

# Another Way To Secure Passwords

- Complex ain't gonna work
- Let them stay with lowercase letters, but set a long minimum
- To get the LM-killing side-benefit, I suggest a 15 character minimum password
- “15 characters? Won't I get lynched?”
- It becomes more palatable if you teach users to employ not passwords but passphrases

# Example passphrases

- pearspeachesapples
- iwantchocolatefences
- redbreezesbluecurrents
- undergroundlaundryenergy
- toadthedrysprocket
- tellmewhatiwanttotaste
- All longer than passwords, easy to remember, but meaningless and therefore hard to guess

# Why's This Better?

- You get a long password that's easy to remember, unlike complex passwords
- It is also then harder to guess by humans

# Running The Numbers Again

- 15 lowercase letters =  
1,677,259,342,285,725,925,376 possibilities
- Try a million a second, it'll take 531,855 centuries to try them all
- Run *that* past those annoying security auditors and see if maybe you can't
  - Get rid of lockouts
  - Extend password-changing period to 6 months

# How Long Will This Work?

- Passphrases sound good, but are they secure?
- In theory someone could write a cracker that worked on words rather than characters but nothing like that exists
- Assume that there are five characters per word and therefore about three words per passphrase

# Running the numbers AGAIN

- Assume most Americans know about 10,000 words
- There are, then, only about 1,000,000,000,000 (one trillion) passphrases
- These could be pre-computed
- Furthermore, most passphrases will be something mildly grammatical, like noun+verb, so the numbers get smaller

# Cat and Mouse

- But how long before the bad guys do that?
- Counter-measure: misspell a word, or throw in a name, or...
- There will *never, ever*, be a foolproof 100 percent technological way to secure passwords
- So the best we can do is some user education and a few reasonable minima
- Any clever trick we come up with now will be echoed in crackers in the future

# Advice On Passwords: Users

- Avoid dictionary words at all costs
- Adding a space or other punctuation makes things *much* harder for the cracker programs
- If you like, 5u6st1tution\$ can't hurt
- Again, 15 character passwords automatically kill LM hashes
- People must understand that passwords are valuable and must be protected

# Advice On Passwords: Admins

- Protect the hashes
- Consider a password auditing tool like LC5
- Invite users to a brown-bag lunch presentation – offer sodas and chips – and talk about how passwords get stolen; people *hate* lectures, but they *love* to hear true tales of crime!
- The lever will probably be “okay, you couldn’t give a hoot if people hack the company’s stuff, but I’ll bet that a lot of you use the same password for here as for, perhaps, your online banking...”

# If you liked this...

- Please consider buying the entire 10-CD lecture set of “Securing Your Windows Systems”
- It includes 10 hours of security lecture from techie expert Mark Minasi
- Visit [www.minasi.com/seccd](http://www.minasi.com/seccd) for more info
- Thanks!