APTA 2011 Rail Conference

Control System Security – The Threat to Transit and Other Industry Sectors

David J. Teumim, CISSP
Working Group Facilitator
Teumim Technical, LLC

Outline

Control System Security – the “New Kid” on the Block

Examples Across Industry Sectors

US Government Response

APTA Response

Birth of Control Security Field

September 11th was impetus

Realized critical infrastructure was vulnerable

Realized infrastructure could be attacked through cyber means

Recent trends in control and communication system design have added cyber vulnerabilities:

- Networking (Ethernet, TCP/IP)
- COTS Hardware, Software, network components

Who's Out There ?

Lone Hackers

Disgruntled ex-employees and contractors

Criminal cyber-gangs

Cyber-terrorists, sponsored or condoned by nation-states

What Tools Do They Use ?

Individual hacking knowledge

How-to websites

Malware “kits” on the web

Exploit Packages especially made for SCADA and Control Systems (e.g. Metasploit, “Luigi”)

Control System Incidents Across Sectors

Rail transit

Waste treatment

Auto manufacturing

Aircraft

Schoolboy hacks into city's tram system

By Graeme Baker

Last Updated: 2:48am GMT 11/01/2008

The boy, described as a 'genius‘ and some of the equipment he used

Twelve people were injured in one derailment, and the boy is suspected of having been involved in several similar incidents. The teenager, who was not named by police, told them he had changed the points for a prank.

The Telegraph, Graeme Baker, January 11, 2008

Australian Sewage Treatment Hack

Maroochy Shire, Australia

- http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/

Wireless hack by former contractor (insider)

Spilled millions of gallons of raw sewage onto local parks, rivers and the grounds of the Hyatt Regency Hotel

Police found computer and radio equipment in his car

Total amount of sewage spilled…would fill up a football field to depth of 1 – 2 feet

Zotob, PnP Worm Slams 13 DaimlerCrysler Plants

(eWeek.com article dated 8-18-2005 by Paul F. Roberts)

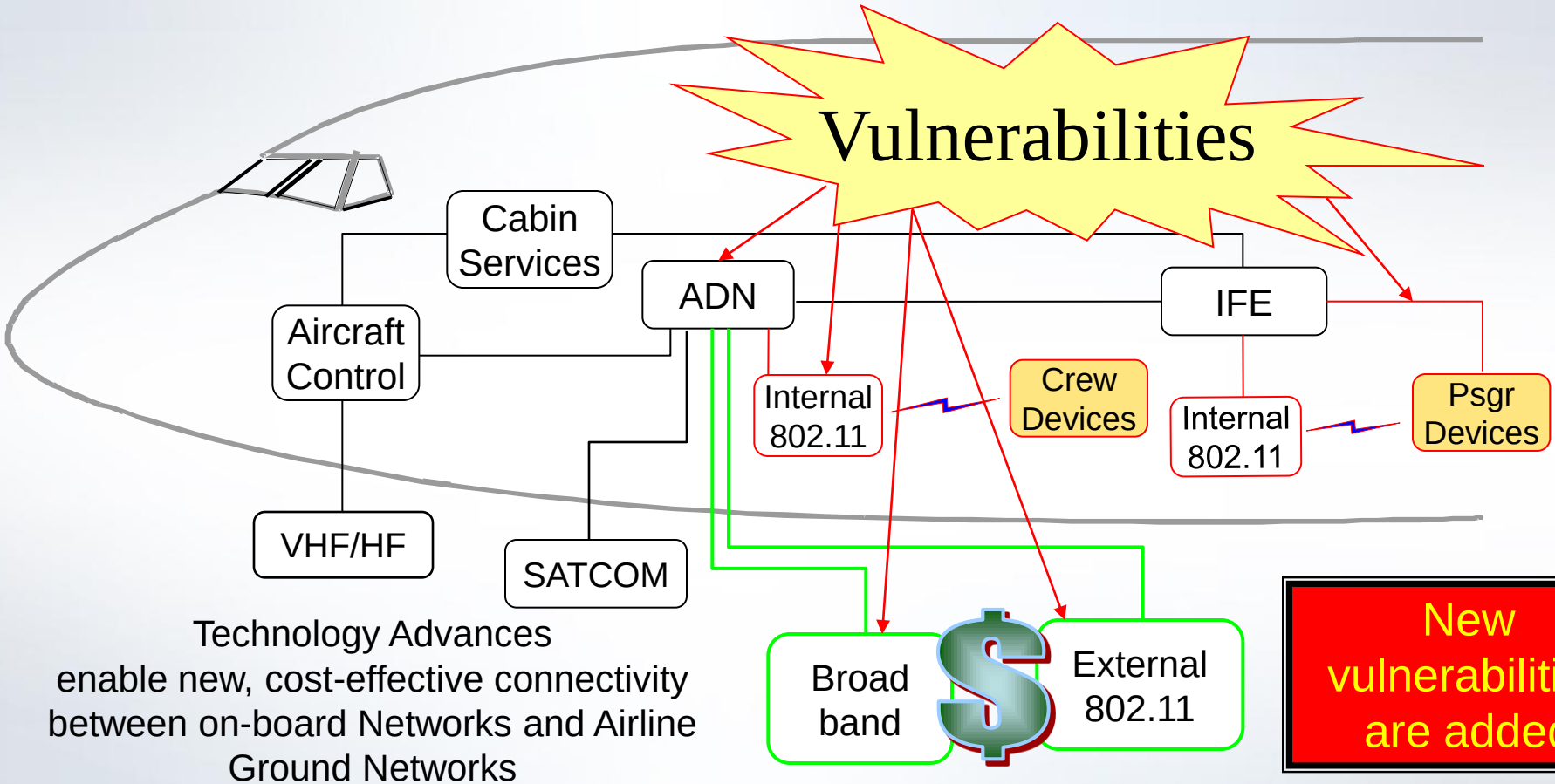
Thirteen DaimlerChrysler assembly lines down for one hour, idling 50,000 workers

