Password Cracking
Not Just for Hackers

April 9, 2013

Why Crack Your Own Passwords?

Assess “true” risk of an infiltration (Better than simple “calculation” analysis)

Assess effectiveness of password policy & training
Internal Pen-Test (Red Team)

Test Strength of Chosen Hash Function
(Custom Applications)

Why Crack Your Own Passwords?

Telling a personal story is always more effective than citing statistics in motivating action

Which will generate more action towards implementing a multi-factor solution?

A typical attacker can do 16 billion cps, and our password policy includes 92 possible characters with 8 characters required, so…

Or…

We cracked 50% of the company passwords with a tool we built for $3,000

April 9, 2013

The Basics: Hashes & Cracking

Passwords should be stored as hashes, not plaintext

Offline cracking is different than online password attacks

Hash algorithms are different than encryption
One way
Unique fingerprint or code (hash/digest)
14a54c88dc3a2067dbc89b628de73eef

Hash tastes better with salt

April 9, 2013

The Basics: Hashes & Cracking

Common Hash Types

MD5 – not secure unless properly salted

NTLM – Windows, different than authentication protocol!

SHA1, SHA2 (SHA224, SHA256, SHA384, SHA512)

Bcrypt – Slow … which is good!

Old School vs New School

Old School

CPU

- Using main computational element of computer to … compute
- Slow: Not easily parallelized
- Still used for:
  - Slow, memory-bound hashes
  - Rare hashes – widest compatibility; easiest to port

Old School vs New School

Old School

- Rainbow tables
  - Pre-computed hashes
  - Massive speed increase over CPU
  - ~60TB for len9 NTLM
  - Unique salts = death
  - Still used:
    - Non-salted, low characters
    - Static salt (username)
    - Not necessarily dead yet

Old School vs New School

New School

GPU

- Current leading trend
- Massively parallel computation
- Power & heat concerns

Getting the Hashes

SQL Injection

System Breach

Shadow File

Windows Domain Controllers

Don't run pwcrack on your PROD systems. There are safer ways…

You just need SYSTEM hive and ntds.dit file

http://pauldotcom.com/2011/12/safely-dumping-hashes-now-avai.html

http://bernardodamele.blogspot.com/2011/12/dump-windows-password-hashes_16.html

Build or Lease (Cloud)?

Lease Cost:
$2.10/hour for 2 ancient GPUs (by GPU cracking standards)
~2.9B c/s for NTLM
&
All your passwords in the cloud

Build Cost:
~$2,000 - $2,500 per system
~16B c/s for NTLM

Do the math…or just build your own

Build Your Cracking System

April 9, 2013

Build Your Cracking System

Case, Power & Heat

- Consumer Parts – Gaming!
- Concerns: Heat, Power, Price
- Is it getting hot in here?: Airflow
- Purpose-built cases (GPGPU vs Standard)
- Chenbro RM41300-FS81

- Tyan B7015F77V4R

- 3-4 Card system: less heat, less money, more power

April 9, 2013

Build Your Cracking System

GPU

AMD

More pipelines/Special Ops

NVIDIA

Less pipelines

Newer is not always better

Cooling matters

Why not TESLA?
(optimized for floating point, crazy cost)

April 9, 2013

Build Your Cracking System

Power

7970 = 250W TDP

Lots of good, clean power

1200W is likely best

Don’t risk frying expensive cards

Build Your Cracking System

CPU & Motherboard

Just pushing data to GPUs

Processor: AMD is cheaper and sufficient

Motherboard: Ports for 4, spaced GPU cards

RAM: Don’t need much, but its cheap

April 9, 2013

Build Your Cracking System

OS & Driver

Linux

Drivers = More Work

More Cracking Tools

Other utilities prove necessary

Less Cruft

Windows

Quicker Start

Need cygwin installed

Less Cracking Tools

Least Worst Option = 12.8

April 9, 2013

Build Your Cracking System

Software

oclHashCat Suite
Fastest GPU cracker
lite & plus versions

Cryptohaze Multiforcer
Open Source
Best Distributed Cracking Support
(high latency)

