Applying Systems Engineering to Deliver Cyber Security for the 21st Century

Col Charlie Flores, USAF (Ret)

Systems Engineering to Deliver Cyber Security

- Beginnings - DARPA

- Current Issues – Tactical vs. Strategic
  - Stats: FBI, Verizon, IBM

- Systems Engineering and Cyber Security
  - Solar Sunrise

Col Charlie Flores, USAF (Ret)

Hispanic Heritage and Prostate Cancer Awareness

September
　　National Hispanic Heritage month
　　Prostate cancer awareness month

Gentlemen
　　Talk to your doctors and
　　Give the prostate the finger…test… for your family;
　　Your life may depend on it. Avoid the cancer surprise!

I'm here today because of early detection and timely surgery….
And I feel like a kid again… so please … **get tested y'all!!!**

Col Charlie Flores, USAF (Ret)

In the beginning there was DARPA Internet

- University of Wisconsin-Madison Trace Center (http://trace.wisc.edu/docs/nature_of_cyberspace/naturcyb.htm):
- "The Internet had its origins in 1969 as an experimental project of the Advanced Research Project Agency ("ARPA"), and was called ARPANET.
- The ARPANET was known as the "DARPA Internet" and eventually, simply as the "Internet."
- This network linked extremely powerful supercomputers located at a few key universities and laboratories owned by the military, defense contractors, and university laboratories conducting defense-related research.
- The Internet, evolved into this worldwide system of systems that connects the world and that we now call cyberspace!

Cyberspace and Cybersecurity

- National Institute of Standards and Technology (NIST)
  - Cyberspace is "a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

  - Cybersecurity – is "the ability to protect or defend the use of cyberspace from cyber attacks." http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Time's flying away surrender or else...

The bottom line when you have no cyber security

Col Charlie Flores, USAF (Ret)

Cyber Security Statistics from Verizon

Verizon 2014 | Data Breach Investigations Report

Conducted by Verizon with contributions from 50 organizations from around the world.

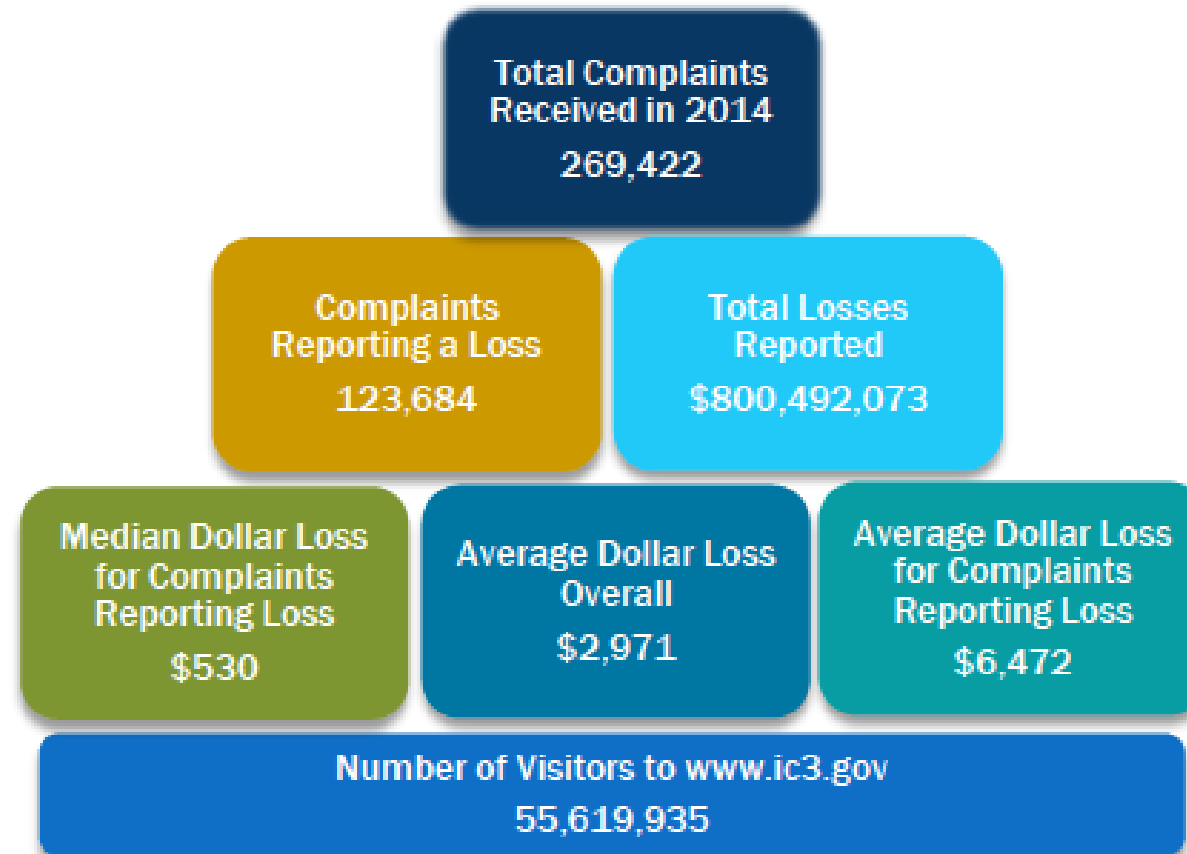**Energy/Utilities**
Just two patterns—web app attacks and crimeware—covered 69% of all incidents.

