

Make yourself comfortable.
Play it safe.



sales@comforte.com
www.comforte.com

data at rest encryption
on the NonStop platform

Thomas Burg
Chief Technological Officer
comForte Inc.

June 2006

This presentation was given at N2TUG in Dallas und SUNTUG in Tampa in early June 2006.

Company Profile

Our Mission: Assisting enterprises to deploy secure, manageable and cost-effective NonStop server access

➔ comForte GmbH / Germany

- ➔ Founded: Oct 1998
- ➔ CEO: Dr. Michael Rossbach
CTO: Michael Horst
- ➔ Offices:
 - ➔ Neuruppin (north of Berlin)
 - ➔ Wiesbaden (near Frankfurt)

➔ Employees: 20

➔ Revenue 2005: 2.5 Mio Euro

➔ comForte Inc. / USA

- ➔ Founded: June 2005
- ➔ President: Knut Rossbach
CTO: Thomas Burg
- ➔ Office: Old Tappan, New Jersey



communication is our Forte

Intro - questions

- What's data at rest anyway ?
- Have you thought about encrypting it back in 2002 ?
- Are you thinking about encrypting it today ?

from SearchStorage.com:

Data at rest is a term that is sometimes used to refer to all data in computer storage while excluding data that is traversing a network or temporarily residing in computer memory to be read or updated

for example:

\$DATA16.B24FILES.PTLF

a SQL table

a backup tape containing your database

an Excel Sheet on your Notebook

your contact list on your PDA

Part I: Encryption of backup tapes

- Why bother ? (It's „Tandem format“ after all)
 - Google for “Tandem Archive Unlabelled” and get: <http://www.e-mediaplus.com/emag/MMPC.htm>

MediaMerge for PC (MM/PC)

Part of our suite of MediaMerge software products, this Windows based software sits on 95, 98, 2000, NT, and brings a plethora of capability to the management and manipulation of data residing on tapes, CDâs or hard drives. Tape drives need to be connected via SCSI to the PC hosting MM/PC. MM/PC is an options based software and in standard format its capabilities are huge, but there are also some authorization-coded options for more specialized work or [advanced features](#).

MM/PC Applications

The applications for MM/PC are almost limitless. If it involves moved data between computers on magnetic tape, then MM/PC can probably help solve any incompatibility problems. Data interchange, media conversion, and restoring backups from any type of computer are all within a single software package.

Restore backups from any source

Tandem Archive	R	X		X	X	X	X	X		
Tandem Archive Unlabelled	R	X		X	X	X	X	X		

Part I of this presentation talks about encryption of backup tapes.

This sildes makes the point that backup tapes written on NonStop system can be read using vanilla PC hardware.

A history of data breaches

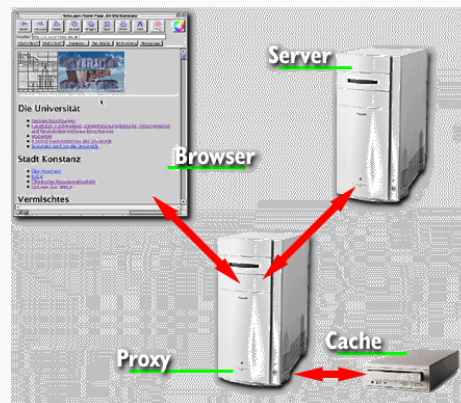
→ from <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

DATE MADE PUBLIC	NAME	TYPE OF BREACH	NUMBER
Feb. 15, 2005	ChoicePoint	Bogus accounts established by ID thieves	145,000
Feb. 25, 2005	Bank of America	Lost backup tape	1,200,000
March 12, 2005	NV Dept. of Motor Vehicle	Stolen computer	8,900
April 20, 2005	Ameritrade	Lost backup tape	200,000
June 16, 2005	CardSystems	Hacking	40,000,000
Feb. 9, 2006	Unknown retail merchants, apparently OfficeMax in N. Calif., Sam's Club .	Hacking. Debit card accounts exposed.	200,000

The URL above list major data breaches and lost backup tapes are prominently present on that site.

What is a "proxy" ?

