



Weaving a Fabric of Trust

Ensured Security, Privacy, Resilience, and Accountability

Dr. Greg Shannon
Chief Scientist

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Copyright 2017 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

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.

Carnegie Mellon® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

CERT® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM17-0308

First Bits

Congressional Testimony on Understanding the Cyber Threat and Implications for the 21st Century Economy

Mar 3, 2015 U.S. House of Representatives
(114th Congress)

Hearing before the Subcommittee on Oversight and Investigations of the Committee on Energy and Commerce.

Question was...

“How do businesses deal with consumers and inform and educate them as to what they are doing to create the virtual marketplace, and prohibit incursions in cyber?”





E WHITE
WASHINGTON

Consistent Approach



Official White House Photo by Chuck Kennedy



Associated Press/Pablo Martinez Monsivais

NIST Framework

NIST

☰ NIST MENU

CYBERSECURITY FRAMEWORK

Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure

Cybersecurity Framework (PDF)

Cybersecurity Framework (Excel)

Draft Version 1.1

Industry Resources

Frequently Asked Questions

Events and Presentations

News


CSF Reference Tool

Workshops


Additional Information +

Latest Updates

- Cybersecurity Framework Workshop on May 16-17, 2017 at NIST in Gaithersburg, Maryland – [Agenda, Webcast & Presentations](#)
- To support agency heads in responding to the Presidential Executive Order on [Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure](#), NIST released the draft Interagency Report 8170 [The Cybersecurity Framework: Implementation Guidance for Federal Agencies](#)
- The [initial analysis](#) of [stakeholder comments](#) on the [proposed Cybersecurity Framework updates](#) is available. See also [Federal Register notice](#); [Frequently Asked Questions](#)
- [Video and downloadable presentations](#) are available on Cybersecurity Framework overview and proposed updates



Cybersecurity Framework Shared



The Cybersecurity Framework

Building the Future

What's the problem we're trying to solve?



Building the Future

What's the hard part of the problem?



Building the Future

Where's the “promise of possibility”?



Building the Future

What can we do?

What can YOU do?!?

Let's do it.



