Intel Subsidiary Agrees to $750,000 Penalty for Unauthorized Encryption Exports

| Print |

FOR IMMEDIATE RELEASE

Wednesday, October 8, 2014

www.bis.doc.gov

BUREAU OF INDUSTRY AND SECURITY

Office of Congressional and Public Affairs

202-482-2721

Intel Subsidiary Agrees to $750,000 Penalty for Unauthorized Encryption Exports

WASHINGTON – The U.S. Department of Commerce's Bureau of Industry and Security (BIS) today announced that Wind River Systems of Alameda, Calif., a wholly-owned subsidiary of Intel Corporation, has agreed to a $750,000 civil penalty to settle charges that it sold encryption software products to foreign government customers and to organizations identified on the BIS Entity List without the required Department of Commerce licenses.

In April 2012, Wind River Systems voluntarily disclosed to BIS that between 2008 and 2011 the company made 55 exports of operating software valued at $2.9 million to governments and various end users in China, Hong Kong, Russia, Israel, South Africa, and South Korea. The operating software is controlled under Export Administration Regulations for national security reasons, and some of the export recipients in China are on the BIS Entity List.

"I approved penalties in this case because the violations were ongoing over a period of several years," said Assistant Secretary of Commerce for Enforcement, David W. Mills. "Because the violations were voluntarily disclosed, the company received significant mitigation. This penalty should serve as a reminder to companies of their responsibility to know their customers and, when using license exceptions, to ensure their customers are eligible recipients.

BIS controls exports and reexports of commodities, technology, and software to support national security and foreign policy, including nuclear, chemical and biological weapons, and missile non-proliferation, human rights, regional stability, and curbing terrorism. Criminal penalties and administrative sanctions can be imposed for violations of the Export Administration Regulations. For more information, please visit **www.bis.doc.gov**.

WIND RIVER

Wind River VxWorks Platforms 6.9

Table of Contents

The market for secure, intelligent, connected devices is constantly expanding. Embedded devices are becoming more complex to meet market demands. Internet connectivity allows new levels of remote management but also calls for increased levels of security.

More powerful processors are being considered to drive intelligence and higher functionality into devices. Because real-time and performance requirements are non-negotiable, manufacturers are cautious about incorporating new technologies into proven systems. To succeed, companies must optimize their device software across the entire product life cycle: from design through development, from QA to the remote management of deployed devices. The challenge for many device developers is in balancing the need for increased speed, greater efficiency, and lower cost with an acceptable level of development risk.

Wind River VxWorks platforms meet this challenge with an embedded platform solution that combines VxWorks 6.9, the industry's leading 32-bit and 64-bit capable real-time operating system (RTOS); Wind River Workbench, the premier device software development suite; and essential security, device management, and connectivity middleware, including drivers and protocols for connected devices on the factory floor, wireless peripherals, and other devices within the network infrastructure. The VxWorks platforms are backed by Wind River's 25 years of device software industry experience, a world-class support organization, a comprehensive partner ecosystem, and a specialized professional services team.

Wind River VxWorks platforms provide comprehensive multi-core processor support, including asymmetric

debugging support for processors with hardware breakpoint capability provide another way to track data values, by setting breakpoints that trigger on data accesses at a specified address.

Identifying the Best Functions to Speed Up

To increase performance by applying parallelism, begin with the parts of your program that consume the most CPU cycles. The Wind River development environment for VxWorks and Linux provides several ways to collect this information. The VxWorks Spy() capability and the top command available in a Linux environment provide one alternative. Wind River Performance Profiler (formerly ProfileScope) and System Viewer make it easy to identify which functions in an application are consuming the most CPU cycles. In an SMP system, additional threading will help to increase system performance. In an AMP system, these are the functions that may benefit from decomposition or reassignment to a processor with a lighter load.

Uncovering Shared Resource Contention

The rich data collection capabilities of Wind River System Viewer can be used to log information that can later be analyzed to expose a range of resource contention–related issues.