- <http://www.cs.cornell.edu/wya/DigLib/MS1999/glossary.html>
 - A computer that acts as a bridge between two computer systems that use different standards, formats, or protocols.
- http://www.uni-konstanz.de/proxy_doc/Proxy.gif



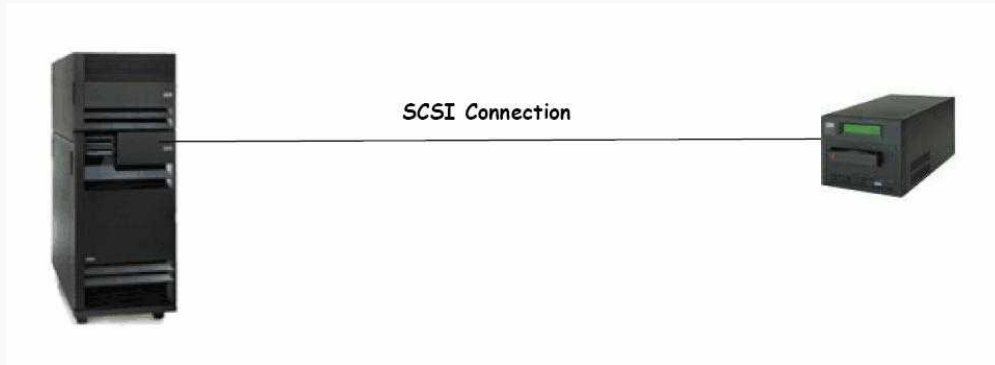
Introducing the proxy concept which is used in both solutions for backup tape encryption we are talking about later.

Question to audience

- Now as we know what a proxy is:
 - how can we use the proxy concept to encrypt backup tapes ?

Backup tape encryption: Paranoia2

→ Before adding encryption using Paranoia2



Backup tape encryption: P2 (contd.)

→ Adding encryption using the Paranoia2 product



The Paranoia2 (P2) product serves as a hardware-proxy in the physical backup setup.

Backup tape encryption: P2 (contd.)

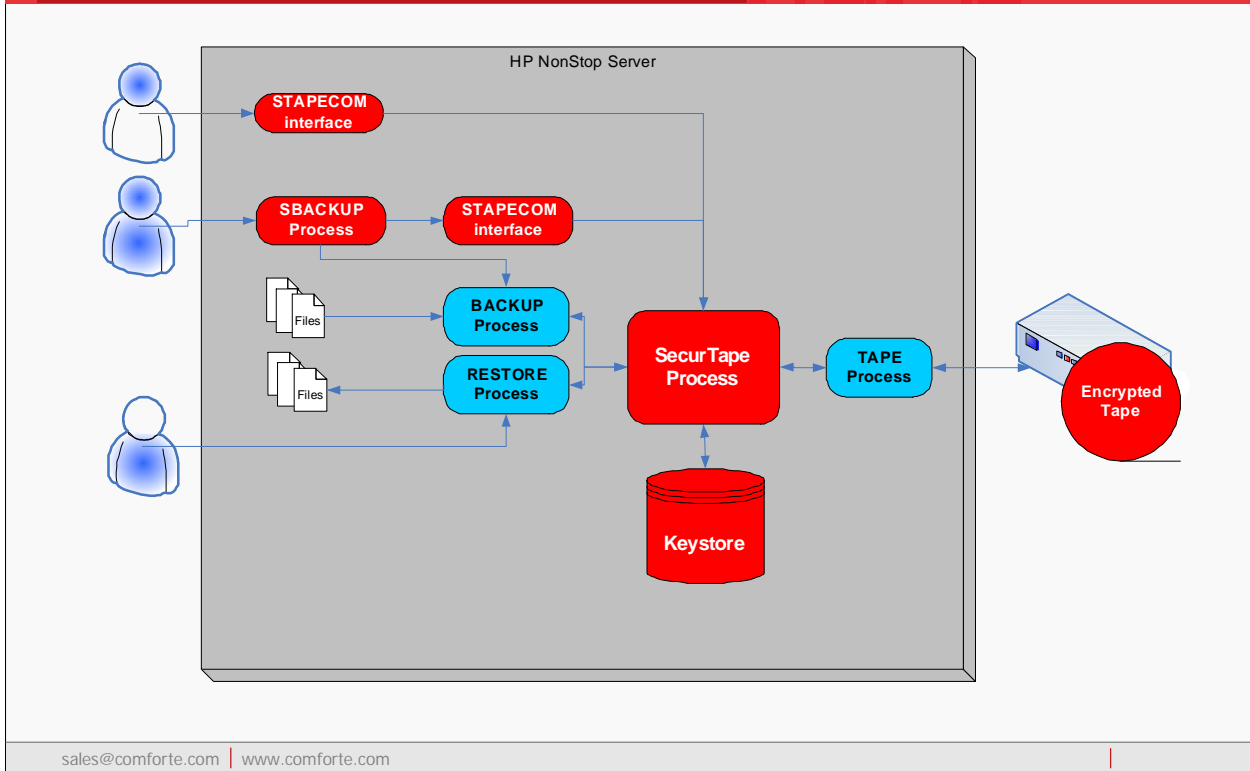
→ advantages:

- key resides in hardware
- no performance degradation
- transparent to existing environment

→ disadvantages

- you may need at least two boxes for fault tolerance (although you can duplicate the chip containing the key only)
- additional hardware to install and maintain
- not covered under HP hardware warranty

SecurTape - Architecture



This slide shows the concep of SecurTape: the SecurTape process will work as software proxy process between the \$TAPE process and the BACKUP and RESTORE process opening it.

SecurTape – Key Benefits

→ Features

- Strong ciphers, including
 - 168-bit 3DES-EDE (triple DES)
 - 256-bit AES-CBC (Advanced Encryption Standard)
 - 256-bit AES/CCM encryption, as proposed by the IEEE P1619.1/D5 Draft Standard Architecture for Encrypted Variable Block Storage Media
- Public/Private key cryptography, keys protected in key store
 - Easy-to-use command line interface for managing keys
 - Access to keys can be controlled on a per-user basis
 - Export keys for restoring tapes on other systems

→ Benefits

- Requires no new hardware purchase or installation.
- Installs easily, and is simple to maintain.
- Uses the existing, unaltered BACKUP and RESTORE objects. There are no additional libraries to bind.

→ Disadvantages

- It **will** be a CPU-hog for large backups (roughly 200 CPU ms/MB of data)

Backup tape encryption: comForte solution details

Product	Description	Comment
Paranoia2	Hardware-based solution	<ul style="list-style-type: none"> ➔ transparent to the existing environment ➔ no performance impact on backup and restore ➔ safely stores encryption keys in hardware.
SecurTape	Software-based solution	<ul style="list-style-type: none"> ➔ easy to install and maintain ➔ places a high burden on the CPU for huge data volumes ➔ Uses software key store ➔ available Q2 2006

Questions backup tape encryption ?

→ http://www.comforte.com/ecomaXL/index.php?site=COMFORTE_PCI_standard

Payment Card Industry Data Security Standard

Protect Cardholder Data

- 3.4 Render sensitive cardholder data unreadable anywhere it is stored (including data on portable media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:
- One-way hashes (hashed indexes), such as SHA-1
 - Truncation
 - Index tokens and PADs, with the PADs being securely stored
 - Strong cryptography, such as Triple-DES (Data Encryption Standard) 128-bit or AES 256-bit with associated key management processes and procedures

The **minimum** account information that needs to be rendered unreadable is the payment card account number.

We now move to Part II in this presentation, looking at database encryption on the NonStop format.

Among institutions processing credit card data, database encryption is primarily driven by the Payment card Industry Standard. The Payment card Industry Standard (PCI) is a set of security standards that Visa and Mastercard sets for merchants and service providers who are involved in processing credit card transactions. Entities that do not comply can be either fined or being restricted for future business. The PCI standard makes various specific statements on how data needs to be protected, we will focus on encryption on this page:

Sections 3.4 through 3.6 talks about proper usage of encryption methods to protect sensitive cardholder data such as the credit card number while being stored in a database or on a backup tape.

Section 8.4 talks about protection of passwords both in transmission and storage.

The challenge (contd.)

