Hello, my name is Mustaque Ahamad. I'm a professor of computer science at Georgia Tech, and also a member of the Georgia Tech Institute for Information Security and Privacy. I've been at Georgia Tech for 30 years. And it's been a great journey. My research interests are in computer systems and system security. In addition to doing research and teaching, I served as Director of the Georgia Tech Information Security Center from 2004 to 2012. I also co-founded Pindrop Security that is commercializing our research that we did here in telephony security.

I'll be co-teaching this course with Professor Wenke Lee. Both of us have taught this course on our campus many times. We're delighted to bring this course to all of you in this new format. The course, Introduction to Information Security, provides a broad overview of the field of cyber security. Unlike our adversaries who just have to find one way to compromise our systems, we have to secure every aspect of these systems. I'll be starting with topics like software security, Operating system security, database security and so on. Once I'm done with part one, we're going to move on to part two with Professor Wenke Lee.

Hello. My name is Wenke Lee. I'm a professor of Computer Science at Georgia Tech. I'm also the co-director of the Georgia Tech Institute for Information Security and Privacy. My research interest are in systems and network security, applied cryptography, and data mining. I've also cofounded company called Amala. It commercializes our research in detection. I'll be covering the second half of this course. The topics will include cryptography, security protocols, network defenses, malware, web security, and mobile security.

Mustaque, I'm very excited about bringing this course to students. Absolutely, and by the time we are done, hopefully they'll have great understanding of the basic principles of cyber security, and walk over lots of practical techniques that help us all stay safe in our online world.

Security Mindset
Lesson Introduction

- Why is **cyber security** important?
- How do we **understand cyber security**?
- What needs to be done to **address cyber security**?

We're going to start this course by trying to understand why cyber security has become such a huge problem. We're going to do this by developing what we call a security mindset. Once we're done with that we're going to talk about a number of basic design principles that can help us better secure computer systems.

Why Cyber Security?

We worry about **security** when...

...we have **something of value** and there is a **risk it could be harmed**.

And obvious question is why worry about cyber security?

Actually, before we get into the cyber side of things, let's talk about when or why do we worry about security. We worry about securing something, or we worry about the security problem, wWhen we have something of value, but there also has to be a threat source that poses some kind of a risk to it. So clearly you worry about security when there's something of value, and you perceive that there's risk that is posed to that thing that is of value.

Why Cyber Security?

Individuals store a lot of sensitive data online

- if stolen, criminals can profit from it

Societies rely on the internet

nefarious parties could profit by controlling it

So let's get back to cyber security now. So let's ask those same questions:

- What is of value in the context of cyber security?
- And where do the threats come from?
- What kind of risk are we talking about?
- Who is the source of the threat?

In terms of what is of value, all of us store a lot of sensitive data. If criminals, if they get their hands onto this sensitive data that we're talking about, of course they can monetize it and

profit from it. And it is no exaggeration to say that societies actually rely on the internet for really important things. So these are again critical resources that we all rely on. Which could be attractive targets for our adversaries. In this case the reasons may be different from simply profiting from it.

Why Cyber Security?

Smart Grids rely on cyber systems

- whoever controls the grid controls the community infrastructure

Business and government proprietary information is often stored on the internet

- unauthorized access could be economically or politically disasterous

To look at sort of a quick example of what we just talked about. In particular our critical infrastructure.

People talk about smart grids, they're basically talking about the electric power generation, distribution, billing, all the different things that we do to make sure that we have electricity when we need it. If the computer is controlling the smart grid, whoever sort of takes control of those computers, is controlling a extremely important infrastructure on which the community relies. Obviously every business and government agency now use computers and networks to carry out what they're supposed to do their daily activities. But what happens if hackers, or adversaries, or unauthorized parties gain access to it? So it's an easy argument to make that cyber security is extremely important.

It seems like it is important, but is it important only for companies, or is it really important for every one of us?

Security Impact Quiz

Each of these organizations **suffered data breaches** of more than 30,000 records. Check the companies that **you have patronized**:

- ☐ Home Depot
- ☐ Facebook
- ☐ Ebay
- ☐ Apple
- ☐ JP Morgan Chase
- ☐ Snapchat
- ☐ Anthem
- ☐ Target
- ☐ Twitter
- ☐ UPS
- ☐ Mozilla
- ☐ Nintendo

So to make this point, we actually going to do a quick quiz.

