Verifying the Integrity and Authenticity of Software

The Software Assurance Guardian™ (SAG™) Background Check Methodology

Dick Brooks, Reliable Energy Analytics LLC

IEEE SMART GRID

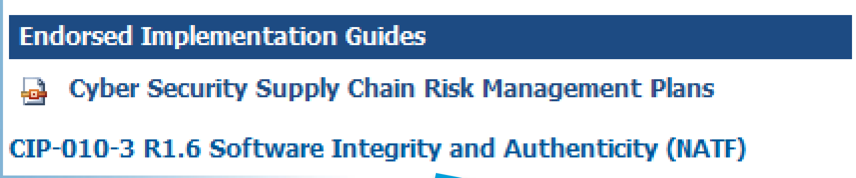
Cybersecurity Workshop 2019

InterContinental Buckhead, Atlanta, GA – December 12-13

Notice

NOTE: The materials contained in this presentation describe **PATENT PENDING TECHNOLOGIES** that are the intellectual property of Reliable Energy Analytics LLC and have been designed to protect the integrity of the Bulk Electric System Critical Infrastructure and its software components. All of the materials presented and discussed as part of this overview presentation, in both printed and verbal form, are the intellectual property of Reliable Energy Analytics LLC and are protected under US Patent Laws. This notice page must accompany all copies of this presentation that may be distributed.

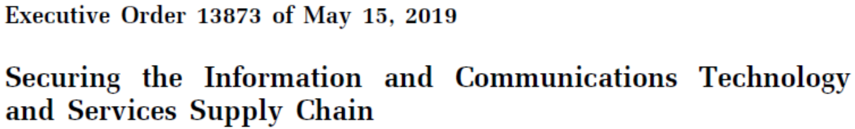
NERC/NATF GUIDANCE ORDER 850



Endorsed Implementation Guides

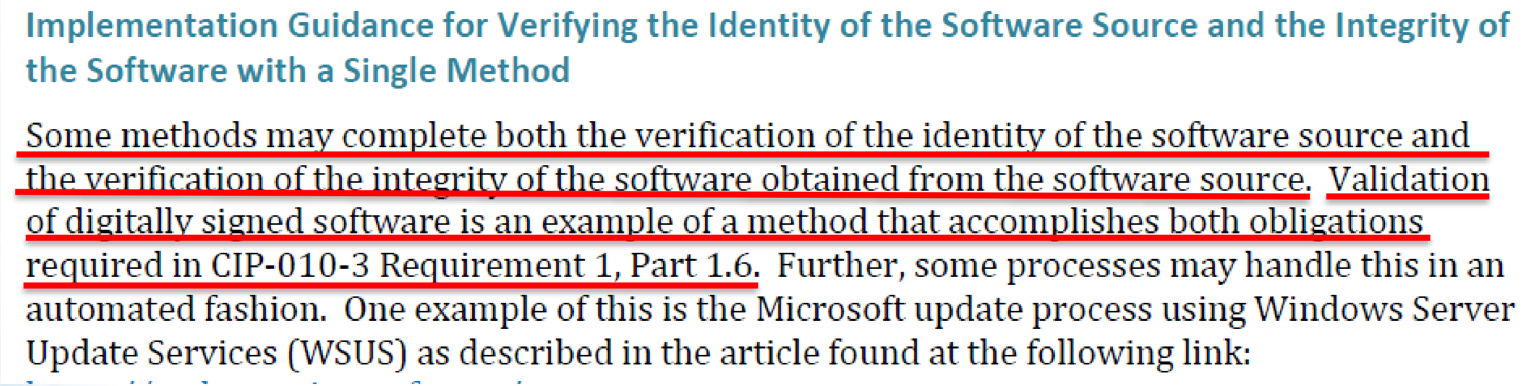
Cyber Security Supply Chain Risk Management Plans

CIP-010-3 R1.6 Software Integrity and Authenticity (NATF)



Executive Order 13873 of May 15, 2019

Securing the Information and Communications Technology and Services Supply Chain



Implementation Guidance for Verifying the Identity of the Software Source and the Integrity of the Software with a Single Method

