Securing Multiple Platforms for Safeguarding Personal, Enterprise and Cloud-based Information

Navin Govind <navin@antargata.com> CEO, Antargata Pvt. Ltd.

Bhaktha Ram K <bhaktha@antargata.com> CTO, Anatargata Pvt. Ltd.

Abstract: Secure code execution[1] and secure data storage on general purpose computer systems is a known problem for which various solutions hardware and software solution exist. Current hardware based solutions are secure, expensive point solutions with complex deployment models. Software based variations in use now offer a mix between simplicity and ease of integration but, insecure due to inherent vulnerability to malware and rootkit attacks. A patent pending, CPU-based secure code execution approach and method to achieve robust hardware corresponding security with a balanced software approach for easy integration across multiple platforms is presented in this paper. The approach requires judicious use of x86[2] and ARM[3] CPU micro architecture features to hide code execution and data on heterogeneous platforms. In addition to hiding the bits this method is also resistant to differential power analysis (DPA) and cold-boot attacks. Furthermore, to avoid class break scenarios a new encryption algorithm is generated for every instance a client device downloads data or conducts a transaction. The algorithm is based on many combinatorial factors such as device, user ID, time etc., enabling for the first time a true **Multi Factor Security** (MFS) system. The solution has been tested and implemented on several operating systems that include Windows, Linux, Mac OS X, Android as well as hypervisors for x86 and ARM CPU architectures. The implementation of our MFS system is perfectly transparent to the legitimate user and at the same time presents an insurmountable barrier to malicious use. The approach and methods used to implement the MFS system, design implications, resistance to various attacks and performance results are discussed in this paper. Future work involving porting to new architectures is recommended along with suggestions for generating a class of reconfigurable algorithms which are robust to cryptanalysis.

Overview: Software application security and data storage security are still unsolved problems, lack a whole solution on general purpose computing platforms. Securing financial transactions, protecting health records, securing rich applications against malware attacks and securing e-gov transactions benefit greatly from our CPU-based secure code execution technology approach due to a whole solution. Further, securing system software like operating systems, firmware, virtualization layers and anti-malware improves overall system security. The resulting code and data security exponentially increases the value of the overall platform and provisioned services broadly. Figure 1 describes the MFS architecture for securing multiple platforms.

