Nick Bentz
Graduate Student
Comp. Networking and Applications
College of Science and Engineering
St. Cloud State University
beni0502@stcloudstate.edu

Tirthankar Ghosh
Assistant Professor
Comp. Networking and Applications
College of Science and Engineering
St. Cloud State University
tghosh@stcloudstate.edu

Network Performance Evaluation for Large Scale Deployment of Biometric Security

ABSTRACT

The advent of biometric access control devices presents us with great opportunities for increased computer and network security along with time and cost savings. An inexpensive fingerprint reader can be obtained for as little as $39.99 and connected to a PC's USB port. Each time a user wishes to log-on a finger is merely placed on the scanner and, if accepted, the authorization takes place in seconds. Fingerprint readers work by comparing a sample captured during the initial enrollment against a sample obtained during an attempted log in. Most systems don't store a full digital image of a fingerprint but rather an analysis of that image. This saves on storage space, processing power and possibly bandwidth. The exact analysis methods vary from vendor to vendor but they usually rely on analyzing *minutia* which are the specific characteristics of each fingerprint. When a predetermined number of minutia are matched authentication takes place. Increased security is a major advantage of fingerprint readers over traditional forms of security such as passwords and tokens. Moreover, cost savings can also be realized in many ways by switching to a fingerprint reader. Savings can be realized by users, server administrators, information security personnel, and help desk personnel. The increased security and time and cost savings surrounding the use of such systems will probably be driving the push toward implementing these systems in the near future. However, determining the impact these devices will have on a Local Area Network (LAN) remains to be seen. Our study explores the use of fingerprint readers on a LAN to determine their effect on traffic and performance. We will perform an experimental analysis over an existing LAN by deploying several fingerprint readers and will carry out performance evaluation of the whole network by studying the traffic flow over a period of time

1. Introduction

The advent of biometric access control devices presents us with great opportunities for increased computer and network security along with time and cost savings. An inexpensive fingerprint reader can be obtained for as little as $39.99 (like the Microsoft DG2-000020) and connected to a PC's USB port. Each time a user wishes to sign on, a finger is merely placed on the reader and if accepted the authorization takes place in seconds. The fingerprint is certainly one of the easiest to use biometrics, and their uniqueness has been proven through history.

Fingerprint readers work by comparing a sample obtained during an attempted sign on against a sample captured during the initial enrollment. The initial enrollment fingerprint image data is encrypted and stored on the desktop for local authentication, or stored on a domain controller for network authentication. Most systems don't store the full digital image of a fingerprint but rather rely on an analysis of that image. This saves storage space, processing power and possibly bandwidth. The analysis methods vary from vendor to vendor but they generally rely on analyzing *minutia* which is the specific characteristics of each print. When a predetermined number of minutia are matched authentication takes place [1].

Increased security is a major advantage of fingerprint readers over traditional forms of security such as passwords and tokens. Biometric access control devices link the authorization process to the biometric characteristics of an individual, unlike tokens and passwords which may be used by others. Although tokens are in themselves secure they can be lost, stolen, or given to someone else. The same is true of passwords that are written down. The advent of password cracking software like L0phtcrack or Rainbow that can be purchased by an individual and can easily crack 14 character or less passwords is bringing to an end the use of weak passwords. Biometric solutions like fingerprint readers combine high security with convenience. The fingerprint scanners may be used alone or as part of a multi factor authentication process.

Cost savings can be realized in many ways by switching to a fingerprint reader. Savings can be realized by users, server administrators, information security personnel, and help desk personnel.

Users spend a lot of time typing in passwords. Fingerprint readers can greatly reduce that time. An average user may have to type their password 5-10 times a day, not to mention all the times the screen saver starts up and requires another password entry. This may seem like a small amount of time for an individual but when multiplied by the number of employees in an organization and the number days worked it can add up. Additionally time is spent at each change interval trying to create a new password that is complex enough to not be broken yet easy enough to remember.

