

RE: Whitespace in passwords – From Security focus

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-09/0349.html>

From: Craig Wright (cwright_at_bdosyd.com.au)

Date: 09/22/05

Date: Thu, 22 Sep 2005 15:39:16 +1000
To: <Steve.Cummings@barclayscapital.com>

But there are new tools – These do know about the alt code. Some are commercial – some are free.

We have Dell notebooks – yes I do have a separate keyboard, but I also use the machine on the road so to speak. The Dell notebook keyboard makes alt+xxx chars VERY difficult!!!

Alt+255 is equal to ONLY logging into the system when I have an attached keyboard with keypad.

MSFT does not record the alt+xxx chars in complexity requirements (at least last time I checked) – nor for that matter spaces. Thus the complexity requirements do not enforce this without writing your own password definitions

Craig

-----Original Message-----

From: Steve.Cummings@barclayscapital.com [<mailto:Steve.Cummings@barclayscapital.com>]

Sent: 22 September 2005 3:31

To: Craig Wright; BMcAninch@PENSON.COM; pen-test@securityfocus.com

Cc: pand0ra.usa@gmail.com

Subject: Re: Whitespace in passwords – From Security focus

But the traditional cracking tools don't know anything about alt code but they do know traditional key presses

-----Original Message-----

From: Craig Wright <cwright@bdosyd.com.au>

To: Craig Wright <cwright@bdosyd.com.au>; Cummings, Steve: IT (LDN) <Steve.Cummings@barclayscapital.com>; BMcAninch@PENSON.COM <BMcAninch@PENSON.COM>; pen-test@securityfocus.com <pen-test@securityfocus.com>

CC: pand0ra.usa@gmail.com <pand0ra.usa@gmail.com>

Sent: Thu Sep 22 05:36:07 2005

Subject: RE: Whitespace in passwords – From Security focus

Myth #10: Use ALT+255 for the Strongest Possible Password

It common to see recommendations to use high-ASCII characters as the ultimate password tip. High-ASCII

SecurityFocus Penetration: RE: Whitespace in passwords – From Security focus

characters are those that cannot normally be typed on a keyboard but are entered by holding down the ALT key and typing the character's ASCII value on the numeric keypad. For example, the sequence ALT-0255 creates the character <ÿ>.

Although they are useful in some situations, you should also consider the disadvantages. First of all, holding down the ALT key and typing on the numeric keypad is something that can easily be observed by others. Second, creating such a character requires five keystrokes that must be memorized and later typed every time the password is entered. Perhaps a more effective technique would be to make your password five characters longer, which would actually make your password much stronger for the same number of keystrokes.

For example, a five-character password made up of high-ASCII characters will require 25 keystrokes to complete. With 255 possible codes for each character and five characters, the total possible combinations are 255^5 (or 1,078,203,909,375). However, a 25-character password made up of only lower-case letters has 26^{25} (or 236,773,830,007,968,000,000,000,000,000,000) possible combinations. Clearly, you are better off just making longer passwords.

Another thing to consider is that some laptop keyboards make numeric keypad input difficult and some command-line tools may not accept high-ASCII characters. For example, you can use the character ALT+0127 in Windows, but you cannot type that character at a command prompt. Conversely, I have found that some character codes such as Tabs (ALT+0009), LineFeeds (ALT+0010), and ESC (ALT+0027) can be used when setting your password from a command prompt but cannot be used in any Windows dialog boxes (which may actually be a desirable side-effect in some rare cases).

Craig

-----Original Message-----

From: Craig Wright

Sent: 22 September 2005 8:45

To: 'Steve.Cummings@barclayscapital.com'; BMcAninch@PENSON.COM; pen-test@securityfocus.com

Cc: pand0ra.usa@gmail.com

Subject: RE: Whitespace in passwords

If you are this worried and the users are capable enough – than use OTP's or certificates or something

RSA keyfobs or SKEY beat passwords hands down

Craig

-----Original Message-----

From: Steve.Cummings@barclayscapital.com [mailto:Steve.Cummings@barclayscapital.com]

