[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Using Data to Define Current Security Knowledge Gaps

Carol Woody, Ph.D.
Principal Researcher

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Copyright 2021 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

DM21-0987

Software is Everywhere and it is All Data

You think you're building (or buying, or using) a product such as:

car or truck	satellite	mobile phone	development tools
home security system	aircraft	pacemaker	security tools
home appliance	financial system	bullets for a gun	

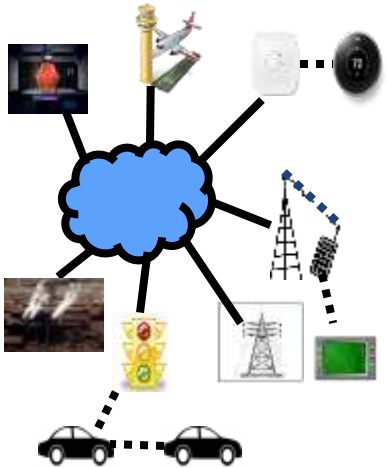
Actually you're getting ***a software platform:***

- Software is a part of almost everything we use.
- Software defines and delivers component and system communication.
- Software is used to build, analyze and secure software.

All software has defects:

- Best-in-class code has <600 defects per million lines of code (MLOC).
- Good code has around 1000 defects per MLOC.
- Average code has around 6000 defects per MLOC.

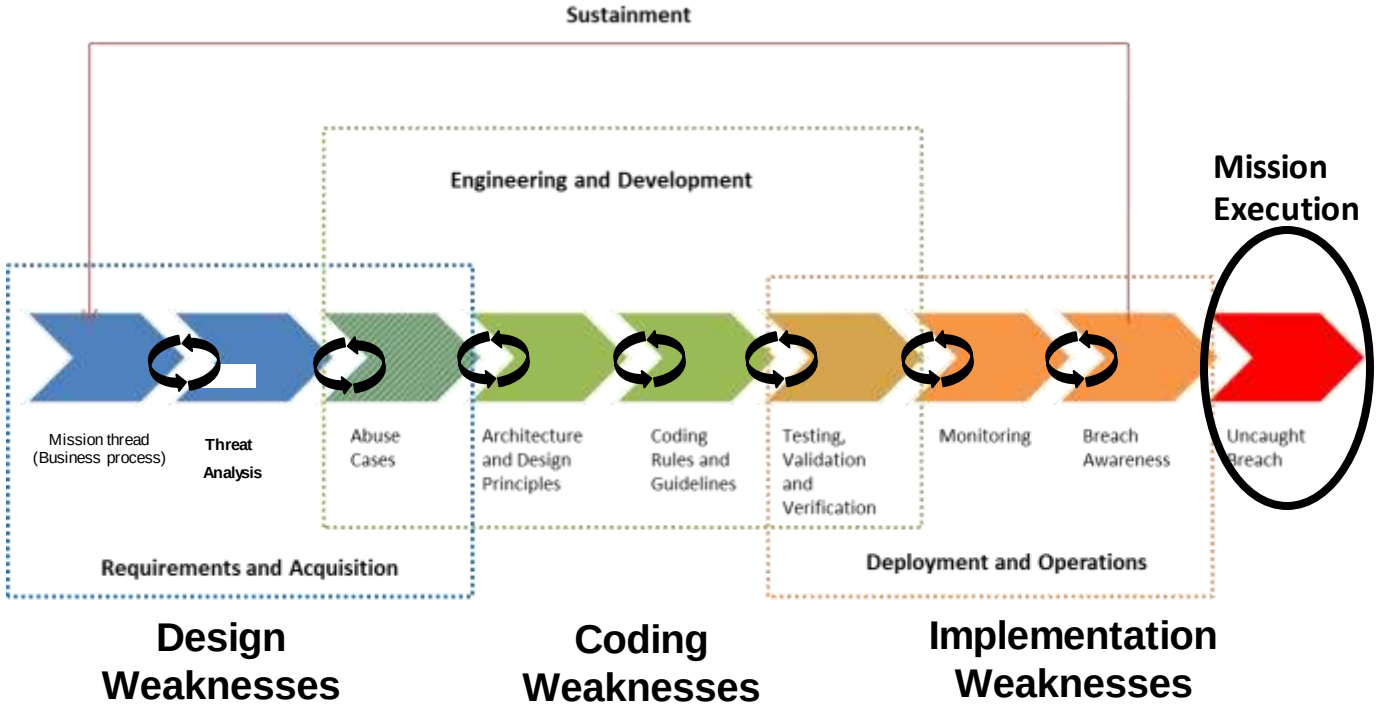
(based on Capers Jones research http://www.namcook.com/Working-srm-Examples.html)



