AVAILABLE
POWER

AP Cyber & The Glarus Group

Response to Request for Information 6540-01-P: Ensuring the Continued Security of the United States Critical Electric Infrastructure

Presented to:

Patricia A. Hoffman, Acting Assistant Secretary
Office of Electricity

Daniel Gregory, daniel.gregory@available-power.com,
+1 (970) 732-2600

JD Hammerly, jd.hammerly@theglarusgroup.com,
+1 (425) 572-5907

Table of Contents

Proposal for Securing the U.S. Transmission System

All 15 critical infrastructures are dependent on the energy sector. Any prolonged disruption in the electricity can cripple our ability to operate our information systems that fuel our economy, way of life, and national security. An electrical outage of more than a few hours causes tangible economic losses and disrupts our digitally-reliant society. In the future, with widespread transportation electrification, an extended outage would bring our country to a standstill.

Decarbonization also lowers dependency on large, centralized generation because geographic generation diversity improves electricity supply flexibility, but it increases reliance on electricity transmission. Transitioning our electricity supply to intermittent renewable resources also increases the need to move electricity across the grid to serve load reliably.

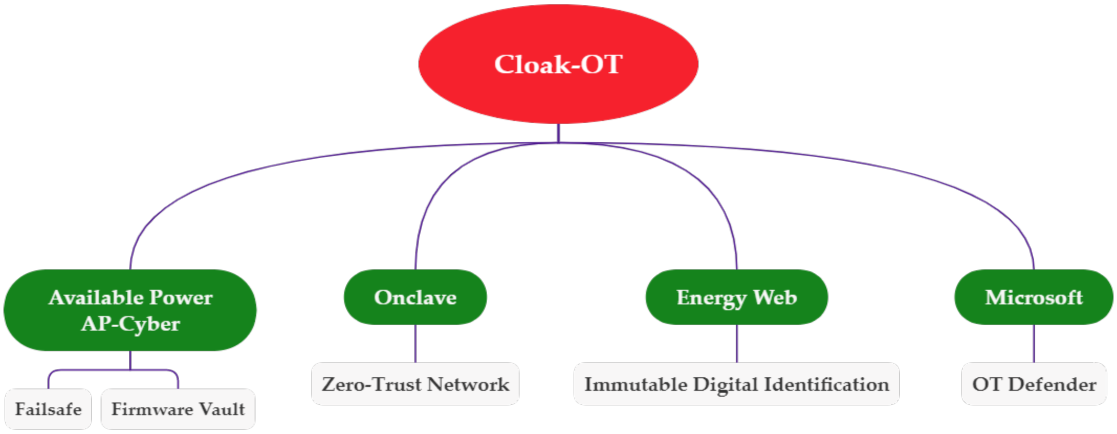
Fortunately, our existing electricity supply system has been exceptionally resilient to natural disasters, operational errors, and physical attacks. But recent events like the Colonial Pipeline cyberattack indicate we cannot assume the electricity supply system's historic reliability will be assured without immediate action to further secure it from cyberattacks.

Transmission grid operation relies on monitoring and controlling geographically dispersed assets. The monitoring and control data is sent across diverse communication media using standard, DNP3, and Modbus protocols. Cyberattacks disrupting this data flow blinds operations and prevent reliable electrical transmission, which threatens extended electrical outages. Just as hope is not a plan, we can no longer rely on "security-by-obscurity" to protect our electric system. Therefore, ensuring dependable and trustworthy data communication, shielded from cyberattacks, becomes paramount to maintain and improve transmission reliability.

The AP-Cyber Cloak-OT™ solution can secure all transmission operations and field assets communication today. The AP-Cyber team – Available Power ("A.P."), Microsoft, Jacobs Engineering, Onclave, Energy Web, Black & Veatch, Chinook Systems – brings the capabilities to design, build, deploy, train, support, and, if need be, operate the solution to secure the U.S. transmission system's operations against cyberattacks.

Central to this solution are the following components:

- ✓ AP-Cyber – solution design and protocol encryption
- ✓ Onclave – Zero-Trust network
- ✓ Energy Web – Immutable Digital Identification
- ✓ Microsoft – Azure Defender for IoT, Azure IoT Hub, Azure Sentinel
- ✓ Jacobs Engineering and Black & Veatch bring extensive experience in cybersecurity and deployment scalability necessary to secure all transmission substations in the United States



Successfully securing the transmission system's operational communications requires both a technical and industry-acceptable solution. The former must address the reality that transmission operators cannot simply replace equipment to secure operational communications. Since only a small percent of transmission assets are replaced annually, some field assets are decades old and cannot be retrofitted to implement rigorous cybersecurity and allow future evolution to respond to new threats. Also, Energy Management Systems (EMS) that control the transmission system is extraordinarily complex, and although upgraded every few years, are only replaced once a decade or longer. Cloak-OT solves this dilemma because it is transparent to the sources and destination of the data flow, not requiring changes to the field assets or the EMS.

The U.S. transmission system is operated by over 100 FERC Transmission Tariff utilities with a clear focus on the need for reliability. This reliability focus makes them cautious and slow to change, even in the face of a tangible threat like cyberattacks. Although spanning 100+ entities, transmission operations is a tight-knit community because our transmission grid is highly interconnected across the U.S. The AP-Cyber team brings access, and more importantly, credibility because of decades of working with these transmission operators.

Cloak-OT™ is ready to deploy today by the AP-Cyber team, which brings the technology and domain knowledge to secure the U.S. transmission system from cyberattacks.

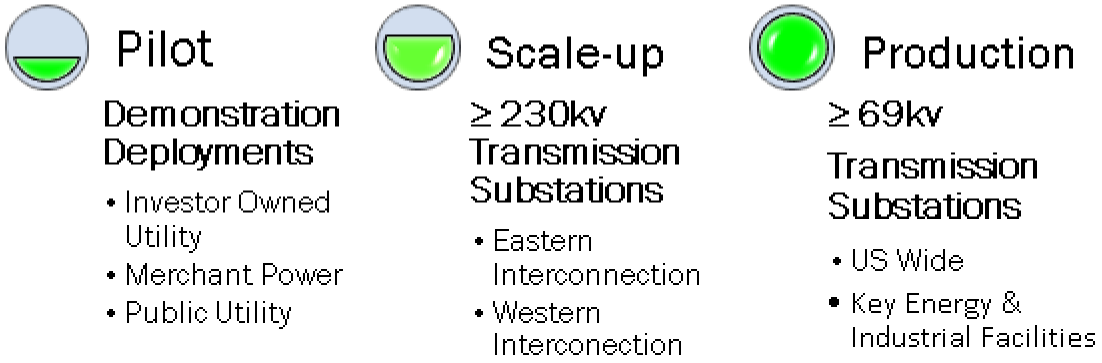
Approach

The AP-Cyber solution will augment proven technology from Onclave (Zero-Trust+ network) and Microsoft (Azure Defender for IoT) with a secure edge-device to create the technology platform that provides secure telemetry. AP-Cyber has patented its edge device and is currently in development. When available, the edge device will add additional security capability to the existing field assets.

Microsoft Azure Defender for IoT identifies all devices connected to the communication system. Through its advanced AI/ML, it creates a profile of each device discovered that Azure Defender for IoT uses to monitor behavioral characteristics such as message content or message frequency. Should behavior change Azure Defender for IoT logs and issues alerts allowing Cloak-OT™ to respond, if need be, shutting communications down.

Cloak-OT™ uses Energy Web’s immutable digital identification to ensure the identity of the message senders and the intended message receiver. Once certain of the sender and receiver identity, Cloak-OT™ employs Onclave Networks, Zero Trust to create a secure message tunnel between the sender and receiver. Further, Zero Trust encrypts all traffic through the tunnel.

Since much of this technology is field-proven and deployable today, rolling out Cloak-OT™ can begin immediately, as shown below.



Pilot

Demonstration Deployments

- Investor Owned Utility
- Merchant Power
- Public Utility

Scale-up

≥ 230kv Transmission Substations

- Eastern Interconnection
- Western Interconection

Production

≥ 69kv

Transmission Substations

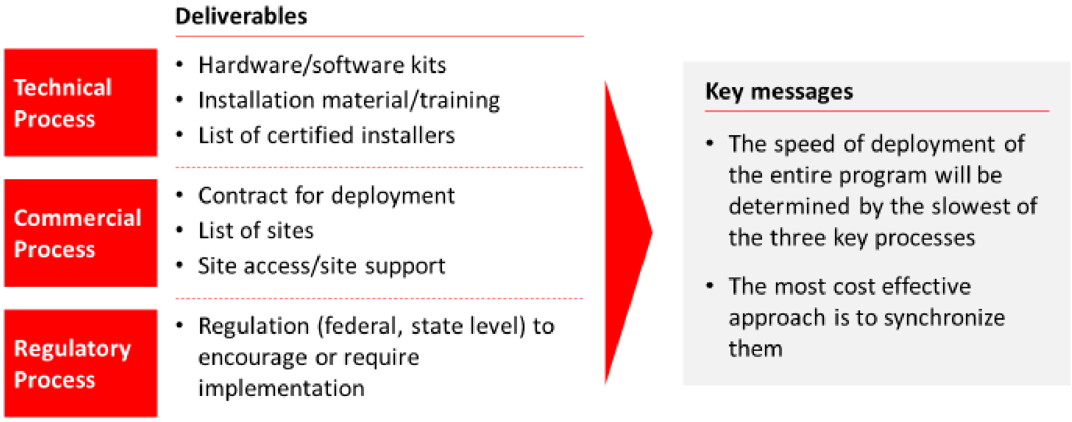
- US Wide
- Key Energy & Industrial Facilities

Jacob’s Engineering will provide testing and security certification. Black & Veatch and Jacob’s Engineering will deploy, commission, and train the users. AP-Cyber Cloak-OT™ will provide necessary monitoring services.

The Cloak-OT™ solution is deployable either as a solution or service.

A.P. Cyber’s vision for this program has three parallel processes: technical development, commercial roll-out, and regulatory coordination.

Rolling up the AP Cyber Protection Program



Deliverables

Technical Process

- Hardware/software kits
- Installation material/training
- List of certified installers

Commercial Process

- Contract for deployment
- List of sites
- Site access/site support

Regulatory Process

- Regulation (federal, state level) to encourage or require implementation

Key messages

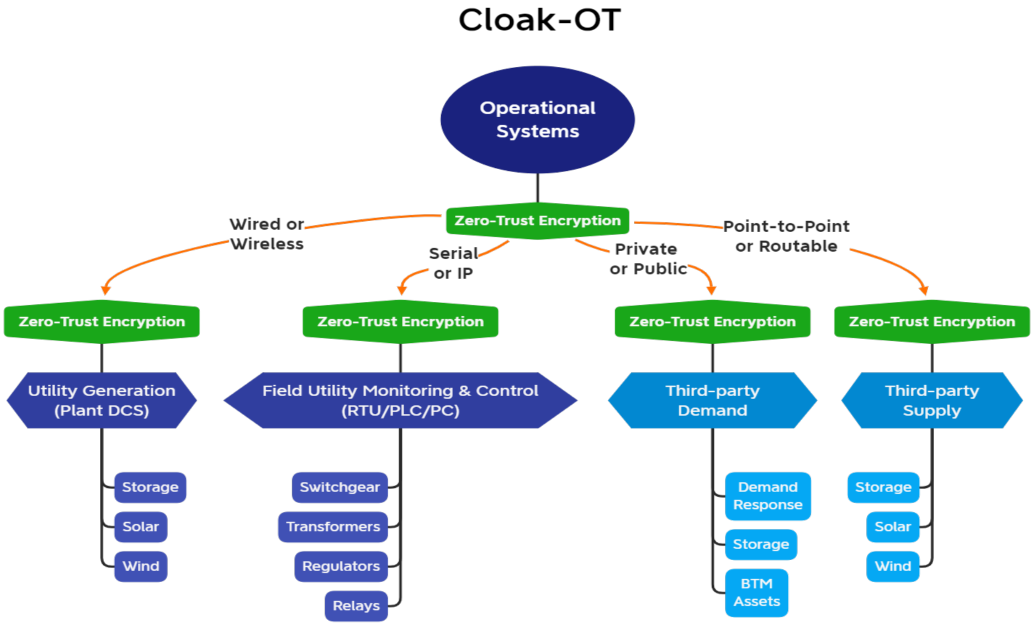
- The speed of deployment of the entire program will be determined by the slowest of the three key processes
- The most cost effective approach is to synchronize them

A.P. Cyber Program Plan

	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023
#Substations-Installations	**3**	**100**	**1,000**	**10,000**	**60,000**
Technical	• Solution Development • Bespoke Sandbox Installations • Testing – Certification	• First Kit Produced • First Installer in place	• Kit Version 2.0 • Installer Manuals – Docs • First Installer Certified	• Production Ramp Up • Inventory • Multiple Installers certified	• Industrialized Production • Cost Reduction • Continuous Improvement on installations
Commercial	• DOE Site Selection • OTA Funding to Kick Start Program	• First Contract • Sites Under Direct DOE Control	• Final Contract • Sites Under Direct DOE Control	• Sites Under Direct DOE Control • Expanded Utility Deployments	• Broad Utility Industry Roll-Out
Regulatory	• DOE Support	• Brief FERC – NERC	• State Engagements 1-2	• FERC Regulations	• Engagement with 3-5 States

Architecture

Shown below is a high-level architecture diagram of the Cloak-OT™.

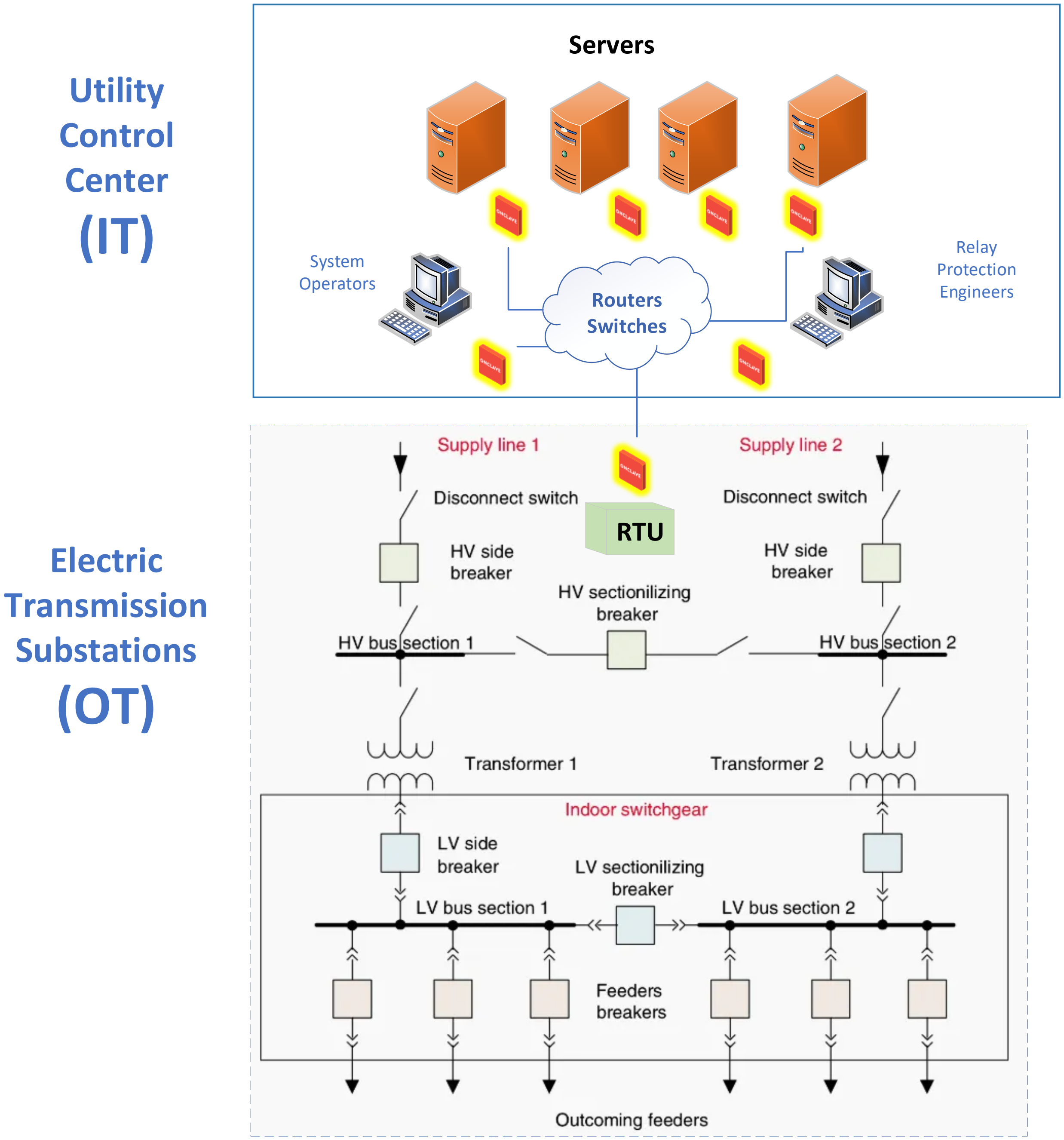


As indicated, the architecture is extendable beyond high voltage transmission systems to enable distributed energy resources connected to utility communications (telemetry).

