The Need for Cybersecurity Standards

As of 10 Feb 2015

COL Charles T. Ames, Mr. Patrick A. Thompson and Mr. Robert L. Laughman

U.S. Army Evaluation Center

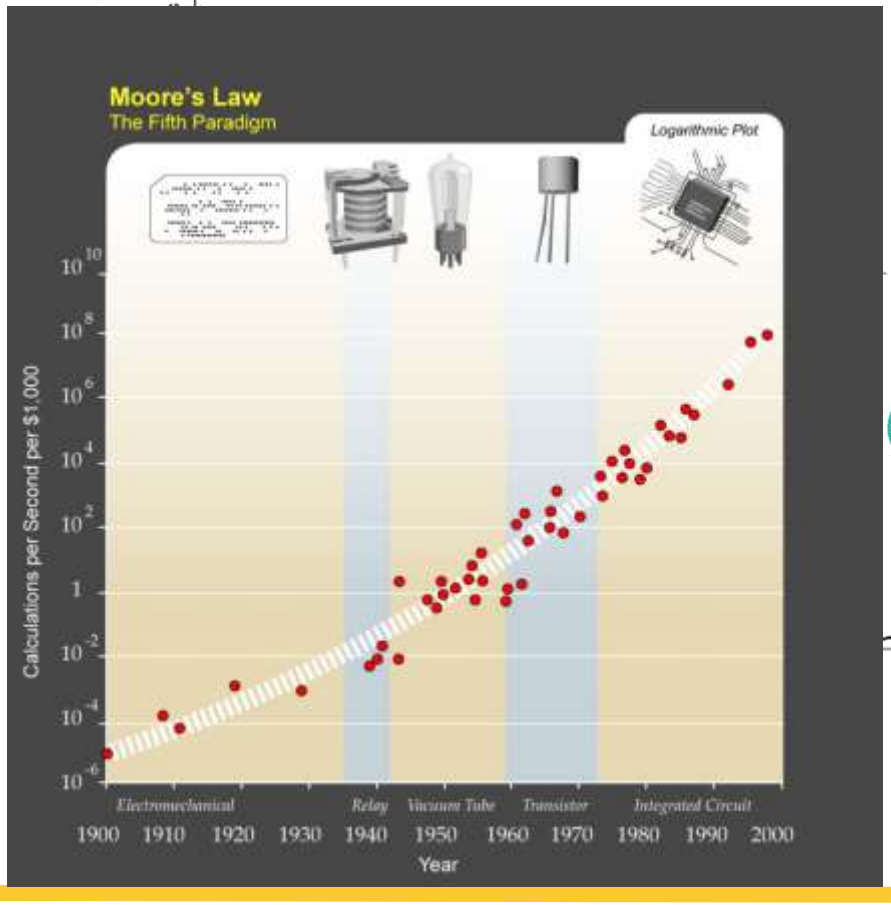
Understanding

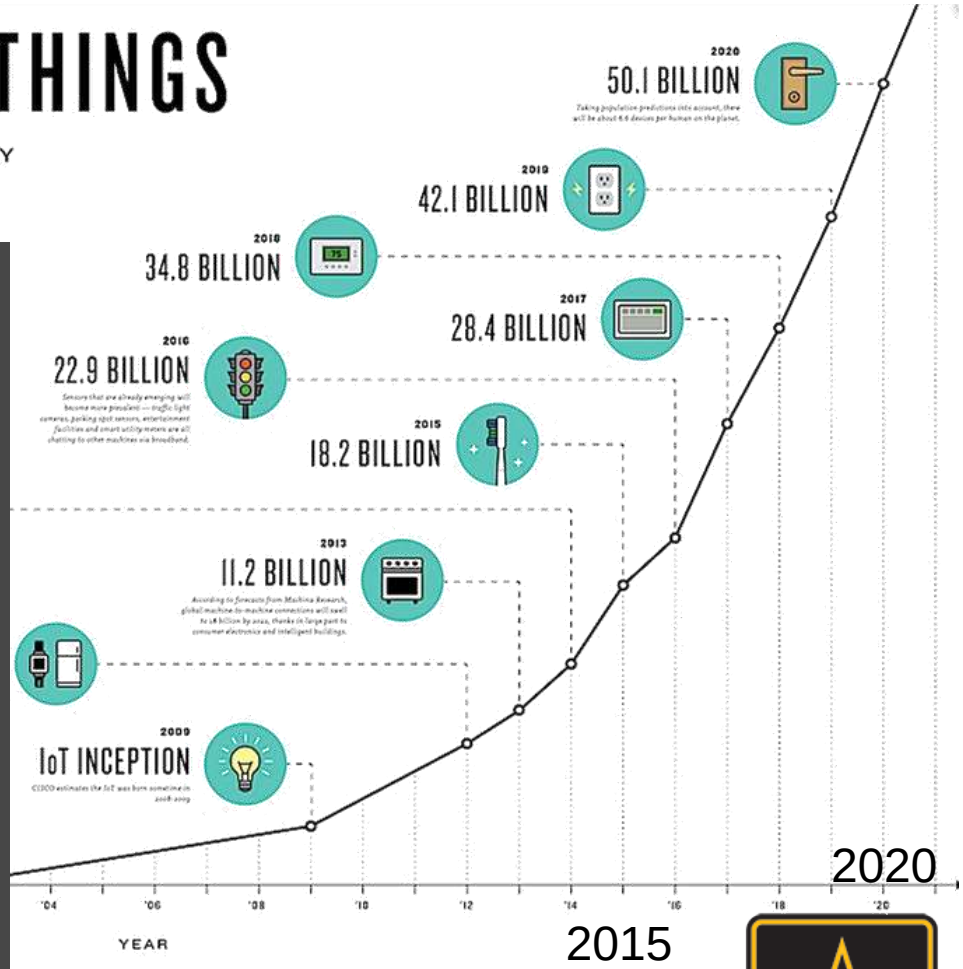
Approved for public release; distribution is unlimited.

Agenda

- Why the new emphasis?
- Trends
  - Technology
  - Cyber Security
- Testing & Evaluation
  - New Approaches
- Challenges
- Standards

Engineers demonstrate live hardware, in this case a radio, being emulated and tested in a lab setting, while the adjoining image shows a drawing of the radio used in the field.


