The End of Passwords

By M. E. Kabay, PhD, CISSP-ISSMP
CTO & Program Director, MSIA / School of Graduate Studies
Associate Professor of Information Assurance / School of Business & Management
Norwich University, Northfield VT

I detest passwords. Why do I loathe passwords as a method for authentication? Let me count the ways:

1. Most systems allow users to choose their own passwords. Most users have no clue how to choose passwords that will resist even the mildest guessing based on elementary research of their interests (family, hobbies, pets, favorite sports teams) or simple dictionary-based attacks (ordinary short words). Many users choose the word "password" or their own name as their password.

2. If the system applies filters to passwords to impose content and structure requirements (e.g., minimum length, inclusion of numbers or special characters, exclusion of words in a dictionary) then most users use the same password over and over and for every possible application requiring a password including their external e-mail, offshore gambling sites, auction sites, book clubs, and pornography vendors.

3. Reasonable system administrators require periodic changes of passwords; paranoid system administrators require changes of passwords so often that the users become desperate because they keep forgetting their passwords.

4. Users faced with demands for changes of passwords adopt a policy of using the same password all the time, or possibly changing a single number in the password; e.g., ramo1bilu, ramo2bilu, ramo3bilu and so on.

5. Some administrators make the mistake of having a single day (e.g., once a month) on which all passwords expire; they thus create a flurry of interventions as support staff help users who have forgotten their new passwords.

6. If the system applies password histories to prevent reuse of passwords on a particular system, users write their passwords down on scraps of paper and stick them to every available surface, often with helpful identifying notes such as, "Password for accounting system."

7. Most users share their passwords with anyone who asks; e.g., technical support staff, the guy in the next cubicle, and even complete strangers on the street who offer them a chocolate or nothing at all.

8. Many users respond to having to remember difficult passwords by writing them down and posting them on sticky notes on their terminals, under their keyboards, under their chairs, on their foreheads….

9. Some system administrators still leave their password files accessible to any eight-year-old who wants to run a password cracker for fun and profit. A very few still use unencrypted password files.

10. Many system administrators still receive no (or ignore any) real time alert when attackers try online password guessing, especially if the attacker uses slow scans that attack many different user IDs, but only one at a time, over many hours or days.

11. Some system administrators still believe that inactivation of user IDs under password-guessing attack is a reasonable response; they thus hand their system over to attackers for a simple denial of service: try every account with a dummy password. Admittedly, most system administrators understand that requiring manual intervention to reset a lost account is not the most clever policy in the world; therefore, they configure their systems to have a reasonable timeout (e.g., a few minutes).

12. Sometimes organizations send users both their user ID and their password in the same unencrypted message, making it too easy for accidental or deliberate interception to break security.

13. In environments where time pressure is extreme, such as medical facilities, many users bypass the nuisance of constant logon/logoff cycles by having workstations logged on every morning by whoever gets there first and then simply using that session all day.

Alternatives

Practically everyone already knows that the four fundamental mechanisms for binding social identity to user ID – that is, authentication – are:

- What you know: passwords or passphrases such as nonsense strings or supposedly private information (e.g., your first love's pet name).

- What you are (static biometrics): characteristics of your body such as retinal patterns, iris patterns, hand geometry, fingerprints, face, height-to-weight ratio.

- What you do (dynamic biometrics): e.g., dynamics of voice, speech, signatures and typing.

- What you have (tokens); e.g., keys, passcards, badges, photo IDs, or anything unique or nearly unique that is difficult to obtain or counterfeit.

I'm not going to go into the details of these systems in this essay. What I want to point out is that most of these systems are good for session initiation but not so great for automatic session termination. One can place one's finger on a fingerprint reader, insert a magnetic card into a reader, look into an iris scanner, speak into a microphone, type on a keyboard, sign one's name -- all of these methods can allow an authorized user to log on to a system.

The problem is that once the interaction is complete, there is usually no mechanism for automatically detecting the departure of the authorized user. Indeed, if one tries to use tokens such as magnetic cards to detect departure by forcing the user to leave the card in the reader while the

session is in progress, one of two unpleasant consequences will result: either the user will leave the card in the reader and walk away or the user will walk away with the card attached to his or her wrist and either be yanked backward or pull the equipment onto the floor with a clatter.