Public Sector
The most frequent incidents were errors (34%), insider misuse (24%), crimeware (21%) and lost/stolen assets (19%).

Healthcare
Physical theft and loss of assets occurred most often in the office—not from personal vehicles or homes.

Travel/Hospitality
Three-quarters of the attacks targeted POS devices and systems—a good argument for PCI compliance.

38% Web app attacks were responsible for the highest number of incidents.

98% Just four patterns accounted for almost all attacks.

46% of security incidents were the result of lost or stolen assets.

75% Most attacks came from point-of-sale intrusions—highest for all industries.

92% of all security incidents we analyzed over a ten-year period fit into nine basic patterns.

75% The majority of incidents came from web app attacks, DOS, and card skimming.

54% Combined number of attacks from cyber-espionage and DOS.

37% Number of incidents attributed to DOS attacks.

33% DOS attacks were most frequent, followed by point-of-sale intrusions (31%).

Nine classification patterns covered the majority of security incidents.

In 2013, we analyzed over 63,000 security incidents and more than 1,300 confirmed breaches to provide new insight into your biggest threats and to help improve your defenses against them. This year's report identifies nine basic patterns that covered 92% of all the 100,000 security incidents we've looked at from the past 10 years.

- Point-of-Sale Intrusions
- Web Application Attacks
- Insider Misuse
- Physical Theft/Loss
- Miscellaneous Errors
- Crimeware
- Card Skimmers
- Denial of Service Attacks
- Cyber-Espionage
- Everything Else

ENERGY AND UTILITIES — FINANCIAL SERVICES — MANUFACTURING — PUBLIC SECTOR — PROFESSIONAL SERVICES — HEALTHCARE — TRAVEL AND HOSPITALITY — RETAIL

