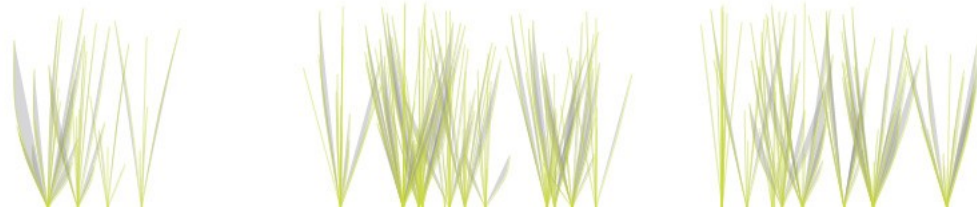
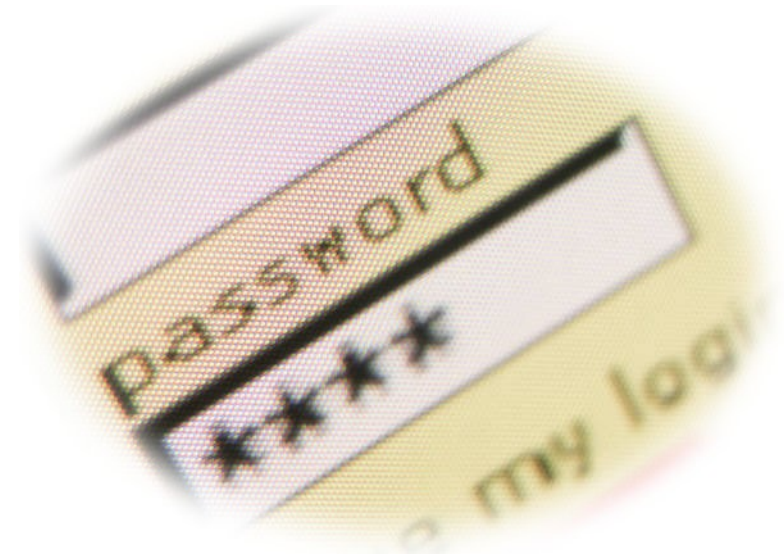


Keys to the Kingdom

A presentation to: E-Business 2008

Mike Auty
E-Security at WDL
Date: 16th October 2008



Overview

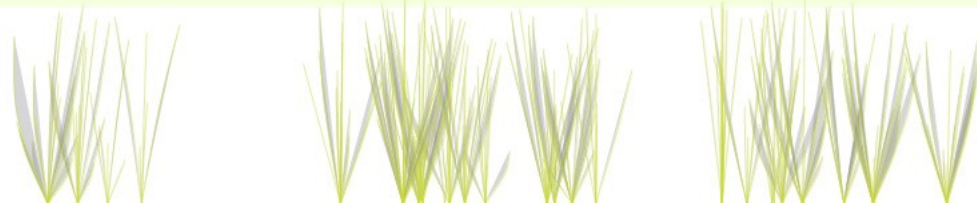
- Securing Systems
- Passwords
- Storing Passwords
- Guessing Passwords
- What can I do about it?



Securing Systems

Securing a computer system is a difficult task

- Are you who I think you are?
- Are you allowed to do that?
- What should I do if you're not?
- How do you ensure the person using the machine is the right person?
 - Authentication & Authorization
- We want to check “something you have and something you know”
 - Password, RFID, Fingerprints, Retinas, Chip & PIN, etc
- So far, there isn't an answer, but the most common solution is a password



Passwords

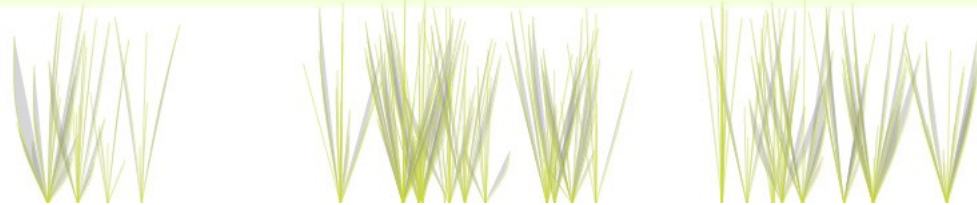
A Password is a pre-arranged *secret* shared between two parties.

