Identify and Protect your Sensitive Data with Seamless Interception

**Jack Di Giacomo
TANDsoft, Inc.**

Identify and Protect your Sensitive Data with Seamless Interception

Jack Di Giacomo

TANDsoft, Inc.

Jack loves the outdoors

30 years of experience in the design, development and support of NonStop software solutions.

Former Tandem instructor and Specialist in intercept technology.

Let's define Interception Technology as it applies to computer programming

Interception technology covers a range of techniques that can be used to alter or augment the behaviors of applications, operating systems, or other software components by intercepting function calls or system calls.

Interception Technology on NonStop
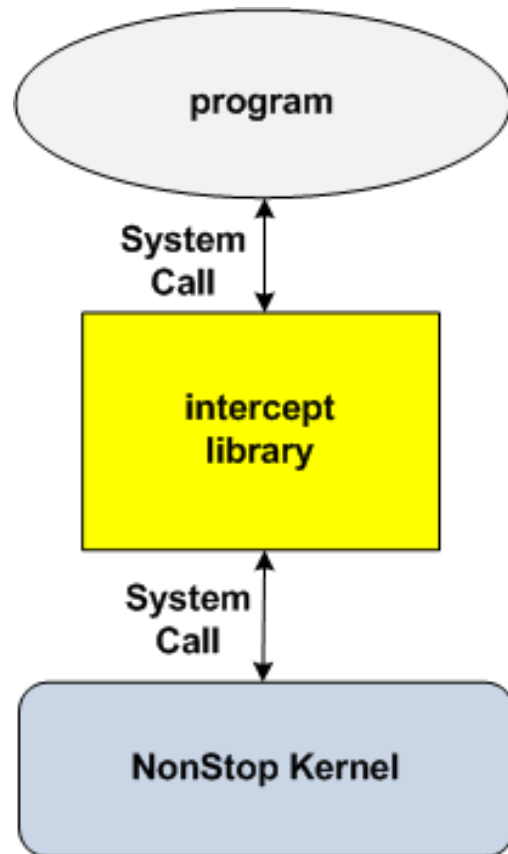
The code that handles intercepted function calls, system calls, events, or messages is called a "hook" or an "intercept" library.