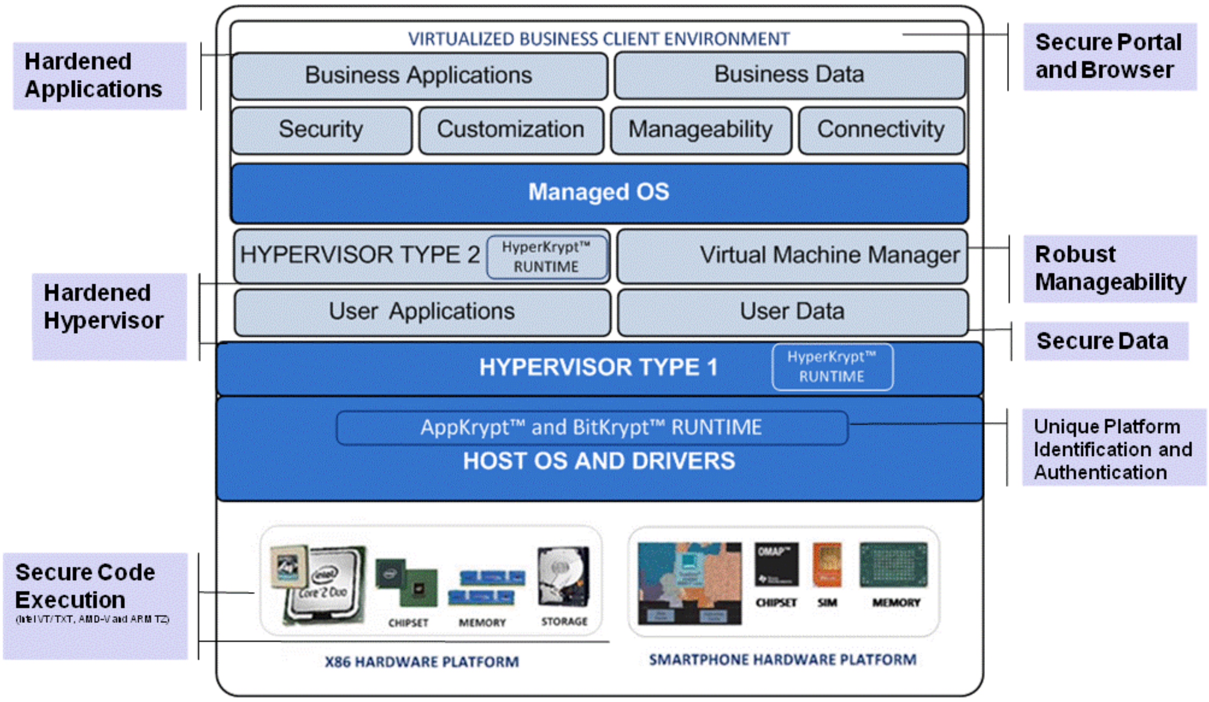

Figure 1: Securing Multiple Platforms with Multi Factor Security Architecture

Theory of operation: Fundamentally there are two main techniques that are used in securing code and data on general purpose processors:

i. **Hiding code and data in CPU micro-architecture constructs:** The basic idea here is that bits of information, code or data, is always in encrypted form on secondary storage and main memory. The encrypted bits are fetched into a CPU core and locked down inside a core using CPU specific hooks. The encrypted bits are decrypted inside the CPU, processed and results obtained. The decrypted bits are then flushed from the CPU innards. Thus the decrypted bits (in the clear) are present transiently inside a CPU core concealed and out of reach of the usual attacks listed in the abstract section.

ii. **Re-configurable algorithms:** Bits of information, code or data, are always downloaded from a server. The server before the download, queries the client machine for various identification strings (e.g. MAC ID, RFID tag, bio-metric data of user, portal CA) then constructs an encryption algorithm which is specific to that machine-user-portal combination. The bits to be downloaded are encrypted using the new algorithm and are downloaded onto the client machine with the library and driver files that are specific to the machine. The functionality and driver implementation is described in the following sections. In the event of a malicious attack to the algorithm the risk of information leakage is limited only to a particular machine avoiding a large class break scenario as is evident in today’s solutions.

With the above two techniques, we can now provide reasonable guarantees for secure code execution and secure data containment on general purpose platforms. The bits downloaded are now linked to a machine-user combination. The encrypted blobs can be moved around at will but can be processed only with a specific machine-user combination. Since the code execution and data processing does not happen in the main memory the technology is resistant to DPA, cold-boot and memory dumping attacks.

The machine-user specific algorithm takes into account multiple factors: machine ID's, User ID's, passwords, bio-metric information, credit card information, portal CA digital keys etc., thus effectively resulting in a Multi Factor Security solution. The technology has proven implementation on x86 and ARM architectures. This MFS solution is now available on Windows, Linux, Mac OS and Virtualization layers.

The implementations we have proven in deployment offer a transparent experience to the user. As long as the legitimate machine-user combination uses the data there is no additional step needed to be performed by the user. This greatly enhances the user experience with a one click encryption and authentication process.