Some people worry about their side of the password:

- Shoulder surfing
- Sharing the password
- Entering it on an untrusted webpage

Security people worry about the other side:

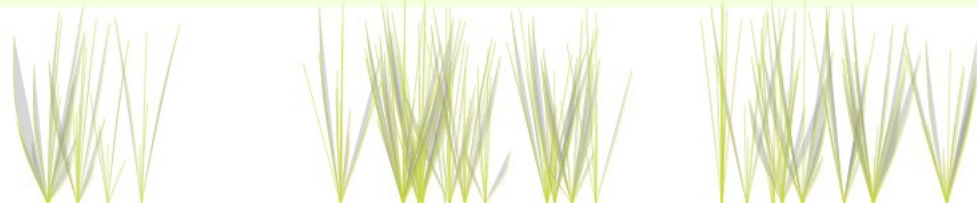
- Attacks on servers



Storing Passwords

Attempt Number 1: Just store them

User	Password
Alice	@halw!fwga5
Bob	Dobbin7
Charlie	Dobbin7



Storing Passwords

Just writing the plain password down is bad

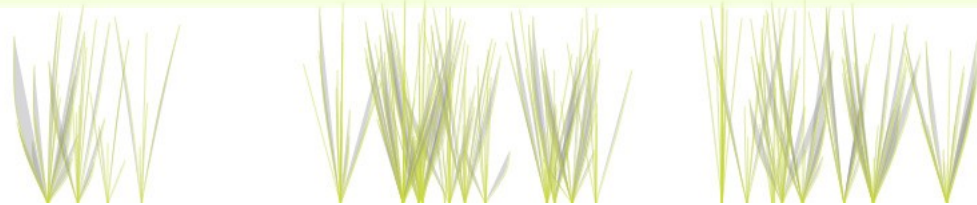
- Imagine if Amazon wrote down the passwords of all their customers?

Why not encrypt the password?

- Just another key to keep secret

Hash the password!

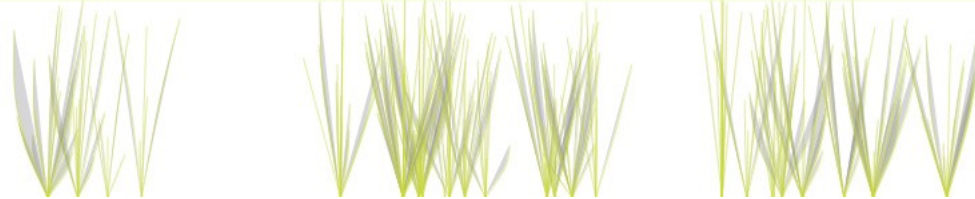
- Hashing is a one-way process that turns words into gibberish
 - Crucially, it always turns the same word into the same gibberish
 - And it's very unlikely to turn two different words into the same gibberish
- Lots of different ways of producing gibberish!



Storing Passwords

Attempt Number 2: Hash them

User	Hash
Alice	8ed7edb463cddb...
Bob	06f7e833953d846b...
Charlie	06f7e833953d846b...



Storing Passwords

Better, but not great... identical passwords are stored identically

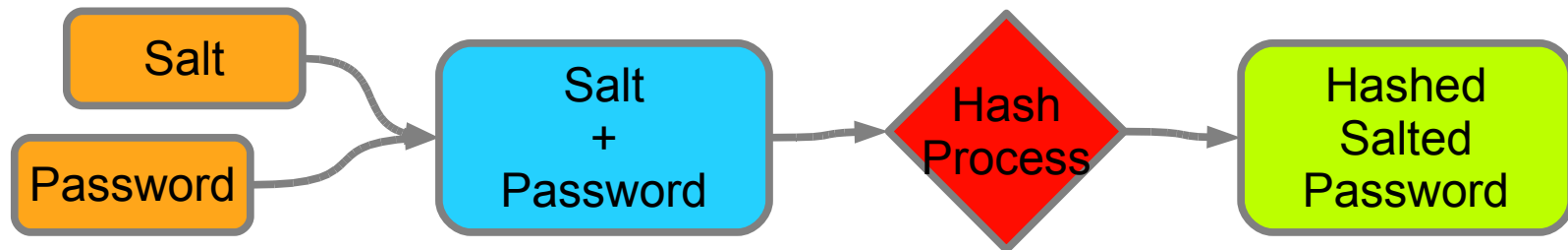
- Back at Amazon, of all the millions of users, many will have the same password

We need something to make the hashes different

- It doesn't need to be entered by the user

How about a “Salt”?