Architecture of Interception
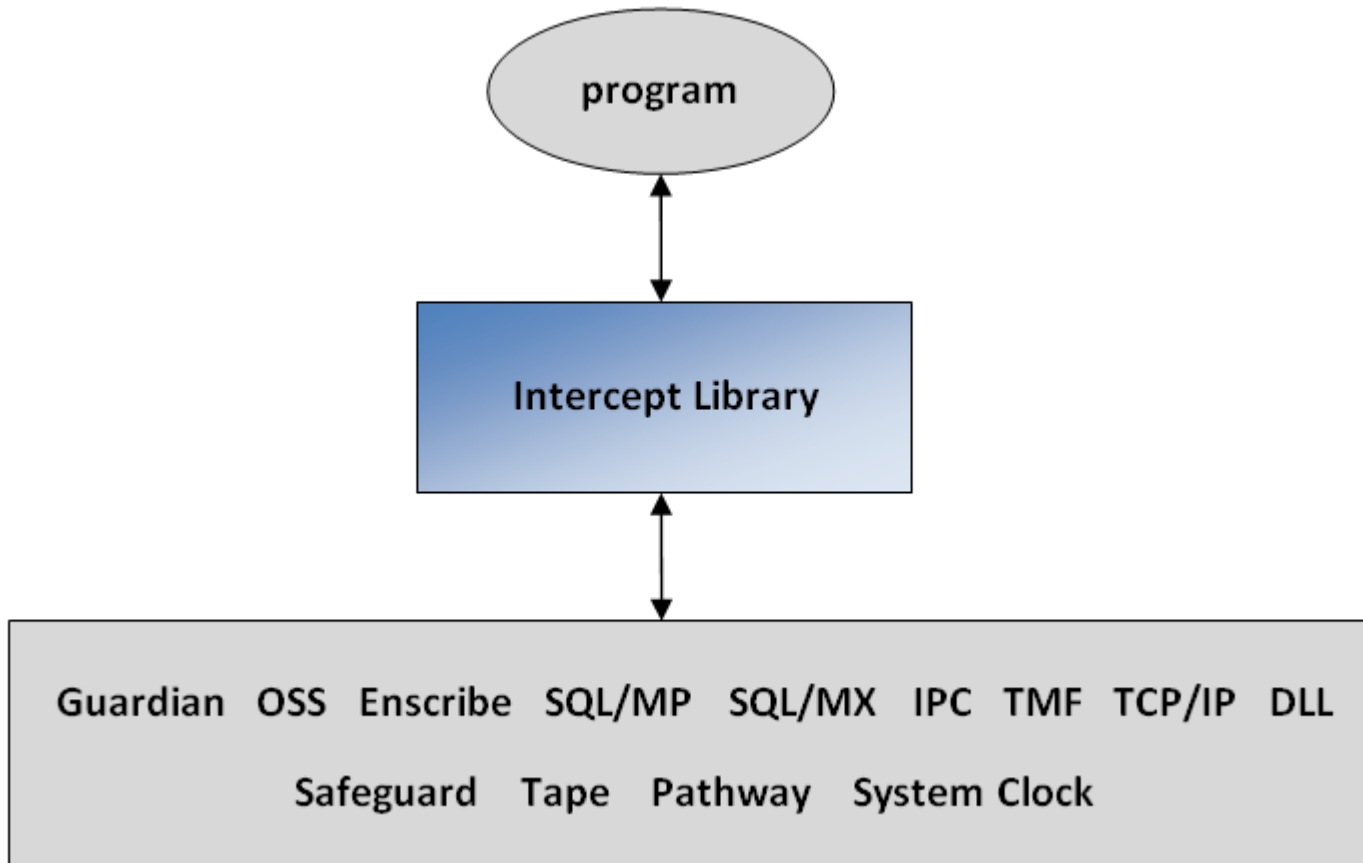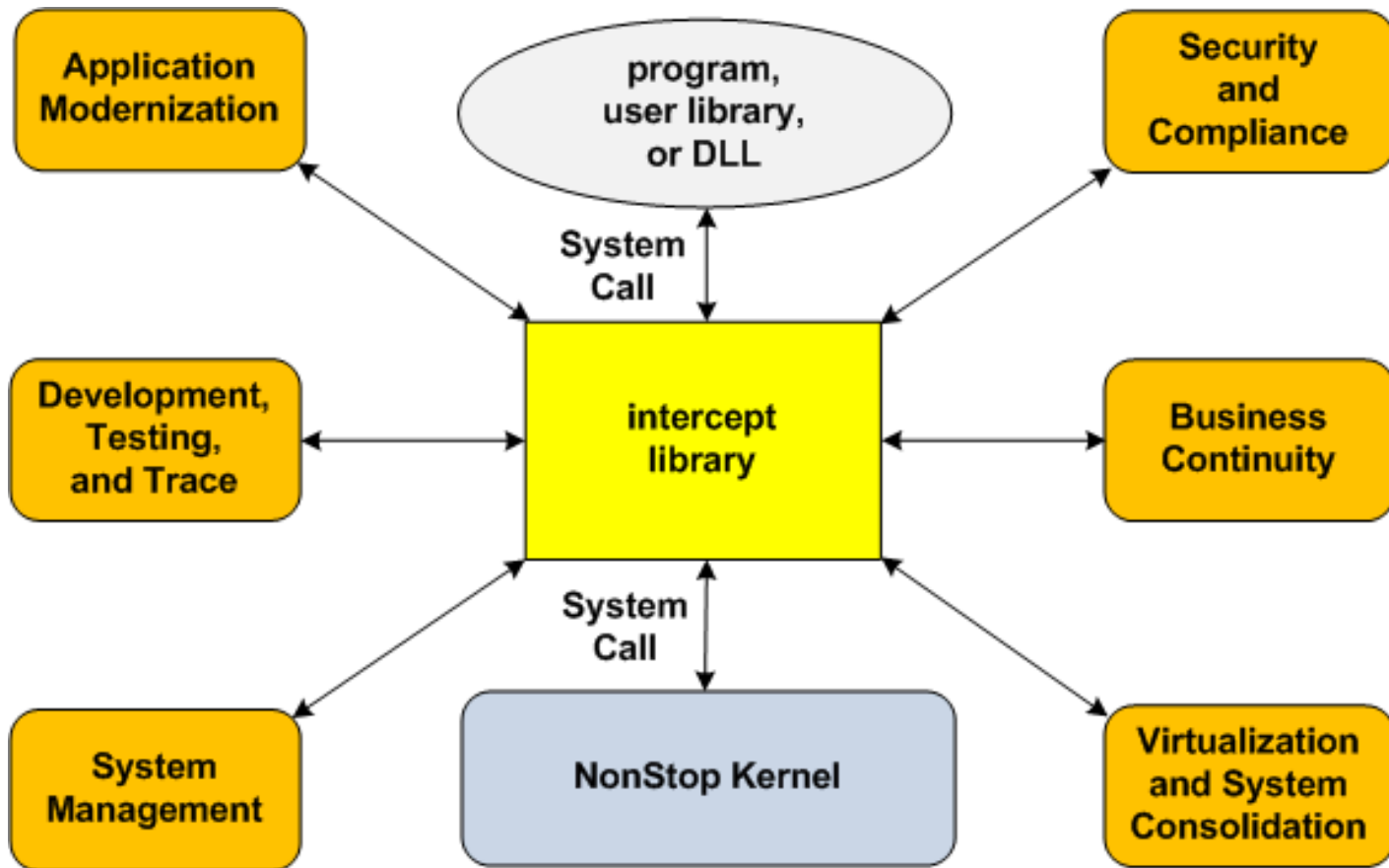
The best thing about Seamless Interception...