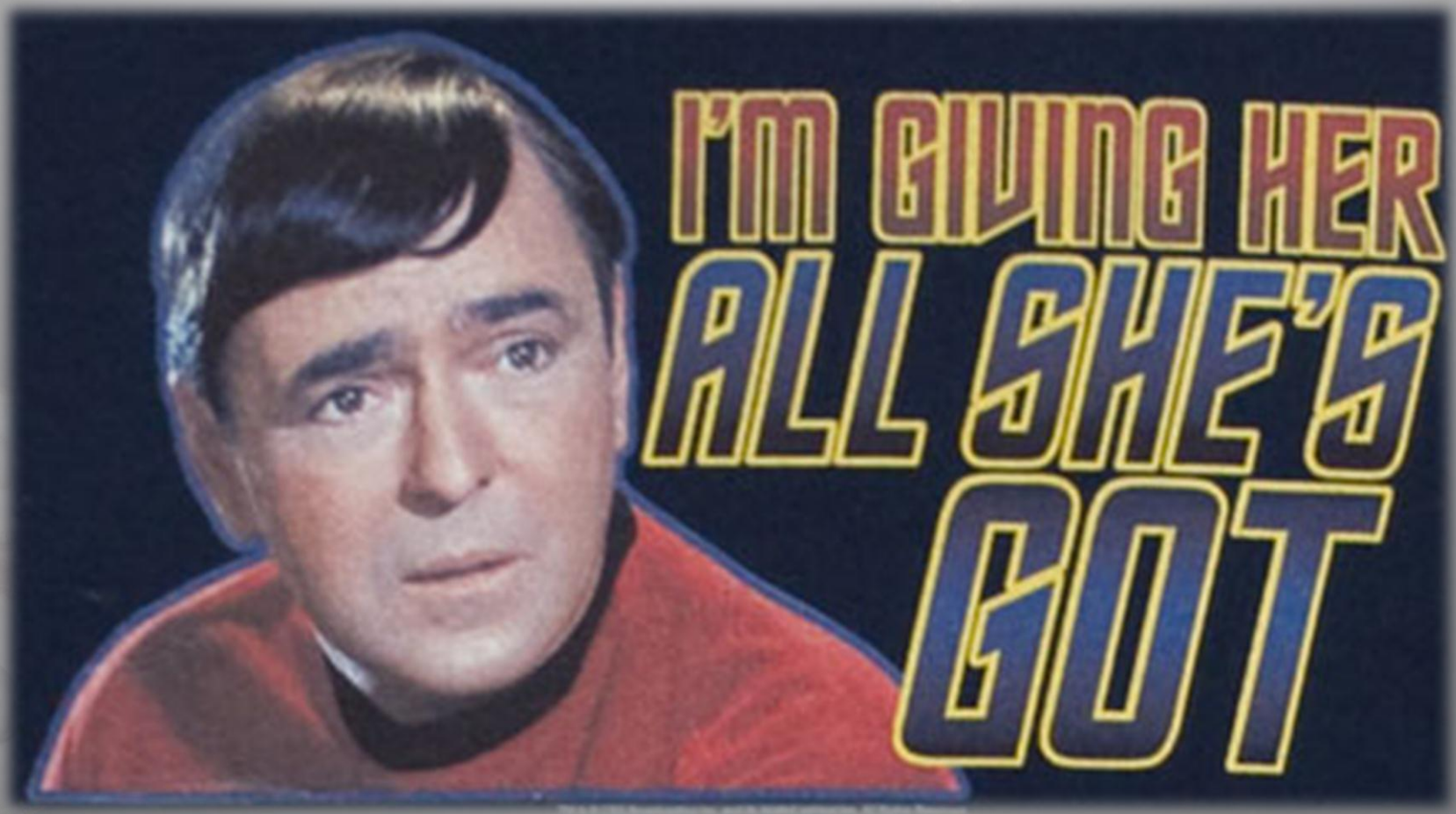
John (jtr-jumbo)
Massive hash format support
Very limited GPU ability

L0phtcrack
Enterprise Friendly

Cain
Windows Only
Simple, Basic, Quick

Build Your Cracking System

I NEED MORE POWER!