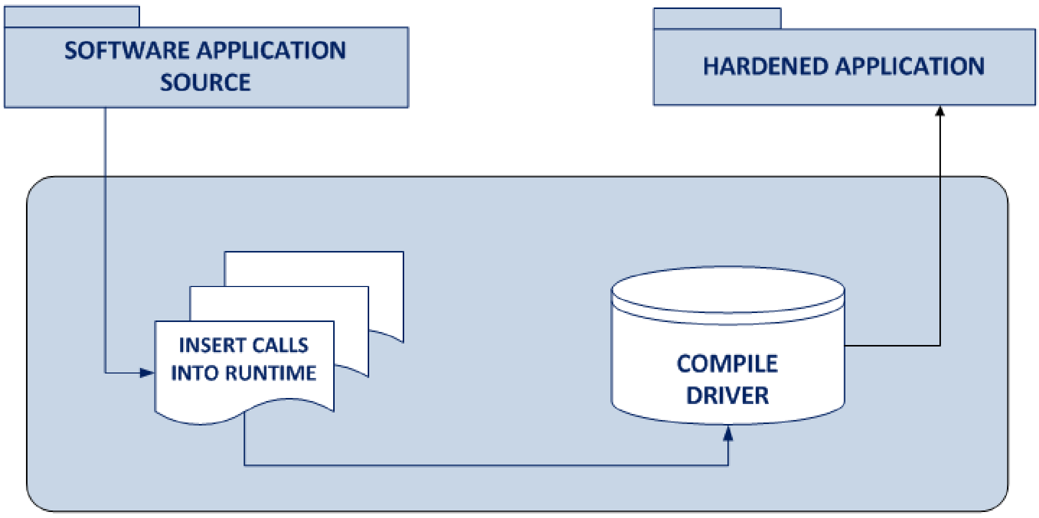

Figure 2: Application Software Encryption and Deployment

Deployment Process: The information bits that need to be secured, code or data, need to be downloaded from a server. A process on the server that implements the MFS technology will encode the bits in a machine specific form, build the necessary infrastructure to access the bits on the legitimate machine-user combination and download the data and infrastructure files to the client as shown in Figure 2.

Benefits of Multi Factor Security Technology:

Securing Applications: The software application author, developer identifies complete C functions which need to be securely executed. The author prepares a table of these functions that need to be securely executed in a XML file and places it on the server. The author will also use preamble code to call the function in the application. For example; instead of just calling a function with func(); the author will use AntargataDecryptRun(func, ...) with no further changes. Secure code execution for the selected code segments are handled automatically by the accompanying driver and library files.

The author places the application software binaries on the download servers owned and maintained by the author's organization or trusted entity that hosts the portal. These servers will also have the critical components of the MFS technology running on it. End users wishing to purchase and download the software title are expected to complete the business transaction to start the download of the application. At this point in time the server authenticates the client, generates a proprietary algorithm that is specific for that user-machine combination, encrypts the selected code segments of the binary with the new algorithm, generates a driver and a library file that is specific to the machine and creates an install module.

The end user installs the install module by accepting the download instructions. The installation process will install the application, the drivers and the library. When the application is run and the execution hits the encrypted portions of the executable, the driver and the library will initiate execution of the selected portion of the code securely and then hand over control back to the application. This mechanism as detailed in Figure 3 ensures application integrity, protection and prevention from malicious events.