- 3.5 Protect encryption keys against both disclosure and misuse.
 - 3.5.1 Restrict access to keys to the fewest number of custodians necessary.
 - 3.5.2 Store keys securely in the fewest possible locations and forms.
- 3.6 Fully document and implement all key management processes and procedures, including:
 - 3.6.1 Generation of strong keys.
 - 3.6.2 Secure key distribution.
 - 3.6.3 Secure key storage.
 - 3.6.4 Periodic key changes.
 - 3.6.5 Destruction of old keys.
 - 3.6.6 Split knowledge and dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key).
 - 3.6.7 Prevention of unauthorized substitution of keys.
 - 3.6.8 Replacement of known or suspected compromised keys.
 - 3.6.9 Revocation of old or invalid keys (mainly for RSA keys).
 - 3.6.10 Requirement for key custodians to sign a form specifying that they understand and accept their key-custodian responsibilities.

Database encryption: The armwrestling

- It's VISA vs. "you"
- The PCI standard **does** have valid points

Encryption databases - approaches

- ➔ Approaches on Windows/Unix/other platforms
 - ➔ transparent within database
 - ➔ at file/disk level
 - ➔ at application level
 - ➔ commercial solutions for all three approaches are available

- ➔ All approaches have pro's and con's

- ➔ Pro app-level encryption
 - ➔ Complete control over when and where to enforce encryption
 - ➔ Minimal performance impact given the selective use of encryption calls
 - ➔ Equality queries are much easier: simply encrypt the search criteria and search for its match in the encrypted table
 - ➔ Protects against a broad range of threats, VERY strong security model (Even a malicious DBA cannot see encrypted data)

sales@comforte.com | www.comforte.com

transparent within database:

available ie for Oracle/SQL Server

what's gained: DB admin can still read data at will

Pros of application-level encryption

- Complete control over when and where to enforce encryption
- Minimal performance impact in application logic given the selective use of encryption calls
- Equality queries are much easier: simply encrypt the search criteria and search for its match in the encrypted table
- Protects against a broad range of threats - VERY strong security model. Even a malicious DBA cannot see encrypted data.
- Comforte can do all the programming work!

Cons of database-level encryption

- Limited protection against malicious DBAs, since DBAs can control views & triggers
- Indexing/searching becomes problematic due to view-based implementations: everything has to be decrypted before any searching can be done.
- Equality queries are not supported unless deploying in conjunction with application encryption
- Schema changes may have to occur for proper and practical implementation
- Performance impacts can be severe in large searches

comForte and Ingrian

The screenshot shows the comForte website interface. At the top, there is a search bar and a navigation menu with links for COMPANY, SOLUTIONS, PRODUCTS, SERVICES, SUPPORT, and NEWS. The main content area features a news article titled "comForte partnering with industry leader Ingrian for database encryption" dated May 2, 2006. The article text describes the partnership between comForte and Ingrian Networks, Inc. to allow applications running on HP NonStop servers to interact with the Ingrian DataSecure platform. A quote from Michael Horst, CTO of comForte, is also included. On the right side of the page, there are sections for "PRODUCT FINDER" with dropdown menus for "Access a NonStop system", "Security", and "Legacy Extension/Integration", and a "RELATED TOPICS" section listing links for "Database Encryption", "Encryption of Backup Tapes", "The PCI standard", and "comForte and Ingrian Networks Join Forces".

http://www.comforte.com/

comForte

Search GO

LOGIN AREA

PRODUCT FINDER

Access a NonStop system
Choose solution

Security
Choose solution

Legacy Extension/Integration
Choose solution

RELATED PRODUCTS

RELATED TOPICS

- Database Encryption [\[more\]](#)
- Encryption of Backup Tapes [\[more\]](#)
- The PCI standard [\[more\]](#)
- comForte and Ingrian Networks Join Forces [\[more\]](#)

COMPANY | SOLUTIONS | PRODUCTS | SERVICES | SUPPORT | NEWS

Home → News → Company News

NEWS

- Company News
- Product News
- Success Stories
- In the media
- Events

comForte partnering with industry leader Ingrian for database encryption

May 2, 2006

comForte and Ingrian® Networks, Inc., the leading provider of data privacy solutions are announcing a partnership that will allow applications running on HP NonStop™ servers to interact with the Ingrian DataSecure platform.

Ingrian DataSecure platforms provide an intelligent, cost-effective way to protect critical data from threats inside and outside the network. Featuring dedicated hardware appliances and patent-pending cryptography software, Ingrian's solutions deliver capabilities for granular encryption, seamless integration and centralized security management.