No Source Code Required!

No Need to Recompile Programs!

Works with all Apps!

Interception Technology is used to monitor behaviors and to modify application functions

NonStop customers use interception to extend application functionality

Business Continuity

Business Continuity

Business Continuity

- **Automatic TMF protection of Enscribe files.**
  - Insert TMF transactions BEGINTRANSACTION, ENDTRANSACTION

- **Replicate Enscribe unaudited files or Enscribe file modifications to a backup site**

- **Replicate Enscribe, SQL/MP, and SQL/MX DDL changes to a backup site**

TAND
Soft
NonStop Interception
& Availability Solutions

CONNECT

NonStop customers use interception to extend application functionality

Virtualization and System Consolidation

- **Time-Zone simulation**

  - Allows Guardian and OSS applications to operate within any virtual time zone

- **System Clock simulation**

  - Allows Guardian and OSS applications to operate with any virtual system clock or current time value

Large North American bank used interception to consolidate applications requiring multiple time zones into one data center

Virtualization and System Consolidation

The bank decided to consolidate its West-Coast operation into its East-Coast data center as a cost-savings measure. A challenge was determining how to run applications that needed to run in the Pacific Time Zone on a system with a clock set to the Eastern Time Zone.

Using interception technology, the bank created virtual time zones that allow one production system to service two time zones and one disaster recovery system to service two time zones.

TAND
NonStop Interception
& Availability Solutions

connect

NonStop customers use Seamless Interception to Identify and Protect Sensitive Data

Security and Compliance

- **Identifies and logs all sensitive database access**
- **Protects sensitive data at rest via**
  - **encryption or tokenization**
  - **data masking**
- **Supports Enscribe, SQL/MP, SQL/MX, TNS/R,E,X**
- **All without the need for any application modifications**
- **Helps organizations comply with government and industry regulations (PCI, GDPR)**

Seamless Intercept Technology Example for Security and Compliance

Security

Intercepts HPE NonStop database access calls, then works with HPE, third-party, or in-house security solutions to protect sensitive data by encrypting / tokenizing data written to disk and decrypting / de-tokenizing data read from disk.

Intercepts and Masks sensitive data.

Compliance

Intercepts and Logs sensitive database access and statements.

TAND
Soft
*NonStop Interception
& Availability Solutions*

CONNECT

Identify and protect Enscribe, SQL/MP and SQL/MX Sensitive Data

We all agree, it is critical to protect sensitive data

Protect - NonStop sensitive data

Using Seamless interception technology +

- comForte SecureDPS
- Micro Focus (Voltage, Xypro) SecureData
- Protegrity and others
- Data masking

Identify - NonStop sensitive data

Using Seamless interception technology to

- Log all access to NonStop DB

Seamless Data Protection - Example

Protect (with no source code changes) two columns in <u>EMPLOYEE SQL/MP table</u>

mxci (version with intercept library, IL) will be used to access the EMPLOYEE SQL/MP table.