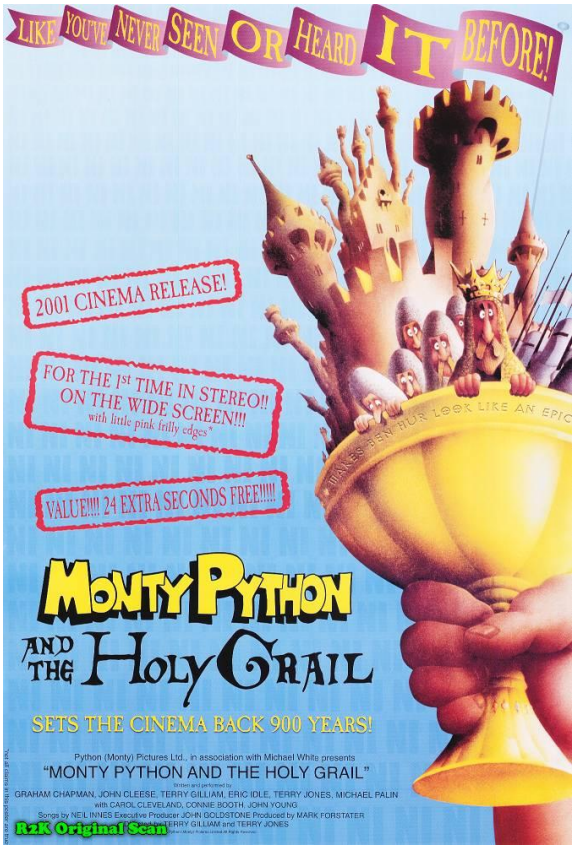
One promising biometric technology to allow automatic session initiation and termination is face recognition. Theoretically, it ought to be possible to set up a camera-based facial recognition system that can correctly detect the departure of an authorized user. However, I don't know of such a system in use (let me know if you do).

Another technology that should allow the kind of automatic logon and logoff I've been dreaming of is proximity cards. We already have long-established access-control systems that use Wiegand cards, which have metal particles embedded in plastic so they produce a unique signature in response to radio waves. Proximity sensors can be placed in the wall to control door locks and allow people to go in and out without having to touch their cards.

For the last 20 years, I have wanted to see a proximity sensor used with workstations to control automatic logon and logoff. At the end of May 2004, I learned of the authentication equivalent of the Holy Grail: we finally have a good method for fast, effective password-free access control using proximity badges and sensors. And the results are even better than I had imagined.

The Holy Grail

In the previous sections in this short article, I have explained that I have long sought a system for using proximity devices as the basis for identification and authentication, especially in the medical environment where most users are under too much pressure to tolerate logon/logoff procedures. Such applications would benefit from a system that automatically allows session initiation when an authorized user approaches a workstation and then either suspends access or terminates the session when the user leaves – all without any particular human intervention.



Imagine my delight when I received a press release from Ensure Technologies Inc < http://ensuretech.com/ > announcing precisely this technology. Within a few seconds (literally) I was on the phone and arranged to interview Tom Xydis < mailto:tom@ensuretech.com >, CEO of this corporation and inventor of the XyLoc proximity devices.

Here is an abbreviated version of that interview.

Q: Tell me about your background.

A: I went to Northwestern University for my BS in electrical engineering (EE) and have a MSc and a PhD in EE from Michigan. I worked on digital radios and other equipment in 1970s and developed the key-fob keyless entry system for cars; that got me into low-power wireless. After that I was involved in various committees for 802.3 and .4 and .11 and now Bluetooth. But the genesis of the invention for Ensure was my involvement in a wireless controls company in the 1990s; we built wireless control systems for everything – lights, fans and so on. We had a security breach where the salary information for the executives ended up on a bulletin board. So people said, "Someone must have hacked in." Actually, somebody used an unattended terminal that was already logged in. The comptroller tried to use a password-protected screen saver, but it kept interrupting her work, so she started locking her door and moved her administrative assistant in front of her office rather than use the screensaver. It was that incident that made me realize how passwords were getting in the way of productivity. I formed a new company – Ensure Technologies – where I invented and patented the XyLoc in 1998. We knew it was a good product and realized that healthcare was the ideal vertical market. They needed security but they couldn't let security get in the way of their efficiency and workflow. Physicians and nurses want to treat patients, and they have to respect security they don't want to waste time logging in.