Moore's Law
The Fifth Paradigm
Logarithmic Plot
Calculations per Second per $1,000
Electromechanical
Relay
Vacuum Tube
Transistor
Integrated Circuit
1900 1910 1920 1930 1940 1950 1960 1970 1980 1990 2000
Year

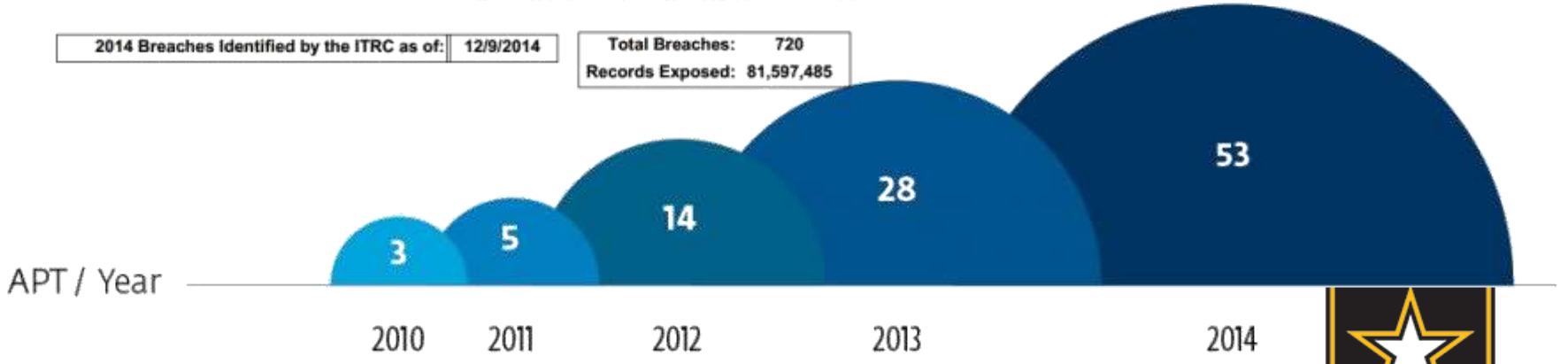

THE INTERNET OF THINGS
AN EXPLOSION OF CONNECTED POSSIBILITY
2020
50.1 BILLION
2019
42.1 BILLION
2018
34.8 BILLION
2017
28.4 BILLION
2016
22.9 BILLION
2015
18.2 BILLION
2013
11.2 BILLION
2009
IoT INCEPTION
'04 '06 '08 '10 '12 '14 '16 '18 '20
YEAR
2020
2015

