



Info Tech Talk

A Newsletter on Enabling Information Technologies by the IRMC E-Government and Technology Department

People and Passwords

By Professors James E. Kasprzak and
Mary Anne Nixon

Inside this issue:

Warlords 2004	4
E-Government Enterprise Architecture Conference 2004 High- lights	5
My Personal Favorites	6
Manager's Guide to RFID Technology (Part 1)	7

Passwords are one of the most frustrating, expensive and time-consuming aspects of operational security. According to Forrester Research, it costs IT organizations between \$340 and \$800 per user to administer passwords each year, primarily because users can't remember the darn things. Another expert notes that users with password problems take up 30 percent or more of help desk time. The task has become so burdensome that a significant number of password management software utilities have been developed to assist help desks and security managers. Costs range from \$2.00 to \$75.00 per user.

The authors have experienced the password problem in teaching and administering distance learning programs. After reviewing the security literature and finding no simple or inexpensive answers to our problems, we decided to approach the question from a fresh perspective – that of the user. By asking current users how they select, remember and use passwords, we hoped to better under-

stand the problems of password management.

What is a Password?

A password is a word or phrase that authenticates the identity of the user. The original concept of "passwords" was first described in the Bible. The book of Judges tells of a battle between two tribes. When one side fled the field of battle, sentries stopped them and asked them to pronounce the word "shibboleth," which means "ear of wheat." Those who pronounced it incorrectly were killed.

*Then said they unto him,
Say now Shibboleth: and
he said Sibboleth: for he
could not frame to pro-
nounce it right. Then they
took him, and slew him at
the passages of Jordan:
and there fell at that time
of the Ephraimites forty
and two thousand.
(Judges, 12:6)*

Computer passwords have the same purpose: they authenticate

(Continued on page 2)

*Hackers...use
"auto dialers" to
access their tar-
gets. The auto di-
aler works by re-
peatedly attempt-
ing to access a
computer, each
time trying a differ-
ent password.*

People and Passwords (cont.)

(Continued from page 1)

the identity of a user. The individual using the password presumably is the only one who knows that password and is therefore authorized to use a system. Originally, computer passwords tended to be short and simple: something the user could remember. Typically those passwords were names of pets, children, football teams or other simple words. In many cases clever hackers could guess these passwords. The most foolish of users might even type in the word "password" as their password. Computer professionals who wanted simple passwords to help them manage large numbers of computers also used such tricks, giving a single standard password to all computers "right out of the box." The new users could then change the password to some better, more secure password. But, of course, many users never did.

Hackers Attack Weak Password Protection

And then things got worse. Hackers began to use "auto dialers" to access their targets. The auto dialer works by repeatedly attempting to access a computer, each time trying a different password. The computer works at high speed, making thousands or tens of thousands of attempts. In theory, protective software can counter this tactic by refusing multiple unsuccessful attempts to access one account. Typically, policy dictates that after "three" or "five" or "ten" tries, the system will deny access to that account. For several reasons, most computer software operations do not employ that strict protection. For example, the average user makes two or three mistakes in any given month. If these errors are made one immediately after another, the user will be denied access until s/he contacts the system administrator. Such denial of access may have serious consequences and is always annoying to the user. In addition, the very use of

such security software may be a danger in itself. A hacker who attempts to access any account four or five times could shut it down and deny access to the bona fide user. Such vulnerability to denial of service attacks could be a very serious weakness in a computer system.

Early auto dialing devices only had access to short dictionaries of the most common passwords. However, advances in computing power and memory allowed hackers to use entire dictionaries to mine for passwords. Today, hacking dictionaries also contain slang words and expressions, proper names and sports jargon. Naturally, there are hacker dictionaries in all major languages, and they include obscene words, regional dialect and expressions taken from movies, television and pop culture. Words, names, even phrases can no longer be used as passwords. They are "weak" passwords.