Server administrators are constantly spending time adjusting their corporate password policies to make them more and more secure. At this point in time a complex password is considered to be at least 15 characters long, contain upper and lower case letters, include numbers and special characters, and be changed every 30 days. Fingerprint readers would

ease the burden of server administrators placed on them by the user community. The fingerprint readers could even be used by the server administrators themselves for server access.

Information Security departments can spend a lot of time harvesting password hash files and cracking weak passwords. Then they need to notify the users associated with the weak passwords, insist they change them, and provide guidance for creating yet again even more complex passwords. I.S. departments must also stay on top of the latest password cracking technology and purchase tools and create strategies to prevent it.

Help desks perform password resets on an ongoing basis. The Gartner Group [2], an IT industry research and analysis firm, states that 40% of all help desk calls are for forgotten passwords, and that each year companies spend $200-$300 dollars per user trying to maintain secure passwords. The time involved includes taking the phone call, opening up a ticket, logging in to reset the password, and then closing the ticket. Users constantly forget or mistype their passwords. A user may come back from a 2 week vacation having lost all recollection of passwords, but one would usually still have all of their fingertips to use on a fingerprint reader.

The increased security and time and cost savings surrounding the use of such systems will probably be driving the push toward implementing these systems in the near future. The information available about the fingerprint reader authentication process used by each vendor is often proprietary and many of the details are limited. Determining the impact fingerprint readers will have on a LAN remains to be seen. Although there is an abundance of information regarding biometric fingerprint readers, precious little deals with the bandwidth usage of these devices. This lack of information is what interested us to research this subject. There are several questions that need to be answered.

This paper will explore the use of fingerprint readers on a Local Area Network to determine their impact. We have chosen the DigialPersona U.are.U 4000 model of fingerprint reader and will be performing all experiments on this model. The research will answer the following questions:
1. Does the use of a biometric fingerprint reader adversely affect network performance on a LAN?
2. Do the fingerprint database files stored on the server for authentication affect server performance?

The rest of the paper is organized as follows. Section 2 explores a detailed literature review. Section 3 describes our experiment with a detailed analysis of the results. Finally, section 4 concludes the paper.

2. Review of Literature

The majority of information available on the subject of biometric fingerprint scanners is centered on technology, security, cost savings, and deployment costs. The lack of information on the bandwidth implications of their use can indicate that it is unknown, un-researched, or that it is simply a non-issue. Of all the common biometric sources

available (fingerprint, retinal pattern, hand print, voice print, keystroke, and signature) the fingerprint is the most convenient to use. However, Whitman [3] points out that when thinking about security the fingerprint is ranked second to the iris pattern. People are still concerned that their fingerprints are personal data and they are concerned how it may be used. An International Biometric Group report released on September 5, 2001 showed that fingerprint scanners held 48.8% of the market share, while second place was facial recognition with 15.4% [4].

Weaver [5] asserts that since 1892 when fingerprint data was first collected there have been no known cases of two people having the same fingerprints. Global features may be the same but the minutia are always different. Chang [6] points out that minutia points were first identified by British anthropologist Sir Francis Galton in 1892.

Fingerprint scanners operate by scanning the fingerprint, analyzing it, and then transmitting the analysis to the PC or domain controller for authentication. Weaver [5] states that the fingerprint image taken during authentication is turned into a mathematical template of 256 to 512 bytes and then sent on for comparison against the "enrolled" template. Because the entire fingerprint scan is not transmitted, the possibility of a replay attack is diminished.

Nanavati et al [7] are of the opinion that fingerprint scans will be small. They state that fingerprint scan sizes will be 200 to 1000 bytes, and that is, "…a very small amount of data by any measure". The authors go on to mention that the competing scanning technologies are minutia based and pattern matching, with minutia based holding 80% of the market as of 2002. The larger base of minutia based scanners could be the fact that their files (200-500 bytes) are 2-3 times smaller than pattern matching (1000 bytes). Ruggles [8] presents a similar view of the size of a fingerprint scan. He places a fingerprint scan at 512 to1000 bytes, a retinal scan at 35 bytes, and an iris scan at 256 bytes.

