

Information Security 101



Spring/Summer 2015

Inside this issue:

Vulnerability Management in the ARC

Facebook message: 'Friend' or Foe

We All Work in Information Security Now

ARSLs System Security Plan

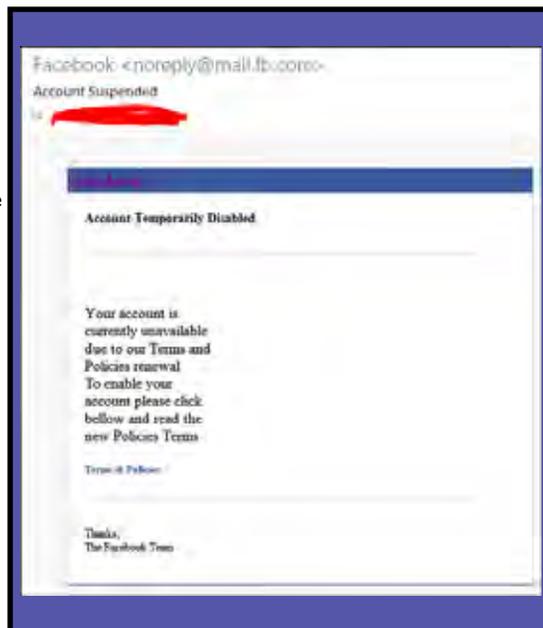
ARC IT Spotlight: Mike Dover

IT Vulnerability Management in the ARC

The February ARC Information Assurance Working Group served as a special session to introduce and discuss the how IT vulnerabilities are tracked and addressed in the ARC program. The ARC Program Vulnerability and Remediation Action Tracker (VRAT) Management Process provides a standard schedule and process for the review, update, and closure of IT vulnerabilities, allowing RSL PMs have an accurate picture of the ARC IT enterprise's security posture. These vulnerabilities are uncovered during regular ARC security program continuous monitoring efforts such as Security Control Assessment & Risk Assessment. The ARC Security team collaborates with the responsible ARC Program IT stakeholder (s) to identify remediation milestones and timelines. Managing ARC program vulnerabilities includes a Federal Information Security Management Act (FISMA) compliant process for formally accepting risk that has been mitigated to an acceptable level. Table-top simulations of an IT system outage at two locations allowed the ARC IT security team to discover, document and prioritize steps necessary to restore critical systems and processed dependent on IT. Through this process, other vulnerabilities have been mitigated and an Incident Response plan developed that specifies the steps to follow in the event of a malicious hack or other event. If a full technical remediation is unavailable or unreasonable due to cost, labor, or other constraints, the ARC program VRAT Acceptance of Risk process allows RSL PMs to accept mitigations that lower the overall residual risk of a particular vulnerability, and close out the risk. This process allows the ARC program to keep a detailed log of vulnerability items and have a tailored program solution for those items that simply cannot be fixed under current resource constraints. Program IT representatives are an integral part of the team in identifying, tracking, and remediating vulnerability items throughout the program.

Facebook messages - 'Friend' or Foe?

The online security magazine net-security.org featured an article in February about a Trojan virus sweeping the web in the form of a Facebook message. Users would receive a message claiming to be from the site itself indicating that the users account has been temporarily disabled and inviting the user to click a link labeled "Terms & Policies." Unwittingly, users clicking on the email initiate an executable file, a type of malicious code that changes the instructions a computer will carry out based on the malicious content of the virus code. This type of attack is called a "Trojan" after the mythical attack on the city of Troy, when the Greek army concealed itself inside a wooden horse to circumvent Troy's defenses. Likewise, a Trojan attack is carried out through a seemingly harmless vector such as a .pdf file or a .jpeg. While it's difficult to prevent every attack, especially those that come in such cleverly disguised means, users can take action to protect their machines and data. Familiarize yourself with the standard communication forms and customer service email addresses for sites you use often, like google, facebook, and youtube so that you will notice subtle differences in fake addresses. Do not click on any link sent to you. Instead, navigate to the site independently and log-in as normal to see if you get the same notification via that method; and don't hesitate to verify the message by phone or email from another account. Most importantly, keep anti-virus software up to date on your machine. The Facebook Trojan featured here was a common virus and would have been recognized by at least half of common antivirus solutions currently in use. To prevent further attacks, be sure to use the sites feature to report malicious activity; or, in the case of an email, mark as junk or spam.



Security Learning Corner: White House Cyber Summit & US Digital Service

On February 13, 2015, the White House and Stanford University hosted a meeting of industry, government, and academic leaders to a summit on cybersecurity and consumer protection. The summit was part of a larger commitment by the Obama administration to improve the country's strategic defense in cyberspace and protect cyberspace as a common asset like power or natural gas. The summit identified areas that require immediate attention from both lawmakers and industry, including secure payment methods and the complexity of international law as it applies in cyberspace. To aid in

their part of the move towards a brighter digital future, the



White House has engaged the nation's best and brightest to begin research on technical

projects through the establishment of the U.S. Digital Service. Hired from companies like Google, Facebook, and IBM, U.S. Digital Service members will act as consultants to the highest levels of government agencies with the goal of "remaking the digital experiences that citizens and businesses have with their government." Both the Cyber Summit and the Digital Service are evidence of the country's sharpened focus on cybersecurity as a critical asset for national security and economic productivity, not to mention the comfort of the average citizen.