Tracking Inter-processor Communication and Synchronization

In multiprocessor systems, the interaction of processors is at least as important as what happens on any single processor. Spinlocks are commonly used to provide synchronization in multi-core systems. Spinlocks are supported with VxWorks SMP, and spinlock activity is trackable in System Viewer visualization. System Viewer instrumentation of TIPC messages also provides insight into the interaction between processors.

Displaying Static or Dynamic Routing of Interrupts to Processors

The assignment of hardware resources, including interrupts, to specific processors is an important multi-core design decision. The ability to query the state of VxWorks kernel objects allows developers to see how interrupts are assigned to processors. This will apply to static and dynamic assignment.

Middleware Technology

Security

Wind River IPsec and IKE

Wind River IPsec is a scalable implementation of IPsec, as specified by the IETF. It provides authentication, data integrity, encryption, and replay protection of any network traffic on the IP layer. It is implemented as a tightly integrated software module for Wind River Network Stack, for both IPv4 and IPv6 operations. Wind River IPsec is interoperable with other IPsec implementations and conforms to the IPsec RFCs, as specified by the IETF.

Features of Wind River IPsec 6.9 include the following:

- 64-bit support
- Updates to the PF_Key v2 management interface
- New keyadm commands and options
- RFC 4301, 4308, 4835, and others
- Support for IP forwarding with IPsec on Cavium Networks CN38xx and CNN58xx processors
- Support for IPsec ESP cryptographic offload to Cavium Networks CN38xx and CN58xx processors
- Addition of new commands and parameters as well as changes to existing keyadm shell commands
- Tunnel and transport mode in any security association (SA) combination
- Support for AH and ESP modes
- IP in IP tunneling
- Bypass/apply/discard IP packet filtering with both input and output selectors
- Support for IPsec monitoring MIB
- Key and SA management with PF_Key Management API v2 with openbsd extension
- Support for all required authentication transforms and encryption algorithms
- Validated with Common Cryptography Interface (CCI)
- Extended Sequence Number (ESN) Addendum to IPsec
- Integrated and validated with optional security coprocessors, demonstrating significant performance improvement over software processing
- VPN-A and VPN-B suites
- Traffic flow confidentiality (TFC)
- IPsec offloading with SMP systems
- Support for FIPS 140-2 mode

Wind River IKE is a scalable implementation of IKE versions 1 and 2, as specified by the IETF, and it provides for secure key exchange for IPsec.

Features of Wind River IKE 6.9 include the following:

- Support for IKE v1 and IKE v2
- Support for address and port ranges in the IPsec SA configuration (IKEv2 only)
- Support for listening on any address (0.0.0.0 for IPv4, or :: for IPv6)
- Support of Online Certificate Status Protocol (OCSP) extensions to IKEv2, as defined in RFC 4806
- Ability for IKEv1 and IKEv2 to verify the validity of a given certificate against a certification revocation list issued by an appropriate certificate authority
- IKE v1 support of accepting both ESP and AH negotiation in the same proposal for a given IPsec flow configuration, required for interoperability with Windows Vista and Windows Server equivalents, which allow such policy specifications
- NAT traversal of ESP packets over UDP
- Integration with Wind River Network Stack
- Authentication based on X.509 certificates and preshared secrets (passwords)
- Passive and active establishment of IPsec connections
- Secure, interoperable communication with other IPsec endpoints
- Plug-and-play integration with Wind River IPsec
- VPNC certification for Basic, AES, IKE v2, IPv6, and certificate interoperability
- Support for FIPS 140-2 mode
- IKE SA rekeying
- 64-bit support
- Support for Section 2.24: Explicit Congestion Notification (ECN) of RFC 4306 Internet Key Exchange (IKEv2) Protocol
- Support of RFC 4718 IKEv2 Clarifications and Implementation Guidelines
- Support for secure key storage
- Enhanced dead peer detection (DPD)
- Enhanced IKE daemon to renegotiate proposals in the IKE stack if the first specified group is not accepted
- ipike_identification-extract( ) routine optimized to avoid unnecessary malloc() calls to enhance memory usage
- Fetching certificates using HTTP
- Matched delete sequence during rekeying for IKEv1 and IKEv2

