USER AUTHORIZATION: WHO'S WHO?

APRIL 2004 EJEMS

BY WILLIAM E. OTT

One of the most time consuming and frustrating tasks for an IT manager or database administrator, not to mention that it is an area with security exposure, is user password maintenance and administration of user permissions on the network and data system. Some estimates are that upwards of $500 per user per year or more are spent on these tasks. In a large organization with 100 or more users the problem of maintaining user passwords and permissions can literally turn into a full-time job. Personnel are always coming into the agency, leaving the agency, or changing responsibilities within the agency. All of this turnover requires IT related maintenance.

Obviously your network and data systems require some type of user authentication for security, you do have security, right? There are many opinions on how IT systems are best secured to balance usability with security. In an ideal world, you would have what is known as 'triple factor' authentication for your users; this means that the user must authenticate by knowing something, bringing something, and having something. An example of this would be the user bringing a 'smart card,' knowing the PIN or password for the card, and having their finger, eye, or voice for biometric recognition. Without all three, the user can't gain access to IT resources. This is the ideal but many find it cumbersome and too expensive for the value of what they are trying to protect.

Many agencies go with simply a password for each user. This is known as ‘single factor’ authentication and while better than no user authentication, it is usually relatively easy to defeat for the committed hacker. If you opt for the password only approach, each user should have a unique password; the passwords should be changed at least every 30 days. Additionally passwords should be at least eight characters, not match any word in a dictionary, not be something obvious like spouse or kids names, should contain numbers, letters, upper and lower case, a punctuation symbol or two, and passwords should never be allowed to be used more than one 30 day period. Every thirty days every user should have to create a new, unique password.

There are many technologies available for user authentication and IT security. The IT industry has really started to take security seriously and most new products are built with detailed and robust security in mind. There are varying degrees of sophistication for single, dual, and triple factor authentication. Some of these technologies can run into the thousands of dollars per user. Typically you find these technologies in classified areas of defense and intelligence information systems. The devices I describe for fingerprint and iris scanning are very affordable, rugged, and easily implemented.

‘Dual factor’ authentication is the best compromise of usability and security. This requires the user to know something and to bring or have something. An example is the user bringing a smart card or token and knowing the PIN, or a user knowing their password and having their iris or fingerprint scanned.

Many sub $200 products are on the market now to assist in user authentication and security. Among these are smart cards, proximity cards, fingerprint scanners, iris scanners, and voice print devices. I've used and have been very impressed with both fingerprint scanners and iris scanners for over three years now. One of my clients has more than 1500 fingerprint scanners deployed and in 2 years with nearly daily use we've never had a single false positive reading. Typically personnel register every finger into the security system and when the user goes to any PC, scans their finger, their normal PC profile and permissions are then available to them at that point. There is always some concern that the scanners are 'recording' their fingerprints. That is not how fingerprint or iris scanners work. They typically measure 90 to 150 distinctive points in the scan and then with a mathematical process assign a value. These processes are unique to everyone. The actual print as would be used in criminal investigations is not read or recorded.

The process of using something of the person to identify them is known as biometrics. Long the realm of James Bond, biometrics are now inexpensive enough and certainly accurate enough to deploy to secure IT resources. My personal favorites are the fingerprint and iris scanners. The iris scanners are even good enough that glasses wearers don't have to remove their glasses and contact lenses do not pose a problem to them.

There are a number of products available, those that I use daily in my office and at client sites are the Panasonic Iris Scanner and the Digital Persona UareU

fingerprint scanner. The fingerprint equipment can usually be installed for less than $100 per PC, the iris scanners for roughly $200 per PC.

While these devices can be used to eliminate passwords, they are best applied as a part of your security mix. The underlying IT issues of user maintenance and updates still remains. New users must be added and their respective scans added to the network. Users leaving the agency must have their accounts disabled; you do disable accounts of personnel no longer there don't you? Users changing responsibilities must still have their permissions updated. So biometrics perhaps make the user side of the IT system easier or friendlier, but there isn't much change in what is required on the back office or IT side, in fact it usually gets more complicated.

Why you may ask is this even an issue for my little EMS agency? The answer is really quite simple. HIPAA certainly is the most recent impetus to secure networks and data system where patient information resides, but it is also just good business practice to allow personnel access to only what they need to accomplish their jobs, and it also just the right thing to do.

Hopefully the days of unsecured systems or systems where everyone shares the same password and that password is taped under the keyboard in the top desk drawer are drawing to a close in the EMS industry. It is time to take notice and get serious about data security issues.

I welcome your comments, criticisms, feedback, and ideas. You may contact me at ejems@cpcstech.com

William Ott is president and chief consultant of CPCS Technologies, a NC-based technology consultancy providing services to the public safety and defense communities. He's been involved in EMS since 1981, in field, education and administrative capacities

William E. Ott

Digitally signed by William E. Ott
DN: CN = William E. Ott, C = US, O = CPCS Technologies, OU = Management
Reason: I am the author of this document
Location: Cary, North Carolina
Date: 2004.02.19 21:02:17 -05'00'