Sent: 21 September 2005 5:27

To: Craig Wright; BMcAninch@PENSON.COM; pen-test@securityfocus.com

Cc: pand0ra.usa@gmail.com

Subject: RE: Whitespace in passwords

I never said that I didn't agree with you but the alt system in my book is a more useful way of protecting passwords than 14 character password etc

Regards

RE: Whitespace in passwords – From Security focus

SecurityFocus Penetration: RE: Whitespace in passwords – From Security focus

Steve Cummings
Barclays Capital
DDI 0207 773 4245

-----Original Message-----

From: Craig Wright [mailto:cwright@bdosyd.com.au]
Sent: 21 September 2005 07:32
To: Cummings, Steve: IT (LDN); BMcAninch@PENSON.COM; pen-test@securityfocus.com
Cc: pand0ra.usa@gmail.com
Subject: RE: Whitespace in passwords

John was a tool which was good a decade ago

The tools have moved on – just because not everyone here has used precomputed tables and quadratic methods does not mean that an attacker does not know of them. I am sure that Barclays Capital has enough of a presence to attract the corporate criminal type...

I reiterate – the real issue is to stop an attacker getting this info in the first place.

Secure Server plus secure client settings in group policy on a MSFT network and this is no longer an issue. "An Ounce of Prevention is worth a pound of cure"...

Craig

-----Original Message-----

From: Steve.Cummings@barclayscapital.com [mailto:Steve.Cummings@barclayscapital.com]
Sent: 21 September 2005 3:37
To: Craig Wright; BMcAninch@PENSON.COM; pen-test@securityfocus.com
Cc: pand0ra.usa@gmail.com
Subject: Re: Whitespace in passwords

Try the password of your choice with alt 255 in the middle currently things like lopht and john don't get near it

-----Original Message-----

From: Craig Wright <cwright@bdosyd.com.au>
To: Cummings, Steve: IT (LDN) <Steve.Cummings@barclayscapital.com>; BMcAninch@PENSON.COM <BMcAninch@PENSON.COM>; pen-test@securityfocus.com <pen-test@securityfocus.com>
CC: pand0ra.usa@gmail.com <pand0ra.usa@gmail.com>
Sent: Tue Sep 20 20:27:52 2005
Subject: RE: Whitespace in passwords

HI

1st it does not make them untouchable

Next, MOST applications do not accept Alt+xxx based passwords – very few users will use them as well

Do your users authenticate via a Radius systems, the web...? Any of these will not accept Alt+xxx chars.

RE: Whitespace in passwords – From Security focus

SecurityFocus Penetration: RE: Whitespace in passwords – From Security focus

Most users will have issues using this

the following does not make a very memorable password – see how often it is remembered?

!B?]?O11s

Craig

-----Original Message-----

From: Steve.Cummings@barclayscapital.com [mailto:Steve.Cummings@barclayscapital.com]

Sent: Wed 21/09/2005 2:41 AM

To: Craig Wright; BMcAninch@PENSON.COM; pen-test@securityfocus.com

Cc: pand0ra.usa@gmail.com

Subject: Re: Whitespace in passwords

Why aren't alt characters feasible alt255 is an easy one for anyone to remember and if the policy for passwords dictates the requirement then most large firms would accept this especially if it made the password in the current view untouchable for the foreseeable future

For more information about Barclays Capital, please visit our web site at <http://www.barcap.com>.

Internet communications are not secure and therefore the Barclays Group does not accept legal responsibility for the contents of this message. Although the Barclays Group operates anti-virus programmes, it does not accept responsibility for any damage whatsoever that is caused by viruses being passed. Any views or opinions presented are solely those of the author and do not necessarily represent those of the Barclays Group. Replies to this email may be monitored by the Barclays Group for operational or business reasons.

Audit your website security with Acunetix Web Vulnerability Scanner:

Hackers are concentrating their efforts on attacking applications on your website. Up to 75% of cyber attacks are launched on shopping carts, forms, login pages, dynamic content etc. Firewalls, SSL and locked-down servers are futile against web application hacking. Check your website for vulnerabilities to SQL injection, Cross site scripting and other web attacks before hackers do!
Download Trial at:

http://www.securityfocus.com/sponsor/pen-test_050831