Wind River Wireless Security

Wind River Wireless Security is a suite of security protocols implemented by Wind River that includes a supplicant and authenticator for the 802.1X-2001 standard and Wi-Fi Protected Setup (WPS). The Wireless Security authenticator is integrated with the Wind River RADIUS and Diameter, Wind River Learning Bridge, and Wind River Wireless Ethernet Driver, providing all the core functionality for typical authenticator products, such as wireless access points. Both supplicant and authenticator can be used in the same product, allowing greater flexibility and a range of application support. Wind River Wireless Security works together with Wind River EAP that supports multiple Extensible Authentication Protocol (EAP) types. Integration with Wind River SNMP is included to interface with the 802.1X MIB.

Also part of Wind River Wireless Security is Wind River's implementation of WPS. WPS simplifies the setup and management of wireless networks by automating the configuration of access points and peripheral devices. Wind River Wireless Security comprises the following components:

- COMPONENT_DOT1X
- COMPONENT_8021X
- COMPONENT_WPS

Features of Wind River Wireless Security 6.9 include the following:

- Support of WPS for the enrollee, AP without registrar, and AP with registrar models
- Capabilities including 802.1X, Wi-Fi Protected Access (WPA and WPA2), 802.11i, Temporal Key Integrity Protocol (TKIP), AES, preshared keys
- EAP types and EAP type combinations added with use of new independent EAP module (IPEAP), allowing EAP to be used by other Wind River modules
- Full integration and testing with Wind River Wireless Ethernet Driver (station and access point modes), easily portable to other wireless driver solutions
- Support for both authenticator and supplicant modes
- Support for wide range of encryption and hashing algorithms
- Support for dot1xPaeConfigGroup supplicant MIB
- New commands to support run-time configuration of multiple port access entity (PAE) instances
- Support for the coexistence of WPS and 802.1X in a single image, allowing parameters to be supplied through WPS, followed by 802.1X authentication with an authentication server

Wind River EAP

Extensible Authentication Protocol (EAP) allows a client and a server to negotiate an authentication method and establish client and, optionally, server authentication. The protocol defines a packet structure that contains commands and attributes used by the client and server during an authentication session. A number of EAP types and EAP type combinations are available to implement an authentication method.

EAP is a separate module based on the IPCOM EAP (IPEAP). EAP is used by the Wind River Wireless Security supplicant to negotiate an authentication method.

EAP supports the WPS EAP method (EAP-WSC). EAP-WSC is used for registrar and enrollee discovery and for credential establishment in a WPS environment.

Wind River EAP 6.9 supports 64-bit operation. In addition, EAP includes VSB configuration enhancements, support for the use of the secure key database to store EAP passwords and private keys, and EAP Session-Id.

The following are the EAP types supported in Wind River EAP 6.9:

- EAP-AKA
- EAP-GTC
- EAP-LEAP
- EAP-MD5
- EAP MS-CHAPv2
- EAP-PEAPv0
- EAP-PEAPv1
- EAP-SIM
- EAP-TLS
- EAP-TTLS
- EAP-WSC

Wind River Firewall and NAT

Wind River Firewall supplies a powerful filtering engine that allows device manufacturers to optimize their software to provide advanced features that protect valuable data. This engine is ideally suited to a wide range of products, including SOHO routers, broadband access devices, and small to medium-size enterprise devices.

