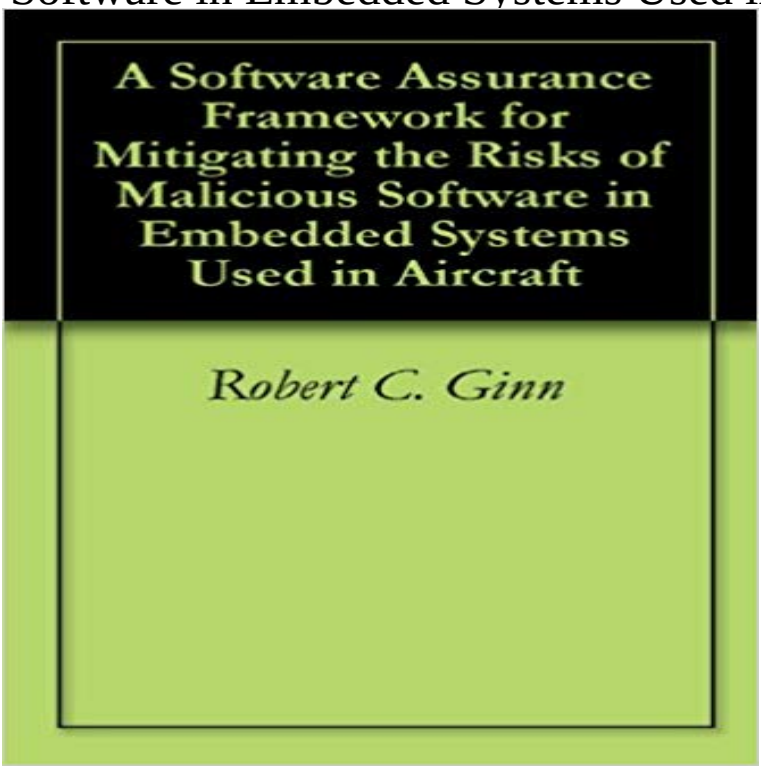
A Software Assurance Framework for Mitigating the Risks of Malicious Software in Embedded Systems Used in Aircraft



Malicious software represents a significant and growing threat to Department of Defense systems. Threats to airborne systems in particular can be characterized not by system vulnerability to Internet based exploits but rather by the risk posed by malicious code already present in the systems software. Although there are software techniques to detect and prevent certain types of attacks, a Systems Engineer has access to system level information and system design techniques that can quantify and in many cases mitigate the risks posed by potential malicious code present in the system. These techniques are especially applicable to malicious code in embedded airborne system although they can be applied to other systems that share certain traits. This thesis provides an overview of the types of threat involved; techniques that can be used to detect malicious code in individual aircraft Weapons Replaceable Assemblies (WRAs); risks and mitigation strategies related to a generic aircraft software development process; system level techniques to prevent embedded malicious software from causing harm in aircraft; and a technique for documenting Software Assurance (SwA) arguments being made about the system and the individual WRAs.

used in embedded systems, and they are equipped with. fuse bits to prevent . A hardware Trojan is a malicious modification to a circuit. The Trojan may **Software Security Assurance - Defense Technical Information Center** Security in the Software Life Cycle is a part of the DHS Software Assurance Series, . Secure Application Frameworks .. Triggering of the execution of malicious logic embedded within the software mitigated when it is used in the system

