

Weaving a Fabric of Trust

Table of Contents

SEI WEBINAR Keeping you informed of the latest solutions	3
Copyright 2016 Carnegie Mellon University.....	3
Carnegie Mellon University.....	4
First Bits.....	4
Greg in DC	7
Consistent Approach.....	8
NIST Framework.....	10
Building the Future	11
Building the Future	12
Building the Future	13
Building the Future	14
The Takeaway	15
Trust	16
2006 Aha! Trust Rabbit Hole.....	17
Digital Disruption	18
Digital Intermediation?.....	20
The Essence of Trust	21
Trust in a Digital World	22
Engineering Trust.....	24
Trust Poll	26
Ensure	28
Cyber Delusions	29
Cyber Delusions	30

Cyber Delusions	31
Cyber Delusions	32
The Weakest Link Paradox in Cybersecurity.....	33
Security Built in?	34
Elements of Defensive Deterrence	38
3 E's for Cybersecurity	39
Foundations for Weaving Trust	40
Recent Advances.....	41
Ensure Poll	43
Technologies	51
1994 Aha! Simple Technology	51
Startup!	53
Block Bit Coin Chain	55
Block Bit Coin Chain	56
Mark Sherman.....	57
Android App Sets: Sensitive Dataflow	59
Cost of Failure	61
Fuzzing.....	62
What you can do.....	64
Technology Poll.....	65
SEI WEBINAR SERIES Keeping you informed of the latest solutions.....	70

SEI WEBINAR | Keeping you informed of the latest solutions



Copyright 2016 Carnegie Mellon University

Copyright 2016 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® and CERT® are registered marks of Carnegie Mellon University.

DM-0003841



Software Engineering Institute | Carnegie Mellon University

Data Science: What It Is and How It Can Help Your Company
July 12, 2016
© 2016 Carnegie Mellon University
Distribution Statement A: This material has been approved for public release
and unlimited distribution. Please see the distribution statement for details.

2

Carnegie Mellon University

Carnegie Mellon University

This video and all related information and materials (“materials”) are owned by Carnegie Mellon University. These materials are provided on an “as-is” “as available” basis without any warranties and solely for your personal viewing and use.

You agree that Carnegie Mellon is not liable with respect to any materials received by you as a result of viewing the video, or using referenced websites, and/or for any consequences or the use by you of such materials.

By viewing, downloading, and/or using this video and related materials, you agree that you have read and agree to our terms of use (www.sei.cmu.edu/legal/).

Distribution Statement A: Approved for Public Release; Distribution is Unlimited

© 2016 Carnegie Mellon University.



First Bits



Carnegie Mellon University
Software Engineering Institute

Weaving a Fabric of Trust
© 2017 Carnegie Mellon University

[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.

**003 Presenter: And hello from the campus of Carnegie Mellon University in Pittsburgh, Pennsylvania. We welcome you to

the Software Engineering Institute's webinar series. Our presentation today is "Weaving a Fabric of Trust". Depending on your location, we wish you a good morning, a good afternoon, or a good evening.

My name is Shane McGraw. I'll be moderator for today's presentation, and I'd like to thank you for attending. We want to make today as interactive as possible, so we will address questions throughout the presentation and again at the end of the presentation. You can submit those questions to our event staff at any time by using the Ask a Question or Chat tabs that are found on your control panel. We will also ask a few polling questions throughout today's presentation and they will appear as a popup window on your screen.

In fact, the first polling question I'd like to ask is: How did you hear of today's event? And that will be on your screen now.

Another three tabs I'd like to point out are the Download Materials, Twitter, and Take Survey tabs. The Download Materials tab has a PDF copy of today's presentation slides there now, along with other work and resources from the SEI. For those of you using Twitter, you want to be sure to follow @SEInews, and use the hashtag #seiwebinar.

And now I'd like to introduce our presenter for today. As chief scientist for the CERT division at Carnegie Mellon University's Software

Engineering Institute, Dr. Greg Shannon spearheads expanding cybersecurity research, advancing national and international research agendas, and promoted data-driven science for cybersecurity.

Dr. Shannon recently finished a 17-month detail to the White House Office of Science and Technology Policy as the assistant director for the cybersecurity strategy, where he focused on accelerating innovation and policy to create effective cybersecurity technologies and practices. Additionally, Greg has testified before Congress on cybersecurity, science for security, critical infrastructure, reliance, and cyber threats. And now I'd like to turn it over to Dr. Greg Shannon.

Presenter: I think that actually the marketplace has an opportunity to make this decision. I've seen some startups coming out that are promoting security higher to their users, and so if the company can indicate we're making things maybe a little more inconvenient for you, but it also makes it extremely more inconvenient for the hacker.

Woman: Dr. Shannon, why do you think companies have not done that.

Presenter: Well, because they see it as an impediment to their profit-loss. They want to retain users, they want to make their services easy to use, and so they haven't been forced to essentially admit that--

Woman: But then their customers become very angry--

Presenter: That's correct.

Woman: --When there is an--

Greg in DC



**008 Presenter: Well, welcome, and I look forward to today's conversation about weaving a fabric of trust. As you can tell, this is an issue that's been longstanding, the notion of cybersecurity and how it affects our nation, our critical infrastructure, our society, and the world writ large.

Working at the White House is an interesting experience. Taking a tour of the press room is part of the interesting part, but it's also a fairly somber place at times because you're dealing with important national

security issues. This is a scene from the 9/11 ceremony in 2015 that staff were invited to with the President and First Lady.

So you're dealing with important topics all along, and you're serving the American public, you're serving the president, trying to support the nation's interests in our national security as well as our economic prosperity and civil liberties.

What's interesting about the cybersecurity in general, trust in particular, is that it's been a longstanding theme.

Consistent Approach

First Bits

Consistent Approach



Carnegie Mellon University

Weaving a Fabric of Trust
© 2017 Carnegie Mellon University

[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.

10

**010 And it's actually been fairly consistent in terms of how it's been dealt with. When I was there at the White House for 27 months, there was the Cybersecurity National Action

Plan. It incorporated the Cybersecurity Research and Development Strategic Plan. There was a component of it recognizing the importance of science and technology as we go forward in improving cybersecurity. But also, in the current administration, there's the executive order for cybersecurity, and that executive order is quite consistent, both with the past administration as well as the previous administration. So over a course of three administrations we see a lot of continuity and clarity about what's important.

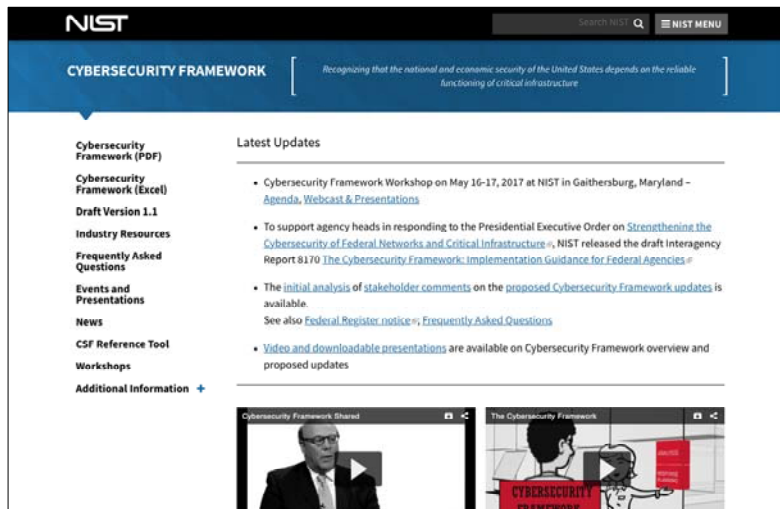
In the current executive order, the notion of improving-- securing the federal networks, improving critical infrastructure protection, worrying about national cybersecurity writ large, especially as it relates internationally, and then developing an effective workforce to meet the nation's needs.

The real challenge is how do we make sure it's a different and better world in 10 or 15 years. But again, we're seeing a consistency and a clarity across the administrations, and remarkable that the approach is unremarkable.

NIST Framework

First Bits

NIST Framework



Carnegie Mellon University

Weaving a Fabric of Trust
© 2017 Carnegie Mellon University

[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.

12

**012 One of the common elements that's developed and of course has some of its beginnings here at Carnegie Mellon University in the CERT division, is the notion of the NIST framework and how to manage cybersecurity risks. Again, this has been an element of the past two administrations, a foundational element in terms of how any organization, all organizations, can take a first cut at improving their cybersecurity, building trust with their customers, both for federal agencies, for international companies, for small businesses, for nonprofit institutions. It's a way to take a first cut at improving one's cyberspace, and it deals with the reality of the way things are today.