Strong Password Protection

Modern password practice requires users to employ "strong" passwords. A strong computer password is a random string of characters that employs a series of letters, numbers and punctuation marks. The password should be (at minimum) more than six characters in length and have both upper and lower case letters. If the number of potential characters is raised, the total number of possible combinations rises sharply. It is therefore much more difficult to break these passwords by hacking and nearly impossible to guess them by auto-dialing with dictionaries. A great many security advisors go even further: they require users to generate passwords up to eight characters in length. They also require these passwords to be periodically changed. Of course, a new password cannot simply repeat the old pass-

(Continued on page 3)



word—perhaps not even any of the previous five passwords. And there may be many other restrictions placed upon those who select passwords. For example, no repetitive characters should be used within the password. Of course, it is forbidden to write these passwords down.

Now that security software and security policies require increasingly complex and difficult passwords, it is becoming difficult or impossible for people to remember them. Psychologists believe that random strings of numbers or characters over seven are difficult to remember at all. In fact, random strings over eight characters in length cannot be stored in short-term memory by a significant percentage of the population. The randomness of these characters not only foils the would-be hacker, it also prevents the authorized user from moving the information to long-term memory storage.

And the result? Users have resorted to a variety of unfortunate coping mechanisms just to remember their passwords (e.g., writing the passwords down). Computer security lore is filled with stories of passwords being posted on bulletin boards, pasted on computer screens, written on computer keyboards or hidden under desk blotters. Experts also say that users frequently share their strong passwords.

The situation has become much worse as computer systems have become ubiquitous and as less disciplined users have accessed them. The two authors of this article collectively access a total of more than 30 systems requiring passwords. These systems include classroom, grading, administrative and support systems. In our personal lives, we need passwords for banking, insurance, credit, brokerage, personnel and retail accounts. To add

insult to injury, several of these accounts have different user names -- names assigned by computers. Finally, a number of these password systems require periodic change -- and they don't all change at the same time or allow for the same number of characters from system to system. Naturally, none of this is supposed to be written down. A difficult situation has become impossible.

Coping Mechanisms

Users, faced with this absurdity, have reacted in a variety of ways.

- *Use the same password.* Some people reuse the same password (as much as possible) for many accounts. In a variety of ways, this weakens the password protection. While some systems are highly secure, others have much weaker security. If an individual uses the same password in both a “weak” and a “strong” system, the strong system is clearly undermined. Sharing passwords between systems also insures that if hacker knows a single password, s/he can immediately access other accounts.
- *Write it down.* Because of the complexity and constant changing nature of multiple passwords, many users write them down. We used to laugh at individuals who posted their passwords on their computer screens. Now even sophisticated users can't remember the blizzard of passwords. It is even more certain that passwords are written down somewhere. An intelligent user will take care to secure these passwords or perhaps hide them in a purse or wallet, but this practice represents a significant vulnerability. One security manager recommends putting all of your pass-

(Continued on page 10)



Warlords 2004

By Professor John Feeney

For the last three years the Defense Modeling and Simulation Office (DMSO) has hosted an inter-academy gaming competition between the USMA, USNA, and USAFA. This year's competition was held in Annapolis, MD September 16-18, 2004. The main focus of this DMSO event is to engage the cadets and midshipmen in a competition focused on joint operations in a war gaming context.

Each academy fielded a team of eight players to compete in Warlords 2004. For this year's competition three games were selected: Command and Conquer: Zero Hour, Empire Earth and InfoChess. Each game had a scenario created specifically for this competition.

The Command and Conquer and Empire Earth scenarios were constructed so that the Command and Conquer scenario naturally progressed into the scenario for Empire Earth. The InfoChess competition had two versions: a force on force scenario played over the Internet and an asymmetric warfare scenario played with the board version of the game.

I served as a member of the White Cell as well as

an InfoChess scorer for the competition. While the teams enjoyed the computer games played over the network, they also found the board version of InfoChess with the asymmetric terrorism scenario very engaging.