* Payment Card Industry (PCI) Data Security Standard

FBI's Internet Crime Complaint Center (IC3) 2014 Cyber Crime Statistics
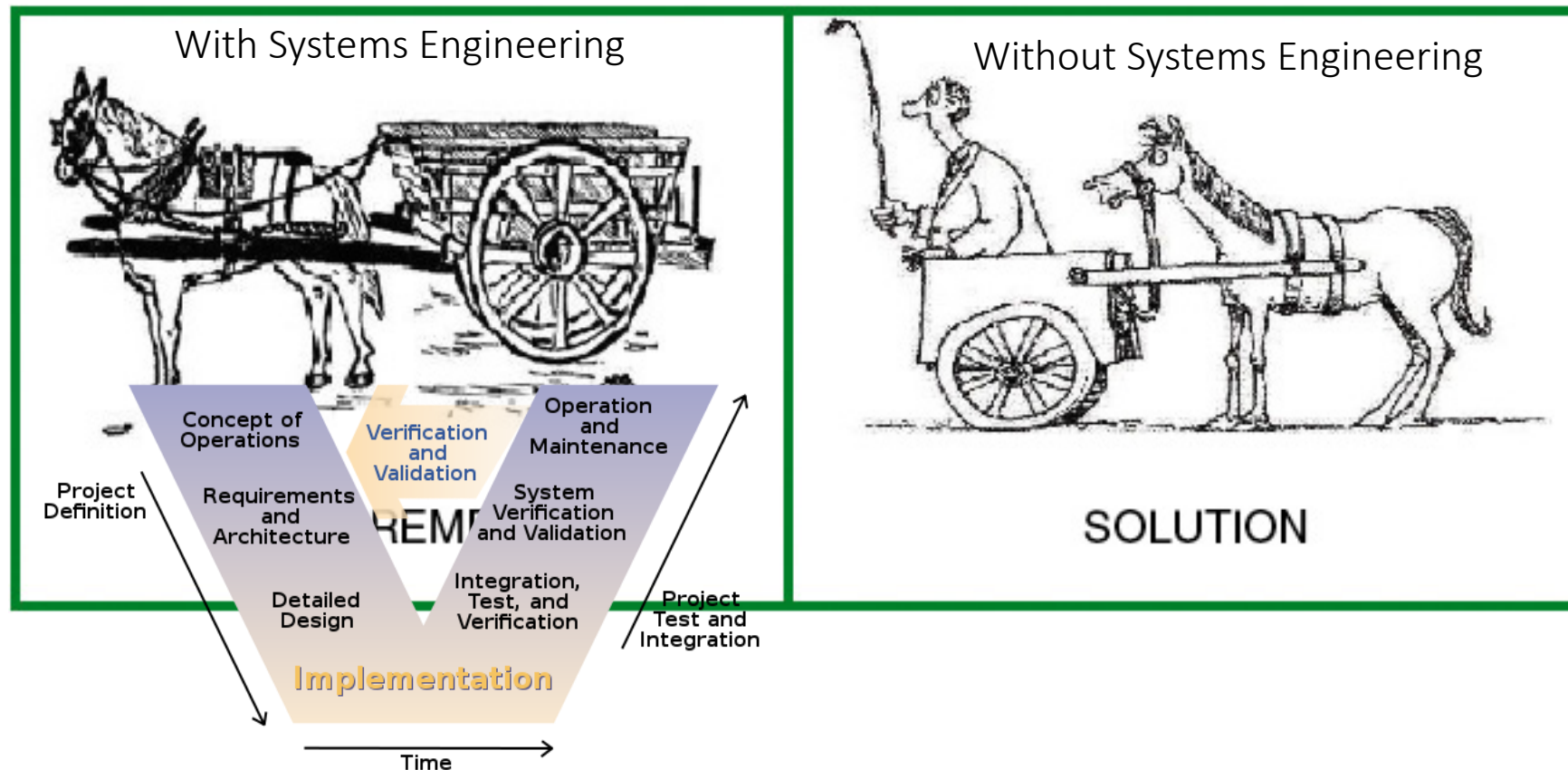
2014 Overall Statistics

Total Complaints Received in 2014
269,422

Complaints Reporting a Loss
123,684

Total Losses Reported
$800,492,073

Median Dollar Loss for Complaints Reporting Loss
$530

Average Dollar Loss Overall
$2,971

Average Dollar Loss for Complaints Reporting Loss
$6,472

Number of Visitors to www.ic3.gov
55,619,935

http://www.ic3.gov/media/annualreport/2014_IC3Report.pdf

Tactical vs Strategic effects

- Tactical – at the "you, me , us" level
  - Affects you personally: you, your family, your immediate friends
  - Personal data leaked for future gain?

- Strategic – "the big picture"; at the "National" or "Global" levels
  - Affects the nation as a whole: banks, hospitals, first responders, etc.
  - Global effects: Government relationships, alliances, global reputation
  - "The JPMorgan Chase & Co. data breach affected 76 million households and seven million small businesses"*…
  - "JPMorgan Chase will invest $250 million and have a staff of 1,000 committed to IT security"*
    - *Source: IBM and Ponemon Institute 2015 Cost of Data Breach Study: Global Analysis.

Col Charlie Flores, USAF (Ret)

Why does Systems Engineering deliver Cybersecurity?