It's a challenging world for CIOs, for CISOs, to deal with the legacy issues, the legacy equipment. Users are


always providing new ways to challenge the system as well as the evolving threat, and it's the NIST framework that really is an important part of this continuity that we see across administrations.

Building the Future

First Bits

Building the Future

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



13

**013 Working in the White House, one of the questions that you're trying to deal with as a technologist in particular is being clear about what's the problem we're trying to solve. There's lots of policy issues, there's always political challenges, many constituents that are trying to have a voice, but as a technologist, it's really trying to answer: What's the problem we're trying to help society solve?

Building the Future

First Bits

Building the Future

What's the hard part of the problem?



14

**014 And what's the hard part of the problem? All too often it's easy to find an easy part of the problem that you can make progress on, and it looks good, but maybe it's not really solving the problem in the long-term, and that's been a particular focus of my work, it's a particular focus of Carnegie Mellon and CERT and Software Engineering Institute, is how do we deal with these long-term problems so that in 5, 10, 15 years we're in a different place than we are today.

Building the Future

First Bits

Building the Future

Where's the “promise of possibility”?



15

**015 And finally, what's the promise of possibility? What are the technical opportunities? What are the components-- as R&D evolves, as basic research evolves-- that believe that we can create that better future.

Building the Future

First Bits

Building the Future

What can we do?
What can YOU do?!?
Let's do it.



16

**016 So as we try and support the president in the job of being in the Executive Office of the President, what can we do together-- what can you do, when you're in that office-- particularly what you can you personally help make happen from a policy point of view, from prioritizing, from engaging with industry, academia, and the broader world? And then you actually do it. And that's part of what we want to be talking about today as we weave a fabric of trust and try and build a better future in the coming years.

The Takeaway

First Bits

The Takeaway



Carnegie Mellon University

Weaving a Fabric of Trust
© 2017 Carnegie Mellon University

[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.

18

**018 The key takeaway here is, just as a very simple takeaway, if there's only one thing you take away, is when you talk to vendors, what's their evidence of efficacy and efficiency of their products for enhancing trust? We need to get to a point where as consumers we want to demand that evidence, we want to demand evidence that shows efficacy that things actually work, and we really want to have evidence that it's efficient. The last thing we need are controls, whether it's for security, privacy, resilience, accountability, that are onerous, difficult to implement, and impede the work that we really want to get done, which is running our business, protecting the nation, building a better future.

Trust



Carnegie Mellon University
Software Engineering Institute

Weaving a Fabric of Trust
© 2017 Carnegie Mellon University

[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.

**020 So let's talk about trust.

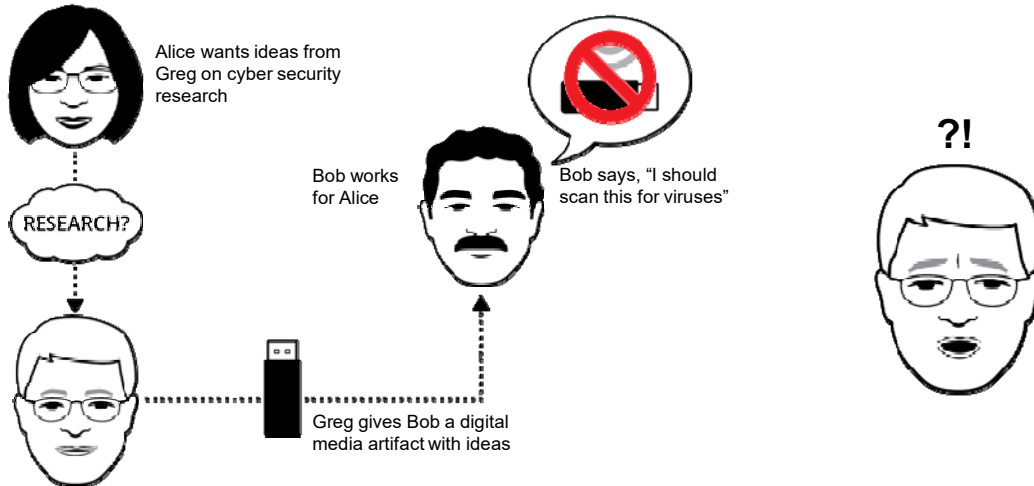
What I want to do is-- I've got-- the next 80 minutes is broken into three parts, three vignettes, and I'll introduce each with a story essentially about how-- some of the inspirations that I've had in the course of my career.

And the first one here is what I call the trust rabbit hole.

2006 Aha! Trust Rabbit Hole

Trust

2006 Aha! Trust Rabbit Hole



Carnegie Mellon University

Weaving a Fabric of Trust
© 2017 Carnegie Mellon University

[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.

21

**021 This occurred in 2006, and I had a colleague working at a federal research organization, and they wanted me to provide some information, some ideas to them about how to improve cybersecurity. Great. This is what, as a researcher, you hope for, that someone in the government will reach out to you and ask for ideas. So Bob worked for Alice, and I provided Bob with a job of that information. Actually at the time it was a CD disk, but I don't know if we had any images to put on there of a CD disk.

Regardless, I hand this to Bob and Bob says, "Oh." I mean, I vividly remember these words. "I should scan this for viruses." Fully acknowledge-- he knew what the policy was, he knew what he should do, he knew why he should do it. He didn't do it. And I was like, "Okay,

this is an organization asking for research ideas on cybersecurity and the policy wasn't followed." Fortunately no harm was done, but it certainly left me wondering what is going on here. There's something I really don't understand about security, about trust, and about the way that we really make improvements.

Digital Disruption

Digital Disruption



**023 I think we have to click it.
There we go.

Man: Since the dawn of the industrial age, humans have trusted machines. That trust has continued to increase as the centuries have worn on. When we wake up in the morning and get in our cars, we trust that the brakes are going to work when we need to stop. When we go to the airport and we get on an

airplane, we trust that that airplane is going to safely and reliably get us to our destination. When humans trust those machines, it's not actually the machine they're trusting; it's the designers and the engineers and the builders of those machines. The 21st century will be defined by humans teaming with machines and trusting that they'll not only operate effectively, but they'll actually trust that those machines will make decisions for them safely and effectively.

Presenter: So what we have going on is essentially digital intermediation, digital disruption, and we have to-- it's important to understand how this is taking place, both in terms of it's disintermediating people in various ways, but it's also putting technology in play. So for example, the notion of people texting each other while they're in the same room. There's a disintermediation of the technology in that interaction. On the other hand, in a more positive way, the notion of telemedicine disintermediating the direct physical contact with a doctor in order to work with them.

Digital Intermediation?



**025 So part of the question we want to ask is: What might we lose with digital intermediation and what might we gain.

So from a loss point of view, it's our sense of trust and how we normally think about trust-- when you can look someone in the eye, when you have a trust transaction that's based on decades or centuries of that type of interaction.

What sort of things might we gain? Efficiency. Having to interact with someone to do every transaction you want to do, every purchase you want to make, can slow things down. So digital intermediation helps accelerate that. So there's a lot of value to putting these into a digital world.

The Essence of Trust

Trust

The Essence of Trust



Carnegie Mellon University

Weaving a Fabric of Trust
© 2017 Carnegie Mellon University

[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.

27

**027 But let's talk about what the essence of trust is: The notion that a truster relies on the trustee, that you're going to rely on someone in a way that in the future you know that they might do something-- they have the opportunity to do something negative, to do some harm to you. And so even someone walking past you on the street, there's a degree of trust involved, that you're assuming that the person won't push you into the path of an oncoming bus, but you're not 100 percent sure. You're being wary. You're looking at the situation to try and make an assessment. You've got kind of biological indicators that let you know when something is there that you should be nervous about.

