

Auditing the Security Level of Passwords using a Cluster

**Miguel Dilaj (Nekromancer)
Vice-President of IT Security Research, OISSG
Barcelona (Spain), 26/Nov/2004**

IT Security: Protecting the Crown's Jewels...

Our most important assets:

Information



Business Secrets

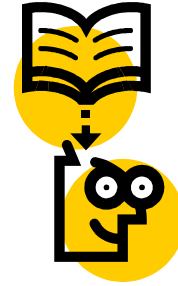


Identity
(including corporate image)

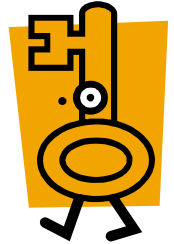


HOW we protect them

We make people aware of the importance of protecting our assets



We use passwords to allow access only to authorized individuals

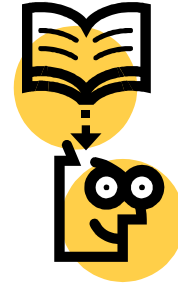


We encrypt the most important information using PKI

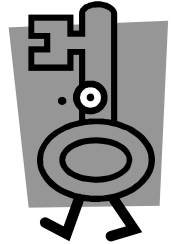


HOW we protect them

We make people aware of the importance of protecting our assets



We use passwords to allow access only to authorized individuals



We encrypt the most important information using PKI



Awareness I

MYTH:

Making people conscious about the importance of protecting our assets, they will take all the steps needed to enhance the security of our systems...

REALITY:

People are lazy

People tend to select the most simple password possible

People will avoid encryption if it's complicate for them to use it

People don't feel that their pockets or lives are at risk

People are HUMAN

Awareness II

There's the need to have clear regulations about the level of security we expect and **how to achieve it**

These must be **WRITTEN** and **APPROVED** documents

These must be easy to read for non-technical people

These must be easy to access for reading

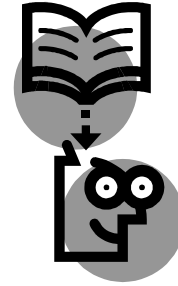
... and ...

IT Security has to play a “police role”
if it's intended to enforce them!

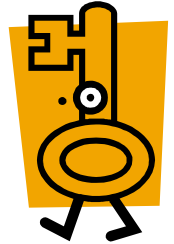


HOW we protect them

We make people aware of the importance of protecting our assets



We use passwords to allow access only to authorized individuals



We encrypt the most important information using PKI



Passwords I

MYTH:

Passwords are encrypted with a one-way hashing algorithm that makes **impossible** to recover them – (Microsoft statement some years ago, some people believed that and, what is worse, still believe that)

REALITY:

No one cares about DECRYPTING the passwords, it's much easier just to ENCRYPT know plaintext and then compare with the encrypted one until a match is found

It's plenty of programs out there to automate this process, for almost every imaginable algorithm

A LOT of the algorithms in active use are WEAK

MOST of the passwords the users choose are WEAK

Passwords II

Logon password now usually relies on Windows XP security...

Kerberos – high security, often don't used for legacy compatibility

NTLMv2 – medium security, often don't used for legacy compatibility

NTLM – medium/low security, most widely used, but...

LM – very low security, this one is still supported for legacy compatibility in many installations

Legacy compatibility is one of the factors that kills security

[Suggested Action: retire all legacy systems]

A simple password can be guessed, no matter if we use Kerberos!!

A simple password can be cracked, no matter if we use Kerberos!!

Passwords III

Kerberos – can be cracked *

NTLMv2 – can be cracked

NTLM – can be cracked

LM – can be cracked



Kerberos – only dictionary words will be feasible to crack (SLOW!)

NTLMv2 – probably only dictionary words as well

NTLM – dictionary words and hybrids, all possible combinations if rainbow cracking is used

LM – all possible combinations, rainbow cracking recommended to reduce the cracking time

*: Thanks Microsoft for flawing the Kerberos implementation in MS Windows to ease this one!