Customer can use any Encryption or Tokenization engine.
- **NonStop Partner solutions**
- **Micro Focus/HPE/Voltage SecureData**
- **Protegrity or other**

For this example, a simple encryption technique was used;
- **Character substitution: 0 = 9,   1 = 8,   2 = 7, . . . $ = %**

Seamless Data Protection - Example

SQL/MP Table EMPLOYEE

```
( EMP_ID          SMALLINT NO DEFAULT NOT NULL
, NAME            CHAR(10) NO DEFAULT NOT NULL
, SSN             CHAR(11) DEFAULT NULL
, HIRED_DAY       DATETIME YEAR TO DAY DEFAULT NULL
, END_DAY         DATETIME YEAR TO DAY DEFAULT NULL
, SALARY          CHAR(10) NO DEFAULT NOT NULL )
```

Protected Table EMPLOYEE , Columns SSN, SALARY

Data in the Clear (Green)

Data is Encrypted / Tokenized (Red)

Data is Masked (Purple) SSN mask = (xxx-xx-x???)

Seamless Intercept Library (Transparent, NO App changes) (Dark Red)

TAND Soft
NonStop Interception
& Availability Solutions

CONNECT

Seamless Data Protection - Example

mxci (with IL) will be used to access the SQL/MP table.

    Intercept Library name = **sdSQLdll**
    Original mxci = /usr/tandem/sqlmx/bin/mxci
    mxci program = **/demo/mxci**
    eld -change libname '$sas21.sdi2.**sdSQLdll**' /demo/mxci

run mxci (with IL):
    osh -c "run **/demo/mxci**"

Seamless Data Protection - Example

mxci - INSERT into **=employee** values (2, 'John D', **'222-12-3456'** ,
      datetime **'2017-08-01'** YEAR TO DAY, NULL, **'$60,000'**);

PROCESS_MX_TABLE (Table=$SAS21.SDI2.**EMPLOYEE**)
REGISTER_MX   **(SSN, SALARY)**
Registered Columns   **(Table=$SAS21.SDI2.EMPLOYEE: SSN,SALARY)**
Process_Col.in.   **{SSN, InsUpd, (222-12-3456)} {SALARY, InsUpd, ($60,000)}**
Process_Col.out. {SSN, InsUpd, (777-87-6543)} {SALARY, InsUpd, (%39,999)}

--- 1 row(s) inserted.

Seamless Data Protection - Example

Original SQLCI - SELECT * from =employee;

EMP_ID	NAME	SSN	HIRED_DAY	END_DAY	SALARY
2	John D	777-87-6543	2017-08-01	?	%39,999

mxci - SELECT * from =employee;

Process_Col.in.   {SSN, Read), (777-87-6543)} {SALARY, Read), (%39,999)}
Process_Col.out.   {SSN, Read), (xxx-xx-x456)} {SALARY, Read), ($60,000   )}

EMP_ID	NAME	SSN	HIRED_DAY	END_DAY	SALARY
2	John D	xxx-xx-x456	2017-08-01	?	$60,000

Seamless Data Protection - Example

mxci - UPDATE **=employee** set salary = **'$65,000'** where emp_id = 2;

    Process_Col.in.   **{SALARY, InsUpd ($65,000)}**
    Process_Col.out.   **{SALARY, InsUpd (%34,999)}**

--- 1 row(s) updated.

Original SQLCI - SELECT * from **=employee**;

EMP_ID	NAME	SSN	HIRED_DAY	END_DAY	SALARY
2	John D	777-87-6543	2017-08-01	?	%34,999

--- 1 row(s) selected.

mxci – DELETE from **=employee** where emp_id = 2;

    --- 1 row(s) deleted.