Helpful Tips:

You don't have to be Uncle Sam's digital service team to do your part. If your computer's performance changes and/or you suspect you may have a virus or malware, take steps to prevent further damage:

- ⇒ Notify your security POC immediately
- ⇒ Ensure you have the latest software updates & antivirus for your machine
- ⇒ Run a scan with the updated antivirus tool
- ⇒ Quarantine or delete detected malicious files
- ⇒ Forward suspicious emails (without opening attachments) to your security POC

"We All Work in Security Now" - ARC Information Security Awareness & Response

According to an industry report of hacks and data breaches for the last few years, 63% of breaches in 2013 were attributable to

human error, particularly to failure to perform routine security processes. Other common sources of compromise were employees falling prey to social engineering attacks or acting without regard for information security policy in their daily job duties.

CIO magazine published an article in early 2015 entitled, "We All Work in Security Now" that highlights the critical role of the average user in the protection of any organization's IT assets and network. According to the engineers featured in the article, technical safeguards like firewalls and strict password policies are useless without diligent participation by the user community and extensive security awareness training to prepare those users to function in an IT

environment where they face increasingly sophisticated social engineering attacks. The IT and InfoSec teams for the ARC program have devoted a great deal of energy to preparing quality Information Security Awareness training for ARC users. This newsletter and other awareness pieces are provided in the interim to keep security fresh in everyone's mind, but a robust, comprehensive training solution is underway. Another user-dependent aspect of security featured in the article is Incident Response. The ARC Information Assurance Working Group recently provided input to the ARC Incident Response Plan, putting in action the article's assertion that "an effective IR plan can make attacks more of a nuisance than a disaster."

Information Security is certainly a team effort, and the ARC Information Security team welcomes the input of everyone in the program on how to improve security processes that are accessible and useful for your daily worklife. Contact us anytime with suggestions or questions.

More Information

<http://www.cio.com/article/2886325/security0/we-all-work-in-information-security-now.html>

<http://qz.com/201699/the-single-biggest-cause-of-government-data-breaches-is-oops/>

<http://www.cio.com/article/2848478/security0/the-top-infosec-issues-of-2014.html>

ARC Program Update: ARSLS Program Applications System Security Plan

Arctic Sciences Section
Information Security Support
is provided by SPAWAR
Office of Polar Programs

Robert Myer, Program
Manager, SPAWAR Office of
Polar Programs (SOPP)
843.345.0800
robert.l.myer.civ@mail.mil

Sarah Vassel
Polar Program Manager
843.364.3350
vassel_sarah@bah.com

Maria Petrie
Arctic Information Security
706.414.1412
Petrie_maria@bah.com



Special Projects: ARSLS SSP

The ARC Security team in conjunction with CPS recently authored an update of the system security plan (SSP) for the Arctic Research Logistics Support System (ARSLS) Program Application System. ARSLS is a system of systems that contains data about past, present, and future research projects, field plans, and related information. It also feeds the Arctic Research Mapping Application (<http://armap.org/>). While no Personally Identifiable Information is kept in ARSLS, the integrity of the system is paramount for NSF, CPS, and its customers. The ARSLS SSP update was developed through extensive system documentation analysis and ARSLS system stakeholder interviews. The ARSLS SSP now contains up

to date asset, processes function and support information for the ARSLS Program Application System

What is a System Security Plan?

The purpose of the System Security Plan is to provide an overview of Federal and program security requirements of the system and describe the controls in place or planned, and references other documents that define responsibilities and expected behavior of all individuals who access the system.

System Security Plans as an element of Risk Management

Up to date security documentation is an essential organizational tool used to plan for unknown risks that accompany the use of Information Systems. While some level of risk is inevitable, accurate and up to date security documentation gives organizational leadership a realis-

tic understanding of its risk posture for a given system, asset, or program. In the event of an incident, documents like System Security Plans help leadership understand what assets may have been affected and what control gaps may have potentially contributed to the incident. System Security Plans and other support security documentation also allow for continuous improvement of an organization's assessment and remediation of IT risk. Though it's not always glamorous, annual review of security documentation is critical to federal compliance, timely restoration of IT services in the event of an incident, effective risk management, and the overall success of the ARC program mission.

ARC IT Spotlight: Mike Dover, ARSLS Principal Developer CH2MHill Polar Services

The complex web of applications known as the Arctic Research Logistics Support System Program Applications System is composed of numerous applications that independently support ARC program operations. The ARSLS system of systems is the single biggest segment of the ARC program IT assets and has been the focus of many security efforts this quarter. In this edition of the ARC IT Spotlight, we interviewed the man who keeps ARSLS up and running for the team—Principal Developer Mike Dover.

Q: Mike, what is your favorite part of the job?

A: Number one would be the people I work with. The polar program includes so many great people doing interesting, challenging and important work. And what I truly enjoy, as with so many others in this program, is a great challenge. And there is no shortage of challenges in this program.

Q: How did you come to support the ARSLS system? Is it most of your job or just a little bit?

A: Supporting the ARSLS program is my full time job. I joined the program as an IT Application Developer in 2000 when the prime contractor was VECO. At that time, it was named the ARLSS program. I have worked for VECO, CH2M HILL, Critigen and now back to CH2M HILL all the while doing exactly the same job to act as the lead IT Application Developer for the polar program. I have been fully involved in developing many of the software applications used by the CH2M HILL Polar Services (CPS)



team from the ground-up, from initial inception through many new releases to where we are today for these applications. I continue to support and maintain these applications and I continue to extend these applications as the CPS team finds new ways to use the applications. There have been so many IT advancements during this time, and it has been exciting and challenging to learn new technologies and apply new technologies to benefit the program wherever applicable.

Q: From a personal perspective, what are you excited about right now?

A: I'm looking forward, as always, to seeing if the Denver Broncos can get back to, AND WIN, the Super Bowl. Thanks, Mike, for your time for this interview and your dedication to the Arctic Program!