VeroGuard Systems

VeroMod IoT Industry Applications

Protect your devices and data at the network edge.
Lock out hackers.
Confidently move to Industry 4.0.

The Problem

The security of IoT devices has recently been shown to be less than adequate. With devices being easily hijacked a remote hacker can take control, view device data streams, and in some cases gain access to private networks and exfiltrate sensitive data. This has been made possible, as IoT device manufacturers have not been accustomed to working in the hostile and security conscious environment of the internet, leaving a large proportion of IoT devices simply not being designed for these operating conditions.

The Solution

VeroMod is a secure embedded HSM level Digital ID and encryption to ensure IoT devices are irrefutably identified, and device to base communications are securely encrypted.

Embedded or connected in-line the VeroMod handles the processing load for cryptographic calculations meaning the IoT devices are not impacted by the security overhead.

IoT Industry Strategic Need and Issues

The Internet of Things (IoT) refers to the growing billions of connected devices measuring, monitoring, collecting and sharing information, images and data without the need for human interaction. Enabling these otherwise dumb devices to be widely connected and automatically communicate has created extraordinary utility, which has seen the exponential growth in the breadth of use and number of connected devices.

IoT security has recently been shown to be less than adequate with devices being easily hijacked, enabling a remote hacker to take control of the device, view device data streams and in some cases gain access to private networks. This is possible because device manufacturers have not been accustomed to working in the hostile and security conscious environment of the internet, leaving a large proportion of IoT devices exposed and which were not designed for these operating conditions. Even with widely publicised IoT security breaches such as the hacking of coffee machines bringing down industrial plants, large numbers of new devices being deployed are providing malicious actors with innumerable new attack vectors daily.

This is not surprising, IoT hacking has been very effective to date. Hackers were able to exploit thousands (potentially millions) of unsecure connected devices to create a huge botnet, which unleashed the biggest DDoS attack to date (the Mirai botnet attack brought down the likes of Twitter, Reddit, Netflix and CNN). While this hack used exploited devices to attack external networks, an exploited device could easily be used as a gateway to look for deeper levels of a network to seek out and exfiltrate sensitive and valuable private data.

Forbes predicts by 2025, there will be over 80 billion smart devices on the internet and most of the embedded firmware being unsecured and highly vulnerable, which potentially exposes an innumerate number of critical systems and private data sources. It is for this reason a recent Bain and Co report suggests that enterprise customers would buy 70 percent more IoT devices if they had better security. Nearly all respondents would be prepared to pay 22% more for the comfort of a higher level of security.

For the IoT industry to meet these huge growth predictions, an investment in strong cybersecurity practice and solutions will be required before businesses will be confident enough to widely deploy these devices.

A Security Layer for IoT

VeroGuard's globally innovative shared digital infrastructure can provide the security posture required by the IoT Industry and provide a response to the barriers faced by organisations looking to secure an existing fleet of devices. VeroGuard's solution will enable device manufacturers to immediately lift their security profile without the need to retrofit security architecture into low power devices.

VeroGuard protects machine communications via black box[1] to black box security. All services are provisioned from the platform removing the need to source security expertise. This solution covers machine and human identity, removing duplicated investment and complexity.

Build a Trusted Device Ecosystem via:

- Provision of an HSM[2] based secure access platform for all your devices;
- Provision of a universal, unified HSM based Digital Identity to irrefutably identify the machine
- Provision of bank to bank level encryption of data between end points.
- Provision of communications tamper detection for machines

[1] "Black box" security refers to devices which contain Hardware Security Modules (HSM's) and encrypt communications based on processes where the security keys are maintained within hardware that safeguards and manages digital keys for strong authentication.

[2] Hardware Security Module

Solution Overview Use Cases

Use Case: Physical Security of Facilities

VeroGuard's technology can be applied to physical security applications such as site access and machine to machine communications (IoT). VeroGuard is a single platform that guarantees identity of humans and machines to ensure communications can only take place by verified actors, improving and extending the closed-circuit nature of private networks. Providing bank to bank/military grade security for every device prevents cybercriminal acts via a non-reputable, out of band, multi factor means of authentication and encrypted communications.

