

Charles Pak, Ph.D.
2315 Sycamore Pl., Hanover, MD 21076
cp1032@georgetown.edu; charlespak1@outlook.com; (410)805-2110

SECURITY CLEARANCE

Active DOD TOP SECRET with SCI eligibility

ACADEMIC DEGREES AND TECHNICAL CERTIFICATIONS

- Ph.D. in Information Assurance (IA), Cyber, and Information Security research fields. Completed all required doctoral course works, the final dissertation, and published his work in 2011.
- Master's in network security (currently Information Assurance) with class Honors, Curriculum mapped to the committee on National Security Systems and National Security Telecommunications and Information Systems Security Instructions (CNSS/NSTISSI)
- DoD Zero Trust and E-ICAM expert with technical solutions.
- AWS Certified Cloud Practitioner Architect, (FMQ7DYX1WE4EQ2KS) April 2023.
- CISM, Certified Information Security Manager, (CISM#1117661), October 2011
- CRISC, Certified in Risk and Information Systems Control, (CRISC#1115022), September 2011
- CISSP, Certified Information Systems Security Professional (CISSP#256490), June, 2008
- SSCP, Systems Security Certified Practitioner (SSCP#256490), July, 2008
- Security + Certification, (#COMP001006531743), 2007
- Information Technology Infrastructure Library (ITIL) Foundation Certification, (ID#6241)
- MCSE 2000, Microsoft Certified Systems Engineer, 2001 (MCP#21660)
- MCT, Microsoft Certified Trainer 1994 (MCP#21660)
- MCSE 4.0, Microsoft Certified Systems Engineer, 1995 (MCP#21660)
- MCSE 3.51, Microsoft Certified Systems Engineer, 1994 (MCP#21660)
- CCNA, CISCO Certified Network Associate (#CSCO10350538)
- Department of Army Certificate as Security Systems Administrator, Ft. Monmouth N.J. 4/2002
- Department of Army Certificate as Network Security Management, Ft. Monmouth N.J. 4/2002

PUBLICATIONS

Pak, C. & Cannady, J. (2010). Risk Forecast Using Hidden Markov Models. *Research in Information Technology, ACM, SIGITE*, 7(2), 4-15.

Pak, C. & Cannady, J. (2009). Asset Priority Risk Assessment Using Hidden Markov Models, *ACM SIGITE'09*, 65-73, October 2009 – (Ranked as one of the highest by the conference's peer reviewers and received an invitation for submission to the next issue of *Research in IT*)

Pak, C. (2008). The Near Real Time Statistical Asset Priority Driven Risk Assessment Methodology (NRTSAPD), *ACM SIGITE'08*, 105-112, June 2008

ACM SIGITE 2008 SIGITE Conference Paper Reviewer

ACM SIGITE 2009 SIGITE Conference Paper Reviewer

ACM SIGITE 2010 SIGITE Conference Paper Reviewer

Information Security Journal (ISC2): A Global Perspective, Paper reviewer.

PRESENTATION

The Maryland Higher Education Information Assurance Academic Society, Pak, Charles (2008). Two Factor Authentication using smart cards, Towson University, Maryland.

TECHNICAL EXPERTS

- Cyber Security, Network Security and IA, College and Graduate School Levels
- CISSP, CEH, MCSE, CCNA, Security+ Certification Track Education
- Cloud Security, AWS Certified Cloud Practitioner.
- Ethical Hacking, Penetration Test Techniques
- Microsoft Exchange Server 4.x/5.x/2000/2003/2007/2008
- Windows 2003/2008 Active Directory Design and Implementation
- Defense Messaging System (DMS) Design and Implementation
- Microsoft SQL Server and Database Design, Migration and Implementation
- Microsoft BackOffice Products Implementation and Management
- Microsoft Developer Applications, Visual Studio and InterDev.
- Network Information System Protection Security Expert
- CISCO Technology Design and Implementation
- Information Technology Infrastructure Design and Implementation
- Securing and Protecting IT Computer Data with Cryptology
- Secure Network, Perimeter Protection, Firewall, LAN-WAN, Remote Access, Server Hardware Management (Blade Servers, SAN Storage, Virtual Center) Design and Implementation

TEACHING EXPERIENCE

Adjunct Assistant Professor, Information Assurance (IA) Course Chair, University Maryland University College (UMUC), Delphi, Maryland
Adjunct Professor, Georgetown University, Washington, D.C.

