SSC16-IX-02

Cyber Security Awareness for SmallSat Ground Networks

Ted Vera
RT Logic
12515 Academy Ridge View, Colorado Springs, CO 80921; 719-598-2801
tvera@rtlogic.com

ABSTRACT

Satellite ground networks are exposed to an increasing number of targeted cyber threats. Successful cyber-attacks have resulted in substantial data leaks and billions of dollars in material damages. SmallSat ground networks have distinct cyber security challenges associated with mission-unique equipment; specialized protocols; untimely patching due to configuration freezes and high regression test costs; and tight budgetary constraints.

Recognizing that SmallSat ground network operators may lack the resources and budgets of traditional satellite ground operators, it is beneficial to leverage lessons learned, frameworks and tools from Government and Industry to help better defend their networks.

This paper is intended to be a security primer for SmallSat ground network operators, discussing security best practices such as Information Assurance (IA) hardening and continuous monitoring; leveraging frameworks such as Defense Information Systems Agency (DISA) Security Technical Information Guides (STIGs); and tools such as Security Information & Event Managers (SIEM) and Security Content Automation Protocol (SCAP) compliant applications.

Beyond the technical controls that are often the initial thought for network designers, a solid security program must include policies and procedures to help manage the security and organizational needs of the ground network. The National Institute of Standards and Technology (NIST) publishes guides and frameworks that should be used to help establish and drive policy.

THREAT OVERVIEW

With numerous examples in recent news reports, it should come as no surprise that cyber security attacks are on the rise. Verizon's 2016 Data Breach Investigations Report summarizes 64,199 cyber security incidents including 2,260 breaches with confirmed data loss that occurred during 2015 alone.[1] Intel Security / McAfee's conservative estimate of the annual cost to the global economy from cybercrime is more than $375 billion in losses.[2] These attacks targeted all types of public and private organizations and industries, highlighting the fact there are no network connected systems that are immune from online threats.

SmallSat Tip: SmallSat ground networks are no exception; they too are exposed to an increasing number of targeted cyber threats including those attempting to exploit vulnerabilities not found in most traditional Information Technology (IT) network environments.

MISSION-UNIQUE ATTACK SURFACE

Legacy Satellite Ground Networks do not resemble traditional information systems. Satellite ground architectures historically are located in secure areas with stand-alone networks consisting of specialized serial-based hardware and software using proprietary protocols. Over the years, the industry has shifted towards lower-cost commercial-off-the-shelf Internet Protocol (IP) enabled devices and the use of Wide Area Networks (WANs), which increases the possibility of cyber threats.

SmallSat ground networks have unique cyber security challenges such as: mission-unique equipment and applications; specialized protocols; high regression test costs; and tight budgetary constraints. As end-to-end IP architectures become mainstream in SmallSat ground networks, additional security challenges are introduced.

Mission-unique equipment found in satellite ground networks primarily consists of radio frequency (RF) signal processing gear such as: radios, modems, up/down converters, RF recorders, multiplexers, telemetry front-end processors, bit synchronizers, and RF recorders; test equipment such as oscilloscopes, spectrum analyzers and channel simulators; along with specialized protocols and applications such as Software Defined Radio (SDR) and Command & Control (C2)

suites. These niche devices, applications and protocols present unique attack surfaces for potential exploitation.

A recent study published in 2014 illustrates threats associated with mission-unique equipment. IOActive Researchers conducted vulnerability assessments of ten commercially available satellite communications terminals. Their findings included numerous severe security vulnerabilities including weak password reset mechanisms, backdoors, hard-coded credentials, and insecure protocols. Attack scenarios for six widely used Inmarsat and Iridium satellite communications (SATCOM) terminals describe how vulnerabilities can be exploited. The impacts of successful attacks could result in denial of service, data spoofing, execution of arbitrary code, full remote control of devices and even physical damage.[3]

Unlike traditional network environments which are primarily concerned with IP based attacks, satellite ground networks also need to consider RF based threats. For example, in addition to Internet based scans, amateur satellite enthusiasts are on the constant lookout for new satellite feeds detectable using low-cost commodity RF hardware and open-source software. Online satellite enthusiast resources such as SatBeams.com, FeedHunter.com and FastSatFinder .com are used to collaborate and catalog their findings.