Seamless Intercept Technology API - Example

**mxci - INSERT into =employee values (2, 'John D', '222-12-3456',
datetime '2017-08-01' YEAR TO DAY, NULL, '$60,000');**

Seamless Intercept API	**+**	Protection Code

calls PROCESS_MX_TABLE (=employee)

For a protected table (=employee),
   calls REGISTER_MX (SSN,SALARY)

calls PROCESS_COL

input = {SSN, (222-12-3456)},
         {SALARY, ($60,000)}
output = {SSN, (777-87-6543)},
         {SALARY, (%39,999)}

mxci - SELECT * from =employee;

calls PROCESS_COL

input = {SSN), (777-87-6543)}
         {SALARY), (%39,999)}
output = {SSN), (xxx-xx-x456)}
         {SALARY), ($60,000)}

TAND
*NonStop Interception
& Availability Solutions*

connect

Identify and Log NonStop DB Access - Example

Log NonStop DB access (Insert, Update, …) to <u>EMPLOYEE table (columns SSN and SALARY)</u>

- **Program name, Process name, Login name, File/ Table name, Column Name, DB Access, Time Stamp**

<u>Log DB SQL statements from mxci program</u>

- **Program name, Process name, Login name, Time Stamp, SQL Source Statement**

** Data from Seamless Data Protection example used for following slides **

Identify DB Access – Example
(NonStop DB Access Log)

SELECT * from **=SDIAUDE**;

Program	Process	Login Name	Table	Column	Access	Time Stamp
/mxci	$Z123	TAND.JACK	=EMPLOYEE	SSN	Insert	2017-10-07 19:11:27.088123
/mxci	$Z123	TAND.JACK	=EMPLOYEE	SALARY	Insert	2017-10-07 19:11:27.097439
/mxci	$Z123	TAND.JACK	=EMPLOYEE	SSN	Read	2017-10-07 19:11:27.482625
/mxci	$Z123	TAND.JACK	=EMPLOYEE	SALARY	Read	2017-10-07 19:11:27.491312
/mxci	$Z123	TAND.JACK	=EMPLOYEE	SALARY	Update	2017-10-07 19:11:27.582885
/mxci	$Z123	TAND.JACK	=EMPLOYEE	SSN	Read	2017-10-07 19:11:27.770105
/mxci	$Z123	TAND.JACK	=EMPLOYEE	SALARY	Read	2017-10-07 19:11:27.779283

Identify DB Access - Example
(NonStop DB Statement Log)

SELECT * from =SQLAUDE;

Program Process Login Name Time Stamp   Statement

/mxci $Z123 TAND.JACK 2017-10-07 19:11:27.085 select variable_info from table (statistics
(null, cast(? as char(256) character set iso88591)))

/mxci $Z123 TAND.JACK 2017-10-07 19:11:27.086 select attr_value from
nonstop_sqlmx_NSBLDE4.system_defaults_schema.system_defaults where
subsystem = 'SQLMX' and attribute = 'M

/mxci $Z123 TAND.JACK 2017-10-07 19:11:27.381 insert into =employee values (2, 'John D' ,
'222-12-3456' , datetime '2017-08-01' YEAR TO DAY, NULL , '$60,000');

/mxci $Z123 TAND.JACK 2017-10-07 19:11:27.482 select * from =employee;

/mxci $Z123 TAND.JACK 2017-10-07 19:11:27.685 update =employee set salary = '$65,000'
where empid = 2;

/mxci $Z123 TAND.JACK 2017-10-07 19:11:27.770 select * from =employee;

/mxci $Z123 TAND.JACK 2017-10-07 19:11:27.998 delete from =employee where emp_id = 2;

Identify - NonStop DB Access - Usage

Industry compliance (PCI, GDPR)

Auditing - Log all sensitive data access.

List all access to the Primary Account Number (PAN)
- select * from =SDIAUDE where Column = 'PAN' ;

Detect Fraudulent or unauthorized access

List all DB access to PAN column between midnight & 6 am
- select * from =SDIAUDE where Column = 'PAN' and cast (timestamp as datetime HOUR) between
  datetime '00' HOUR and datetime '06' HOUR ;

Identify - NonStop DB Access - Usage

Quality Control and Testing

Compare SQL source statement repository for each product release.

List all SQL statements from program remote/banking server
- **Select * from =SQLAUDE where program like '%remote/banking%';**

List all SQL statements from mxosrvr (JDBC/ODBC) server.
- **Select * from =SQLAUDE where program like '%mxosrvr%';**

TAND
*NonStop Interception
& Availability Solutions*

CONNECT

The best thing about Seamless Interception for Sensitive Data ...

No Source Code Required!

No Need to Recompile Programs!

Works with all Apps!

In Production and available today!

Thank You for Attending

Any Questions?

Ask them now, or contact me later at

jack.digiacomo@tandsoft.com

www.tandsoft.com