TRANSCRIPTS

# January 2024 Videos

A complete transcript of every recorded talk from the January 2024 Videos.

| 1 | 10:28 |
| --- | --- |
| TALKS | RUNTIME |

November 26, 2026

# CONTENTS

Full transcripts of all 1 recorded sessions, in the order they appear in the archive.

01 2024-01-02-Introduction-to-KERI-Samuel-M-Smith-yP3ell4VgA 10:28

TALK I

# 2024-01-02-Introduction-to-KERI-Samuel-M-Smith-yP3eII4VgA

January 2024 Videos · talks · 10:28

This is an introduction to KERI, the Key Event Receipt Infrastructure. My name is Samuel Smith and I am the inventor of KERI. The reason I invented KERI is because the internet is broken and I wanted to solve it. And so the problem that KERI solves is called the universal secure attribution problem. Okay, what do we mean by universal secure attribution problem? Well, universal means everywhere.

We want it to be solved everywhere. And secure means do it in a way that can't be hacked or forged or impersonated or attacked in the normal way that we get attacked on the internet. Attribution means assigning a communication to its source. We want to attribute where something came from to its source. We know who's sending it to us. And so the problem is, how do we do that everywhere on the internet in a secure way so that we know who's sending us information? So that doesn't mean we want to enable anybody to track everybody's conversations. We want to do it in a privacy protecting way. So that poses additional challenges. But first we have to get the security down. Many people approach this problem and they sacrifice security. And if you sacrifice the security, then you don't have privacy either. So, what we want to do is solve all of these problems at the same time in a very integrated, elegant, simple way. Let's talk about what it means. Secure attribution is another way of saying we want to establish the authorship of data, any and all data sent over the internet, any and all documents, things like credentials, entitlements, authorizations. We want to be able to say that we can securely attribute who's doing what in a privacy-preserving way. And I keep saying privacy because I don't want to give the false impression that we're trying to build this universal tracking system. The hard problem is to be able to do this all in a way that keeps confidentiality and privacy along with secure attribution.

That's always been the hard problem. So to restate, the problem is we want to have verifiable secure attribution of any communications to its source. Now I added the word verifiable. What does verifiable mean? It means that if we're receiving information, we need some way to verify where it came from. When I say verify, it means in a cryptographic sense. It means doing it without having to trust any third party. I don't want to have to trust somebody else to verify what somebody that I want to communicate with in a private confidential way says. I need to be able to do it by myself. If I have to trust someone, then the security of whoever I'm trusting now becomes something I have to worry about. And that is a problem.

Another way of looking at secure attribution is to say that we want to have provenance of any data by anyone, to anyone, from anyone. And so a way we can describe that is as authentic data. And then we want authentic data provenance.

Authentic has two meanings. It means like true to yourself, like you're being authentic. That's not the meaning of authentic we're using here. We're meaning authentic as you can attribute it to its source. Who painted that painting is an authentic painting, right? As opposed to when something's not authentic. It means it was forged or somebody was impersonated. Somebody sends you information and they say it came from Joe when it really came from Sue. And so the whole problem is back to the same thing. We need to securely attribute the source of information. So what do I mean by provenance? We often hear the term provenance when we talk about like a painting, like fine art, right? Was it painted by Rembrandt? And how do you know it was painted by Rembrandt? Well, one way that you would provenance it is that you would establish a chain of custody of that painting from Rembrandt to whoever Rembrandt sold or gave the painting to whoever sold or gave the painting and so on. And if you can follow that chain of custody to the present owner or holder of that painting, then you can say, yeah, it came from Rembrandt. So if we can solve data provenance, then we can solve many of the security problems on the internet because most of them come from the fact that we can't solve data provenance. We don't have universal secure attribution.

And because we don't have universal secure attribution, people can forge things. People can impersonate things. Well, when we send data over the internet, we have a similar problem. Somebody sends a message. It gets sent to some server in the cloud who then sends it to another server, who routes it to another server, who routes it to another server, and then it ends up in your inbox. And you go, did it come from where it said it came from? Anybody that was in the path could have intercepted it, spoofed it, done something to it, and then it shows up in your box and it says, oh yeah, this came from Sue, but it really came from Bob. So provenance is about establishing secure attribution even though the data traverses multiple hosts or servers on the internet. It didn't come directly to us. It wasn't given to us in person. It came over the internet and the internet is public. The internet is public infrastructure. It's public, which means that lots of people have the ability to see what you're sending or to change what you're sending or to mess with it. And many of the attacks on the internet come from the fact that it's public infrastructure and therefore publicly accessible for attackers to attack. So we want to solve this secure attribution problem. Let's dig a little deeper. On the internet, we're just sending information. Data is information. It's just bits. Now we talked about chain of custody. When we normally think of chain of custody, we think of a physical item. So I'll call it those its. They're atoms. So if I actually have a painting, there's only one of them. And it takes a lot of work to copy that painting. And if I have two, then I have a problem because somebody made a copy. How do you tell the original from the copy? Well, if the copy is done really, really well, just looking at the two, you can't tell the original from the copy. That's why you have to have a chain of custody. You say the original was in possession of somebody and they gave it to somebody else and they gave it to somebody else. And the copy was never in their possession. possession. So you know it's a copy because it wasn't part of the chain of custody. That works for atoms. It doesn't work for information bits. So we have a harder problem to provenance data information. So we have to use cryptography to do that. One of the first things we do with cryptography is that we give an identifier to the source. The source now has an identifier. That identifier is an electronic identifier.

It's more information. It's more bits. To make the ability to security attribute to a source, that identifier needs to be unique. And in order to have universal secure attribution, that identifier needs to be universally unique. There can only be one in the whole universe. The only way that we can guarantee your universally unique identifiers is to use cryptography or to use some trusted third party who creates them. Well, we don't want to have to rely on a trusted third party, so the identifiers must be cryptographic in nature. So, let's suppose that we have a system for generating cryptographic identifiers. Now, we must be able to prove who controls that identifier, and we have to do it in a verifiable way without trusting the third party. If I have a cryptographic identifier and a way to verifiably prove controller over that identifier, then I have what is called a root of trust. I have the ability now to attribute data to that identifier where that identifier is the source of that data. So, I now have constructed the basic problem. The way that I can control an identifier or prove control of an identifier is to use what we call cryptographic keys. And the specific type of key that we use belongs to something called a public key pair or a public private key pair where I have a public key and a private key. That is going to be in a completely new subject to talk about the basics of public private key pairs. But what we've done is set up the core idea of how we get to universally secure attribution. And we haven't even really talked about how KERI does it, but I've given you an introduction to the hard problem. The hard problem is universal secure attribution. Follow along to learn more. Leave any questions in the comments.

Thank you.

Thank you.