For example, FastSatFinder.com publishes transponder frequencies, symbol rates, and polarization information for 162 Satellites including >7000 channels / transponder frequencies. Data can be downloaded in extensible markup language (XML) format for a broad range of satellites including: ABS, Afghansat, Amazonas, AMC, Amos, Anik, Apstar, Arabsat, Arsat, AsiaSat, Astra, AzerSpace, Badr, Brasilsat, ChinaSat, DirecTV, EchoStar, Eutelsat, Express, G-Sat, Galaxy, Hellas, Hispasat, Horizons, Insat, Intelsat, JCSat, KazSat, KoreaSat, MeaSat, N-Sat, Nilesat, Nimiq, NSS, Optus, PakSat, QuetzSat, SES, Simn Bolvar, Sky Mexico, Spaceway, Superbird, Telkom, Telstar, Thaicom, Thor, TKSat, TrkSat, Turkmenlem, Y1A, and Yamal.

In August 2015 at the Chaos Communication Camp hacker conference held in Germany, security researchers “Sec” and “Schneider” in their talk entitled “Iridium Hacking: Please Don’t Sue Us”, demonstrated how to eavesdrop on Iridium pager communications using low-cost commodity hardware and open-source software.[4]

SmallSat Tip: Attacks like this demonstrate that when possible, it is important to encrypt not only command & control links, but also telemetry / downlink channels. Even simplex telemetry containing unencrypted metadata can lead to potential exploits. One such exploit is described in a report by Kaspersky Labs which claims that a Russian-speaking spy gang known as Turla uses hijacked satellite IP addresses of legitimate users sent as unencrypted metadata to steal data from other infected machines in a way that hides their malware command and control server.[5]

RESOURCES AND BEST PRACTICES

Recognizing that SmallSat ground network operators may lack the resources and budgets of traditional satellite operators, it is beneficial to leverage lessons learned, along with frameworks, and tools from Government and Industry to help better defend their networks.

The NIST Special Publications (SP) library provides a wealth of information and resources that can be leveraged by SmallSat ground network operators who are just getting started developing a security program.

The SP800 series consists of Computer Security related guidelines, recommendations and reference materials. The new SP1800 series Cyber Security Practice Guides provide practical user-friendly guidance to help public and private sector users adopt a standards-based cyber security approach.

SmallSat Tip: The list of publications in Table 1: NIST Special Publications below is not comprehensive, but serves as a good list to get started with:

Table 1: NIST Special Publications

Publication	Title	Link
NIST SP 800-37 Rev. 1	Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach	http://dx.doi.org/10.6028/NIST.SP.800-37r1
NIST SP 800-34 Rev. 1	Contingency Planning Guide for Federal Information Systems	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf
NIST SP 800-115	Technical Guide to Information Security Testing and Assessment	http://dx.doi.org/10.6028/NIST.SP.800-115
NIST SP 800-100	Information Security Handbook: A Guide for Managers	http://dx.doi.org/10.6028/NIST.SP.800-100
NIST SP 800-94	Guide to Intrusion Detection and Prevention Systems (IDPS)	http://dx.doi.org/10.6028/NIST.SP.800-94
NIST SP 800-92	Guide to Computer Security Log Management	http://dx.doi.org/10.6028/NIST.SP.800-92
NIST SP 800-64 Rev. 2	Security Considerations in the System Development Life Cycle	http://dx.doi.org/10.6028/NIST.SP.800-64r2
NIST SP 800-50	Building an Information Technology Security Awareness and Training Program	http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

SECURITY PROCESS

Before diving in to the technical controls that are often the initial thought for network engineers, a solid security program must include policies and procedures to help manage the security needs of the organization. NIST SP guides and frameworks can be used to help establish and drive policy. Using these tools, such as the Risk Management Framework and Contingency Planning Guide, can help an organization get a strong starting point for security and IT infrastructure beyond purely hardware related controls.