The Digital Persona [9] U are U 4000 product generates a host interrupt when a fingerprint has been captured, signaling that it is ready to send a template. Other vendors fingerprint readers constantly send video captures that the host must analyze to determine if it is a fingerprint capture or not. This will certainly consume some level of bandwidth.

The IBEA (International Biometric Industry Association [10] reported on March 21, 2006 that a researcher in the Finnish military hacked into a Microsoft fingerprint scanner and is able to effect an authentication with the information he gathered between the scanner and the USB port. The researcher, Mikki Kiviharju, noticed a statement in the Microsoft fingerprint literature that warned that the scanner should not be used to protect sensitive data. It should only be used as a convenience. This led him to sniff the scanner to USB connection only to discover it was not encrypted.

3. Methodology and Results

A careful selection of hardware and software has been done to perform the experiment. The domain controller is an HP BL20P with a single Intel Xeon CPU running at 3.3 Ghz. The hard disk drive is 36 gigabytes, and it has 3 gigabytes of memory. The domain controller operating system selected for this project is Microsoft Windows XP, and is running Miscrosoft Active Directory. The workstation operating system selected for this project is Microsoft Windows XP Professional. All workstations involved in this testing were either Dell Optiplex GX240 with Pentium 4 CPU's running at 1.50 GHz, 512MB of RAM, and 18GB HDD, or Dell Latitude D610 with Pentium M CPU's, running at 1.86 GHz, .99GB RAM, and 55.7GB HDD. We have chosen the Digital Persona U.areU. 4000 model. Although there is no completed industry standard on the subject of fingerprint readers, the U.S. military has the most stringent guidelines we found so far and this model fits their criteria. This model can read the fingerprint in any direction, and it will ignore the latent print left on the reader from the last use. It has fake finger detection and will deny 2 dimensional copies and 3 dimensional models. The software works with Microsoft Active Directory, and has 512 dpi resolution. 20 fingerprint readers were purchased along with a 20 user license. The LAN used to test the fingerprint readers is an Ethernet network comprised of a Cisco 3750 core switch, and 12 Cisco 3550 edge switches for user access (See Fig. 1). Attached to this network are 201 user PC's, 15 printers, and 17 servers. All switch ports are set to auto-negotiate and are running at 100 mbps., full duplex. To gather and analyze the data we used a Dell Latitude D610 Laptop running Network General Sniffer Portable LAN Suite version 4.80.044. The network architecture is shown in the figure below.