Zotob worm attacked the Windows 2000 systems, exploiting holes in the PnP (Plug and Play) service

Other businesses, such as the New York Times and SBC also hit

Other Transportation Issues – Next Generation Aircraft

Airborne Cyber Security Issues



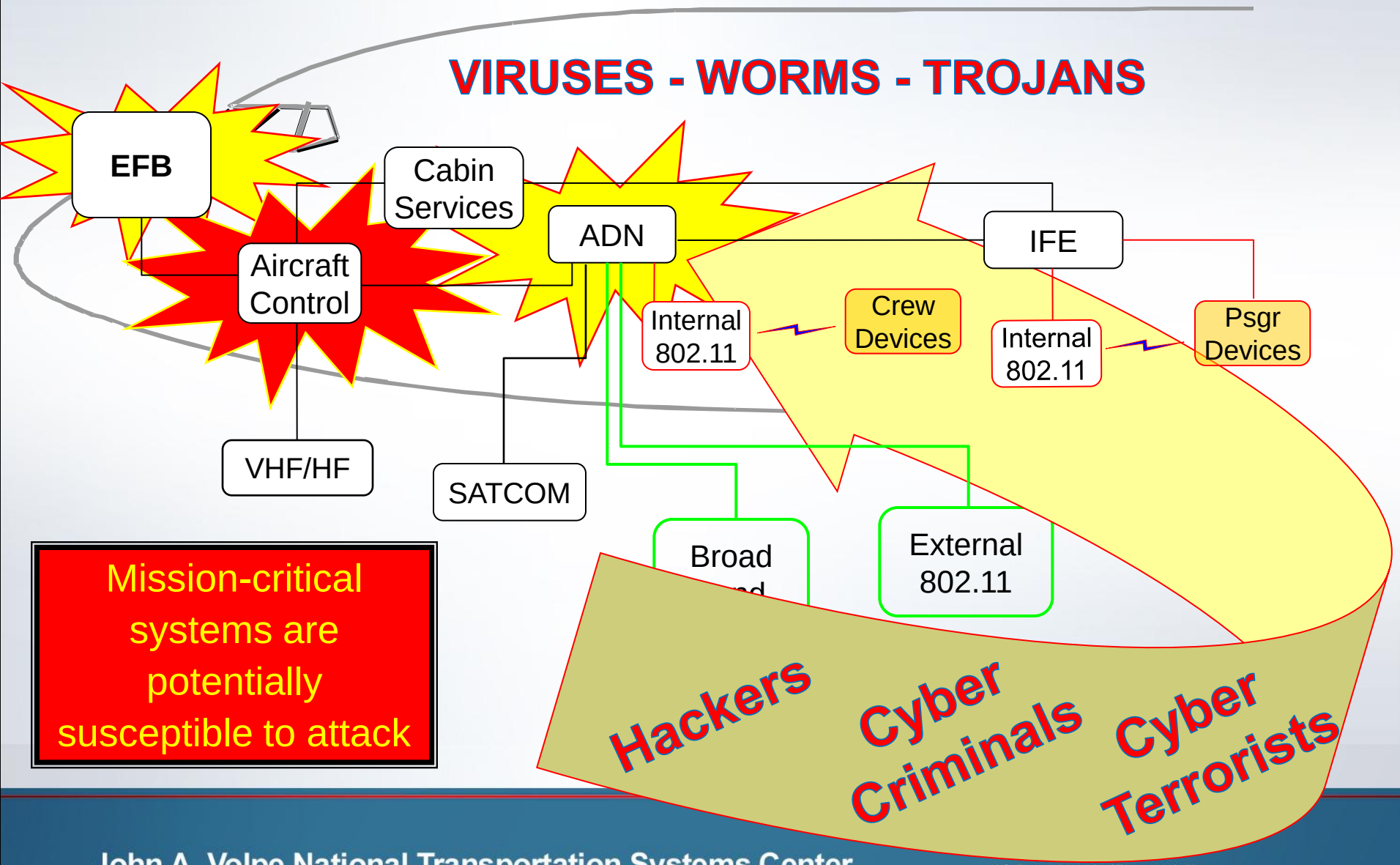
Technology Advances enable new, cost-effective connectivity between on-board Networks and Airline Ground Networks

