МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
КАФЕДРА ІНОЗЕМНИХ МОВ
ЛІНГВІСТИЧНИЙ НАВЧАЛЬНО-МЕТОДИЧНИЙ ЦЕНТР

МАТЕРІАЛИ

VIII МІЖВУЗІВСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ

КОНФЕРЕНЦІЇ

ЛІНГВІСТИЧНОГО НАВЧАЛЬНО-МЕТОДИЧНОГО ЦЕНТРУ

КАФЕДРИ ІНОЗЕМНИХ МОВ

“TO LIVE IN A SAFER WORLD”

(Суми, 28 березня 2014 року)

The eighth scientific practical student`s, postgraduate’s and teacher’s

LSNC conference

INFORMATION SECURITY: PASSWORDS

Sasha Saltysh– Sumy State University, group IN – 32
S. V. Mikhno – E L Adviser

Many people have accounts in different sites, and the problem is that hundreds of millions of passwords are being compromised by cybercriminals every year.

People finally need to understand that the Internet is a very hostile place, while online service providers need to finally start taking network security seriously.

One of the world's leading password crackers just got better and is now able to crack passwords of up to 55 characters in length and algorithms such as TrueCrypt 5.0+, LastPass and Samsung Android Password/PIN.

Hashcat is a freely available password cracker. It is clearly a dual-purpose weapon: it can be used by security auditors to stress-test company passwords, and it can be used by criminals to crack lists of stolen passwords.

What the new version of hashcat demonstrates is that size is no longer as important as it used to be – it's what the user does with the characters that matters. Length is still important; but rather than just a combination of words or phrases, it should be a mix of characters, numbers and punctuation symbols.

A few weeks ago, SplashData has announced its annual list of the 25 most common passwords:

This year, "123456" has the dubious honor of being the most common –and therefore easiest to crack – password in use on the internet.

The TOP TEN includes "qwerty," "abc123," "111111" and the ever-popular "iloveyou" – all highly susceptible to brute-forcing and cracking algorithms.

List also showed that shorter numerical passwords are coming into use, even though websites are starting to enforce stronger password policies. For example, new to this year's list are simple and easily guessable passwords like "1234" (No. 16), "12345" (No. 20) and "000000" at (No. 25).

Only four in the top 20 seem to be unlinked to numbers or other simple inspirations: “monkey,” “shadow,” “sunshine” and “princess.”

We hope that with more publicity about how risky it is to use weak passwords, more people will start taking simple steps to protect themselves by using stronger passwords and using different passwords for different websites.

So, password strength meters that offer web surfers a visual gauge of how weak or strong a chosen lock may be increasingly present on websites. University of British Columbia and Microsoft studied the effectiveness of a meter that shows users how strong their password choice is compared to other users of a website. In the end, the study shows that password creation behaviors are heavily dependent on context.

One way to create more secure passwords that are easy to recall is to use passphrases – short words with spaces or other characters separating them. It's best to use random words rather than common phrases. For example, “cakes years birthday” or “smiles_light_skip?”

But that’s easier said than done. A good guideline is to use passwords of eight characters or more, with mixed types of characters. But even passwords with common substitutions like “dr4mat1c” can be vulnerable to attackers’ increasingly sophisticated technology, and random combinations like “j%7K&yPx$” can be difficult to remember. Users should consider the use of a password manager, such as Keepass, to generate strong passwords that won’t be found in dictionaries.

And finally, of course, they should use a unique password for each different online account – that way even if it is stolen by a hacker and cracked by hashcat, it will at least be only one account that is compromised.