Some methods may complete both the verification of the identity of the software source and the verification of the integrity of the software obtained from the software source. Validation of digitally signed software is an example of a method that accomplishes both obligations required in CIP-010-3 Requirement 1, Part 1.6. Further, some processes may handle this in an automated fashion. One example of this is the Microsoft update process using Windows Server Update Services (WSUS) as described in the article found at the following link:

https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx

WHY DIGITAL SIGNATURES AREN’T ADEQUATE TO ENSURE TRUSTWORTHINESS

- Digitally signed software provides a “veil” of trust that may not be justified
  - COMODO Fraudulent Certificates

    Microsoft is aware of nine fraudulent digital certificates issued by Comodo, a certification authority **present in the Trusted Root Certification Authorities Store, on all supported releases of Microsoft Windows**
  - ASUS March 29, 2019

    As *Motherboard* reported, researchers at Kaspersky discovered that malicious hackers had **successfully planted malware posing as an official ASUS security update** onto ASUS’s servers **and signed it with two of the company’s legitimate digital certificates.**
  - Sophos Threat Report 2020

    Attackers may attempt to minimize detection by **digitally code-signing their ransomware with an Authenticode certificate.**

WHAT ABOUT UNSIGNED SOFTWARE OBJECTS

- Many software objects are unsigned
  - Commercial products, i.e. Oracle, Microsoft, etc.
  - Numerous GitHub objects
  - Shareware and Open Source software
- Should a Responsible Entity install them anyway?
- Software risks are found in lots of places!

SAG Philosophy: Never Trust software, always verify and report!™

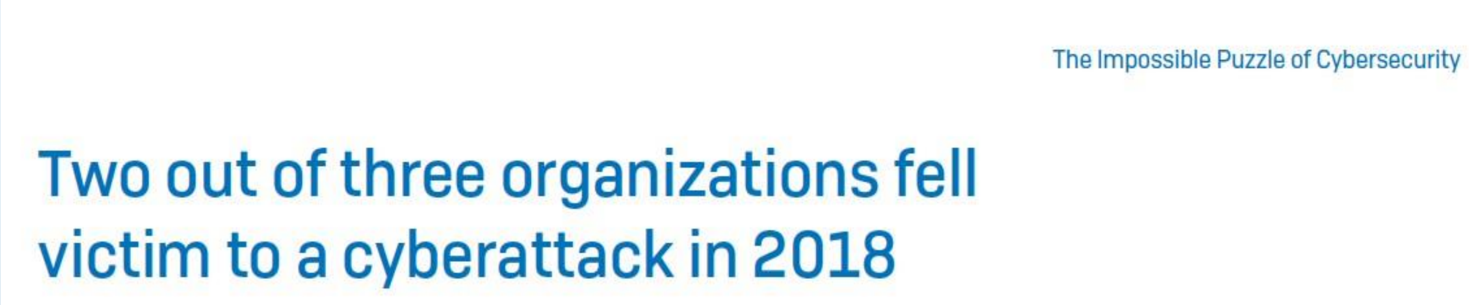
- The philosophy behind SAG's design is based on the same in-depth level of due diligence a Company might apply when hiring a new employee to work in the Control Room; After all that's what many BES software applications do – they work for the Control Room
- Provide Responsible Entities with the most timely, accurate information available to make a risk based decision on the trustworthiness of a software object to perform, without causing harm, in it's BES role
- SAG makes every effort to ensure that a thorough "background check" is performed to determine the integrity and authenticity of a software object, using the best practices available, on an on-going basis
- Produce a SAGScore indicating the statistical level of trustworthiness, based on all of the information collected during SAG Software background check process.

