CyberEdBoard Talks

Zero Trust: Separating the Model From the Myths

A Conversation With Zero Trust Creator John Kindervag and NIST Fellow Ron Ross

CyberEdBoard Talks Excerpt
Access the full interview by becoming a member.
Visit CyberEdBoard.io to submit your application.

CyberEdBoard

John Kindervag
Creator of Zero Trust

Ron Ross
NIST fellow

The CyberEdBoard Talks series is designed to address the most critical challenges executive members are discussing in the private global ecosystem and is presented by respected industry experts and chief cybersecurity practitioners.

One of the unique benefits of CyberEdBoard is that you must be a member to access this session and all other content and engagement opportunities. "The global community continues to grow at a pace that reconfirms the critical importance of cybersecurity collaboration and executive information sharing, and we are thrilled to support each member's unique needs within the private ecosystem," said CyberEdBoard Executive Director Chris Ancharski.

This edition of the CyberEdBoard Talks series was held on April 29, 2021, exclusively for CyberEdBoard members.

The zero trust security model: It's 11 years old now and more popular than ever, but still there is confusion over what it is and isn't. This exclusive – and spirited – CyberEdBoard session exposes the marketing myths and extols the cybersecurity realities.

Join this conversation between zero trust creator John Kindervag, NIST fellow Ron Ross and Tom Field, senior vice president of editorial at ISMG, as they discuss:

- Why we need zero trust;
- Myths in the marketplace;
- Pros and cons of the NIST Zero Trust Architecture.

Kindervag is senior vice president of cybersecurity strategy and an ON2IT Group Fellow at ON2IT Cybersecurity. Previously, he was field CTO at Palo Alto Networks. Earlier, while working at Forrester Research, where he was a vice president and principal analyst on the security and risk team, he created the zero trust model. He also previously served as a security consultant, penetration tester and security architect.

Ross specializes in information security, systems security engineering and risk management. He leads NIST's Federal Information Security Management Act Implementation Project, which includes the development of key security standards and guidelines for the federal government and critical information infrastructure. Ross also leads the Joint Task Force, an interagency partnership with the Department of Defense, the Office of the Director of National Intelligence, the U.S. Intelligence Community and the Committee on National Security Systems, with responsibility for developing the Unified Information Security Framework for the federal government and its contractors. In addition to his responsibilities at NIST, Ross supports the U.S. State Department in the international outreach program for information security and critical infrastructure protection.

Zero Trust: In the Beginning

TOM FIELD: What is the origin of the zero trust model, and what were the conditions that created it?

JOHN KINDERVAG: Zero trust came out of research that I was tasked to do when I joined Forrester Research in 2008. Prior to that, I was a network engineer, security engineer and pen tester. I had been installing old-school firewalls, and I had to arbitrarily apply a trust level to an interface. It drove me nuts because PCI compliance said, "If you are going from a trusted interface in which the internal interface is going outbound to the external interface, you don't need a rule."

There were no rules – all that traffic was allowed because of the trust model – and I realized that this trust model was causing a lot of bad things to happen. Rules are really important, and most data breaches happen because you don't have the right outbound rules.

FIELD: Ron, how did you first encounter the principle of the zero trust model?

RON ROSS: I met John about 10 years ago, and I always thought it was an intriguing concept back in those days. I was doing enterprise security work with the risk management framework and the security controls. Around 2012, I started also working on the system security engineering front and trying to build the engineering guidelines that we now have – the SP 800-160 series. I went back and looked at some of the groundbreaking research that John had done, and I thought that the basic, core security design principles we used for 800-160 aligned very, very closely. You use those principles to achieve the zero trust model.