An overview of the Risk Management Process is contained in NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems. The Risk Management Framework is an iterative process consisting of the following six steps: Categorize, Select, Implement, Assess, Authorize, and Monitor as illustrated in Figure 1 below.

Figure 1. Risk Management Process Steps

Step 1: Categorize the information systems and the information they process, store and transmit, based on a risk/impact analysis. The documentation resulting from this step will feed into subsequent steps and provide a thorough description of the systems and operational environment that can be used for future reference.

Step 2: Select the baseline security controls for the information system, and tailor as needed to meet the organization's risk assessment. NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations contain a comprehensive list of controls grouped by families that serve as a guide.

Step 3: Implement the selected security controls and document how they are employed within the information system and its operational environment. DISA STIGs and SCAP tools can be used to help automate and document portions of this step.

Step 4: Assess the security controls to ensure they are implemented correctly. Assessment can be accomplished using automated vulnerability scanners (i.e.: Nessus) or through manual inspection and validation. DISA STIGs and SCAP tools can be used to help automate and document portions of this step.

Step 5: Authorize operation of the information system based on determination that residual risk is acceptable to the organization.

Step 6: Monitor information system security controls on an ongoing basis. Practice good configuration management to document changes to the system and operational environment. SIEM and SCAP tools can help automate and document portions of this step.

SmallSat Tip: Each step in the process can be tailored to meet the specific needs of the organization.

SYSTEM HARDENING

NIST 800-53 provides general guidance for security controls; however controls do not always translate easily into actionable items that can be implemented on a system. DISA Security Requirements Guides (SRGs) are a compilation of Control Correlation Identifiers (CCIs) which break down NIST SP 800-53 controls into actionable items, grouped into specific technology areas such as operating systems, applications, networking devices, and policy.

DISA STIGs are validated hardening guides, updated quarterly for major operating systems, applications and network hardware. Configuring systems in accordance with applicable STIGs can help to remove or mitigate configuration vulnerabilities present in satellite ground network devices. Coupled with a patching program and routine vulnerability scans, the attack surface of a ground station network can be minimized.

The DISA STIG Viewer is a freely available tool that can be used to complete and document STIG checklists while implementing system security controls. The DISA STIG Viewer can be downloaded from http://iase.disa.mil/stigs/Pages/stig-viewing-guidance.aspx.

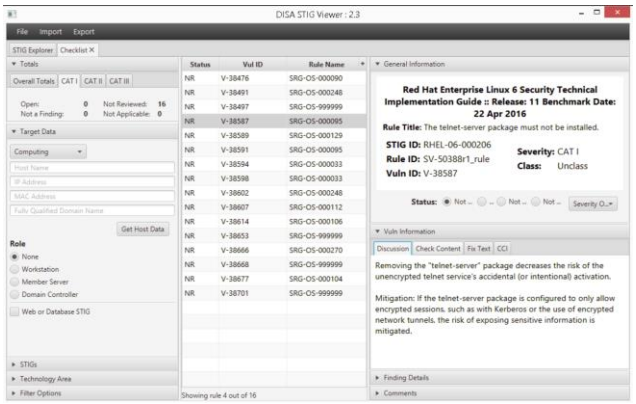

Figure 2. DISA STIG Viewer

Known vulnerabilities are grouped by severity in CAT I, CAT II, and CAT III tabs. For each vulnerability, the tool provides background discussion, steps on how to determine if the vulnerability is present, and steps necessary to fix and verify that implementation was successful.

Small Sat Tip: Be sure to harden all hosts residing in the satellite ground network and be careful not to overlook specialized systems such as oscilloscopes, spectrum analyzers, and channel simulators. They might not be thought of as IT systems but often contain a traditional operating system.

