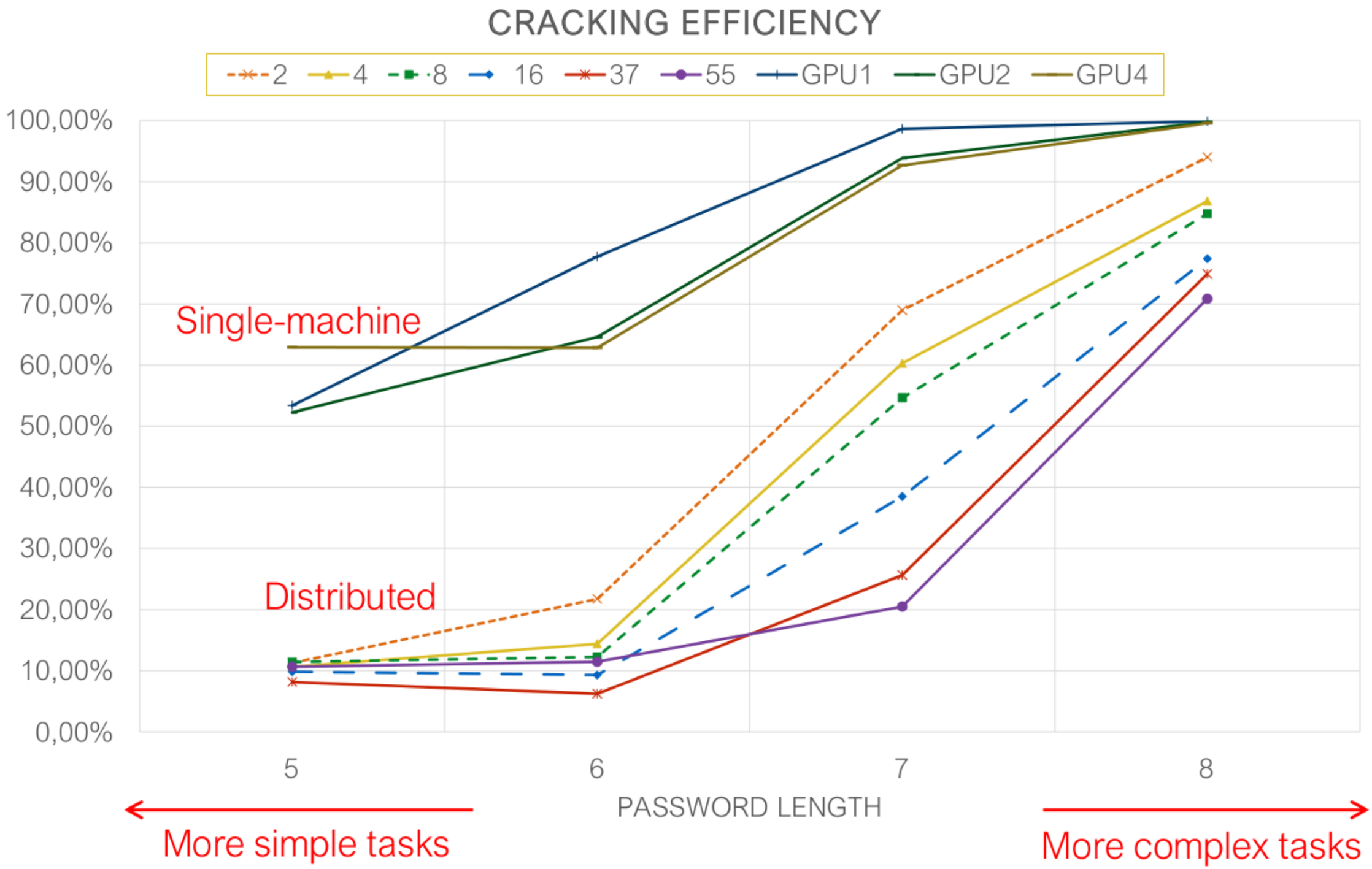
“Distrubuovaný Hashcat” při zachování všech předchozích výhod