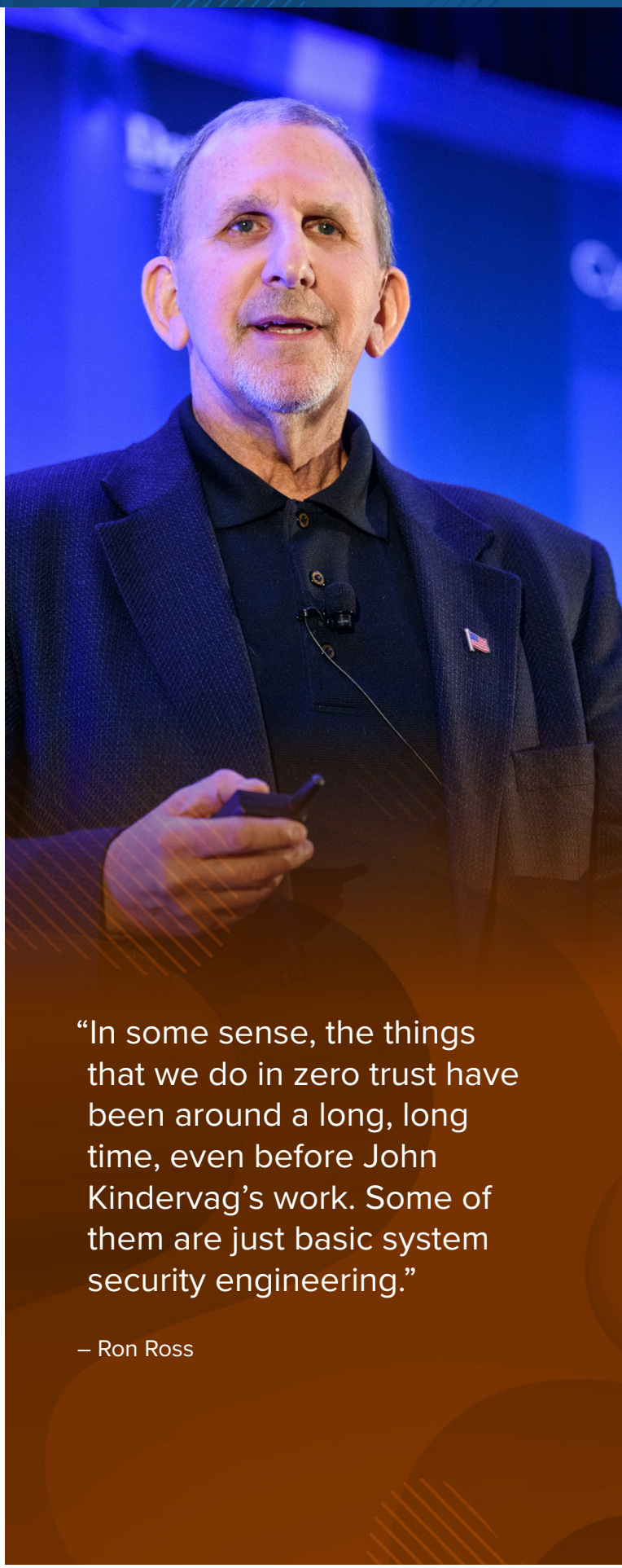
Zero trust's time has come. It's part of our evolution from recognizing that we can't defend the perimeter anymore. The perimeter has gotten very porous due to cloud computing and mobile and cyberattacks.

Zero Trust in the 2010s

FIELD: John and Ron, talk about what progress was made toward zero trust from 2010 to 2019. I would hear it come up in a few conversations, but it wasn't to the degree that we saw on the showroom floor at the RSA Conference in 2020. What happened for most of the decade?

KINDERVAG: From my perspective, when I was at Forrester, I was behind a paywall. In NIST SP 800-207, they don't reference any of the Forrester reports, which I think they should have. They never read any of the reports because they didn't want to pay for them.

I had to get out from behind the paywall. When I moved over to Palo Alto Networks, it was the first vendor who said, "You're not crazy. We're going to support you." Then everybody else started to look and say, "Hey, we have to do this," because Palo Alto Networks, at that time and even today, was the company that you looked at to be innovative. So suddenly all these other vendors had big zero trust initiatives.



"In some sense, the things that we do in zero trust have been around a long, long time, even before John Kindervag's work. Some of them are just basic system security engineering."