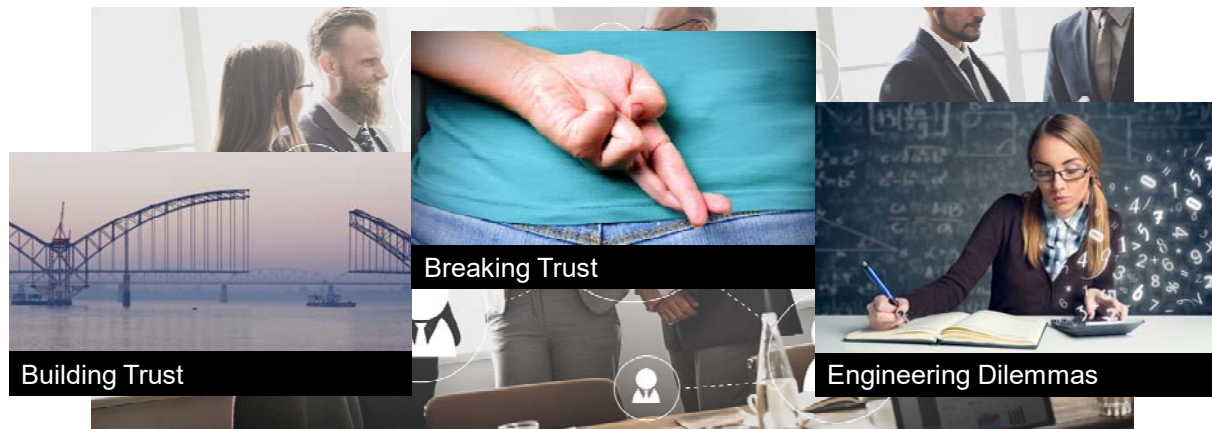
And so as we disintermediate this and put this into a digital world, that makes it very challenging, because a

lot of our normal biological cues and such have disappeared.

Trust in a Digital World

Trust

Trust in a Digital World



Carnegie Mellon University

Weaving a Fabric of Trust
© 2017 Carnegie Mellon University

[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.

29

**029 So in terms of trust in the digital world, it's about building trust. It's about breaking trust, and it's about some of the engineering dilemmas that we have.

So in terms of building trust, we want to be able to verify quickly that there's no need for trust, for example, that the system is fully accountable, it will work as expected, and that there's no reason for concern. And this might seem a little paradoxical in the sense that trust is about exposing yourself to-- recognizing that you have a vulnerability that you have-- that you're making yourself vulnerable to someone, and building trust is about

trying to create situations where that is not at play.

So in other words, if I'm trying to have a trust interaction with you and I want to use my phone, I want to be focused on you as opposed to whether or not the phone is going to disrupt our trust interaction. So building trust is about building that phone, for example, in a way that you can not have to-- in some sense not have to trust it. You can verify it.

Breaking trust is about the illusion of accountability and anonymity. Accountability is an important component of trust, and when you can't hold-- when people can't be held to some sort of account, that makes trust very difficult.

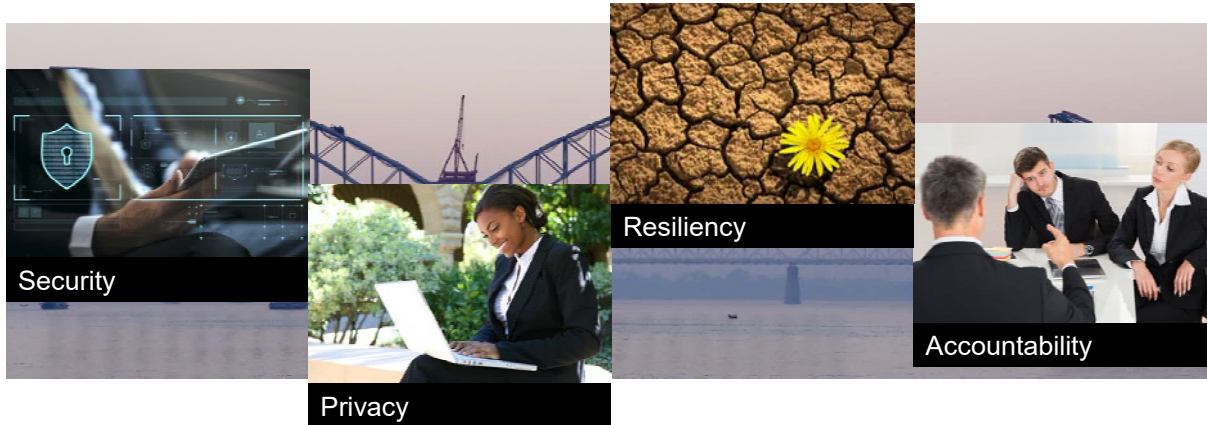
And then in terms of engineering dilemmas, there's two fallacies. There's a fallacy of creation, the notion that if we've created some artifact-- say the internet, the cyberspace-- that that means we should understand it. On the other hand, we do have the power of creation, which means we can influence what the future is; we can engineer that infrastructure to better facilitate trust.

And those are some of the challenges that we have.

Engineering Trust

Trust

Engineering Trust



Carnegie Mellon University

Weaving a Fabric of Trust
© 2017 Carnegie Mellon University

[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.

31

**031 In terms of engineering trust, there's four components. There's the security, cybersecurity traditionally, and this is what many focus as the most important element, but I believe that the other three elements are of equal importance and work together.

The notion of privacy, the notion that you're-- the information that you want to disclose is the information you want disclosed, that when the information is aggregated an adversary can't take advantage of that aggregation beyond what you believe should be done with that information.

The sense of resilience, admitting that systems will break, things will fail, and that they have to continue to work at some limited degree.

And then accountability. And again, this is one that I think is especially underappreciated, the notion of incorporating the ability to hold people accountable at some level. Sometimes this is interpreted as attribution, which potentially is part of it, but you want to know that when things break that there's some degree of accountability, some degree of consequence.

Man: Being able to use your software quickly to maintain both security and competitive advantages, security has to be addressed throughout the dev-ops pipeline from beginning to end. Integrity dev-ops platform will enable to insert security requirements, threat modeling, environment hardening, secure coding, security testing, and beyond. This also enables continuous feedback to all stakeholders, including security team, along with other developers.

Presenter: So that vignette was just talking about how secure dev-ops can help with security engineering as part of the fast-paced process of putting technologies, especially digital technologies, out there. Shane, I think we were going to do a poll?

Presenter: So we do. We have a polling question here.

Trust Poll

Trust

Trust Poll

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

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

Carnegie Mellon University

Weaving a Fabric of Trust
© 2017 Carnegie Mellon University

[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.

34

**034 The second one we like to ask is: What matters most to you in building, growing, and sustaining trust? We'll take about 15 seconds to vote there, and we'll turn it back to you, Greg, and then we'll get the results when they come in.

Presenter: Have you gotten any questions yet?

Presenter: Actually one question came in at the beginning just asking: What has been the progress on that executive order that was started?

Presenter: Yeah, there were a large number of reports that were expected out of that executive order. What will happen with those reports is yet to be determined. But every president comes in and on topics that they care a lot about-- especially around national security-- they will

typically issue a request for various reports. And so this is keeping in pattern with past administrations. So it's important that this president has put cybersecurity front and center as a priority, and asked its many agencies to respond. Many of those reports have already been submitted. There's a report on deterrence, there's reports on workforce going forth. The longest one is one on botnets, about how to protect the public infrastructure against botnet-type attacks, which interestingly has evolved into a discussion about Internet of Things as much as botnets, and the concerns that consumer organizations, industry, the carriers, and government have in that area.

Presenter: Great. And I'll just wrap up the poll real quick. We had 46 percent with security, 8 percent privacy, 11 percent resilience, and 35 percent accountability.

Presenter: Excellent. Well, the last time I gave this talk accountability was also similarly high. It's interesting that the technologies to support accountability are limited today in terms of making it-- accountability that's difficult to compromise. Accountability that's easy to compromise is not particularly good accountability. So there's an interesting technology gap there. Any other questions?

Presenter: That's it for now.