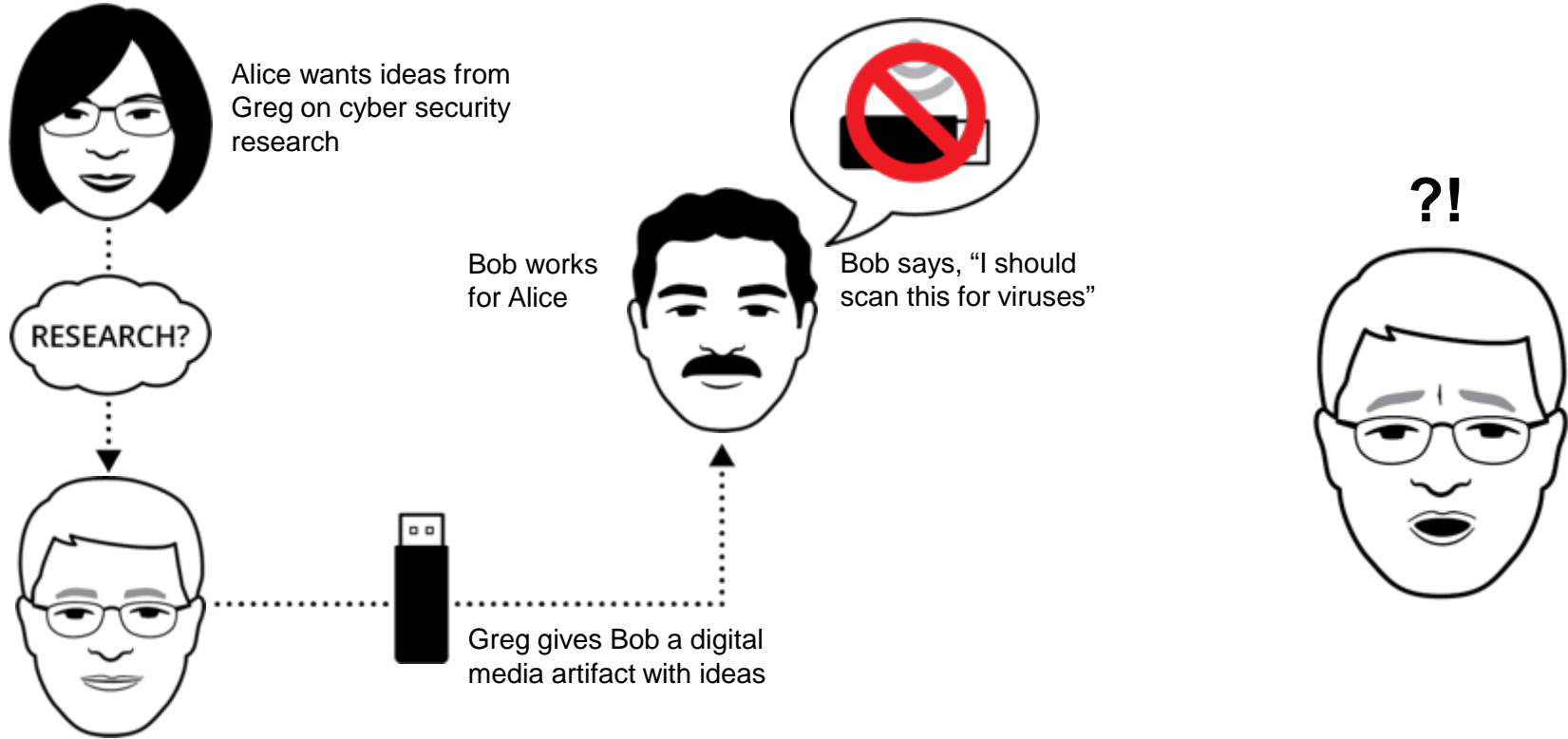
The Takeaway



Trust



2006 Aha! Trust Rabbit Hole





Digital Intermediation?

What might we lose?

What might we gain?



The Essence of Trust



Trust in a Digital World



Breaking Trust

Building Trust



Engineering Dilemmas

Engineering Trust



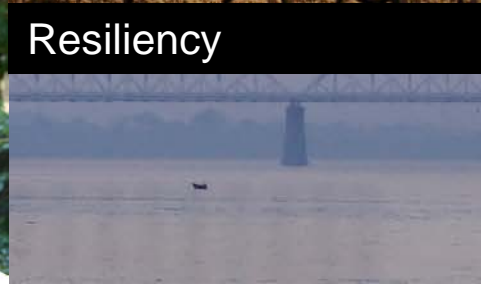
Security



Privacy



Resiliency



Accountability



Trust Poll

What matters MOST to you in building, growing, and sustaining TRUST?