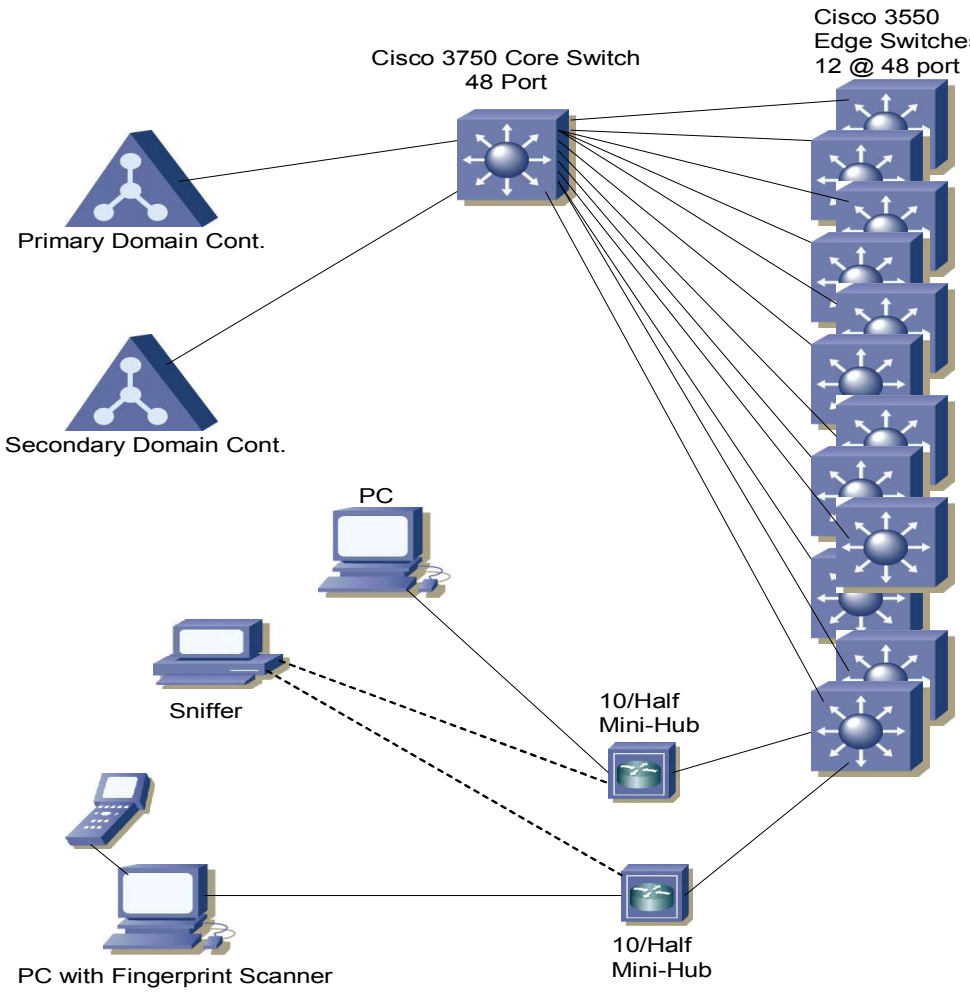

Fig. 1

The two research questions stated earlier can be modified to provide two null hypotheses which can be tested through experimentation.

H1. The use of biometric fingerprint readers does not affect network performance on a LAN?
H2. The fingerprint database files stored on the server for authentication do not affect server performance?

To begin the experiment we first installed the DigitalPersona client software on a Dell Optiplex GX240. The DigitalPersona program file on the client PC was about 18.9

million bytes. Next we loaded the Digital Persona server software on the Active Directory domain controller and the file was about 12.6 million bytes. Connecting the fingerprint reader was a matter of plugging it into a USB port. In order to determine exactly what an authentication looked like, what protocols were used, how large they were, and how long they took, a series of experiments were devised to analyze and compare the logon processes involved in password authentication and fingerprint authentication. A total of 15 experiments were conducted. Experiments 1-5 were of a 9 character password logon on a PC with no fingerprint reader and no DigitalPersona client installed. Experiments 6-10 were of a 9 character password being authenticated on a PC equipped with a fingerprint reader and the DigitalPersona client software installed. Experiments 11-15 were of a fingerprint authentication on the same PC as in experiments 6-10 which were equipped with a fingerprint reader and the Digital Persona client software installed.

Each experiment was conducted in the same manner with the network sniffer connected inline to a 10meg/half duplex hub between the PC and Cisco 3550 edge switch port. The client PC's were thus operating at 10meg/half duplex for all tests. The sniffer capture was started with the client PC at a logon screen. Next the particular type of logon as indicated by each test was performed. When the authentication was accepted and the desktop was built the trace was stopped. A capture filter was set to only include any traffic going to or coming from the client PC. This filtering was done to eliminate broadcast traffic and make the trace easier to analyze

Experiments 1-5 of a 9 character password logon on a PC with no fingerprint reader and no DigitalPersona client installed showed four Kerberos frames being exchanged (Fig 2). 1,710 bytes were transmitted from the test PC to the domain controller, and 2,747 bytes were returned by the domain controller. The total byte count for this exchange is 4,457. All 5 tests provided identical results. The average time for the exchange to take place was 0.009198 seconds.

