Identify and Protect Your Sensitive Data with Seamless Interception

Jack Di Giacomo, TANDsoft Inc.
Beaconsfield, Quebec, Canada

Your name is John Doe. Your nine-digit U.S. Social Security Number (SSN) is 123-45-6789. You earn an annual salary of USD $93,000, and your employer maintains all your personal information as *unprotected* data in the company database. Do you think that John Doe's unsecured data is an isolated incident? Think again. Although we all may agree how critical it is to protect sensitive data, there exist many companies that continue to keep such data in the clear. Firewalls may offer some protection, and many companies believe that their firewalls are good enough. Reality check – often, they're not. Should hackers succeed in gaining unauthorized access into John Doe's company network, his data will be just as vulnerable as if it were plastered in flashing neon lights all over a highway billboard.

EMP ID	NAME	SSN	HIRED DAY	END DAY	SALARY
2	**John D**	**123-45-6789**	**08-01-2017**	**?**	**$93,000**

*Green = data in the clear

Nowadays, the exposure of sensitive personal information via data breaches takes places on an all-too-regular basis. Among them: Equifax (2017) – 143 million users of one of the United States' three major credit reporting agencies had their private data exposed. Yahoo (2013/2014) – all three billion Yahoo users worldwide had their names, email addresses, and passwords accessed by hackers. Uber (2016) – 57 million riders and drivers of this global ridesharing company had their personal data compromised. My Fitness Pal (2018) – Sportswear brand Under Armour announced that 150 million users of its popular nutrition app had their user names and passwords breached.

Once a firewall is breached, what makes the difference between stolen data being rendered useless to hackers or being offered for sale on the Dark Web is whether that data was further hack-proofed via tokenization and/or encryption, two methods by which to secure personal data. *Tokenization* is the process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token, that has no exploitable meaning or value. *Encryption* translates personal data into another form, or code, so that only people with access to a secret key (decryption key) or password can read it.

EMP ID	NAME	SSN	HIRED DAY	END DAY	SALARY
2	**John D**	**631-32-6789**	**08-01-2017**	**?**	**$39,999**

***Secured Data with Format Preservation** (last four SSN digits remain in the clear for verification purposes)

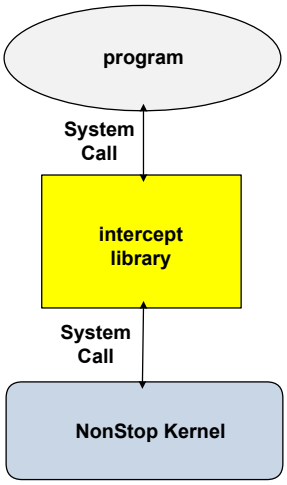
In the case of both tokenization and encryption, what allows unencrypted (plaintext) operations performed by authorized users to be converted into encrypted (ciphertext) data for interpretation by a protected data file, then reconverted into plaintext data for return to the same authorized users is the concept of interception technology.

Let's Define Interception Technology

Interception technology covers a range of techniques that can be used to alter or augmentthe behaviors of applications, operating systems, or other software components by intercepting function calls or system calls. The result is the creation of new application functionality without the need to make costly, time-consuming modifications or complete recompiles.

The code that handles intercepted function calls, system calls, events, or messages is commonly called a hook. In the HPE NonStop world, a hook is known as an intercept library. It sits between an operating system and a program, a user library, or a dynamic link library (DLL). As a process carries out a function (read/insert/update/delete), the attached intercept library captures the system call, modifies the call to handle whatever new functionality is intended, and sends the modified call to the operating system, represented here by the NonStop Kernel.

When the intercept library receives a response from the operating system, it returns the modified response to the process. The entire operation is so seamless that at no time is the process aware that any modifications were made to its original system call.

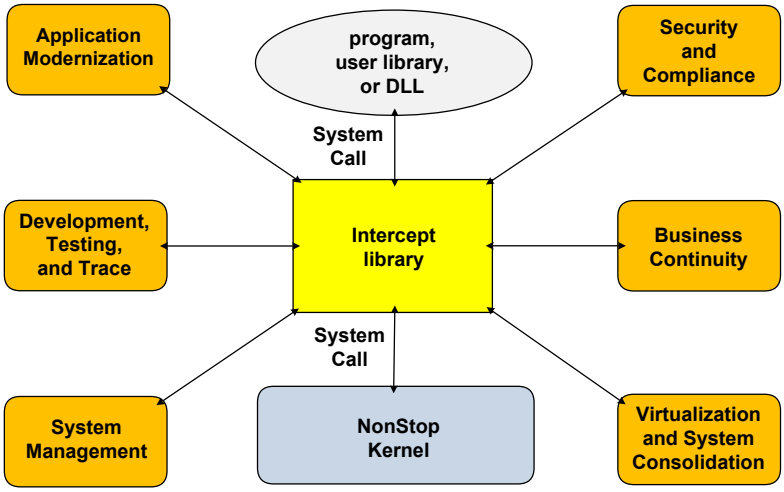


No Source Code Required

The best thing about interception technology is that no source code is required, of particular importance when the source code is unavailable. Interception technology does not alter application logic and is language-ambivalent because it works directly with object files.

