AN SDR DESIGN THAT SUPPORTS MULTIPLE SECURITY LEVELS AND NETWORK ROUTING USING AN UNTRUSTED ROUTER

Charles F. Haight, Staff Scientist (ITT Industries, Aerospace Communications, M/S 8526, 100 Kingsland Road Clifton, NJ; charlie.haight@itt.com)

ABSTRACT

Over the past several years the world has witnessed tremendous advances in commercial networking technologies. Many of the advances concern routing techniques and devices used in commercial networks, and networks of networks often referred to as the Internet. Typically, commercial routers are used in unsecured environments, at least from a data perspective. That is, commercial routers have been developed for commercial use without regard to supporting classified information. Although commercial routing devices typically undergo many reliability and quality tests, they are not designed, nor are they tested, with the goal of handling multiple levels of security.

The security issues become significant when the router is embedded in a software defined radio that is multi-channel while supporting military waveforms. Within these two constraints, the software defined radio needs to support two types of routing called black-side routing and red-side routing. Red-side routing contains the ultimate end-to-end source and destination routing information. Black-side routing contains the intermediate information that allows the data packets to find a path to reach the end-user. This paper addresses the security concerns of a multi-channel radio with red-side routing and suggests an approach that is certifiable which uses commercial routing while isolating data packets at different security levels.

1. INTRODUCTION

The typical router operates on Ethernet data or streaming data as it enters the radio. If a streaming data input is used, the radio must packetize the data into IP packets prior to being sent to the router. The router will parse the IP packets, optimize the packet size and determine the best routing path. The algorithm that determines the routing path is dependent on the network topology and the goals of the network. In other words, the algorithm is not fixed and one solution does not fit all.

This paper is not a security tutorial. References to security requirements have been made so that the reader can fully appreciate the subject matter.

2. PROBLEM DEFINITION

The ultimate goal for a software defined radio, at least in the Joint Tactical Radio (JTR) sense, is to have independent user data sources, each user data source operating at its own classification level. It is also a requirement that the JTR provide router functionality so that the user input data can be routed to the ultimate destination while using the desired instantiated channel. Each channel in a JTR will have a waveform that is used to transmit the data packets.

2.1 Multiple Data Inputs

A typical high-level block diagram of a JTR is show in Figure 1. The router functionality will be either part of a selected waveform, such as SINCGARS, or satisfying a standard red-side router function. The issue that immediately surfaces is whether or not the independent user sources are at a common classification level or at different classification levels. If the data sources are at a common classification level, the router will need to be analyzed for minimal trust. Trust here is defined as, "Totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination responsible for enforcing a security policy." [1] Trust that can be assigned to the router is ultimately determined by a certification

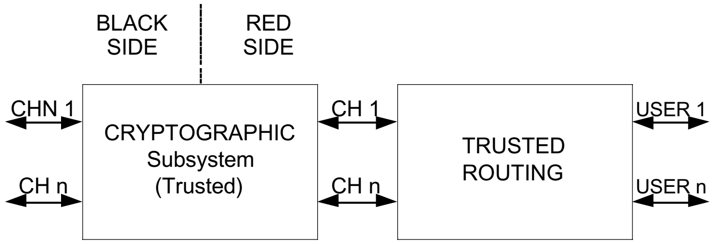

Figure 1 Notional JTRS Block Diagram with Muli-Level Router

methodology such as Common Criteria. The Common Criteria (CC) is the multi-part standard ISO/IEC 15408 which defines criteria to be used as the basis for evaluation of security properties of IT products and systems. The CC is useful as a guide for the development of products or systems with IT security functions; addresses protection of information from unauthorized disclosure, modification, or loss of use and is applicable to IT security measures implemented in hardware, firmware or software. The level of trust that is determined by the Common Criteria analysis dictates how the router implementation can be used in the JTRS environment. As an example, if a particular router implementation receives an evaluation level of EAL2, the router implementation could only be used for unclassified data.