Q: Tell us what the XyLoc does.

A: Our product automatically senses the presence of an authorized user carrying the badge (called the XyLoc KeyCard). It knows how far away the person is, so it provides identification information to the computer when the person is the "Active Zone," which is configurable by system managers. The bearer of the key is identified to the system automatically logged on for appropriate access as defined by the organization's policies. When the person leaves, access is suspended or terminated as required. But when a new person arrives, the system registers the identity of the new user and so the log files are correct and access is appropriate. For example, if the IT manager arrives, (s)he might be able to access the desktop directly without closing the medical application; if a nurse arrives, the system can open a separate session for the nurse. So if the doctor has left the terminal without completing a critical authorization, the system may alert the next nurse who arrives about the situation and suggest that (s)he find that doctor stat (at once)! This will all depend on the organization's security policies in general and for particular classes of users.

Q: So how does it work?

A: The KeyCard is a small radio transceiver that communicates with a "lock" transceiver attached to the workstation (called the "XyLoc Lock" – it is connected via USB). They talk to each other about once a second. Each KeyCard has a unique identification number that gets rolled into a stream of encrypted signals that are decrypted by the lock. The ID is not a secret; what we do is to authenticate the badge itself as an authentic XyLoc badge. The lock communicates with the XyLoc client software – a service running under the operating system which interfaces to the authentication system. So the lock provides a list of all the

badges within range and how far they are; the software can be set to authenticate those within a specific range.

In addition, some of our sites are interested in the proximity information itself even when the employees are not logging on. This is an application that has more to do with accountability, time management and attendance. But 99% of the installations are interested in walk-up-logon/walk-away-logoff security.

I want to stress that in no way do we tamper with the authentication systems of the operating system; we simply interface with its authentication mechanisms.

Q: Tell me about single sign-on using the XyLoc system.

A: In the healthcare field especially, we've added single sign-on capabilities to our authentication software so we can interface directly with medical applications. So if you're running a medical application program, you can access your own tools right away. We call this the "secured kiosk" mode and it's very useful in the clinical context for shared workstations.

Another interesting application is under Citrix, where doctors can establish a session to connect to a clinical-records package for example; in this scenario, when the doctor leaves a terminal, the session follows her securely to the next terminal. There's no logon/logoff; it's ubiquitous computing: the tools are securely available instantly wherever the authorized user goes.

Q: How much does the system cost?

A: It depends on how big your installation is. The server-only version is XyLoc MD and it includes single sign-on and secure kiosk. For the largest, it ends up about $150 per seat and 18% maintenance agreement per year. Smaller installations cost more because of fixed costs. You can buy a single device called the XyLoc Solo (it's really a demo item) at about $180 plus tax – but that doesn't have a lot of software; it just locks and unlocks for Windows.

[MK notes: This interview should not be construed as an endorsement of the products discussed. I have not personally evaluated the XyLoc system and I have no financial involvement whatsoever with Ensure Technologies.]

* * *

For Further Reading

Kabay, M. E. (2003). Identification and Authentication lecture, IS340 course.
http://www.mekabay.com/courses/academic/norwich/is340/14_I&A.ppt

Lynch, C. (1998). A White Paper on Authentication and Access Management Issues in Cross-organizational Use of Networked Information Resources.
http://www.cni.org/projects/authentication/authentication-wp.html

Kessler, G. C. (1996). Passwords – strengths and weaknesses.
http://www.garykessler.net/library/password.html

Quisquater, J-J (2001). Microsoft error message.
ftp://ftp.sri.com/risks/21/risks-21.37

Wagner, R. (2003). Windows password weaknesses could threaten your enterprise.
http://www4.gartner.com/DisplayDocument?doc_cd=116510

Wagner, R. (2004). Will trade passwords for chocolate.
http://www.securitypipeline.com/news/18902074

What is a Wiegand card?
http://whatis.techtarget.com/definition/0,,sid9_gci852292,00.html

This paper was published as three articles in ***Network World Fusion Security Newsletter*** *in June 2004. It was updated and reformatted in 2009.*