For example, the team representing the US forces had to adapt to the augmented capabilities of the terrorist pawn pieces and understand that their opponent's objectives will not be the same as their own. Likewise, the team representing the terrorist faction had to understand how their force capabilities could be most effective in a fight against superior technologies. For all but one of the board games the cadets and midshipmen were actively perusing their objectives for the entire four hours allotted for the game.

This year's competition was close with InfoChess deciding the outcome. The USMA team won the competition with the USNA and USAFA teams tied for second. Each team has now won a Warlords competition. The next competition is slated for February 2005 hosted by the USAFA in Colorado Springs, CO.

E-Government Enterprise Architecture Conference 2004 Highlights

By Professor Carolyn Strano

The theme of this year's enterprise architecture conference presented by the E-government Institute was "Beyond the Theory: From Plans to Reality." The conference was attended by 800 participants reflecting a mix of government employees from the federal, state and local levels as well as private sector service providers who support government activities. The main focus of the conference was on using enterprise architecture as a means to an end and as a valuable management tool. Many actual examples of how this is being done by large and small enterprises were shared.

Keynote speaker Clive Finkelstein, known worldwide as the "Father of Information Engineering" provided an example of using logical data modeling from a business perspective. The main point of his presentation was that it may take years to develop a complete, robust architecture of a very large, complex enterprise. You can do this by focusing first on capturing business rules and relationships, and then the enterprise architecture can be developed a piece at a time and can be useful while it is evolving to a greater level of maturity.

A second keynote speaker, Kim Nelson, the Chief Information Officer from the Environmental Protection Agency (EPA) and Co-Chair of the CIO Council's Architecture and Infrastructure Committee, discussed the need to focus on results. Ms Nelson noted that the words "enterprise architecture" may not resonate well with senior managers and executives who are focused on achieving the business or mission of the enterprise. She pointed out that although the EPA spends several billion dollars per year, they were unable to answer seventy-five percent of the basic questions that the American public wanted to know about the environment and its impact on public health. Noting that over half of the information required to perform analysis providing answers to such questions comes from outside of EPA, there is a need to interoperate with the infor-

mation suppliers. Enterprise architecture can be used to meet this challenge.

A third keynote speaker, Mr. Tom Pyke, the Chief Information Officer from the Department of Commerce, described how the Commerce Department uses enterprise architecture to tie together federations that make up the diverse program within the Commerce Department. He described how the architecture is used to support investment decisions, identify duplicative processes and systems, improve information sharing and quality, and enable technology to support business needs. Mr. Pyke provided several specific examples where the Department has used enterprise architecture to reduce costs and improve services to the citizen.

The conference offered a choice of three tutorials: one on best practices, another focused on practical strategies for using the Department of Defense's architecture framework and the third described how to comply with the Office of Management and Budget's guidance to better align information technology investments with business operations. There were three separate tracks in which presentations and panel discussions focused on three themes: Practitioner's Experience; Planning, Implementing and Managing Enterprise Architecture Programs; and New Applications and Strategies for Enterprise Architecture. There were two "Birds of a Feather" sessions. One session discussed rapid delivery of enterprise architecture and using enterprise architecture to gain rapid Sarbanes-Oxley compliance. The second session examined how to use enterprise architecture to facilitate political transition planning, a very timely topic given the upcoming national election.

The enterprise architecture exhibition featured premier companies showcasing solutions and technologies. While previous exhibitions focused largely on

(Continued on page 6)

My Personal Favorites

By Professor Mary Cole Carroll

As the title indicates, the websites listed here reflect the personal preferences of a member of the IRMC faculty – not the endorsement of the college. We feature the website recommendations of Mary Cole Carroll, Professor of System Management, Information Operations and Assurance Department. She teaches lessons in information infrastructure, enterprise integration and enterprise security strategies. Her favorite websites show both her professional and personal interests.