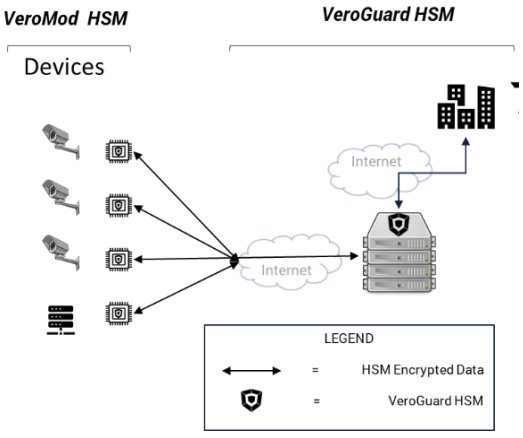
IoT security has recently been shown to be less than adequate with devices being easily hijacked enabling a remote hacker to take control of the device, view device data streams, and in some cases gain access to private networks and exfiltrate sensitive data. This has been made possible, because the device manufacturers are not accustomed to working in the hostile and security conscious environment of the internet, leaving a large proportion of IoT devices simply not designed for these operating conditions.

What's the Risk?

A subset of IoT devices are Video Surveillance Systems (VSS) which are renowned for having little or insufficient security to protect devices and data for increasingly sophisticated cybercrime. Current methods of protection and encryption are being breached and will not protect your environment, networks or data from cybercrime, as the intrusion will be assumed to be authentic when the cybercriminal hijacks, steals or emulates the tokens, taking control of cameras, networks, servers and/or associated data.

The solution

IoT VSS: VeroMod (HSM level embedded Digital ID and encryption) is a secure digital identity that can be embedded into IoT connectivity to irrefutably identify the device and provide encryption for the data. VeroGuard provides HSM to HSM level authentication and switching services, managing the verification of identity, multi-factor authentication and secure VPN for device to base communications.



Video Surveillance Systems

1. VeroMod integrated into devices
2. VeroMod integrated into VSS control server
3. VeroGuard provides HSM to HSM authentication and verification of device identity
4. VeroMod handles the processing load for cryptographic calculations
5. Can be used to secure any device type

Use Case: Security of IoT Data

IoT security has recently been shown to be less than adequate with devices being easily hijacked enabling a remote hacker to take control of the device, view device data streams, and in some cases gain access to private networks and exfiltrate sensitive data. This is possible because device manufacturers have not been accustomed to working in the hostile and security conscious environment of the internet, leaving a large proportion of IoT devices simply not designed for these operating conditions.

VeroGuard's technology can be applied to machine to machine communications (IoT) ensuring data transmitted to central systems is encrypted and stored securely. VeroGuard is a single platform that guarantees identity of machines and humans to ensure communications can only take place by verified actors, improving and extending the closed-circuit nature of private networks, and enabling ultra-secure connectivity over public networks. Providing bank to bank/military grade security for every IoT device prevents cybercriminal acts via a non-repudiable, out of band, multi factor means of authentication and encrypted communications.

What's the Risk?

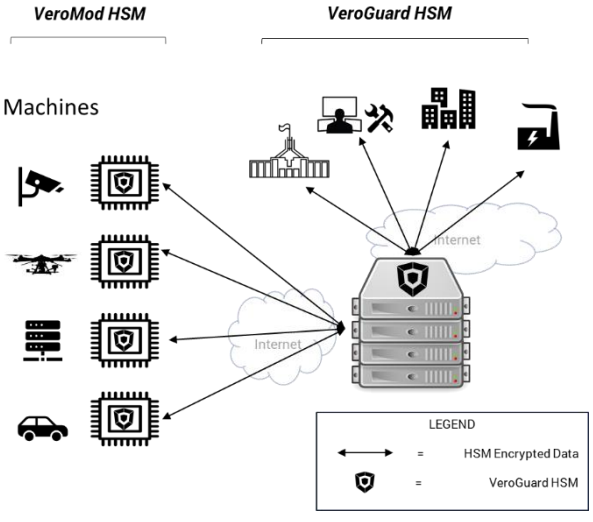
Where IoT is used for monitoring, the data collected by devices can appear to be of little value to a hacker. For example, if that data is related to power consumption at a manufacturing plant this information could be related to production volumes and the information may be of value to a competitor.

