CS 240: Computer Security Overview Transcript

[00:00:00] In this series of videos we're going to talk about computer security.

Start visual description. The professor demonstrates the importance of computer security, emphasizing that anyone who creates software for real-world use needs to be conversant in it. End visual description.

[00:00:03] Computer security is a topic that anyone who creates software for real world use needs to be uh conversant in and have some knowledge about.

[00:00:14] And so we're going to try to at least cover some basics about computer security in these, in these videos.

[00:00:20] So just to provide an overview of, of why this is important, um as you certainly know, there's no shortage of people in the world that, that like to hack into computer systems and uh misuse them in some way and whether your application is connected to the internet, which most applications are anymore or not.

[00:00:42] There may be scenarios where people might want to try to break into your, your uh computer system or your, your software application and do things that they shouldn't be able to do.

[00:00:51] So one reason hackers might want to break into your computer system is to gain unauthorized access to data. So, we're all familiar with um situations where companies have data breaches and, and hackers break into their databases and, and access private customer information, things like that.

Start visual description. The professor explains how hackers might want to break into computer systems to gain unauthorized access to data, such as credit card information or social security numbers. End visual description.

[00:01:09] So that includes, you know, credit card information or uh social security numbers, all kinds of stuff like that.

[00:01:16] Um So the world is full of databases that people might want to try to break into the other scenario where people might want to try to access data.

[00:01:25] They shouldn't is as the data moves across a network or a computer network.

[00:01:29] So for example, the internet or the or the web, so people can, can gain access to the connections that make up the internet.

Start visual description. The professor discusses how hackers can capture data as it flows across a network, such as the internet, to gain unauthorized access. End visual description.

[00:01:38] If they can capture the data that as it flows across the network, then they might be able to, to break in and access that data as well.

[00:01:45] So there's, there's unauthorized data access.

[00:01:47] Uh Sometimes people just want to break into your computer system in general so that they can uh misuse your, your computer hardware uh somehow so that they maybe they want to break into your servers so that they can launch virus attacks on other computers from, from your system.

[00:02:02] So it makes it look like you're the one that's actually doing it.

[00:02:05] Uh They might want to disable your system, they want, might want to break in and, and uh mis figure or reconfigure your system so that it doesn't work anymore.

Start visual description. The professor describes various malicious activities hackers might engage in, such as disabling systems, reconfiguring them, or destroying data. End visual description.

[00:02:15] They might want to break in and actually destroy data rather than just access it.

[00:02:18] Maybe they just want to destroy it.

[00:02:20] So you can imagine a foreign government trying to break in um to a system and, and try to disable it or, or destroy it sometimes people just want to break into your, your system so that they can watch what you're doing so that they can spy on you and, and monitor uh what you're doing.

[00:02:35] And so for all these different kinds of reasons and probably many more, um we need to be security conscious when we create software so that we don't create vulnerabilities and create ways for people to easily break into a system and uh compromise it.

[00:02:51] Now, security, computer security is a vast subject. It's, you know, it's huge. And so, you could spend many courses talking about security. And so, we're just going to provide a brief introduction to some of the basics in this class, some of the basics that every programmer ought to be uh familiar with.

[00:03:09] But I would encourage you to learn as much as you can about security, uh educate yourself as much as you can so that as you design and build systems, you'll be able to create uh secure systems that aren't easy to break into.

[00:03:21] So our agenda for this discussion is, first of all, I want to introduce some basic concepts and terminology.

Start visual description. The professor outlines the agenda for the discussion, including basic concepts and terminology, and specific topics like HTTPS, secure storage of user passwords, and data security. End visual description.

[00:03:28] So that's probably what the bulk of this discussion will be about is there's some core foundational ideas that we need to discuss.

[00:03:34] And once we understand those ideas, we'll be ready to talk about some more specific topics that are of interest such as how does HTTP S work? How can we securely store user passwords how can we securely store data, things like that?

[00:03:47] So that's kind of an outline of what we're going to talk about.

[00:03:51] Now that when we build systems, we have a number of uh goals in mind and there's a lot of angles you can take on, on security and different flavors of security that you can think about.

[00:04:01] So the first important goal we have is data confidentiality.

[00:04:04] We don't want people to be able to access data that they shouldn't be able to see your access.

[00:04:10] And um so that, that's, that's the first thing.

[00:04:14] Another important topic is authentication.

[00:04:18] Whenever somebody tries to use a system, we need to authenticate who they are. We need to verify their identity.

Start visual description. The professor emphasizes the importance of authentication, explaining that it is crucial to verify the identity of users or systems trying to access a system. End visual description.

[00:04:25] So maybe we have a person that's trying to use our system or maybe we have another computer system that's trying to, to communicate or interact with our system.

[00:04:33] In either case, we need to be able to authenticate the identity of who is this person or who is this computer system that's trying to, to access our system to make sure that we know who they are.

[00:04:43] And once we know who they are, then we can decide um to what level they should be trusted and what things they should and shouldn't be allowed to do. So, authentication is AAA big important topic.

[00:04:55] Um Another uh important topic is data integrity.

[00:04:59] We want to verify that data has not been modified from its original form.

[00:05:04] So sometimes people, um a hacker, for example, might try to modify some data that's been um previously created.

[00:05:13] And it's, it's important that we have ways of verifying that that hasn't happened.

[00:05:18] So, when I access some data, I'd like to be able to verify that it's still in its original form and hasn't been tweaked or modified in some way.

[00:05:27] Another important topic is what's called nonrepudiation with non-repudiation.

[00:05:32] There's a couple of things we think about.

[00:05:34] One is we want to be able to verify the origin of data.

[00:05:38] So we already talked about verifying that the data itself has not changed.

[00:05:43] But I'd also like to be able to verify from whom did this data come? Who created this data? Who sent this data and be able to verify the au authorship of the data? Uh One example of that is just deciding if you can trust the data, uh depending on who it came from, you may or may not trust it.

[00:06:00] If it came from your bishop, maybe you would trust it.

[00:06:03] If it came from um some stranger on the street, you, you might not trust it.

[00:06:09] So verifying the origin of data is important.

[00:06:11] Another form of non-repudiation is um Cryptocurrency systems where we perform transactions, financial transactions in a online format.

[00:06:23] And in this case, it's important that we be able to create records of transactions that have been uh performed by people.

[00:06:32] And it's important that people not be able to repudiate or deny that they, they bought something.

[00:06:38] So if I spend some money, uh maybe Bitcoin and I, I purchase something.

[00:06:42] Uh it's very important that we have a way of uh proving that I actually did that so that I can't deny it.

[00:06:48] Um So any scenario where you might want to be able to prove that something happened in, in such a way that it can't be uh refuted is, is part of non-repudiation.

[00:06:59] So those are some important goals that we want to achieve in creating secure systems.

[00:07:06] Now, there are, as I said, some foundational concepts that we need to, to establish and, and learn first.

[00:07:13] And then based on these basic ideas, you'll see that a lot of computer security is, is based on these core ideas.

[00:07:21] And so um on this slide, you can see a list of the foundational concepts that, that we want to cover.

[00:07:26] And uh so we'll, we'll cover these in order.

[00:07:28] So first we have cryptographic hash functions, and we have data encryption.

[00:07:32] Uh then we have secure key exchange and after that, we'll talk about public key certificates and then finally, digital signatures.

[00:07:39] And so each of those is a very important topic that um you'll find in many or most systems that claim to be secure.