With Systems Engineering

Without Systems Engineering

Concept of Operations

Verification and Validation

Operation and Maintenance

Project Definition

Requirements and Architecture

System Verification and Validation

Detailed Design

Integration, Test, and Verification

Project Test and Integration

Implementation

Time

SOLUTION

Cyber Pearl Harbor... Solar Sunrise 1998
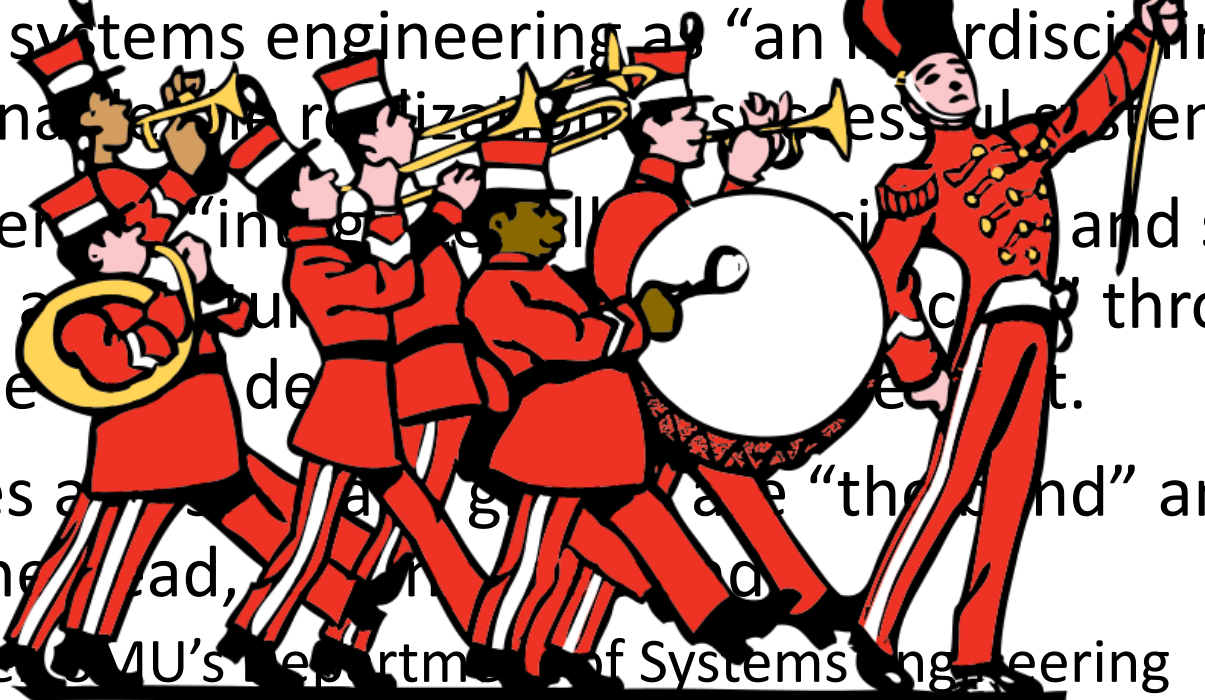
Col Charlie Flores, USAF (Ret)

Solar Sunrise

- Occurred in 1998
- Three "kids" – two in the US and one in Israel
  - They breached DoD networks and research networks
- Basically, they took advantage of system misconfigurations or known system vulnerabilities to access data for which they were not authorized
  - No classified networks were accessed
  - Caused temporary panic
  - Nothing was intentionally destroyed
- Many lessons learned by good guys and bad guys alike!
  - It took another 11 years to standup national cyberspace defense capabilities
- Cyberspace, like land, sea, air and space will require a separate force
  - Cyber warriors must be a blend of disciplines
  - Intelligence, Communications, Science, Engineering plus dreamers
    - Some of the best programmers I've known were artists first
  - Systems Engineers are force multipliers; deliver these skills and more

Systems Engineering

- INCOSE defines systems engineering as "an interdisciplinary approach and means to enable the realization of successful systems".

- Systems Engineering "integrates all the disciplines and specialty groups" ... "into a team effort forming a structured through a system's lifecycle ... development to production.

- These disciplines are marching as one a "the band" and the systems engineer is at the head, with a band leader.
  - Dr. Jim Hinderer, SMU's Department of Systems Engineering
  - Dr. Jerrell Stracener, SMU's Founder and Director Systems Engineering Program

Cybersecurity

What operating system and software should it use?

What do we want?

Who builds the hardware?

Who will assemble it?

What is it for?
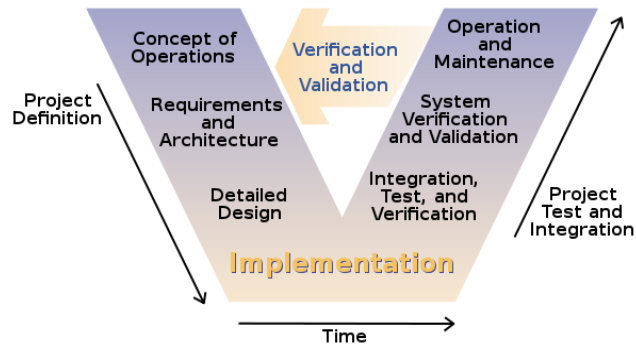
Systems Engineers are too expensive

Antivirus and a firewall should be enough

"Secure Intranet"

I want your data

Hello, I'm available

Bad design

Col Charlie Flores, USAF (Ret)

Going to the Moon!