© 2021 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

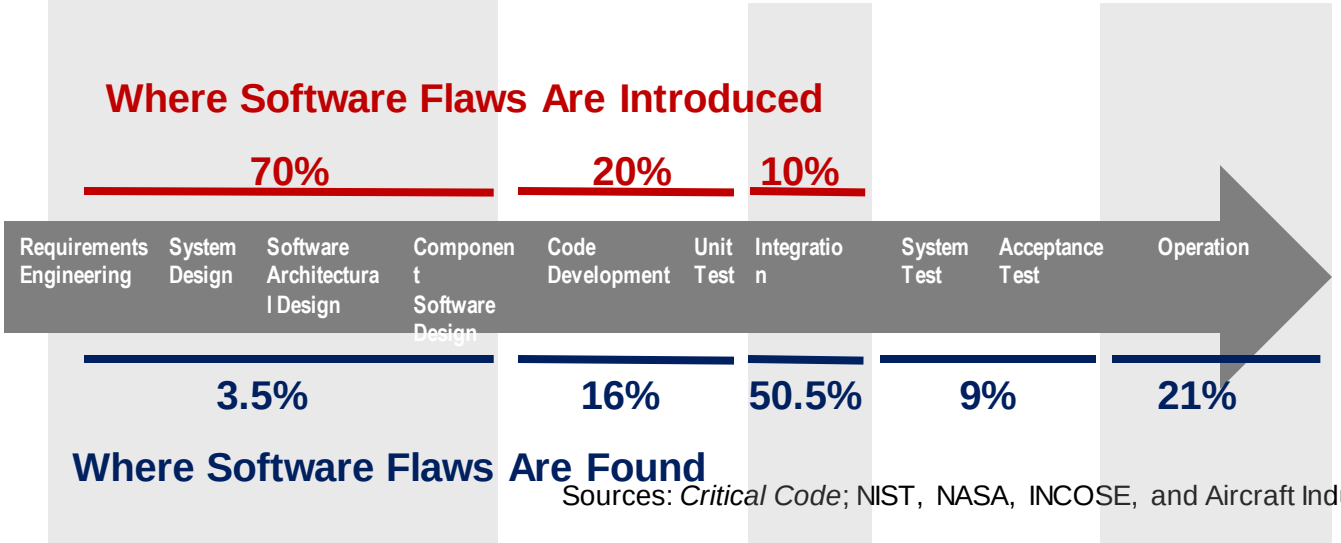
Many Hands Contribute the Security of the Product



© 2021 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

What Does the Data Tell Us About Defects in Software?



Sources: *Critical Code*; NIST, NASA, INCOSE, and Aircraft Industry Studies

All software code contain defects; up to 5% are vulnerabilities

ref: Woody, Carol et al. *Predicting Software Assurance Using Quality and Reliability Measures* http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=428589)

Hundreds of thousands of known software vulnerabilities exist in operations

ref: NIST National Vulnerability Database, https://nvd.nist.gov/general/nvd-dashboard

© 2021 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Today, Operations Plays Whack-a-mole Chasing Attacks

Rapid delivery of features is prioritized over defensibility, reliability, and stability.

Operational missions are jeopardized by weak designs that allow attackers to leverage the many vulnerabilities.

Once software's in an operational system, vulnerabilities can be difficult (or impossible) to mitigate.

© 2021 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Major Shifts In Processes and Design Add Cybersecurity Risk

From…	To…
Hardware-based solution	Software-intensive system
Waterfall methodology	Agile at scale approach
Organization owned infrastructure	Shared infrastructure (e.g. Cloud)
Compliance verification upon completion before fielding (e.g. ATO)	Continuous integrated monitoring (e.g. cATO)
Systems developed from requirements and architectural designs	Systems assembled primarily from reused (often 3rd party) components that map to requirements
Development life cycle tailored to the system under development	DevSecOps Development Factory using 3rd party tools and automation

© 2021 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Key Knowledge Gaps

- System Engineers are not required to understand software
- Systems Engineers are not learning from current operational experience
- Acquisitions can be defined using standards, guidelines, and controls as a substitute for effective system security requirements
- Program Managers are not required to define and manage the risk of software failure

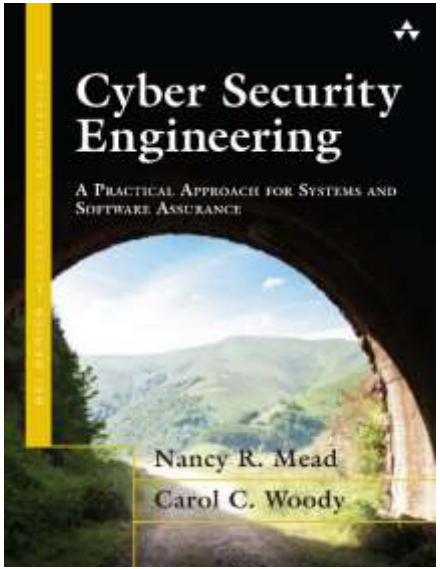
© 2021 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

My Contributions to the Knowledge Gaps

Textbook

Cybersecurity Engineering



SEI Book Series

Professional Certificate

CERT Cybersecurity Engineering and Software Assurance

https://sei.cmu.edu/education-outreach/credentials/credential.cfm?customel_datapageid_14047=33881

Online training in five components

- Software Assurance Methods in Support of Cybersecurity Engineering
- Security Quality Requirements (SQUARE)
- Security Risk Analysis (SERA)
- Supply Chain Risk Management
- Advanced Threat Modeling

© 2021 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Contact Information

Carol Woody, Ph.D.

cwoody@cert.org

Web Resources

Building security into application lifecycles

https://sei.cmu.edu/research-capabilities/all-work/display.cfm?customel_datapageid_4050=48574

CMU SEI Home Page

https://sei.cmu.edu/

© 2021 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.