National Cybersecurity Center of Excellence

Increasing the deployment and use of standards-based security technologies

Harry Perper – Chief Engineer
National Cybersecurity FFRDC
The MITRE Corporation

18 January, 2017
Welcome to the NCCoE

STRATEGY

VISION
ADVANCE CYBERSECURITY
A secure cyber infrastructure that inspires technological innovation and fosters economic growth

MISSION
ACCELERATE ADOPTION OF SECURE TECHNOLOGIES
Collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

GOAL 1
PROVIDE PRACTICAL CYBERSECURITY
Help people secure their data and digital infrastructure by equipping them with practical ways to implement standards-based cybersecurity solutions that are modular, repeatable and scalable

GOAL 2
INCREASE RATE OF ADOPTION
Enable companies to rapidly deploy commercially available cybersecurity technologies by reducing technological, educational and economic barriers to adoption

GOAL 3
ACCELERATE INNOVATION
Empower innovators to creatively address businesses’ most pressing cybersecurity challenges in a state-of-the-art, collaborative environment
STAKEHOLDERS

PARTNERS/SPONSORS
Advise, assist, and facilitate the Center’s strategic initiatives

- The White House
- National Institute of Standards and Technology
- U.S. Department of Commerce
- U.S. Congress
- Montgomery County
- Maryland State

TEAM
Collaborate with innovators to provide real-world cybersecurity capabilities that address business needs

- NCCoE
- National Cybersecurity FFRDC*
- Tech Firms
- Industry
- Academia
- Government
- Project Specialists
- Project-Specific Collaborators
- National Cybersecurity Excellence Partnership (NCEP) Partners

CUSTOMERS
Collaborate with center on project-specific use cases that help our customer’s manage their cybersecurity priorities

- Business Sectors
- Academia
- Government
- Cybersecurity IT Community
- Systems Integrators

*NIST, the National Cybersecurity Federally Funded Research & Development Center (FFRDC) is operated by the MITRE Corporation
ENGAGEMENT & BUSINESS MODEL

DEFINE + ARTICULATE
Describe the business problem
Define business problems and project descriptions, refine into a specific use case

ORGANIZE + ENGAGE
Partner with innovators
Collaborate with partners from industry, government, academia and the IT community on reference design

IMPLEMENT + TEST
Build a usable reference design
Practical, usable, repeatable reference design that addresses the business problem

TRANSFER + LEARN
Guide users to stronger cybersecurity
Set of all material necessary to implement and easily adopt the reference design
The NCCoE seeks problems that are:

- Broadly applicable across much of a sector, or across sectors
- Addressable through one or more reference designs built in our labs
- Complex enough that our reference designs will need to be based on the combination of multiple commercially available technologies

Reference designs address:

- Sector-specific use cases that focus on a business-driven cybersecurity problem facing a particular sector (e.g., health care, energy, financial services)
- Technology-specific building blocks that cross sector boundaries (e.g., roots of trust in mobile devices, trusted cloud computing, software asset management, attribute based access control)
Cybersecurity solutions that are:

- based on standards and best practices
- usable, repeatable and can be adopted rapidly
- modular, end-to-end and commercially available
- developed using open and transparent processes
- matched to specific business needs and bridge technology gaps
CURRENT PROJECTS

- Attribute Based Access Control (SP)
- Consumer/Retail: Multifactor Authentication for e-Commerce
- Data Integrity
- Derived PIV Credentials
- DNS-Based Secured Email (SP)
- Energy: Identity and Access Management (SP)
- Energy: Situational Awareness
- Financial Services: Access Rights Management
- Financial Services: IT Asset Management (SP)
- Health Care: Electronic Health Records on Mobile Devices (SP)
- Health Care: Wireless Medical Infusion Pumps
- Manufacturing: Capabilities Assessment for Securing Manufacturing Industrial Control Systems
- Mobile Device Security (SP)
- Privacy-Enhanced Identity Federation
- Public Safety/First Responder: Authentication for Law Enforcement Vehicle Systems
- Public Safety/First Responder: Mobile Application Single Sign-On
- Transportation: Maritime: Oil & Natural Gas
- Trusted Geolocation in the Cloud
Harry Perper, Chief Engineer

harry.perper@nist.gov, harry@mitre.org

1+ 301-975-0367

Twitter: @hperper