"Driven by regulatory standards in several vertical markets, we see an increased demand for data-at-rest encryption for HP NonStop servers," said Michael Horst, CTO of comForte. "Partnering with an industry leader allowed us to

http://www.ingrian.com/news/pr060501.html

INGRIAN NETWORKS Enabling Data Privacy in the Enterprise

CONTACT US SITE MAP

HOME ABOUT PRODUCTS SOLUTIONS SUPPORT PARTNERS NEWS + EVENTS

NEWS + EVENTS

Press Release

comForte and Ingrian Networks Join Forces to Deliver World Class Data Encryption Solution on HP NonStop Servers

comForte announces interoperability of the Ingrian data encryption offerings on HP NonStop servers

OLD TAPPAN, New Jersey, and REDWOOD CITY, Calif.—May 1, 2006—comForte Inc., a market leader for network encryption solutions for HP NonStop™ servers, and Ingrian® Networks, Inc., the leading provider of data privacy solutions, today announced a partnership that will allow applications running on HP NonStop servers to easily integrate with Ingrian DataSecure® Platforms.

"Driven by regulatory standards in several vertical markets, we see an increased demand for data-at-rest encryption for HP NonStop servers," said Michael Horst, CTO of comForte. "Partnering with an industry leader allowed us to focus on the specifics of the NonStop server rather than having to 'reinvent the wheel'. Bringing the Ingrian offerings to the NonStop server results in a world-class cross-platform database encryption solution becoming available to NonStop users around the world."

HP NonStop servers "own" the business-critical infrastructures fueling the vast majority of the world's electronic commerce. Companies that rely on

HIGHLIGHTS

[Ingrian Nets \\$15.4 Million in Fourth Round Funding](#)

[Ingrian Customer Vegas.com featured in eWeek](#)

[InformationWeek: Ingrian helps Union Bank better protect customer data](#)

"DataSecure provides a rich range of encryption methods and role-based security that can be mapped to SQL or LDAP databases. It also nails auditing. You easily see anything that's ever been done in the system, including failed encryption attempts, configuration changes, and system reboots... Overall, an excellent solution for protecting sensitive

sales@comforte.com | www.comforte.com



Ingrian DataSecure Platforms encrypt and secure critical data stored in applications and databases.

By centralizing encryption, keys, and policies, Ingrian enables data privacy— with ease of implementation, scale and cost-effectiveness.



Gain the security of encryption, without the headaches

Ingrian Networks, Inc. Confidential Disclosure Presentation

21

Ingrian offers a solution for encrypting critical data in applications and databases, and it enables organizations to implement encryption while avoiding the traditional obstacles of encryption just cited.

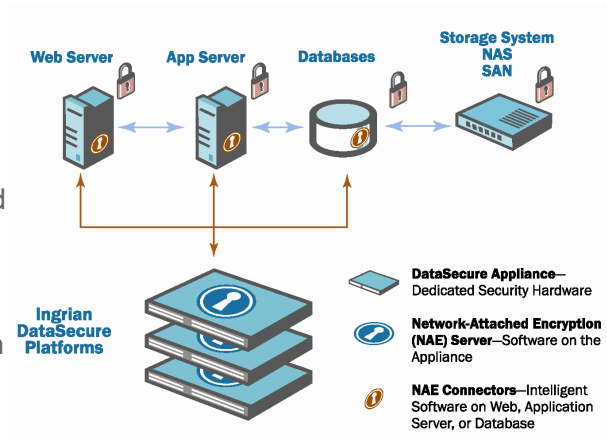
Ingrian has invested a lot of R&D into enabling column-level encryption with application transparency, meaning organizations don't need to alter application code to implement Ingrian

By doing all cryptographic processing on a dedicated appliance, Ingrian offers high performance processing, and it offloads this processing from application and database servers that would otherwise need to do this processing.

Because all keys and cryptographic policies are managed on a central appliance, keys are more secure and maintenance is streamlined dramatically

And because this solution can be deployed at multiple integration points with a variety of servers and databases, costs and administration are reduced, particularly in heterogeneous environments.

- Integrated with Web server, app server, or database
- Column- or field-level encryption of sensitive data in applications and database
- Cryptographic keys, security policies managed centrally from appliance



Here's a diagram to illustrate where Ingrian can fit in a network environment.

The way the process works is this:

Application or database calls local agent and passes data to be encrypted.

