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
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?”
NIST Framework

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
What’s the problem we’re trying to solve?
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.
First Bits

The Takeaway
Trust
2006 Aha! Trust Rabbit Hole

Alice wants ideas from Greg on cyber security research

Bob works for Alice

Greg gives Bob a digital media artifact with ideas

Bob says, “I should scan this for viruses”

?!
Digital Intermediation?

What might we lose?  What might we gain?
The Essence of Trust
Trust in a Digital World
Trust Poll

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

* Security
* Privacy
* Resilience
* Accountability
Discussion
Cyber Delusions
Cyber Delusions
Cyber Delusions

PHOTO: JOHN R. COUGHLIN/CNNMONEY
Security Built in?

Selected Typing Rules.

Obj: \[ \Gamma \vdash \text{Obj}(e_1, \ldots, e_n) : \{ \tau_i \}_{i \in [1,n]} \]

PropA: \[ \Gamma \vdash \delta \quad \text{Arr} \vdash \{ \tau \} \]

StrD: \[ \Gamma \vdash x : \text{string} \quad \Gamma \vdash y : \text{number} \]

Scope: \[ \Phi(x) = \tau \]

RecScope: \[ \Gamma, \Phi \vdash x : \tau \]

Assign: \[ \Gamma \vdash e_1 : \tau \quad \Gamma \vdash e_2 : \tau \]

With: \[ \Gamma \vdash e : \{ \delta : \Phi \} \]

function: \[ \Gamma \vdash (\text{this}, \delta) \{ \tau \} : (\rho, \alpha) \rightarrow \tau \]

function (\text{this}, \delta): \[ \Gamma \vdash (\delta) : \delta[\rho] \rightarrow \tau \]

MetDef: \[ \Gamma \vdash e : \mu \quad \Gamma \vdash \delta : \alpha \quad \mu : \alpha \rightarrow \tau \]

FunCall: \[ \Gamma \vdash e(\delta) : \tau \]

MetCall: \[ \Gamma \vdash e, x(\delta) : \tau \]
Elements of Defensive Deterrence

- Impose extreme/intractable resource requirements on adversaries
- Ensure that small breaches/successes are minor
- Ensure that significant attacks are detectible and attributable and recoverable
3 E’s for Cybersecurity

Ensure

Efficacy

Evidence

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
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
Block Bit Coin Chain
Android App Sets: Sensitive Dataflow

```java
void main() {
    a = new A();
    b = a.g;
    foo(a);
    sink(b.f);
}

void foo(z) {
    x = z.g;
    w = source();
    x.f = w;
}
```

1. x.f
2. x.f
3. x.f
4. z.g.f
5. a.g.f
6. foo(a)
7. b.f
Cost of Failure
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
- SEI Webinars

SEI Cyber Minute
- SEI Cyber Minutes

SEI PODCAST SERIES
- SEI Podcasts
Reading

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