Data exfiltration is one aspect of risk, another is industrial sabotage. When IoT is utilized in the production process, for example monitoring temperature, devices could be compromised and recalibrated to deliberately introduce defects or quality control issues.

IoT devices are renowned for having insufficient security to protect devices and data for increasingly sophisticated cybercrime. Current methods of protection and encryption are being breached and will not protect your environment, networks or data from cybercrime, as the intrusion will be assumed to be authentic when the cybercriminal hijacks, steals

The solution

VeroMod (HSM level embedded Digital ID and encryption) is a secure digital identity that can be embedded into IoT connectivity to irrefutably identify the device and provide encryption for the data. VeroGuard provides HSM to HSM level authentication and switching services, managing the verification of identity, multi-factor authentication and secure VPN for device to base communications.



IoT

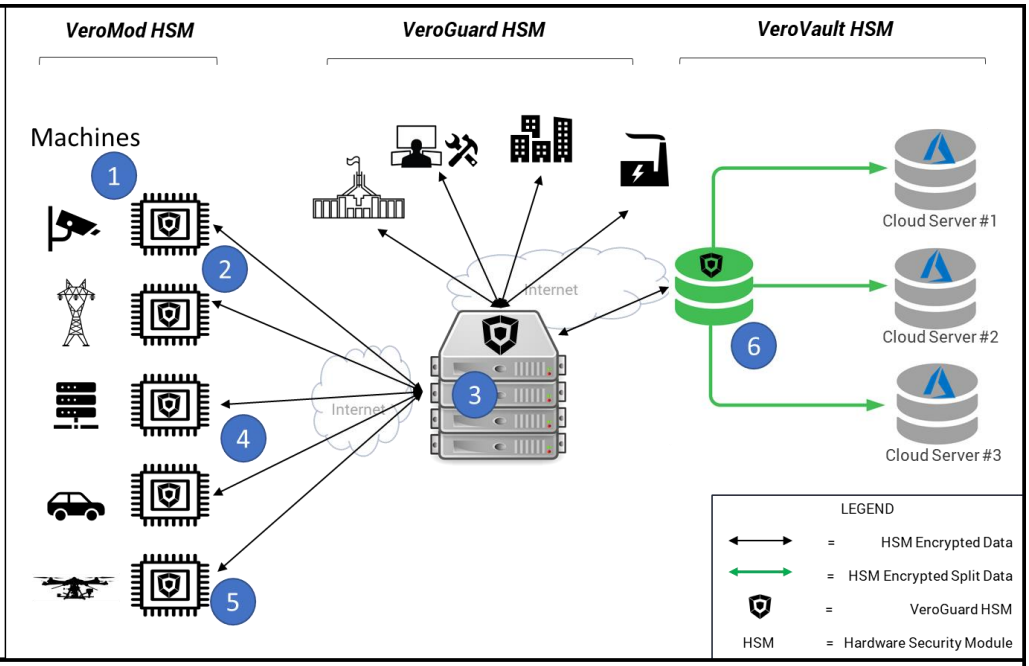
6. VeroMod integrated into devices
7. VeroMod integrated into IoT central server
8. VeroGuard provides HSM to HSM authentication and verification of device identity
9. VeroMod handles the processing load for cryptographic calculations
10. Can be used to secure any device type

VeroGuard Schematic for Machine Identity

VeroGuard Systems

How Does VeroGuard Work?