These are companies that you and I patronize. And all of them actually, unfortunately, have suffered data breaches, which means data they have about their customers was stolen by somebody malicious.

So the quiz is really just asking you to check all the companies that you have done business with.

Instructor Notes - World's biggest data breaches

I do go to Home Depot, I actually have the credit card because I buy things that I need around the house. I have lot of iDevices and have done business with Apple. I held insurance at Georgia Tech, a BlueCross Blue Shield at parent company at this Anthem. I'm sure I have or some family member of mine has shopped at Target. I have shipped packages at UPS. So for me, it's at least five. I'm sure many of you have Facebook, Twitter accounts and things like that. So, it's not just the data that lives on our computers. But it's the data that lives on the computers of businesses that we patronize. And our data could actually be breached from those companies. And then we could become targets, or harm can come our way from malicious actors.

How do we understand the risk that is posed to the cyber assets that we have?

So this is going to require that we understand the risk to the online information, and the systems where it is who they can be accessed by.

Instructor Notes - Anonymous

So these kind of questions are exactly what we call developing a security mindset. A security mindset is really asking the kind of questions that I was just talking about. So if you say, well what exactly, how do you define a security mindset? You have to say:

- Well, who are the bad actors?
- What can possibly they exploit?
- What vulnerabilities do I have?

And if they are successful in exploiting a vulnerability, what is that attack going to be?

Cyber Assets at Risk

Threat source: who wants to do harm to us in our online lives

Cybercriminals: want to profit from our sensitive data for financial gain.

Hacktivists: activists who do not like something you are or something you do.

Nation-states: Countries do it for political advantage or for espionage.

So in the security mindset, the first thing we worry about is "what is the threat source?"

In particular, who is the entity that wants to do us harm? So, there are obviously these criminals who are in it for the money, professional criminals who want to profit from the data that they can steal.

There's another sort of threat source people worry about. These are activists who use the Internet, in particular, hacking. That's why they're called hacktivists, and they have some sort of an agenda. People may agree with it, or may not agree with it. When you sort of think about Snowden, well he had an agenda. He didn't like certain things that the US government was doing, and that was the reason for him. It wasn't that he was trying to profit from the information that he took, but the reason really was activism.

Finally, threats can come from nation-states. And countries are actually doing this, they're doing it for political advantage, they're doing it for spying on each other.

So the risk comes from sort of the threat source, sort of the entire spectrum, from a set of group of criminals all the way to nation-states. So the threats are clearly very real.

Vulnerabilities and Attacks

- **threat actors** exploit vulnerabilities to launch attacks
- **attacks** lead to compromises or security breaches
- **vulnerabilities** can be found in software, networks, and humans.

We said old threats exist, what about vulnerabilities? So vulnerabilities could be of many kind.

For example, if you use a weak password, that is a vulnerability. Someone can guess that password and then be able to use that to launch an attack which in this case would be taking control of your account.

If they are able to take control of your account, well, that is a compromise of your account. If able to do it more broadly to a system, that's a security breech. So an attack is a successful

exploitation of vulnerability by a threat source, resulting in this system that has been compromised.

Unfortunately whatever it is, are very hard to get rid of completely. And they can be found in software that runs on our computer systems, networks, and lot of times the biggest source of vulnerability people say humans are the weak link. We do things that actually introduced vulnerability into the systems. So the security mindset starts with threats, then we have to talk with vulnerabilities, and exploitation of those [vulnerabilities] will lead to attacks, and attacks result in compromise and security breaches.

We're going to use a really simple example - You can call it a trivial example. To illustrate this idea of a vulnerability an attack.

So many of us ride our bikes. And, of course it's an important asset to us. It costs money to get one, it gets you around, so obviously, it's useful to you, so, it's the valuable asset. There are threats against it, people steal bikes. Let's think about, if we just leave it anywhere, obviously, there's a serious vulnerabilities in it. The thief can walk and take the bike away.

So what we normally do, is we lock it. So as you see in this graphic, this person who is security conscious actually has locked the bike. And they've gone off to class, or to work, or whatever it is, and you look at the system and you say well, are there any vulnerabilities?

