A Government Security Control Organization

Bloombase® Spitfire StoreSafe™ Storage Security Server

Bloombase® Spitfire StoreSafe™ Lite Storage Security API

Bloombase® Spitfire KeyCastle™ Key Management Server

CUSTOMER SPOTLIGHT

Sensitive departmental information interchange and storage data of government security organization are encrypted using Bloombase® Spitfire StoreSafe™ storage encryption solution achieving end-to-end data in-flight and data at-rest security

AT A GLANCE

ABOUT THE CUSTOMER

- Government security control organization
- Employees: More than 10,000

SUMMARY

To protect privacy of sensitive data interchange information submitted from various trusted data providers and secure contents in storage sub-systems and backup tapes from secret data exposure to unauthorized parties caused by physical or electronic theft

KEY CHALLENGES

- Support heterogeneous host operating systems including Microsoft Windows, IBM AIX, etc
- No change to end user, administrator and operator workflow
- No coding or second development required
- Sensitive information are physically stored encrypted at all times and no physical plain originals and copies are allowed
- Interoperable with IBM WebSphere application server and IBM DB2 Universal Database (UDB) server
- Encrypted archives on backup tapes
- High performance encryption and decryption

PROJECT OBJECTIVES

- Protects in-flight data submitted from third parties by HTTP form posts
- Protects filesystem objects, relational databases and backup media
- Encrypts dynamic database data stored in storage area network (SAN)

SOLUTIONS AND SERVICES

- Spitfire KeyCastle™ key management server
- Spitfire StoreSafe™ Lite storage security API

Overview

A municipal security control organization dynamically allocates their task forces and automatically reacts to potential incidents based on a self-developed intelligence information system. Hundreds or even thousands of information feeds including weather forecast and reports, local news, foreign news, traffic reports, border and coastal data, calendar events, etc are collected from hundreds of data sources every minute. These real time information, structured and/or unstructured, in form of flat files, are parsed, extracted and aggregated before they are loaded into a central data warehouse.

Based on various pre-defined data mining rules, real time security data are analyzed to generate reports, milestones and alerts to proactively monitor potential hazards and risks. With response to these possible outcomes closely monitored and tracked by the 24x7 operation unit, the bureau dynamically reacts and allocates resources and task forces to combat such potential incidents, better control the worsening situation, if any, or even suppress outbreak of the incidents.

Among these incoming information feeds, data warehouse and reports repository are extremely sensitive and are under airtight political and security privacy regulatory. In application's perspec-

BLOOMBASE®

tive, security measures limit access to the system to authorized personnel only, protecting from unauthorized access. Network communications of these controlled information are secured by secure socket layer (SSL) powered by AES 256 -bit strong encryption with industry proven secure key exchange, thus, sensitive data exposure due to eavesdropping is eliminated. Physical access to the computing hardware, whether at primary data center or disaster recovery (DR) site, are securely isolated and under strict physical access control, blocking possible physical tampering and data/hardware theft.

With all these security measures in place which are generally considered border or perimeter protection, the data system is vulnerable to core attacks, unknown attacks and outbound threats such as operator/insider attacks, spyware attacks and viral outbreaks, etc.

The Mission Critical Encryption

To cope with these challenges and meet national data privacy requirements, end customer needs to implement effective data encryption to secure information exchange with various data providers, protect data repository storage, data warehouse and backup archives at both primary and disaster recovery systems.

Implementing encryption on this mission critical system is full of constraints, baseline requirements being data in-flight and at-rest are securely encrypted by AES 256-bit cryptographic cipher, high availability ready and fault-tolerant, tamper proof and tamper resistant key protection and management. On the other hand, the encryption solution has to fit perfectly into end customer's three-tier architecture at zero change, no application change, no database object change and last but not least, to be fully transparent to applications, administrators, operators and users.

WHY BLOOMBASE SOLUTIONS

- All in one solution to achieve data in-flight and at-rest security
- Platform independence
- NIST FIPS-140-2 level-3 tamper proof and tamper resistant key protection
- Full lifecycle key management
- Tamper proof and tamper resistant key protection

IMPLEMENTATION HIGHLIGHTS

First customer to practice both data-in-flight and data-at-rest protection for end-to-end security of highly available sensitive business data interchange and persistence

KEY BENEFITS

- No client user training required for third party data providers
- Application transparency
- High encryption performance
- Highly available and fault-tolerant

HARDWARE

- IBM x-Series servers
- IBM p-Series servers
- IBM TotalStorage DS4100 SAN storage
- IBM tape library
- Sun Microsystems Sun Fire X2100 servers