Agent connects to Ingrian DataSecure Platform, passes authentication credentials, establishes secure connection, and performs load balancing and connection pooling.

DataSecure authenticates application or database, authorizes key access, performs cryptographic functions, and logs all processes.

Encrypted data is securely sent back to application or database.

Robust security—protect against a broad range of threats

Implementation—centralized, intuitive, automated

Scalability and reliability

Flexible, multi-tier integration—deploy in multi-vendor environments, and at Web, app, and/or database level

•Robust security.

- Secure appliance with physical and administrative safeguards, unlike servers, only accessible to admins.
- Secure key management—keys always encrypted, never on servers; secure key backup; FIPS hardware security module option
- Segregation of administrative duties.
- Secure, multi-factor authentication and access control.
- Granular authorization capabilities applied to groups and users.
- Active alerting capabilities.
- Comprehensive, secure, and centralized logging and auditing.

Streamlined implementation. Integration is automated and transparent to applications; administration is intuitive; and because all keys and policies are managed on a centralized appliance, ongoing maintenance is streamlined. The product features automated and centralized key rotation, backup and recovery

Scalability and reliability. Offloads processing-intensive cryptographic functions from servers, and offers throughput and high availability for even the most demanding environments, featuring capabilities for load balancing, failover, and disaster recovery.

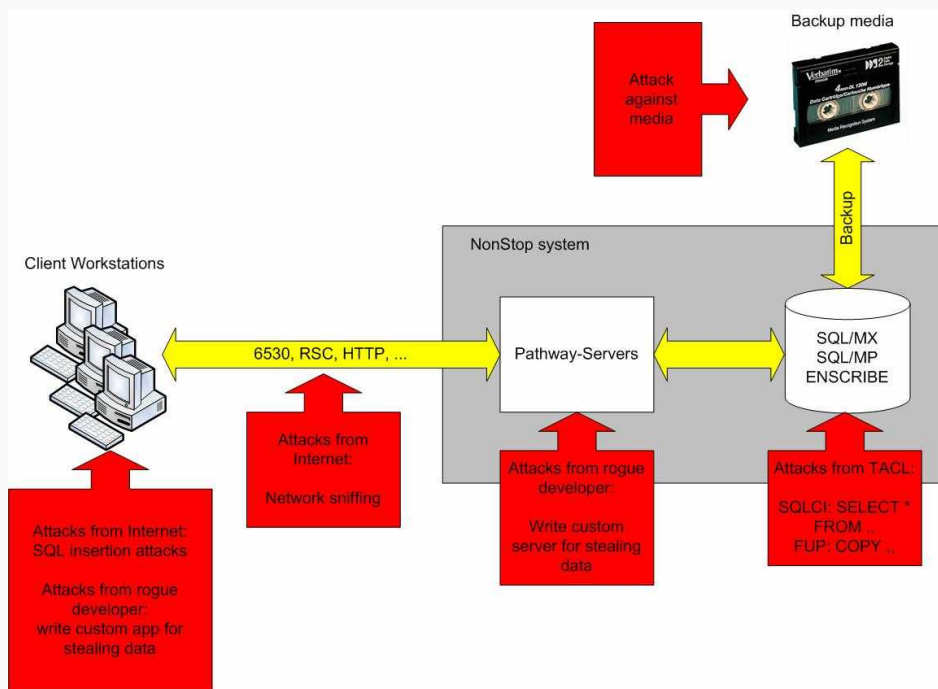
Flexible, multi-tier integration. This centralized solution can be deployed in multi-vendor environments, and can be deployed easily at the Web, application, and/or database level.

Some devils in the details

- database encryption is not a simple „switch it on“ project
- some devils in some details
 - no integration with ENSCRIBE or SQL (yet)
 - need to define key management policy
 - need to implement key rotation
 - a proper protection of a database application goes beyond “just” encrypting the database (ie protect against SQL injection attacks, next slide)
 - treatment of alt keys
 - crypto details (initialization vectors, algorithms, ...)
 - performance considerations

This slide discusses some of the reasons why database encryption is not easy to implement. Customers have to understand that implementing database encryption requires careful consideration and planning.

An OLTP App on NonStop – attack vectors



sales@comforte.com | www.comforte.com

This slide shows potential attacks against an OLTP application on a NonStop system. As the data can be attacked in various ways it has to be protected at several levels.