Supply Chain Protection

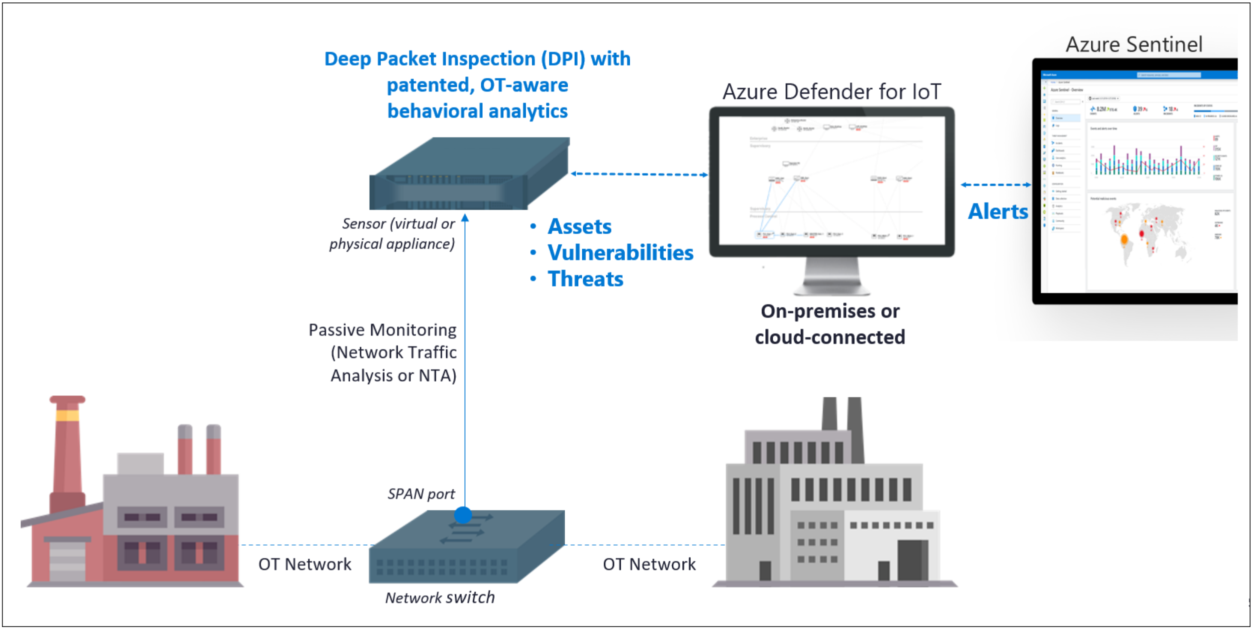
Our solution provides Enterprises, OEMs, and Service Providers with an opportunity to improve supply chain protection against nation-state level attacks with a unique way to secure communications to any endpoint *post-deployment*. This capability is an extension to our Zero Trust platform that will enable Government, Commercial Enterprises, and suppliers of technology and services with the ability to collaborate and improve protection and maintenance while reducing costs.

The Cloak-OT™ detailed solution architecture for securing transmission substations and control is shown in the figure below:

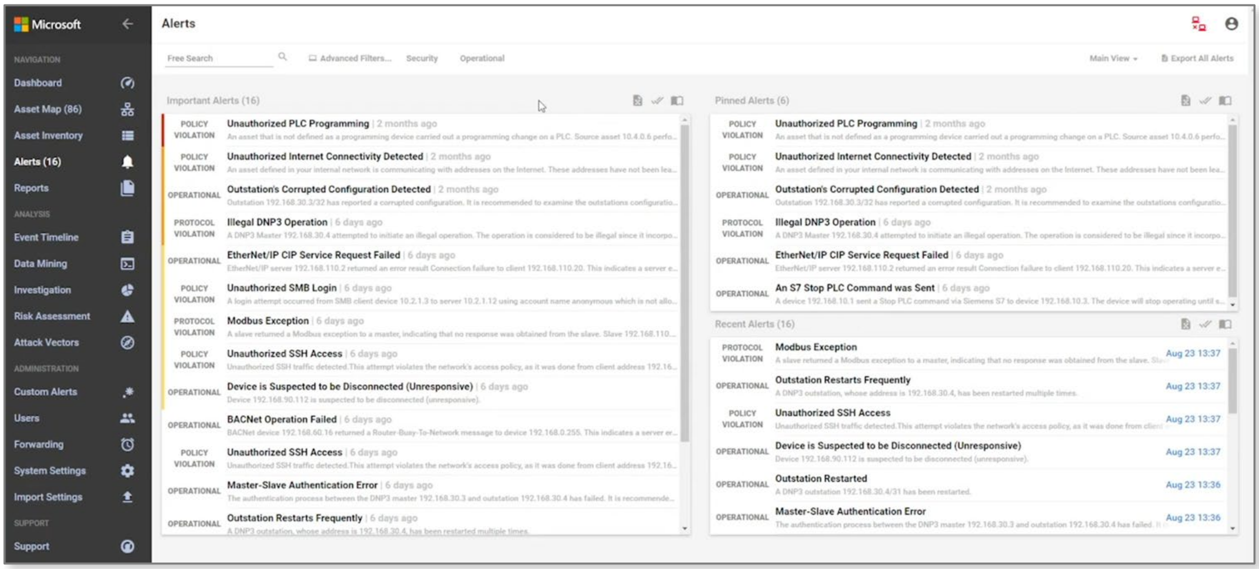


This architecture addresses telemetry, monitoring, and control of the transmission substations and will be extended to include protection and control as well as substation metering.

In the architecture, Azure Defender for IoT will use passive, agentless network monitoring to gain a complete inventory of all IoT/O.T. assets, with zero impact on the IoT/O.T. network. With the ability to analyze diverse industrial protocols to identify device details, including manufacturer, type, serial number, firmware level, and I.P. or Media Access Control (MAC) address. This will visualize the entire IoT/O.T. network topology, see device communication paths, and quickly identify the root cause of operational issues such as misconfigured devices.


Deep Packet Inspection (DPI) with patented, OT-aware behavioral analytics
Azure Defender for IoT
Azure Sentinel
Sensor (virtual or physical appliance)
Assets
Vulnerabilities
Threats
Alerts
On-premises or cloud-connected
Passive Monitoring (Network Traffic Analysis or NTA)
SPAN port
OT Network
OT Network
Network switch

The solution will provide a bird's-eye view across IT/OT boundaries with interoperability with [Azure Sentinel](), Microsoft cloud-native SIEM/SOAR. Automate response with IoT/O.T. playbooks. This will allow the agency to use machine learning and threat intelligence from trillions of signals. Manage your security posture across cloud workloads with [Azure Security Center](), and protect them with extended detection and response (XDR) from Azure Defender.



Important Alerts (16)

POLICY VIOLATION Unauthorized PLC Programming | 2 months ago
An asset that is not defined as a programming device carried out a programming change on a PLC. Source asset 10.4.0.6 perfo...

POLICY VIOLATION Unauthorized Internet Connectivity Detected | 2 months ago
An asset defined in your internal network is communicating with addresses on the Internet. These addresses have not been lea...

OPERATIONAL Outstation's Corrupted Configuration Detected | 2 months ago
Outstation 192.168.30.3/32 has reported a corrupted configuration. It is recommended to examine the outstations configuratio...

PROTOCOL VIOLATION Illegal DNP3 Operation | 6 days ago
A DNP3 Master 192.168.30.4 attempted to initiate an illegal operation. The operation is considered to be illegal since it incorpo...

OPERATIONAL EtherNet/IP CIP Service Request Failed | 6 days ago
EtherNet/IP server 192.168.110.2 returned an error result Connection failure to client 192.168.110.20. This indicates a server e...

POLICY VIOLATION Unauthorized SMB Login | 6 days ago
A login attempt occurred from SMB client device 10.2.1.3 to server 10.2.1.12 using account name anonymous which is not allo...

PROTOCOL VIOLATION Modbus Exception | 6 days ago
A slave returned a Modbus exception to a master, indicating that no response was obtained from the slave. Slave 192.168.110...

POLICY VIOLATION Unauthorized SSH Access | 6 days ago
Unauthorized SSH traffic detected.This attempt violates the network's access policy, as it was done from client address 192.16...

OPERATIONAL Device is Suspected to be Disconnected (Unresponsive) | 6 days ago
Device 192.168.90.112 is suspected to be disconnected (unresponsive).

OPERATIONAL BACNet Operation Failed | 6 days ago
BACNet device 192.168.60.16 returned a Router-Busy-To-Network message to device 192.168.0.255. This indicates a server er...

POLICY VIOLATION Unauthorized SSH Access | 6 days ago
Unauthorized SSH traffic detected.This attempt violates the network's access policy, as it was done from client address 192.16...

OPERATIONAL Master-Slave Authentication Error | 6 days ago
The authentication process between the DNP3 master 192.168.30.3 and outstation 192.168.30.4 has failed. It is recommende...

OPERATIONAL Outstation Restarts Frequently | 6 days ago
A DNP3 outstation, whose address is 192.168.30.4, has been restarted multiple times.

Pinned Alerts (6)

POLICY VIOLATION Unauthorized PLC Programming | 2 months ago
An asset that is not defined as a programming device carried out a programming change on a PLC. Source asset 10.4.0.6 perfo...

POLICY VIOLATION Unauthorized Internet Connectivity Detected | 2 months ago
An asset defined in your internal network is communicating with addresses on the Internet. These addresses have not been lea...

OPERATIONAL Outstation's Corrupted Configuration Detected | 2 months ago
Outstation 192.168.30.3/32 has reported a corrupted configuration. It is recommended to examine the outstations configuratio...

PROTOCOL VIOLATION Illegal DNP3 Operation | 6 days ago
A DNP3 Master 192.168.30.4 attempted to initiate an illegal operation. The operation is considered to be illegal since it incorpo...

OPERATIONAL EtherNet/IP CIP Service Request Failed | 6 days ago
EtherNet/IP server 192.168.110.2 returned an error result Connection failure to client 192.168.110.20. This indicates a server e...

OPERATIONAL An S7 Stop PLC Command was Sent | 6 days ago
A device 192.168.10.1 sent a Stop PLC command via Siemens S7 to device 192.168.10.3. The device will stop operating until s...

Recent Alerts (16)

PROTOCOL VIOLATION Modbus Exception — Aug 23 13:37
A slave returned a Modbus exception to a master, indicating that no response was obtained from the slave. Sla

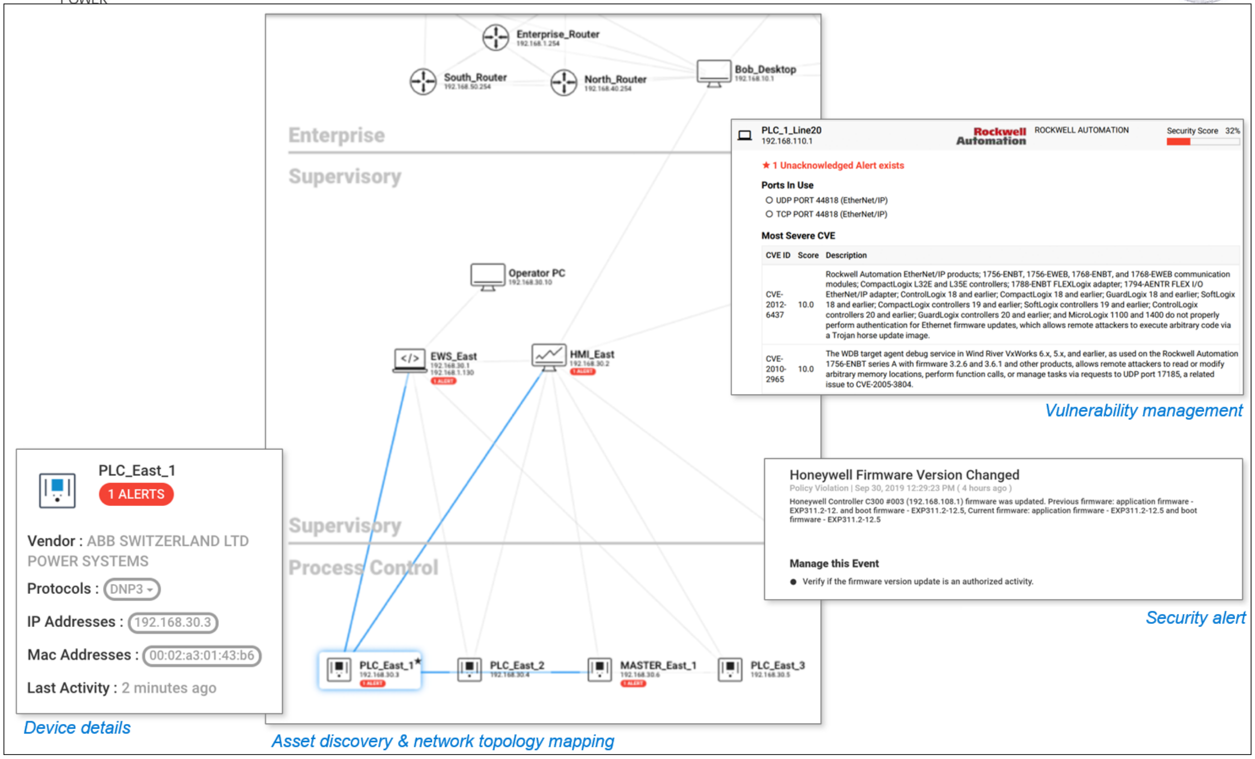
OPERATIONAL Outstation Restarts Frequently — Aug 23 13:37
A DNP3 outstation, whose address is 192.168.30.4, has been restarted multiple times.