- * Security
- * Privacy
- * Resilience
- * Accountability

Discussion

Ensure

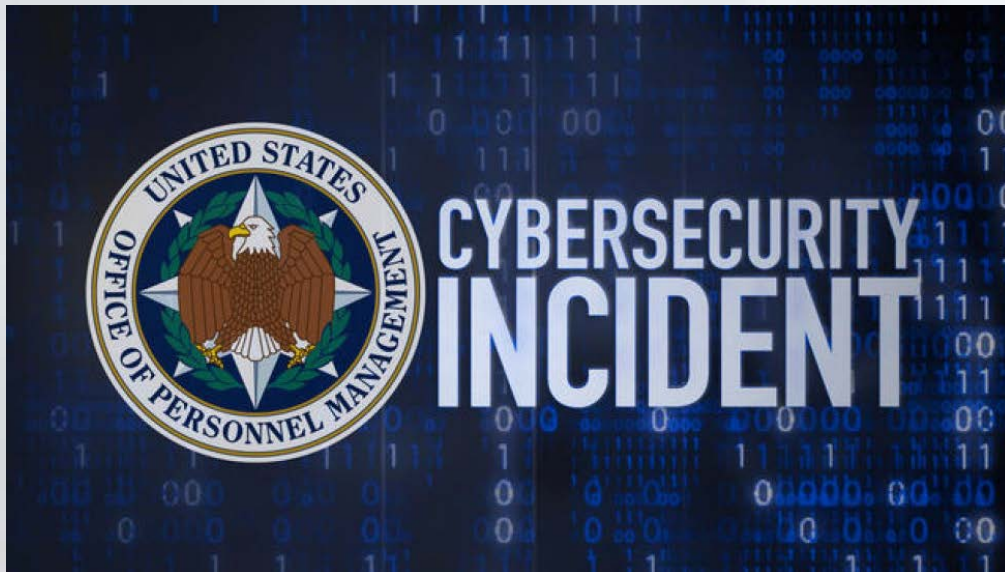
Cyber Delusions



Cyber Delusions



Cyber Delusions



Cyber Delusions

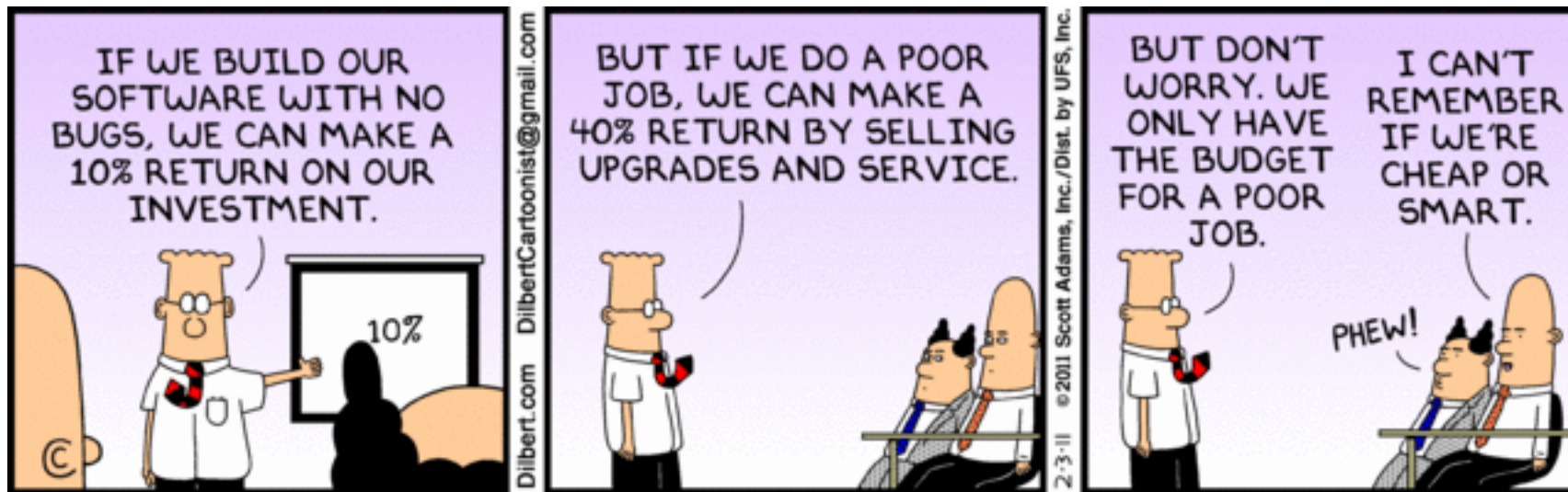


PHOTO: JOHN R. COUGHLIN/CNNMONEY





Security Built in?



<http://www.dilbert.com/strips/2011-02-03/>

2014 Aha! Cyber Energy Barrier



Selected Typing Rules.

$$\begin{array}{c}
 \text{Obj} \frac{\Gamma \vdash e_i : \tau_i \quad i \in [1..n]}{\Gamma \vdash \{x_1 : e_1, \dots, x_n : e_n\} : \{x_i : \tau_i\}_{i \in [1..n]}^*} \quad \text{PropA} \frac{\Gamma \vdash e : \delta \quad \delta <: \{x : \tau\}}{\Gamma \vdash e.x : \tau} \\
 \\
 \text{StrD} \frac{\Gamma \vdash x : \text{string} \quad \Gamma \vdash y : \text{number}}{\Gamma \vdash ((y \ggg = 0) < x.\text{length} ? x[y] : @string) : \text{string}} \\
 \\
 \text{Scope} \frac{\Phi(x) = \tau}{\Gamma, [\Phi]_x \vdash x : \tau} \quad \text{RecScope} \frac{x \notin \text{dom}(\Phi) \quad \Gamma \vdash x : \tau}{\Gamma, [\Phi]_x \vdash x : \tau} \quad \text{Assign} \frac{\Gamma \vdash e_1 : \tau \quad \Gamma \vdash e_2 : \tau}{\Gamma \vdash e_1 = e_2 : \tau} \\
 \\
 \text{With} \frac{\Gamma \vdash e : \{\bar{x} : \bar{\tau}\} \quad \Gamma, [\bar{x} : \bar{\tau}]_o \vdash s : \text{undefined}}{\Gamma \vdash \text{with}(e)s : \text{undefined}} \quad \text{MetDef} \frac{\Gamma \vdash \text{function } (this, \bar{x})\{s\} : (\rho, \bar{\alpha}) \rightarrow \tau}{\Gamma \vdash \text{function } (\bar{x})\{s\} : \bar{\alpha}[\rho] \rightarrow \tau} \\
 \\
 \text{FunCall} \frac{\Gamma \vdash e : \mu \quad \Gamma \vdash \bar{e} : \bar{\alpha} \quad \mu <: \bar{\alpha} \rightarrow \tau}{\Gamma \vdash e(\bar{e}) : \tau} \quad \text{MetCall} \frac{\Gamma \vdash e : \mu \quad \Gamma \vdash \bar{e} : \bar{\alpha} \quad \mu <: \{x : \bar{\alpha}[\rho] \rightarrow \tau\}}{\Gamma \vdash e.x(\bar{e}) : \tau}
 \end{array}$$