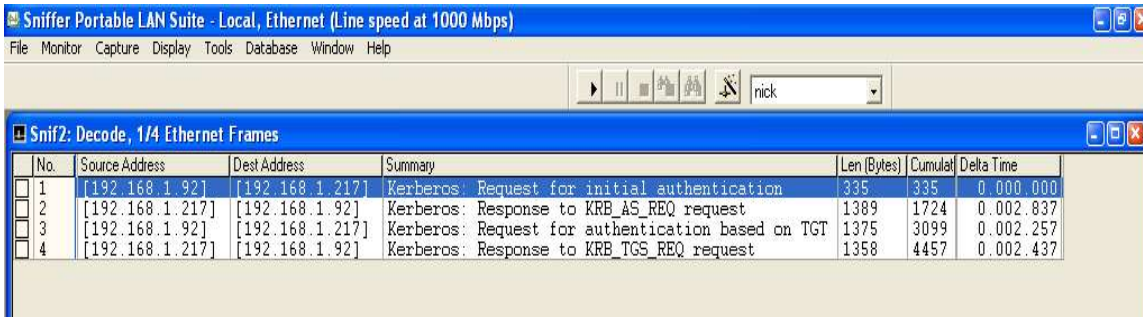

Fig. 2

Experiments 6-10 of a 9 character password being authenticated on a PC equipped with a fingerprint reader and the DigitalPersona client software installed showed results similar to experiments 1-5. The same Kerberos exchange took place and the frame sizes were almost identical (Fig. 3). The total byte count of Kerberos frames was always 4,439. The average time to complete the exchanges was 0.007855 seconds.

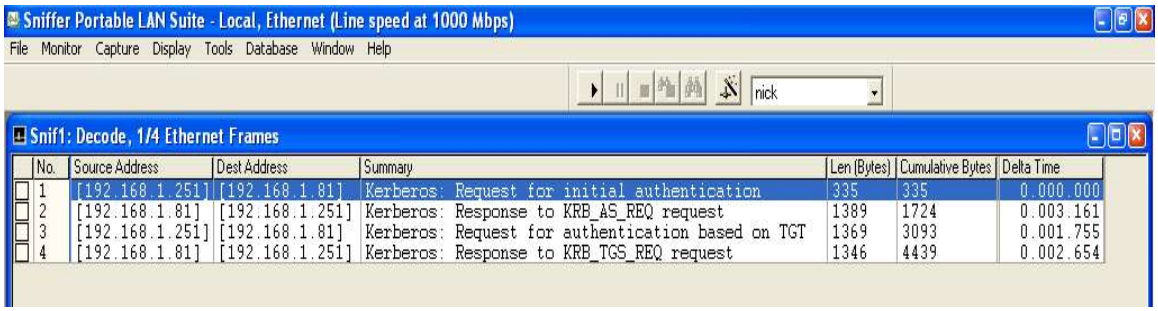

Fig. 3

Experiments 11-15 of a fingerprint authentication showed a different sequence of events (Fig. 4). When using the fingerprint reader the first event to occur is an RPC exchange, followed by the same Kerberos traffic as seen previously. The RPC exchange is as follows: Bind, Bind Ack, Alter Context, Alter Context Response, Request, and Response. All five tests showed the same sequence. The RPC frames exchanged always total 3,023 bytes. With the Kerberos portion being 4,439 bytes and the RPC frames being 3,023 the total byte count is 7,462. Since the average time to complete the RPC portion was . 006,811 seconds, and the average Kerberos time was 0.007855 seconds, that puts the total exchange time average at 0.014666 seconds.