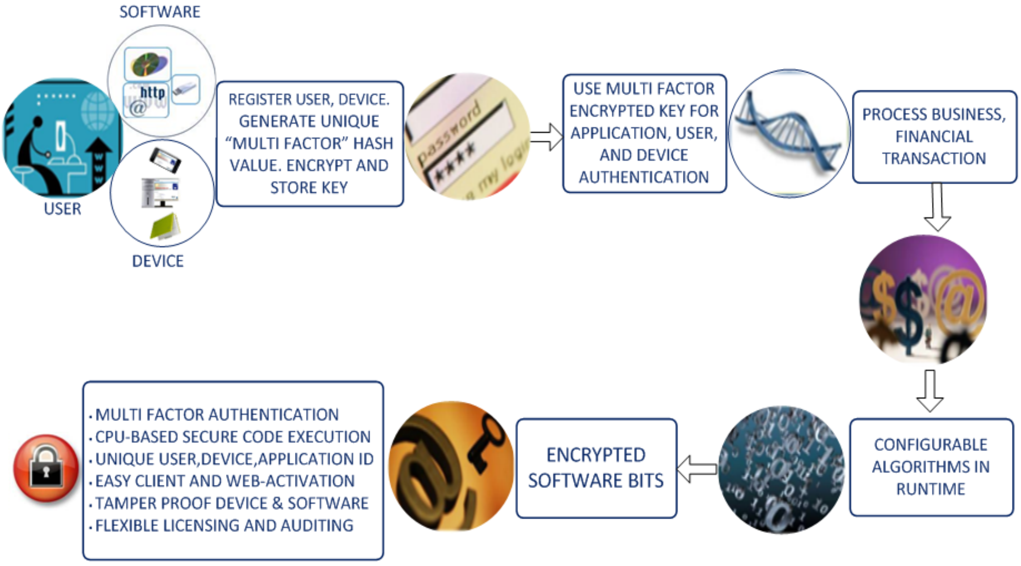
SOFTWARE
USER
DEVICE
REGISTER USER, DEVICE. GENERATE UNIQUE "MULTI FACTOR" HASH VALUE. ENCRYPT AND STORE KEY
USE MULTI FACTOR ENCRYPTED KEY FOR APPLICATION, USER, AND DEVICE AUTHENTICATION
PROCESS BUSINESS, FINANCIAL TRANSACTION
CONFIGURABLE ALGORITHMS IN RUNTIME
ENCRYPTED SOFTWARE BITS
· MULTI FACTOR AUTHENTICATION
· CPU-BASED SECURE CODE EXECUTION
· UNIQUE USER,DEVICE,APPLICATION ID
· EASY CLIENT AND WEB-ACTIVATION
· TAMPER PROOF DEVICE & SOFTWARE
· FLEXIBLE LICENSING AND AUDITING

Figure 3: One Click Encryption and Authentication

Securing Data: This section applies to any data that needs to be protected on a server, client, net top and smart devices. When the user downloads the data, the data is encrypted using the machine-user specific algorithm with the infrastructure files for accessing and processing the encrypted data. Applications that need to process data use the API exposed by the infrastructure files. Secure data exchange between two users is accomplished by the first user sending the data to a trusted server and the second user downloading the data from the trusted server eliminating the need for complicated key exchange protocols. This ensures data encryption simplicity, lowers encryption cost per bit by a significant margin and limits data loss and device tampering.

Securing System Software: Critical sections of firmware, operating system, anti-malware software, virtualization layers such as entire hypervisors can now be secured and protected against malicious attacks. Furthermore, relevant sections such as jump tables can be encrypted using this technology to prevent key logging, root kit attacks since encrypted sections now present a barrier to be "hooked" by root kits.

Securing Cloud Computing and SaaS Environments: Server farms implementing a cloud computing framework typically have several physical servers with local and global storage. The key advantage of cloud computing comes from the fact that physical servers can be dynamically allocated to a particular application and virtualized. This gives rise to the situation wherein processes belonging to several applications, user, device, might reside physically on the same machine creating risks of data leakage between applications. Applications and data can be encrypted in an application specific form preventing data leakage between processes. Employing the encrypted MFS hash value to include CA digital keys enhances use models wherein users are securely streamed applications, data based on policies and profiles setup by IT administrators anywhere, anyplace and anytime.

Identity and Access Management: Our approach can also be used for securely and reliably identifying a machine-user combination[4]. Since the algorithms for each machine-user pair is unique, encrypting an arbitrary piece of data (a challenge or a PIN) will always give rise to a unique encrypted string of bits. This unique string can be used for securely identifying the user-machine pair. More importantly, the derivation of the hash value prior to encryption ensures personal user information is not stored thereby delivering a powerful solution for protection against identity theft and fraud. This application of MFS technology is particularly useful in financial, SaaS and e-Gov services where identifying the end machine-user pair for delivering secure and reliable services or performing transactions is of paramount importance.

Practical Applications for Personal, Enterprise and Cloud Information Security

Healthcare

A recent report4[5] cited 80% of healthcare organizations experience lost and stolen information. Patient personal information and medical data breaches cost patients, providers and payors alike. A recent case involving the loss of a medical worker's laptop impacted hundreds of patients by compromising personal and medical information contained in records on the laptop. Another case involved unauthorized individuals to access patient records at a large hospital. In another significant case, hundreds of patient's personal information was stolen using peripheral devices, transferred over the network by unauthorized hospital staff systematically over a period of time. Additionally, as Internet usage in the healthcare world continues to evolve, emerging technologies like cloud computing along with the rapid surge in use of smart devices a comprehensive MFS solution helps protect health information.