Vulnerabilities, some we may actually know about, others many not even know about it. It's the threat actor who actually discovers it. And in cyber security we call them zero day. The thief actually is not going to fight the security that you have in place here, which is the lock.

And certainly what it is going to do is, it is going to walk away with the bike minus the wheel. So vulnerability here was that this asset that we have here the bike. Of course the people have to buy a new wheel. But what he or she is able to walk away with is actually still fairly valuable, isn't it? It's most of the bike, add a wheel and you have a functioning bike. So the vulnerability we never thought was that we had to secure more than just the wheel, okay. The lock that we put is actually only protecting the wheel. It's not protecting the entire bike. That's the example of vulnerability.

One of the better-known breaches, cyber attacks, that occurred towards the end of 2013 was the Target store breach.

So in this case, you would want to ask this question, what is of value that somebody was after? And if somebody was after, who was that? What is the threat source? Then we can say, well, what vulnerability did they exploit?

So the Target case, essentially what they were after was credit card data that is there on the point-of-sale systems that are in Target stores. The people who are after it are cyber criminals because they want to profit from the stolen information. And the vulnerability they exploited is an interesting one. So, Target stores had an HVAC contractor. The hack actually began with a phishing message to an employee of that HVAC company. Through that phishing attacks, they were able to get credentials that gave the cyber criminals access to Target's network. And once they were on Target's networks, then they were able to get to the point-of-sales systems where they installed malware to siphon off the credit card numbers. So this is a real-world example where the security mindset, essentially we are saying, where does the threat come from? Cyber criminals. What are they after? Credit card data. What vulnerability was there in the system that was exploited? Well, we just talked about it.

Black Market Prices Quiz

What is your **hacked/stolen data worth** on the Black Market (as of March 2015)? Enter **dollar amounts** in the boxes next to the data.

- ☐ **3 digit security code on your credit card**
- ☐ **Credit card information**
- ☐ **PayPal/Ebay account**
- ☐ **Health information**

So an obvious question is why are they doing it? What's in it for them? And I said what's in it for them is that they monetize the data. All right, this is like walking into a bank and stealing cash. They're able to do it online. So one way that this works is that you steal data, you sell it to somebody who's actually able to use it. So if you're going to sell it to somebody. What kind of price does it fetch you?

So we have a couple of examples:

- The security code that you have on your credit card.
- Credit card number or other information that is stored in magnetic strip.
- Paypal/eBay account.
- Some health information about you now that we have electronic medical records.

Think about how much would credit card information sell for? How much would an eBay account sell for? Then we'll come back and see what those numbers look like.

So the numbers that I'm going to give you here come from a report in the first quarter of 2015:

- The CVV or 3 digit code we have credit cards actually goes for $2, not very much.
- Credit card information, actually there's a range for it depending on what kind of credit card you have, so this could go anywhere from $5 to $45.
- A PayPal or Ebay account was going for $27.
- And health information could be obtained for $10 in the black market.

So the exact numbers are not as important as something that's striking. These values are not very high, well that's okay because they have millions of these. So if you take these values and you multiply the two, you can see that this could be an attractive thing for a criminal who's out to make some money.

Sony Pictures Quiz

With regards to the "The Interview" (2014) related hack, answer the following questions. Put the number of the correct answer in the box next to the question:

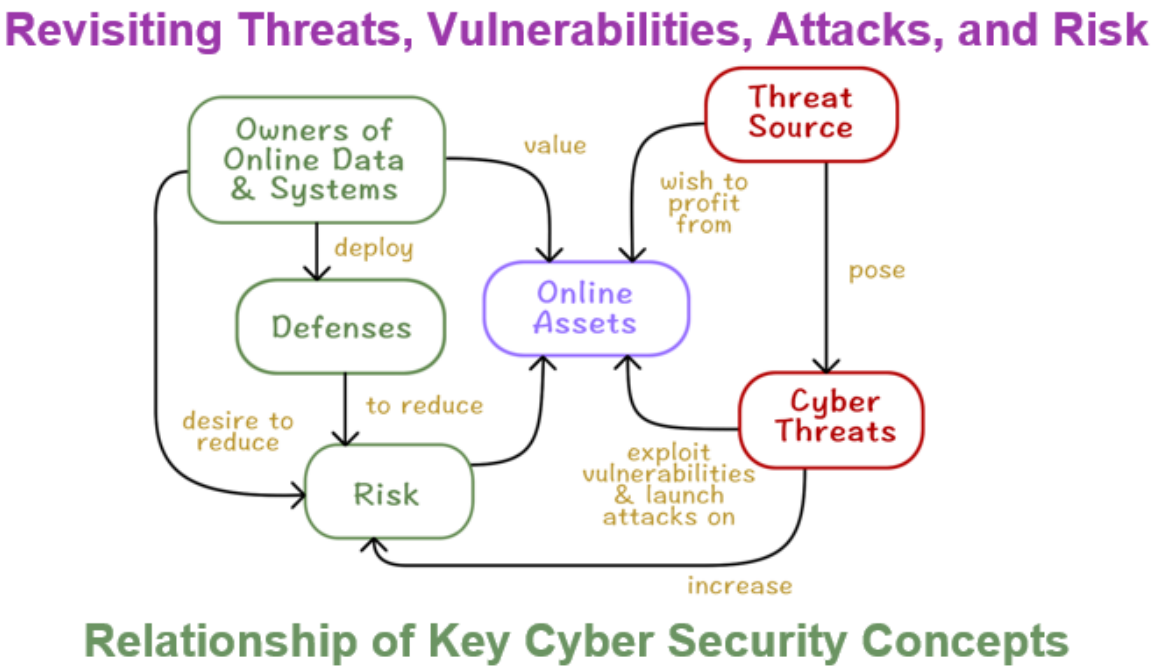
- **The threat source was:** ☐
  [1] cybercriminals, [2] Hacktivists, or [3] Nation-State
- **Goal of the attack was:** ☐
  [1] Monetize stolen information, [2] Stop Sony from releasing the movie "interview"), [3] Extort money from Sony
- **What did the attack accomplish:** ☐
  [1] Disclosed sensitive data, [2] Destroyed Sony computers

So we're going to talk about another big cyber security incident that happened in the later part of 2014, and it involved Sony Pictures. There was a movie called, The Interview, and it didn't show the North Korean leader in positive light. Just before the movie was going to be released, Sony Pictures' networks were hacked. We're going to use that incident to explore our security mindset that we're talking about. So the first question is, what was the threat source? What was the goal of the attack, and what happened as a result of the attack? Think about, again, why would someone want to do it, and what did they accomplish?

I should say that there was some debate that they're really North Korean government affiliated hackers who were responsible for this attack. So Nation-States [#3] would be the answer I would pick here. The goal of the attack was threaten Sony to stop it from releasing this movie [#2]. Sony did eventually release it, and the attack actually disclosed a lot of sensitive data [#1].

Instructor Notes

The Sony Pictures Hack Explained



Instructor Notes - Fig 1.1 in Computer Security Principles and Practice, Stallings & Brown.

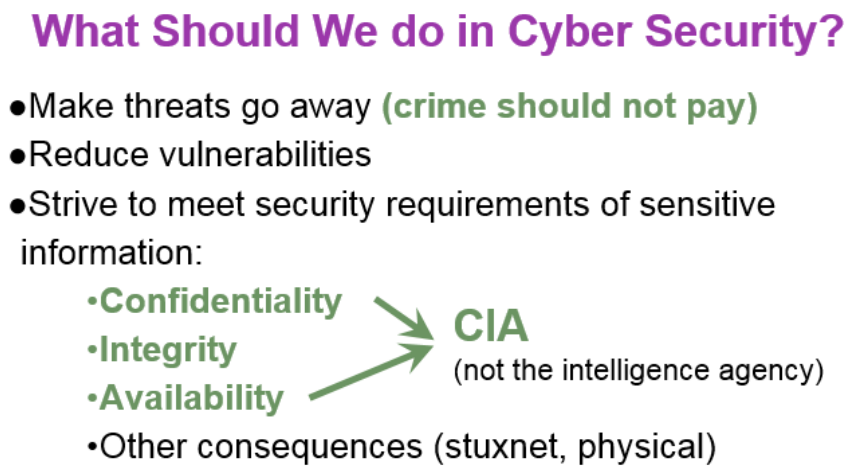
This picture that we have here actually puts a number of different concepts, in terms of how they're related to each other, so let's just sort of quickly look at it from two sides.