POLICY VIOLATION Unauthorized SSH Access — Aug 23 13:37
Unauthorized SSH traffic detected.This attempt violates the network's access policy, as it was done from client

OPERATIONAL Device is Suspected to be Disconnected (Unresponsive) — Aug 23 13:37
Device 192.168.90.112 is suspected to be disconnected (unresponsive).

OPERATIONAL Outstation Restarted — Aug 23 13:36
A DNP3 outstation 192.168.30.4/31 has been restarted.

OPERATIONAL Master-Slave Authentication Error — Aug 23 13:36
The authentication process between the DNP3 master 192.168.30.3 and outstation 192.168.30.4 has failed. It



PLC_East_1
1 ALERTS

Vendor : ABB SWITZERLAND LTD POWER SYSTEMS

Protocols : DNP3

IP Addresses : 192.168.30.3

Mac Addresses : 00:02:a3:01:43:b6

Last Activity : 2 minutes ago

Device details

PLC_1_Line20
192.168.110.1
Rockwell Automation — ROCKWELL AUTOMATION
Security Score 32%

★ 1 Unacknowledged Alert exists

Ports In Use

○ UDP PORT 44818 (EtherNet/IP)
○ TCP PORT 44818 (EtherNet/IP)

Most Severe CVE

CVE ID	Score	Description
CVE-2012-6437	10.0	Rockwell Automation EtherNet/IP products; 1756-ENBT, 1756-EWEB, 1768-ENBT, and 1768-EWEB communication modules; CompactLogix L32E and L35E controllers; 1788-ENBT FLEXLogix adapter; 1794-AENTR FLEX I/O EtherNet/IP adapter; ControlLogix 18 and earlier; CompactLogix 18 and earlier; GuardLogix 18 and earlier; SoftLogix 18 and earlier; CompactLogix controllers 19 and earlier; SoftLogix controllers 19 and earlier; ControlLogix controllers 20 and earlier; GuardLogix controllers 20 and earlier; and MicroLogix 1100 and 1400 do not properly perform authentication for Ethernet firmware updates, which allows remote attackers to execute arbitrary code via a Trojan horse update image.
CVE-2010-2965	10.0	The WDB target agent debug service in Wind River VxWorks 6.x, 5.x, and earlier, as used on the Rockwell Automation 1756-ENBT series A with firmware 3.2.6 and 3.6.1 and other products, allows remote attackers to read or modify arbitrary memory locations, perform function calls, or manage tasks via requests to UDP port 17185, a related issue to CVE-2005-3804.

Vulnerability management

Honeywell Firmware Version Changed
Policy Violation | Sep 30, 2019 12:29:23 PM (4 hours ago)

Honeywell Controller C300 #003 (192.168.108.1) firmware was updated. Previous firmware: application firmware - EXP311.2-12. and boot firmware - EXP311.2-12.5, Current firmware: application firmware - EXP311.2-12.5 and boot firmware - EXP311.2-12.5

Manage this Event

- Verify if the firmware version update is an authorized activity.

Security alert

Asset discovery & network topology mapping

Deliverables

The A.P. Cyber program aims to protect the nation's 70,000+ high voltage (230kV and above) transmission substations within two and a half years, or, in other words, by the end of 2023, provided we get a greenlight by July 1st, 2021.

The program will ramp up progressively, starting with three "sandbox or pilot" installations, with a semestrial scale-up cadence. A preliminary version of the solution will be implemented and tested in these first three sites, deployed further in the next 100 sites. The final version (2.0) of the solution will start deployment after one year, incorporating the learnings from the first 103 installations and further technical development such as the A.P. Cyber OT™ Firewall technology.

A.P. Cyber and its team will install and monitor the operation of the deployment. In parallel, A.P. Cyber will continue discussions with DoD and other federal agencies intending to securitize other critical energy infrastructure.

Proposed Program Cost

A.P. Cyber is proposing that DOE participate in this significant undertaking by supporting the early stage of the program for the first 103 sites and developing version 2.0 of the technical solution. These initial installations will provide the electric transmission industry with a demonstrated solution to securitizing the transmission grid that can be readily and effectively implemented nationwide. DOE's leadership in this program enables near-term success in defending the country's electric grid against harmful intrusions and catastrophic damage to our critical infrastructure.

We propose that the DOE supports this initiative in three ways:

- $4.5M to support the three pilot projects.
- By granting us access to (some of) the first 103 sites – through assets the DOE controls directly (e.g., BPA, WAPA, other).
- $15M to support scale-up for the next 50 sites.

Program Leadership and Contributing Companies

A.P. Cyber (www.available-power.com) leads this program, providing thought and technical innovation addressing the securitization of the nation's electric transmission grid. The company will take this solution for cybersecurity to the utility marketplace.

A.P. Cyber has assembled a world-class team of contributing US-based companies, each of whom plays a critical role in the execution and success of this program. A.P. Cyber also contributes its patent-pending O.T. firewall technology and financing services that will accelerate the penetration into the electric transmission systems in the U.S.

As highlighted in the program organization chart below, these partners are very complementary and have the deep cybersecurity capabilities needed to ensure this program's success. A summary of the contribution to the project and key contact information follows:

AP-Cyber, LLC- (Daniel Gregory, CEO, daniel.gregory@available-power.com, Daniel Constantine Gregory | LinkedIn)

The Glarus Group Inc- (JD Hammerly, CEO, jd.hammerly@theglarusgroup.com, John (J.D.) Hammerly | LinkedIn)

Onclave – (Glen Gulyas, Founder, ggulyas@onclavenetworks.com) – Onclave's scalable ***Zero Trust+*** Networks secure all IT/OT devices and systems are leveraging the same methods and technology as the Department of Defense (DOD) and the U.S. Intelligence Community (I.C.). Continuous monitoring secures these devices and systems from future risks and potential intrusions.

Energy Web - EW – (Doug Miller, Global Markets Lead, doug.miller@energyweb.org) – E.W. provisions immutable digital identities to relevant assets, individuals, and organizations and provides decentralized authorization, authentication, and accounting services to these identities. E.W.'s **Switchboard** platform delivers these services.

Jacobs Engineering – (Bret Muilenburg, VP, bret.muilenburg@jacobs.com) (Adi Karisik, CEO, karisika@jacobs.com) – Jacobs Engineering provides architecture-engineering services for both DoD and private sectors, including software, hardware, firmware, and network system integration for complex systems. Jacob will also provide site selection advice and installation services.

Black and Veatch – (Martin Travers, President, traversmg@bv.com) – Black and Veatch provides engineering and installation services globally, including an extensive list of electric utilities. Its contributions extend from detailed design to implementation to commissioning of cybersecurity solutions and service-level agreements.

Quantico Cyber Hub – (Matt Weaver, Director, matt@cyberbytesfoundation.org) – Quantico Cyber Hub is the largest Cyber Security Center of Excellence, providing innovation and services in thwarting attacks. They will provide testing and security audits for this program.

Chinook – (Wanda Lenkewich, CEO, wlenkewich@chinooksystem.com) – Chinook was extensive experience in commissioning (Cx) facilities in the 16 critical infrastructure sectors. Cybersecurity is integrated into their commissioning and monitoring processes.

Microsoft – (Maryam Rahmani, Senior Security Partner Development, Rahmani.Maryam@microsoft.com, Jorge Diaz, Federal Security Specialist, jodiaz@microsoft.com) Mark McIntyre, Chief Security Advisor-Federal Sector Mark marmci@microsoft.com M.S. provides overall cloud services in their Azure cloud. Including Azure Defender for IoT for IoT anomaly monitoring, Azure IoT Hub, and Azure Sentinel, the industry-leading and cloud-native SIEM/SOAR solution. Additionally, innovative AI/ML profiling tools will enhance monitoring and proactive identification of intrusion or other bad actors' activities and provide proactive automation capabilities to isolate and remediate.

University of Texas Austin – (Dr. Alex Huang, Chair Professor in Power Electronics, aqhuang@utexas.edu) Grid America Center, harmonized with Grid America Cyber Activities. The Grid America Center will work with AP Cyber to validate and independently test the Cloak-OT™ solution.

Idaho National Labs – (Timothy McJunkin, Distinguished Researcher, timothy.mcjunkin@inl.gov) INL will assist UT Austin with testing and independent verification of the solution as part of the Grid America Center Consortium.

Utilities' Interest

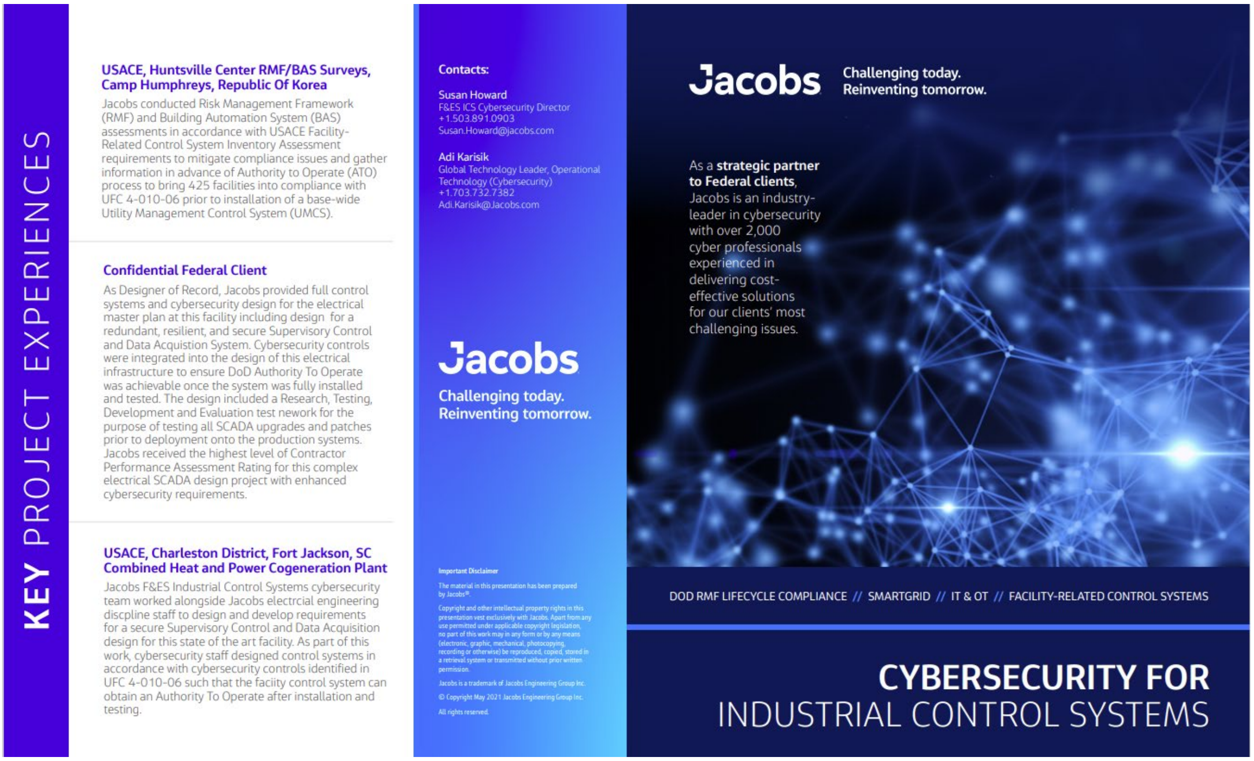
The A.P. Cyber team and its partners have extensive relations with electric utilities in North America and globally. Discussions have started with several major utilities that have expressed interest in pursuing the early proposed sandboxes involving one or more transmission grid substations. Based upon our experience and relationships, the following utilities have been prioritized in our discussions:

- CPS San Antonio – a public municipal utility in Texas known for its innovative technology programs. Additionally, a major military base nearby is and could be a part of the transmission sandbox.
- PJM – this is the largest Regional Transmission Operator in the U.S., serving the Mid-Atlantic and Mid-West states.
- Exelon – is one of the largest utilities in the country, reaching from Chicago to Washington DC. Exelon has expressed keen interest in this program.
- Louisiana Offshore Oil Platform: top 50 U.S. infrastructure in Louisiana managing a large portion of U.S. oil imports.

Exhibits

The Exhibits and Attachments reflect the technology, architecture, and delivery capabilities used to deploy AP Cyber's Cloak-OT™ solution.

Jacob's Engineering



KEY PROJECT EXPERIENCES

USACE, Huntsville Center RMF/BAS Surveys, Camp Humphreys, Republic Of Korea

Jacobs conducted Risk Management Framework (RMF) and Building Automation System (BAS) assessments in accordance with USACE Facility-Related Control System Inventory Assessment requirements to mitigate compliance issues and gather information in advance of Authority to Operate (ATO) process to bring 425 facilities into compliance with UFC 4-010-06 prior to installation of a base-wide Utility Management Control System (UMCS).

Confidential Federal Client

As Designer of Record, Jacobs provided full control systems and cybersecurity design for the electrical master plan at this facility including design for a redundant, resilient, and secure Supervisory Control and Data Acquistion System. Cybersecurity controls were integrated into the design of this electrical infrastructure to ensure DoD Authority To Operate was achievable once the system was fully installed and tested. The design included a Research, Testing, Development and Evaluation test nework for the purpose of testing all SCADA upgrades and patches prior to deployment onto the production systems. Jacobs received the highest level of Contractor Performance Assessment Rating for this complex electrical SCADA design project with enhanced cybersecurity requirements.

USACE, Charleston District, Fort Jackson, SC Combined Heat and Power Cogeneration Plant

Jacobs F&ES Industrial Control Systems cybersecurity team worked alongside Jacobs electrcial engineering discpline staff to design and develop requirements for a secure Supervisory Control and Data Acquisition design for this state of the art facility. As part of this work, cybersecurity staff designed control systems in accordance with cybersecurity controls identified in UFC 4-010-06 such that the faciity control system can obtain an Authority To Operate after installation and testing.

Contacts:

Susan Howard
F&ES ICS Cybersecurity Director
+1.503.891.0903
Susan.Howard@jacobs.com

Adi Karisik
Global Technology Leader, Operational Technology (Cybersecurity)
+1.703.732.7382
Adi.Karisik@Jacobs.com

Jacobs

**Challenging today.
Reinventing tomorrow.**

Important Disclaimer

The material in this presentation has been prepared by Jacobs®.

Copyright and other intellectual property rights in this presentation vest exclusively with Jacobs. Apart from any use permitted under applicable copyright legislation, no part of this work may in any form or by any means (electronic, graphic, mechanical, photocopying, recording or otherwise) be reproduced, copied, stored in a retrieval system or transmitted without prior written permission.

Jacobs is a trademark of Jacobs Engineering Group Inc.

© Copyright May 2021 Jacobs Engineering Group Inc.