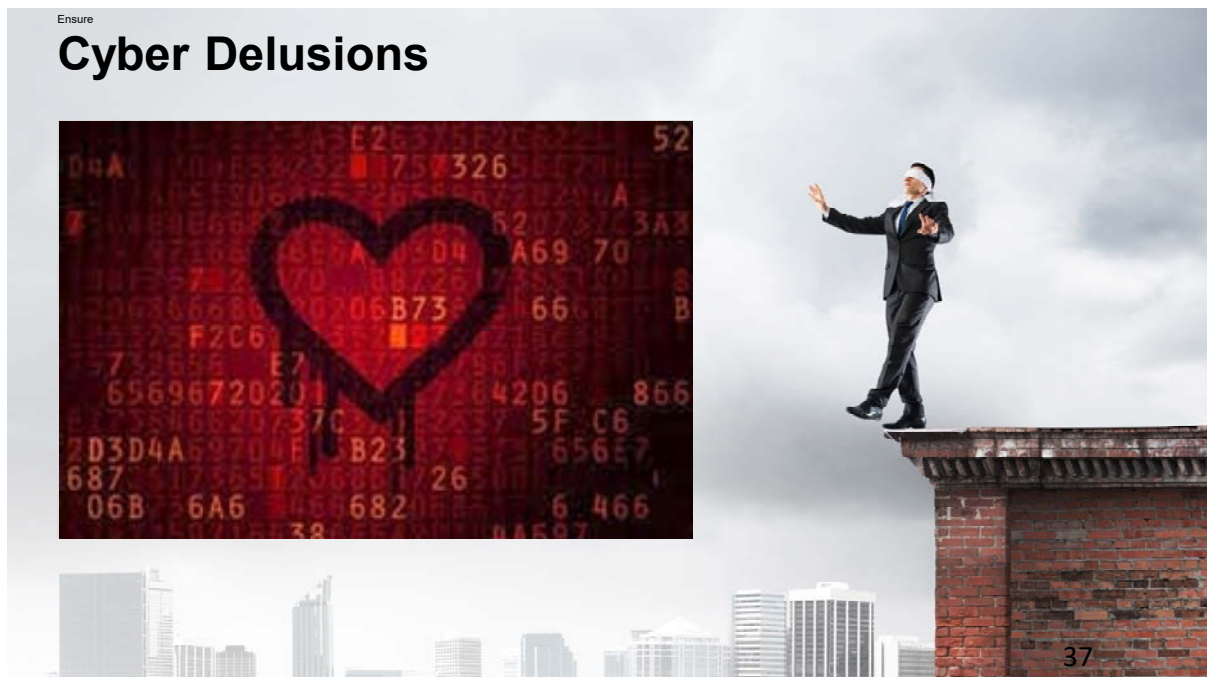
Presenter: Okay. So we'll move on to the ensure component.

Ensure



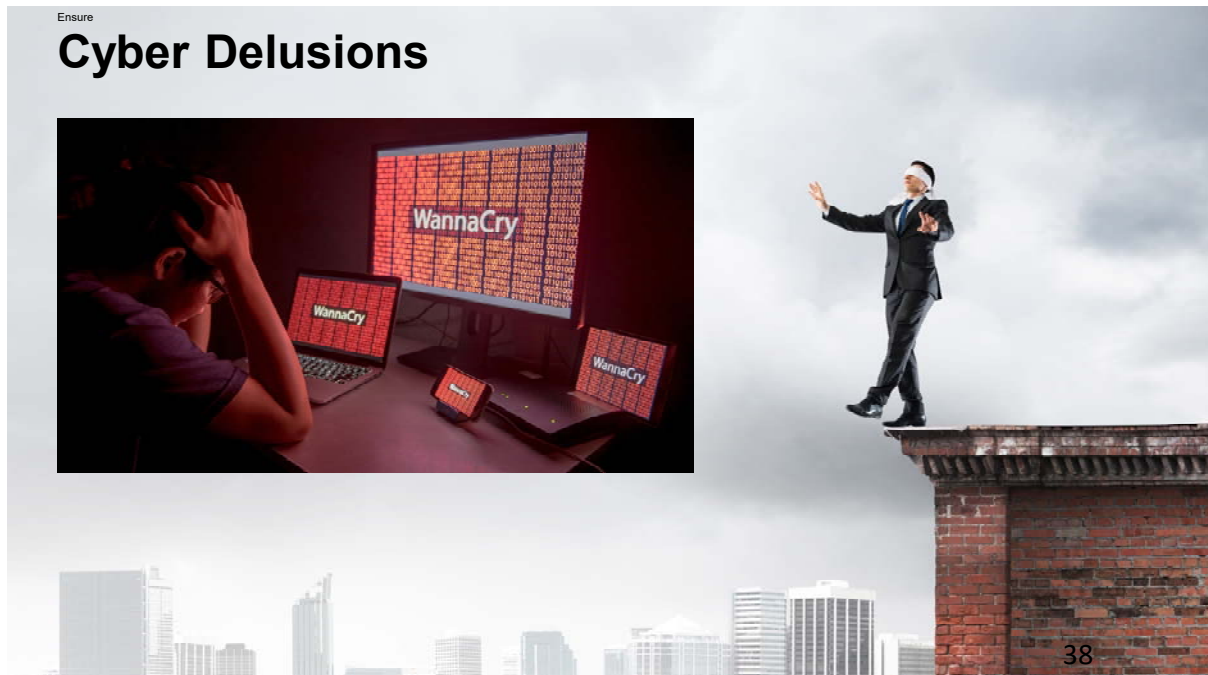
**036 So this is about-- we've identified some components of trust, and now we want to talk about how do you actually ensure that you have the trust that you want, and I want to touch on what I call cyber delusions before we talk about how to ensure things.

Cyber Delusions



**037 The first one is this notion-- here's the logo for Heartbleed. You know it's an important vulnerability or an important incident if it has its own logo. One of the interesting things is that many times that we're still writing software, still using software that has easy-to-discover vulnerabilities, easy-to-exploit vulnerabilities. And so there's this delusion that we're actually making significant progress, and that is actually one of the real concerns that the Internet of Things has to many technologists, many policymakers, is how are we going to change this pattern where vulnerabilities are-- I mean, many policymakers just assume things will be vulnerable forever, and that's there no hope in the future.

Cyber Delusions



**038 Another delusion is the notion that policies are out there to make changes, and so with WannaCry, it was effective because organizations hadn't patched known vulnerabilities. They hadn't implemented patches that were known to exist. And there's numerous other large, important incidents where it was a policy-- I wouldn't say a policy failure, but policies were in place, people knew what the right thing to do was, but they didn't do it for whatever reason. So ransomware-- many of the successes in ransomware in general are predicated on unpatched systems. Why don't we patch them?

Cyber Delusions



**039 With incidents, there's been many sophisticated organizations-- and I'll let you consider your own definition of sophistication-- but if you look at incidents over the last five, ten years, there have been many sophisticated organizations that have been compromised in spite of their attention to it. So the delusion is that you have sufficient attention, sufficient ability to identify incidents and respond to them quickly.

Cyber Delusions



**040 And then finally, the notion of recovery-- the ability to recover quickly, this notion of resilience, to have anticipated certain types of failures. We're still learning there. Cybersecurity is still a fairly young industry, and so the delusion is that just because you haven't had an incident is that you're ready to respond to it, and a number of organizations have found out over the past years that that's not quite so.

The Weakest Link Paradox in Cybersecurity



**042 And so--

Man: And one of the things that makes this such a challenging problem is all you need is one weak link. You can have nine companies--

Woman: Well, in any defense.

Man: Right. You can have nine companies that have great protocols, authentication systems-- you name it. You have one that's not doing a good job, and that penetrates the entire system.

Presenter: So President Obama reiterated this at the February 2015 White House summit on cybersecurity and consumer protection. I've heard generals reiterating this in various forms also the notion of one weak link, which, on the one hand, as a theoretical computer scientist, this is

a bit of a tautology; there is always a weak link. So the real technical challenge is how do we make it-- that weak link a strong link, in spite of the fact that it is the weakest? And so that's part of the thread that we want to pull here.

Security Built in?

Ensure

Security Built in?



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

**044 We do have this sort of challenge where there seems to be incentives pushing against this. I like this cartoon from Dilbert where, are we cheap or are we smart, because we're making a decision not to implement security? I think organizations, large organizations especially, are starting to discover that that short-term payoff is ephemeral, and if you're really trying to build critical infrastructure, you're really trying to build a sustained enterprise, a large enterprise, that you have to pay attention to security,

and you need to be able to do it efficiently, and that's I think one of the key themes that we're going to see in the coming years, is this focus on efficiency, how much effort does it take to achieve security.

Professor Bill Scherlis here at Carnegie Mellon has used the phrase "invisible security", and I think that's really the wave of the future, is how do we make security invisible so that engineers, users get the benefits of it without having to take any real mental effort to see it implemented or to use it.

2014 Aha! Cyber Energy Barrier

Ensure

2014 Aha! Cyber Energy Barrier

The image is a collage. On the left, there are server racks with blue and yellow cables. In the center, there's a green padlock with binary code (0s and 1s) and various alphanumeric characters. On the right, there's a white box with a black border containing the text 'Selected Typing Rules.' followed by several mathematical expressions for typing rules.

