Enterprise Security Initiative Roadmap

Sunil Rachakonda
As of October 23, 2018
Two-Step Verification
What Does Two-Step Verification Provide?

Provides an extra layer of security to PJM’s single sign on tools

Uses a password and additional information – a token
- Used by banks, government sites and some email providers

Prevents a breach even if a password is successfully compromised

Already in use with PJM’s Account Manager application
How Does Two-Step Verification Work?

- Triggered on logon from an unrecognized device
- Uses a password and email token combination
  - Validated email addresses become essential
  - CAMs will be able to manage email domains (e.g., @pjm.com)
- Leverages valid email addresses
  - PJM will provide a means to manage email domains

Validated email addresses become essential.
CAMs will be able to manage email domains (e.g., @pjm.com).

PJM will provide a means to manage email domains.
Three Easy Steps

1. Sign in
   - Username:
   - Password:
   - Sign In
   - Forgot Password

2. PJM Account Manager Soft Token
   - Account Manager_STG <accountmanager-donotreply@pjm.com>
   - Sent: Mon 10/16/2017 12:08 PM
   - To: 
   - Hello [redacted]
   - You have requested a Soft Token for [redacted]
   - Your Soft Token is 08188826
   - Please return to your browser and enter this token into the form to finish your login.
   - Note that this Soft Token will expire in 10 minutes.

3. Enter Soft Token
   - Finish Login
   - Sign Out
   - Request New Soft Token

NOTICE: This system and the information processed or contained within is for the use of authorized users only. At any time, and for any lawful purpose, PJM may monitor, intercept, record and search any communications or data transmitted or stored on this information system, and may disclose such communications or data to the U.S. Government and its authorized representatives. Anyone using this system expressly consents to the terms and conditions contained in this notice. Individuals using this computer system without authority, or in excess of their authority, are advised that if monitoring reveals possible improper or criminal activity, system personnel may provide the evidence of such monitoring to management or law enforcement officials for disciplinary proceedings and/or criminal and civil proceedings under local and foreign laws.
Post Implementation Updates

Key Stats:
- Logins since September 2018: 21000
- Logins with Two-step Verification: 6800
- Number of calls in first 2 days: 25*

Recurring themes
- Emails in junk folders
- Weren’t expecting emails
- Too many accounts
- Details on impacts
- Too many emails

Next steps
- Redesign UI for clarity
- Continue working on SUMA
Recurring questions

When will the email get to me?

- It can take a few minutes
- An email is sent immediately you log in – no need to click on anything

Will I have to go through this again after a software upgrade?

- Yes. If the upgrade changes settings that are used to identify your browser including version, plugins etc.
• There is an FAQ document on PJM.com
Appendix - Enterprise Security
PJM’s priority is to protect the accounts, data and information entrusted by our members

Critical infrastructure is a higher profile target

- Nation states are increasing their attacks.
- Password spraying has become an effective tool to compromise user accounts.

PJM recognizes member feedback must be incorporated into security approaches
PJM’s Response to Cyber Threats

More restrictive cybersecurity controls

Block network traffic from outside the U.S. and Canada via Geo-IP blocking
PJM’s Approach to Geo-IP Blocking

- Analyze network traffic by country
- Analyze the use of authenticated services by authorized user
- Correlate service use against analysis of traffic by country
- Build up whitelisting for valid, correlated network traffic
- Monitor whitelisting
- Successively block groups of countries based on risk/use
PJM’s Support/Response Approach

- Communicate change process
- Collecting the right feedback to quickly determine username, source IPs, services being accessed, error information, etc.
- An escalation process in place to quickly respond to problems
- Response process for member-related problems
- Regular meetings to review process effectiveness
What Has PJM Done to Date?

PJM has begun implementing Geo-IP blocking with:

- High risk countries
- Limited access to internet SCADA