COMPUBLOX incorporated

the Biometric Pragmatist

Software Engineering Solutions for the Real World

Vol. 1, #1
March, 2002

Welcome…

…to our inaugural issue. This bulletin will be published on a quarterly basis to bring you information, news, and commentary on developments in the world of biometrics, security, and information technology.

In this issue:

Identity Theft: Crime of the Millennium

- Financial Institutions have made great strides in countering credit card fraud, but staying ahead of the crooks on the technology curve remains a challenge.

Biometric Consortium Conference 2002

- The Biometric Consortium conference, originally scheduled for September 12-14, 2001, was held in Washington D.C. in February.

The CompuBlox Value Proposition

- There are many directions you can turn for help with your software engineering needs. Why CompuBlox?

Regular Features:

In the News –news items from around the Web

Coming Events – conferences of interest

Privacy Corner – toward a working definition

Words – concepts you need to know

Quotable – what people are saying

Contents

The *Biometric Pragmatist* is available online in PDF format at:
www.compublox.com

Identity Theft: Crime of the Millennium

Identity theft is the fastest growing crime in North America. The main objects of identity theft, in order of frequency, are to:

- Obtain or take over credit cards
- Obtain telecommunications services
- Obtain or take over bank accounts

As the convenience of financial services has grown, so has the risk of having one's identity compromised by a growing number of tech-savvy thieves.

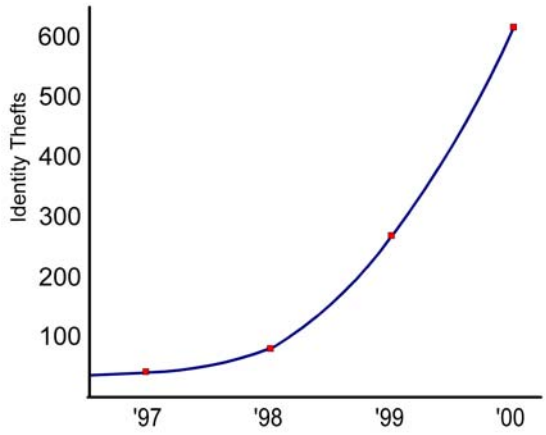
In the late '90s, the majority of credit card fraud was through counterfeit cards. The major financial institutions met this challenge head on, and losses due to counterfeit cards have actually been dropping for the past several years. However, during the same time frame, identity theft rose exponentially, and continues to do so at an alarming rate.

What makes identity-theft fraud different from counterfeit-card fraud is that it is a dual-victim crime. While the majority of the financial burden is shouldered by the financial institutions, those who have had their identities stolen also spend substantial time and resources repairing their reputations. Identity theft is doubly vexing for financial institutions: it not only costs them a substantial (and rapidly growing) amount of money, but also poses a potential public-relations problem as consumer concern grows.

There may always be a certain amount of tradeoff between convenience for customers and the risk of identity theft, but what if you could implement a technology that provides customers with additional convenience while protecting them, and the financial institution, from identity-theft fraud? This dual benefit is precisely what biometric authentication offers.

see Identity Theft, p. 2

The Rise of Identity Theft



Source: *U.S. Treasury Department, Financial Crimes Enforcement Network (FinCen)*

Identity Theft (continued from p. 1)

The Statistics

Recently, a survey conducted by **Gartner Inc.** revealed that, over the past 12 months, 1 in 20 consumers has been a victim of credit card fraud, and that 1 in 50 has been a victim of identity theft. The survey also indicated that public concern on this issue is increasing.

Financial Institutions have made great strides in countering credit card fraud. In 2000, the **Canadian Banking Association** (CBA) reported:

> "Although, associated credit card fraud had been steadily increasing since 1990, we are pleased to report that the last two quarters of credit card statistics indicate a significant decrease in the total dollar losses associated with credit card fraud. The dollar loss figures have gone down from nearly $227 million reported at the end of 1999 to approximately $203 million for the 12 month period ending June 30, 2000."