Selected Typing Rules.

$$\text{Obj} \frac{\Gamma \vdash e_i : \tau_i \quad i \in [1..n]}{\Gamma \vdash \{x_1 : e_1, \dots, x_n : e_n\} : \{x_i : \tau_i\}_{i \in [1..n]}} \quad \text{PropA} \frac{\Gamma \vdash e : \delta \quad \delta \triangleleft \{x : \tau\}}{\Gamma \vdash e.x : \tau}$$

$$\text{StrD} \frac{\Gamma \vdash x : \text{string} \quad \Gamma \vdash y : \text{number}}{\Gamma \vdash ((y \gg= 0) < x.length?x[y] : @string) : \text{string}}$$

$$\text{Scope} \frac{\Phi(x) = \tau}{\Gamma, [\Phi]_x \vdash x : \tau} \quad \text{RecScope} \frac{x \notin \text{dom}(\Phi) \quad \Gamma \vdash x : \tau}{\Gamma, [\Phi]_x \vdash x : \tau} \quad \text{Assign} \frac{\Gamma \vdash e_1 : \tau \quad \Gamma \vdash e_2 : \tau}{\Gamma \vdash e_1 = e_2 : \tau}$$

$$\text{With} \frac{\Gamma \vdash e : \{\bar{x} : \bar{\tau}\} \quad \Gamma, [\bar{x} : \bar{\tau}]_o \vdash s : \text{undefined}}{\Gamma \vdash \text{with}(e)s : \text{undefined}} \quad \text{MetDef} \frac{\Gamma \vdash \text{function } \langle \text{this}, \bar{x} \rangle (s) : \langle \rho, \bar{\alpha} \rangle \rightarrow \tau}{\Gamma \vdash \text{function } \langle \bar{x} \rangle (s) : \bar{\alpha}[\rho] \rightarrow \tau}$$

$$\text{FunCall} \frac{\Gamma \vdash e : \mu \quad \Gamma \vdash \bar{x} : \bar{\alpha} \quad \mu \triangleleft \bar{\alpha} \rightarrow \tau}{\Gamma \vdash e(\bar{x}) : \tau} \quad \text{MetCall} \frac{\Gamma \vdash e : \mu \quad \Gamma \vdash \bar{x} : \bar{\alpha} \quad \mu \triangleleft \{x : \bar{\alpha}[\rho]\} \rightarrow \tau}{\Gamma \vdash e.x(\bar{x}) : \tau}$$

**045 But the aha moment for this angle is recognizing that there is always a weak link. You want to make that weak link strong, relatively speaking, and what are the elements that are going to make this happen.

And what you're seeing here is a picture of the Oakridge National Laboratory during World War II where uranium was being separated to make the nuclear weapons that we used in World War II. At one point this facility was consuming somewhere between 10 and 15 percent of all energy in the United States. So clearly, from a national security point of view, energy was a key component, and without it we wouldn't have been able to create those weapons.

And this plays into cybersecurity because what we're really trying to do is to make something especially strong. We would like to use our computing energy to make something strong and sustainable, difficult to exploit, difficult to find exploits.

So what goes into this is, first, computation. As we've seen at the Cyber Grand Challenge, for example, the notion that computers can find vulnerabilities quickly, they can patch them, is one component. We want to be able to use the computing infrastructure, as opposed to, for example, the wetware-- when I say wetware, I mean our brains-- to try and reason, try and think about where the vulnerabilities are. The better we can automate this, the better we can scale, the better we can efficiently deter our adversaries and have a strategic advantage for our country.

Another element is being able to use encryption. There are new encryption techniques coming out that essentially put controls on data, both from a security and privacy point of view, an accountability point of view, put controls on actions and data and policy that make it so that you can't kind of-- it's exceptionally difficult to compromise it without breaking essentially a crypto-hard problem. This includes secure databases, verified computation, homomorphic computation, and technologies like that.

And the third element then is really some new types of math, and when people talk about high-performance computing they usually think of models-- modeling the flow of air over a jet wing in order to optimize it. In the cybersecurity area it's logic that we really are relying on and is really at the core element of being able to show that systems having properties that are important and have properties that are difficult for adversaries to violate.

I'm involved in a study called Industrial Scale Formal Methods for cybersecurity that should be out this fall, and trying to look at how can you scale formal methods in particular, and it's these components that all fit together. You want to be able to formally verify the crypto-type elements that you're using; you want to be able to use the high-end computing to solve the theorems, to prove the proofs, to look for counter-examples in order to make it difficult

for the adversary to be successful.
And so I see these as three real
elements, and these came together
for me in 2014.

Elements of Defensive Deterrence

Ensure

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

**047 So the elements of defensive
deterrence-- and this is an idea that
I've-- a phrase I've been promoting.
In the executive order you'll see it
also referenced as deterrence by
denial-- and again, it's trying to make
the amount of resources that an
adversary needs intractable. Today
one could argue that if you have--
certainly if you have a million dollars
you can probably do some very
interesting malicious activity online.
The goal is to make it so, "Well, let's
at least get that to a billion dollars,
and for an important system, a trillion
dollars is probably a good bar to
shoot for," that you want to make it
so that a country needs that sort of

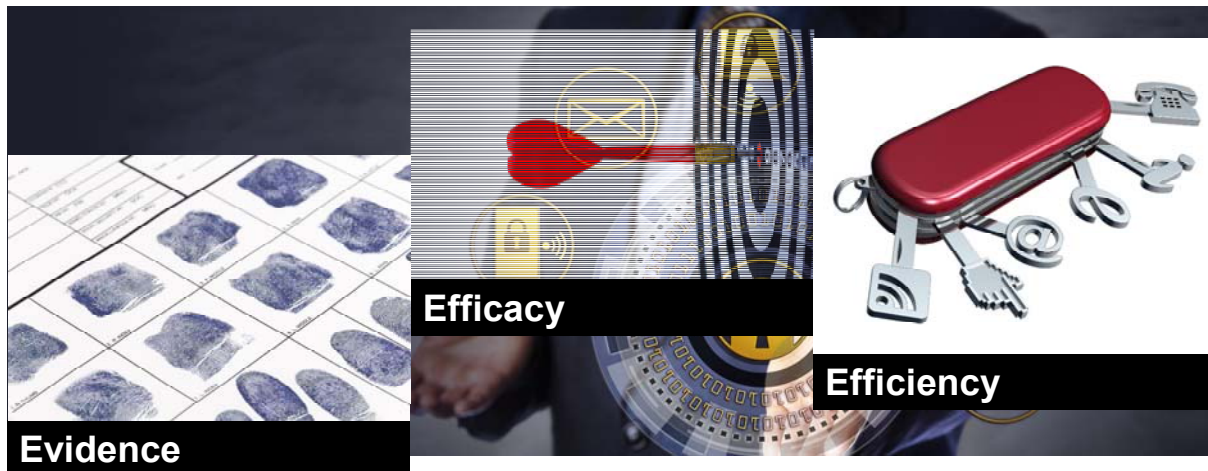
resource in order to compromise, say, a national security system.

And we're making progress on that with some of the new techniques and technologies, but it's-- part of the work I've been doing is how to accelerate that.

3 E's for Cybersecurity

Ensure

3 E's for Cybersecurity



Carnegie Mellon University

Weaving a Fabric of Trust
© 2017 Carnegie Mellon University

[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.

49

**049 So, again, we come back to these three E's for cybersecurity that I've mentioned before. The notion of evidence-- we want to have evidence that a system is providing the insurance for trust that we want. We want to know that it's effective, that it actually does achieve what we say it's going to achieve. And then we want a sense of efficiency, that there's an economy of resources, there's an economy of effort, and a really important element is the cognitive load that we put on users,

the cognitive load that we put on developers. At the end of the day, most of us have a different job than security, and so this efficiency element is really important.

Foundations for Weaving Trust

Ensure

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

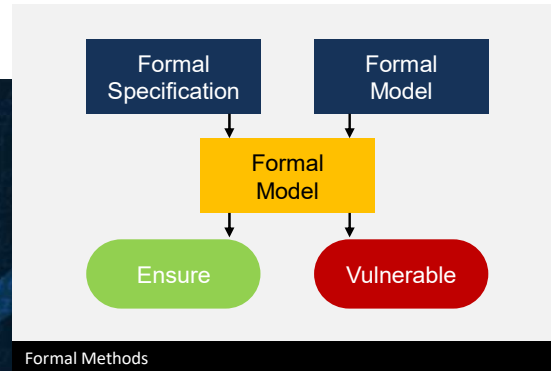
- Weave together formal methods (warp) with encryption (weft) to expand security, privacy, resilience, accountability

**051 So to kind of wrap up some of this in terms of weaving trust, it's about weaving together encryption, some of these strong encryption methodologies and formal methods, and again, it's about trying to make it so that the adversary takes exceptional resources to compromise the security, and if you're familiar with how weaving works, it's really about taking some fairly weak elements and creating a very strong fabric.

