Another Free MacWorld Platinum Pass? Yes in 2008!

Another Free MacWorld Platinum Pass? Yes in 2008! - Kurt Grutzmacher, grutztopia.jingojango.net.

- Published: date not stated
- Original: <http://grutztopia.jingojango.net/2008/01/another-free-macworld-platinum-pass-yes.html>
- Preserved from: http://grutztopia.jingojango.net/2008/01/another-free-macworld-platinum-pass-yes.html (stored) on 2026-08-16
- Licence: unknown

Content

> UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

[[image: image]]
(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhCBNB3lwKCGYh2QJzjDXjEmXGw_nlKTKUrzYtFHocxn52Lm_iuSqP7jDbN6aHCKbZtPddyjmaYGYS5Fe35XncDRxp2hVEgzKQhw88yeW7qj6m50ZFDIFFreR-ROqdrLgW1Uc0LKQ/s1600-h/MacWorld2K8-badge.jpg) Last year at this time I disclosed an issue with the IDG/MacWorld Expo registration that allowed people Free Platinum Passes (valued at $1,695). I communicated this issue with IDG the week of MacWorld and they removed all the codes, fixed the site, and said thanks. Questions were asked on how to write better code and I gave them a few tips (don't trust user input, don't give your secret codes to everyone, encryption is not one-way, etc). Did they listen?

Nope.

Why Do I Do This?

Who wants to stand in line to see the Steve Jobs keynote at MacWorld? I mean have you SEEN the lines there? Really? I want to know WHATS IN THE AIR(tm)!!!

Honestly it's academic to me. I didn't even go to the keynote. :P

Getting Your Golden (Well, Blue) Ticket:

This year the cost of Platinum Passes has gone up to $1,895. That's a lot of money but you get a lot of cool things:

- A free lunch every day
- Free ticket to the MacWorld Blast

- Seminars (MacWorld is more than just the keynote and Expo)
- Priority Access Line to the Keynote

You can see why the cost. Last year the word "CREDIT" provided a 100% discount on checkout. These are called Application Logic Flaws and aren't new attacks but they can be devastating .

Like last year IDG is passing a long list of MD5 hashes to the client browser and validating them in JavaScript before sending a request to the server -- but that's really only a problem if the codes that give the discounts exist and are easily cracked. Lets see if we can get lucky this year.

Obtaining the codes -- Same as last year:

Step 1. Navigate to the main registration page Step 2. Submit your initial data and view the source of the main registration page, search for "Priority Code" Step 3. See the JavaScript "onchange" function? It's calling "check_password()" Step 4. Search for "check_password()" and you'll find the list of valid codes in MD5 Step 5. Format the data for your cracker of choice and start cracking!

Cracking the codes:

I like John The Ripper for all my hash cracking needs. It's flexible, easy to use and affordable! There are two main methods used to crack passwords in John, using a wordlist or incrementing through a given keyspace. I always begin with a wordlist run just to kick out the quickies. The hash for "NONE" breaks but we already know that doesn't do anything for us.

Incremental mode is our next step but we know lower case letters aren't used so a quick look at the configuration file shows an external mode "Filter_LanMan" that throws everything to upper case. A quick run through doesn't net any cracked hashes unfortunately. There are still over 1,000 hashes to crack so we have to be a bit more intelligent in our cracking (or throw more machines, wait longer, get a PS3, etc).

A Brief Cracking Sidebar:

Incremental cracking can take a long time to perform. The size of your keyspace (k) and the maximum word length (l) determine the total number of permutations that have to be encrypted to check every instance (P). P=k^l. Take the benchmark cracks-per-second your machine takes (Cs), do the math (P/Cs) and you have the number of seconds it takes to run an Incremental.

For example lets make k = 69, l = 8 and Cs = 30 million:

> ((69^8)/30M) / 60 = 285,443.54 minutes (3.68 months!)

Changing l for different lengths and the time changes accordingly:

> ((69^7)/30M) / 60 = 4,136.86 minutes for 7 chars ((69^6)/30M) / 60 = 59.95 minutes for 6 chars

and so on. . . The time is cumulative and those are just my numbers. Some have found ways to increase the speed to 1 billion cracks-per-second. Until that code is released or we write our own, we have to work with clusters of machines to reach that. My little cluster of 9 nodes can do just about 60 million MD5's a second so a full 8 character run would take nearly 2 months to complete.

Now that you know the math and the big mountain ahead of us, how can we get on the gondola that takes you over half of it without much effort? The answer is simple, vendor codes and keyword masking!

Here Come The Free Codes:

Vendors receive a group of codes each to pass along to their customers, potential customers, friends, family, etc. These typically provide free Expo access but maybe they'll help trim down this mountain to something manageable. These free codes get passed around like candy so finding one takes a few Google searches. 08-G-PC189, 08-G-PC178, 08-G-PC260, do you see the pattern?

Time To Build An External Filter:

Now that we have a mask (08-x-y(n)) time to modify the john.conf accordingly:

> [Incremental:MW] File = $JOHN/lanman.chr MinLen = 6 MaxLen = 6 CharCount = 69 [List.External:MW] void filter() { int i, c; i = 0; while (c = word[i]) { // If character is lower case, convert to upper if (c >= 'a' && c <= 'z') word[i] &= 0xDF; i++; } // We know the static filter 08-?-????? // Add or remove word[]s to fit the incremental length word[9] = word[5]; word[8] = word[4]; word[7] = word[3]; word[6] = word[2]; word[5] = word[1]; word[4] = '-'; word[3] = word[0]; word[2] = '-'; word[1] = '8'; word[0] = '0'; }

With that, we run and wait...

> # john -i=MW -e=MW mw2k8.codes --format=raw-MD5 Loaded 1341 password hashes with no different salts (Raw MD5 [raw-md5 SSE2])

.. but not too long because the first code looks REALLY interesting: 08-S-STAFF. Lets try it!

Download the High Quality version.

Voila. For the second year in a row, a free Platinum Pass in less than a day.

On January 7th we noticed the MD5 hashes changed in the source code. While the special code was still listed it no longer gave a 100% discount when entered. Some codes still provide a small percentage discount and a few do provide a free expo pass. We still have 14 codes left to crack so no telling if those are any good. :)

Thanks to Josh Bernstein and Garrett Gee for reminding me MacWorld was coming up and independently confirming these findings.

Maybe next year the problem will be fixed? Anyone in a betting mood? :)
