Bloombase
Least Invasive Security

Achieving Data Confidentiality with Bloombase Least Invasive Security Solution

WHITE PAPER

Gramm-Leach-Bliley Act

The United States of America Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act (GLBA), includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule and pretexting provisions.

The GLB Act gives authority to eight federal agencies and the states to administer and enforce the Financial Privacy Rule and the Safeguards Rule. These two regulations apply to "financial institutions," which include not only banks, securities firms, and insurance companies, but also companies providing many other types of financial products and services to consumers. Among these services are lending, brokering or servicing any type of consumer loan, transferring or safeguarding money, preparing individual tax returns, providing financial advice or credit counseling, providing residential real estate settlement services, collecting consumer debts and an array of other activities. Such non-traditional "financial institutions" are regulated by FTC.

The Financial Privacy Rule governs the collection and disclosure of customers' personal financial information by financial institutions. It also applies to companies, whether or not they are financial institutions, who receive such information.

The Safeguards Rule requires all financial institutions to implement and maintain safeguards to protect customer information. The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions - such as credit reporting agencies - that receive customer information from other financial institutions.

Personal Data Privacy Ordinance

The Office of the Privacy Commissioner for Personal Data has brought the Personal Data Privacy Ordinance in 1996.

The purpose of the Ordinance is to protect the privacy interests of living individuals in relation to personal data. It also contributes to Hong Kong's continued economic well being by safeguarding the free flow of personal data to Hong Kong from restrictions by countries that already have data protection laws.

The Ordinance suggested the following data protection principles

Purpose and manner of collection This provides for the lawful and fair collection of personal data and sets out the information a data user must give to a data subject when collecting personal data from that subject.

Accuracy and duration of retention This provides that personal data should be accurate, up-to-date and kept no longer than necessary.

Use of personal data This provides that unless the data subject gives consent otherwise personal data should be used for the purposes for which they were collected or a directly related purpose.

Security of personal data This requires appropriate security measures to be applied to personal data (including data in a form in which access to or processing of the data is not practicable).

Information to be generally available This provides for openness by data users about the kinds of personal data they hold and the main purposes for which personal data are used.

Access to personal data This provides for data subjects to have rights of access to and correction of their personal data.

Non-compliance with an enforcement notice served by the Privacy Commissioner carries a penalty of a fine at Level 5 (at present HKD25,001 to HKD50,000) and imprisonment for 2 years.

The Security Challenge

To protect data from unwanted disclosure, one might suggest access control and block unauthorized users from reading the sensitive data. However, to administrators and operators who have superuser privileges, they have full access to any system resources even if the resources are not owned by them. Access control to these privileged users means nothing.

Existing security measures cannot protect data from alteration. Statistics showed private enterprises raise their investment by 30% yearly on data security. However, the number of data security incidents grows at the same rate if not exceeding [CERT, IDC, RBCCM 2002].

PricewaterhouseCoopers reported that 50-80% of data attacks are from company insiders. CSI/FBI investigation in year 2002 showed insider attack has caused the industry monetary loss of more than USD 50 million.

Command-based encryption utilities only work with offline archives instead of processing real-time data on-the-fly. They require much operation by administrators and at the end, it is still unsafe. Volume protection is considered transparent, however, it is limited to direct attached storage and is not scalable for enterprise use.

Bloombase Solution

Bloombase created Spitfire security platform to address compliance requirements suggested by GLBA and Personal Privacy Ordinance to safeguard corporations and agencies from unwanted private data disclosure. Spitfire security appliances protect encryption and digital signing keys inside hardware security module (HSM) from disclosure and duplication. Spitfire appliances encrypt data with NIST certified AES, 3DES and DES cryptographic algorithms and create digital signatures to assure data integrity by international standards including Public Key Infrastructure (PKI), X.509 digital certificates and W3C XML digital signature.

Data Confidentiality

Spitfire StoreSafe protects storage data by strong encryption. Encrypted data appears as garbage and meaningless information to unauthorized users. Intruders will have to pay tremendous efforts to undo the encryption process which is considered technically impossible.

Application Transparency

Spitfire appliances are network based hardware which can easily fit in any enterprise systems and do not invade existing computing infrastructure. Spitfire operates as a network blackbox transferring data between components of a system. Spitfire detects network packets for plain data and encrypt them before sending to data's original destination. As encrypted data pass through Spitfire, Spitfire Cryptographic Engine (SCE) immediately decrypts data and delivers plain data to the next hub. Spitfire gaurantees zero-downtime deployment and works transparently under the covers without applications or users' intervention.

No Single Point of Failure

Mission critical systems require extra high level of service availability. To cope with the ever increasing storage and challenging service requirement of customers, Spitfire appliances have prepared for mission critical use as well. Spitfire appliances are high availability (HA) ready. Corporations can multiplex Spitfire boxes to run in a cluster. Failure of any single Spitfire appliance will not affect service of the entire cluster. Spitfire appliances are built with concern on failover and non-stop - redundant cooling fans, redundant and hot-swappable power-suppy and multiple network and storage interfaces.

Effective Compliance

To address GLBA, Personal Data Privacy Ordinance and other numerous data privacy compliance requirements, enterprises should act immediately to secure their customer personal data and various information archives. Bloombase Spitfire Security Platform provides a cost-effective, scalable and secure solution to protect these information from unattended disclosure.

Bloombase
Least Invasive Security

Bloombase Technologies - Least Invasive Security **email** info@bloombase.com **web** bloombase.com