

Passwords: An Invitation to Compromise



Control access to computer workstations and automatically manage multiple passwords without user intervention—using advanced fingerprint biometrics and RFID technology.

21st century data security has changed considerably. No longer can encryption technologies effectively protect organizations from experiencing data compromise. Because computers are the brain of every enterprise, protecting the information they store should be at the forefront of any organization that uses a computer. How safe are those files and are they protected from unauthorized access?

If your organization is like most, you utilize passwords to secure access to your network, applications and data. You use a lot of passwords and these have to be changed every 30, 60, or 90 days. Your users have to keep track of many different passwords of varying degrees of complexity that are constantly changing. Your employees are very busy and often forget their new passwords. This results in lost time, lost productivity and general stress and frustration. This applies not only to the user forgetting the password, but to the help desk employees that have to reset hundreds of passwords every month because people keep forgetting what their new password is. Dealing with a user forgetting his/her password (s) may seem minor, but in actuality, it is not a matter of chump change – a 1,000 employee organization can spend \$150,000 a year or more on password-related help desk calls.

The human factor plays a major role in password effectiveness. To cope, users are writing their passwords down, leaving them lying around here and there, or using obvious passwords. It comes as little surprise that for his/her computer alone, a typical user can have more than ten passwords and that's not including the passwords required for work. In any case, chances are that most computer users are actually compromising the security they were meant to improve – rather than being the guardian of the gateway they once were,

passwords today frequently become the key to unsecured access. Passwords can be easily stolen, lost, shared or cracked. Due to the need to manage multiple passwords and to ensure the effectiveness of passwords used, organizations have adopted stringent password policies. This has translated into more complex passwords and consequently, made them more difficult to remember. Passwords remain a fundamental security weakness regardless of the strength of the password policy.

Recent research from the Ponemon Institute revealed that a majority of users disobey company security standards — and they do so knowing that they're violating protocol. In addition, survey data just released by RSA shows that trusted insiders “create data exposures of extraordinary scope” through their everyday behaviors. End users are smarter than ever. The advent of the PC at home and not just work anymore, as well as the ability to look up and verify what the IT people are saying to users, is new territory. Additionally, users can easily find detailed accounts of how to sidestep corporate policies. These are readily available from countless Internet sites and even laid out clearly in publications such as The Wall Street Journal. With compliance regulations a constant factor, finding a balance between the need for expanded access to information and the requirements to protect information from unauthorized and inappropriate use is next to impossible.

Passwords, as a rule, are ridiculously easy to guess or crack, even in the strictest environments but these aren't your organization's only concern. Worms used



Sales@crystalit.us
www.crystalit.us

Passwords: An Invitation to Compromise



Control access to computer workstations and automatically manage multiple passwords without user intervention—using advanced fingerprint biometrics and RFID technology.

by hackers like Agobot / Phatbot / Polybot / SDBot / RBot all ship with dictionaries of passwords numbering in the hundreds and they can easily replicate to a system that has a password in this word list. The hackers are really good at keeping these wordlists up to date with passwords that they've cracked from other systems. Worse still, attackers (either automated or human) don't even need to GUESS the password. There are hacking tools a-plenty that will let a hacker sniff your network traffic to scoop out authentication material for the LM, NTLM and Kerberos protocols and then brute-force that material back into a working password. Granted there are ways to protect your network: segmentation, encryption (IPSec etc.), 802.1x. Unfortunately, they just are just a workaround for an issue that you still need to address; the inherent vulnerability in your network which is - the password.

The Avert CDLS access control module eliminates these concerns by removing the responsibility from the user and placing it within the technology. Furthermore, no longer will passwords threaten an organization's security, drain its financial and technological resources or hinder productivity. Let our world class access control solution manage your passwords and provide true security for your organization.



Sales@crystalit.us
www.crystalit.us