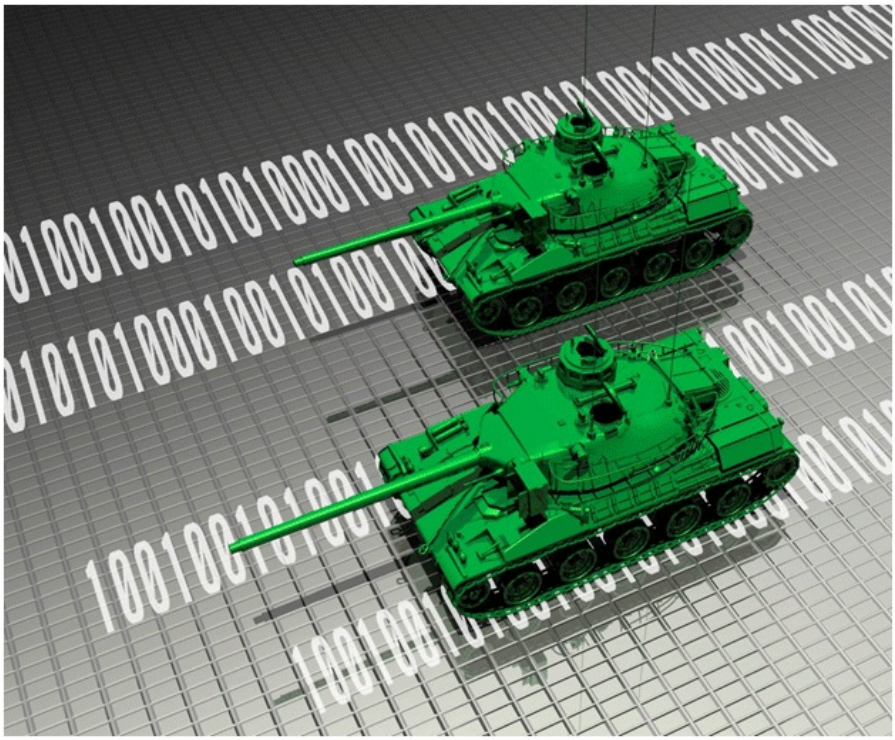
Addressing the concerns of CYBER Warfare

Kiran Kumar , Wind River, India

3 days ago by electronics Comments Off on Addressing the concerns of CYBER Warfare



Information Technology which covers almost all domains viz., Defense, Banking, Government, Utility, and Citizen Information are the backbone and also a vital part of every nation. Any form of damage caused to such a data by another nation can be termed as Cyber Warfare. The various methods to accomplish this viz, Trojan, Virus, Malware, Phishing, E-mail Spamming which are intend illegal applications hosted on specific targets. Besides this, "Denial of service" attacks which is intended to generate excessive requests than the infrastructure can handle and thereby disrupting the legitimate requests. Such unauthorized access to sensitive information can pose serious threat to the country. For example, illegal access to the financial data can paralyze the economic condition of the nation and severely affect its Sovereignty.

Relying on one common firewall for the entire system, in which a breach could give an intruder access to the whole system. One of the classic examples is that of an International leading Shopping mall where an access to the air-conditioning control system provided illegal access to the credit/debit card information of customers. The shopping mall besides shelling out huge compensation, had to face various lawsuits. For more information refer http://www.lawyersandsettlements.com/lawsuit/data-breach.html#.VRFBOuGS8mc.

Besides hacking, phishing and malware which are the most common ways of attacking an Information system, the sophistication of attacks is also increasing rapidly posing challenges. According to the Indian Computer Emergency Response Team (CERT-In) a total of 32,323 websites including about 155 Government websites were hacked in 2014 alone (Source: http://ibnlive.in.com/news/government-telecom-defence-sectors-most-attacked-by-cybercriminals/535148-3.html).

Safety and Security in A&D

Until recent past, Information and data concerning Aerospace & Defense was considered to be secure due to the perception and mindset that the systems are not connected to the Public Internet in majority of cases. However,

there are various ways that a security breach could occur:

1. Forfeited Hardware, which can transmit information in encrypted form without knowledge of the user.
2. Access to systems by un-authorized personnel which can provide a source for security breach.
3. Executing unwarranted applications (for eg: malwares), which passes vital data under the hood.

With multiple deployed systems which are connected to each other in some form either through satellite links, Radio Frequency, Custom networks, exposes devices to more security risks than ever before.

Few reported cases are:

- Indian Navy command system infected with malware transmitted data to an international destination (http://www.bbc.com/news/technology-18703508)
- Attempt to transmit sensitive data from a defense research & development establishment (DRDO) was prevented (http://gadgets.ndtv.com/internet/news/cyber-attack-on-indian-defence-research-lab-thwarted-quick-heal-601330)

As pointed out in EFYTimes, (http://www.efytimes.com/e1/fullnews.asp?edid=162425), India is still vulnerable to Cyberattacks as most government organizations are flooded with dangerous malwares.