Reported Breaches by Year

Totals for Category:	Banking/Credit/Financial	# of Breaches: 41	# of Records:	1,182,492
		% of Breaches: 5.7%	%of Records:	1.4%
Totals for Category:	Business	# of Breaches: 237	# of Records:	64,731,975
		% of Breaches: 32.9	%of Records:	79.3%
Totals for Category:	Educational	# of Breaches: 54	# of Records:	1,243,622
		% of Breaches: 7.5%	%of Records:	1.5%
Totals for Category:	Government/Military	# of Breaches: 84	# of Records:	6,494,683
		% of Breaches: 11.7	%of Records:	8.0%
Totals for Category:	Medical/Healthcare	# of Breaches: 304	# of Records:	7,944,713
		% of Breaches: 42.2	%of Records:	9.7%
Totals for All Categories:		# of Breaches: 720	# of Records:	81,597,485
		% of Breaches: 100.0	%of Records:	100.0%

2014 Breaches Identified by the ITRC as of:	12/9/2014

Total Breaches:	720
Records Exposed:	81,597,485



Operational Cybersecurity Testing

Blue Team Assessment Tools

- Nmap – network mapping, traffic generation
- Q-Tip, Retina, Nessus – signature based vulnerability scanners, malware signatures updated daily
- SCAP Compliance Checker – Automated scanner of systems based on DISA Secure Technical Implementation Guidelines (STIGs)
- Burp Proxy – web application proxy (man-in-the-middle for assessing web application vulnerabilities)
- Wireshark, Tcpdump – traffic analysis, can capture wired and wireless packets.
- John, Cain – password crackers
- THC-Hydra – password guessers

Red Team Assessment Tools

- Nmap – covert network mapping, firewall evasion, traffic generation
- Metasploit – exploitation and post-exploitation toolset (exploits vulnerabilities and delivers a payload)
- Meterpreter – Windows Metasploit Payload used for keyboard logging, enabling camera, microphone, data theft, maintaining access, and covert communications.
- Burp Proxy, Zed Attack Proxy –web application attacks
- BEEF— web browser exploitation toolset
- MimiKatz – memory forensics
- Cobalt Strike – advanced exploitation toolset with graphic interface
- John, Cain – password crackers
- THC-Hydra – password guessers