Recent Advances

Ensure

Recent Advances



**052 Some of the recent advances I want to talk about are, as I mentioned, encryption. Let's see, I think-- yeah, informal methods. In the encryption realm, one of the interesting advances recently was what's called verified computation. This is where I create-- let's say I want to do a matrix multiply or I want to do some sort of graph algorithm, and I want to have an untrusted party execute that computation for me. So how do I know that I'm getting back actually the right answer? And if I can pay someone else to do it-- I don't want to use my resources, I want someone else to use their resources-- they may have inexpensive resources I want to take advantage of but for whatever reason I really can't trust them.

There's methods now-- and this was a milestone that was achieved a couple years ago-- where I can do some math on my problem, I can hand it to my adversary, they can execute it, and when I get it back I will know with very high probability in the sense of a crypto kind of probability, that it is correct. And the fact that-- the border that was crossed was the amount of effort it takes me to package it up, send it off, and then get it back and unpackage it is now less than if I had actually done the computation myself. So at least on my side I have an efficiency.

Now, on the computer side, the entity doing the computation, I think there's either six or nine orders of magnitude of cost to have the other entity do the computation. But again, that community is working hard to improve that efficiency and is knocking off orders of magnitude pretty much every other year. So in a number of years, we will have that as a more general capability in which to engineer systems.

The other part is formal methods, as I mentioned, with this study I'm involved in on Industrial Scale Formal Methods, and it's about being able to have formal models that represent the type of interaction that you're going to have with an adversary, and you want to be able to prove that the adversary won't be successful given the resources that they have.

Again, we're probably a decade away from that, but part of the work we're doing here is to make that a priority. Part of the policy work I've done is to make that a priority so that in 10 or 15 years we're in a different place.

Ensure Poll

Ensure

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

Carnegie Mellon University

Weaving a Fabric of Trust
© 2017 Carnegie Mellon University

[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.

54

**054 Presenter: Okay, that leads us to our third polling question with the Ensure section, and the question up now is: What matters most to your organization in thwarting malicious cyber activity? Is it undiscoverable vulnerabilities, unexploitable vulnerabilities, detect malicious activities, attribute malicious actors, or recover from malicious activities? So we'll give you a chance to vote there. We'll go back to a question, Greg, if you don't mind.

Presenter: Yep, please.

Presenter: It was actually in our chat window, asking about: What are your thoughts on the new password complexity, no longer valid, defying the traditional NIST standards?

Presenter: Could you please repeat that again?

Presenter: One more time, it says: What are your thoughts on the new password complexity, no longer valid, defying the traditional NIST standards?

Presenter: Yeah, so there is a discussion about whether-- what is appropriate password complexity, I believe is what the question is getting at. I know one of the-- I believe in some of the government requirements, this notion of changing password, which is related to this issue. The consensus of the community is that changing passwords actually doesn't improve security. It's kind of this one plus one does not necessarily equal two. You would think that a password plus changing, that that's more security. It turns out the way people actually do their passwords, they don't-- the amount of entropy as they change their passwords is not sufficient really to justify the change. And similarly with the complexity rules, what the researchers have found is that we're all human, we tend to think similarly in terms of what might be a good password and what we remember and kind of the keys that we might use in our head to remember a powerful, and so unless we're using a

completely randomly generated password, there's a pattern there, and the researchers have shown that especially when you look at a corpus of passwords, you're able to identify patterns that give you a chance of guessing a fair number of passwords. Not all of them necessarily, but a fair number.

I just heard recently that there's some research going on here at Carnegie Mellon University by Manuel Blum in tackling this challenge of how do you create passwords. What are password schemes that humans can create, humans can remember, humans can use, that have some good properties in terms of resilience to adversary behavior? One of the properties they'd like to have is that if someone's shoulder-surfing you and actually sees you use a password that they are not able in the future to use that password again and that there's some scheme that you're using in your head.

As a colleague explained to me as well, if you use the one-way hash function every time you want to use a password, that would work great, except one-way hash functions are kind of hard to do in your head, so it doesn't really work. But that's kind of the notion, that you have something that even if someone were shoulder-surfing or had a keyboard logger that that would not give them access to your credentials.

Presenter: And one other comment I'm going to pass along-- not a

question-- again, just a comment, but in case you have any thoughts to it. You had made a comment I think in jest talking about HeartBleed and how you see a logo and now you know it's made it. But I think someone made a good point. It says: Researchers have learned to logo in order to increase the media visibility of potential issues.

Presenter: No, I think that's an important part, and thanks for bringing that up. I mean, there's been a fair number of discussions while I was there, because there were new rules on export control, the Wassenaar agreement, where the community was very vocal about recognizing the importance of vulnerability discovery, and I think we're going to continue to see that evolve. I mean, at the end of the day the digital infrastructure continues to increase in value. It's going to make the owners of that infrastructure all the more nervous about those that are trying to discover vulnerabilities and always think they'll be-- especially organizations or leaders that are new to thinking about cyber and security-- that they're going to be resistant to that.

On the other hand, given the bug bounty success that we're seeing-- this was programs promoted in the last administration and continued in this administration-- the Department of Defense is the one-- I think DSS Digital Security Service-- creating the bug bounty program within the DoD.

They're looking to expand that, and it's got buy-in from the leadership and the stakeholders within the Department of Defense to improve the security of the web-facing applications the Department of Defense has.

So that ties in with the notion of being able to responsibly deal with vulnerabilities, and I think that's really what it comes back to, is responsible disclosure. It can be challenging, especially when organizations are resistant to releasing vulnerabilities that are important, or when organizations are resistant to patching vulnerabilities that are important to their user base.

Presenter: Right. And I'll wrap up the polling question. So we had 21 percent undiscoverable vulnerabilities; 15 percent unexploitable vulnerabilities; 50 percent detect malicious activities; 3 percent attribute malicious actors; and 12 percent recover from malicious activities.

Presenter: So I think this is actually a really good indication of where the attention today is focused, is on detect. You have the notions of cyber-intelligence out there, data mining for cybersecurity. In fact, tomorrow I'll be speaking at a workshop on cyber and data science down in Arlington, and it's an important component given the way the world is today, that you have to live with the frailties of the system, and you want to be able to thwart

the cyber actors. Part of the message that I'm trying to deliver in this webinar though is making vulnerabilities undiscoverable and unexploitable would seem like a really efficient approach as opposed to focusing on detecting. If you knew that only difficult-to-discover or difficult-to-exploit vulnerabilities were what you had to detect, it really would change things. I mean, right now the volume of what you have to detect and sort through to figure out what is a serious threat as opposed to, "Yes, it's a threat, but it's maybe not as big a threat," or dealing with infrastructure that you're uncertain about its provenance, you're uncertain about-- there's no insurance about what it's supposed to really do-- there's no insurance about the software underlying it.

So yes, I can understand where half the respondents see detection as the priority. But again, to me, is that really where we want to be in 5, 10, 15 years? I would hope no. Any other questions?

Presenter: We do have another one asking: What about industry's continued belief that vulnerability automatically equals significant impact or worse, equating to risk? I'll read that one more time: What about industry's continued belief that vulnerability automatically equals significant impact, or worse, equating to risk?

Presenter: Yeah, I mean, it gets into the whole risk calculation about

where adversaries are going to be active. Typically an adversary has a number of vulnerabilities that they could potentially exploit, could potentially take advantage of, whether it's in the digital world, the physical world, and it's about what are they-- part of it is about what they're paying attention to, and that's an operational challenge. When I look at it from a science and technology point of view, I want to make it easy so that there's few vulnerabilities that an organization has to worry about and that they can identify them and know where they actually are.

But yeah, that risk management, it's always a delicate calculation for the organizations to really admit-- it's difficult for a manager to say, "Okay, I'm going to accept this risk." Actually, I'll tell a small story. I sit on the evaluation panel for our CISO program here with the Heinz school, and part of the practicum discussion, I always close with this notion that where we're trying to get to with resilience is this notion that an organization will make a risk assessment, they'll mitigate those risks, they'll acknowledge there's some risks that they're going to live with in order to move their business forward. An incident will happen. It will be within the risk profile that they had talked about and planned for, and it'll be okay. No one will get fired. They may tweak things a little bit, but it'll have been expected, anticipated, planned for, dealt with in a reasonable manner, and it won't be

pants-on-fire because there is yet another incident. And I think that's really where I hope to see kind of the resilience perspective and the risk management perspective evolving to over the next couple of years.

Presenter: Great. And just a real quick follow-up comment from the same person that posed the question, which says: A great number of discovered vulnerabilities are in context already unexploitable or whose impact is of no attacker value.

