Federal Aviation Administration (FAA)

Information Technology (IT)

Information Systems Security (ISS)

Research and Development (R&D)

Workshop

Tuesday, May 6, 2003 through Thursday, May 8, 2003

8am – 4:30pm

LOCATION:

MITRE 2

7515 Colshire Dr.

McLean, VA

Website:  http://sunset.usc.edu/events/2003/faasec2003/index.html

AGENDA

As of 4/25/03
TUESDAY, May 6, 2003
FAA IT-ISS R&D Workshop
Presentations on Existing Initiatives

8-8:30 Registration, Continental Breakfast
8:30-8:40 MITRE Welcome
8:40-8:55 Workshop Concept of Operation - John R, Rossi, Conference Coordinator

9-9:10 Introduction to the IT-ISS R&D Workshop - Marshall Potter, FAA Chief Scientist for Information Technology

9:15-9:45 Keynote Address - Dr. Daniel J. Mehan, Assistant Administrator for Information Services and Chief Information Officer, AIO-1

9:50-10:10 Naval Postgraduate School - Cynthia Irvine
  • Biometrics for Continuous Authentication of Flight Deck Personnel
  • In-Flight Backup of Black Box Data to Ground Stations

Break

10:30-11:45 Air Force Research Laboratory (AFRL)/FAA Computer Security Incident Response Center (CSIRC) - James Sidoran
  • AFED JAVA GUI R&D Project - Lt. Matt Manger
  • CyberWolf R&D Project - Lt. Matt Manger
  • Distributed Agents for Information Warfare Operational Transition DAIWatch - Lt. Matt Manger
  • Wireless - Paul Ratazzi
  • Development of Trustworthy Systems from Untrustworthy Components with Untrustworthy Actors - Dr. Indrajit Ray

11:45-12: AIO-4 Research and Development - Marshall Potter, FAA Chief Scientist for Information Technology

12-1pm: LUNCH

1-1:30 Intrusion Detection Research and Development - Peter Heldt, Marc Zissman, Richard Lippmann, Bill Porto, MIT Lincoln Lab and Natural Selection, Inc.


1:55-2:15 Extending COCOMO II to Estimate the Cost of Developing Secure Software - Ed Colbert, University of Southern California (USC) – Center for Software Engineering (CSE)

Break
2:30-3:00 Development of a Robust Security Infrastructure for Data Warehousing - John Brackett, Software Engineering Resource Center (SERC), Boston University

3:05-3:25 Unintended Information Revelation Alert Agent - Rohini Srihari, State University of New York (SUNY) at Buffalo

3:30-4:00 Summary and Discussion

4:00 Adjourn

5:00-6:00 Social/Reception

6:00 Workshop Dinner
WEDNESDAY, May 7, 2003
FAA IT-ISS R&D Workshop
Presentations on Existing Initiatives
and
Breakout Sessions

8-8:30  Registration, Continental Breakfast

8:30-8:50  FAA’s Information Systems Security Architecture - John Kinkel


9:20-9:50  Cyber Panel (presentation and demonstration) - John Smith, SRA, Inc.

9:55-10:15  FAA Computer Security Incident Response Center (CSIRC) Overview - Erik Smith

Break

10:30:

4 Breakout Sessions

(1) Real Time Intrusion Protect, Detect Response & Recovery
(2) Integrity and Confidentiality in the Mobile Environment
(3) Trustworthy Systems from Untrustworthy Components with Untrustworthy Actors
(4) Information Technology issues such as the need for Knowledge Management and Enterprise Architecture

Breakout Sessions:

I  Intrusion Security - Chairs: Bennie Sanford, Rob Cochran
   (“Real Time Intrusion Protect, Detect, Respond, & Recovery”)

II  Wireless Security - Chairs: Marie Stella, Vic Patel
    (“Integrity and Confidentiality in the Mobile Environment”)

    Discussion: 9/11, the increase in cyber terrorism and cyberwarfare introduce constraints to the NAS, which requires open communications to allow situational awareness for pilots and controllers. The challenge in the new NAS environment is to provide authentication, integrity and in some cases confidentiality in an airspace environment with high performance and low latency requirements and users and aircraft base whose identify changes from flight to flight. Come join the challenge of securing a truly mobile environment.

    Over the past several years, wireless networks have become a focus for security activities in commercial environments. High-profile problems like cloning in cellular
networks and WEP hacks in WLAN have been identified and are being addressed. The introduction of wireless data networks like ACARS, ATN, CPDLC, and NEXCOM brings wireless security to the forefront of the security challenges facing FAA. The possibility of attacks against the NAS by wireless intruders is of particular concern.

This session will address questions like:

- What threats exist against wireless civil aviation networks?
- To what extent do the problems and solutions mirror those of commercial networks?
- What security solutions have been defined, and what should FAA do to implement these solutions?
- Where are new solutions still needed?

III  Securing Networked Systems - Chairs: Mary Beth Dormuth, Kevin Harnett ("Trustworthy Systems from Untrustworthy Components with Untrustworthy Actors")

We will be discussing the topic of "Trustworthy Systems from Untrustworthy Components with Untrustworthy Actors". Cyber Security Research in this area has been discussed in several sources over the years, most notably "Trust in Cyberspace, Committee on Information Systems Trustworthiness, National Research Council, 1999". To be labeled as trustworthy, a system not only must behave as expected but also must reinforce the belief that it will continue to produce expected behavior and will not be susceptible to subversion. The question of how to achieve assurance has been the target of several research programs sponsored by the Department of Defense and others. FAA is currently transitioning from propriety/legacy NAS systems to new open system/COTS systems infrastructure and there are many ISS challenges and opportunities for the FAA (both IPTs and ATS) to develop a R&D program to meet these needs.

The FAA relies on infrastructures for communications, power, energy, and transportation—all increasingly dependent on networked information systems (NIS). When these FAA, private-owned, and government NISs perform badly or do not work at all, they put life, liberty, and property at risk. Interrupting service can threaten lives and property; destroying information or changing it improperly can disrupt the FAA or disclosing confidential information can embarrass the agency. The widespread interconnection of NISs could allow outages and disruptions to spread from one system to others; it enables attacks to be waged anonymously and from a safe distance; and it compounds the difficulty of understanding and controlling these systems.

IV  Information Technology - Chairs: Ernie Lucier, Con Kenney

We will be discussing Knowledge Management, Enterprise Architecture, Seamless Communications, and other pertinent topics
THURSDAY, May 8, 2003
FAA IT-ISS R&D Workshop
Outbriefs and Executive Session

8:00  MORNING: Outbriefs from the 2nd day’s breakout sessions.

12:00  Conference ends.

AFTERNOON: Workshop Leadership Team Meeting to finalize action items. (USC, MITRE, FAA)