NERC-CIP, Cybersecurity, and Authentication in Hydropower infrastructure

Phish Friendly Dams?

SECURITY CLOUD
Digital Infrastructure

By: Collin Miller
A little about me...

- Collin Miller – Director of Cloud Security
- 15 years at Structured
- Almost 20 years in InfoSec
- NW native - personal interest in hydropower
- Grandson of Army Corps of Engineers Civil Engineer Jim Perry
- Thru-hiked the PCT from Mexico to Canada in 2015
In this presentation

• Overview of NERC-CIP
• Authentication requirements: CIP-007-6
• Passwords and Phishing
• Advanced Authentication
Don’t FERC it up

**FERC**

- Federal Energy Regulatory Commission
- US Federal Agency
- Licenses and inspects private, municipal, and state hydroelectric projects

**NERC**

- North American Electric Reliability Corporation
- Non-profit Corporation, mission is to “ensure the reliability of the North American bulk power system.”
- Develops and enforces standards
NERC-CIP

• CIP – Critical Infrastructure Protection
• Set of standards (9) and requirements (45)
• NERC CIP-007-6: 6th revision of the Cyber Security - Systems Security Management standards, covers password requirements
Figure A.6: Most Violated Reliability Standards Discovered in Q1 2018

Authentication Requirements: CIP-007-6

5.1 - Have a method(s) to enforce authentication of interactive user access, where technically feasible.

5.2 - Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).

5.3 - Identify individuals who have authorized access to shared accounts.

5.4 - Change known default passwords, per Cyber Asset capability.
5.5 - For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters:

   5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and
   5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.

5.6 - Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.

5.7 - Where technically feasible, either:
   – Limit the number of unsuccessful authentication attempts; or
   – Generate alerts after a threshold of unsuccessful authentication attempts.
Compliance vs. Security
Passwords in 2019

• Length is strength; think passphrase (12 character minimum)
• Complexity is a myth; think uniqueness
• Changing passwords frequently can do more harm than good*

* Unless you change them everytime (i.e. OTP: one-time passwords)
Through 20 years of effort, we’ve successfully trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess.
Phishing

• Phishing makes even complex passwords easy to defeat
• Targeted phishing (spearphishing) is extremely difficult to protect against
• Cloud has made phishing even harder to defend
Recommendations

• Use MFA wherever possible
• Use strong passwords if MFA not available
• Don’t write down passwords
• Don’t share passwords
• Don’t reuse passwords
Connect with us!

- structured.com
- 1.800.881.0962
- @StructuredInc

THANK YOU
SECURITY CLOUD
Digital Infrastructure