Software Background Check Methods

- Software background check process/methods
  - Verify the source location where SW was acquired
  - Verify the path taken to acquire SW – did the Internet path pass through Iran?
  - Verify the party hosting the source location – are they trustworthy?
  - Verify the SW object is free of known defects, i.e. viruses/malware
  - Verify the party that developed and licensed the SW
  - Verify the party that distributed the SW – are they trustworthy
  - Search for known vulnerabilities with the SW object
  - Search for known compromises of parties within the supply chain
  - Assign a SAGScore™ indicating a level of trustworthiness for the SW object based on results of the above background checks
  - Produce SAGScore™ using the most current information available, on an on-going basis
  - Capture all background check and other contextual information in a tamperproof record for posterity and forensic purposes
  - Report Findings to E-ISAC and ICS-CERT , as needed

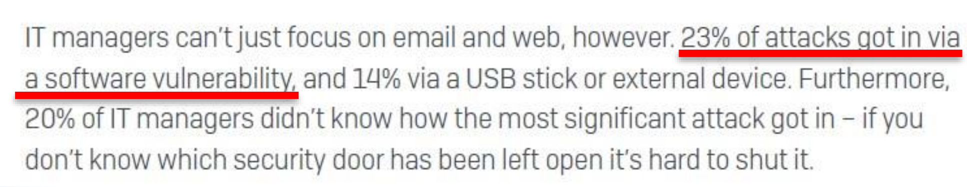
SAGScore™ Calculation

- Proprietary Algorithm incorporating 16 weighted factors
- Modeled after FICO score
- 50% contribution from each set of checks (Integrity and Authenticity)
- Used as a Risk Assessment tool
- A software object with a SAGScore below 95 should never be installed in a Grid command/control system

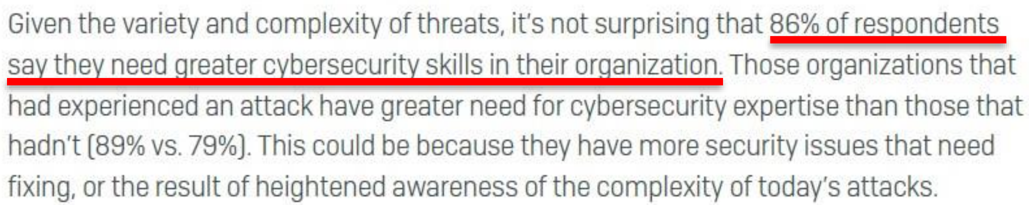


The Impossible Puzzle of Cybersecurity

Two out of three organizations fell victim to a cyberattack in 2018



IT managers can't just focus on email and web, however. 23% of attacks got in via a software vulnerability, and 14% via a USB stick or external device. Furthermore, 20% of IT managers didn't know how the most significant attack got in – if you don't know which security door has been left open it's hard to shut it.



Given the variety and complexity of threats, it's not surprising that 86% of respondents say they need greater cybersecurity skills in their organization. Those organizations that had experienced an attack have greater need for cybersecurity expertise than those that hadn't (89% vs. 79%). This could be because they have more security issues that need fixing, or the result of heightened awareness of the complexity of today's attacks.

2018 NERC Compliance Issues

- **Focus on Serious Risk Issues**
- In 2018, NERC filed 12 Full NOPs with **a combined penalty amount of $4,279,000**. These Full NOPS included 6 serious, 14 moderate, and 15 minimal risk violations. The Full NOPs filed in 2018 included a range of serious risk issues that NERC has identified as potential areas for future focus of ERO Enterprise resources:
- **Multiple instances of noncompliance with CIP standards as a result of issues with implementing new tools and processes**, asset and configuration management, inadequate training and management oversight, **contractor and vendor failures**, failure of situational awareness, development of organizational silos, and **a lack of clearly defined internal policies**;

- Source: NERC **2018 Compliance Monitoring and Enforcement Program Annual Report,** February 6, 2019

SUMMARY

- SAG background check methods provide Responsible Entities of all sizes and skills with the best practices available to verify software integrity and authenticity consistently throughout the BES ecosystem
- A statistically produced SAGScore provides Responsible Entities with a confidence level indication of the trustworthiness of a software object to aid in the final decision to install a SW object in a BES cyber asset
- Background check results and other contextual information is stored in a tamperproof record for posterity and forensic studies

Contact Info

Thank you for your time and attention

Software
Assurance
Guardian™

R E A
RELIABLE ENERGY ANALYTICS LLC

Dick Brooks
dick@reliableenergyanalytics.com
https://reliableenergyanalytics.com/