INFORMATICA
INFORMATION SECURITY & RISK MANAGEMENT

SGOP:
Securing Good Old Passwords

By Claudiu Popa, President
Informatica Corporation

With recent statements about the demise of passwords and statistics around their insecurity pointing to a whopping 2/3, it's easy to make the assumption that the trusty old gatekeeper is on its way out. Fortunately for some of us who know better, we can remember that passwords have been with us for millennia and they aren't going away anytime soon. In fact, statements about their demise are grossly exaggerated.

While it's true that more methods for uniquely identifying individuals are well on their way, two and three-factor authentication are still two methods that require more technology, work and a learning curve before they will be widely adopted. In fact, the reason behind the shift away from single-factor authentication (passwords) to two-factor (physical tokens and keys) is simply that there is a greater understanding of information and asset sensitivity.

We are now beginning to understand data classification and with this understanding comes an appreciation for risk and value associates with these assets. We 'feel' as if we must secure certain things more tightly than others, and we're right. That said, we will always have more trivial systems that require a simple login than things that need strong authentication.

As with everything else, the effectiveness of passwords, tokens, biometric systems lies in their implementation. It is easy to discard passwords as ineffective and insecure on systems that have no controls, because the weakest link is the human being who is allowed to choose and use them. A proper password implementation however, will provide administrators with many years of relatively solid security around our favorite method of user authentication.

For that to happen, administrators need to keep in mind the five simple rules of password security:

1. Complexity – asking users to create alphanumeric passwords of 8+ characters that also include case variations is a very adequate way to vastly increase the strength of the protection especially assuming that users will have ways to make them easier to remember (i.e. "@RT1CH0Ke*")

2. Expiry – ensuring that a password's life ends in less than three months (sometimes as little as one) is an excellent way to ensure that compromised passwords have been flushed and old accounts are automatically disabled. While frequent expiry is a leading cause of users actually writing passwords down in an effort to remember them, a reasonable gap is considered acceptable, as long as old passwords (called password history) can not be reused.

3. Delay – to reduce the likelihood of dictionary or even manual attacks, a delay between password prompts, even a couple of seconds, is useful. This simply slows down the process of brute force attacks and ensures that only a very small number of attempts will work in a certain amount of time.

4. Lockout – it is reasonable to assume that the right user can only make so many mistakes due to typing mistakes and memory lapses, usually a maximum of five. After that, the account should be suspended and the administrator will need proof of identity to re-enable it. Setting this value too low, will create unnecessary work so care should be taken to match the sensitivity of the data to the usage conditions.

5. Logging – this is the only way to monitor password usage trends, errors, security attempts and other abnormal use. System administrators need to review password statistics and select Expiry and Lockout values – in particular – accordingly.

From a technical and security perspective, this will reduce the need to perform password audits – aside from looking for sticky-notes on the side of monitors – and simplify the job of implementing them. If a certain system doesn't support all these controls, implementing the rest will still be very useful, with the emphasis being on the first two.

These security measures will go a long way towards extending the usefulness of password-based systems. Coupled with a policy instructing users not to write down or disclose them, they will ensure that we won't have to adopt 'overkill' technologies for systems that just don't require the effort and expense.