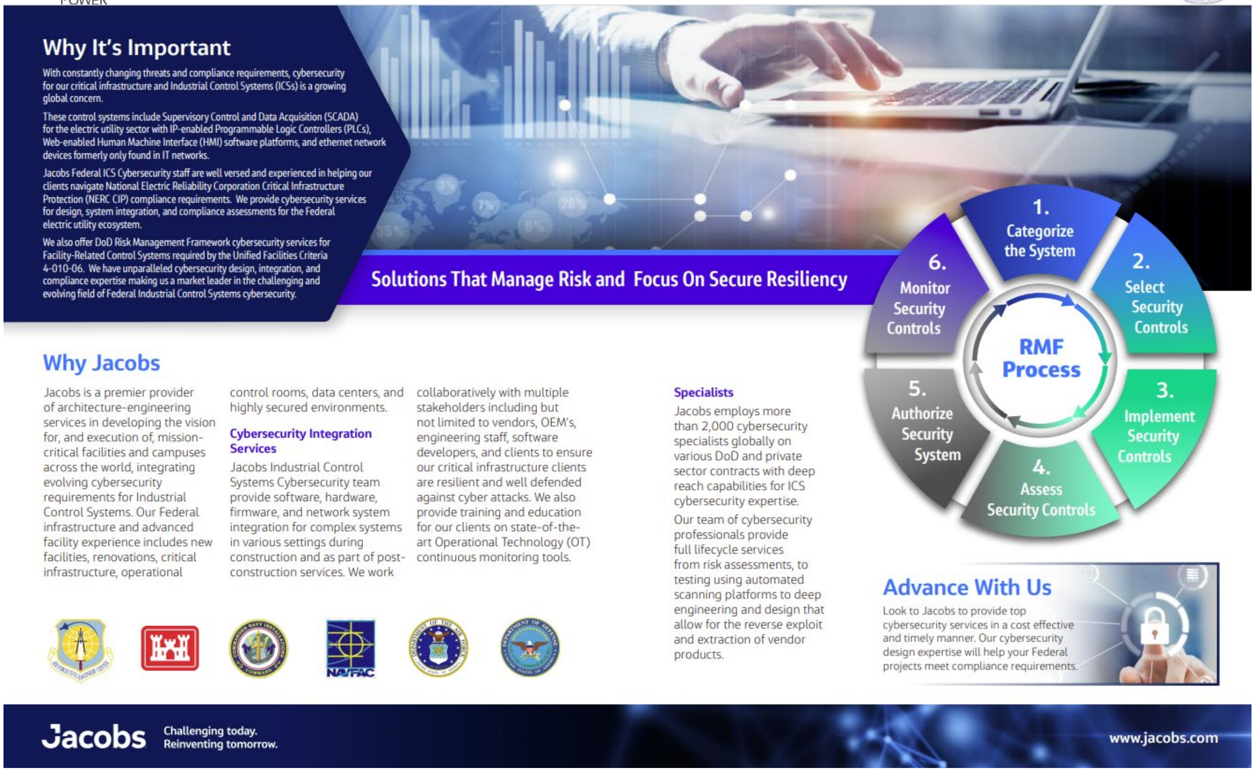
All rights reserved.

Jacobs **Challenging today.
Reinventing tomorrow.**

As a **strategic partner to Federal clients**, Jacobs is an industry-leader in cybersecurity with over 2,000 cyber professionals experienced in delivering cost-effective solutions for our clients' most challenging issues.

DOD RMF LIFECYCLE COMPLIANCE // SMARTGRID // IT & OT // FACILITY-RELATED CONTROL SYSTEMS

CYBERSECURITY FOR
INDUSTRIAL CONTROL SYSTEMS



Why It's Important

With constantly changing threats and compliance requirements, cybersecurity for our critical infrastructure and Industrial Control Systems (ICSs) is a growing global concern.

These control systems include Supervisory Control and Data Acquisition (SCADA) for the electric utility sector with IP-enabled Programmable Logic Controllers (PLCs), Web-enabled Human Machine Interface (HMI) software platforms, and ethernet network devices formerly only found in IT networks.

Jacobs Federal ICS Cybersecurity staff are well versed and experienced in helping our clients navigate National Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) compliance requirements. We provide cybersecurity services for design, system integration, and compliance assessments for the Federal electric utility ecosystem.

We also offer DoD Risk Management Framework cybersecurity services for Facility-Related Control Systems required by the Unified Facilities Criteria 4-010-06. We have unparalleled cybersecurity design, integration, and compliance expertise making us a market leader in the challenging and evolving field of Federal Industrial Control Systems cybersecurity.

Solutions That Manage Risk and Focus On Secure Resiliency

RMF Process
1. Categorize the System
2. Select Security Controls
3. Implement Security Controls
4. Assess Security Controls
5. Authorize Security System
6. Monitor Security Controls

Why Jacobs

Jacobs is a premier provider of architecture-engineering services in developing the vision for, and execution of, mission-critical facilities and campuses across the world, integrating evolving cybersecurity requirements for Industrial Control Systems. Our Federal infrastructure and advanced facility experience includes new facilities, renovations, critical infrastructure, operational control rooms, data centers, and highly secured environments.

Cybersecurity Integration Services

Jacobs Industrial Control Systems Cybersecurity team provide software, hardware, firmware, and network system integration for complex systems in various settings during construction and as part of post-construction services. We work collaboratively with multiple stakeholders including but not limited to vendors, OEM's, engineering staff, software developers, and clients to ensure our critical infrastructure clients are resilient and well defended against cyber attacks. We also provide training and education for our clients on state-of-the-art Operational Technology (OT) continuous monitoring tools.

Specialists

Jacobs employs more than 2,000 cybersecurity specialists globally on various DoD and private sector contracts with deep reach capabilities for ICS cybersecurity expertise.

Our team of cybersecurity professionals provide full lifecycle services from risk assessments, to testing using automated scanning platforms to deep engineering and design that allow for the reverse exploit and extraction of vendor products.

Advance With Us

Look to Jacobs to provide top cybersecurity services in a cost effective and timely manner. Our cybersecurity design expertise will help your Federal projects meet compliance requirements.

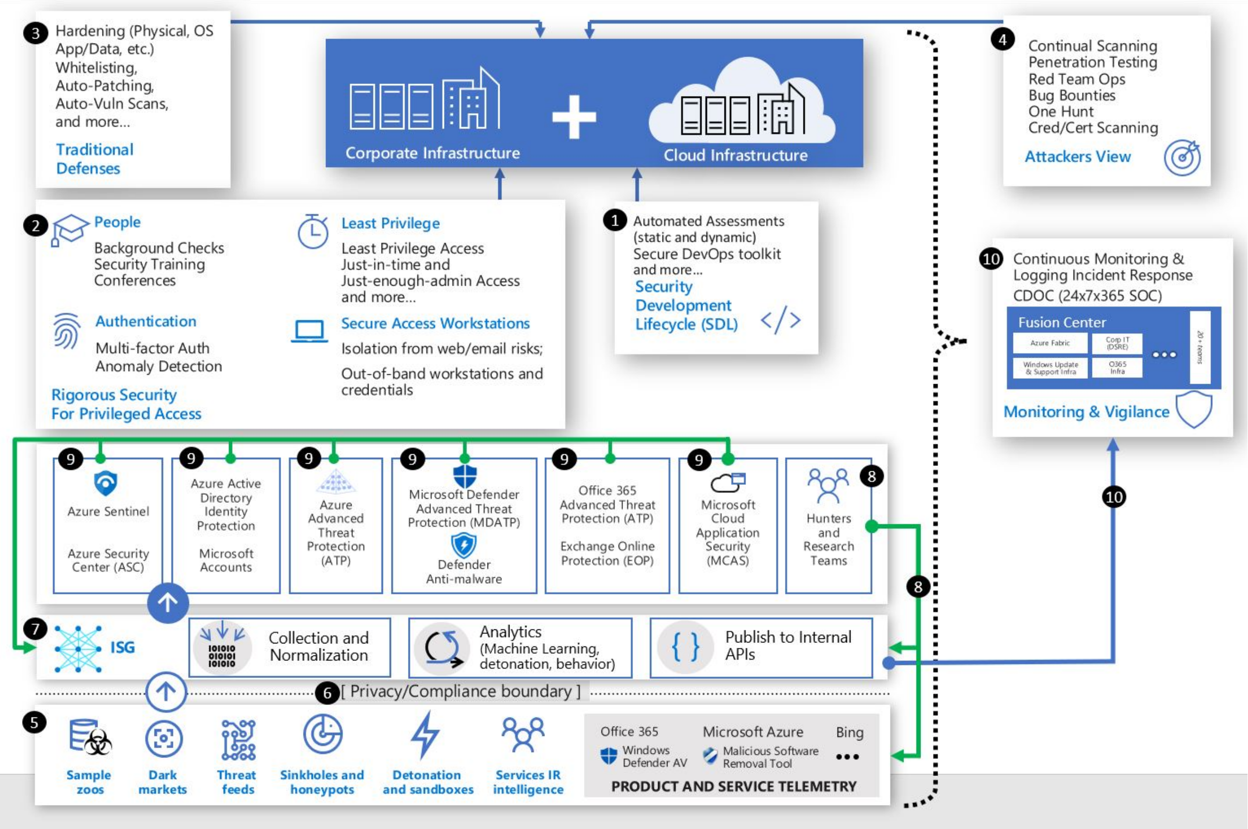
NAVFAC

Jacobs Challenging today. Reinventing tomorrow.

www.jacobs.com

Microsoft Azure Defender for IoT

The Cloud’s-potential to accelerate digital transformation must be balanced by the DOD’s unique security needs. Microsoft will protect the confidentiality, integrity, and availability of DOD data and meet compliance to applicable standards by applying a defense-in-depth-cybersecurity approach from years of experience running critical enterprise services and infrastructure. This is backed by $1b/year investment in cybersecurity personnel and R&D, unparalleled telemetry, and cloud-powered security management tools. Industry analysts have validated our strategy by naming five of our security products as market leaders. We operate highly automated, optimized services with multiple overlapping administrative, technical, and physical controls (see graphic below). The Service Trust Portal demonstrates our commitment to transparency by providing dozens of internal and third-party security reviews, penetration test reports, Azure and O365 SOC audits, NIST 800-53 reports, and other assurance artifacts.


3
Hardening (Physical, OS App/Data, etc.)
Whitelisting,
Auto-Patching,
Auto-Vuln Scans,
and more…
Traditional Defenses
Corporate Infrastructure
Cloud Infrastructure
4
Continual Scanning
Penetration Testing
Red Team Ops
Bug Bounties
One Hunt
Cred/Cert Scanning
Attackers View
2
People
Background Checks
Security Training
Conferences
Authentication
Multi-factor Auth
Anomaly Detection
Rigorous Security For Privileged Access
Least Privilege
Least Privilege Access
Just-in-time and Just-enough-admin Access
and more…
Secure Access Workstations
Isolation from web/email risks;
Out-of-band workstations and credentials
1
Automated Assessments (static and dynamic)
Secure DevOps toolkit
and more…
Security Development Lifecycle (SDL)
10
Continuous Monitoring & Logging Incident Response
CDOC (24x7x365 SOC)
Fusion Center
Azure Fabric
Corp IT (DSRE)
Windows Update & Support Infra
O365 Infra
20 + teams
Monitoring & Vigilance
9
Azure Sentinel
Azure Security Center (ASC)
9
Azure Active Directory Identity Protection
Microsoft Accounts
9
Azure Advanced Threat Protection (ATP)
9
Microsoft Defender Advanced Threat Protection (MDATP)
Defender Anti-malware
9
Office 365 Advanced Threat Protection (ATP)
Exchange Online Protection (EOP)
9
Microsoft Cloud Application Security (MCAS)
8
Hunters and Research Teams
8
10
7
ISG
Collection and Normalization
Analytics (Machine Learning, detonation, behavior)
Publish to Internal APIs
6
[Privacy/Compliance boundary]
5
Sample zoos
Dark markets
Threat feeds
Sinkholes and honeypots
Detonation and sandboxes
Services IR intelligence
Office 365
Windows Defender AV
Microsoft Azure
Malicious Software Removal Tool
Bing
•••
PRODUCT AND SERVICE TELEMETRY

The figure above shows how Microsoft uses multiple preventive administrative, physical, and technical hardening practices to shrink the attack surface. Groups one through four represent foundational ‘prevent and detect’ security practices and controls throughout our company. These are core policies on personnel, policy and automation, and rigorous internal controls that combine to minimize the ability of attackers to exploit ours or our customers’ systems. We readily share security policy documentation, reference architectures and programmatic and technical implementation details on our public website and through other mechanisms, so DOD security teams can use in your development, security management and operational efforts. Examples include:

- **Security Development Lifecycle (SDL):** Security starts from the first line of code, by delivering platforms and applications that are resilient to attack. Consistent with NIST 800-64, SDL is a proven methodology for developing more secure and resilient code. All Microsoft enterprise software services are SDL-compliant. DOD developers can use SDL processes and tools such as automated fuzz testing to build more secure apps and evaluate vendors' apps.
- **Operational Security Assurance (OSA):** OSA offers a cycle of continuous learning that includes continuous Dev/SecOps practices, automated credential and certificate scanning, persistent Red Team (i.e. Insider Threat, External Access, Post-Exploit scenarios) and penetration testing, hunting programs, and Bug Bounty offerings that incentive researchers to protect users by sharing findings with Microsoft.
- **User Access Controls:** Administrators are especially attractive to attackers, so our admins use 'Secure Access Workstations', purpose-built, hardened Windows 10 devices that separates identities and isolates service accounts and functions, complemented by RBAC and granular just-in-time and just-enough-access administrative controls. MSFT admins have zero standing access to customer resources; all requests require authorization; and they are audited. MFA is required. It is important to note that the DOD can implement SAW in your Admin environment to protect these sensitive personnel from phish attacks.

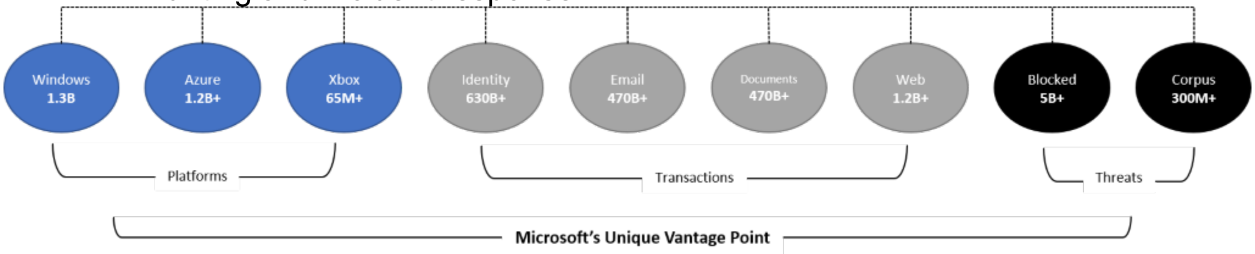
All cybersecurity programs, policies and solutions exist fundamentally to protect data. To help DOD achieve this goal, Microsoft has implemented logical isolation architecture that protects individual tenants--and their data—by providing cryptographic certainty through the following:

- **Encryption of Data at Rest**. Azure Storage Services Encryption (SSE) encrypts all data that is serialized to physical media in Azure Storage, using two layers of NSA-approved encryption, and allows DOD users to control their encryption keys by storing them in a FIPS 140-2/Level 2-validated Hardware Security Modules (HSMs) with Azure Key Vault. BitLocker Drive Encryption secures storage drives throughout Azure infrastructure. BitLocker is implemented using AES 256, and is deployed in conjunction with a Trusted Platform Module (TPM). Microsoft deploys BitLocker to protect storage drives in the Azure Cloud infrastructure at all classification domains and in tactical edge devices.
    - Azure Disk Encryption (ADE) provides the ability to use BitLocker to protect virtual disks when running in Azure or on tactical edge devices. ADE uses KEK (RSA-2048, FIPS certificate stored in Azure Key Vault, to protect the AES-256 key used to encrypt a BitLocker enabled virtual disk. This feature provides an additional layer of protection in which users can control the encryption keys. Users can use Azure Policy to require the use of Azure Disk Encryption as a best practice in addition to the two layers of encryption provided by Azure SSE.
- **Encryption of Data in Transit.** For data in transit Azure uses Transport Layer Security (TLS), I.P. Security (IPSec), Azure Policy, and Azure VPN Gateway, which combine to meet requirement for two layers of encryption using algorithms and procedures.