1. VeroMod is integrated directly into the device or via RJS connection.
2. Machine requests connection and is verified with non-repudiable out of band and hardware encrypted multi factor authentication.
3. VeroGuard provides HSM to HSM authentication and verification of machine identity.
4. Encrypted tunnels are opened to connect machine to machine. All communications are AS 2805/ISO 8583 messaging.
5. VeroMod handles the processing load for cryptographic calculations – IoT machine is not impacted.
6. Data secured in the cloud at rest with hardware encrypted multi server packet splitting.



What makes VeroGuard so secure?

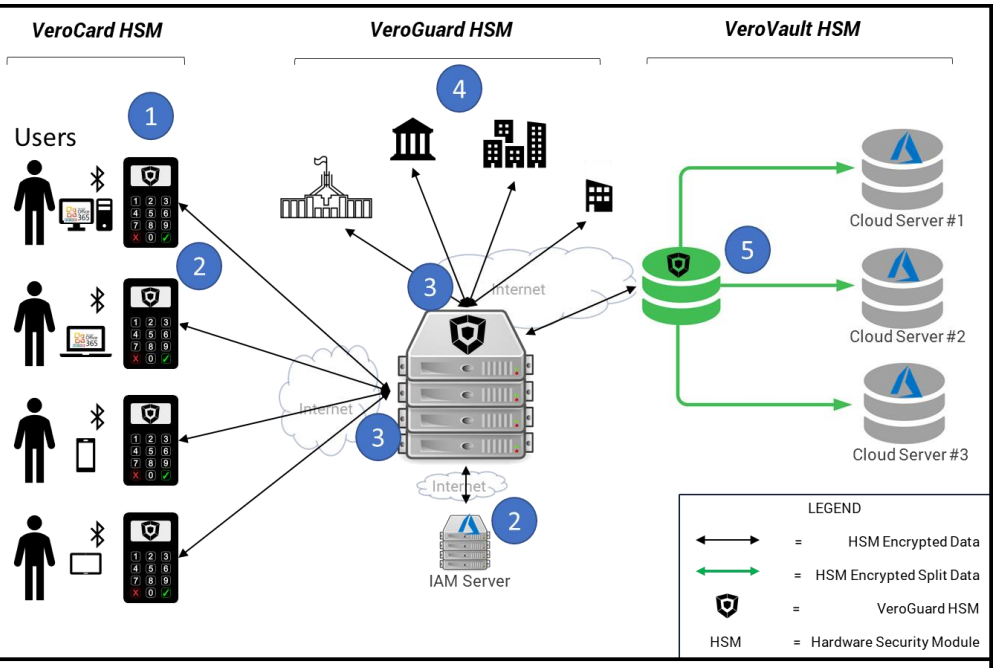
1. No user authentication information exposed
2. Derived Unique Key Per Transaction (DUKPT) Key Management Scheme
   - Every device has a unique derived master key
   - Device key includes the Terminal ID
   - New key derived with every transaction
3. Devices are tamper proof and self destruct keys if tamper is detected
4. Scheme master key stored in the gateway HSM
5. No known source of encryption
6. Every communication is HSM to HSM with ISO 8583 messaging
7. Data split and encrypted at rest over multiple servers. Only accessed with authorised Card or Mod.

VeroGuard Schematic for Human Universal Unified Digital Identity. Secure Access to your IoT Ecosystem

VeroGuard Systems

How Does VeroGuard Work?

1. User requests access to application or data and is prompted to enter their PIN on the VeroCard connected to the device via Bluetooth.
2. User is verified (utilising permissions from IAM server) with non-repudiable out of band and hardware encrypted multi factor authentication.
3. Encrypted tunnels are opened to connect the users device with the authorised application. All communications are AS 2805/ISO 8583 messaging.
4. Shared applications (on premise/in cloud/as a service or hybrid) are host connected to VeroGuard HSM via hardware encrypted tunnels.
5. Data secured in the cloud at rest with hardware encrypted multi server packet splitting.