New vulnerabilities are added

Airlines will use Broadband Internet connectivity to support passenger services then use existing bandwidth to support operations.

Revenue from passenger services provides funding for increased infrastructure costs

Airborne Cyber Security Issues



The Big “R” - Regulation

Chemicals – DHS “CFATS” Regulations, Cyber Section

Nuclear – NRC Cybersecurity Regulation 5.71

Electric Power – NERC-CIP Regulations on Power Transmission Grid - Critical Cyber Assets. Affects critical generation facilities, substations, etc.

NERC-CIP Some Provisions

Electronic Security Perimeter

Physical Security Perimeter

Personnel/Administrative Security

FINES – Maximum penalty of $1MM/day for violations

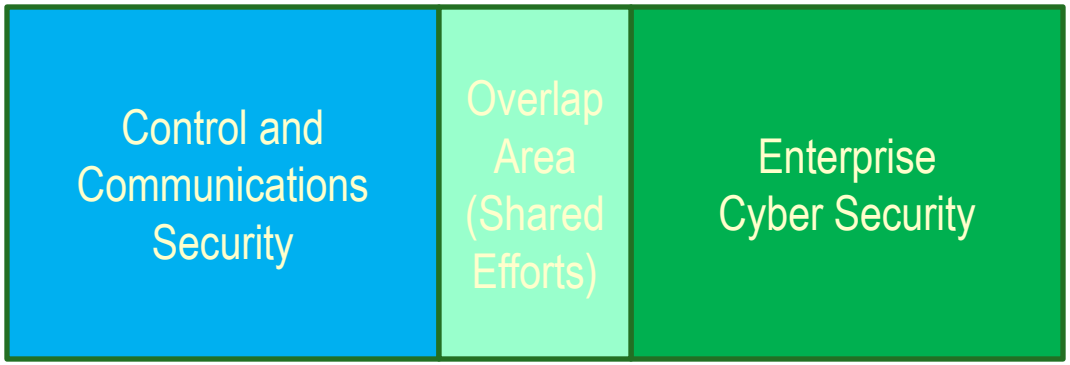
Status of Transit Control Security

No cyber regulations at present

Voluntary Industry Consensus Standards through APTA

Hope is that regulations, if they come, would be based on industry consensus standards

APTA Standards Efforts in Cybersecurity – Two Working Groups



Contact Information

Dave Teumim

Teumim Technical, LLC

dave431@enter.net

610-398-5546