- Na vývoji již pracujeme
- Do září 2017 očekáváme funkční prototyp

Náročnost úlohy x počet uzlů



Náročnost úlohy x počet uzlů

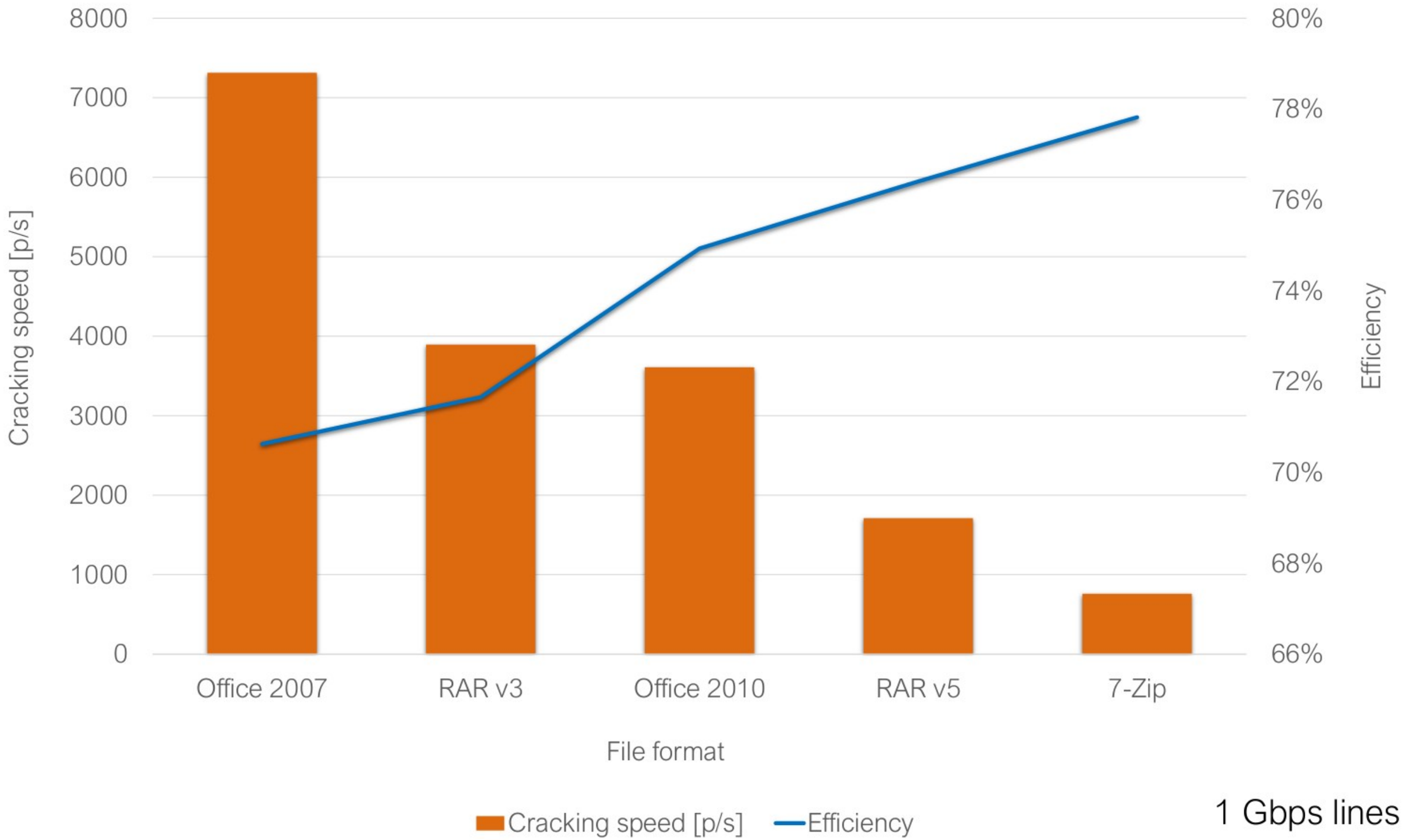


Rychlost se odvíjí od formátu...

Formát souboru	Rychlost obnovy (f) [h/s]
MS Office < 2003	2 743 900 000
MS Office 2003	2 667 600 000
MS Office 2007	1 073 500
MS Office 2010	535 400
MS Office 2013, 2016	70 884
PDF 1.1 – 1.3	3 014 200 000
PDF 1.4 – 1.6	129 300 000
PDF 1.7 (Acrobat 9)	22 938 300 000
PDF 1.7 (Acrobat 10 – 11)	256 200
RAR v3	239 200
RAR v5	290 300
WinZIP - AES	8 463 300
7-ZIP	60 750

Hashcat 3.30 – 8x GTX 1080 Ti FE

Distribuovaný slovníkový útok



Publikace, odkazy

- HRANICKÝ Radek, ZOBAL Lukáš, VEČEŘA Vojtěch a MATOUŠEK Petr. **Distributed Password Cracking in a Hybrid Environment**. In: *Security and Protection of Information 2017*, Proceedings of the Conference. Brno: Universita Obrany v Brně, 2017, s. 75-90. ISBN 978-80-7231-414-0.
- HRANICKÝ Radek, HOLKOVIČ Martin, MATOUŠEK Petr a RYŠAVÝ Ondřej. **On Efficiency of Distributed Password Recovery**. *The Journal of Digital Forensics*, Security and Law. 2016, roč. 11, č. 2, s. 79-96. ISSN 1558-7215.
- HRANICKÝ Radek, MATOUŠEK Petr, RYŠAVÝ Ondřej a VESELÝ Vladimír. **Experimental Evaluation of Password Recovery in Encrypted Documents**. In: *Proceedings of ICISSP 2016*. Roma: SciTePress - Science and Technology Publications, 2016, s. 299-306. ISBN 978-989-758-167-0.
- Web: http://fitcrack.fit.vutbr.cz/
  http://wrathion.fit.vutbr.cz/

Související BP/DP

- Obnova hesel dokumentů **Microsoft Office** s využitím GPU
- Obnova hesel archivů **ZIP** s využitím GPU
- Obnova hesel archivů **RAR**, **BZIP** a **GZIP** s využitím GPU
- Obnova hesel v **distribuovaném prostředí**
- Využití **heuristik** při obnově hesel pomocí GPU
- Útok na **šifrované diskové oddíly** s využitím GPU
- Útok na šifrování systému **Android** s využitím GPU
- Útok na šifrování dokumentů **OpenDocument** s využitím GPU
- Generování hesel na základě **pravidel**

Shrnutí

- Od projektu Sec6Net – výrazný posun směrem k použitelnému distribuovanému řešení
- Vytvořen prototyp systému Fitcrack
- Platforma BOINC pro distribuovaný výpočet
- Podpora nových formátů, GUI pro snadnou obsluhu

- Aktuálně je stále ještě problémem rychlost
- Přidáním podpory pro nástroj Hashcat očekáváme, že tento problém vyřešíme!

Dotazy?