<http://www.bitsinfo.org/bitsxmatrix2004.xls> provides a spreadsheet of security questions and concerns that should be addressed prior to entering into an outsourcing relationship. It was developed by BITS, a non-profit consortium of major financial institutions and can be tailored to meet the needs of your organization.

<http://www.csrc.nist.gov/> is a great source of information about security information. It provides links to many related NIST Information Technology Laboratory projects and updates on new publications and events.

<http://techcenter.gmu.edu/programs/cipp.html> provides information about the Critical Infrastructure Protection Project (CIP Project), a joint effort of George Mason University and James Madison University. Links to the monthly CIP reports are provided.

<http://wordsmith.org/awad> is the source of the A. Word.A.Day newsletter. Daily words, grouped by themes, include definitions, examples and pronunciation.

<http://www.pcmag.com/article2/0,1759,1516939,00.asp> provides links to “50 from the Best of the Internet.”

And, great sources for information security:

<http://iase.disa.mil/index2.html>
<http://www.ists.dartmouth.edu/ISTS/>
<http://www.infosyssec.net/index.html>
<http://www.sans.org/rr/>
<http://www.s bq.com/index.html>

E-gov Conference (cont.)

(Continued from page 5)

the tools used to develop and manage the enterprise architecture, this year there was growing emphasis on the tools needed to implement and use the architecture to support executive and management decisions and planning.

The conference concluded with the Excellence in Enterprise Architecture Awards Reception that recognizes best practices in enterprise architecture leadership and government transformation. The Federal Railroad Administration was honored for using private sector best practices for future scenario planning. The Department of Interior won for leadership in government transformation using enterprise architecture methodology and repository.

The U.S. Marine Corps' First Expeditionary Force was recognized for implementation of its enterprise architecture to screen suspects in Iraq. The Department of Defense Medical Logistics Standard Support won for using enterprise architecture to standardize medical logistics processes across the joint services. Lastly the Government Accountability Office (GAO) was recognized for their contribution to maturing enterprise architecture as a discipline across the federal government.

Manager's Guide to RFID Technology (Part 1)

By Professor Les Pang

Similar to bar coding, Radio Frequency Identification (RFID) provides information about people, animals, goods and products in transit. However, unlike bar coding which tracks product lines or groups, RFID technology uses radio frequencies to automatically detect *individual* units and the information about these units. Use of radio frequency eliminates line of sight requirements and permits wireless detection.

Although functionalities provided by this technology far surpass those provided by bar coding, it does not mean that RFID will replace bar codes. RFID tags are far more expensive than bar coding. Nevertheless, RFID offers a number of advantages over the current bar-code technology which uses Universal Product Codes (UPC). Codes in RFIDs are long enough so that each tag may have a unique code whereas a specific line of products are limited to a single UPC code. The distinctive nature of RFID tags results in an object that can be individually tracked as it moves from location to location. For product items, this characteristic can help retailers reduce theft of specific units and other forms of loss.

The U.S. Department of Defense (DOD) has mandated that its partners use RFID technology. The agency is requiring its roughly 40,000 suppliers to put RFID tags on pallets and cases as well as on single items costing \$5,000 or more beginning Jan. 1, 2005. As an incentive, suppliers that tag their shipments can participate in the agency's fast-track billing process which will be brought about by the quicker processing of deliveries.

RFID technology ensures better inventory control which leads to improved merchandise availability. As this technology expands, RFID technology is expected to keep costs down for all players involved in the supply chain.

Wal-Mart, Target, Albertson and other private sector retailers are aggressively pursuing the use of RFID tags on cases and pallets by their suppliers.

Wal-Mart has required that its top 100 suppliers provide the tags by 2005 for tracking merchandise, matériel, and goods.