Presenter: Yeah. That's probably subject to debate. Again, in the engineering environment, it would be ideal if it precluded really even that. I mean, presuming that there's no path to exploit a particular vulnerability, it can be a dangerous calculation. But from a policy point of view, I'll admit that there's lots of vulnerabilities you should be able to live with.

And so the next segment is about technologies.

Technologies



Carnegie Mellon University
Software Engineering Institute

Weaving a Fabric of Trust
© 2017 Carnegie Mellon University

[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.

**056 And so this is about my aha moment in 1994, going back a few years now.

1994 Aha! Simple Technology



Carnegie Mellon University

Weaving a Fabric of Trust
© 2017 Carnegie Mellon University

[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.

57

**057 And at that time I was

working at a national lab, and two interns there told system administrators that from their accounts-- those interns-- that from their accounts they could gain root access to these important systems that the system administrators were operating.

Of course the staff didn't believe the interns. They said, "Let's go to lunch," and the interns said, "Well sure, let me run this program real quick." And so off to lunch they go. They get back from lunch and the interns walk in and say, "Oh, and here's your root passwords." The system administrators were a little surprised, to say the least, especially given the importance of the systems that these passwords were taken from, and what it showed to me, with some very simple technology-- this was essentially vulnerability scanning technologies that were first coming out in the early '90s-- really could be quite powerful.

And part of their power came from all the assumptions that people were making about the security of the system. Again, at a national lab, a trained IT staff dealing with important systems, and yet interns being able to come in and identify their root passwords.

My reaction to this was, "Let's start a company," and so I was able to license the technology from the two interns, started a company in the cornfields of Iowa.

Startup!

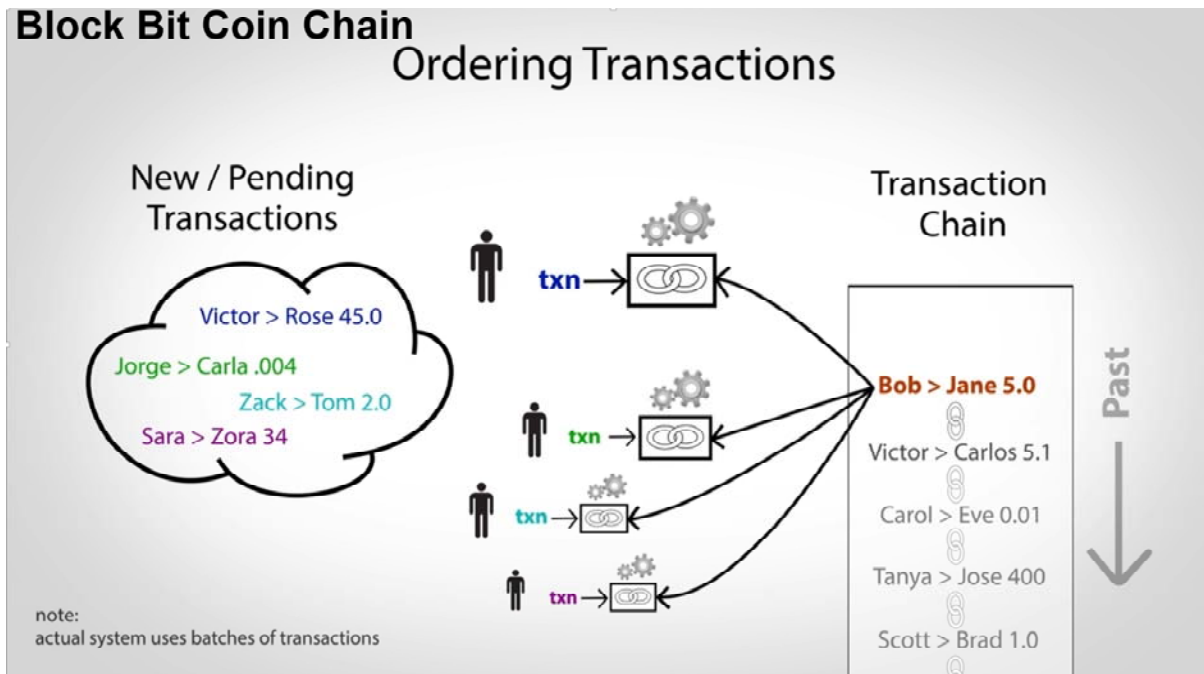


**059 Ames, Iowa, in particular-- and it was very exciting, and-- oops, I don't want to go there. It was very exciting, but it was also recognizing that just because you can find some information about security that it's much more complicated than that, and had been an important part of understanding what the real role of technology in policy, in society, as it tries to make decisions about important things like trust.

Man: In our traditional banking system, if Alice wrote two checks but only had enough money to cover one of them, the bank would pay the first person attempting to cash his check but refuse the second because Alice's account would be empty. So the order of these checks is critical because it determines who should get paid. Unfortunately order is much harder to determine in

bitcoin, where instead of a single bank there are individuals all over the world. Network delays might cause transactions to arrive in different orders in different places, and fraudsters could lie about timestamps. Two recipients might both think their transaction is first and ship a product, effectively allowing Alice to spend money twice. Bitcoin prevents this by providing a way for the entire world to decide on transaction order. As new transactions are created, they go into a pool of pending transactions, and from here they'll be sorted into a giant chain that locks in their order. To select which transaction is next, a kind of mathematical lottery is held. Participants select a pending transaction of their change and begin trying to solve a special problem that will link it to the end of the chain. The first person to find a solution wins and gets to have their transaction selected as next in the chain.

Block Bit Coin Chain



**061 Presenter: So you might wonder why I threw up this-- if you pardon my characterization-- block bitcoin chain video, but I think it shows a couple of things. One is this is an exciting new technology. By the title here, I think it's an exciting new technology that many don't understand it-- how's it related to bitcoin, what does chained hashing really mean, what's blockchain, how's that different from other technologies that are coming out there-- and so there's a tremendous amount of activity in terms of startup.

But I really want to pull this actually back to trust, and talk about how this sort of technology can be disruptive just the same way that vulnerability discovery technologies were disruptive in the '90s in terms of being able to identify easy misconceptions. For blockchain, it's

really about disintermediating trust, and it's one of a number of technologies where--

Block Bit Coin Chain



**062 The digital world is able to take a third-party out of the transaction, and the power of bitcoin in particular, or bitcoin-like technologies, is that instead of having to trust your bank who holds your money, you trust the technology; you trust the math that's behind it.

Interestingly, you get into interesting questions then about: Well, who governs the software that actually implements bitcoin? Do you trust those engineers? One of the things that fascinates me about bitcoin is that here you have billions of dollars of value created; there's no real governance in terms of how do I as a

citizen, how do I as a user of this technology, hold anyone accountable who is controlling this technology, who controls the code base? It turns out you don't, and this is something that makes users nervous, it makes industry nervous, it makes governments nervous, because they understand that to maintain social order, you need governance, you need accountability in infrastructures like this.

So for as much as bitcoin is about disintermediating trust, it actually introduces some really new trust issues into the equation about how do we as a society trust technology, and what are our mechanisms to ensure that it's secure, private, resilient and accountable. Let's see.

Mark Sherman



**064 Another video here.

Man: Surveys show that 90 percent of applications are assembled from third-party components. Most applications are assembled from hundreds of open-source components. However, over one quarter of the most popular open-source components have high-risk vulnerabilities. Nearly two billion vulnerable components are downloaded annually. The result? The average application has over 20 open-source vulnerabilities. What can be done? Know the supplier. Have a single point of contact in an organization who will source components. Do not let every developer scour the web in search of componentry. Know the product. Check the CVE database and third-party evaluators for vulnerabilities. Know the distribution. Track where all components have been used and institute ways to update fixed components. Know the operating environment. Reevaluate the application for attack surfaces whenever existing components are newly connected. Open-source components speed production and reduce cost, but can also be a source of vulnerability.

Presenter: So what we've seen is part of the research that we're doing here at Software Engineering Institute and CERT division to think about how is software engineering really done today and how does that affect security and trust.

Android App Sets: Sensitive Dataflow

Technologies

Android App Sets: Sensitive Dataflow

```
void main() {  
  a = new A();  
  b = a.g;  
  foo(a);  
  sink(b.f);  
}  
  
void foo( z ) {  
  x = z.g;  
  w = source();  
  x.f = w;  
}
```

© Carnegie Mellon University

Weaving a Fabric of Trust
© 2017 Carnegie Mellon University

[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.