  - Azure VPN Gateway enables traffic between Azure Virtual Networks (VNETs), tactical edge devices, and other untrusted spaces (e.g. on-premises locations). The VPN Gateway encrypts traffic between endpoints and supports a wide range of FIPS-certified encryption algorithms.
  - Azure Policy with custom machine extensions, can be used to enforce IPSec communications and compliant algorithms to secure IaaS traffic originating from customer applications on V.M.s.
- **Separation of Tenant Network Traffic.** VNETs provide isolation of network traffic between tenants and the foundations of their design enforce this isolation with cryptographic certainty. A workspace can contain multiple logically isolated VNETs, including firewall, load-balancing, and network address translation. Network access to V.M.s is limited by packet filtering at the network edge, at load balancers, in the Azure network fabric and at the host O.S. level.
- **Encryption of Data in Process**: Azure Confidential Computing provides protection for data as it being processed. ACC works by minimizing the Trusted Execution Environment; Microsoft does not have access to encrypted data in processing.

Items four through nine in the graphic above demonstrate the resources that we bring to this fight against attackers. Microsoft operates multiple SOC teams for each business, but the Cyber Defense Operations Center (CDOC) functions as the nerve center for our global cyber monitoring and defense. CDOC is a 24/7/365 team co-located in Redmond, WA and Reston, VA. Security defenders from around the company collaborate in these facilities, monitoring our global infrastructure for threats, regularly running table-top exercises.

- The Intelligent Security Graph (ISG) is a critical capability: ISG is an exobyte-scale big security data cluster that ingests and processes 9T+ cyber events/day from our enterprise and consumer services; it's the industry's largest cyber telemetry capability (see graphic below). Microsoft security teams use the ISG to identify and evict actors and build protections into our products and services.
  - We will provide DOD with API access to augment your SecOps' threat hunting and incident response.



We use sensors built into our own products and services to defend not only Microsoft's enterprise and our cloud infrastructure, but also to offer critical end-to-end detection and response capabilities for the DOD. Our security tools detect and defend on-premises, hybrid and multi-cloud environments, working end-to-end throughout an attacker lifecycle, from attack attempt and initial compromise, through client and infrastructure, to data exfiltration attempt. These technologies are readily available to the I.C. through the "Microsoft 365" suite, and include, but not limited to:

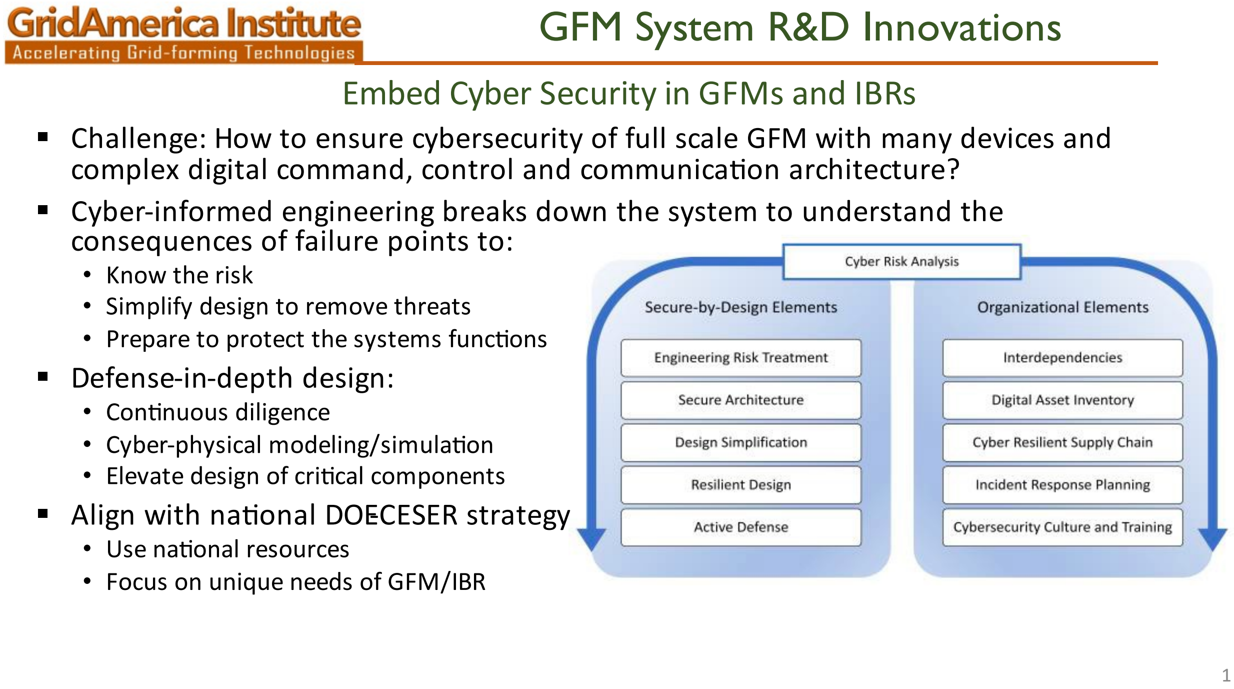
- **Azure Sentinel**, a SIEM/SOAR service that uses the MITRE Attack Framework; I.T. handles Microsoft and third-party logs, reducing DOD dependencies on point solution providers.

- **Azure Security Center** manages hybrid infrastructure configuration, compliance, and security. It will help DOD teams launch and maintain secure infrastructure and monitor configuration errors and drift.
- **Microsoft Defender for Endpoint** offers multi-platform Endpoint Detection and Response (EDR) capabilities. Security Intelligence Updates for MDE Next Generation Protection and the antivirus engine will leverage an approved cross-domain solution to deliver security content to DOD air-gapped clouds.
- **Microsoft Defender for O365** provides pre-breach payload and analysis detonation to prevent malicious content from reaching and executing via O365 on clients.
- **Microsoft Defender for Identity** is a UEBA tool that looks for insider threat activity and suspicious activities involving credentials.
- **Azure Defender for IOT extends traditional I.T. monitoring and detection into your operational technology and IOT ecosystem.**

We use a continual learning approach to defeating cyberattacks: we apply massive telemetry to understand and anticipate attacker activity; rapidly detect and respond to attacks by automation; continuously build learnings, detections and heuristics into our technologies; and constantly train and improve ML/AI algorithms to optimize signal-to-noise. Examples of our experience, scale, and scope of effort include:

- **Scale**: As the world's largest provider of enterprise I.T. services, we experience over 1.6M attacks and at least two global DDoS attacks/day.
- **Automation**: We automate over 97% of tier-one analysis and remediation, freeing up tier-two and -three to focus on more important alerts.
- **Partnerships**: Microsoft maintains partnerships with U.S. government and internal Computer Emergency Response Teams (CERTs), and around the cybersecurity industry. One initiative is the **Government Security Program (GSP)**, through which we provide no-cost programmatic access to cybersecurity threat information, and access to Microsoft security and product engineering teams to support your information assurance and product evaluation needs.
- **People & Teams:** Over 3500 cybersecurity personnel keep Microsoft and our ecosystem as secure as possible; in addition to the CDOC, other important teams are:
    - **Digital Crimes Unit** uses legal enforcement action against criminal actors, for example taking down 19 botnet actors' (mostly Russian) command and control infrastructure. DCU directs this traffic to sinkholes and shares infected host data with the DOD via the GSP and through several of our commercial services within the M365 suite.
    - **Microsoft Threat Intelligence Center** monitors and combats over 100 of the world's leading nation-state and criminal threat actors. Most MSTIC personnel come from U.S. and U.K. national security agencies and work with DOD counterparts. MSTIC's analyses are readily available to the DOD.
    - **Microsoft Defender Research** uses ML/AI capabilities that are built into our products to detect and defeat new malware attacks, in milliseconds; their work has defeated actors such as Bad Rabbit, Emotet, Dofoil, Ursnif and Astaroth.

UT Austin Grid America Institute



GridAmerica Institute
Accelerating Grid-forming Technologies

GFM System R&D Innovations

Embed Cyber Security in GFMs and IBRs

- Challenge: How to ensure cybersecurity of full scale GFM with many devices and complex digital command, control and communication architecture?
- Cyber-informed engineering breaks down the system to understand the consequences of failure points to:
  - Know the risk
  - Simplify design to remove threats
  - Prepare to protect the systems functions
- Defense-in-depth design:
  - Continuous diligence
  - Cyber-physical modeling/simulation
  - Elevate design of critical components
- Align with national DOECESER strategy
  - Use national resources
  - Focus on unique needs of GFM/IBR

Cyber Risk Analysis

Secure-by-Design Elements
- Engineering Risk Treatment
- Secure Architecture
- Design Simplification
- Resilient Design
- Active Defense

Organizational Elements
- Interdependencies
- Digital Asset Inventory
- Cyber Resilient Supply Chain
- Incident Response Planning
- Cybersecurity Culture and Training

1

ATTACHMENTS

Attachment – A: AP's OT endpoint gateway/firewall patent pending.

Attachment – B: Onclave's Zero Trust Network Patent Abstract

Attachment A

AP Cyber’s OT endpoint gateway/firewall patent pending.

DISTRIBUTED ENERGY RESOURCE COMMUNICATIONS GATEWAY AND FIREWALL WITH METHODS FOR PROTECTION AGAINST CYBERATTACK

ABSTRACT

The subject matter herein is a distributed energy resource communications gateway and firewall ("gateway/firewall") for secure monitoring and control of a distributed energy resource or a plurality of distributed energy resources by a cloud-based host computer system and/or an artificial intelligence computer algorithm. The gateway/firewall consists of a combination of electronic components, electromechanical components, communications protocols, firmware, and packaging. Specifically, the gateway/firewall protects a remotely monitored distributed energy resource and/or remotely controlled distributed energy resource against hacking, cyberattack, and unauthorized access. For purposes herein, a distributed energy resource is defined as an electric microgrid, diesel generator, natural gas generator, solar generator, wind generator, battery energy storage system, hydroelectric generator, electric vehicle charging station, inverter, natural gas fuel cell or hydrogen fuel cell, and any form of remote terminal unit or industrial control system that may require remote access.

TECHNICAL FIELD

The subject matter described herein relates to securing electric grid operations, with focus on host computer systems supporting energy management system ("EMS") interfaces to distributed energy resources, distributed management system ("DMS") interfaces to distributed energy resources, supervisory control and data acquisition ("SCADA") interfaces to distributed energy resources, and virtual power plant ("VPP") interfaces to distributed energy resources. For the subject matter herein, the interface protocols to be secured are DNP 3.0 level 1, 2, and 3 plus encryption, IEC-870-5-101, or Modbus RTU. Physical layer media may be via point-to-point hardwire, dedicated radio, broadband, fiber optics, telecom carrier wireless, microwave, cable, laser, or other media. The interface port to the distributed energy resource shall be either serial RS-232-C port or serial RS-485 port, or TCP/IP port.

BACKGROUND

Cyberattacks and undetected intrusions into all types of computer-based systems are prevalent. Electric grid operations are especially vulnerable to such threats. Utilities operate complex cloud-based systems across large areas to manage the electric grids and connected distributed energy resources in real-time. Clearly, the recent news about previously undetected Russian/Chinese intrusions into our government systems and nation's infrastructure constitutes a real and present danger to our national security. Additionally, the widescale deployment of distributed energy resources and electric microgrids may requires expansion of these cloud-based real-time systems to properly utilize and monetize these distributed energy resource assets. The adoption of these advanced technologies, such as virtual power plants, is exciting on many levels, but also adds to the already concerning electric grid vulnerabilities. Therefore, the focus of the subject matter herein is to eliminate the threat of cyberattack on our grids and connected equipment, with particular focus on virtual power plants, distributed energy resources, and electric microgrid vulnerabilities to cyberattack, hacking, and/or undetected intrusions by unauthorized individuals, organizations, or foreign government actors.

SUMMARY

The gateway/firewall described herein is specifically designed to eliminate the possibility of any form of unauthorized remote access to the control and monitoring of distributed energy resources connected to the electric grids or operating islanded from the grid but still remotely controlled and/or monitored. For example, a plurality of distributed energy resources may be connected to a virtual power plant for the purpose of enabling power trading on an open market, such as Texas ERCOT, by a third party. The gateway/firewall described herein will protect each distributed energy resource connected to the virtual power plant from hacking or any form of unauthorized access. The primary method of eliminating the possibility of any form of cyberattack, hacking, or unauthorized digital intrusion to the protected distributed energy resources is to embed the required protocol into a dedicated “system-on-a-chip” custom processor. All programming to support the functionality required to monitor and control each distributed energy resource will be “hardcoded” in firmware into nonvolatile memory managed by the system-on-a-chip. No user programming or software-based configuration of the gateway/firewall will be available remotely or locally. All user configurations will be limited to enabling or disabling a limited number of features via on-board dipswitch selection. For example, each gateway/firewall will support three protocols, DNP 3.0, IEC-870-5-101, and Modbus RTU. A dipswitch setting will enable either DNP3.0, IEC-870-5-101, or Modbus RTU protocol. Additional settings will select the communications port type for both the host computer interface and the distributed energy resource interface (i.e., serial or TCP/IP). If DNP 3.0 protocol is selected, another switch will set the option for level 1, 2, or level 3, and another switch will enable or disable encryption, and so on. In all cases, the options selected by the user shall be limited to preprogrammed functions implemented by factory personnel in firmware and burned into EPROM or EEPROM. No user programmable memory, including flash memory, disk drive, or other user writeable programmable memory will be employed in the gateway/firewall. Therefore, no one can programmatically modify the executive program, kernel, operating system, or functionality of the gateway/firewall. However, the EPROM or EEPROM shall be socketed on the gateway/firewall circuit board to facilitate field modification. The gateway/firewall shall contain predefined protocol input/output maps, with dipswitch settable options, to passthrough all protocol commands and requests via a RS-232-C/RS-485 serial port to the distributed energy resource control system, remote terminal unit, metering system, or monitoring system, as directed by the DNP 3.0, IEC-870-5-101, or Modbus RTU host computer system. Standard firewall features such as authentication, denial of service prevention, anti-cloning protection, and other best practices will be implemented as required. The specific purpose of the gateway/firewall is to secure the connected distributed energy resource from hacking, cyberattack, or any form of unauthorized access that may cause misoperation, damage, or loss of function of the connected distributed energy resource. Note that the subject matter herein may be applied to applications other than protecting distributed energy resources. For example, the subject matter herein may be applied to protect similar systems to distributed energy resources, such industrial control systems, remote terminal units, protective relays, substation automation networks, substation gateways, and power plant automation networks.