What makes VeroGuard so secure?

1. No user authentication information exposed
2. Derived Unique Key Per Transaction (DUKPT) Key Management Scheme
   - Every device has a unique derived master key
   - Device key includes the Terminal ID
   - New key derived with every transaction
3. Devices are tamper proof and self destruct keys if tamper is detected
4. Scheme master key stored in the gateway HSM
5. No known source of encryption
6. Every communication is HSM to HSM with ISO 8583 messaging
7. Data split and encrypted at rest over multiple servers. Only accessed with authorised Card or Mod.

What has VeroGuard Systems Developed?

VeroGuard has developed a solution to the problem of not knowing who or what is at the other end of an online transaction, and therefore the authenticity of the interrogation, communication and associated data. VeroGuard provides this surety via a non-repudiable Digital ID and authentication platform, capable of irrefutably identifying humans or machines – making it applicable to any online interaction. VeroGuard combines this non-repudiable ID with hardware encrypted protection for data in transit and at rest in the cloud.

VeroGuard provides a single gesture, out of band, multi-factor authentication solution based on existing proven bank to bank protocols applied as a first of its kind to the cloud, and can provide hardware encrypted and verified security access across platforms regardless of device, network or location.

VeroGuard's system can provide the necessary infrastructure to extend protection to any organisation, secure communication between parties, create a trusted environment and to reduce incidence of attacks based on identity or credential loss.

The VeroGuard solution has three main elements:

1. Portable **non-repudiable Digital Identity that is unified, universal and irrefutable**. A single platform that authenticates people and/or machines over the internet using ATM authentication and bank to bank level communications.
2. **Ultra-secure cloud communications** combined with simple API's to enable hyper convergence for online services.
3. **Ultra-secure storage**. VeroGuard has partnered with Data61 (CSIRO) to also secure data at rest in the cloud, to take cloud data protection to above protected levels leveraging a multi-server splitter and the non-repudiable identity of the actors.

How does VeroGuard address Cyber Security issues?

Solution	Benefit	Issues Addressed	Online & IoT Security
Portable non-repudiable Digital Identity	A single platform providing Unified, Universal and Irrefutable Identification	**Prevention** Bad Actors cannot access devices **Universal** Identity unified at the device – not the system, enabling wider integration	Guarantees identity of persons authenticating to an application, or machines on your network with bank to bank level security
Ultra-secure cloud communications	Simple API's to enable integration of any online service	Enables hyper convergence for online services, as the identity layer is already catered for	Guarantees data transmission is secure and ensures communications can only take place by verified actors
Ultra-secure storage	Lifts cloud data protection to a completely new level (above protected)	Data at rest is not subject to being accessed by a single attack	Files are split across multiple storage solutions and each component is encrypted, meaning multiple successful attacks would need to be accomplished

What are the components of the VeroGuard Solution?

VeroGuard is a unique technology that enables online authentication and encrypted transmission across fixed and mobile networks with same level of identity security as the ATM network. VeroGuard delivers non-repudiable secure open internet-based login which can be integrated into any environment. It has proven significant defensive security using multiple layers, including anchored ID and multi-factor authentication for best of breed digital identity verification, suitable for use by employees and clients.

The VeroGuard platform serves as a central exchange enabling authentication of users and devices online. Once authenticated ultra-secure communications and storage options can also be provided to create trusted member ecosystems, opening new possibilities for collaboration amongst members. The core components of the solution are:

VeroGuard: The central platform providing HSM to HSM level authentication, interoperability and switching services, managing the verification of identity, multi-factor authentication and secure VPN to secure shared services such as cloud storage and email. VeroGuard can protect machines and users equally on a single platform providing a solution to protect IoT or machine-to-machine interfaces, protecting and verifying end points, applications, communications and data with hardware encryption and encrypted packet splitting.