– Ron Ross

> “Zero trust is a framework, but I don’t want it to be prescriptive, as in, ‘Here’s how you have to do it.’”
>
> – John Kindervag

ROSS: I don’t think we’ve made a whole lot of progress on the ground in the last 10 years because the way we do business today is largely reactive. We’re always chasing the last cyberattack. Going back to the concept of zero trust, if you go into SP 800-60 and look at Chapter 2, we define a system-of-interest as being a grouping of system elements, and those could be operating systems, applications, network devices, people, processes, and procedures. All of those elements come together to give that system capability, but the important thing from a system security engineering point of view is that for every one of those elements, you look at the level of assurance – the trust or lack of trust, as John would say – and how they interact with each other.

We don’t routinely take that architectural and engineering approach. The industry has grown so fast and so large with the innovations that we’ve been experiencing. There has been such a drive to bring in more and more technology, and we have not been emphasizing the architectural aspects. In some sense, the things that we do in zero trust have been around a long, long time, even before John’s work. Some of them are just basic system security engineering.

People Started Talking

FIELD: Zero trust went from being a marketing buzzword into today’s hottest business strategy. John, you were at Palo Alto Networks at the time. Tell us about how you saw it happening.

KINDERVAG: What changed is that people started talking about it. The first rule of zero trust used to be the same as the first rule of “Fight Club”: Don’t talk about it.

In 2019, I spent over 200 days on the road and went to 13 countries. There are zero trust environments on every single continent on this planet but almost none of them will talk about it. Because of the movement at DISA [the Defense Information Systems Agency], Gen. Nakasoni [Paul Nakasoni, commander, U.S. Cyber Command and director, National Security Agency] and Adm. Norton [Nancy Norton, former DISA director] started talking about it, and that really moved the bar. Then NIST moved the bar in the special publication that made people aware of zero trust. It’s a very prescriptive document.

Zero Trust Today

FIELD: Ron, what motivated the development of SP 800-207, Zero Trust Architecture, in 2020?

ROSS: It’s a recognition that the traditional strategy that we had been working on for the past decade or two or three wasn’t always working. It’s an attempt to take a fresh look at the problem by going back and looking at some of the previous research and the work that John had done when he was at Forrester, and then following up after that.

There’s no doubt that the pandemic and this massive exodus from within the federal agencies and the private sector to remote work put a spotlight on the problem. People had to continue to work, but all the resources that were behind that so-called trusted perimeter, which was never really trusted, were now scattered everywhere. This gave us an opportunity to explore different ways of looking at the problem.

"We have to help regulators and auditors understand that we're living in a risk-based world and we have to be able to think out of the box."

– Ron Ross

Controversy Around Zero Trust

FIELD: John, you've got strong feelings about the zero trust model getting anywhere close to a framework. Why is that?

KINDERVAG: No, it is a framework, but I don't want it to be prescriptive, as in, 'Here's how you have to do it.' And I don't want it to be tied to a technology. It's all based on protect surfaces. The first thing you need to do is define your protect surface: What do you need to protect? And what you protect is called a DAAS element – data, applications, assets or service. You take a single DAAS element, put it into a single protect surface and map the transaction flows around it, so that you understand how it works. A lot of failures are because we don't understand how the system actually works. Understanding how the system works will show you how to architect. It will show you the controls you need to put in place. So, the architecture is the third step. It was the first step in the way we traditionally did things in our legacy '80s and '90s world.

ROSS: I would say that the very first thing organizations have to do is figure out what's most valuable to you within the organization. Criticality analysis is job number one. Today you have to really ask yourself: How much loss am I willing to endure? What kind of negative effects or negative consequences are acceptable to me? Then the system has to be engineered to achieve that level of assurance. Assurance is the key word because it gets down to what we can achieve through good architecture and good engineering.

Security Control Testing and Zero Trust

ANDREW KIM (CISO, ALLSTATE): How important do you think security control testing is in the context of zero trust?

KINDERVAG: I can send two pen testers out two different days and they'll give me different results. I can send the same pen tester out two different days and they'll give me the same result. But that assumes that your perimeter is the thing that we have to worry about, and we have to worry about the protect surface. In Allstate's case, that's the data about your clients. That's what you need to put the controls around and then test that particular protect surface, but not the entire perimeter, the internet, everything. You just can't know that, so break the problem into smaller chunks because we have so many problems, we will run out of money before we run out of problems.