DISTRIBUTED ENERGY RESOURCE COMMUNICATIONS GATEWAY AND FIREWALL WITH METHODS FOR PROTECTION AGAINST CYBERATTACK

BRIEF DESCRIPTION OF DRAWINGS

Preferred embodiments of the subject matter described herein will now be explained with reference to the accompanying drawings of which:

Figure 1 is a schematic diagram of a gateway/firewall according to an embodiment of the subject matter described herein.

Figure 2 is an architecture diagram of a host computer system connected to a gateway/firewall according to an embodiment of the subject matter described herein.

DETAILED DESCRIPTION

The subject matter described herein is an application specific gateway/firewall that prevents cyberattack, hacking, and unauthorized access to distributed energy resources that communicate via DNP3.0 protocol over TCP/IP or serial port, IEC-870-5-101 protocol over TCP/IP or serial port, or Modbus RTU protocol over TCP/IP or serial port. Specifically, the subject matter herein eliminates a remote user's ability to modify the gateway/firewall and connected distributed energy resource systems in any manner whatsoever. Further, a local user cannot programmatically modify the gateway/firewall. The gateway/firewall employs a "system-on-a-chip" CPU running a firmware kernel that supports all features and functions. The kernel, DNP3.0 protocol stack, IEC-870-5-101 protocol stack, Modbus RTU protocol stack, and the user configuration including the input/output map and communications port settings, is stored in nonvolatile EPROM or EEPROM computer memory mounted in an onboard socket. Use of random access memory is limited to supporting kernel functions and buffering of protocol read/write commands and corresponding data in a FIFO stack. A watchdog timer is employed to ensure that the CPU and computer memory is functioning properly. The watchdog timer maintains power to an onboard single pole double throw latching relay during normal operation. The relay coil output is wired in series with the gateway/firewall power supply and is normally closed. The relay will latch open due to loss of power supply from the watchdog timer if the gateway/firewall CPU stops operating for any reason. Reasons for the relay coil to latch open include gateway/firewall power supply failure, kernel lockup, self-diagnostic alarm, random access memory overflow, failure of the nonvolatile memory chip, or removal of the nonvolatile memory chip from its socket. The output of the relay shall be hardwired to an external system, such as a remote terminal unit, sequence-of-events recorder, protective relay, or other monitoring system or intelligent electronic device capable of monitoring the watchdog timer relay coil output. In the event that the watchdog timer relay latches open resulting in power supply interruption to the gateway/firewall, the host computer system shall alert operators to dispatch personnel to the location of the gateway/firewall to diagnose the problem and manually reset the watchdog timer relay thus restoring remote communications with the host computer system. Diagnostic procedures that are to be conducted prior to local personnel resetting the watchdog timer latching relay of the gateway/firewall may include at a minimum determination if the gateway/firewall was tampered with, replaced with an alternate unauthorized device, or damaged. Note that the gateway/firewall will be custom made by authorized vendors only and under strict license control and the nonvolatile memory chip will be programmed and supplied by the original manufacturer only. Specifically, the source code for the kernel of the gateway/firewall will be written from scratch inhouse, kept secret, and protected from distribution, license, or resale. However, it is feasible that a person could obtain a valid gateway/firewall from inventory, replace the factory supplied nonvolatile memory chip with a rouge program, and place the corrupted gateway/firewall in service during a new install without detection. Therefore, a provision is made for the "system-on-a-chip" CPU of the gateway/firewall to verify the validity of the kernel firmware during bootup. The details of such provision shall remain secret.

FIGURE 1 BASIC SCHEMATIC BLOCK DIAGRAM OF GATEWAY/FIREWALL

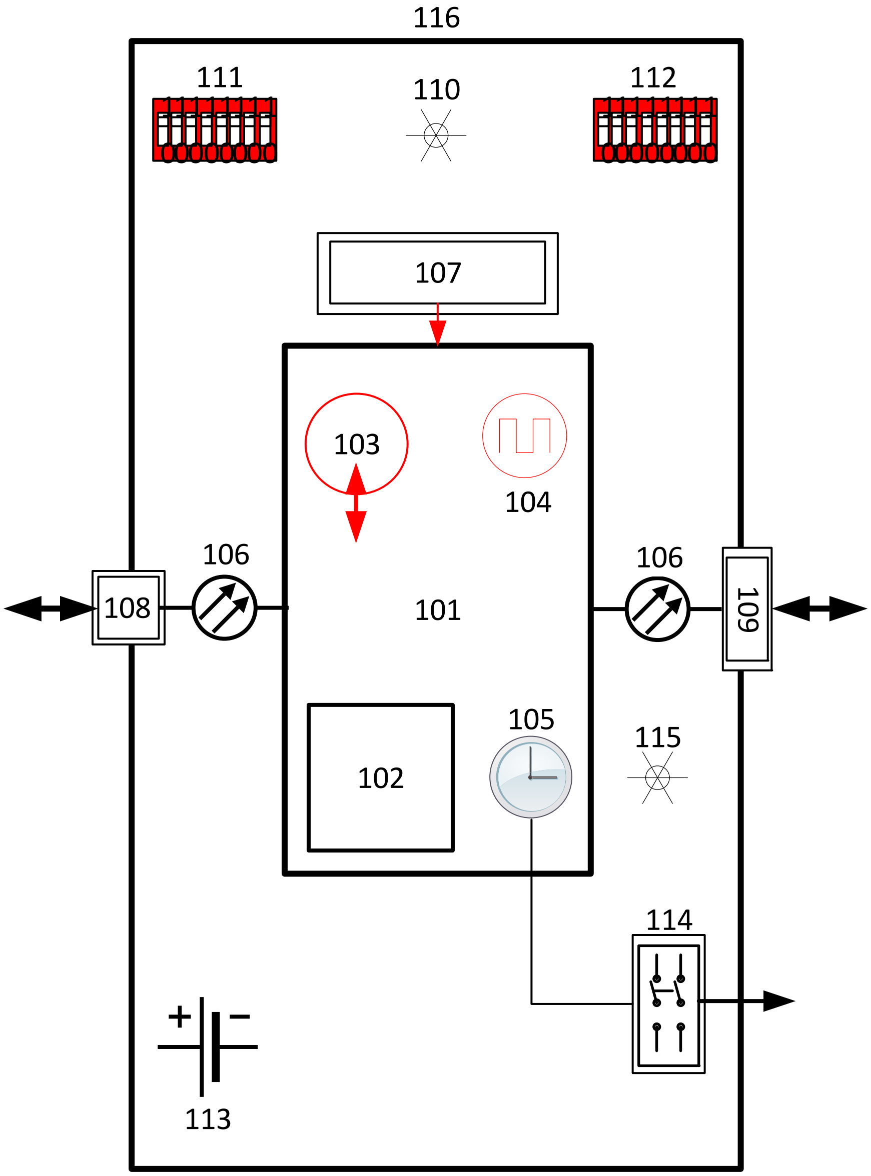


TABLE 1 KEY TO FIGURE 1

101 SYSTEM-ON-A-CHIP WITH INTERNAL INTERFACE BUS

102 PROCESSOR
103 RANDOM ACCESS MEMORY
104 CLOCK
105 WATCHDOG TIMER
106 OPTICAL ISOLATOR
107 NON-VOLATILE MEMORY (E.G., EPROM, EEPROM)
108 TCP/IP PORT
109 SERIAL PORT (RS-232-C, RS-485)
110 SELF DIAGNOSTIC INDICATOR LED
111 DIP SWITCH FOR DNP3.0, IEC 870-5-101, AND MODBUS RTU PROTOCOL SETTINGS
112 DIP SWITCH FOR TCP/IP AND SERIAL PORT SETTINGS
113 DC POWER SUPPLY
114 SINGLE POLE DOUBLE THROW LATCHING RELAY FOR POWER RESET AND EXTERNAL MONITORING
115 WATCHDOG TIMER FAULT INDICATOR
116 CIRCUIT BOARD

SYSTEM ARCHITECTURE

The gateway/firewall shall connect via its on-board TCP/IP port to a TCP/IP network router, network switch, or equivalent device. The TCP/IP router enables the gateway/firewall to connect to the host computer system by supporting the end user standards and practices for network security. Standards and practices which shall be supported by the gateway/firewall include MAC address, authentication, denial-of-service prevention, fixed IP address and subnet mask, VPN support, and other features as required by the end user. Note that these standards and practices may be customized and burned-in to the nonvolatile memory chip, as required by the end user. Alternatively, the gateway/firewall shall include a standard set of network features and allow the end user to set IP address and subnet mask via on-board dipswitch settings. Network settings cannot be set by programmatically in any case.

The gateway/firewall shall connect to the distributed energy resource via Modbus RTU, IEC870-5-101, or DNP 3.0 protocol over serial port connection. TCP/IP connection between the communication firewall and the distributed energy resource is not recommended but shall be supported. Careful end-user network security management is required if the gateway/firewall and a distributed energy resource or plurality of distributed energy resources are connected via TCP/IP on a local area network. Note that telecommunications carrier systems no longer support or are moving away from point-to-point leased communications service and POTS lines in favor of network connections. Further, distributed energy resources typically support Modbus RTU, DNP3.0, or IEC-870-5-101 over serial port. Therefore, the gateway/firewall also serves as a gateway between telecommunications carrier system network ports and distributed energy resources that do not support TCP/IP connectivity but do support serial port connectivity.

FIGURE 2 SYSTEM ARCHITECTURE

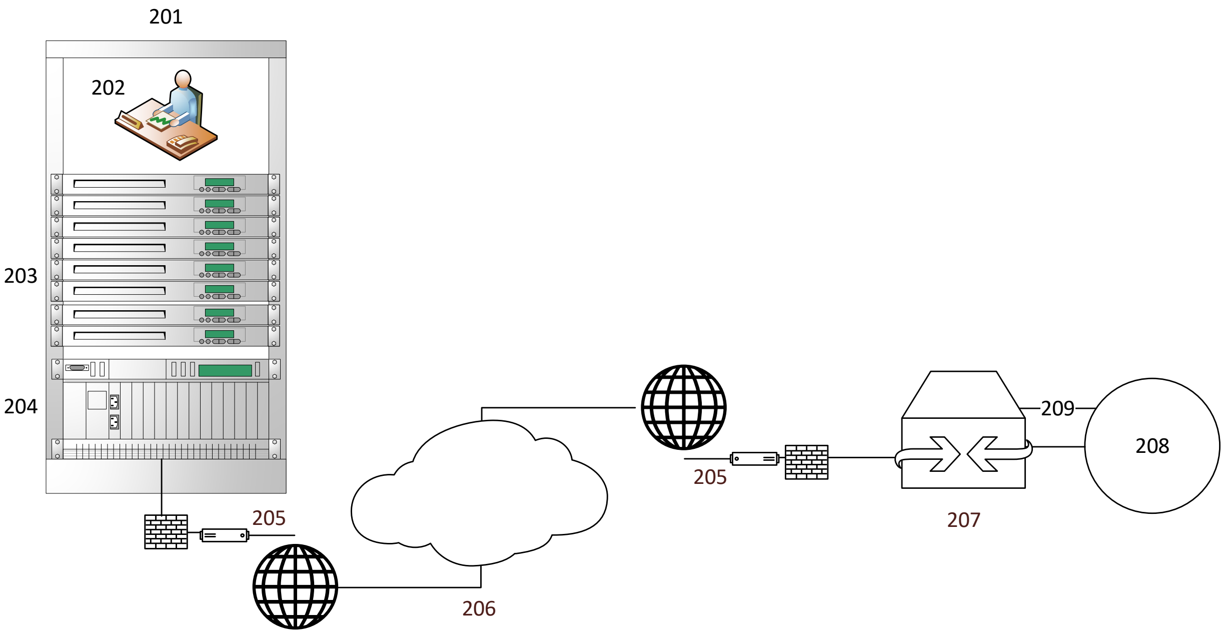


TABLE 2 KEY TO FIGURE 2

201 HOST COMPUTER SYSTEM SUPPORTING EMS, VPP, DMS, SCADA FUNCTIONS
202 OPERATOR/DISPATCHER
203 COMPUTER SERVERS
204 APPLCIATIONS, ALGORITHMS, AI APPLCIATIONS
205 TCP/IP ROUTER WITH GENERAL PURPOSE FIREWALL WITH VIRTUAL PRIVATE NETWORK
206 INTERNET CLOUD
207 GATEWAY/FIREWALL
208 DISTRIBUTED ENERGY RESOURCE WITH DNP3.0, IEC 870-5-101, OR MODBUS RTU SERIAL PORT
209 WATCHDOG TIMER RELAY OUTPUT TO THIRD-PARTY INTELLIGENT ELECTRONIC DEVICE INPUT

PLAUSIBLE APPLCIATIONS

The subject matter herein describes an application specific gateway/firewall for protecting distributed energy resources, as defined above. Generally, the gateway/firewall as described herein shall protect against cyberattack or similar “hacking” threats to any computer control and/or monitoring system that communicates via DNP3.0, IEC-870-5-101, or MODBUS RTU over a TCP/IP network. Such control and/or monitoring systems may include industrial control systems, programmable logic controllers, SCADA remote terminal units, water and wastewater control systems, factory automation systems, distributed control systems, transportation control systems, and many other systems that rely on remote monitoring and/or control.

MANDATORY FEATURES

The following features are unique to the subject matter herein:

1. No programmatic user modifications to the gateway/firewall are supported.
2. User configuration of the gateway/firewall options are set by electromechanical means (e.g., dipswitch, jumpers).
3. The gateway/firewall employs a dedicated kernel operating system, not a generic operating system (e.g., Linux, Microsoft).
4. The gateway/firewall employs no third-party software, drivers, or applications.
5. To prevent tampering, a latching relay controlled by a watchdog timer interrupts power to the gateway/firewall preventing further interaction with the distributed energy resource until the latching relay is manually reset.
6. In its highest security configuration, the gateway/firewall connects to the distributed energy resource via a serial port connection over Modbus RTU, DNP3.0, or IEC-870-5-101. The gateway/firewall connects to the host computer or local area network via TCP/IP port connection over Modbus RTU, DNP3.0, or IEC-870-5-101. This configuration provides no means for a remote user to access the distributed energy resource system's user configuration, memory functions, or other means by which a remote user could access the distributed energy resource, thus providing a physical layer barrier between the remote user and the distributed energy resource.
7. The gateway/firewall employs firmware techniques and features that shall remain secret.
8. End users may opt to specify a proprietary version of the gateway/firewall firmware which shall be designed and implemented by the factory only.
9. The gateway/firewall shall be designed to operate with minimal CPU and memory resources with little or no extra resources available. In some embodiments, this design technique may require that the firmware be implemented as efficiently as possible (e.g., machine code), further impeding a third-party from modifying the gateway/firewall firmware by adding new code.
10. The CPU shall employ a secret algorithm to verify the firmware authenticity during bootup and periodically verify during normal operation. The gateway/firewall shall fail safe and latch open the onboard relay in case the firmware authenticity check fails for any reason whatsoever.

DISTRIBUTED ENERGY RESOURCE COMMUNICATIONS GATEWAY AND FIREWALL WITH METHODS FOR PROTECTION AGAINST CYBERATTACK

CLAIMS

What is claimed is:

1. A method for securely monitoring and controlling a distributed energy resource as described herein.

2. The method according to claim 1, including each and every novel feature or combination of features disclosed herein.

3. The method according to claim 1, wherein the secure monitoring and control of the distributed energy resource is executed via a gateway and/or firewall device.