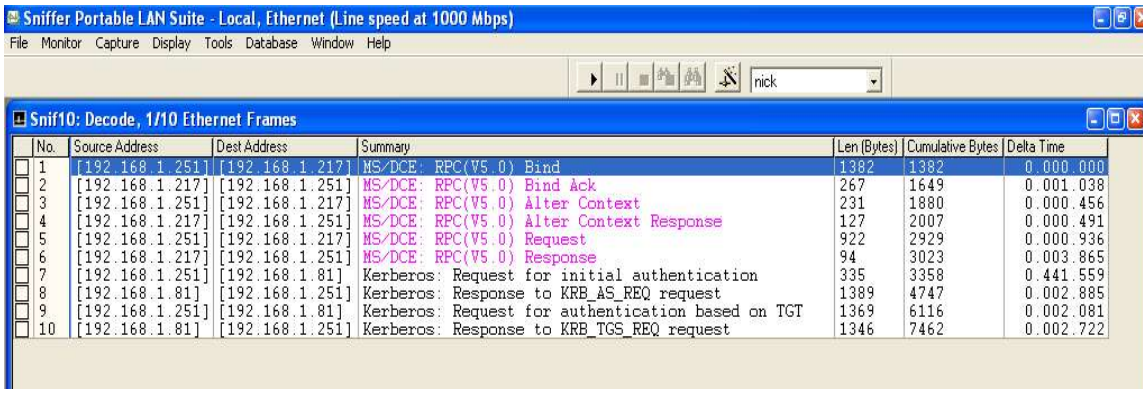

Fig. 4

It can be seen from the above results that no RPC frames are found at logon when only using a password on either PC. The observation that a particular collection of RPC frames are only found during logon on when a fingerprint reader is used gives an indication that the RPC frames are indeed a result of the fingerprint scan. It can be reasoned then that the first, and largest RPC frame transmitted from the client, the RPC Bind frame, which is 1,382 bytes long is probably the frame that contains the fingerprint information. Although this frame is only 1,382 bytes long it should not be viewed individually. It should be viewed as a part of a process, and therefore the six RPC frames should be considered together to make up the overhead induced by the fingerprint reader. It can then be said that the fingerprint reader adds 3,023 bytes to the authentication process. The results are summarized in Table 1.

Tests	Frame Type	Bytes	Total Bytes	Milliseconds

1 – 5 Password	Kerberos	4,457	4,457	9.198
6-10 Password	Kerberos	4,439	4,439	7.855
11–15 Fingerprint	RPC/Kerberos	3,023 / 4,439	7,462	14.666

Table 1. Comparison of authentication types in frame types, bytes, and milliseconds.

In an attempt to illustrate the effect of authentication on bandwidth to the domain controller an additional experiment was devised. This time the sniffer was connected to an available port on the Cisco 3750 core switch that housed the domain controller. The domain controller traffic was then copied to the sniffer port using the SPAN command. SPAN is Cisco's Switched Port ANalysis function for port mirroring. This method allowed us to monitor the domain controller at its' true 100 mbps throughput. It was not convenient to coordinate the simultaneous authentication of the 20 fingerprint readers that were deployed so a substitute was created. From the same client PC used for the fingerprint authentication testing we initiated a series of ping tests. We decided to send a series of ICMP ping packets to the domain controller. Five packets at 1500 bytes would produce 7,500 bytes of data, which is just over the 7,462 bytes used in the real authentication. Multiplying this by 20 to simulate the 20 users that could possibly authenticate would send 150,000 bytes. A Sniffer graph of the in/out byte count taken at 15 second intervals showed no discernable indication of excessive activity caused by the simulated logons.