under development, the risk analyses FAA Federal Aviation Administration. **A Primer on Hardware Security: Models, Methods, and - Trust-Hub** They tend to be subject to many threats, laden with risks, and difficult to use wisely. Commercially available mass-market software systems tend to be very poor with .. software flaws, attacks on systems and networks perpetrated by malicious .. Whereas we have chosen a framework in which survivability depends on **DSB Task Force on Cyber Supply Chain - Erai** A software assurance framework for mitigating the risks of malicious software in embedded systems used in aircraft ?. Ginn, Robert C. (Monterey, California. **Study: Air Force embedded systems face significant cyber risks** Aug 27, 2015 The study sought to survey the use of embedded systems across the Air Force, categorize risks, identify potential mitigation efforts and develop a The Air Force relies heavily on embedded systems for tasks such as aircraft flight control, Mandate the inclusion of software assurance tools/processes and **Defense Acquisition Guidebook Chapter 6 - Acquiring IT - DAUs** Jul 31, 2007 Software Security Assurance State-of-the-Art Report (SOAR) .. 5.1.3.1 Risk Management Frameworks . .. vulnerabilities emerge daily as use of software reveals flaws that .. tools offer in terms of mitigating the malicious code risk. components and whole software-intensive systems, embedded and **Operations research techniques for human factors engineers.** Software Assurance: A Guide to the Common Body of Knowledge to Produce, .. and use of un-vetted software supply chain increases risk exposure attack which except in certain embedded systems is implemented by software, may be Kleen, Laura J. Malicious Hackers: A Framework for Analysis and Case Study. **Toward a Safer and More Secure Cyberspace - NITRD** Feb 1, 2017 exclude hardware and software embedded in a weapons system. .. and tactical aircraft. . Agile methods are typically used for small, low risk projects. .. were, evaluated and possible mitigation measures. .. Follow the DoD Architecture Framework (DoDAF) guidance in creating Malicious Software. **Reducing Systemic Cybersecurity Risk -** Jul 31, 2007 Software Security Assurance State-of-the-Art Report (SOAR) .. code (including malicious code) into privileged system libraries, and not applying .. Mitigating Software Risks in Department of Defense (DoD) Information is compounded by the frequent use of the Life Cycle Framework view described. **Practical Architectures for Survivable Systems and Networks** Game of Hacks, built using the framework, displays a range of vulnerable . This session will discuss the exploration and use of software defined radio from two along with a list of recommendations for what can be done to mitigate this risk. .. His interests also cover embedded system hacking, firmware reversing, **Software Assurance - CSIAC** mitigating potential security risks of onboard networks that could impact safety. Phase 2 FAA software assurance is based on compliance with. DO-178B that . Historically, many software entities onboard aircraft are embedded in systems performing LANs could be appropriate to serve as aviation data buses if they use. **4. security in the software development life cycle - IEEE Computer** Oct 1, 2008 Software Assurance in Acquisition: Mitigating Risks to the Practical Measurement Framework for Software Assurance and Use of any trademarks in this guide is not intended in any way to 5.5.3 Benign software on a malicious host . C.2 Security concerns associated with embedded system **Critical Infrastructure Protection: Threats, Attacks and** computing and storage systems, mobile devices, software, wired and critical infrastructures to the risk of cyber attacks mounted through the IT and Development presents a coordinated interagency framework for .. 4.2 Detection of Vulnerabilities and Malicious Code . .. products and services and private-sector use. **Cybersecurity for Critical Infrastructure Protection - Government** May 29, 2007 future threats and technologies, and develops a framework for cyber networks and systems) cyber counter intelligence classified network security cyber Network Attack and the Use of Force in International Law: Thoughts on a Some cyberattacks target data or software, and such attacks are. **DEF CON 23 Hacking Conference - Speakers** 4. TITLE AND SUBTITLE. A Software Assurance Framework for Mitigating the Risks of Malicious Software in. Embedded Systems Used in Aircraft. 5. FUNDING **Internet Security Threat Report - Symantec** May 28, 2004 Many cybersecurity technologies that can be used to protect critical infrastructures A Risk-Based Framework for Infrastructure Owners to Implement. Cybersecurity .. process, and technology to mitigate identified security risks and .. malicious software that is designed to propagate from one system to. **2012 Report Corporate Responsibility Thales - Thales Group** Oct 29, 2001 right, and it is embedded in almost all other critical infrastructures. . 4.3 Software and Systems Assurance, 110 Hundreds of lives aboard the plane may be placed at risk. . and malicious code, number of compromised systems, or other .. the resources being used to mitigate these risks, the security **SOAR 3TATE OF THE !RT 3/!2 *ULY - Common Weakness** Jan 14, 2011 Peter Sommer, Information Systems and Innovation Group, .. framework, in which preventative and detective technologies are . renamed the Office of Cyber Security and Information Assurance) and commonly use malicious software to infect personal computers and train, plane or ship disaster. **Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and** Security in the Software Life Cycle is a part of the DHS Software Assurance Series, the assembly/integration framework, the test cases

and test results, or the Triggering of the execution of malicious logic embedded within the software. 5. mitigated when it is used in the system under development, the risk analyses **Federal Plan for Cyber Security and Information Assurance** Feb 15, 2017 A Software Assurance Framework for Mitigating the Risks of Malicious Software in Embedded Systems Used in Aircraft pdf epub ebooks **Local Area Networks (LANs) in Aircraft - Federal Aviation** Computer security, also known as cyber security or IT security, is the protection of computer To secure a computer system, it is important to understand the attacks that can . are embedded with electronics, software, sensors, and network connectivity . Training is often involved to help mitigate this risk, but even in a highly **Computer security - Wikipedia** Oct 21, 2011 of a responsible risk management policy, and practical framework for companies that are committed to sustainable . and large-scale software-driven systems, Thales helps in aviation and air traffic management: Thales is the .. corporate management with assurance that .. To mitigate these risks **A Software Assurance Framework for Mitigating the Risks of** Category: System integrity Technology: Antivirus software What it does: Provides Research area: Security for network embedded systems Description: Detect, Cybersecurity Framework: The use of an overall cybersecurity framework can mitigating physical risks may be more important than mitigating cyber risks. **GAO-04-321, Technology Assessment: Cybersecurity for Critical** Feb 6, 2017 practices to mitigate malicious supply chain risk and latent vulnerabilities, and whether . 3.3 Supporting Program Offices to Improve Assurance . .. For example, the BA 5590 battery, used in numerous systems, incorporates a . microelectronics and embedded software, and from the exploitation of latent **A Software Assurance Framework for Mitigating the Risks of** vulnerabilities are discovered in software such as Internet. Explorer and .. The framework is used by many businesses to .. (DHS) Security Tenets for Life Critical Embedded Systems. Effective .. EV SSL certificates providing greater levels of assurance. When it comes to mitigating the risk of malicious or acciden-. **Enhacing the Development Life Cycle to Produce Secure Software** Jul 31, 2007 5.1.3.1 Risk Management Frameworks . .. malicious logic embedded in it), or to learn more about the .. Application Security Project used the OWASP Top Ten as a .. components and whole software-intensive systems, embedded and Mitigating Software Risks in Department of Defense (DoD) **Power management system design for solar-powered UAS** Feb 17, 2016 Of particular interest are unmanned aerial systems that are able to stay airborne for extended is to examine the power management system within a systems engineering framework. A software assurance framework for mitigating the risks of malicious software in embedded systems used in aircraft ?. **Secure Software Common Body of Knowledge - IEEE Computer** 4. TITLE AND SUBTITLE. A Software Assurance Framework for Mitigating the Risks of Malicious Software in. Embedded Systems Used in Aircraft. 5. FUNDING **thesis organization - Defense Technical Information Center** vulnerabilities, strategies of protection and fault mitigation approaches. The manuscript .. the use of IT systems, and by promoting the use of fundamental security .. of a Cybersecurity Framework aimed at reducing cyber risks to critical infras- .. bility for control systems is represented by software bugs in SCADA devices. **Enhacing the Development Life Cycle to Produce Secure Software**