2.1.1 Issues with trusted router

The basic problem with a trusted router is in the implementation. It is not possible to take a commercial router algorithm and supporting operating system (OS), compile the software and achieve an useful Common Criteria EAL rating in the JTRS radio. The router software and the associated operating system need to be analyzed before a level of trust can be assigned.

2.1.2 Length of time for certification and product availability

The certification is lengthy. It generally takes a couple of years to certify a product which includes testing at a national lab to achieve an EAL 3 rating. Embedded in the router implementation will be specific security mechanisms that are tailored for the product. The added security mechanisms become part of the router implementation so security changes can affect router functionality. Conversely, code changes to improve router functionality must be individually analyzed and documented to assure that the security mechanisms have not been compromised.

A high EAL rating means that the router can accommodate higher classification levels or different classification levels simultaneously. Certification takes longer and is more difficult as the EAL ratings get higher. The areas of impact are additional security mechanisms, additional documentation and more rigorous testing.

2.1.3 Technology insertion very difficult

Let's say Company X has a team which finished embedding a trusted router in a product. The

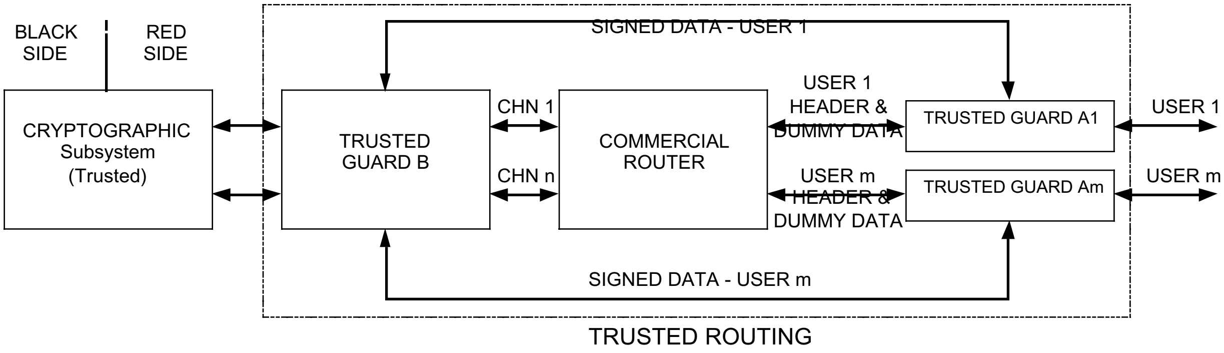

Figure 2 Notional JTRS Block Diagram Using Guards

product has received the desired EAL rating. Along comes a new router algorithm that is applicable to your team's product. The change would enhance your product's performance. The problem will be changing the router while maintaining the security mechanisms. The team must carefully review the changes that need to be made to implement the new router. Additionally, all the documentation that was delivered to support the previous certification will need to be updated with any changes. The product will also need to be tested again to validate the security mechanisms have not been compromised.

2.2 Multi-level Router and Performing Write-Down

A single router that simultaneously handles multiple classification levels is called a multi-level router. The discussions included in this paper do not imply that an unclassified packet that was received on a port that normally handles classified packets can be routed to an unclassified channel. The type of function is called a write-down. The other type of write-down is the examination of the packet to determine its classification. Either of these approaches requires an additional level of complexity which is very significant and is not part of this paper.

3. SOLUTION - COMMERCIAL ROUTER WITH CERTIFIED GUARDS

Armed with the information above, one has to hope there is a better way to introduce technology without having significant cost and schedule impacts. The remainder of this paper discusses a unique approach that isolates the router from the required security mechanisms. In other words, the router and security implementations are independent of each other.

3.1 User Perspective

First and far most, any solution must be done such that the user will not know if the JTRS radio contains a trusted router or uses some other method to accomplish the same function. The solution being presented provides the same functionality as a trusted router and allows router upgrades to be made. The trusted routing function shown in Figure 2, has the same capability as the multi-level router shown in Figure 1. The user would not know the difference even though the implementations are entirely different.

