Strong(er) User Authentication

By TAN Teik Guan, CTO, Data Security Systems Solutions PL

Web: www.dsssasia.com
Email: teikguan@dsssasia.com

Teik Guan has many years of hands-on experience in designing and implementing data security solutions for many highly-sensitive projects including the Interbank RTGS Systems, Cheque Clearing Systems and several Internet banking and trading systems. Teik Guan is well-versed in the niche area of cryptographic security programming and integration, having developed numerous successful products such as CAs, smartcards (Javacard), HSMs, Authentication Servers, etc. Teik Guan holds a MSc from the National University of Singapore.

Abstract

As more people use the electronic and Internet platform to carry out more sensitive and higher valued transactions, the need for organizations which operate such systems to have the ability to remotely ascertain the identity of the user becomes extremely critical.

In this paper, we highlight some of the questions that organizations must ask when sourcing for 2-factor authentication solutions, and show that with a flexible solution, 2-factor authentication need not be painful nor costly.

Banks take the lead in the area of Internet authentication. Already, there are banking regulations that require Banks operating Internet Banking sites to have end-to-end security for the passwords. Yet, password breaches are not uncommon, and that translates to direct and indirect monetary loss.

Whoose fault is it ?

Our basis for advocating proper authentication systems stems from the growing awareness by organization decision makers that the straight-forward use of passwords ("something you know") for Internet use is no longer sufficient. It cannot be fully the individual user's responsibility in the case of an unauthorized identity breach in the system.

The problem is mostly systemic. If organizations do not constantly look into introducing stronger authentication means for their systems to counter the ever-increasing sophistication of the "wild-wild web" hacker, the number of unauthorized breaches will increase regardless whether users adopt good password practices.

With responsibility also comes liability. When an unauthorized breach happens, a weak authentication

system is likely to be attributed much more blame, as compared to a poorly chosen password by a user. However, if the organization offers strong authentication, but the user chooses not to use it out of convenience, then the individual user will have to bear more blame in the latter case.

What do organizations have to do ?

2-factor authentication is widely touted as the proverbial bitter (and costly) pill for organizations to swallow in order to have stronger user authentication. These 2-factor authentication systems typically require each user to carry a key fob or calculator-like device that generate a one-time-use password as the 2nd factor (?Something you have?) means of authentication. Other 2-factor systems also include the use of cryptographic smart cards or tokens to perform a challenge-response handshake, or using a GSM mobile phone to receive a one-time password via SMS. While such systems are effective, they tend to be rigid and neglect several organization considerations of user authentication systems. Let us examine 3 of these issues:

- **Does the system provide end-to-end protection and policy enforcement for the user password ?**

  A good 2-factor authentication system requires both the 1st factor user password and 2nd factor one-time password to be correctly implemented. End-to-end security, plus enforcing of strict password policies (password aging, length, etc) for the user password must be in place to ensure the non-compromise of the 1st factor user password, regardless whether the 2nd factor is used. Moreover, we should recognize that the use of 2-factor authentication requires a mindset change for the user, and this does not happen overnight for all users at the same time. The system must have the flexibility to support both 1 and 2 factor authentication (transparent to the application) as the actual rollout of 2-factor authentication is a gradual process. Users who still remain on 1-factor authentication (by choice or by sheer logistics impossibility) should be given ample protection on their user password.

- **Is the system flexible support various user combinations of 1st factor only, 2nd factor only, 2-factor using different tokens, PKI, etc ?**

  A flexible and configurable system will allow the organization to adjust the system to suit the application requirements. A system that supports both 1&2-factor authentication will allow organizations to match their application/user requirements (or $-value) against the level of authentication for a more cost-effective and acceptable solution. It becomes a case of who-needs-what. A user who transacts high volumes or at high values should be assigned a hardware token, while another user who rarely logins to the system may be issued one-time passwords via SMS on demand. Not only does this save significant upfront and ongoing costs to the organization, it also caters to the needs to the users since the latter user is most likely to mis-place the hardware token or forget the static password but not lose the mobile phone.

  More significantly, a system supporting multiple types of tokens means that the organization is never "locked-down" to a particular token vendor, and can always take advantage of advances in token technology.

- **Does the system provide a simple & secure way for users to manage lost / misplaced tokens ?**

  Besides costs, the logistics and management of the 2nd-factor tokens consume a substantial portion of the resources needed to maintain such a system. If the management of the tokens can be somehow delegated back to the user, it will bring about significant long-term savings. For example, in a flexible system where a user can be assigned both hardware token as well as one-time password via SMS, then the user would not need to trouble the helpdesk should he/she forget to bring the hardware token. He/she will simply use the one-time password via SMS as an interim measure.

It is obvious that a flexible solution is key for a successful 2-factor authentication system. With a little added flexibility, it allows organizations to tune their implementation in the most resource-effective and cost-effective manner, while catering to the users? needs and preferences.

Conclusion

2-factor authentication is here to stay. The good news is that a successful 2-factor authentication system need not be bitter (nor costly). Rather than adopting off-the-shelf 2nd factor packages as a one-size-fits-all solution, organizations looking to implement 2-factor authentication systems should first examine their applications? and users? authentication needs and next demand the appropriate flexibility in the solution in order to meet the needs.