No
COTS
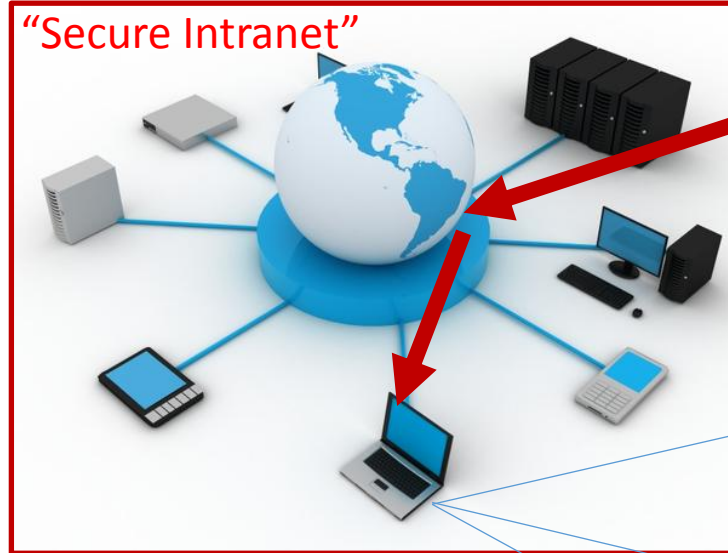
Leadership

Cou[...]
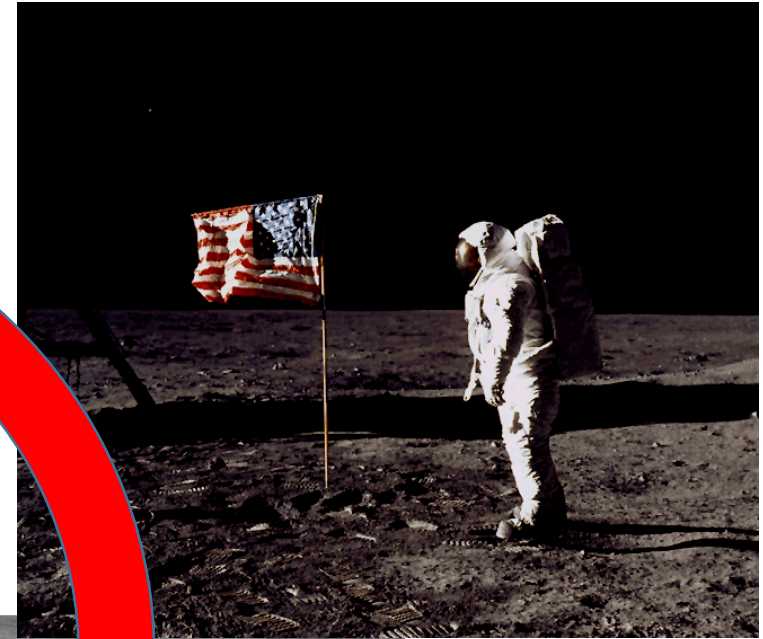
Success!

Determination

Systems Engineering

Defense-In-Depth

- People - We train people to use tools properly

- Technology - Tools to do the job

- Policies - We offer people the procedures "do's and don'ts" for properly utilizing that technology to accomplish the business' mission

Col Charlie Flores, USAF (Ret)

"*Give me your tired, your poor, Your huddled masses*"….

Col Charlie Flores, USAF (Ret)

Cybersecurity

- If Cyberspace represents the world of "interconnected systems", then securing those systems must be cyber security

- Cybersecurity according to NIST
  - The ability to protect or defend the use of cyberspace from cyber attacks.

- It is a bit more complicated … applying defense-in-depth principles

- People – we want to ensure people understand the technology they use

- Technology – because technology is costly, especially when it represents an investment in new designs, we want to protect those designs, our investment and research. We want to support our customer's request to protect their data and the systems and the mission supported or performed by those systems

- Policies - we provide procedures and guideline describing how to properly use the systems in accordance with our rules. We describe authorized and unauthorized use and disclosure of data relevant the new design or mission

- Therefore, we're protecting information, the information within the systems and the ability of the people and systems to properly communicate with other authorized systems and users.

- **Computer Network Defense** (CND): Includes actions taken via **computer networks** to protect, monitor, analyze, detect, and respond to **network** attacks, intrusions, disruptions, or other unauthorized actions that would compromise or cripple **defense** information systems and **networks**. https://www.nsa.gov/careers/career_fields/netopps.shtml

Col Charlie Flores, USAF (Ret)

From Systems Engineering to Cybersecurity

- Since systems engineering enables a disciplined process to develop and deliver technology successfully throughout a system's lifecycle, it follows that systems engineering can and must be the focus to enable cybersecurity

- From defense-in-depth
  - Together with the customer/user, systems engineers:
    - Lead the technology development process – from cradle to grave
    - Work with users to train them in the proper use of [their] technology
    - Develop the policies that affect users, the use of systems and the equities of the customer that need confidentiality

- Without systems engineering, there is no cybersecurity!

Questions?

Col Charlie Flores, USAF (Ret)