At that time, in Canada, the majority of credit card fraud – representing 53% of the dollar loss - was due to counterfeit cards. Lost or stolen cards accounted for 22%, no-card fraud for about 10%, and non-receipt fraud for about 8%. Identity theft (primarily in the form of "fraudulent applications") was a minor consideration, but the CBA noted that the trend was upward:

> "These frauds involve the criminal impersonation of creditworthy persons, in order to acquire credit cards. Although losses attributable to this category account for only 5 per cent of all credit card losses they do represent a fast growing trend."

Such "criminal impersonation," or identity theft, is indeed a criminal growth industry. In the U.S., the Federal Trade Commission has declared identity theft to be the fastest growing crime today.

ePayNews, which focuses on electronic and mobile payment technologies, reported that the most common motive for identity theft is to obtain or take over a credit card account (53%). Second: to acquire telecommunications services (27%). Third: to obtain or take over a bank account (17%).

In June, 2001, the **Associated Press** reported that, according to the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCen), "the number of identity thefts reported by U.S. banks and other financial institutions more than doubled in 2000 from the previous year."

The trend is clear, and there are many indications that the problem is much larger. The same article reported that, by mid-2001, a U.S. government identity-theft hotline was receiving, on average, 1,700 calls per week.

The issue has gained sufficient notoriety to prompt the International Association of Chiefs of Police (**IACP**) issued a resolution that "calls upon all law enforcement agencies in the United States to take more positive actions in recording all incidents of identity theft and referring the victims to the Federal Trade Commission's hotline."

In 1999, **CNN** reported:

> "Identity theft is to the Information Age what rum-running and gangland murders were to the Prohibition era… there is little doubt that this type of fraud…already is the country's fastest-growing financial crime."

If your identity is stolen, you can expect the crime to cost you more than sleep. The **Identity Theft Resource Center** reports that, "on average, victims spend 175 hours and $808 in out-of-pocket expenses to clear their names."

The **Privacy Rights Clearinghouse** has been maintaining statistics on its hotline inquiries since 1992. Identity theft made its appearance in Year Three (1994/95) and hit the charts at number 2 with 18% of the calls. In Year Four (1995/96), identity theft took over top billing and accounted for 25% of the calls to the hotline. By Year Six (1997/98, and the last for which statistics have been published to date), this burgeoning crime was responsible for 30% of all inquiries.

Time Magazine reported in January, 2002:

> "Last year alone, the Federal Trade Commission logged more than 85,000 complaints from people whose identities had been pirated. That may only be the tip of the iceberg; some consumer advocates suggest as many as 750,000 identities are stolen each year."

How Identity Thieves Attack

An identity thief may steal a wallet or mail, or rummage through garbage for documents such as pre-approved credit card offers, or pose as a landlord and obtain credit reports, or somehow gain access to employment records, or tap into the victim's Internet activities.

As careful as consumers may be, they remain vulnerable to such attacks, and it is only because the number of targets is so great that the majority of consumers have not yet been affected. However, as public awareness and concern grow, consumers will be less inclined to depend on the benign neglect of identity thieves, and they will want financial institutions and technology providers to take action to safeguard their interests.

Biometric Authentication to the Rescue

Biometric authentication uses something the consumer is to verify the identity they claim. In a standard scenario, the consumer presents a token, such as a debit or credit card, which makes a claim as to the identity of the person carrying it. The biometric system captures a biometric sample (e.g., finger, iris, face) and compares the captured sample against the biometric template on record for the consumer. If it matches the two, the consumer's identity is verified, and the consumer is authorized to carry out the transaction.

The biometric template, which can be stored in central or distributed database, or on a smart card, replaces PINs, passwords, and signatures. It has an advantage over all of these: it cannot be stolen, guessed, or imitated. Because of this feature, biometric authentication provides the ultimate in accountability.

For more information, visit www.compublox.com.