VeroMod: HSM level embedded Digital ID and encryption for Machine to Machine interfaces. It is a secure digital identity that can be embedded into IoT connectivity to irrefutably identify the device and provide encryption for the data. VeroMod can be embedded into devices or connected in-line and in conjunction with VeroGuard which provides HSM to HSM authentication and verification of device identity. The VeroMod can be used to secure any type of device and handles the processing load for cryptographic calculations meaning the IoT devices are not impacted by the security workload.

VeroCard: An HSM level Digital Wallet for users to manage secure identity access, authentication and transmission. This card is tamper-proof and designed to connect to Bluetooth devices on any operating system. If lost, the card has no accessible data contained and can be remotely disabled.

The VeroCard has been developed to be the ultimate in personal security of the most precious personal details as well as protection of all online activity. VeroCard is the personal hardware that enables the VeroGuard system, providing personal ID security and privacy control, it is a credit card sized tamper proof “Black Box”3 Bluetooth device. VeroCard provides an easy and secure point of entry for all sensitive information protected with a PIN.

VeroCard enables the user to access websites, applications, cloud storage or payment systems through a secure server, with real-time authentication back to the VeroCard that the user holds in their hand.

VeroVault is a secure cloud and email service which can be connected to a range of cloud providers, delivering HSM to HSM level secure access and data secured in the cloud at rest with hardware encrypted multi server packet splitting with storage able to be across providers.

VeroCard

[3]“Black box” security refers to devices which contain Hardware Security Modules (HSM) and encrypt communications based on processes where the security keys are maintained within hardware that safeguards and manages digital keys for strong authentication.

VeroGuard Schematic How does VeroGuard address Cyber Security issues?

Feature	Benefit	Description
Hardware Encryption	Private keys and are never exposed to software where they can be harvested or broken by malware or applications.	HSM to HSM encryption for communications based on processes where the security keys are maintained within hardware that safeguards and manages digital keys for strong authentication. This methodology means that the encryption can't be broken or associated if intercepted. Devices are tamper-resistanrt and provide out of band multifactor authentication with a single gesture.
Hardware Token with Single Gesture, Multifactor, Out-of Band Authentication	Provides a separate layer of security for the strongest possible authentication. The VeroCard provides this solution seamlessly for each login with the user only required to enter their PIN. Uses a single unique pin. Can't be skimmed, can't be tampered with. Locks out anyone who doesn't know the pin.	Out-of-band refers to authentication that requires a verification method through a separate channel.
Portable	Can be used to authenticate access to any online system or encrypt communications end to end between devices.	VeroGuard is a single platform that authenticates people and machines over the internet using bank to bank level security. An ID is anchored to the user and verified on a separate identity solution, enabling the Digital ID to be re-used for any system you wish to bring online, or keep terrestrial.
Ultra-Security	No meaningful data is associated with identity captured or sent, and there is NO KNOWN SOURCE OF THE KEYS.	Keys are stored in Hardware Security Modules (HSM) and never exposed to software, providing ATM like authentication which cannot be broken or associated if intercepted. New key pairs can be exchanged with EVERY transaction..
Flexibility / Interoperability	Any OS, any device, any system	VeroGuard is agnostic to operating system and device types allowing enabled devices and associated servers the ability to participate without significant changes to applications.
Identity Guarantee:	Know who is at the 'other end'	VeroGuard uses a non-repudiable, out of band, multi factor means of authentication which can be applied to both machines and humans and makes every authentication verified.
Information protection:	Ultra-Secure encrypted tunnels and cloud storage	VeroGuard can provide an encrypted tunnel for communications irrelevant of the carriage. VeroGuard provides the most secure, unbreakable cloud storage solution available but able to be applied to existing services.
Low Cost	Low cost solution, and can remove the need for other identity solution and integrations	
Scalable	A single Digital ID is reusable across any online platform.	
Reduces Complexity	Removes the complexity of building security into digital platforms	

VeroGuard Systems Pty Ltd
ABN 25 617 573 001

P / +61 (03) 9558 3090
admin@veroguard.com.au

veroguard.com.au