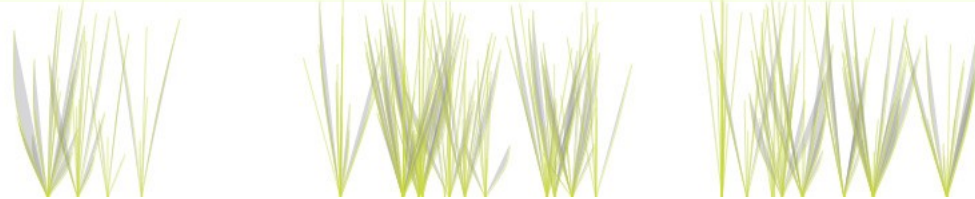
- Random number that just adds a bit of flavour to the output of the hash



Storing Passwords

Attempt Number 3: Hash them with a salt

User	Salt	Hash
Alice	f4	973b503c92b16cef...
Bob	6b	543de38793d57af2...
Charlie	f4	460ebb6f8ad45f3f...



So?

Why do I need to know about all this?

- Your laptop or desktop computer stores your password
- Your business network servers need to know it too
- They should use these techniques to secure your secret

How does windows store your password?



Storing Passwords

Microsoft LanManager version 1

User	Password	LM Hash
Alice	@halw!fwga5	DDDDFF1C4360A1EA0 7728CCC198F4E75E
Bob	Dobbin7	804C41F1209B1977 AAD3B435B51404EE
Charlie	doBBin7	804C41F1209B1977 AAD3B435B51404EE
Dave	5 secur3	B2D1009CBB5F11AC AAD3B435B51404EE



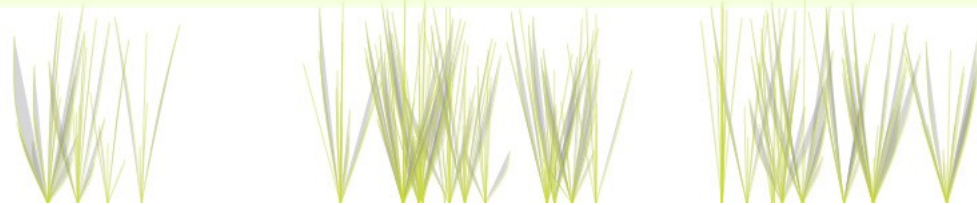
Storing Passwords

What went wrong?

- They changed all lowercase characters to uppercase characters
- They truncated the password at 14 characters
- They split the 14 characters into two sets of 7
 - Imagine splitting your pin number into two sets of two, each verified separately
 - 10,000 x 1 possibilities goes down to 100 x 2 possibilities
- No salt!

Used in NT, and maintained for backwards compatibility in 2000 and XP

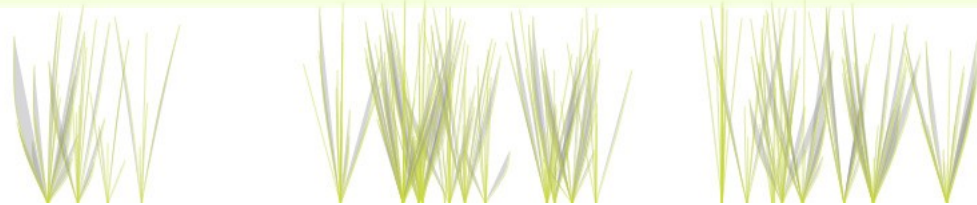
Vista uses the stronger NTLMv2 hash



Guessing passwords

How to guess passwords:

- Write a program to do it
- Optimize the program
- Trade off time for memory
 - Spend a long time guessing lots of possible passwords
 - Write them all down and then check through them when needed



What can I do about it?