Biometric Consortium Conference 2002: Gov't Support, Commercial Success

The Biometric Consortium Conference, originally scheduled for September 12-14, 2001, was held in Arlington VA February 13-15. Not surprisingly, interest in the conference was much stronger than that expressed before September 11, 2001. In fact, the conference sold out both for attendee and exhibitor space. The theme of this year's conference was homeland defense.

The Biometric Consortium is jointly sponsored by the Information Technology Laboratory of the U.S. National Institute of Standards and Technology (NIST/ITL) and the U.S. National Security Agency. Its purpose is to serve as "a focal point for research, development, testing, evaluation, and application of biometric-based personal identification/verification systems."

Homeland Defense

The message from these U.S. government agencies was that the current U.S. administration will continue and expand its support for the biometrics industry to accelerate the development of advanced technologies for homeland defense.

While the primary focus of the conference was the use of biometrics in homeland defense, there were also some outstanding success stories from the private sector.

Case Studies Show Commercial Viability

Two widely different case studies showed that biometric technology is indeed ready to secure facilities, support business processes, and provide added convenience to users.

San Francisco International Airport has been using biometrics to control access to restricted areas for a full decade. They use a hand geometry system developed by Recognition Systems to ensure that only authorized personnel can enter sensitive areas of the airport.

Disney World in Orlando uses a similar system to admit season pass holders.

These two success stories point not only to the general viability of biometrics, but also to the wide variety of applications for which biometrics are suitable.

The focus of each of these systems is completely different from the other. Keeping intruders out is a matter of life and death at SFIA, so a near-zero False Acceptance Rate (FAR) is critical. At Disney World, a false acceptance costs the company the price of a day pass. It is far more important for them to keep the admission lines moving and the customers happy, so False Rejection Rate (FRR) is their key measure.

In the News

Hong Kong Plans Digital ID

N.Y. Times – The border between Hong Kong and mainland China is frequently choked with travelers. To remedy this situation, Hong Kong will introduce a smart-card ID solution.

Each ID card will contain a biometric template of the cardholder's thumbprint. When the user presents the ID at the border checkpoint, his or her thumbprint is scanned and compared to the template on the card. If there is a match, the user is allowed to pass. The process is nearly instantaneous, and no immigration officer needs to attend the screening.

BioAPI Standard May Spur Biometrics Acceptance

searchSecurity.com – The emergence of standards is always a sure sign that a new technology is ready to make the leap into the technology mainstream. The BioAPI standard, which governs the interaction of biometric software and biometric hardware devices, is just such a standard.

BioAPI has the backing of major industry organizations, such as the International Biometric Industry Association (**IBIA**), and many U.S. government agencies.

Link Between Identity Fraud and National Security

U.S. Newswire – The revelation that U.S. federal authorities are seeking 20 employees of Boston's Logan International Airport on suspicion of identity fraud is raising questions concerning the effectiveness of the existing U.S. identity documentation system.

The two flights that crashed into the World Trade Center originated at Logan International.

Quotable

Just over 1 percent of all transactions conducted online are fraudulent… 7 percent of all [online] transactions are rejected because they are "suspicious."
- Gartner Research, MSNBC

Identity theft is to the Information Age what rum-running and gangland murders were to the Prohibition era.
- Heather Hayes, CNN

The gaping holes in our national system of documentation and lack of any meaningful security to safeguard those documents is a dangerous threat to America's national security.
- Dan Stern, executive director, FAIR

Words

There are a number of acronyms you will hear used to measure the effectiveness of biometric systems:

- **FAR – False Acceptance Rate:** the probability, expressed as a percentage, that a biometric system will incorrectly verify or identify an individual or will fail to reject an impostor.
- **FRR – False Rejection Rate:** the probability, expressed as a percentage, that a biometric system will fail to verify or identify a legitimate enrollee.
- **EER – Equal Error Rate:** the point, expressed as a percentage, at which FAR and FRR converge.
- **FTE – Failure to Enroll:** The rate at which a system fails to capture and process initial biometric samples needed to build a biometric template for an individual.