Features of Wind River Firewall 6.9 include the following:

- Ability to run on a 64-bit platform
- IP filtering with stateful inspection for IPv4 or IPv6 packets
- MAC (media access control) filtering
- Logging at the network (L3) and data link (L2) layers
- HTTP content filtering for URLs (both specific and by keyword), proxy traffic, Java applets, ActiveX controls, and cookies
- Nonvolatile (NV) storage of firewall rules
- Input and output filters
- Stateful inspection
- Rate limiting
- Filter on network interface
- Support for the pktflags keyword that's used to filter IPsec, NAT, and tunneled packets
- Rule grouping
- Simplified procedure for excluding Wind River Firewall from a VxWorks Image Project

Wind River NAT is a full-featured implementation of the industry-standard Network Address Translation Protocol (NATP) for use in routers, firewalls, DSL and cable modems, and residential gateways. A device running Wind River NAT can connect an entire department or a small office to the Internet using a single global IP address. Address mapping effectively conceals the size and topology of the private network from the outside, providing a basic level of security.

The chief advantage of NAT is that addresses on the private network are hidden from the public Internet, providing a measure of security. A second advantage, realized with certain varieties of NAT, is that scarce IP addresses are conserved, reducing network administration costs.

Wind River NAT supports the two most widely used NAT modes. Basic NAT performs one-to-one mapping of private IP addresses to a preallocated block of external IP addresses. The more commonly used NATP maps port numbers as well as IP addresses. NATP allows multiple private addresses (up to 64,000 address/port combinations) to be multiplexed on a single public address, offering the full benefit of address conservation and security.

NAT provides basic security by blocking all incoming connection requests that don't map to recognized address translations.

Wind River NAT supports the following features:

- Ability to run on a 64-bit platform
- Basic NAT
- Network Address Port Translation (NAPT)
- Bidirectional NAT
- Network Address Translation-Protocol Translation (NAT-PT)
- Demilitarized zone (DMZ) host
- Application-level gateways (ALGs)
- Port triggering
- Support for the Session Initiation Protocol (SIP) Application-Level Gateway (ALG), allowing simple SIP UDP sessions to pass through a NAT device

Wind River Cryptography Libraries

Wind River Cryptography Libraries 6.9 is an implementation of standard cryptographic algorithms and supporting utilities that can be used in developing secure applications. It is based on the cryptographic portions of the open source project OpenSSL. It is also used by other components requiring access to crypto functions. Wind River Cryptography Libraries can run on a 64-bit platform.

Wind River Cryptography Libraries includes the following:

- Software implementations of cryptographic algorithms
- An API for creating interfaces to hardware cryptographic devices for offload of computationally intensive cryptographic algorithms
- An implementation of a hardware interface for Freescale SEC devices
- An implementation of a cryptography offload engine that is supported and included for Cavium OCTEON CN38xx and CN58xx processors
- X.509 certificate support
- Support for AES key wrap and AES CMAC algorithms

Wind River Cryptography Libraries continues to provide support for the Federal Information Processing Standard (FIPS) 140-2. The set of available cipher suites is reduced when building VxWorks in FIPS 140-2 mode because some security algorithms are not FIPS-approved.

When VxWorks is compiled in FIPS mode, the affected algorithms are compiled out. The MD5 hash algorithm is not compiled out, but it is disabled in run-time if the system is running FIPS 140-2 mode. Since these algorithms are not FIPS-approved and are compiled out, it is not possible to select components that use them in your VSB when you enable the FIPS 140-2 option. Some components will not be possible to enable, for example, Mobile IP v4. This exception applies to specifications that mandate the use of non-FIPS-approved algorithms, such as MD5. There are also some modules that will simply compile out features that use non-FIPS-approved algorithms. For example, in TCP the MD5 checksum option will be compiled out. When FIPS mode is turned off, the MD5 hash is enabled.

Customers have the ability to build a non-FIPS image that includes all components and a FIPS image including the encryption library and SSL. In order to configure FIPS 140-2 mode, the VSB option needs to be enabled.