4. DATA FLOW DESCRIPTION

Guard A1 processes the input data from User 1 as shown in Figure 2. The data is hashed which reduces the amount of data to be signed. The hash portion is then signed. Guard A1 then sends the signed data to Guard B. Guard A1 also sends the header information and the dummy data that was substituted for the user data to the commercial router. The router processes the header information by determining the optimum route and sends the routing information and dummy data to Guard B. Guard B replaces the dummy data with the same amount of user data that was previously Guard B. The hash and signature is stripped from the data packet and the data packet is sent to the Cryptographic Subsystem. Conversely, Guard B will perform the same function as Guard A when the JTRS radio is in a receive mode and has the end user connected. (Guard B sends dummy data to the router and sends signed data to Guard A as long as Guard A is the intended recipient.)

A typical JTRS implementation is show in Figure 3. This approach isolates the router from the outside world. It is surrounded by trusted components that are certified. Since the router never sees the user data, it does not have to be certified.

5. DESIGN DETAILS

The Guard that is depicted in Figure 3 has many intermediate processing blocks. These blocks and the related data flows will be briefly described.

5.1 Guard Functionality

In this scenario, the guards perform several functions. Its most important function is to limit information flow by assuring that a given data packet is processed and labeled with the assigned channel. Conversely, the Guards prevent this same packet from being processed by another channel.

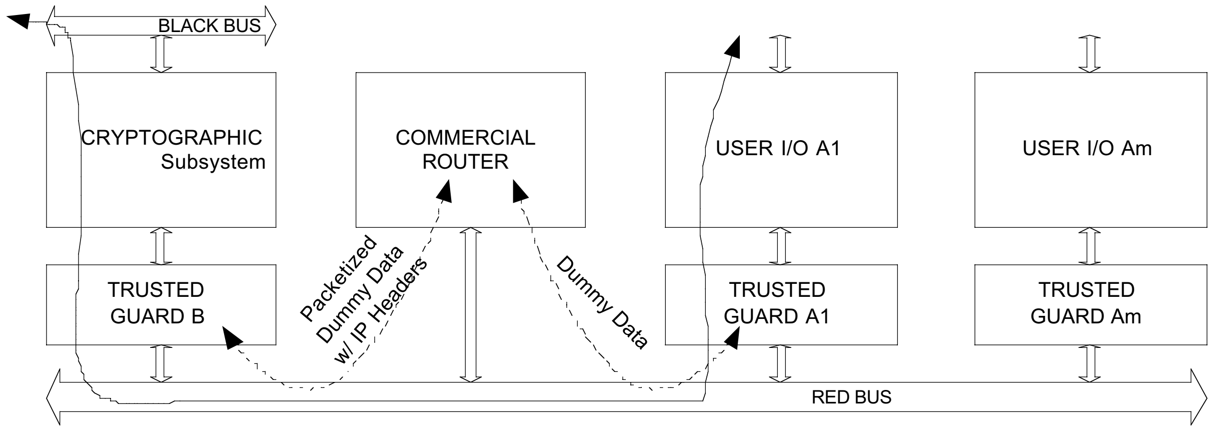

Figure 3 Multi-Level Routing Block Diagram Using A Commercial Router

5.2 Cryptographic interaction of guards

Prior to processing traffic data, each guard, Guard A1 … Guard An; has unique cryptographic information that allows it to sign a data packet. Also, during the instantiation/creation of a channel; a virtual channel assignment is made that associates the guards, the virtual channel and the cryptography to be used. (In the example here, the writer has chosen to use Channel 1 as a virtual channel assignment.) Guard B, also known as the Cryptographic Guard, verifies that the data from Guard A1 belongs with Channel 1. It is validated by verifying the signature that arrived with the traffic data from Guard A1. This signature is also unique to Channel 1.

5.3 Data input to guard

The user data and guard shown in Figure 4 form a unique pair that allows the physical data to be associated with a virtual channel. Since each input data source has a unique guard associated with it, the guard can validate the virtual channel assignment. The virtual channel information is also used by the Operating Environment to track data flow through the entire system.