OPERATING SYSTEM

- Microsoft Windows Server 2003
- IBM AIX 5.3
- Novell SUSE Linux Enterprise 9

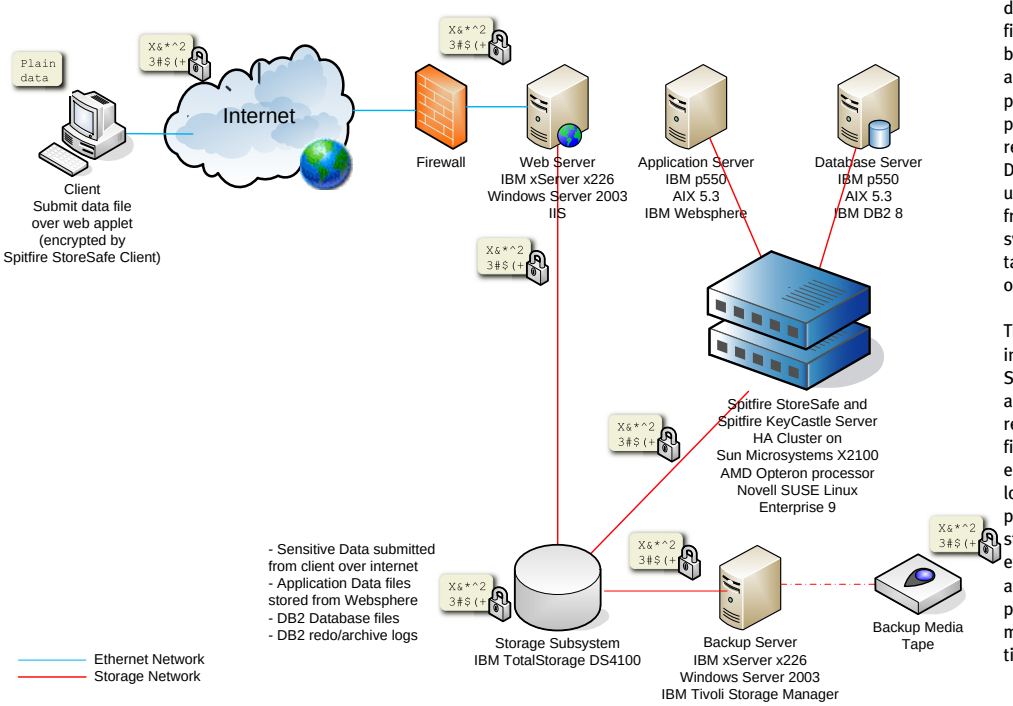
SOFTWARE

- IBM WebSphere application server
- IBM DB2 Universal Database
- IBM Lotus Domino messaging server
- IBM Tivoli Storage Manager (TSM)

After a three-months evaluation process, end customer selected Bloombase® Spitfire™ enterprise security solution over rivals taking kernel-based, database column-based, and hardware appliance-based encryption approaches.

Deployment of Bloombase® Spitfire™ KeyCastle key management servers and Spitfire™ StoreSafe storage security servers completed within 3 days whereas initial data migration of incoming information feed repository, IBM DB2 UDB data files and report storage area took merely another surprisingly 2 days.

An active self executing component is deployed at every data providers' internal network to poll for latest news and information. These sensitive information feeds are encrypted automatically as they are uploaded to the intelligence system by Spitfire™ StoreSafe Lite storage security API with channel further protected by SSL. The ciphered information feed is temporarily stored at a staging area physically located at IBM TotalStorage DS4100 SAN in form of flat file. A job is scheduled to run every other minute at an IBM WebSphere application server to scan for latest information feeds, access of ciphered incoming files via Spitfire™ StoreSafe security server provides a virtual plain view of sensitive contents to be extracted and bulk imported into a data warehouse powered by IBM DB2 UDB. Read/write access of DB2 UDB is made via a highly available Spitfire™ StoreSafe server cluster. Thus, during bulk import of information, sensitive information are first encrypted on-the-fly by Spitfire™ StoreSafe before they are persisted onto SAN, vice versa, on execution of data -mining procedures, ciphered data warehouse data are deciphered at real time on demand prior to actual query reads. Analysis results in form of data records and large binary objects are stored in another DB2 UDB instance which is also protected by Spitfire™ StoreSafe storage encryption servers. Again, only when these sensitive milestones are accessed and presented to authorized personnel will the private information be deciphered at wire-speed by Spitfire™ StoreSafe. Ciphered block based SAN storage updates are automatically synchronized from primary site to DR site via a virtual private lease line to be further reconstructed and applied to the DR SAN sub-system. Further, backup archives are created directly from ciphered physical storage system and stored on magnetic tape cartridges for backup and sent offsite for safe storage.



The entire life-cycle of sensitive incident information is secured by Spitfire™ StoreSafe at complete application transparency. Highly regulated digital data in form of files, disk data blocks, database entries and tape are privately locked down onto generic enterprise storage infrastructure by strong encryption at all times, effectively forbidding possible core attacks that might lead to serious private data exposure at the minimal costs and risks of implementation.

4AA0-0696AAC 09/2006

BLOOMBASE®