Password self-defense

- 1) DO NOT REUSE PASSWORDS
- 2) REALLY, DO NOT REUSE PASSWORDS
- 3) Passwords can actually be phrases: “Alice had a little wolf, it's fur was gray as slate”
- 4) Things that look random can still be remembered: @halw!fwga5
- 5) Not everybody gives you good advice

HOME PERSONAL CARDS FINANCIAL SERVICES TRAVEL SMALL BUSINESS CORPORATIONS MERCHANTS

AMERICAN EXPRESS

Site Help | Search | Contact Us

Change Your Password

Current or Temporary Password

Create New Password

Verify New Password

Your Password should:

- Contain 6 to 8 characters - at least one letter and one number (not case sensitive)
- Contain no spaces or special characters (e.g., &, >, *, \$, @)
- Be different from your User ID and your last Password



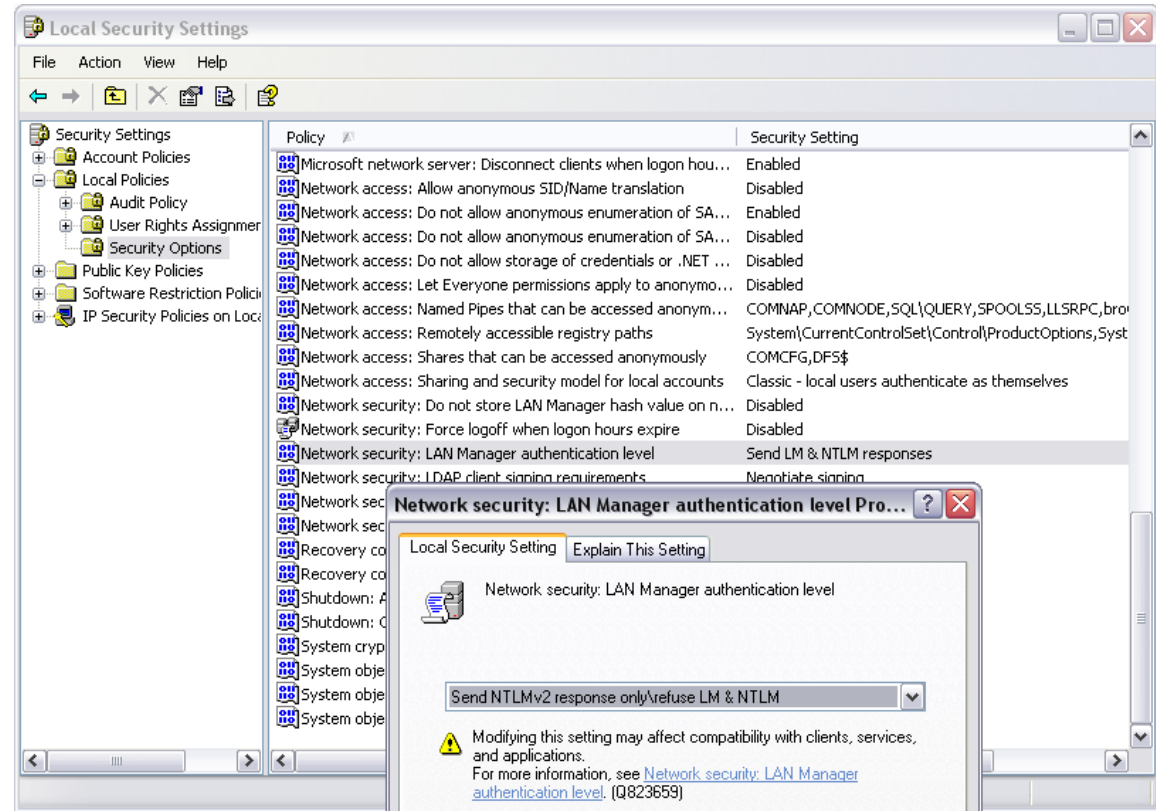
What can I do about it?

Turn off LM hashes:

- Control Panel > Administrative Tools > Local Security Policy
- Local Policies > Security Options
- Select Network Security: LAN Manager authentication level
- Right click for Properties
- Set it to NTLMv2 response only

Now all **new** passwords
will be secure so...

Choose a new one!





Questions?

