Digital Energy - BPT

Paul Coggin[1]*

[1] Dynetics, Inc., 1002 Explorer Blvd, Huntsville, AL 35805
(*Email: Paul.coggin@dynetics.com and Phone: 256-713-5328)

FORMAT

30 minute presentation

KEYWORDS

ICS\SCADA, energy, APT, network, fiber, Telco, utility, infrastructure smart grid, convergence, hack, exploit, secure, defend, attack, protect, strategy, offense, defense, target, threat, security, cyber, critical, VPN, router, firewall, OSI, Optical, SONET, DWDM, 3\4G, Cellular, remote, access, vendor, backdoor, OSS, BSS, Management, MPLS, FTTX, GPON, ANSI\ISA99

ABSTRACT

There are a great deal of conversations today regarding the advanced persistent threat (APT – worms, viruses, trojans such as Stuxnet) and critical infrastructure networks for ICS/SCADA, smart grid and service provider networks. The basic persistent threat (BPT) issues are being ignored in many cases. How can the APT be mitigated when the BPT issues have not been resolved? Typically, the technical features and capabilities required to mitigate BPT issues are present in existing hardware and software on the network. Proper attention to information flows, trust relationships, integration and interdependencies are often not secured during a network architecture design and implementation. When the BPT issues are addressed an APT threat will find it more difficult to spread horizontally and vertically throughout a network. In this presentation common network BPT issues that are often discovered during security consulting engagements will be discussed. BPT network architecture mitigations including separation of services for control, management and data traffic as well as securing and monitoring trust relationships and interdependencies will be covered.

ABOUT THE AUTHOR

Paul Coggin *is an Internetwork Consulting Solutions Architect with Dynetics, Inc in Huntsville, Alabama. Paul is responsible for architecting and securing large complex tactical, critical infrastructure and service provider networks. Paul's expertise includes tactical, service provider and ICS\SCADA network infrastructure hacker attacks and defenses as well as large complex network design and implementation. Paul's experience includes leading network architecture reviews, vulnerability analysis and penetration testing engagements for critical infrastructure networks.*

Paul is a frequent speaker on offense and defense topics related to critical infrastructure networks. He has presented at the following conferences DeepIntel, DerbyCon, BSides, Hacker Halted, COUNTERMEASURE, TakeDownCon, DeepSec, SCADA [in]Security and DC3. Paul is a Cisco Systems Certified Instructor # 32230, Certified EC-Council Instructor and a certified SCADA security architect. He has a BS in Math, an MS in CIS

and is currently pursuing an MS in IA\Security. In addition he holds a wide array of professional certifications. Paul is the organizer for BSides Huntsville.