Protecting against a misuse of "SUPER" rights (by simply dumping large parts of the database from SQLCI or TACL) is the prime reason to encrypt the data within the database.

SQL insertion attack

➔ Enter Username:

```
SELECT * FROM people WHERE first_name="frank";
```

➔ Enter Username:

```
SELECT * FROM people WHERE first_name="frank" OR first_name LIKE"*";
```

➔ Enter Username:

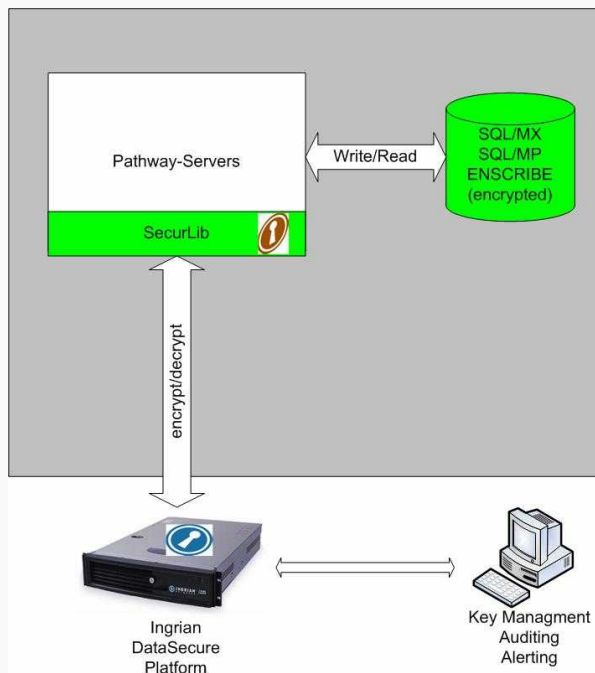
```
SELECT * FROM people WHERE first_name="frank"; DROP TABLE people; " ";
```

This slide presents the infamous SQL insertion attack which completely bypasses all other security mechanisms and has to be prevented at the application level by implementing proper input validation.

Performance of database encryption

- Performance is probably less of an issue than expected:
(all values shown are "*CPU ms consumed for one crypto operation*")
 - Performance in software alone (AES/256): < 1 ms / Transaction (for crypto)
 - Performance using Ingrian device: < 1 ms (for IO via IP and message generation/parsing)
 - for bigger blocks of data or 3DES, Ingrian device is faster

Database encryption using SecurLib



- ➔ comForte is partnering with Industry leader in DB encryption (Ingrian Networks)
- ➔ Leverage a centralized, standard-based approach to increase ROI
- ➔ Hardware encryption for
 - ➔ compliance with legislation and policy, secure key storage
 - ➔ cross-platform support
 - ➔ FIPS-140-2 Level 3 compliant if needed
- ➔ Optional integration with SecurCS, SecurFTP, SecurTN
- ➔ SecurLib also works “stand-alone” with identical API and encryption in software only

This slide shows the architecture of SecurLib when using the “application integration” approach discussed on earlier slides (rather than direct integration at the database level).

SecurLib: today and in the future

→ SecurLib today

- High-level API for cryptographic operations
- encryption either in software or using the Ingrian DataSecure™ platform
- integration at application level
- key management/rotation also at application level

→ SecurDB tomorrow

- transparent encryption of ENSCRIBE databases
- key rotation handled transparently by SecurDB

→ SecurDB next year

- integration within SQL/MX ?
- needs “hooks” provided by HP
 - if you would want that product, please contact comForte & HP

Why comForte for DB encryption

- partnership with industry leader for DB encryption
- crypto/security know-how
- a viable solution available *today*, open to your requests for enhancements

Summary

- ➔ Backup tape encryption
 - ➔ solution in software and hardware
 - ➔ both solutions transparent to existing environment

- ➔ Database encryption
 - ➔ solution with or without key/crypto offloading to Ingrian DataSecure platform
 - ➔ application-level integration available today
 - ➔ transparent ENSCRIBE support available “tomorrow”
 - ➔ SQL integration subject to hooks provided by HP

Questions ?

contact:

sales@comforte.com

t.burg@comforte.com

<http://www.comforte.com>