EXPERIENCE SUMMARY

Dr. Pak is a seasoned Sr. Cyber Security Solution Architect and Technical Program Manager with 28 years of hands-on technical background from a low-level microprocessor design to a high level Web application programming and cloud computing. He is a world recognized IA research scholar and published several novel conference and journal papers. He is an invited speaker in IA education. He is a hands-on practitioner who holds industry certifications such as CISSP, CISM, CRISC, SSCP, ITIL, MCSE, MCT and CCNA with more than 20 years of leadership in engineering, supporting, and servicing complex centralized and distributed Information Technology environments; Windows 2012/2008/2003/2000/NT LAN/WAN/MAN and, IBM Blade Center, EMC Virtual Center, Cloud Computing, SAN, PKI, CISCO Network design, development, testing, installation, configuration, operation, and support; working with a wide range of network protocols and topologies; systems reengineering; user training; and mini/micro-computer multi-tier Help Desk support environments. Dr. Pak is also experienced in program management including the performance of staffing, workload forecasting, budgeting, scheduling, customer relations, proposal-writing and performance evaluation.

PROFESSIONAL EXPERIENCE

Leidos 2023 – Present, Security Architecture and Engineering Manager.

Dr. Pak manages the cybersecurity and engineering team for the DISA Enclave Agency (DES) program for mission operations, modernization migration to DES enclave for DISA at Fort Meade. While sustaining, and maintaining the on premise DISA mission operations, he managed the DES migration for user applications, infrastructures, network and computing to the cloud

environment. He managed emerging technology insertion into the mission enclave and staffing for 24x7 operations.

GDIT 2011 – March 2023, Sr. Cyber Security Solution Architect. Dr. Pak architected and provided cyber security solutions to the Federal and Commercial clients as EPA, FBI, FSA, HHS, CDC, GSA and CMS. He provided cost effective security solutions to the client by identifying, analyzing security requirements that is most beneficial to the clients in cost and technology. He is specialized in Cloud Computing solutions as part of the FDCCI initiatives. He provided health security solutions to the NIAID, NIH, DHSS agencies for their Cyber Technologies (CT) initiatives to protect their information system confidentiality, integrity, and availability. He ensured the agency Security & Privacy (S&P) are protected from data breach, compromise, or destruction.

Dr. Pak managed Cyber Security Contract with 3 sub-contractors for the Department of Education/FSA that encompassed over 55,000 computer network nodes throughout the U.S. LAN/WAN. He designed Cyber Security measures to safeguard the department assets and operation. He conducted IA security scans of several dispersed datacenters to discover vulnerabilities on perimeter protection, boundary networks, internal business applications, authentication and authorization policies, standards, and procedures, using security tools such as Metasploit, Nexpose, Nipper, Fluke Etherscope, Retina and Nessus. He completed project management plan, staffing, network discovery and mapping, IT enterprise security profile and vulnerability assessment, remediation of risks and vulnerability, strategy for maintenance of the enterprise model to represent the department's changing security posture. He briefed the department CIO weekly on the IA project status.

Technical Program Manager and Sr. Principal Security Architect.

Dr. Pak was an expert in the areas of client/server technology and was experienced in managing both on-site and off-site technical support projects. Dr. Pak was highly respected by his customer for both his technical expertise and his ability to communicate with all levels of systems administrators, users, and project personnel. Dr. Pak served as General Dynamics Information Technology (GDIT) in-house network and system engineering subject matter expert and extended his expertise on a number of in-house and client projects in addition to his normal project management assignments.

As a Sr. Principal Security Architect, he supported the DIACAP process to ensure the appropriate risk management is applied to the Pentagon Telecommunication Center (PTC) infrastructures and to maintain the C&A process for the Pentagon affiliated agencies such as OSD, AF, Navy, Army, Coast Guard, WHS, etc. As part of the C&A process, he ensured continuous vulnerability scanning, assessment, mitigation and validation to maintain the IA posture for the Pentagon Telecommunication Center (PTC). Further, he supported the Pentagon E-mail Infrastructure and Defense Messaging System (DMS) project. He managed 55 Microsoft Exchange E-mail sites for 95,000 mail users in the organization. Managed Messaging backbone infrastructure includes all Intra/in-terns site messaging connectivity within/to the Pentagon network infrastructure. Implemented Cipher Trust Iron Mail SPAM filter to block email SPAMS inbound to the Pentagon Email infrastructure. He supported all DMS implementation with new product developments. He resolves all types of E-mail Related problems from all Pentagon related agencies. He manages all in/out of Pentagon SMTP email messages. He ensured all SMTP messages are delivered without interruption. He maintained all Pentagon Email Messaging (DMS/Commercial) infrastructures,