Additionally the DigitalPersona software does induce other overhead to the communication process but it is quite minimal. An example of this is when the client PC sends a Query Name frame to the DNS to indicate that a DigitalPersona UareU reader is installed and available. The DNS responds with an OK, and the sequence is repeated one more time. This process only puts 4 packets on the network, and exchanges a total of 580 bytes (Fig. 5). This exchange only occurs once in a sign on session. For example if the PC has been sitting idle for some time and not logged on, the first time a finger is placed on the scanner the DNS exchange will take place. We tested this by trying to authenticate with a non registered finger. This caused the DNS exchange and the authentication was denied. We then tried to authenticate 3 other incorrect fingers, and these subsequent attempts did not trigger the DNS exchange.

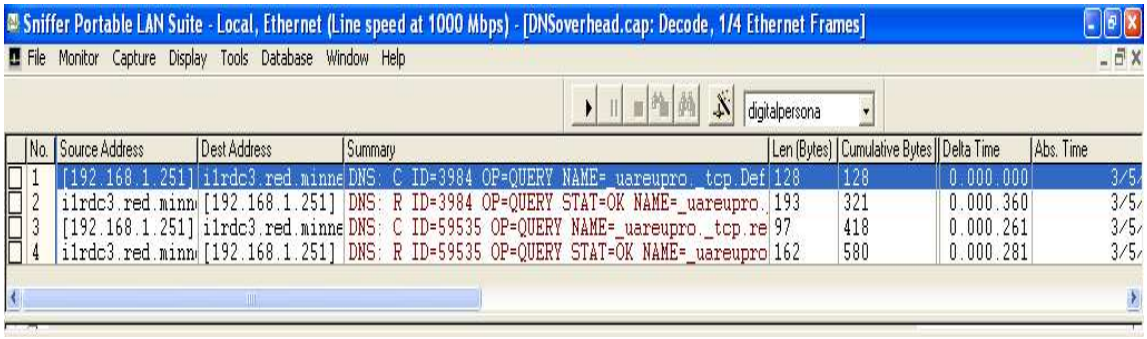

Fig. 5

4. Conclusions

The domain controller had the Digital Persona server software installed and the space required for this was minimal, as was the space required for each fingerprint template. We only had a 20 user license, and the fact that the templates are encrypted and compressed meant that they took up very few server resources.

This study was designed to examine the bandwidth implications of deploying biometric fingerprint readers to a network, and the impact they might have on domain controller server performance and resources. As can be seen from the results although fingerprint authorizations are 59% larger than ordinary password authorizations the overhead they induce (3,023 bytes) is still quite small and their impact is almost immeasurable. From a network bandwidth perspective fingerprint authorizations should be considered no different than password authentications.

References

[1] "DigitalPersona Fingerprint Recognition System Technology Overview & Competitive Analysis", White Paper, September 20, 2005, http://www.digitalpersona.com.
[2] Vance, B. (2003), "Eliminating the Password Nightmare", 2003, http://www.digitalpersona.com/docrequest/pdf1?pdf=18.
[3] Whitman, M. (2004), "Principles of Information Security", Course Technology, Inc., 2004.
[4] Hakala,David, "Buying into Biometrics", http://www.channelweb.com/showarticle.jhtml?articleid=18819358&pub=crn.
[5] Weaver, Alfred C., "Biometric Authentication", Computer, Feb 2006, vol 39, no. 2. pages 96-97.
[6] Chang, David H., "Fingerprint Recognition Through Circular Sampling", http://www.galton.org/fingerprinter.html.
[7] Nanavati, Samir, Thiene, Michael, Nanavati, Raj, "Biometrics: Identity Verification in a Networked World", Pages 52-56, 2002.
[8] Ruggles, Thomas, "Comparison of Biometric techniques", http://www.bio-tech-inc.com/bio.htm.
[9] "DigitalPersona. U.are.U Fingerprint Recognition System Technology Overview & Competitive Analysis, http://www.digitalpersona.com.
[10] International Biometric Industry association, "Researcher Hacks Microsoft Fingerprint Reader", March 21, 2006. http://www.ibia.org/biometrics/industrynews-view.asp?id=451.