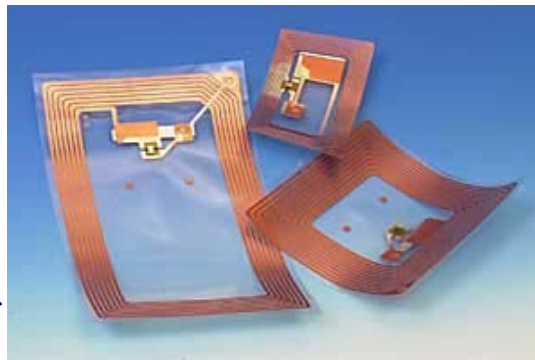
How Does It Work?

The system detects tags through readers in a network consisting of antennas. It wirelessly and seamlessly collects data without human error. The RFID application does not end at keeping track of products; it goes a step further by identifying the product and then taking a specific course of action based on its detection such as adding or deleting an item from a database.

RFID implementations require four elements: tags, readers, antennas and network systems. This technology extracts information from tags, also known as transponders, wirelessly and automatically. Consider an arrangement of antennas connected to reader, which in turn is connected to a computer.

When a tag enters the radio frequency (RF) field, it derives power from radio frequency signal. This energy allows a "passive" tag (no battery power) to transmit data, typically an identity, often in the

(Continued on page 8)



Manager's Guide to RFID Technology (cont.)



(Continued from page 7)

form of an Electronic Product Code (EPC). Unlike bar codes which tell you that a carton contains product XYZ, EPCs can specifically identify one box of XYZ from another box of XYZ.

This information is fed to a reader via the antenna. The reader interprets the information and translates it into binary format before relaying it to the connected computer. The computer can perform an action based on data received -- this could be simply identifying existence of an item or adding or deleting it from its inventory. In some cases, the computer can also send a message back to the tag. Not all but some types of tags do allow writing data back to them.

Applications

RFID technology has been in use since World War II. During that conflict, the Royal Air Force employed the technology to track fighter bombers over the English Channel. The DOD has been using active (battery-powered) RFID tags since the early 1980's to track equipment. Mobil's Speed Pass has been used at gas stations to provide faster access since 1997.

Potential applications for RFID run in the thousands and they can be implemented in almost any kind of industry and environment. Here is a sample of RFID applications:

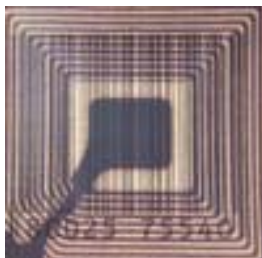
Access control - Many buildings are using contactless RFID tags as physical access cards. Washington DC's transit system uses an RFID-based smart card system called SmarTrip. Used by more than 360,000 of its Metrorail travelers, a passenger carrying the card can simply stroll by a reader at the entrance of one station and past another at the exit of a another station and the cost of the trip can be automatically calculated and deducted from a pre-paid account. This helps the passenger avoid waiting in line for purchasing paper fare cards. These cards are also used to pay commuter parking lot fees and bus trips within the regional network.

Toll booths - Toll facilities are equipped to read RFID tags mounted on the front side of vehicles. Examples of automatic toll collection systems include Virginia's SmartTag system, the EZ-Pass system in the northeast U.S., and California's FasTrak. The tag is linked to a prepaid replenishable account that is debited to pay for the toll. These tag-equipped vehicles no longer need to stop and pay the toll thereby reducing back ups at these locations.

Livestock tracking - Vermont Senator Patrick Leahy told a Georgetown University audience that he had first-hand experience with RFID technology from his own involvement in a Vermont pilot program tracking cattle to thwart outbreaks of illnesses such as mad



The U.S. Department of Defense (DOD) has placed a strong mandate for its partners. The agency is requiring its approximately 40,000 suppliers to put passive RFID tags on pallets and cases, as well as on single items costing \$5,000 or more, delivered to the DOD beginning Jan. 1, 2005.



(Continued on page 9)



(Continued from page 8)
cow disease.

House pet identification – RFID tags have been embedded in dogs and cats to ensure their identification if they are lost or stolen.

