CS 240: Encryption Applications Transcript

[00:00:00] Having talked about both symmetric key and asymmetric key encryption algorithms.

[00:00:04] Let's just talk a little more generally about uh some applications of data encryption.

Start visual description. The professor demonstrates the concept of data encryption, explaining the importance of keeping data private by encrypting it. He shows examples of symmetric and asymmetric key encryption algorithms on the screen. End visual description.

[00:00:11] So we, we talked earlier about how we want to keep our data private and, and to keep it private, we encrypt it.

[00:00:17] And there's two basic um scenarios where you want to, to keep your data private.

[00:00:22] One is when the data is in motion and that means it's being transferred across a network typically.

[00:00:29] And um HTTPs is something you're probably familiar with.

Start visual description. The professor discusses the use of HTTPS for secure communication over the internet. He shows a web browser with a URL starting with "https://" and explains how the "S" indicates that the data is encrypted. End visual description.

[00:00:35] So when you use a web browser and you type in a URL, usually a URL in your web browser starts with http S colon slash.

[00:00:42] And that means that uh secure, http S is the protocol that's being used when the, the browser and the server communicate with each other.

[00:00:50] And the S in that case uh means secure.

[00:00:54] And so what that really means is that the data is being encrypted as it's passed back and forth between the, the web browser and the web server.

[00:01:02] And so http S adds encryption.

[00:01:06] So you can be pretty confident that people aren't snooping on your data as it goes across the internet because it's, it's encrypted.

[00:01:13] So HTTP S is a, is a super important application of encryption.

[00:01:18] But in general, anytime data is in motion across the network encryption can, could be used even if you're not using HTTP S OK. The next scenario for protecting your data is when data is at rest.

[00:01:29] So we say data is at rest when it's stored in a file or in a database.

Start visual description. The professor explains the concept of data at rest and the importance of encrypting stored data. He shows a database and a file on the screen, discussing how encryption can protect data from unauthorized access. End visual description.

[00:01:33] So it's not moving across the network, it's just sort of stored in a file or a database somewhere.

[00:01:40] And um it's, it's important to think about if you're storing data in a, in a database or a file, should I encrypt it? I always think about what if a hacker with bad intentions was able to break into my system and get access to my database or my

data file, what would they be able to do with it? How valuable, how valuable would it be to them? What could they do with it? How damaging would it be to my customers or to my company? And so, if, if you really, really feel like you're storing some data that's sensitive, you probably need to encrypt it when it's at rest.

[00:02:16] And um there's a couple of different ways you could do that.

[00:02:18] One is, you could do application-level encryption.

[00:02:21] That means in your application code, you could write code similar to the examples we've looked at in this lecture and encrypt the data yourself.

[00:02:31] And that's not that hard to do.

[00:02:34] Another thing you could do is use a database that does database level encryption.

[00:02:40] So with a database that supports encryption, they'll actually um encrypt the files that they're using to store the data on disk because of course, a database really ultimately is just a bunch of files on disk.

[00:02:52] So a database that supports encryption would, would encrypt the data files that are, they're stored on disk.

[00:02:58] So that if, if anybody got their hands on your database, uh files, they wouldn't be able to access the data because it's encrypted.

[00:03:06] So you can encrypt it yourself. You can depend on a database to encrypt it.

[00:03:09] But either way, um you're going to, I need to think about should I be encrypting my data? And the answer will oftentimes be uh yes, for at least some of the data, another encryption application that you're probably familiar with is a password manager.

[00:03:25] You're familiar with the idea that you have uh like 3000 accounts on different websites.

Start visual description. The professor talks about password managers and their role in securely storing passwords. He demonstrates how a password manager encrypts the password file and uses a master password to derive an encryption key. End visual description.

[00:03:31] And it's hard to keep track of all those passwords.

[00:03:34] If you want to be secure, you should use long passwords that are uh very, very hard to guess and you should use different passwords on each website. But on the other hand, that makes it almost impossible to remember your password and so on.

[00:03:49] And so you have this, this, this conundrum, right? So, a lot of people use, use password managers so that they can have good passwords for each user account that they have, but they don't have to try to remember the passwords.

[00:04:02] And so how does, how does the password manager really work? Well, let's talk about it.

[00:04:10] So basically what a password manager does is it allows you to, to store all your passwords in an encrypted file.

[00:04:16] So you can add a new password to your password file.

[00:04:20] And what the password manager does is it encrypts your password file when it's stored on disk.

[00:04:25] So if somebody got a hold of your password file, they wouldn't be able to decrypt it.

[00:04:30] Ok. So, the question becomes, um, yes, I have a password file.

[00:04:34] It's got all my passwords in it and the password manager encrypts it.

[00:04:38] But what, what key does it use to encrypt it? Because anytime you use encryption, you have to have a key.

[00:04:45] And so what, what key, for example, AES key would your password manager use to encrypt your password file? So, it's kind of a recursive problem.

[00:04:54] You, you need a password to use your password manager essentially is the way it turns out.

[00:05:00] So with a password manager, you'll typically have um, a master password.

[00:05:06] So you only have one password that you really have to remember.

[00:05:09] And that is the password for your password manager.

[00:05:13] And so anytime you want to add or modify uh, passwords in your password manager, you have to type in the master password. Sometimes people call this a pass phrase.

[00:05:23] So just think of it as your password and this is one that you do need to remember probably through memorization and what they do, then the password manager would take your master password and pass it through what's called a key derivation function.

[00:05:40] So they will actually take whatever password you type in and they'll run it through an algorithm that converts your, your master password into an AES encryption key, for example.

Start visual description. The professor explains the key derivation function used by password managers. He shows an algorithm on the screen that converts a master password

into an AES encryption key, highlighting the importance of remembering the master password. End visual description.

[00:05:52] And so they can derive from your password, your master password, an encryption key that they can then use to encrypt your password file and to decrypt it.

[00:06:01] So the security of a password manager is really based on your ability to remember your master password.

[00:06:07] And every time you use it yet, you know, you would pa you would type it in and then they'll turn your password into an encryption key and that allows them to encrypt and decrypt your passwords in a file.

[00:06:18] So that's, that's kind of how that works.

[00:06:20] So obviously, encryption is the key element of making a password manager work.