Seamless Interception in the NonStop Environment

HPE NonStop customers use seamless interception in a variety of ways to extend the functionality of their applications. For instance:



Application Modernization – provides automatic TMF protection of non-audited Enscribe files. Enables the conversion of Enscribe files to SQL tables.

Business Continuity – replicates Enscribe, SQL/MP, and SQL/MX DDL changes to a backup site. Replicates Enscribe unaudited files or Enscribe file modifications to a backup site.

Development, Testing, and Trace – lists program procedure calls to the NonStop Kernel. Identifies deadlocks and program sequencing errors. Monitors process stack usage to avoid abends caused by stack overflow. Adds Enscribe file-format modifications without the need to reprogram.

System Management – files accidentally purged or deleted can be recovered from a recycle bin. Scripts can be executed upon process termination. Workloads can be balanced between CPUs and disks. Low-pin resources can be optimized across all CPUs.

Virtualization and System Consolidation – allows Guardian and OSS applications to operate within any virtual time zone. Allows Guardian and OSS applications to operate with any virtual system clock or current time value.

Use Seamless Interception for NonStop Security and Compliance

Security and Compliance

Within the NonStop world, an intercept library seamlessly intercepts NonStop database access calls from Guardian and OSS applications, then works with a variety of HPE, third-party, or in-house security solutions to protect sensitive data (Enscribe, SQL/MP, SQL/MX) by encrypting / tokenizing data written to disk and decrypting / detokenizing data read from disk. For instance, TANDsoft's Sensitive Data Intercept (SDI) is an intercept library that is embedded into the solutions of HPE security partners comForte and XYPRO.

Interception technology also helps companies comply with government and industry regulations as well as enforce security policies by identifying all sensitive database access and statements, then logging the data for authorization and authentication.

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

Protect - NonStop sensitive data

Use seamless interception technology +

- **comForte SecurDPS**
- **Micro Focus (Voltage, XYPRO) SecureData**
- **Protegrity and others**
- **Data masking**

Identify - NonStop sensitive data

Use seamless interception technology to

- **Log all access to NonStop DB**

Intercept Libraries Satisfy Multiple Security Preferences

As mentioned earlier, an intercept library can serve numerous purposes. Since it functions directly with object files, application modifications can be made without the presence of source code. If you purchased software from a third-party provider, you don't need the source code. If you use HPE code, you don't need the source code. Even if you wrote the application in-house and have the source code, you don't need the source code.

Identify Sensitive Data

The process of auditing/logging company data is often manual, labor-intensive, and particularly challenging when companies must work with auditors for the purpose of regulatory compliance. An intercept library can be configured to capture all of a customer's database calls and then to log that access. Customers can see who or what is accessing sensitive data, the times of access, and what specific data is being accessed. In these cases, no sensitive data is being encrypted or decrypted. Only database interception is taking place. The auditing/logging process also is valuable for the purposes of fraud detection and security whitelisting from both internal and external sources.

Mask Sensitive Data

Masking data is a 24x7, year-round effort to protect sensitive data. It is used for internal purposes, preserves the original format (SSN = 123-45-6789), yet is altered in such a way as to make unauthorized detection and reverse engineering impossible (SSN = XXX-XX-6789). Because the formatting is preserved, the masked data still can be used for application development, testing, training, and other functions.

Protect Sensitive Data – Three Scenarios

Scenario 1 – No intercept library, No NonStop security solution

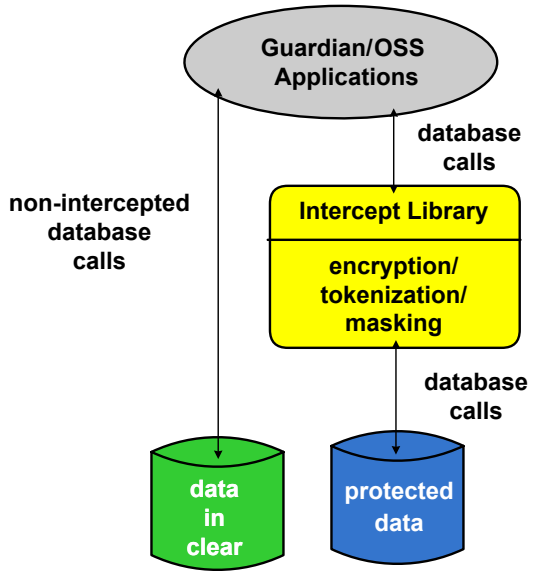
Regardless of whether a firewall is present or absent, application database calls are made with clear data; and responses are received with clear data. No encryption or tokenization takes place. If the firewall is breached, often because of network configuration errors, system security is compromised and can result in data being vulnerable to theft and misuse by unauthorized parties.

Scenario 2 – No intercept library, Presence of NonStop encryption / tokenization engine

Available to HPE NonStop customers are several outstanding security solutions. Once an encryption or tokenization engine is selected, the result allows customers to protect their sensitive company, individual, and customer data from unauthorized access, regardless of whether a network incursion takes place.