The following are included algorithms:

- AES
- Blowfish
- CAST
- DES
- RC2
- Arcfour
- RC5
- AES key wrap
- SHA-1
- MD2
- MD4
- MD5
- RIPEMD-160
- HMAC
- AES CMAC
- Diffie-Hellman
- DSA
- RSA

Wind River Security Libraries

Wind River Security Libraries continue to be deprecated. New development should use Wind River Cryptography Libraries, which provides enhanced functionality.

Starting with VxWorks 6.6, cryptographic services are provided by the Wind River Cryptography Libraries. Wind River Security Libraries is also included for backward-compatibility with prior versions of VxWorks. This includes a library of cryptographic algorithms, the common crypto interface (CCI), used by other components requiring access to crypto functions, and the crypto provider interface (CPI), which supplies a mechanism for developers to add other crypto libraries or hardware-based crypto functions.

Wind River SSL and SSH

Wind River SSL is a client server technology used to secure any higher layer protocol that uses sockets. A typical application is to secure HTTP connections (HTTPS) for e-commerce.

Security is provided by the following:

- Privacy, using data encryption
- Authentication, using digital certificates
- Message integrity, using message digests

Features of Wind River SSL 6.9 include the following:

- Support for FIPS 140-2 (the set of cipher suites is reduced when running SSL in FIPS 140-2 mode due to not all algorithms being FIPS approved; customers can only use cipher suites using AES, 3DES, and SHA1 when running in FIPS 140-2 mode)
- Operation in VxWorks 6.9 for both 64-bit and 32-bit modes
- Support for AES-GCM (Advanced Encryption Standard in Galois Counter Mode), including AES-128-GCM and AES-128-CCM
- SSLv2, SSLv3, TLSv1, and DTLSv1 support
- HMAC-SHA-1 and HMAC-MD5
- DES, 3DES, and AES
- RSA public-key cryptography
- Implementation of OpenSSL APIs to allow for easy porting of existing applications
- Advanced Encryption Standard (AES) Ciphersuites for TLS (RFC 3268)
- Datagram Transport Layer Security (RFC 4347)
- Updated version of OpenSSL

Wind River SSH (Secure Shell) is an implementation of the Secure Shell protocol that provides secure remote login, file transfer, and port forwarding over an unsecure network. This means embedded systems can communicate at the application level over a connection that is encrypted and provides data integrity and replay protection. This

effectively eliminates eavesdropping, connection hijacking, IP spoofing, and other network-level attacks.

In addition, embedded SSH provides several secure tunneling capabilities that may be used to create VPNs. A variety of authentication methods is also supported.

Features of Wind River SSH 6.9 include the following:

- SSH server mode
- SFTP client support
- SSH versions 1.5 and 2.0
- Support for key-exchange/regeneration as defined in section 9 of RFC 4253
- Support for arcfour128 encryption algorithms
- Support for the diffie-hellman-group14-sha1 key exchange algorithms
- Operation in VxWorks 6.9 for both 64-bit and 32-bit modes
- Support for SSHv1 RSA fingerprints and calculating in a way that matches OpenSSH fingerprints generation

Wind River RADIUS and Diameter

Wind River RADIUS Client is a full-featured implementation of the industry-standard remote authentication dial-in user protocol. Wind River RADIUS Client supports a complete set of functions for authentication, accounting, and security, and it has been verified against several commercial RADIUS servers, ensuring compatibility with a wide range of applications.

Wind River RADIUS Client 6.9 allows the network to determine whether a user is allowed access (authentication). Authentication is also used to determine that a message has not been fabricated or altered in transit. Authorization determines which network resources a user may access, and the accounting functions provide a record of usage. The RADIUS tunneling protocol and roaming chargeable user identity (CUI) is supported.

The Diameter authentication, authorization, and accounting (AAA) protocol provides support for peering AAA transactions across the Internet. The Diameter base protocol provides the minimum requirements needed for AAA protocol, Mobile Internet Protocol version 4 (MIPv4), and remote network access applications. Diameter runs on one or more network access points, sending authentication requests to a shared Diameter server.

