

IdQuanta

The Problem

Enterprises in diverse sectors (e.g. banking, technology, media, and entertainment and government) and consumers regularly come under cyber attack. Hacking accounted for the largest number of breaches in the first quarter 2011 with about 37% of breaches due to malicious attacks on computer systems [*Identity Theft Resource Center® Report, 2011*].

Online fraud and related crimes such as identity theft are on the rise. Recent high profile attacks have affected millions of accounts, credit cards and even customers of the very security systems intended to prevent these exploits. The impacts on enterprises are usually very expensive in terms of loss of reputation and cost. Cost can reach in the billions of dollars taking into account both the cost of fixing and securing the systems, lost business and protection against future attacks.

Over 8 million adults in the North America were identity fraud victims in 2010. The average consumer out-of-pocket costs (e.g. expenses for paying off fraudulent debt and legal costs) due to identity fraud increased to \$631 per incident, up 63 percent from \$387 in 2009. [*Javelin Research, 2011 Identity Fraud Survey Report*]

As a result enterprises are surrounding their internal networks with fortress-like security making hitherto easy pickings for cyber criminals much more difficult to obtain. But these criminals are turning their attention to the unprotected zones of users' computing devices, using new web threats enabled by Web 2.0 Internet technologies to deploy malware which can attack enterprise networks.

The Situation

The current solutions such as strong authentication, strong passwords and malware monitoring and surveillance are not effective as they do not address the source of the problem: the untrusted browser where the user unknowingly propagates the malware. Two-factor authentication, based on "something you know" (e.g. PIN, username and password) and something you have (e.g. a smart card, hard ware token or certificate) is recommended by the U.S. Federal Financial Institutions Examination Council (FFIEC) [*FFIEC Guidance on Authentication in an Internet Banking Environment, 2006*]. However the two-factor authentication solutions, used mainly for customers doing high-value transactions, are considered too expensive for widespread consumer use. They are inconvenient to end users

and place added burdens on IT resources as they require provisioning, ongoing administration, pin management, re-synchronization and replacing lost or broken tokens. As well, the required infrastructure and network authentication server increase cost of ownership. Two-factor authentication does not protect against malware.

Strong passwords are recommended but they are difficult to remember and are usually shared across multiple accounts. Over forty percent of users have over 20 web accounts requiring usernames and passwords [*Symantec, 2010*]; and security risks get higher as sixty per cent of users use the same password with many accounts [*Guardian, 2008*].

Another area of concern is the maintenance of user identities, including compliance costs (e.g. PCI DSS). The maintenance of user identities consumes, on average, 25 to 30 percent of an IT organization's time. About 15 to 40 percent of help desk calls deal with password reset with each call costing between \$20 and \$25. [*John Hunt, PWC, 2003*].

The risk of malware attacks is increasing at an alarming rate. In 2010, 95,000 malware pieces were analyzed every day. This represents one file every 0.9 seconds, 24 hours per day, each day of the year. Legitimate web sites are being compromised in record numbers of about 30,000 new malicious URLs created every day with 70% of the malicious URLs hacked were legitimate websites [*SophosLabs, 2011*].

The objective of malware today is to gain access to the user's private, financial, and confidential information. This is done by capturing bank login credentials, credit card details and other sensitive financial and personal details. The web is used to transmit emails bearing malicious links and attachments, email scams, exploits targeting browsers and other software, drive-by downloads, questionable storefront operations and implantation of malicious advertisements onto websites. Spammers are also using more focused email scams, known as "spearphishing" to lure specific targets in businesses and institutions for disclosing personal data, identity theft and corporate espionage.

The feelings of trust and community promoted by social networking websites have made it easier for criminals to transmit malware and turn members into accomplices unknowingly in attacks against members of the same community. In addition the bad guys are focusing more on "social engineering" tricks, such as opening an email attachment, clicking a button, following a link, or filling in a form with sensitive personal information, that persuade users to undermine their own online security.

InBay Technologies Inc. (InBayTech) Solution

InBayTech offers an innovative approach to address the online privacy problem based on uncertainty principles that disguise the user's real credentials and sensitive information. The InBay Technology eServices Platform assumes that the browser can never be trusted. Bank login credentials, credit card details and other sensitive financial and personal details are never exposed to the browser. In addition, the solution provides for user end two-factor authentication using a device that a user already owns as the "something you have" factor and a secret PIN as the "something you know" factor. This authentication must be done before proceeding to login with an alias user identity and alias password to access all web accounts. Users possess and control their own credentials.

The InBayTech flagship product, **IdQuanta**, converts a personal device such as a PC or a smart phone into a Trusted Personal Device (TPD) that is used in conjunction with a secret PIN for two-factor authentication without the need for network based authentication servers. A Trust Relationship Profile (TRP) server is used to invite clients and to provide administrative functions such as user self-registration, management and methods to positively identify access to secured eServices.

IdQuanta hides user's real credentials from the most pervasive malware impacting home users computing devices leading to the most frequent theft of credentials. It is easy to use, offers very strong authentication, protects against malware (e.g. man-in-the-browser, phishing and spear-phishing) hides credentials from would be cyber spies and on top of that eliminates the day to day frustration of user identities and passwords. For the enterprise it provides simple administration, reduces the burdens associated with maintenance of user identities and password reset and works with existing infrastructures.

The user identity and password used to access your account are of no use at all to an identity thief, being an alias for the true credentials that are never ever made visible to the browser or fillable forms such that they can be entrapped by key stroke loggers or other common browser attacks. This makes it easy for users to comply with the need for more stringent user admission control whilst at the same time reducing the cost of password resets, enabling the green objectives of postage and paperwork to be attained and enhancing trust in on-line transactions.

The IdQuanta benefits:

1. One UserId and Password for all web accounts: reduced password reset costs
2. User end two- factor authentication: reduced authentication server and hardware costs
3. Protection against malware: reduced ID theft/ID fraud costs
4. Simple administration: reduced admin costs

InBayTech Hosting Services (optional)

The ultra secure Data Centre for InBayTech is located in Ottawa, Canada with connections to Toronto, London and Vancouver for Internet connectivity 100% of the time. Our Class "A" Canadian Data Centre Facilities features include:

- 24 x 7 monitoring and technical support
- Sophisticated Biometric access control systems and video camera surveillance
- Gas fire suppression system and pre-action sprinkler systems
- Advanced climate control systems with redundant, computer-grade air conditioning and humidity control systems
- Massive power distribution systems with full redundant battery, UPS backup and diesel generator protection
- Redundant fiber-based multi-homed internet backbone with redundant multi-gigabit Internet connections to multiple Tier 1 Internet providers using BGP-4 routing protocol
- Aggregate backbone bandwidth of over 3800Mbps (3.8 Gbps)
- Full PCI Compliance, CICA 5970 Type B, and SAS70 Type II Certifications

For further information please contact:

Codework, Inc.

1-613-368-4300

info@codework-systems.com

www.codework-systems.com