installations and upgrades on Blade Servers and SAN Storage. He migrated legacy systems to the latest state of the art systems that include Exchange 5.5 to Exchange 2003, 2007, Windows 2000, 2003 to Windows 2008 operating systems and the IBM Blade Servers to virtual servers (VMWARE). Designed and implemented NIPR and SIPR National Security Agency's Secure Mobile Environment Portable Electronic Device (SMEPED). He performed IA tasks by scanning numerous computers assets, mitigating any discovered vulnerabilities, ensuring all network assets are secure. Conducted a regular vulnerability scan, risk mitigation, DISA STIG application, patch management, and monitoring the organizational assets on a daily basis to build knowledgebase in IA. He is a proponent of real-time IA vulnerability discovery, assessment, and mitigation to proactively countermeasure real-time threats. Dr. Pak also designed and implemented Public Key Infrastructure (PKI) on all production servers and removed username and password vulnerabilities by implementing digital two-factor authentication smart cards – common access cards (CAC). He managed all Pentagon Telecommunication Center (PTC) users' digital certificates and enabled their smart cards authentication to access the PTC assets rather than using username and passwords.

Dr. Pak managed 21 General Dynamics Network Systems on-site engineers in support of Night Vision & Electron Sensors Directorate (NVESD) at the U.S. Army Ft. Belvoir, VA. He managed all incoming and outgoing technical issues with users for their technical and personnel problems. He also architected Microsoft Technology deployments to better support NVESD user community. He ensured all network connectivity is up 100% and managed all Network Support Branch staff. He worked closely with DOIM, PMNV, PEOSOLDIERS and the US ARMY VPS (Virtual Prototyping and Simulation) to provide better engineering support to their group. He deployed many Night Vision Modeling and Simulation equipment and programs to other Army Battle Labs such as Ft. Knox and Ft. Benning via DREN (Defense Research and Engineering Network). He is very knowledgeable with the U.S. Army Modeling and Simulation Research Projects. He also upgraded, managed, and maintained the Veteran Affairs (VA) networks with the newest CISCO technologies as a CISCO channel partner.

Dr. Pak possesses extensive technical knowledge in the Army C4I Programs, DMS Architecture and Microsoft Exchange Mail connectivity among Pentagon, Ft. Monmouth, Ft. Myers, Ft. Meade and other Military District Washington (MDW) sites. He migrated legacy email systems to Exchange Systems and consolidated all Email Servers onto Ft. Monmouth Mail Organization. He managed all site crypto communications over the military TECHLANE crypto devices in a secure connection. He generated crypto keys and established secure communication lines from one crypto device to the next and resolved any cryptology related problems. He has played a vital technical and logistic management point of contact among all these branch organizations.

Dr. Pak improved and enhanced the NVESD network and its UNIX/Windows NT/2000 operations. He enhanced the NVESD Microsoft Windows operating systems by improving their configurations and by conducting a good system performance tunings. He consolidated Night Vision's Email Servers onto CECOM U.S. Army Enterprise Exchange Domain and configured all mail connectivity among multiple Exchange Mail sites. He worked with DOIM (Ft. Belvoir Govt. Network Management Group) very closely to enhance existing network connection and its equipment. The network equipment he monitored and supported are FORE ASX1000 and CISCO 5500/6500 series systems. SGI, Linux and SUN systems were predominant UNIX machines that his UNIX engineers managed to support the NVESD Network activities.

Dr. Pak served as Project Manager and technical lead for General Dynamics Information Technology's 10-person Standard Army Ammunition System Modernization (SAAS-MOD) contract team. Dr. Pak's team performed the successful consolidation of Windows NT workstations/servers and UNIX workstations into a Microsoft Windows NT network as a single domain model, then integrated non-network workstations/servers into a campus network over TCP/IP. Dr. Pak's team also redesigned the legacy network infrastructure integrating all servers/workstations to have Internet connectivity with Defense Message System (DMS) servers and present a true client and server development environment. His team also applied information engineering techniques to reengineer Army's ammunition supply system and implement a new ORACLE database solution.

Dr. Pak also served as Project Manager on a Coast Guard Research and Development Center (RDC) contract. Dr. Pak's five-person project team supported Coast Guard systems end users based in Groton, CT during their participation as part of Coast Guard on-going migration from CTOS-based information management systems to Microsoft NT platforms. Dr. Pak's five-person team upgraded all on-site LAN networks, installed and tested 130 NT workstations, and established an on-site Help Desk at the Research and Development Lab in Groton, CT. Dr. Pak managed the scheduling, staffing, tracking, and support of all required post-implementation service requirements.