The MFS approach has a proven[6] simple, easy to implement software solution that works on multiple devices and platforms to encrypt user ID, applications and data using a unique encryption algorithm that is specific to the user and device. Uniquely secures user IDs, device and data, enables seamless authentication and secure user access to health portals, avail of value-add services with PCI secure payment and protect health record information. With medical tourism on the rise, secure health record portability is ensured for payors thereby providing clinicians secure patient data access remotely, in office or on hospital premises for improved patient outcomes.

Finance and Banking

As more consumers prefer online and mobile financial services for shopping, bill payments and loans; fraud and identity theft has doubled. There was an overall increase in card fraud losses of 14% in 2008, but a more shocking 132% increase in online banking fraud[7] (*Apacs.) Varying regulations require non-uniform means of authentication and security standards for compliance to effectively protect consumers that add to banking and infrastructure implementation costs.

Cumbersome user experience is thereby dulling demand for value-add services. The MFS software computing framework is built to execute unique, comprehensive security functions that are software, user and device platform specific for end-to-end data encryption. The simple software solution provides significant cost savings, better user ID, device software and data protection compared with existing silo, multi click, two-factor authentication and “Chip and PIN” solutions. Co-exists with standard financial transaction protocols with zero changes to current financial transaction processing infrastructure in place. When implemented, provides a seamless and transparent user experience which encourages users to embrace new value added service offerings. This approach now has the capability to prevent identity theft, control fraud, protect financial data with improved user experience.

Conclusions: Our secure code execution and data security approach and method using CPU micro-arch constructs’ and re-configurable algorithms are an elegant and robust solution for multi factor security on general purpose x86 and ARM based platforms. The CPU overhead for typical applications are in the low single percentage points within the realm of measurement errors. Fundamentally, the MFS technology secures information bits, code or data on general purpose computing platforms. Any application which needs their bits to be secured is a good candidate for application of this technology. The applications mentioned in the previous sections are only a small example of the applications that are potentially possible.

Future work: Design of classes of reconfigurable algorithms, identifying peculiar machine signatures that are not limited toID's and porting the technology to other processor architectures are some of the research areas that are being actively looked at by the researchers in the company.

References:

1. http://www.trustedcomputinggroup.org/
2. http://www.intel.com/technology/security/
3. http://www.arm.com/products/security/trustzone/index.html
4. IEEE Communications, (Sept. 1994) B. C. Neuman and T. Ts'o. Kerberos: An authentication service for computer networks.
5. The Ponemon Report (Oct. 2009) Electronic Health Information at Risk: A Study of IT Practitioners.
6. Aventyn (Oct 2009) Secure eHealth Software with healthKrypt to Prevent Vulnerabilities That Expose User Information and Health Data.
7. UK Payments Association (Mar. 2009) APACS Fraud Report.

Author(s) Bio:

Navin Govind has developed winning global strategies for the adoption of new technology, architecture and products. As founder, CEO of Aventyn, he implemented unique Health IT interoperability and security technologies. As founding team member at Tarari, Navin managed the industry's first hardware XML Content Processor product developed for enterprises to secure and accelerate enterprise applications. At Intel, Navin held group and business unit positions, managed technical teams within Intel Labs responsible for wireless architecture, software development, 3D graphics, embedded products and development platforms. Navin has served as advisor at numerous industry panels, standards initiatives with several domestic and international publications.

Bhaktha Ram Keshavachar is a seasoned senior technical leader with extensive breadth of experience working in the computer and communications industry for 15+ years at BPL-India, SHARP and Intel. Most recently at Intel, Bhaktha extensively worked on CPU micro-architecture modelling and defined next generation processor cores. He has served as advisor and CTO at Aventyn, has several industry publications and patents awarded to his credit.