

The Market for DigitalPersona Biometric Security Solutions

The Value of Information

Revolution. We've used the word almost to the point where it is meaningless, but there really is no better word to describe the dramatic change in both the value and volume of electronic information. With this change has come the realization that businesses face an increasing amount of exposure from the loss or theft of that data. Lost or stolen information can potentially cost millions of dollars in lost strategic advantage, lost business, and legal proceedings. And nearly half of these losses are caused by the company's own employees, not outside hackers. It is no wonder then that International Data Corporation (IDC) predicts that security software will become a \$7 billion market by 2002. According to IDC, security problems will increase as the value of the data on the Internet skyrockets. IDC also predicts the value of e-commerce will grow to \$1.3 trillion by 2003, up from \$50 million in 1999.

Increasing Security Needs

Enterprise network security is an art form that combines many elements, but the absolute foundation of a security solution is authentication. As the value of information has increased, IT managers have increasingly focused on authenticating users to their shared networks. In a 1998 study of the economics of security of Fortune 1000 companies, Forrester Research listed authentication as one of the four cornerstones of a good security system. The study concluded that passwords should be replaced with a single sign-on solution for access to applications and network resources. Yet the same study recognized that the technology at the time, smart cards with digital certificates, involved an elaborate and costly implementation. To support the technology, every single application had to be retrofitted to support digital certificate technology. Those modifications alone would cost a corporation of 20,000 employees \$4,000,000 in the first year. This doesn't include the ongoing support cost of smart cards with the required passwords which is astronomical.

Security Must Protect Privacy

Privacy is also a growing concern for enterprises, employees, and Internet users. They face a loss of privacy with the growing proliferation of electronic information available about them, their company, their accounts, and more. The U.are.U system is designed around the guiding principle of protecting personal privacy. The user's identity and privacy are always protected by U.are.U due to our intelligent sensor design.

Who Are You?

From a larger perspective, relying on passwords and smart cards still does not guarantee what the IT manager wants to ensure: that the person logging on (or using your password) is really you. A password security system assumes that by providing a password, you are who you say you are. It's about what you know. However, the best password protection system is at the mercy of Post-It notes

pasted in employee cubicles and passwords that are easy to guess (1234, qwerty). A smart card solution, while an improvement on the password model, still suffers from the fact that it doesn't really identify who you are. It's about what you have. In addition, smart card authentication does not provide you with the single sign-on for all enterprise applications without modification to the individual software itself. Each of these authentication systems requires a leap-of-faith.

Biometrics is the Answer

Biometrics is both the most convenient and the most secure identification device available. It is not based on something you remember like a PIN code, nor is it based on something you have in your possession like a smart card. Biometrics says who you ARE. Because biometric characteristics are unique to each individual, they cannot be lost or stolen like passwords. It is a unique, measurable characteristic or trait for automatically recognizing or verifying the identity of a human being. Biometrics is the best way to ensure that you are who you say you are. Fingerprints are the most popular biometric in use because they are very accurate, technically mature, economic to implement, and one of the least intrusive of the biometric methods available.

Biometrics is Changing the Face of IT Security

Through biometrics, the IT manager achieves what they are trying to obtain: definitive proof that you are you. And this is the only security method that can be designed for convenience to the user. Gartner Group recognized the importance of biometrics by forecasting it to be a key component of future security systems. In a study of the 1999 biometrics market, IDC believes the biometrics market associated with IT authentication will grow to \$1.8 billion by 2004, with fingerprint technology prevailing with a 55 percent market share. A March 1999 Lehman Brothers report predicted, "Although the biometric device industry may be less than \$100 million today, we estimate that this market will grow 30 – 35 percent annually to reach \$400 million in five years." Similarly, Salomon Smith Barney predicted in May 1999 that "spending in the security and personal identification market will grow at a compounded annual growth rate of more than 60 percent to approximately \$1 billion by 2001."

Major Corporations are Embracing Biometrics

The corporate market is ready for enterprise authentication systems based on fingerprint recognition. Technology for enterprise authentication systems based on fingerprint recognition is here today. Microsoft acknowledged fingerprint recognition during their Windows 2000 launch and will be incorporating compatibility to biometrics in their next OS. IBM and other computer manufacturers are offering biometric security through partnerships with companies such as DigitalPersona.