Some figures **in my T30 laptop...**

NON DICTIONARY WORDS TEST

LM (max. possible length 7 characters)

All alphanumeric passwords: 2.5 hours

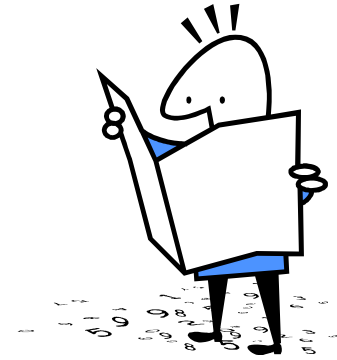
All alphanumeric + 14 symbols: 24 hours

NTLM 8 character passwords

All alphanumeric passwords: 297 days

All alphanumeric + 14 symbols: 4.2 years

Rainbow table lookup average time, **ANY LENGTH**: 15 minutes



Passwords IV

Do we want to wait until someone else cracks our passwords?

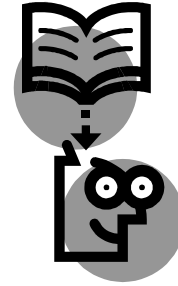
Or do we want to try to crack them ourselves to identify the weakest ones and report that to the user to enforce it to be changed?

If we don't do it, we make life easier for anyone who wants to do it, for whatever reasons...

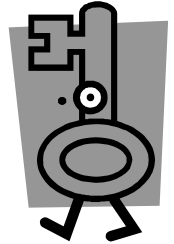
We NEED to identify such passwords as '{name of company}', 'password' and 'acapulco' and FORCE them to be changed!

HOW we protect them

We make people aware of the importance of protecting our assets



We use passwords to allow access only to authorized individuals



We encrypt the most important information using PKI



PKI I

**Public Key Infrastructure... the magical solution to ALL our problems
There's plenty of articles with titles "The End of Hackers" or similar...**

PKI is based on a CERTIFICATE and a PASSWORD

Usually the certificate resides in a "personal" network drive, anyone who knows your logon password can access it

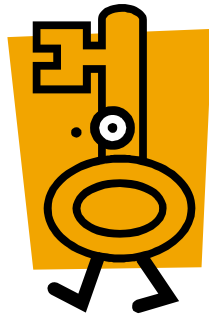
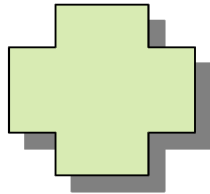
It's very likely that you set your PKI password equal to your logon password

Even if it's different, anyone with such "password power" can install a keylogger in your machine and get the PKI password when you first use it

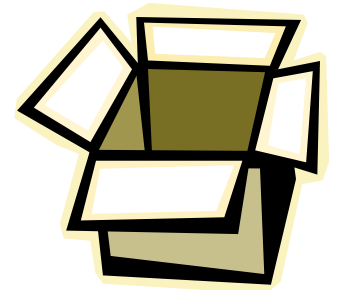
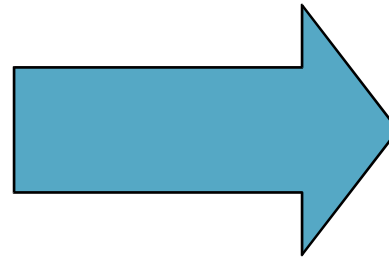
PKI II



Certificate



Password



MS security

Storing your secrets, locked with a high-security steel padlock, together with the key, in a cardboard box...

- Nekromancer

Consequences of doing nothing

Someone can steal, disclose, tamper or delete some or all of our Crown's Jewels (information, business secrets, identity), or use and abuse our systems

Can we trust the figures in this report from Finance?

Why our new formula has been shown in a website in China?

I've been fired! The memo is electronically signed by the President!

Just reported to Management that email full of insults I received from your secretary!

Where are all the files in my personal drive???

What is this program running in the background?

Etc...

What to do

MYTH:

We can achieve a certain level of security that will allow us to relax...

REALITY:

It's impossible to have 100% secure systems, we need ongoing processes to assure the level is as high as possible all the time

One of the things to do is to have secure passwords

We need to audit our current passwords and change the weak ones

We need...



Auditing the Security Level of Passwords using a Cluster

Composed of Password Auditing and Reporting, done in a Secure Environment

Password Auditing: password cracking

Best if done with fast and efficient tools

Best if done in a cluster

Best if done by generating rainbow tables

Reporting: emails (Alec Muffet's "nastygrams")

Must NOT disclose the password

Only email to users with weak passwords

3 levels of emails, after the 3rd one with no changes the account must be locked

Secure Environment: room with lockable door, no connection to the LAN, no clear-text passwords to leave the room, careful with hashes

The process...