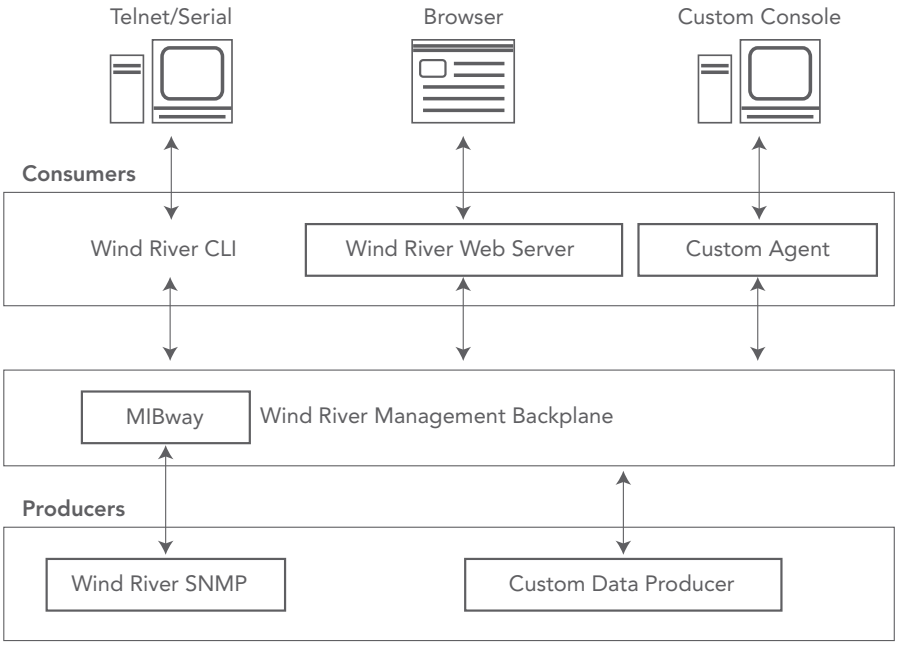

Figure 9: Wind River network management architecture

The Diameter protocol has several advantages over previous AAA protocols in that it offers improvements in the areas of reliability, security, scalability, and flexibility. Wind River Diameter Client 6.9 supports Diameter Proxy Agent.

Wind River RADIUS and Diameter 6.9 add the following:

- Support for 64-bit
- Diameter secure key storage
- Support for RFC 4675: RADIUS Attributes for virtual LAN and priority support
- RADIUS support for RFC 5247: Extensible Authentication Protocol (EAP) Key Management Framework, section 5.9

Management

Wind River provides a scalable, unified, small-footprint management framework that enables creation of Web-based, CLI-based, or custom management interfaces to manage networked elements. As shown in Figure 9, it consists of a management backplane, which acts as a conduit for data-handling between management interfaces (consumers) and manageable elements (producers). The scalable framework can have any type of consumers and any type of producers.

Wind River Management Backplane interfaces with a CLI agent, Wind River CLI; an embedded web server, Wind River Web Server; and an SNMP implementation, Wind River SNMP (Simple Network Management Protocol). In addition, the framework comes with a full-featured, Windows-based developer tool (GUI), Wind River Management Integration Tool (WMIT). This tool eases the development of management interfaces by bringing all the framework components together.

Management Configuration Editor (MCE) is a simplified Eclipse plug-in to help with development of CLI- and Web-based management interfaces. MCE is integrated with Wind River Workbench and may be run on any host that Workbench supports. Developers may choose MCE, WMIT, or both tools to configure a project. MCE is intended as a replacement for WMIT.

WMIT supports only 32-bit target code and cannot be used for 64-bit projects. The MCE can produce 64-bit target code, even if it is run on a 32-bit host. You cannot convert between WMIT and MCE if you are generating 64-bit code with MCE.