4. A system for securely monitoring and controlling a distributed energy resource as described herein.

5. The system according to claim 4, including each and every novel feature or combination of features disclosed herein.

6. The system according to claim 4, wherein the system includes a gateway and/or firewall device configured for the secure monitoring and control of the distributed energy resource.

7. A computer-readable storage medium having computer-executable instructions stored thereon which, when executed by one or more processors, cause one or more computers to perform functions for securely monitoring and controlling a distributed energy resource as described herein.

8. The computer-readable storage medium of claim 7, including each and every novel feature or combination of features disclosed herein.

9. The method according to claim 1, wherein the secure monitoring and control of the distributed energy resource is executed via a gateway and/or firewall device.

Attachment B

Onclave's Zero Trust Network Patent

United States Patent Application	***20200112430***
Kind Code	**A1**
Taylor; James ; et al.	**April 9, 2020**

Systems and Methods for Deployment, Management and Use of Dynamic Cipher Key Systems

Abstract

Dynamic Cipher Key Management (DCKM) of the present invention enables the protection of sensitive electronic data by assigning symmetric or asymmetric cipher keys using a process that delivers the cipher key to a network endpoint device by means of a key installation, delivery, and storage methodology. DCKM may negate the need to physically touch the network device under protection. Further, DCKM's process is based on a set of operating principles that maintains the highest levels of assurance that the cipher key pairs are issued with only devices that have the right and authorization to create a secure communication path. The DCKM process realizes the same level of security confidence that is only achieved today with conventional token based key management services with respect to the paired devices linked via a cipher key public and private relationship.

Inventors: **Taylor; James**; *(Potomac Falls, VA)* **; Dwyier; John**; *(Chantilly, VA)* **; Lawn; Joseph**; *(Arlington, VA)* **; Gulyas; Glen**; *(Arlington, VA)*

Applicant:

Name	City	State	Country	Type
Taylor; James	Potomac Falls	VA	US	
Dwyier; John	Chantilly	VA	US	
Lawn; Joseph	Arlington	VA	US	
Gulyas; Glen	Arlington	VA	US	

Family ID:	**62064108**
Appl. No.:	**16/705518**
Filed:	**December 6, 2019**

Related U.S. Patent Documents

<td< td="" style="color: rgb(0, 0, 0); font-family: "Times New Roman"; font-size: medium; font-style: normal; font-variant-ligatures: normal; font-variant-caps: normal; font-weight: 400; letter-spacing: normal; orphans: 2; text-align: start; text-indent: 0px; text-transform: none; white-space: normal; widows: 2; word-spacing: 0px; -webkit-text-stroke-width: 0px; text-decoration-thickness: initial; text-decoration-style: initial; text-decoration-color: initial;"></td<><td< td=""

style="color: rgb(0, 0, 0); font-family: "Times New Roman"; font-size: medium; font-style: normal; font-variant-ligatures: normal; font-variant-caps: normal; font-weight: 400; letter-spacing: normal; orphans: 2; text-align: start; text-indent: 0px; text-transform: none; white-space: normal; widows: 2; word-spacing: 0px; -webkit-text-stroke-width: 0px; text-decoration-thickness: initial; text-decoration-style: initial; text-decoration-color: initial;"></td<><td< td="" style="color: rgb(0, 0, 0); font-family: "Times New Roman"; font-size: medium; font-style: normal; font-variant-ligatures: normal; font-variant-caps: normal; font-weight: 400; letter-spacing: normal; orphans: 2; text-align: start; text-indent: 0px; text-transform: none; white-space: normal; widows: 2; word-spacing: 0px; -webkit-text-stroke-width: 0px; text-decoration-thickness: initial; text-decoration-style: initial; text-decoration-color: initial;"></td<><td< td="" style="color: rgb(0, 0, 0); font-family: "Times New Roman"; font-size: medium; font-style: normal; font-variant-ligatures: normal; font-variant-caps: normal; font-weight: 400; letter-spacing: normal; orphans: 2; text-align: start; text-indent: 0px; text-transform: none; white-space: normal; widows: 2; word-spacing: 0px; -webkit-text-stroke-width: 0px; text-decoration-thickness: initial; text-decoration-style: initial; text-decoration-color: initial;"></td<>

Application Number	Filing Date	Patent Number
15668521	Aug 3, 2017	
16705518		
62370567	Aug 3, 2016	

Current U.S. Class:	**1/1**
Current CPC Class:	H04L 63/0428 20130101; H04L 63/06 20130101; H04L 63/062 20130101; H04L 9/3234 20130101; H04L 63/0272 20130101; H04L 9/0861 20130101; H04L 2209/38 20130101; H04L 9/0877 20130101; H04L 9/14 20130101; H04L 9/3236 20130101
International Class:	H04L 9/08 20060101 H04L009/08; H04L 29/06 20060101 H04L029/06; H04L 9/32 20060101 H04L009/32; H04L 9/14 20060101 H04L009/14

Claims

1. A method of creating a secure communications channel across the Internet or other network environment comprising: providing a secure blockchain based application on a computing device having one or more transactional applications; providing a cryptographic communications module for use by the secure blockchain based application using a hashing function from the cryptographic communications module as a seed to create a cipher trust key in conjunction with the one or more of the transactional applications; establishing a trust relationship between two or more computing devices based on the cipher trust key; using a network interface device to couple a trusted computing device to one or more remote trusted computing devices

over the network; and creating a secure communications channel between the trusted computing device and the one or more remote trusted computing devices.

2. The method of claim 1 further comprising posting a unique identity record containing a cipher trust key in a private blockchain node.

3. The method of claim 1 further comprising using one or more unique cipher keys to enable the segmentation of a private blockchain using a linking set of hashes.

4. The method of claim 3 further comprising enabling a previous segment of the private blockchain to be archived without compromising the integrity of new cipher trust keys.

5. The method of claim 4 wherein the enabling further comprises archiving an active segment of the private blockchain, wherein a new hash for linking an archived segment to the existing active segment of the blockchain is created.

6. The method of claim 4 wherein the enabling further comprises updating the private blockchain based on changes to a remote device, which includes one or more of the following: a cipher trust key, network address, operational characteristics, and availability.

7. The method of claim 1 wherein the cryptographic communications module comprises, at least in part, specialized semiconductor circuitry device.

8. The method of claim 7 wherein the specialized semiconductor circuitry device is a secure device deployed at an endpoint node.

9. The method of claim 7 wherein the specialized semiconductor circuitry device is tamper-resistant and includes one or more of the following: a public/private key pair (Endorsement Key); a Storage Root Key (SRK); and Attestation Identity Key (AIK).

10. The method of claim 5 further comprising an application that can retrieve transactions in archived private blockchain segments.

11. The method of claim 5 further comprising an application that determines a point in time to write a new transaction into an active private blockchain segment.

12. The method of claim 5 further comprising an application that can determine if the time required to perform a transaction in an active private blockchain segment is too long, and if so, trigger an archive operation for that segment.

13. The method of claim 5 further comprising preconfiguring the secure blockchain based application on some master devices, slave devices, or other devices that write or read transactions in the private multi-segment blockchain.

14. The method of claim 5 further comprising registering the secure blockchain based application into a private multi-segment blockchain in order to create additional transactions based on changes to a device's state.

15. The method of claim 5 further comprising creating a custom ledger in a private multi-segment blockchain using an identity record that contains state and/or cipher trust keys for master and slave devices with the secure blockchain based application that are a part of a master/slave trust relationship.

16. The method of claim 5 wherein network devices have a unique transaction ledger for all of their secure blockchain based applications and each manufacturer have their own private multi-segment blockchain node.

17. The method of claim 5 further comprising an application that reads a state of the master device and slave device, and using a deterministic model establishing an action to create a trust relationship between the master and slave devices.

18. The method of claim 5 further comprising identifying master slave device pairs in a network.

19. The method of claim 1 for protecting security of electronic data transmitted across a network comprising: identifying a master device coupled to the network; identifying a slave device coupled to the network; selectively pairing the slave device and the master with one another; and dynamically generating a session cipher key at the master device and the slave device when electronic data is transmitted such that a secure data path is created between the master device and the slave devices.

Description

PRIORITY CLAIM

[0001] This application is a continuation of U.S. patent application Ser. No. 15/668,521 filed Aug. 3, 2017 which claims priority from U.S. provisional application Ser. No. 62/370,567 filed on Aug. 3, 2016 the contents of which are hereby incorporated by reference in its entirety.

BACKGROUND OF THE INVENTION

[0002] In cryptography, a cipher is typically an algorithm for performing encryption or decryption. This is usually a series of well-defined steps that can be followed as a procedure. An alternative, but less common term is encipherment. To encipher or encode is to convert information into cipher or code. In common parlance, "cipher" is synonymous with "code", as they are both a set of steps that encrypt a message; however, the concepts are distinct in cryptography, especially classical cryptography.

[0003] Codes generally substitute different length strings of characters in the output, while ciphers generally substitute the same number of characters as are input. There are exceptions and some cipher systems may use slightly more, or fewer, characters when output versus the number that were input.

[0004] Codes operated by substituting according to a large codebook which are linked to a random string of characters or numbers to a word or phrase. For example, "UQJHSE" could be the code for "Proceed to the following coordinates." When using a cipher the original information is known as plaintext, and the encrypted form as ciphertext. The ciphertext message contains all the information of the plaintext message, but is not in a format readable by a human or computer without the proper information or mechanism to decrypt it.

[0005] The operation of a cipher usually depends on a piece of auxiliary information, called a key (or, in traditional NSA parlance, a cryptovariable). The encrypting procedure is varied depending on the key, which changes the detailed operation of the algorithm. A key must be selected before using a cipher to encrypt a message. Without knowledge of the key, it is extremely difficult, if not impossible, to decrypt the resulting ciphertext into readable plaintext.

[0006] Most modern ciphers can be categorized in several ways. For example, they may work on blocks of symbols (block ciphers) usually of a fixed size, or on a continuous stream of symbols (stream ciphers). In some cases, the same key is used for both encryption and decryption (symmetric key algorithms), or if a different key is used for each (asymmetric key algorithms). If the algorithm is symmetric, the key must be known to the recipient and sender and to no one else. If the algorithm is an asymmetric one, the enciphering key is different from, but closely related to, the deciphering key. If one key cannot be deduced from the other, the asymmetric key algorithm usually has a public/private key property and one of the keys may be made public without loss of confidentiality.

[0007] In a symmetric key algorithm (e.g., DES and AES), the sender and receiver must have a shared key set up in advance and which is kept secret from other parties. The sender uses this key for encryption, and the receiver uses the same key for decryption. One type of cipher, the Feistel cipher uses a combination of substitution and transposition techniques. Most block cipher algorithms are based on this structure. In an asymmetric key algorithm system (e.g., RSA), there are two separate keys: a public key that is published and enables any sender to perform encryption, while a private key is kept secret by the receiver and enables only him to perform correct decryption.

[0008] Cipher block chaining (CBC) is a mode of operation for a block cipher (one in which a sequence of bits are encrypted as a single unit or block with a cipher key applied to the entire block). Usually in an iterative way. Cipher block chaining uses what is known as an initialization vector (IV) of a certain length. One of its key characteristics is that it uses a chaining mechanism that causes the decryption of a block of ciphertext to depend on all the preceding ciphertext blocks. As a result, the entire validity of all preceding blocks is contained in the immediately previous ciphertext block. A single bit error in a ciphertext block affects the decryption of all subsequent blocks. Rearrangement of the order of the ciphertext blocks causes decryption to become corrupted. Basically, in cipher block chaining, each plaintext block is digitally processed using an exclusive OR (XOR) operation on the immediately previous ciphertext block, and then encrypted.

[0009] Within the construct of the aforementioned encryption and decryption methods for cypher keys, three forms of key management are typically employed. The method of deployment maps to the need and scale of the cypher key requirements

[0010] Native Key Management tools utilize the basic key management capabilities that are native to the individual encryption product or products being deployed. Localized Key Management tools better manage risk and ensure control of the entire cipher key life cycle. Centralized Key Management are used in larger scale deployments where the scale of the key management requirements necessitate the automation of the cipher key life cycle and the amalgamation of key management policies. This approach establishes a demarcation between the cipher key management tasks performed centrally and the endpoint device functions where the keys are actually used.

[0011] The existing forms of key management have several drawbacks in so far as; efficient deployment of cypher keys, human intervention in the deployment of new cypher keys, and risks in how the keys themselves are issued. In the case of Centralized Key Management, most require either a public or private Certificate Authority that issues public or private certificates used to establish a key pair. There is a considerable amount of human intervention during this period and cost for public keys when securing these certificates. Further, since the certificate can be easily hijacked, a man-in-the-middle attack (MITM) is far more likely.

SUMMARY OF THE INVENTION

[0012] It is therefore an object of the present invention to provide systems and methods that provide secure management of cipher keys across a network.

[0013] It is therefore also an object of the present invention to provide systems and methods that provide secure management of cipher keys across large and very large computer network.

[0014] It is therefore an object of the present invention to provide systems and methods that provide secure management of cipher keys across a network without periodic human intervention.

[0015] It is therefore also an object of the present invention to provide secure dynamic cipher key management to enable the secure communication of trusted devices.

[0016] It is therefore also an object of the present invention to provide an amalgamated rule based cipher key management policy that adheres to the NIST Special Publication 800-57 Part 1 Revision 4 guidelines while providing dynamic creation and delivery of cipher keys.

[0017] It is therefore also an object of the present invention to store and forward private keys utilizing the present invention's private multi-segment Blockchain technology for extremely large scale key management of endpoint devices.

[0018] These and other objects of the present invention are accomplished by providing methods apparatuses that, in one embodiment, allow a computer network system to store and forward cipher keys using a blockchain decryption approach that provides a scalable cipher key management environment and robust deployment and maintenance over large and very large networks. This established a way to create a novel safe and adaptable network environment for the exchange of electronic information over a cryptographically secured network connection.

[0019] Other aspects of the invention are directed toward enabling the protection of sensitive electronic data by assigning symmetric or asymmetric cipher keys, based on certain commonly used cipher algorithms, using a novel process that delivers a cipher key to a network endpoint device by means of a novel key installation and delivery methodology. Such embodiments may employ the Dynamic Cipher Key Management (DCKM) system of the present invention as further described herein.

[0020] In at least some embodiments, DCKM enabled network devices will fully or partially negate the need to physically touch the network device.

[0021] Further, processes in accordance with certain paradigms of the present invention, which can include DCKM, may be based on a set of operating principles that maintains high levels of assurance that cipher key pairs are issued substantially exclusively (or exclusively) with devices that have both the right and authorization to create a secure communication path. The DCKM process realizes the same (or higher) level of security confidence that is only achieved today with conventional token based key management services with respect to the paired devices linked via a cipher key public and private relationship.

[0022] In some embodiments, the DCKM system of the present invention will work with various known cipher algorithms such as AES, DES, TripleDES as well as the two major types of public-key ciphers used today: Diffie-Hellman and RSA. However, other similar or suitable cipher algorithms may be used if desired. The DCKM system using the various know cipher algorithms will also have its own root of trust negating the need for public or private Certificate Authorities.

BRIEF DESCRIPTION OF THE DRAWINGS

[0023] The above and other objects and advantages of the present invention will be apparent upon consideration of the following detailed description, taken in conjunction with the accompanying drawings, in which like reference characters refer to like parts throughout, and in which:

[0024] FIG. 1A is a generalized block system diagram illustrating a typical LAN-WAN-LAN link that connects Segment 1 to Segment 2 via a layer 3 switch over the Internet.