Tracking wounded soldiers - RFID technology was used for tracking wounded soldiers in the war in Iraq. The U.S. Navy's Fleet Hospital in Pensacola, Florida, tested a system involving RFID wristbands, which store the soldier's identification and medical information regarding his condition and treatment as he moves from the battlefield to a hospital. This system replaced a manual, labor-intensive system consisting of pen and paper, cardboard tags, and a centrally located whiteboard that showed patient movement throughout the hospital. The U.S. Navy is also using RFID technology to track the status and location of prisoners of war, refugees, and others arriving at the hospital.

Anti-counterfeiting - The Internal Revenue Service is investigating the potential of embedding RFID tags in money to prevent or at least reduce the incidence of counterfeiting.

Euros, the paper currency for the European Union, may get RFID tags to stop counterfeiting. These tags will also have the ability of recording data such as details of the transactions involving the subject paper note. It is expected that this approach would prevent money-laundering, track illegal transactions and also prevent kidnappers demanding unmarked bills.

Personal Identification - One way personal identity can be determined is through the use of VeriChip, a small RFID chip about the size of a grain of rice. Each VeriChip contains a unique identification number which is used to access a

database consisting of personal information. It is implanted just under the skin not unlike receiving a shot and it is scanned with a proprietary scanner. Because of this approach, the developers claim that the VeriChip cannot be lost, stolen, misplaced or counterfeited.

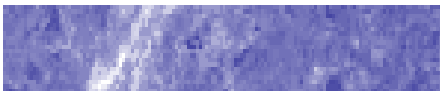
One interesting example of the use of the VeriChip can be found at the Baja Beach Club in Barcelona, Spain. VeriChip is used in a VIP area where select customers can volunteer to have a RFID chip implanted to expedite access to the club. These customers no longer have to wait in line to pay and get in. They merely walk through the scanner, which notifies the club that they are authorized to enter. Club members can have the chip implanted into any part of their body as long as it is accessible to a scanner. Tuesday nights has been designated “Implant Night” where customers can be implanted between drinking and dancing.

IPv6 – Because of the overwhelming popularity of the World Wide Web, we are running out of IP addresses based the present 32-bit IP version 4 addressing scheme. IPv6 offers a new expanded IP address space designed to use 128 bits, of which 60-bit chunks are typically allocated to end-users. This allocated space provides enough room to hold EPC numbers. Therefore, the integration of RFID technology and the Internet presents tremendous opportunities. One example is that you can assign IP addresses to “smart” appliances and monitor their status remotely.

This article will be continued in the next issue. The following is a list of remaining subjects that will be covered:

- ◇ *Pro's and Con's (including privacy concerns)*
- ◇ *Recommendations*
- ◇ *Conclusions*

People and Passwords (cont.)



It's time for IT professionals to recognize that the current demands for password use and security are not reasonable, and many password controls are being skirted by users – including IT professionals themselves.

(Continued from page 3)

words on a floppy disk and storing it in a safe place. She does point out that if the magnetic medium fails, all passwords will be lost.

- *Create patterns.* Some users employ a mechanism we call “pattern creation.” Individuals are making physical patterns, shapes or sequences of keystrokes on the keyboard. When the time comes to change the password, a succeeding pattern is selected. For example, one such pattern is “1Qwerty.” “Qwerty” is the name of the standard secretarial keyboard. Trace out the pattern on your own keyboard and you will see how the concept is implemented. When the password needs to be changed, it will be revised to the second row of the keyboard “2Asdfg.” Many such patterns are possible on the keyboard. *(Note: The authors note that this coping mechanism has also been found in users of cellular telephones. Some users do not remember the numbers they are dialing, but push the buttons according to specific patterns on the telephone keypad.)*
- *Repeat the password.* Computer policy may require that all passwords must be changed but the same passwords may not be duplicates of those used for the past three times. Some clever individuals have changed their passwords three times in rapid succession, ending up with the original password. This enables them to continue to use the same password while ostensibly complying with the password policy.
- *Omit vowels (or consonants).* Some users

(Continued on page 11)



(Continued from page 10)

omit the vowels from a common word and use the consonants as the password. Others conversely take a common word or phrase and omit the consonants and use the vowel sequence in the phrase as the password.