CONTINUOUS MONITORING

Security Information & Event Managers are a product class that can help organizations to meet their continuous monitoring requirements through real-time event processing, alerting and reporting. Market leaders of SIEM technologies include IBM, HP, Splunk, Intel, and LogRythm as cited in Gartner's 2015 Magic Quadrant for SIEM Report.[6] Alienvault is ranked as a visionary and is responsible for the Open Source Security Information & Event Manager (OSSIM), which is freely available from: http://www.alienvault.com.

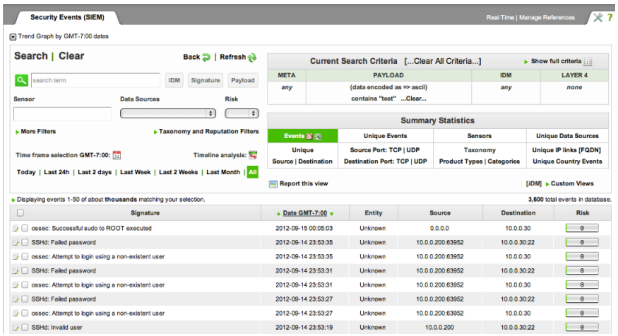

Figure 3. OSSIM Security Events View

The use of SIEMs in the commercial sector has become an industry-accepted best practice for monitoring security risks. Real-time alerting helps mitigate the risks associated with vulnerable mission-unique equipment, specialized protocols, untimely patching, and deprecated protocols. Furthermore, scripted active response capabilities allow an organization to fight through a contested network environment.

SmallSat Tip: Challenges associated with implementing a SIEM for a SmallSat ground network include: developing custom plug-ins for mission-unique equipment; monitoring specialized protocols, and writing rules and scripts for active responses to detected threats.

Another class of product that can help organizations to monitor security controls on an ongoing basis is SCAP validated products.

NIST maintains a list of SCAP validated products that perform authenticated configuration scanning and support Common Vulnerabilities and Exposures (CVE) here: https://nvd.nist.gov/scapproducts.cfm

Commercial SCAP validated products include: IBM Big Fix, Rapid 7 Nexpose 6, Microsoft SCAP Extensions, Tenable Security Center 5, SAINT, RedHat OpenSCAP 1.0, and Tripwire Enterprise 8.

SmallSat ground operators unfamiliar with SCAP tools should consider exploring the RedHat OpenSCAP Project, which publishes tools that are freely available for a number of Linux platforms from: https://www.open-scap.org. OpenSCAP Base is a NIST certified command line tool that can be used to perform configuration and vulnerability scans.

CONCLUSION

Smallsat systems are vulnerable to cyber threats and care should be taken as ground networks are designed. The guidelines and tools presented here can help secure SmallSat ground networks from potential hackers and cyber threats. SmallSat Ground Operators can benefit from the resources and tools that are broadly in use among Government organizations. NIST Special Publications provide a solid framework for establishing a comprehensive security program. DISA STIGs and tools can be used to perform and document information assurance hardening of SmallSat ground network devices and applications. Security Information & Event Managers and SCAP compliant tools help the organization to continuously monitor security controls on an ongoing basis.

REFERENCES

1. Verizon, "Verizon 2016 Data Breach Investigations Report", Basking Ridge, NJ, April 2016.
2. Intel Security / McAfee, "Net Losses: Estimating the Global Cost of Cybercrime", Santa Clara, CA, June 2014.
3. Santamarta, R., "A Wake-up Call for SATCOM Security", Seattle, WA, April 2014.
4. Schnieder, S., "Iridium Hacking: Please Don't Sue Us", Chaos Communication Camp 2015, Germany, August 2015
5. Tanase, S., "Satellite Turla: APT Command and Control in the Sky", September 2015
6. Kavanagh, K. and O. Rochford., "Gartner Magic Quadrant for Security Information Event Management", July 2015