There are innumerous instances where technologically highly advanced countries too encounter cyber threats (http://www.cdse.edu/documents/toolkits-fsos/cyber-threat-case-examples.pdf)

In most cases, many cyber-attacks go un-noticed or not treated as a threat and that is where Cyber Security policies play a big role.

Security Challenges for Warfighters

Determining optimum security is certainly the most important specification in order to build a commercially viable solution, while also considering the holistic view of the environment where the mobile platforms shall be deployed. As an example, an Un-Manned Vehicles which is on a surveillance sortie to gather a nation's security information reaches wrong hands and provides access to information can be catastrophic. Another example could be intrusion to the data being transmitted between the soldiers/command-post similar to electronic warfare which again can lead to disasters.

The biggest challenge is to overcome the mindset where security is considered as a feature whereas it is an integral part of the overall design process.

Having a generic security specifications covering wider range of applications is yet another challenge. Adhering to the specifications of each country would make the system very complex and difficult to maintain. Hence there is a need for "Common-Criteria" for addressing security concerns.

Security Platform

The root of trust must be built right from the Hardware, software stack, applications running on the system.

Considering the Un-manned vehicle example quoted previously, the security aspects to be taken care of while build the platform would be to

> *Hardware: Builds root-of-trust right from the hardware platform and there by not transmit data under the hood.*
>
> *As an example Intel has Identity Protection Technology (IPT)® where security elements that are built-in the hardware enabling multi-factor authentication solutions.*
>
> *Data-Storage: The data being captured are stored on on-board storage device. If the unmanned vehicle gets lost/stolen, the stored data would be accessible to anyone if it is not encrypted. Hence encrypting the storage devices on-board would become essential.*
>
> *Booting mechanisms: Assuming the Unmanned vehicle reaches wrong hands and access to data will be available when the system is restarted. If boot authentication is not provided, then the system is vulnerable for not only providing access to the contents, but also paves way for reverse engineering and thereby affecting the entire security system*
>
> *Access to Program: The access points to the system, viz., serial-port, Ethernet, USB etc act as potential entry points through which malwares/un-intended applications can be introduced to system. If user-level privileges are considered for accessing, loading an application and booting, it will prevent any un-authorized access to the running system. Also, if the system is designed to accept signed binary, additionally protection will be ensured.*

The security requirements for each deployed system will be unique based on the environment that the systems will be deployed along with interaction with other sub-systems. For example the security requirements for an on-board infotainment system and that of the landing gear of a commercial aircraft are not the same. Also, if both the systems are inter-connected,isolation between the systems are essential, i.e., a mal-function in the infotainment system should not affect the landing gear system.

Wind River Solutions

Wind River which is fully owned subsidiary of Intel has decades of experience in addressing the safety and security aspects of not only Military/Defense systems but also the commercial world. Wind River has various technologies to address the varying security needs.

Wind River® VxWorks® MILS Platform provides an operating run-time environment designed for systems having high security, high assurance, and high performance requirements. The platform implements an industry-standard system architecture called Multiple Independent Levels of Security (MILS) that enables multiple software components with different security levels, or from different domains, to safely and securely share the same hardware platform. VxWorks MILS has been designed to meet the safety critical requirements of RTCA DO-178C (EUROCAE ED-12C) DAL A.

For lesser critical systems, Wind River offers Security Profile for VxWorks 7 which is a comprehensive set of software-based security elements which delivers capabilities to protect inter-connected devices at various stages:

***Boot-up**: Using secure boot mechanisms, Security Profile for VxWorks verifies binaries at every stage of the boot-up process by virtue of which if there is signature verification failure, the boot stops. On supported architectures, the target system can be configured to only allow digitally signed VxWorks images to load. On Intel®-based platforms, for example, Security Profile delivers a secured Unified Extensible Firmware Interface (UEFI)–based VxWorks boot loader to prevent unauthorized VxWorks images from being loaded.*

***Operation/Run-time**: Protect from code-tampering and un-authorized access via a secure run-time and advanced user management. Wind River has partnered with Wibu-Systems to deliver a solution that can decrypt (AES) and verify digital signatures (ECC) of downloadable kernel modules and real-time processes (RTPs). This solution effectively protects the integrity of the system and safeguards your intellectual property from piracy and code from reverse engineering.*

***Data Transmission**: Secure network communications and prevent attacks with network security features.*

***Rest/Shut-Down**: Safeguard data even when the device is powered down by using True Crypt-compatible encrypted containers.*