- *Misspell a common word.* Another mechanism is to take a common word and repeat a consonant, transpose two letters and/or use a homonym to produce a unique but easily remembered password. For example, instead of “lied to,” use “Lyedtoo” as the password.
- *Use the license plating technique.* This mechanism uses numbers or symbols which allow you to phonetically sound out a word or phrase rather than writing it out (e.g., “ILVU2” or “IN A MNIT” or “1 HIP 1.”) We commonly see this technique used on vanity automobile license plates.
- *Manipulate familiar character strings.* Using some numbers of your social security number, previous home address or telephone number plus some other word or combination of letters can be used to create passwords.

Conclusions

We see no immediate answer to password problems. Administrators use software programs to enforce security rules that require humans to do things beyond their capabilities. People are coping in ways that make the systems more vulnerable. How long will it be before hackers include keyboard patterns like “Qwerty” in their password dictionaries? Even the security industry itself seems uncertain as

to how to deal with this complexity. Password coping techniques suggested by prestigious experts at the Canadian Management Association include such oddities as using recognition of “a random series of inkblots”. Another professional at the Idaho Business Review suggests using the “initials of your children and the order they were born in, throwing an ampersand between each: m1&j2&s3” or “substitute some other character for some of the letters.... Using this method the common word ‘houses’ could become the robust password: (H0u\$e5)”. Such techniques are not practical and only show how unreasonable password requirements have become. Some experts have given up entirely and say that users can’t manage their own strong passwords without supporting software. There are small software packages designed to help users manage their personal passwords.

It’s time for IT professionals to recognize that the current demands for password use and security are not reasonable and many password controls are being skirted by users – including IT professionals themselves. IT managers need to provide assistance to users – with access cards, user password management programs and other technical assistance, rather than simply setting policies that cannot be enforced.

The ultimate answer, if there is one, will be in the implementation of biometrics, probably in concert with simple passwords and complex algorithms placed on computer cards. As every security expert knows, access to computers ideally is governed by “something you are”; “something you have”; “something you know”. The password is the “something you

(Continued on page 12)

People and Passwords (cont.)

(Continued from page 11)

know” and until we get much more reliable, cheaper biometrics or until we distribute secure common access cards for all users, it will remain a weak first line of defense for computer systems.

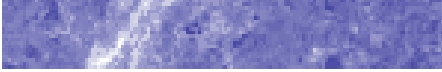
Portions of this article were published previously in the Journal of Information Assurance, Security and Protection. This version has been updated and supplemented for IRMC use, with permission of JIASP. The earlier version, with supporting citations and bibliography, is available on request.

“The views expressed in this publication are those of the authors and do not reflect the official policy or position of the National Defense University, the Department of Defense or the U.S. Government.”

Here’s Our Web Address!!!

<http://www.ndu.edu/irmc/elearning/infotech.html>

CHECK OUT OUR PREVIOUS ISSUES!



The ultimate answer, if there is one, will be in the implementation of biometrics, probably in concert with simple passwords and complex algorithms placed on computer cards.

INFORMATION RESOURCES MANAGEMENT COLLEGE

The World Leader in Information Resources Management Education

300 5th Avenue Marshall Hall (Building 62)
Fort Lesley J. McNair, DC 20319
(202) 685-2096
<http://www.ndu.edu/irmc/>

Director: Dr. Robert Childs

**Dean of Faculty & Academic
Programs: Dr. Elizabeth McDaniel**

**Chair, eGov and Technology
Department: Dr. Judith Carr**

Newsletter Editor: Dr. Les Pang