Cybersecurity Testing

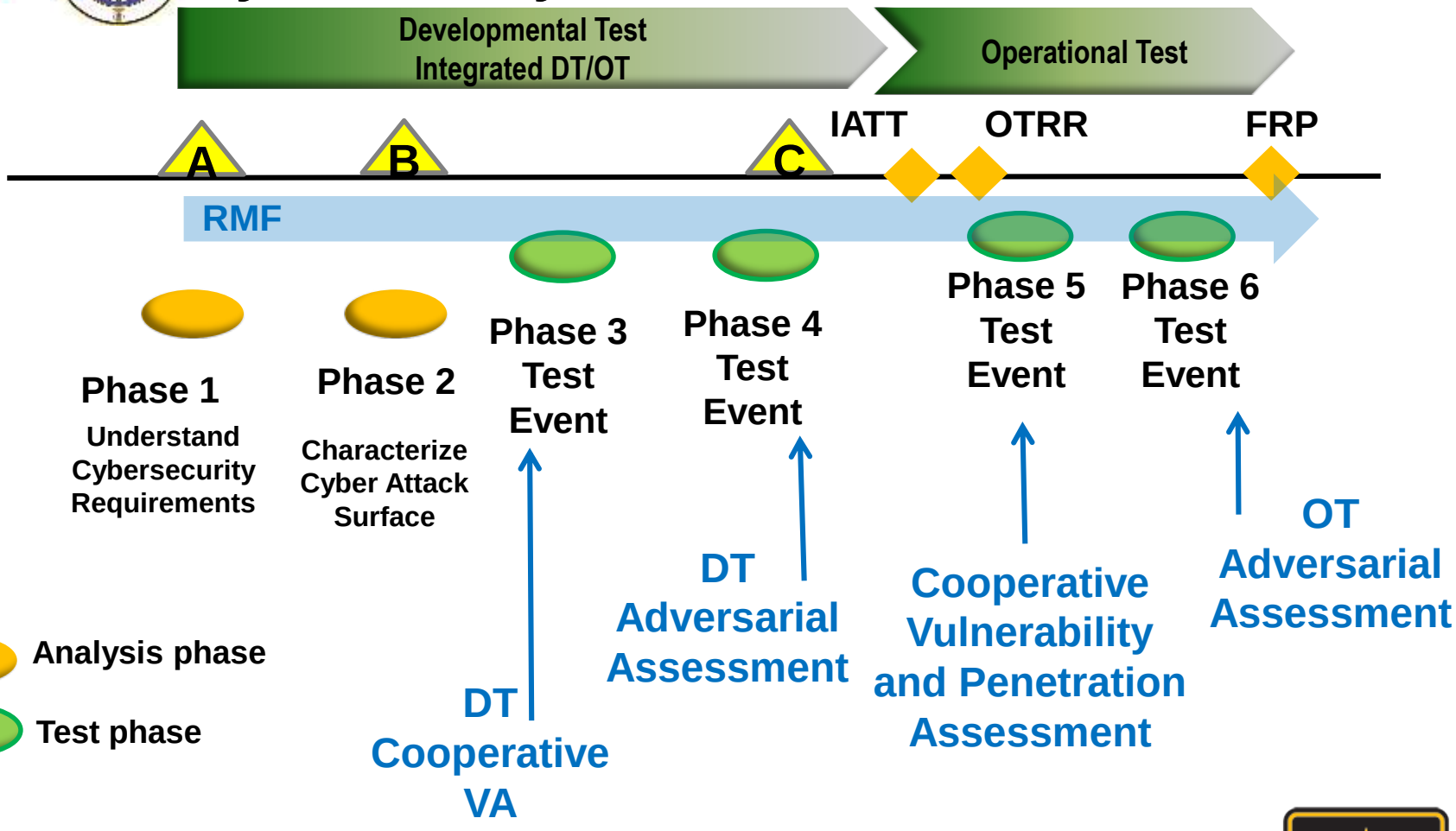
- Shift Left
  - Formally add cybersecurity DT to the TEMP
- ATEC: Leverage existing test capabilities rather than build new
- Build T&E plans starting with Risk Management Framework (RMF) products
  - RMF replaces DIACAP with intent to manage risk over the system's lifecycle
- Score Card

Planning for (event/milestone)

Event	Score	Comments
TEMP	G Y R	Date; Unresolved Issues, related to DOT&E Attachment D
Draft TEMP Part II	G Y R	Date; Unresolved Issues
OTRR 1, T-240	G Y R	Date, Venue, ARL Lead; Unresolved Issues
TAWG	G Y R	Date; Unresolved Issues
Core System Protection, and Core Cyber Defense Performance – Data and Metrics	G Y R	Unresolved Issues, related to DOT&E Attachment C
Operational Test Plan	G Y R	Unresolved Issues, related to DOT&E Attachment E
1st (DT) Blue Team Assessment	G Y R	Date; Unresolved Issues
1st (DT) Red Team Assessment	G Y R	Date, Venue, TSMO Lead; Unresolved Issues
OTRR 2, T-90	G Y R	Date; Unresolved Issues
Verification of Fixes	G Y R	Date, Venue, Provider; Unresolved Issues
OTRR 3, T-5	G Y R	Date; Unresolved Issues
2nd (OT) Blue Team Assessment	G Y R	Date, Venue, ARL Lead; Unresolved Issues
2nd (OT) Red Team Assessment	G Y R	Date, Venue, TSMO Lead; Unresolved Issues

Shift Left

Cybersecurity T&E Earlier Than IOT&E



Events derived from draft DASD(DT&E) DoD Cybersecurity Test and Evaluation Guidebook, and DOT&E Cybersecurity Operational Test and Evaluation Guidance Memo (01 August 2014)

Cybersecurity Test and Evaluation Approach
Major Software Updates

Cybersecurity T&E approach (IAW AR 25-2, DoDI 8510.01, and DASD(DT&E) & DOT&E guidance*) mitigates software and security risks of fielding unproven platform equipment. Applicable data will be leveraged whenever available.

