CS 240: Secure Key Exchange Transcript

[00:00:00] **INSTRUCTOR:** As we've previously discussed, public key encryption is really powerful because the encryption key and the decryption key are different.

[00:00:09] And what that lets me do is it lets me publish my public key to the world and keep my private key private, and then anyone who wants to send me encrypted data can encrypt the data with my public key using an algorithm like RSA, and then they can send the encrypted data to me, and then I'm the only one that can decrypt the data because I'm the only one that has access to the private key.

[00:00:35] And so that's a very powerful idea. The challenge we have is, as we've also discussed, that public key encryption algorithms tend to be really slow.

[00:00:48] And so to encrypt large amounts of data with a public key algorithm isn't really feasible because it just takes too long. The symmetric key algorithms like AES are much more efficient and a lot faster, and so if we're going to encrypt a lot of data, we really want to use a symmetric key algorithm.

[00:01:07] And so the question becomes, how can we still take advantage of public key encryption's unique capabilities but also use a symmetric key algorithm to actually encrypt the data? And this is where the topic of this video comes in.

[00:01:26] So in this video, we're going to talk about secure key exchange. And so the big idea with secure key exchange is if somebody wants to send me some encrypted data, rather than have them encrypt all the data with my public key using a public key algorithm, what we'll do instead is we'll generate a key for a symmetric key algorithm like AES, and then we can securely exchange that symmetric key using public key encryption.

[00:02:00] And then once we've securely exchanged the key using public encryption, then we can use the symmetric key algorithm to actually encrypt the data that's being

transferred or exchanged. And so that allows us to still take advantage of public key encryption to exchange the symmetric key that we're going to use to actually encrypt the data.

[00:02:21] So that's the big idea with secure key exchange. So this slide demonstrates how secure key exchange works. So this is basically the same idea I just talked about. It's just a little more detailed. So in this slide, we're going to assume that Bob wants to send some data to Alice.

Start visual description. Slide titled Secure Key Exchange. The slide shows a chart of how data is sent with an example of the data sender being Bob and the data receiver being Alice. End visual description.

[00:02:43] Now, this could be in many different ways, right? They may transfer the data over a network, or they may transfer it through a thumb drive, or whatever the situation is. All we are assuming here is that Bob wants to send a large amount of data to Alice.

[00:03:01] So the first step in this process, this key exchange process, is that Alice will send her public key to Bob. Now she doesn't mind doing that because her public key is indeed public. She doesn't mind giving it to anybody and everybody who wants it.

[00:03:18] And so she first sends her public key to Bob. And then what Bob will do is he will generate a random symmetric key for an algorithm like AES. So once he's generated a key for the symmetric key algorithm, then what Bob will do is he'll encrypt that symmetric key with Alice's public key.

[00:03:40] And then he'll send that encrypted symmetric key back to Alice. And then of course she'll decrypt the encrypted symmetric key that Bob sent her. And once she's decrypted that key, now Bob and Alice both have access to the symmetric key.

[00:03:57] And then once they both have that key, they can easily encrypt and decrypt data going back and forth. So the next step in this process would be Bob would go ahead and encrypt the data that he wants to send to Alice using the symmetric key that he generated and send the encrypted data over to her.

[00:04:12] And then she would just decrypt the data using the symmetric key as well. So that way we have efficiency and speed, but we also still have this ability to use a public and private key pair to encrypt at least the symmetric key as it's being exchanged.

[00:04:30] And so that really is kind of the best of both worlds. Now one thing I should point out is that if you ever study real world secure key exchange algorithms, you'll see that they're a little bit more complicated than what I just described, but not that much. And so the big idea is what we just talked about.