CS 240: Digital Signatures Transcript

[00:00:00] So the question we had before was why should a client trust that a server's certificate came from a certificate authority that they can trust? And we said the, the answer is that the certificate authority is going to digitally sign the certificate file so that people can trust it now to be able to trust that, that means the client needs to be able to verify the signature on the, on the certificate file and, and make sure that it's, it's legitimate.

[00:00:27] But if we step back more generally, we could ask the question, if somebody is going to send me a file or a set of data doesn't have to be in a file, maybe it's over a network or whatever.

[00:00:40] But if somebody wants to send me um a, a bunch of data, how can I verify for sure that the data actually came from who I think it came from? And so, you can imagine that in a digital economy, this kind of question comes up a lot.

[00:00:55] How can I trust this data that I've been given? Somebody sent it to me, they said who they were, but I've got to be able to verify that they are, who they, they say they are.

[00:01:04] So this is more general be even beyond digital certificates is how can I validate the, the authorship or the origin of, of some data? That's where digital signatures come in? OK, so the idea of digital signatures is going to combine a few of the ideas that we've already talked about.

Start visual description. The professor demonstrates how to validate the authorship or origin of data using digital signatures. The professor explains that digital signatures combine cryptographic hash functions and public key encryption. End visual description.

[00:01:26] So we've talked about cryptographic hash functions like sha 256 we've, we've talked about um public key encryption.

[00:01:36] And so both of those technologies are going to be involved with, with digital signatures.

[00:01:41] So let's say that I want to send some data to somebody else and I want to put my signature on it so that they can, can trust it.

[00:01:48] First of all, let's look at the process from the, the side of the, the person who's sending the data, we're going to call that person the signer because they want to sign their data.

Start visual description. The professor demonstrates the process from the sender's side, showing how to create a digital signature by running data through a cryptographic hash algorithm and encrypting the hash with a private key. End visual description.

[00:01:58] So the first thing the sender or the signer of the data is, is going to do is they're going to take their data and they're going to run it through a cryptographic hash algorithm like Shaw 256.

[00:02:10] And so you can see that here on this slide. So, I've got a file of data.

[00:02:15] We're going to pass it through a cryptographic hashing algorithm and the output of the hashing algorithm of course is a digest.

[00:02:22] It's a, it's a fixed size summary of the data that I just hashed.

[00:02:28] And so we're going to call that the, the signer digest.

[00:02:33] And then what I do as the, as the, the center of the data is I take that one-way hash or the, the signer digest and I encrypt it using my private key.

[00:02:46] So take the output of the hash function encrypt it with my private key, which of course nobody else has.

[00:02:53] And then what I do is I take the original data file and the digital signature. So, once I've encrypted the, the signer digest, we call that the digital signature.

[00:03:03] And so what I'm going to do is take the data file.

[00:03:05] I'm going to take the digital signature and I'm going to send both of those things to the receiver of the data.

[00:03:15] Now, on the receiving side, what does the receiver do to validate or to verify the digital signature? So, what the receiver will do is take the data file that was sent to them and pass it through the same cryptographic hash function that the sender used and the output of that uh will be called the receiver digest.

Start visual description. The professor demonstrates the process from the receiver's side, showing how to validate a digital signature by decrypting it with the sender's public key and comparing the resulting hash with the hash of the received data. End visual description.

[00:03:40] So the output of the hashing algorithm is the receiver digest.

[00:03:44] And then what the um the receiver will do then is they will take the digital signature they were given, and they will decrypt it using the signer or the sender's public key.

[00:04:01] Because if you recall the digital signature was encrypted using the sender's private key.

[00:04:06] So it can be decrypted with the, the sender's public key, which is, is public information.

[00:04:12] So the receiver takes the digital signature and decrypt it using the sender's public key and that gives them what, what is the, the signer digest? So, they've now recovered the signer digest.

[00:04:25] And then what they do is they just compare the signer digest and the receiver digest.

[00:04:29] And if as long as those two things are equal, then we know that this data was sent from the sender and that their identity is, is um as described in their public key because the sender's identity is included in.

[00:04:46] Um Well, we obtained uh the sender's identity somehow maybe through a certificate file or some way.

[00:04:54] And because these two digest match, then we know that the sender is the person who actually sent the data. So that's, that's how you verify a digital signature.

[00:05:05] So let's go back to certificate authorities. So, they create certificate files for people that have websites.

Start visual description. The professor demonstrates how certificate authorities create and digitally sign certificate files, explaining the importance of trusting these authorities. End visual description.

[00:05:15] But when a certificate authority creates a certificate file, what they do is they digitally sign that certificate file.

[00:05:24] And of course, they're going to use their private key to digitally sign a certificate file.

[00:05:33] And then when a web browser receives a certificate from a, a web server, then it can go ahead and validate the digital signature that's on the certificate file and ensure that that that certificate was created by somebody they do trust.

[00:05:47] Now at some point, we do have to trust somebody.

[00:05:49] And so that's the idea here is that at some point we have the certificate, authorities that everybody knows who they are, they're well known and, and everybody trusts them.

[00:05:58] And so if, if I can verify that this certificate file was created by somebody, I trust, then I'll go ahead and trust the certificate.

[00:06:05] So that's one big application of digital signatures.

[00:06:08] Another application of digital signatures is in Cryptocurrency.

[00:06:12] So if you have a Cryptocurrency system like Bitcoin, where you have all these digital transactions uh going on digital signatures can be used to verify the authenticity of transactions.

Start visual description. The professor demonstrates the application of digital signatures in cryptocurrency systems like Bitcoin, explaining how digital signatures verify the authenticity of transactions. End visual description.

[00:06:26] What I mean by that is if every transaction is digitally signed by the parties involved in the transaction, then we can, we can validate the identity of the, the people or the organizations that participated in a transaction.

[00:06:41] So what this boils down to is that means digital transactions can't be forged.

[00:06:45] So it's not like I could impersonate somebody else and buy a bunch of uh spend a bunch of their Bitcoin on, on something and get away with it because I don't have their private key.

[00:06:55] So there's no way I could digitally sign that transaction as them because I don't have that ability.

[00:07:01] Um The other thing that digital signatures give us is nonrepudiation.

Start visual description. The professor demonstrates the concept of nonrepudiation, explaining how digitally signed transactions prevent parties from denying their participation. End visual description.

[00:07:06] Meaning if every transaction is digitally signed, then the people involved in the transaction can't deny later that they actually participated in the transaction because we can prove that they did because they signed it.

[00:07:19] Now, of course, all this assumes that people are actually keeping their private keys private.

[00:07:23] If your private key becomes public, then you've got, got trouble at that point.

[00:07:28] So we are assuming that the privacy of the private keys, but even more generally than Cryptocurrency. Anytime you want to send a file to anyone or a body of data to anyone, you could, if you wanted to digitally sign it, so they can uh validate um that the data came from you.

Start visual description. The professor demonstrates the general application of digital signatures in various industries, such as finance, healthcare, legal contracts, and the military, emphasizing the importance of validating identities. End visual description.

[00:07:46] So you can imagine in industries like finance, health care, legal contracts, the military, there's all kinds of very sensitive applications where we really do need to, to uh know who we're dealing with.

[00:08:01] And so digital signatures are really effective in a digital environment for helping validate who people are.

Start visual description. The professor demonstrates the effectiveness of digital signatures in a digital environment for validating identities, highlighting their use in sensitive applications. End visual description.