Coming Events

Successful Applications of Biometric Technologies

San Diego, March 25-26, 2002 – This two-day conference will look at early successes in the biometrics industry and present numerous case studies.

Keynote Address
The theme of the Keynote Address by Sheldon Watson (Sr. Systems Analyst with **Fidelity Investments**) will be *Bringing in Biometrics*. Mr. Watson is scheduled to discuss the process Fidelity went through to form a Biometrics Steering Committee and to deal with major challenges, and vendor relations.

Numerous other speakers will address the real-life issues and lessons learned from implementing biometric systems.

Scott Moody (President & CEO of **AuthenTec**) is scheduled to speak on the transition of the biometric marketplace from vertical competition to horizontal cooperation, and how this development compares with markets of the past.

Paul Reid (Director, Technical Services, **Ankari**) is scheduled to address issues related to network access security, including multi-factor authentication, and the evaluation of biometric technologies.

Spring 2002 Biometrics Summit

Washington D.C., April 3-4, 2002 – This two-day conference focuses on real-life case studies from those who have successfully implemented biometric systems, including new case studies from industries such as banking, retail, airlines & travel, law enforcement, and government.

Tim Robinson (President, **BioPay**) is scheduled to address the topic of securing financial transactions and reducing fraud in the retail, banking, and financial services industries.

Marcel Yon (CEO, **ZN Security** of Germany) is scheduled to discuss the deployment of face recognition technology in law enforcement and banking environments.

Privacy Corner

Privacy is an issue that will not go away. The drive to implement better security solutions will always have to withstand close scrutiny by privacy advocates. We all need to be familiar with this issue.

A working definition of privacy
Defining privacy and its relationship to security is not an easy task, mostly because these two needs are frequently in conflict. The right to privacy is defined by the Online Dictionary of Library and Information Science (**ODLIS**) as:

> "The right of an individual to keep information about his (or her) life from the knowledge and attention of others, including government organizations and commercial enterprises, and to remain free from outside intervention except under the provisions of law."

Your right to privacy is not absolute. It is both guaranteed and restricted by law. In other words you have the right to privacy until there is "probable cause" to suspect you of wrong-doing, in which case "authorities" are sanctioned by law to intrude upon your personal privacy in the greater interest of public security.

Privacy Law
Many countries have enshrined privacy rights in their constitution or legal statutes. In general the primary concerns of privacy law are:

- **Collection:** the types of information collected about you
- **Use, disclosure:** the organizations and people to whom your private information is disclosed, which parts are disclosed, when, and by what means
- **Security:** the type and reliability of measures used to guard the information against involuntary disclosure
- **Storage:** how long the information is kept, and where, when, and how the information is discarded after its useful life

For an expanded discussion of security, privacy, and identity, visit www.compublox.com.

The CompuBlox Value Proposition

CompuBlox is a total **B**iometric **S**ervice **P**rovider (**BSP**):

We use our deep knowledge of biometrics, leading-edge technologies, and solution development to design, build, implement, and support advanced solutions for real problems in the real world.

We are customer-focused - an end-to-end IT outsource partner for all your software, hardware, and network administration needs.

CompuBlox invests the time developing expertise in new technologies so that you can reap the benefits. We will help you re-engineer your business processes and overcome logistical challenges to take advantage of these new technologies. The result for your organization:

- **Simplified Processes**
- **Increased Profits**
- **Reduced Costs**

Contact Us

CompuBlox Inc.
205 Richmond Street West
Toronto, ON M5V 1V3

Telephone: 416-203-8780
Fax : 416-203-9750

Sales Manager: Ron Rusnak
ron@compublox.com

Visit our Web site at:
www.compublox.com

- **Reduce costs.**
- **Maximize your ROI.**
- **Increase your ability to compete.**