Multi Factor Secure Software Solutions

SECURE SOFTWARE COMPUTING

The global software industry had over $53 billion revenue "loss" due to packaged software vulnerabilities. In addition, software insecurities exposed through malware, identity theft, device and data loss add to the billions in direct and indirect revenue loss to enterprises and individual users.

Furthermore, rapid trends on application streaming in Cloud Computing, SaaS, VM, Web 2.0+ platforms challenge security, IP protection, device level user and data security. Now, users desire "multi factor" levels of software security to protect devices, data and personal information from software vulnerabilities.

An approach that hardens software using specific devices is a requirement.

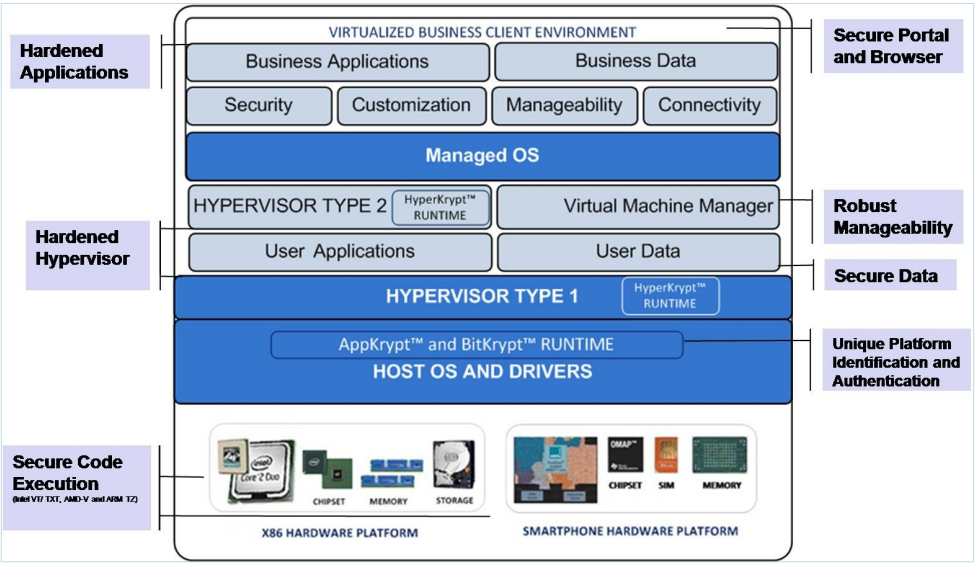
Our patent pending "Multi Factor" secure software computing framework is built to execute security related functions in a processor using known architectural constructs with minimal performance impact. Our custom security algorithms are software, user and device platform specific that prevent class break scenarios. The resulting solution is a lightweight "driver" with defined API(s) for securely executing code and retrieving secure data on existing standard hardware and software platforms. Specific software is further hardened using CPU hardware security hooks such as *Intel AMT/VT/TXT, AMD-V and ARM TZ.

Solution

Our **appKrypt™**, **bitKrypt™** and **hyperKrypt™** products secure applications, system software, hypervisors, device, data and portals with secure code execution, event tracking, identity and multi factor authentication using a secure hash of customizable ID's.

Benefits

- **Unique Identification and Authentication**
- **Harden Against Malicious Attacks**
- **Secure User, Device Centric Data Rights**
- **Tamper Resistant Copy Protection**



appKrypt™ Secure Application Code Execution using "Multi Factor" secure software computing

bitKrypt™ Secure User Device and Data Rights Protection with "Multi Factor" authentication

hyperKrypt™ Secure Hypervisor, Virtual Machine and application container protection

CPU-based Secure Code Execution Provides Unique Software Protection

Secures Users, Devices and Software

Tamper Resistant Device Centric Data Rights

Improved Licensing and Auditing Policies

Protect and Increase Revenue Streams

Evaluate Now!

Contact Us:
support@antargata.com

Works On

CPU: X86 Single-core, Multi-core and ARM
OS: Windows, Linux, Mac OS X and Android
VM: Citrix

Antargata Pvt. Ltd.

No. 98/1, 7th Cross Road, Domlur
Bangalore 560 071
India

URL: http://www.antargata.com
E-mail: info@antargata.com

Finance and Banking

ENTERPRISE APPLICATION

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 (*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.

Prevent Identity Theft, Control Fraud, Protect Financial Data For Improved User Experience.

Our patent pending "Multi Factor Security" 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.

Benefits

Bit-Level Software Encryption Reduces Payment Acceptance Infrastructure and Card Issuer Costs

Conforms to Standards and Data Transmission Protocols across Multiple Devices and Platforms

Unique ID with "Multi Factor Security" Algorithm Safeguards Card, Merchant and Bank Data

Eliminates Banking Software and Intellectual Property Theft

Healthcare

Patient personal information and medical data breaches cost patients, providers and payors alike. A recent case involving the loss of a medical worker laptop impacted hundreds of patients by compromising personal and medical information contained in records on the laptop. Another case involved access by unauthorized clinicians to patient records at a large hospital. In another significant case, hundreds of patients personal information was transferred over the network and stolen using peripheral devices by hospital workers systematically over a period of time. Additionally, as Internet usage in the healthcare world continues to evolve, cloud computing along with the rapid surge in use of smart devices there is need of a comprehensive security solution to protect health information. More importantly, ensuring HIPAA and health standards compliancy is mandatory with proposed changes in the HITECH act.

Secure eHealth Software, Prevent Vulnerabilities That Expose Applications, User information and Health Data to Malicious Uses.

The simple software solution easily 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 securing IDs, device and data enables seamless authentication and secure user access to health portals, avail of value-add services with secure payment and protect health record information. With medical tourism on the rise health record portability can be ensured so that primary physicians can securely access patient data remotely, in office or on hospital premises for improved patient outcomes.

Benefits

Secure User, Device Centric Data Rights that Enables Tamper Resistant Device and Data

Harden ehealth Software and Services with Unique Identification and Authentication Management

Prevents Unauthorized Access to Data, Seamless Transport Authenticated User Data Only on Authorized Devices

Unique Encryption For Each User, Device and Services Combination Ensures Compromising One Device Does Not Break Network or System

FOR MORE INFORMATION CONTACT US: INFO@ANTARGATA.COM