[0025] FIG. 1B is a generalized block system diagram illustrating a LAN-WAN-LAN link of in accordance with aspects of the present invention.

[0026] FIG. 1C is a generalized block system diagram illustrating a LAN-WAN-LAN link of the present invention that illustrates the extensibility of the Master/Slave devices and that Point to Point and Point to Multi Point key management can be easily implemented.

[0027] FIG. 2 shows a flow chart illustrating some of the steps involved in establishing an authorized user with a master device in accordance with one embodiment of the present invention.

[0028] FIG. 3 shows a flow chart illustrating some of the steps involved in pairing a master and slave device in accordance with one embodiment of the present invention.

[0029] FIG. 4 show a flow chart illustrating some of the steps involved in establishing a unique private blockchain in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0030] Prior art systems use a number of methods to create a key pair that can be used to establish cryptographic sleeves between devices. The most common is the Public Key Infrastructure (PKI). Once a PKI structure is established, each entity wishing to communicate securely is required to physically prove his or her identity to a Registration Authority (RA). This identity-proving process requires the presentation of proper credentials. After establishing the correct identity, an individual then generates a public static key pair. Each individual that generates a key pair is considered to be the owner of that key pair. The public key of the key pair is provided to the RA, where it is incorporated with the key-pair owner's identifier and other information into a digitally signed message for transmission to a Certification Authority (CA). The CA then composes the key-pair owner's public-key certificate by signing the owner's public key and the identifier, along with other information. This certificate is returned to the key-pair owner or placed in a certificate repository or both. The private key remains under the sole control of the owner. Two types of public key certificates are commonly used: certificates used for key establishment (i.e., key agreement or key transport) and certificates used for digital signatures.

[0031] In the case of key-agreement certificates, two entities wishing to communicate may exchange public-key certificates containing public static key-agreement keys that are checked by verifying the CA's signature on the certificate (using the CA's public key). The public static key-agreement key of each of the two entities and each entity's own private static key-agreement key are then used in a key-agreement scheme to produce a shared secret that is known by the two entities. The shared secret may then be used to derive one or more shared symmetric keys to be used by a symmetric algorithm to provide confidentiality and/or integrity protection for data. The receiver of the data protected by the symmetric key(s) has assurance that the data came from the other entity indicated by the public-key certificate (i.e., source authentication for the symmetric keys has been obtained).

[0032] PKI is a very labor-intensive key management entity requiring human intervention in the establishment of key pairs. The nature of PKI precludes its use in environments that require the protection of data in motion to the millions of devices commonly known as the Internet of Things (IoT).

[0033] One embodiment of the present invention provides greater protection against man-in-the-middle attacks and leverages a new approach integrated with a Trusted Platform Module (TPM) chip providing the seed for the hash generation. This approach provides the highest level of security and removes all human intervention after the initialization of the pairing of a master and slave device.

[0034] This new and novel architecture approach assures the independent security of the protected enclave and furthers the management of switching the slave device ON or OFF based on the policy of the enclave.

[0035] Since each TPM chip has a substantially unique and secret key burned in as it is produced, it can be used to perform platform authentication. This moves activation from a physical key to a highly scalable and independent endpoint configuration, as in the ability to switch out, or exchange, cameras within an enclave.

[0036] Using TPM chips provide a number of benefits that include: [0037] Their ability to generate cryptographic keys, and limit the key's use by policy. [0038] Remote attestation--creates a nearly unforgeable hash key summary of the hardware and software configuration. The program hashing the configuration data determines the extent of the summary of the software. This allows a third party to verify that the software has not been changed. [0039] Binding--encrypts data using TPM bind key, a unique RSA key descended from a storage key. [0040] Sealing--encrypts data in a similar manner to binding, but in addition specifies a state in which TPM must be in, in order for the data to be decrypted (unsealed).

[0041] DCKM of the present invention provides a cipher key management framework that enables expansion of a cryptographic secure enclave by enabling the dynamic addition of slave devices linked to a common master with a trust relationship as shown in FIG. 1C.

[0042] One embodiment of the invention may use a process that distinguishes the present invention from the prior art is that it creates a framework and establishes a rule based state transition methodology which may impose mutual consent and a set of actions based on the current state of involved network devices that are negotiating with each other in the data transfer process. In some embodiments, these rules dictate that substantially all parties including devices and operators have been trusted in advanced by participating organizations that are providing the devices. In certain embodiments, acquiring parties of the devices must identify at least one trusted operator of the devices purchased.

[0043] FIG. 1A is a generalized block system diagram illustrating a typical prior art LAN-WAN-LAN link that connects Segment 1 to Segment 2 via a layer 3 switch over the Internet. In this depiction, there is no protection of the links between the two segments. Accordingly, the packets traversing the WAN connection can easily be captured and used to penetrate either segment and any devices or endpoints that may exit on those segments.

[0044] FIG. 1B is a generalized block system diagram in accordance with aspects of the present invention illustrating a LAN-WAN-LAN link that connects Segment 1 to Segment 2 via a layer 3 switch and participating DCKM devices providing layer 2 over layer 3 encryption over the internet. The Master/Slave devices could be third party manufactured devices using the DCKM system for key management. In accordance with one embodiment of the present invention, the Master/Slave devices would establish a trust relationship between themselves, only after an authorized user (administrator) of the Master device was authenticated to perform DCKM Key Management. After authorization, the user could establish which slave devices would be used to create a secure cryptographic tunnel between the participating slave devices, thus creating a secure enclave invisible to the anyone or anything on the internet.

[0045] FIG. 1C is a generalized block system diagram in accordance with aspects of the present invention illustrating a LAN-WAN-LAN link that connects Segment 1, Segment 2, and Segment 3 via layer 3 switches and participating DCKM devices providing layer 2 over layer 3 encryption over the internet. This illustrates the extensibility of the Master/Slave devices and that Point to Point and Point to Multi Point key management can be easily implemented.

[0046] FIG. 2 shows a flow chart 200 illustrating some of the steps involved in establishing a dynamic cipher key management framework in accordance with one aspect of the invention ("DCKM"). At step 202, an operator (such as an administrator that is given a user name and password to the master device) is identified as linked to a specific master device. A master device may be, for example, a layer 2 encryptor or any similar or other suitable hard wired network or mobile device capable of establishing a secure cryptographic tunnel using a key pair exchange. Next, at step 204, the operator may be assigned to the master device as an authorized operator (i.e., an operator that can securely communicate across the network through the master device using the DCKM technology described herein). Collectively, steps 202 and 204 may be thought of as a "pre-operational phase" and are labeled as step 206. In some embodiments, these steps may be performed sequentially or together (substantially in parallel).

[0047] After step 206 is complete, the master device may be paired with one or more slave device (s) to establish secure communicate paths through a network such as the Internet, a WAN of LAN. The slave device could be a network element that contains one or more RJ45 network connections and has the TPM chip to establish a trust relationship along with a CPU to perform encryption and decryption between other slave devices and the master device. Next, at step 208, when an organization implements the DCKM solution of the present invention to establish a cipher key pair between a master device and a slave device, the organization first registers one or more of its members as users which are identified to the network as operators of the master device. Lastly, at step 210 the master devices may be registered to one or more users as an administrator.

[0048] In the framework described in FIG. 2, implementation of the DCKM system of the present invention is typically dependent having an authorized operator, at least one master device and one or more slave devices.

[0049] In some embodiments, it is contemplated that an organization which employs a DCKM framework would first acquire DCKM enabled devices. Such devices may have a pre-installed DCKM software application ("app") and/or certain specific hardware and/or firmware to perform the required DCKM functions. In some embodiments, these devices may have the capability to communicate with each other using conventional network connectors such as BNC, RJ45 etc. over network cables such CAT5 or CAT6 which may use IPV4, IPV6 or any other appropriate network communication protocols. However, any suitable or desirable hard wired or wireless connection may be used if desired (e.g., fiber optic, WiFi etc.).

[0050] In other embodiments, certain pre-existing network devices may be configured to be DCKM compliant, for example, by installation of a secure application, either by direct interaction ("hands on" hardware or software installation) or secure remote installation (software, firmware or configurable hardware such as FPGA, etc.).

[0051] One approach to managing dynamic cipher keys (sometimes referred to herein as "key") in a network in accordance with one aspect of the present invention is shown in flow chart 300 of FIG. 3. As shown, at step 302 the state of one or more master devices may be determined. This may include key type, initialization vector and current key state information. Next, at step 304 slave devices associated with the master device may be determined. This may include slave device type, network location (IP address etc.) and whether the identified device is DCKM compliant or needs to be configured as such.

[0052] If no slave devices are recognized, the master device may request to pair with certain slave devices (step 306). Such a request may be generated by polling available (slave) devices by device type, network location, and DCKM status and/or configuration. Once slave devices have been identified, the state of the master and slave devices may be determined. If the slave device is paired with the master already, then the user can invoke commands to establish a secure cryptographic tunnel with the master and all other slave devices pair with the master on the same "VLAN". In this case, the term VLAN may apply to a specific cryptographic tunnel from 1 to 4096 that a master can uniquely segment from other slave devices that the master is paired with.

[0053] Next, at step 310 the user requests from the master the state of slave device to determine if it is available or not. This may be accomplished by exchanging state information on the slave device that indicates the status of the slave device. The state information of the device can be exchanged with any master device with or without a trusted relationship between the two devices. If the slave device is not paired with another master device, then the master device can establish a trusted relationship with the slave device and the slave device enters a state of "PAIRED". Once determined, in some embodiments, the key state of the master and slave may be synchronized such that they may generate common outcomes based on similar or identical input (e.g., depending on key type, symmetric, asymmetric, etc.).

[0054] At this point, a deterministic model/policy may be used to determine and dynamically issue a cipher key to the master and slave the devices to ensure the secure delivery of electronic data to the desired endpoint in the network via a secure transmission channel (step 312). Such deterministic models may include any suitable known such models such as, but not limited to AES (Advanced Encryption Standard), DES (Data Encryption Standard), Triple DES, Diffie-Hellman, RSA or any other suitable technique. Communication between master, slave and endpoint will be governed by workflow outcomes (e.g., outcome of encoding/decoding process) and both master and slave will invoke/create the appropriate actions and responses based on this model.

[0055] In some embodiments, the rule based cipher key management policy used in accordance with aspects of the present invention may comply with the guidelines set forth in the NIST Special Publication 800-57 Part 1 Revision 4 for providing dynamic creation and delivery of cipher keys, which is hereby incorporated by reference in its entirety.

[0056] For example, in operation, paired master slave devices may transfer encoded electronic data based on a symmetric or asymmetric encryption key common to these devices. Such keys may be locally generated and dynamically deployed by the DCKM module in the master/slave device during (or prior to) data transfer by the module in advance of or during the data transfer. Thus, substantially each time data is transferred, a new key is dynamically generated, thereby creating a secure communication path, making key interception and ciphertext decoding exceptionally difficult.

[0057] Embodiments of the invention using a deterministic model for key generation may follows a set of rules on supported master/slave devices such as some or all the following: Paired devices have a master/slave relationship within the context of the DCKM framework.

[0058] Master devices may have a one to many master/slave relationship.

[0059] Master devices may pair with slave devices that are in an "unowned" or slave device pre-activation state.

[0060] Master devices may be preconfigured for a specific customer and/or operator(s) before deployment.

[0061] Operators may only be allowed to work on master devices that have been assigned to them.

[0062] Operators may require two factor authentication (e.g., password and biometric) to manage the master device.

[0063] Unowned slave devices have no master relationship

[0064] Unowned slave devices may be paired with any master

[0065] Owned slave devices may seek their master device and generally cannot be paired with another master device.

[0066] Slave devices may have their master device changed (in some embodiments, this may require a master device to give permission via a trusted operator).

[0067] Another embodiment of the invention may store and forward private cipher keys utilizing a private multi-segment blockchain technology for large scale key management of endpoint devices.

[0068] A blockchain may be thought of as a type of distributed ledger, comprised of unchangeable, digitally recorded data in packages called blocks.

[0069] These digitally recorded "blocks" of data are typically stored in a linear chain.

Each block in the chain contains data (e.g. bitcoin transaction), and is cryptographically hashed. The blocks of hashed data rely upon the previous block data in the chain, ensuring all data in the overall "blockchain" has not been tampered with and remains unchanged.

[0070] Private blockchains, sometimes called permissioned ledgers allow for distributed identical copies of a block(s), but only to a limited amount of trusted participants only.

[0071] In operation, cipher key storage process of the instant invention extends the conventional blockchain storage functionality described above to further enhance the already secure storage of information by establishing a private multi-segment blockchain. In a preferred embodiment, DCKM of the present invention has a set of interface rules that enable the interconnect of blockchains to prevent outside users from accessing the cipher keys.

[0072] Turing now to FIG. 4, a flow chart 400 illustrating some of the steps involved in a blockchain implementation of the current invention are shown. At step 402, a framework for deploying a private multi segment blockchain interconnection system may be created. This may involve some or all of the steps shown in FIGS. 2 and 3. It may further include the pre-configuration and/or deployment of a deterministic model/policy for dynamically issuing cipher keys to master and slave the devices to ensure the secure delivery of electronic data to the desired endpoint in the network via a secure transmission channel. Such deterministic models are based an any suitable known blockchain/distributed ledger technology such as BitCoin, Ethereum, Ripple, Hyperledger, MultiChain, Eris, etc.

[0073] Next, at step 404 extended interface rules between various master slave network elements are created. This may include the nesting of blockchains, as well as, the creation of unique blockchains per customer. In the multi-segment blockchain embodiment, the issue of management of user permissions when mining is solved. For example, the resultant benefit of DCKM's process is that the blockchain's activity is private and can only be seen by chosen participants (master/slave pairs). The DCKM process adds better controls for transactions and removes the miner from having to provide proof of work since cost are no longer demanded for work done. In a closed system, the blockchain will only contain transactions which are of interest to those participants that have negotiated the cipher keys.

[0074] Next, at step 406 execute extended interface rules between various master slave network elements are created. This may include passing the ledgers for new cipher keys to another master device to manage.

[0075] Next, at step 408, cipher keys are encrypted as ledger entries. In operation, as data is transmitted across the network from trusted device to trusted device (master/slave), the cipher from the previous network element is hashed and added as a ledger entry and provided to the next network element in the transmission chain. This information is used to either decrypt the information at an end point or is iteratively added on a network element by element as the information passes through the network to increase the security of the data.

[0076] Based on the rules as stated above, DCKM's deterministic model define the actions taken based on the state that both the master and slave devices are in and establishes the workflow outcome expectations.

[0077] Beyond controlling access to cipher keys, this type of cryptography enables any message to be signed by a user to prove that they own the private key corresponding to a particular address.

[0078] DCKM extended the rules of engagement that occurs when two blockchains interconnect:

[0079] Each blockchain presents its identity as a public address on the endorsed list.

[0080] Each blockchain verifies that the other's address is on its own version of the endorsed list.

[0081] Each blockchain sends a challenge message to the other party.

[0082] Each blockchain replies with a signature of the challenge message, thereby proving ownership of the private key corresponding to the public address they presented.

[0083] It will be understood that these steps are merely illustrative, and are not meant to be comprehensive or necessarily performed in the order shown. Persons skilled in the art will appreciate that the present invention can be practiced by other than the described embodiments, which are presented for purposes of illustration rather than of limitation, and the present invention is limited only by the claims which follow.