As it is with Scenario 1, a Guardian or OSS process will make an operating-system call to the database. This time, however, the database has been encrypted / tokenized by a NonStop security solution.

Encryption/tokenization is wonderful, but here's the challenge. Guardian/OSS applications always make database calls with clear data and expect to receive responses with clear data. If a security solution is present but does not include an embedded intercept library, application source code must be available; and the applications must be modified to encrypt / tokenize the data before sending to the database and decrypt / detokenize the data received from the database. Such modifications can be time-consuming, expensive, and workload-intensive.



Scenario 3 – Presence of intercept library, Presence of NonStop encryption / tokenization engine

In Scenario 3, an intercept library is embedded within the encryption / tokenization engine. The intercept library associates itself with whatever Guardian/OSS applications will be making operating-system calls. By doing so, the applications seamlessly invoke the intercept library instead of the operating system. Working together, the intercept library and the security provider's engine recognize and implement tokenization and encryption algorithms. For example: a) the intercept library receives an insert/update database function call with data in the clear from an application, encrypts / tokenizes the data, and sends the now encrypted or tokenized data to the pertinent database; b) the intercept library receives a read/select database function call made from an application, receives encrypted / tokenized data from the pertinent database, decrypts / detokenizes the data, and returns it to the application in the clear. The application is able to make database calls with clear data and receive responses with clear data. As such, no source code modifications are required in order for the application to access protected database files.

Summary

Your name is John Doe. Your nine-digit U.S. Social Security Number (SSN) is 123-45-6789. You earn an annual salary of USD $93,000, and your employer maintains all your personal information as *protected* data in the company database.

EMP ID	NAME	SSN	HIRED DAY	END DAY	SALARY
2	John D	631-32-6789	08-01-2017	?	$39,999

***Secured Data with Format Preservation** (last four SSN digits remain in the clear for verification purposes)

Your company is a NonStop customer that takes advantage of one of several security solutions providing powerful encryption / tokenization capabilities. Embedded within those solutions is an intercept library. It allows authorized Guardian / OSS programs to make database calls that access your encrypted data without requiring the programs themselves to have expensive modifications made to them. Intercept libraries do not require source code, of particular importance when the source code is unavailable.

TANDsoft Inc.

Since 1993, TANDsoft has been a global provider of innovative HPE NonStop software solutions for use in time virtualization, security, data replication, and application modernization. We specialize in interception technology, which allows our NonStop customers to enhance their legacy application functionalities without the need for program modifications. TANDsoft's innovative products are easy to install, easy to use, and are backed by exceptional support. They include Sensitive Data Intercept (SDI), an intercept library that works with HPE, third-party, or in-house security solutions to protect sensitive data-at-rest (Enscribe, SQL/MP, and SQL/MX) by encrypting/decrypting data written to and from disk. SDI is embedded into the solutions of comForte and XYPRO, two major HPE NonStop security partners. Its masking/auditing/logging solution is sold separately. Yet another product is FileSync for automatic file synchronization, replication, and data deduplication. Within the NonStop community, TANDsoft is the sole source of time-zone virtualization and clock simulation tools (OPTA2000) for use in consolidated IT environments. For more information about these and other TANDsoft solutions, visit **www.tandsoft.com**, or call us at +1 (514) 695-2234.

Jack Di Giacomo has over 30 years of experience in the design, development and support of NonStop software. As a developer in the platform's formative years, Jack recognized the need for additional tools that at the time were unavailable. In 1993, he created TANDsoft, a company focused on delivering quality NonStop solutions for time virtualization, application modernization, business continuity, and security. Many of the TANDsoft solutions rely on a seamless interception technology, designed and implemented by Jack. Today, he continues to oversee the company's innovation, marketing, and support of an expanding line of products for the NonStop community.
Contact him at **jack.digiacomo@tandsoft.com**.

Vale Thomas Burg – A Giant of the NonStop World

After a long and merciless illness, Thomas Burg passed away this past April. He had been fighting for over two years with admirable strength, never giving up hope.

After having finished the university with a diploma in physics, Thomas joined the NonStop World (still TANDEM at that time) in the early 90s. With his remarkable intelligence and his never-ending appetite for new challenges - far beyond IT, into areas like photography, music and woodworking - he soon was deep into the internals of Guardian. His openness and flexibility, his ability to think outside the box also took him into application areas like banking, retail, and telco.

After having worked several years for MR and ACI, he joined comforte in early 2000 where he started working in the security arena. Although known for his speed and passion to dig into and adapt to new technologies, it was amazing to watch how fast he became one of the experts in this complex subject. While he worked on architectural design and development of security products, he readily shared his expertise with the NonStop community. He authored several publications and he became a member of the CONNECT editorial team. He delivered presentations at TUGs and ITUGs. He ignited open and fruitful discussions throughout HP, customers and vendors.

Thomas was well known for his skills and visions, his openness and objectivity, his fairness and social responsibility. He truly was a giant of the NonStop world.

Thanks Thomas, we are grateful that you were with us. We will miss you.

On behalf of Connect Worldwide we thank Thomas for his years of involvement with the NonStop community and invaluable service as a member of our Editorial Review Committee.