Project Manager/Senior Technical Manager. Dr. Pak served as Project Manager and technical lead for Office of Naval Research (ONR) MIS department with a team of 19 hardware and software engineers who integrated, tested, implemented, and supported a Microsoft Windows NT metropolitan network (MAN) and its associated applications software over a FDDI backbone supporting ONR Headquarters and seven field locations located in major cities nationwide via communication media such as FDDI, 100Base Fast Ethernet, 10BaseT Ethernet, TCP/IP, NetBEUI, Frame Relay, routers, bridges, CSU/DSU, ISDN line, and the dial-up modems. His team implemented Microsoft Exchange Server Messaging Systems to all users across the ONR network infrastructure. Dr. Pak re-engineered and upgraded 7 remote ONR locations' hardware, software, and communication devices. He managed these 7 field installations via WAN connections, and also supported all trouble calls originating from these sites. Dr. Pak scheduled, staffed, tracked, and provided technical support required in conjunction with post-implementation service calls.

Dr. Pak also served as Project Manager and technical lead tasked with managing the design and implementation of the Bay State Health Systems' Windows NT MAN used to deploy Windows NT servers/workstations, Windows 95, Exchange Server, and BackOffice applications to 27 remote site locations and more than 25,000 end users. Dr. Pak's seven-person team created a Windows NT network that coexisted with a NetWare IPX/SPX environment on 10BaseT Ethernet and heterogeneous LANs connected to a 100 Mbps FDDI ring. Dr. Pak managed the scheduling, staffing, tracking, and technical support of all required post-implementation service calls.

Dr. Pak was Project Manager and technical lead providing Defense Message System (DMS) support at the Columbia Pike DISA office. Dr. Pak's five-person team developed SUN SPARC 1000-based scripts to improve and maintain DMS development including SUN SPARC stations, Windows NT workstations and servers, AUTODIN, STU-III and CSU/DSU across classified and unclassified DISA communication lines connecting Scott AFB, the DISA Regional Control Center at Columbus, OH, Arlington VA, Reston VA, Columbia Pike (Arlington), VA, and locations in Germany and Hawaii. Dr. Pak provided both telephone and on-site technical support during post-implementation service calls performed at any and all of the remote locations.

Northrop Grumman, 1984 - 2011, Technology Manager. Dr. Pak served as a technical lead in charge of project personnel charged with designing the hardware, software, and telecommunications architectures for a number of Department of Defense (DOD), federal, and commercial applications. For the Department of Agriculture and Social Security Administration (SSA), Dr. Pak served as technical lead in charge of a five-person integration team. Dr. Pak's team installed 45,000 Microsoft NT workstations and associated hardware/software and communication devices in 60 locations spread across the continental US, Europe, and the Far East. This project was performed in support of AT&T. Dr. Pak was responsible for providing technical input, project staffing, and the scheduling and performance of all post-installation service call support efforts.

Dr. Pak also was the technical lead during the design of Department of State Network Infrastructure employing DEC SMP servers and workstations with communication equipment over TCP/IP to support worldwide operations. Dr. Pak directed the system architecture development for the Department of Veterans Affairs in support of the migration of previously non-networked systems to a network environment incorporating state-of-the-art capabilities. Dr. Pak also supported a National Institutes of Health effort by designing network architecture to move from the legacy main-frame SNA infrastructure to a DEC Alpha open computing environment interfacing with PCs over TCP/IP.

Dr. Pak gained "first-hand" service call experience while serving as a Field Engineer supporting the Air Force's deployment of engineering test support equipment and semi-automatic support equipment at customer sites around the world. Dr. Pak performed "hands-on" equipment-related servicing and problem resolution and also trained Air Force personnel in the use of this equipment. The combined equipment service support and customer training effort required service calls to various Air Force facilities located in the U.S., Europe (England), the Middle East (during Operations Desert Shield and Desert Storm), and Korea.

Dr. Pak developed, integrated, and tested a real-time artificial intelligent system in embedded firmware to counter jam radar systems as part of the power management system for F-16, F-14, and F-111 aircraft. He designed and developed a number of software and hardware systems for Navy electronic warfare applications. He also used information-engineering techniques to develop object-oriented software in Atlas, FORTRAN, Pascal, Ada, Assembler, and C languages. He developed real-time transmitter software in "C" on an HP-UX 9000 to test the transmitter section of the power amplifier and Sonar Power conditioner of MK 48/50 Torpedoes. He developed, integrated, installed, modified, and maintained state-of-the art HP-UX 9000, DEC, and IBM computer systems using UNIX, VAX/VMS, and DOS/Windows operating systems. He installed, maintained, modified, and supported electronic counter measure pods such as ALQ119 and ALQ131 ECM (Electronic Counter Measure).

EDUCATION

- Ph.D. in Information Security, Nova Southeastern University, Ft. Lauderdale, Florida. October 2011
- MS, Network Security, Capitol College, Laurel, Maryland, 2005, with class Honors GPA=4.0.
- BS, Electrical Engineering, Pennsylvania State University, State College, Pennsylvania 1984
- Member of IEEE, ACM (Association for Computing Machinery), ISACA, and (ISC)2