Elements of Defensive Deterrence



Impose extreme/intractable resource requirements on adversaries

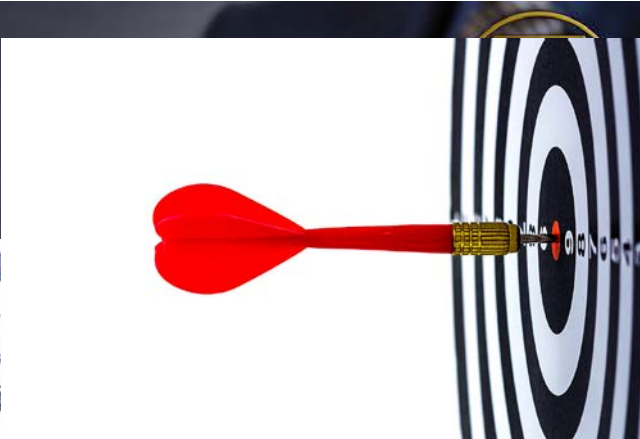
Ensure that small breaches/successes are minor

Ensure that significant attacks are detectable and attributable and recoverable

3 E's for Cybersecurity



Evidence



Efficacy



Efficiency

Foundations for Weaving Trust



Encryption

- Secure communication in the presence of adversaries

Formal Methods

- Logic-based techniques for the specification, development, and verification of protocols, software, hardware, and systems

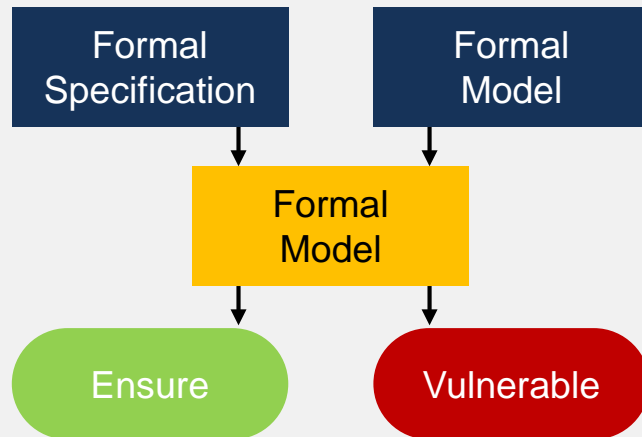
Long-term goal

- Weave together formal methods (warp) with encryption (weft) to expand security, privacy, resilience, accountability

Recent Advances



Encryption



Formal Methods

Ensure Poll

What matters MOST to your organization in **THWARTING** malicious cyber activity?

UNDISCOVERABLE vulnerabilities

UNEXPLOITABLE vulnerabilities

DETECT malicious activities

ATTRIBUTE malicious actors

RECOVER from malicious activities

Discussion

Technologies

1994 Aha! Simple Technology



Startup!