Software Drop Post-OEM Testing | **Software Drop Post-DT** | **Software Drop Post-OT**

Cybersecurity Test and Evaluation Approach

OEM Cybersecurity Testing → **DT Cybersecurity Testing** → **OT Cybersecurity Testing** → **Software Lifecycle Maintenance**

Subsystem Examples

New Hardware	- Computing Systems - Improved Displays - New Processor Units - Maneuver Control Enhancements
New Software	- Cross Domain Solution Adjustments - Enhanced Training - Improved Vehicle Management - Improved Communications Manager
Existing Evaluation New Integration	- CREW Device - Tactical Communication Devices - Battle Command Systems - Power Distribution Systems

"Cybersecurity requirements must be identified, tailored appropriately, and included in the acquisition, design, development, developmental and operational testing and evaluation, integration, implementation, operation, upgrade, or replacement of all DoD Platform Information Technology IAW DoDI 5200.44 and DoDI 5200.39, this instruction, and other cybersecurity-related DoD guidance, as issued."

(Ref: DoDI 8510.01)

Challenges for T&E

- OSD policies on cybersecurity T&E still draft
  - DoDI 5000.02 states need for cybersecurity in DT
  - AR 73-1 Draft in Process
- Modeling & Simulation
- Operational Requirements
- Addressing DOTMLPF
  - Training and CND activity at Echelon
- Metrics – Work underway with MIT-LL
  - Measurable, Testable, Repeatable
  - Configuration

NDIA Summit DoD Program Protection

May 19-22 2014

Security Engineering Challenges

•Incorporation of security engineering as a discipline of systems engineering

–Engineering methodology, processes, and practices

–System security engineering workforce

•Quantification of security risks

–Vulnerability detection, and validated mitigation

•Articulation of security requirements

–Threat-driven, evolving over time

–Risk-based affordable trade off analysis; Measurable, testable system specifications

•Protection of technical data

–Consequences of unclassified controlled technical information losses

Common Themes:

- **Security Engineering as Discipline**
- **Earlier & Often in the Development Process**
- ***Architecture***
- **In Contracts: Part of Section L and M in RFPs**
- **Cyber Testing**

http://www.ndia.org/Divisions/Divisions/SystemsEngineering/Pages/Past_Projects.aspx

Standards

Definition of a Standard – an idea or thing used as a measure, norm, or model in comparative evaluations

Using this definition

- Standards in Operational Context
- Contracts
- Architecture
- Test and Evaluation Methods

Standards -1

- Standards in Operational Requirements
  - Critical Performance Parameter
  - "If there is a computer in something, it *can* be cyber-attacked, and we need to be able to harden it and defend it," the Pentagon's Deputy Chief Information Officer for Cybersecurity Mr. Richard Hale
    - "The Joint Staff has recently put out a formal requirement document that includes cybersecurity as a key part of the survivability key performance parameter [KPP]" for every new system"
  - Concept of Operations
    - Context of Use – Mission Related

Defensible Systems

U.S.ARMY

http://breakingdefense.com/2015/01/cybersecurity-now-key-requirement-for-all-weapons-dod-cio/

Standards -2

- Standards in Contracts
  - RFPs Section L and M
  - CDRLs
  - Core NIST Criteria

Standards -3

- Architecture
  - DoDAF Framework Views
  - Cybersecurity Views?
    - Design of Defense layered onto the Network
    - Encryption Details

Standards -4

- **Test & Evaluation**

- **Addressing DOTMLPF**
  - **Training and CND activity at Echelon**

- **Metrics – Work underway with MIT-LL**
  - **Measurable, Testable, Repeatable**
  - **Configuration,**
  - **IAVA's**
  - **STIGs**


Cybersecurity Challenge
There's one thing more complicated than the
cybersecurity problem!
Yea!
The solution ...