66

**066 That's not quite the right one, but.

If you think back to the blockchain image, it's about the technologies there. If you're going out and grabbing on the internet, how do you know what the integrity is? And part of the technologies we need to develop is to know that the code that exists there is correct, that it does what it says it's going to do, and there's a way for you as the developer to verify that, or you as the organization that is going to use that code that developer has written, to verify that it fulfills its objectives, that it doesn't have certain types of exploitable vulnerabilities in it. And I think that's really what we're trying to get at here, is that provenance of software and how to ensure that.

This next bit focuses on some of the security challenges-- the privacy

challenges. And so let's look at this. Oops, I'm sorry. I thought that was a video.

What this is about is understanding how data flows through Android applications, and the key thing is that you have these app stores; you have a variety of apps then sitting on your phone that have maybe never sat together before, and you want to know that one app is safe from another. It turns out there's some very nice math behind this in terms of being able to figure out whether or not important information in one app can flow to another app. This is part of the research we're doing to ensure that that happens. And part of what it does is it provides tools then for developers that they can use to evaluate their own code to assert that it is secure, and others can then look at their code and determine whether or not it has various sorts of leakages.

This is particularly important for enterprise environments where you want to make sure you've got a cohort of apps that work well together, or say in the Department of Defense, where you've got warfighters with a combination of apps and you want to know that information is flowing correctly within policy in the apps.

Cost of Failure

Technologies

Cost of Failure



Carnegie Mellon University

Weaving a Fabric of Trust
© 2017 Carnegie Mellon University

[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.

69

**069 The cost of failure, I just want to interject here, is when these systems don't have the protections that one might reasonably expect-- I found this particular headline-- this is from earlier this summer-- I found this particular headline compelling for the size of the find. As a colleague of mine explained to me from the medical industry, this particular company actually had made promises that they would protect patient information and it was actually written into law already, or written into their contracts that they would pay these sorts of fines if they failed. But it's fascinating that in spite of all that, they didn't put the protections in, and thankfully they had to presumably pay the fine.

Fuzzing



Carnegie Mellon University

Weaving a Fabric of Trust
© 2017 Carnegie Mellon University

[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.

70

**070 The last story I want to talk about-- again this comes back to the notion of easy-to-discover, easy-to-exploit vulnerabilities, particularly the easy-to-discover. Part of the work that we're doing here at Software Engineering Institute is something called Basic Fuzzing Framework, where it's essentially a way to discover vulnerabilities in software at any point in the lifecycle, whether it's the development, pre-deployment, or software that's already deployed. Fuzzing originally was the idea of, "Well, let's throw some garbage at a system and see what happens."

Embarrassingly, a decade or two ago that was actually a very effective approach. Turns out systems are better; they can usually handle random garbage reasonably well. The more challenge is intelligent garbage that is crafted to exploit

various pathways to the software, but still with noise in that input, and this is one of the primary techniques for discovering exploitable vulnerabilities in systems today. We were able to identify points where you can take control of the operating system, take control of the application, or be able to get data, realize that there's certain points within the program that you can change the data based on the inputs.

And so that notion of discoverability, this notion of fuzzing, really is a best practice that really software developers should be using. Organizations that are delivering software that they've written, that they've compiled, need to be applying these techniques so that they can have some assurance that at least the vulnerabilities aren't trivial to discover.

Where we really want to get to is we want to make it to the point where someone, an individual personally looking at the code, is no longer able to find vulnerabilities. We want to make it so that only machine-assisted techniques can find vulnerabilities, and that would be real progress. I think we're only a few years away from that.

What you can do

Technologies

What you can do



Evidence

Efficacy

Efficiency

Carnegie Mellon University

Weaving a Fabric of Trust
© 2017 Carnegie Mellon University

[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.

71

**071 So, again, and to close, what can you do? It's about asking for evidence of efficacy and efficiency. And again, it's a drum that I've been beating for many years. I first talked about some of these ideas back in 2012 in Congressional testimony. It's ideas I promoted before I came to Carnegie Mellon about the science of security, and science is based on evidence, and the reason why you want evidence is it gives you something to evaluate and you can look at it and you can assess whether or not it's credible, whether it's valid, applicable. Without that, then you're left really in a very challenging situation to try and figure out, "What does this software do? What does this security system do? Does it really protect privacy? What's it mean to be accountable?"

The goal is to go from relying on assurance-- that's with an A. Assurance where I tell you that it's good, or insurance, which means that I will compensate you if something's broken, and we really want to get to ensurance with an E, to ensure, to know that it is what we say it is.

And so with that, I think we have one last poll.

Technology Poll

Technologies

Technology Poll

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

very optimistic

optimistic

neutral

pessimistic

very pessimistic

**072 Presenter: Yeah, final poll question. Before I launch that, there's just a couple questions coming to the Q&A tab just about the download of the slides of today's materials. The file's so large that some of those videos may not play in the PDF version, so if there's any particular video you're looking for, let me know. I will send out an email tomorrow when the archive is

available of this event. Reply to me and I can send you the location of where to find those video files from the PDF.

So I will launch that final poll question now, and the question is: What is your outlook on cybersecurity for the next decade? Are you very optimistic, optimistic, neutral, pessimistic, or very pessimistic? And we'll give you about 15 seconds to vote there.

While we're doing that, Greg, just a question back to SEI's work on blockchain. Why is that particularly relevant to the DoD? Can you speak to that a little bit?

Presenter: Well, one application is potentially how we work with coalition partners and how, as information comes in and being able to track information and understand its provenance, it's potentially one way to disintermediate the trust. You may be working with partners who don't trust at least one other partner. So in that trust-constrained environment, how can you use technology to facilitate capabilities.

Another reason for looking at it is it's a technology adversaries are using to enable malicious cyber activity and fund malicious cyber activity, so it's important to understand how these technologies work, where their vulnerabilities are, and how to protect our nation's interests in that area.

Presenter: Great. A question/comment here saying: In my experience though-- talking back to that fuzzing again. In my experience though, effective fuzzing requires serious amounts of skill. It is not a panacea due to the weakness of this tool set at this juncture, thus requiring deep tester skill.

Presenter: Unfortunately that is generally true today. I think there's a number of business models that are being tested out there in the startup community, anywhere from specific software that's provided to an organization to services that will do fuzzing for you. But at the end of the day the efficacy of fuzzing I think is undeniable, and the notion of putting out software where a week or two of CPU time would find some immediate vulnerabilities I think will hopefully soon become seen as negligent.

Presenter: All right, so that empties our queue, so let's get back to the poll results and see if anybody has any questions while we read those off, and then we'll be able to wrap up. So the question was: What is your outlook on cybersecurity for the next decade? We got 8 percent very optimistic; 30 percent optimistic; 22 percent are neutral; 32 percent pessimistic; and 8 percent very pessimistic. Any surprises there?

Presenter: I'm impressed with the variety. I think what it really says is we don't know. Personally, I'm concerned about the Internet of Things, the lack of tools to create

even reasonably secure systems. One of the issues that we were promoting at OSTP as part of the R&D plan was the notion of secure update, that every system should have the ability to do a secure update. Over at the Department of Commerce, they said, "Well, that's where we want to get to," but their first step was just to even label products about whether or not they were even updatable, regardless of whether or not the update was secure. So I think that shows that there's recognition that we need to be thinking about how we're going to live with some of these elements for decades, potentially, or at least years, and how we're going to deal with the fact that we know that at least today they're going to have vulnerabilities and how do we patch those.

I'm optimistic that we'll deal with things-- we'll manage the risk in the short-term, but I expect there'll be some painful incidents. I expect they'll probably actually occur in other countries. In this country we're fairly well positioned from an incident management, tracking, incident response-- we have national policies in place, both at the private sector, the public sector, on how to deal with challenges. Other countries with much fewer resources are going to have some real challenges. I mean, most other countries, except for a few large countries-- most other countries in the world are the size of a state or much smaller. And so when you think about a state being

able to protect itself, we know that that can be very challenging, and they really need more substantial resources.

Presenter: Right. Now I know you're talking tomorrow at the Data Science Symposium. I think there are some spaces available for people in the D.C. area-- I know it's late notice, but there is some room available for that. That's the last question we have, folks, so we're going to wrap up there. I do ask that you fill out your survey upon exiting today's event as your feedback is always greatly appreciated. I mentioned earlier I will send out a link to the archive which will be available tomorrow morning for replay, and the last thing I'd like to pass along is our next webinar will be September 7, and the topic will be Agile Metrics for Government Programs by Will Hayes and Eileen Wrubel.

Presenter: Excellent.

Presenter: Thank you very much for attending everyone, and have a great day. Greg, thanks again for your presentation.

Presenter: Thank you. Thank you everyone.

SEI WEBINAR SERIES | Keeping you informed of the latest solutions