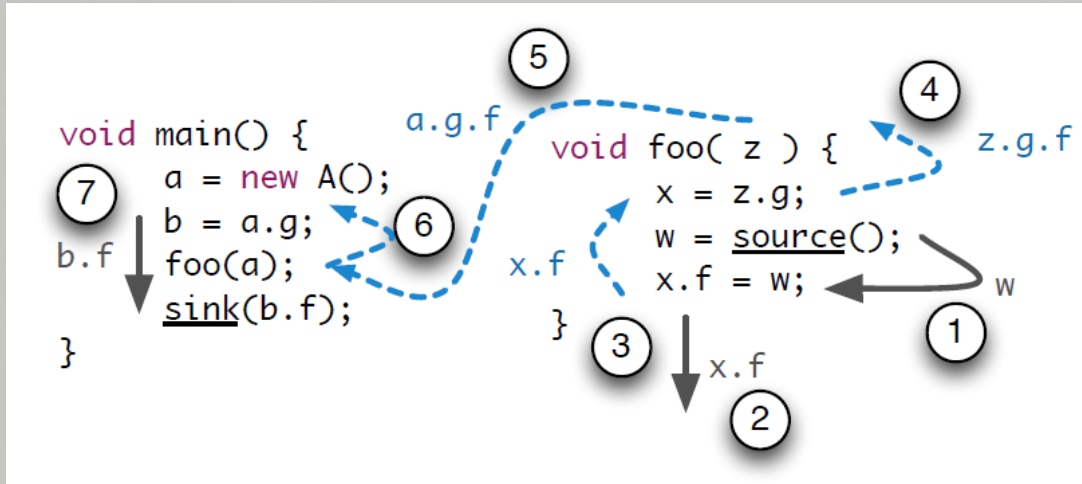
Block Bit Coin Chain

BITCOIN





Android App Sets: Sensitive Dataflow



Cost of Failure

☰ POLITICO Magazine Policy PRO 🔍 👤 🌐 U.S. Edition

- Facebook
- Twitter
- Google +
- Email
- Comment
- Print

Acting U.S. Attorney for Vermont Eugenia Cowles announces a \$155 million settlement to be paid by eClinicalWorks to resolve allegations it misrepresented the abilities of its software and paid kickbacks. | AP Photo

Feds levy \$155M fine against software vendor for faulty patient records

By ARTHUR ALLEN | 05/31/2017 06:56 PM EDT

Share on Facebook Share on Twitter

A leading electronic health records maker and its founders will pay \$155 million to resolve a lawsuit that accused the company of selling faulty software and defrauding the program that subsidized doctors to computerize their patient records, the Justice Department announced Wednesday.

The settlement, the first of its kind involving a health IT company, also states that Massachusetts-based eClinicalWorks paid kickbacks in exchange for promoting its

MOST READ



SYSTEM VULNERABLE

What you can do



Evidence

Efficacy

Efficiency

Technology Poll

What is YOUR outlook on cybersecurity for the next **DECADE**?

very optimistic

optimistic

neutral

pessimistic

very pessimistic

Discussion

SEI /CERT Resources

SEI Blog



- [SEI Blog\(s\)](#)

SEI WEBINAR SERIES | Keeping you informed of the latest solutions

- [SEI Webinars](#)



SEI Cyber Minute

Software Engineering Institute | Carnegie Mellon University • 39 videos • 4,637 views • Updated 4 days ago

In every Cyber Minute video, an SEI expert delivers a quick, informative snapshot of our latest research on the changing world of all things cyber.

▶ Play all

◀ Share

+ Save

- [SEI Cyber Minutes](#)

SEI PODCAST SERIES Conversations in Software Engineering

- [SEI Podcasts](#)

Reading

David DeSteno. *The Truth about Trust*. Hudson Street Press, 2014,

Virgil Gligor and Jeannette M. Wing. 2011. Towards a theory of trust in networks of humans and computers. In *Proceedings of the 19th international conference on Security Protocols (SP'11)*, Bruce Christianson, Bruno Crispo, James Malcolm, and Frank Stajano (Eds.). Springer-Verlag, Berlin, Heidelberg, 223-242. DOI=http://dx.doi.org/10.1007/978-3-642-25867-1_22

Ken Thompson. 2007. Reflections on trusting trust. In *ACM Turing award lectures*. ACM, New York, NY, USA , pages. DOI=<http://dx.doi.org/10.1145/1283920.1283940>

K. Fisher, J. Launchbury, and R. Richards. The HACMS Program: Using formal methods to eliminate exploitable bugs. *Philosophical Transactions A*. Forthcoming.

B.Fuller, et al. 2017. Cryptographically Protected Database Search (Systemization of Knowledge Paper). To appear in *Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP '17)*. IEEE Computer Society, Washington, DC, USA.

Contact Information

Dr. Greg Shannon

Chief Scientist

CERT Division | Software Engineering Institute

Carnegie Mellon University

Telephone: +1 412-268-8545

Email: shannon@cert.org

Web

www.sei.cmu.edu

U.S. Mail

Software Engineering Institute

Customer Relations

4500 Fifth Avenue

Pittsburgh, PA 15213-2612

USA

Customer Relations

Email: info@sei.cmu.edu

Telephone: +1 412-268-5800