April 9, 2013

Build Your Cracking System

Distributed Cracking

Virtual CL:
Use remote systems' GPUs as if they were local
Perfect for distributed cracking clusters

http://passwords12.at.ifi.uio.no/Jeremi_Gosney_Password_Cracking_HPC_Passwords12.pdf

April 9, 2013

How to Crack

Brute-force:
Churn through entire keyspace
Not effective or practical

Mask Attack:
Refined Brute-force
example: -1 ?l?u ?1?l?l?l?l?l19?d?d
keyspace: aaaaaa1900 - Zzzzzz1999

Dictionary/Mangling/Hybrid:
Most effective…by far
Uses dictionary files
Uses mangling rules to turn password into Pa$$w0rd2013

Dictionaries

Dictionaries:
Bigger is not always better
Poor dictionary = poor results
This is the magic sauce

Where to start?
What's the purpose?
Previous breach lists
Tailor to target (company specific words etc.)

Advanced:
Maskprocessor
Website scraping
Combining dictionaries
Clean them up (tags, whitespace, duplicates etc.)

Dictionaries

Rule Sets

Name	Function	Description	Example Rule	Input Word	Output Word
Nothing	:	do nothing	:	p@ssW0rd	p@ssW0rd
Lowercase	l	Lowercase all letters	l	p@ssW0rd	p@ssw0rd
Uppercase	u	Uppercase all letters	u	p@ssW0rd	P@SSW0RD
Capitalize	c	Capitalize the first letter and lower the rest	c	p@ssW0rd	P@ssw0rd
Invert Capitalize	C	Lowercase first found character, uppercase the rest	C	p@ssW0rd	p@SSW0RD
Toggle Case	t	Toggle the case of all characters in word.	t	p@ssW0rd	P@SSw0RD
Toggle @	TN	Toggle the case of characters at position N	T3	p@ssW0rd	p@sSW0rd
Reverse	r	Reverse the entire word	r	p@ssW0rd	dr0Wss@p
Duplicate	d	Duplicate entire word	d	p@ssW0rd	p@ssW0rdp@ssW0rd
Reflect	f	Duplicate word reversed	f	p@ssW0rd	p@ssW0rddr0Wss@p
Rotate Left	{	Rotates the word left.	{	p@ssW0rd	@ssW0rdp
Rotate Right	}	Rotates the word right	}	p@ssW0rd	dp@ssW0r
Append Character	$	Append character to end	$1	p@ssW0rd	p@ssW0rd1
Prepend Character	^	Prepend character to front	^1	p@ssW0rd	1p@ssW0rd
Truncate left	[	Deletes first character	[	p@ssW0rd	@ssW0rd
Trucate right	]	Deletes last character	]	p@ssW0rd	p@assW0r
Delete @ N	DN	Deletes character at position N	D3	p@ssW0rd	p@sW0rd
Delete range	xNM	Deletes M characters, starting at position N	x02	p@ssW0rd	ssW0rd
Insert @ N	iNX	Inserts character X at position N	i4!	p@ssW0rd	p@ss!W0rd
Overwrite @ N	oNX	Overwrites character at postion N with X	o3$	p@ssW0rd	p@s$W0rd
Truncate @ N	'N	Truncate word at position N	'6	p@ssW0rd	p@ssW0
Replace	sXY	Replace all instances of X with Y	ss$	p@ssW0rd	p@$$W0rd
Purge	@X	Purge all instances of X	@s	p@ssW0rd	p@W0rd
Duplicate first N	z	Duplicates first character N times	z2	p@ssW0rd	ppp@ssW0rd

Dictionaries

Rule Sets
built-in for oclHashCat

d3ad0ne.rule
Overall Best

best64.rule
Quick & Efficient

Passwordpro.rule
Nets a few more, but…

April 9, 2013

Contact Info

Austin Appel
i@crackedyour.pw

Jenner Holden
ucant@crackmy.pw

April 9, 2013