5.4 Hashing and Signing To Make a Cryptographic Label

Guards A1 … An need to add a cryptographic label that binds the channel and the data that is unique and unalterable. Generally, just signing the data would accomplish the desired binding function. However, it is ill-advised to sign large amounts of data. A better method is to hash the data first and sign the hash. Hashing is a one-way function that creates a known length result based on a varying data input. A suggested hashing function is FIPS PUB 180-1. Once the hash result (message digest) has been obtained, it is digitally signed to ensure its authenticity as depicted in FIPS PUB 186. (Authenticity means that the recipient knows who sent the data.) The data now has a cryptographic label that is 'bound' with the data packet.

5.5 Cryptographic Guard and Router

The Cryptographic Guard and Router receive two different data streams from the Guards A1 … An. The Cryptographic Guard receives the signed user data. The Router receives the dummy data as shown in Figure 2. The Router performs the usual function of locating the recipient and deciding how to get the packet to the destination according to some algorithm. (This point is one of the main issues of this paper! Each routing algorithm is appropriate only for its intended environment. If the environment is changed, the algorithm is sub-optimal at best.) The router forwards the packetized dummy data and header information to the Cryptographic Guard.

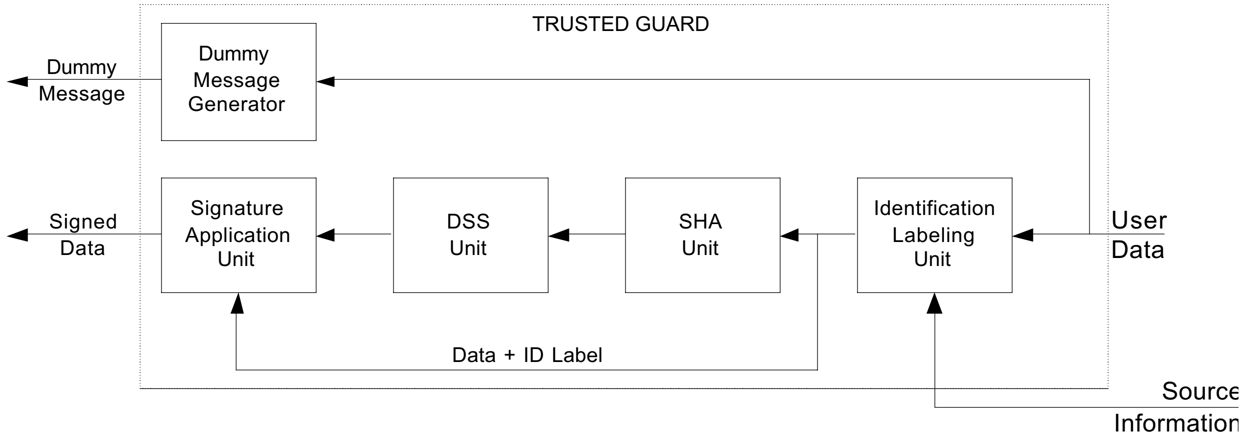

Figure 4 - Functional Decomposition of the Trusted Guard

5.6 Cryptographic Guard performs data substitution

The Cryptographic Guard has the task of substituting the real user data for the dummy data. Before the substitution, this guard validates that the designated virtual channel receives the user data that it was intended to receive by checking the signature. As long as it is the correct channel, it substitutes the user data for the dummy data and forwards the user data to the Cryptographic System as shown in Figure 1. Please observe that the interface between the Cryptographic Guard and the Cryptographic Subsystem is the same as the Trusted Router interface as shown in Figure 1.

6. SUMMARY

The Software Communication Architecture (SCA) defines an architecture that is flexible, extensible and expandable. Implementing a Trusted Router in a JTRS radio does not satisfy the intent of the SCA. This paper presents an approach that uses guards which provides the same functionality as a Trusted Router but also provides the flexibility to upgrade the router as required.

7. REFERENCES

[1] National Information Systems Security (INFOSEC) Glossary, National Security telecommunications Information Systems Security Instruction (NSTISSI) 4009

[2] Federal Information Processing Standard Publication (FIPS PUB 180-1) Secure Hash Standard

[3] Federal Information Processing Standard Publication (FIPS PUB 186) Digital Signature Standard (DSS)