- The hashes will be dumped from a DC using `pwdump2` (second revision) or `pwdump4` in local mode to a memory stick, not to the hard disk, and never transferred over the network
- The memory stick will be connected to the “master” machine in the cluster, and the contents moved to HD
- The hashes will be searched for the ones that mean no password, ‘password’, ‘{company name}’, etc., and password length < 8 characters, all these will be reported to separate files
- The remaining hashes will be formatted in the way used by the password cracking tool, and splitted into n parts (n = number of nodes in the cluster)
- n cracking processes will be launched, and allowed to run for 48 hs
- The remaining cluster time can be used to generate rainbow tables, test a different algorithm, etc.

The process... (cont.)

- **All the files generated will be analyzed (by automatic scripts) to prepare the list of usedIDs with weak passwords, together with the reason:**
 - no password**
 - password too short (< 8 characters)**
 - password too simple (dictionary word based or not complex)**
- **The listings of userID + reason will be transferred (memory stick, floppy, CDROM) to the LAN for emailing**
- **A script can be developed to automate the emailing**
- **History of last 4 runs results to be kept, so accounts that were reported 3 times with no action from the owner can be disabled**
- **TARGET: to have 8+ character passwords, not word based, MiXeD case and numbers as a minimum (critical to re-train users!)**

The cluster and the tools

The most simple, inexpensive and powerful cluster to setup is:

Linux (OS)

openMosix (clustering software)

The 2 above already combined in clusterKnoppix, a Linux live-CD

Two simple, inexpensive and powerful password cracking programs that can be used:

Lepton's Crack (Open Source, GPL'd)

John the Ripper (Open Source, GPL'd)

Some supported cracking methods:

LM, NTLM, Lotus Domino R4, MD4, MD5, Kerberos algorithms

Wordlist, smart wordlist, bruteforce, prepending and appending, and REGEX (REGular EXpressions) cracking modes

The cluster and the tools (EXAMPLE)

Need to audit ~80.000 hashes (typical big company)

Planned a 25-node cluster, this will process ~3200 hashes/node, that's not too much

The architecture chosen makes it easy to add power simply connecting more nodes

Each node will be only:

Motherboard, CPU (Athlon 64/Opteron), Cooler, Memory, onboard Fast Ethernet or Gigabit

Case or Rack-mounted

No HD, no CDROM, no keyboard, no mouse, no screen...

Except the “master” node, that will be used to interact with the cluster

A Cisco Fast Ethernet/Gigabit switch to interconnect all (2 if redundancy is required)

The cluster and the tools (cont.)

The cluster needs:

- **A home (lockable room)**
- **To be kept fresh (HVAC)**
- **To have food (power supply)**

And we can give it a name if we want ;-)

A few scripts have to be produced (Bash, Perl, etc) to do the pre-processing and reporting, and another script in a suitable language to do the emailing in the LAN environment

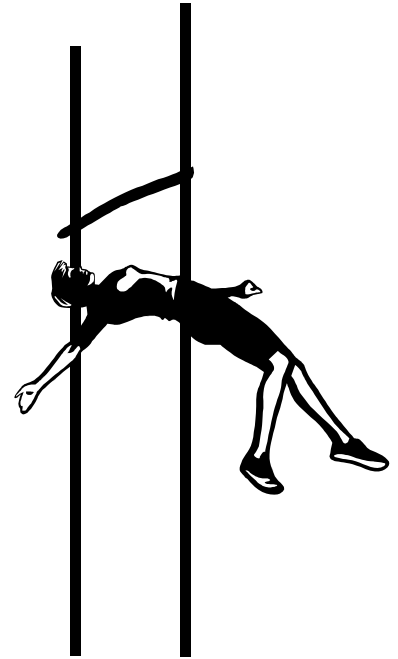
The expected results (based on EXAMPLE)

In the first run, thousands of weak passwords

By the time of the third run, probably down to hundreds

By the time accounts start to lock, down to dozens (base level)

This will definitely raise the bar to crackers!

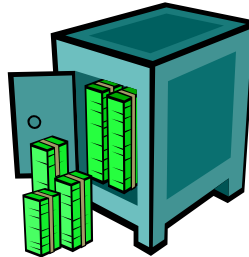


Why then, we can't relax???

We will go from this:



To this:



But it can still be opened, we can do nothing against that.

It WAS DESIGNED to be opened, it HAS A DOOR!

Final Words

We need to keep guarding the Crown's Jewels

Remember that whatever we do, our assets will be still at risk

We can only make it more difficult for crackers, but it's impossible to make it 100% secure

Insiders have much more freedom of movement than outsiders



Questions?