According to Roberto Torres, Frost & Sullivan Automatic Identification Industry Research Analyst, "The underlying driver in the commercial arena is the business community's search for tools which can prevent fraud. Problems stemming from false identification of individuals have seriously hurt the financial industry, government agencies, and business establishments for decades."

Other driving factors are the expense and poor security of passwords. On average, 40% of help desk calls are for forgotten passwords. Password protected systems are only as good as their weakest password. Users cannot remember good secret/cryptic passwords. Fingerprint authentication eliminates forgotten passwords and the related administration costs.

Biometrics Increase Network Security, Prevent Internal Breaches

A user's fingerprint is much more complex than a password, it cannot be copied or written down, and it's impossible to forget. Most corporate network security breaches are inside the firewall—many are from disgruntled employees who have stolen passwords. The 2000 CSI/FBI Computer Crime Survey found that 71% of unauthorized break-ins were by employees inside the company. Fingerprints cannot be copied or stolen. Maintaining the security of a password-based authentication system is so burdensome that users constantly look for ways to simplify the system. The convenience of a fingerprint recognition system ensures that users maintain security without “shortcuts”, such as very simple passwords or writing their passwords on Post-It Notes. Fingerprint recognition systems are the best authentication solution to increase security and convenience and lower administration costs compared to traditional password-based methods.

Targeted Markets for Biometrics

As with any new technology, the adoption of the technology generally begins with the vertical industries and customers who have the greatest need for the solution. DigitalPersona has identified three initial target markets where the use of biometrics will be the most prevalent in the next year.

- ***Healthcare***

In the first quarter of 2000, the Department of Health and Human Services, finalized the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This legislation mandates that all healthcare providers, and any of the organizations with which they conduct business, deploy specific safeguards for the integrity, confidentiality, and availability of its electronic data. Over the next 24-36 months, the organizations affected by this legislation must assess, implement, and maintain appropriate security measures to meet the requirements of HIPAA. Failure to comply can result in monetary fines and possible jail time.

HIPAA has created an incredible opportunity for consultants, system integrators, VARs and resellers to provide healthcare organizations with the information technology systems and solutions necessary to comply with the HIPAA regulations. DigitalPersona's products address many of the security requirements specified by HIPAA, as well as eliminate the administrative cost and burden of maintaining password security.

Healthcare organizations generally do not have the in-house expertise to assess, design, and implement the necessary information technology solutions to meet the requirements of HIPAA. This provides an incredible

opportunity for VARs to fill this gap for healthcare organizations and become their HIPPA consultants.

- ***Finance***

The financial sector is another vertical market where we see the most dramatic increase in use of biometric systems over the next year. The Gramm-Leach-Bliley Act (GBLA) is legislation similar to the HIPPA regulation but specific to the financial services industry. GBLA mandates that firms must ensure the security and confidentiality of customer records and information to protect against any anticipated threats or hazards to the security or integrity of such records. Financial organizations must comply with the regulations by July of 2001.

Like HIPAA, GBLA provides an incredible opportunity for solution providers to provide financial organizations with the systems and solutions they will need in order to comply with these new regulations.

- ***Government***

A recent investigation conducted by the General Accounting Office (GAO), which is the investigative arm of Congress, found that 50% of the 54 federal agencies investigated failed to meet basic security standards. Investigations like this and high profile security breaches (like the missing hard drives at Los Alamos National Laboratory, and the disruption of NASA communications by a teenage hacker) have brought the issue of IT security to the top of the government agenda. During the Clinton administration it was proposed that the national budget for information security be increased by 15% to \$2.3 billion annually.

Pressure is being put on all agencies (federal, state, and municipal) to reevaluate their security practices and institute tougher security measures to protect their computer systems.

Laptop Computers

In 1999 alone, more than 300,000 laptops were stolen at a cost of more than \$800 million, and that does not include the value of the information contained on those laptops. Driven by the need to access critical information all of the time, most mobile computer users maintain a large amount of critical data on their laptops. The vast majority of these laptops lack even basic security, putting valuable corporate information at high risk. Our systems provide a cost effective method of securing sensitive information on mobile computers so that, in the event a laptop is stolen, the information on the laptop remains secure.