ROSS: Security control assessment is interesting because controls can be different. There are management-level controls, operational controls and technical controls. Technical controls typically are buried in hardware, software and firmware, and it depends on what kind of testing you're able to do. If you're a pen tester or you're just doing regular security control assessments, most of the time you don't have access to the internal design documentation of those modules inside that system with the software. So there's a glass ceiling on how much testing you can actually do. Control testing is good but we should recognize it has limits, and it doesn't replace other types of deep-dive evaluations.

Compliance and Zero Trust

DONNA ROSS (CISO, RADIAN GROUP): I understand that standards inhibit innovation. You're talking to a bunch of CISOs; we totally get that. But someone needs to tell our regulators, auditors, clients and customers that, because they come in and use things like checklists and if we don't check the list, they're going to write us up. We would love to innovate. When the endpoint protection tools first came out, I would have been an early adopter but my auditors were checking a box for antivirus and that wasn't it. If you both could address that, I'd love to hear what you have to say.

ROSS: I've always looked at compliance as applying a well-designed security program that's risk-based, allowing people to make decisions, being flexible. That static checklist, or any type of static-view security, is always going to fail because, if your checklist has 10 items, the adversary will go to item number 11 that you didn't have on your list, and that's where you're going to fail. So I get the problem. I've been dealing with this for 30 years in the federal government and outside the federal government.

Regulators and auditors have their view of the world. We have to always push back and try to help them understand that we're living in a risk-based world and we have to be able to think out of the box, innovate and not get locked into these dogmatic things that take us down the wrong road.

KINDERVAG: Congressman Will Hurd was one of the co-authors of the OPM [U.S. Office of Personnel Management] Data Breach Report, which said zero trust should have been adopted because it would have limited the attackers' ability to have access to the sensitive data. Hurd asked me, "What is the fundamental problem in cybersecurity?" and I said, "There are too many compliance mandates. They all overlap. They self-contradict." If you're a CISO, your job is paperwork. We need to streamline that and focus on things that actually protect us. Compliance never protects us. It's not a strategy; it's just a checklist of things. The industry has to push back and say to the compliance world, "You don't get it."

> "CIOs have told me that the reduction in audit costs paid for what they did for zero trust."
>
> – John Kindervag

Selling Zero Trust to the Business

AHMED MOHAMUD (VP, CYBER RISK, MORGAN STANLEY): What have you seen as a successful selling point to the business, and in implementations that you have been a part of, what were the biggest drivers for success?

KINDERVAG: There's a huge reduction in operational expenditures. Auditors love zero trust because they understand it, and most audit requirements were made for old-school networks. CIOs have told me that the reduction in audit costs paid for what they did for zero trust.

ROSS: The biggest selling point for me would be reducing and managing complexity. We have way too many components in this very complicated infrastructure. When the OPM breach happened in 2015, the Department of Homeland Security asked every federal agency to identify its high-value assets and they did that. The second step was determining what those assets were connected to, and they found out a lot of connections that nobody even knew about. The complexity had just grown. Part of the notion of zero trust and engineering and architectural view is discipline and structure in how you build out that network. ■

The full transcript and recording are available for members within the CyberEdBoard engagement platform. Visit CyberEdBoard.io to submit your application.

About CyberEdBoard

CyberEdBoard is the premier members-only community of executives and thought leaders in the fields of security and IT. Membership in Information Security Media Group's CyberEdBoard provides executives with a powerful peer-driven collaborative ecosystem and library of resources to address complex challenges shared by CISOs and senior security leaders worldwide. Executive members use the CyberEdBoard engagement platform to further enhance their professional brands, create and exchange member-exclusive resources, obtain accredited education and content, contribute in the executive mentor marketplace and seamlessly connect with senior security peers and experts around the world.

Join the Community. The CyberEdBoard global community is accepting applications from qualified CISOs and senior security stakeholders. To submit your application for membership consideration, visit CyberEdBoard.io today.

About ISMG

Information Security Media Group (ISMG) is an intelligence and education firm focused exclusively on cybersecurity. Our 30 global media properties provide security professionals and senior decision-makers with industry- and geo-specific news, research and educational events.

CyberEdBoard Talks Excerpt

Access the full interview by becoming a member.
Visit CyberEdBoard.io to submit your application.

CyberEdBoard

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io