

Windows Password Weaknesses Could Threaten Your Enterprise

Ray Wagner

Technology researchers have proved they can crack Windows alphanumeric passwords in less than 14 seconds. This ease of attack requires security directors to take seven steps to boost their Windows password security.

NEWS ANALYSIS

Event

According to news reports published on 23 July 2003, Swiss technology researchers have issued a report that describes how Windows computers protected by alphanumeric passwords can be quickly and easily cracked — in less than 14 seconds — by using precalculated data stored in look-up tables. Such ease of cracking, suggest the researchers, is due to Microsoft not using "salt" (a standard security mechanism applied to encrypted passwords) in its Windows operating system. Other computer operating systems, such as Linux, Mac OS X and Unix, do use salt in their password encoding technologies, which can deter or delay password breaches.

Analysis

The fact that Windows's logon password-encrypted store isn't safe is not new information. However, Gartner believes that this research shows that increases in processing power have greatly increased Windows' security risk. Other operating systems use salt to bolster logon security — which doesn't necessarily mean that their password processes are strong. However, salt unquestionably lengthens the time necessary to crack passwords by making the precalculation of encrypted data more difficult. Although Microsoft does provide good policy and education documents on the need for strong passwords, Gartner believes that the company shouldn't deem achieving technical practices in line with industry norms unduly burdensome, and that Microsoft has said as much as part of its Trustworthy Computing initiative.

For this new cracking technique to be useful, the attacker needs direct access to the encrypted password file on the target computer. This may require administrative access to the machine. Although the captured password affects only Windows log-ins, many users deploy their Windows log-in passwords in other places, such as virtual private networks (VPNs).

Enterprise security directors should:

- Require and enforce strong passwords for Windows logon, using provided Windows password security mechanisms.
- Use password-testing and monitoring tools from third parties (such as Aelita Software, Anixis, Avatier and others) to check for weak passwords.
- Don't permit reuse of the Windows logon password for any other purpose — especially for remote access.
- Don't link other security mechanisms — including VPN credentials and password wallets — to the Windows logon.
- Consider strong drive encryption capability to protect all data and ensure that the password data is re-encrypted by this mechanism.
- Expect an increase in attacks and automated attack mechanisms against encrypted password stores on Windows machines.
- Enforce immediate reporting and credential revocation for stolen laptops or other computing devices.

Analytical Source: Ray Wagner, Gartner Research

Recommended Reading and Related Research

- "Microsoft Security Flaws Highlight Urgent Need for Personal Firewalls" — While enterprises patch Windows security flaws, they should ensure that every laptop has a personal firewall. **By John Pescatore**
- "Microsoft Must Show Trustworthy Computing Involves More Than Security" — Achieving Trustworthy Computing's lofty security goals is a big challenge, requiring of Microsoft new business practices, more open communications and a cultural transformation. **By Steve Bittinger and Dion Wiggins**

(You may need to sign in or be a Gartner client to access all of this content.)

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509