People who rely on computer systems and network systems, these are owners of the data that's stored, and the systems where the data is stored. They deploy those because those [systems and/or data] are critical towards what they do.

At the same time we know that there are threat sources and they're going to pose threats to the systems that we're talking about. But one way we deal with both the threat source and a vulnerability that we may have is deploying defenses. Owners obviously want to reduce this risk. And one way to do that is to deploy the defenses that we have in place. And the risk is to the online assets which are valued by the owners. That's sort of the picture on the legitimate owners and what they do in cyberspace.

In terms of the attackers, or the malicious actors, threat sources, they basically increase risk to these online assets that we have. And that happens because they exploit vulnerabilities and launch attacks. By doing that they wish to profit and that's the way they do it.

The big picture is sort of the center is what is of value, who poses a threat, and what do we do to somehow manage the risk that we have for our online assets from the threat sources. But the key concepts in cyber security, this diagram sort of nicely relates the idea of threats, vulnerabilities, attacks, cyber risk, and so on, and how they're all connected.



So, essentially, we're already saying that we need to do something about cyber security. So how can that be done?

Making them go away is not an easy thing obviously. One thing we can do is we can make sure that crime doesn't pay. We're actually going to talk about cyber laws. But making threats go away is nice idea, but it hasn't really been all that effective.

You can reduce vulnerabilities, but we're never going to have zero vulnerabilities. Complex systems, unfortunately, are always going to be error-prone, and some of those errors are going to be vulnerabilities that can be exploited.

The three things that you always talk about when you talk about securing or protecting access to information, is the data sensitive in the sense that it cannot be disclosed to unauthorized parties. Well that is really means the data has what we call a confidentiality requirement. You want to stop and prevent disclosure. It could be seen, but can only be seen by those who are authorized to see it.

Another requirement is what's called integrity, that's really means that no one should be able to corrupt it. So maybe not sensitive in the sense nobody should be able to see it if they are not authorized, but it could have integrity requirement. Only authorized people should be able to write it or modify it. No one else should be able to change it, and that is an integrity requirement.

The third requirement we have for data is what's called availability. The data is critical in the sense, what we use it for is critical, so if the data goes away in order to be able to do something that's really important to us. We can't access our online banking services because the server has been compromised, is down, or is a denial of service attack, or something like that.

So these are called the CIA, Confidentiality, Integrity, and Availability requirements for sensitive data. So here we're only talking about data which is sort of the cyber side.

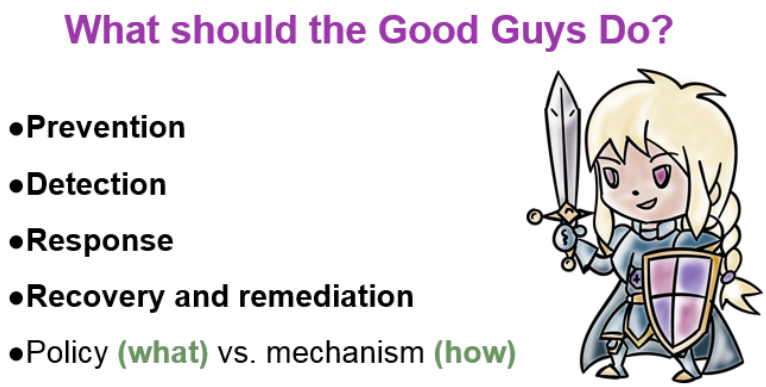
We should say that cyber attacks could also have physical consequences. So by successfully attacking the computers, we will be able to cause harm for their physical system. Most well-known case of this is the Stuxnet malware that infiltrated the Iranian nuclear plant network, and destroyed centrifuges, and so on. So, that's an example where it's not just this information

disclosure, or corruption, but there's actually a physical manifestation of a cyber attack. When we say what should we do? Well, we need to protect data and we need to protect systems.

So, this question said data breaches. Remember a data beach is one that exfiltrates large amounts of data that was sensitive and stored on some server.

So data breaches violate which of the following requirements, that we had for securing information or securing data? The CIA requirement, one was confidentiality, other was integrity, and then last one is availability.

Should data breach actually discloses data to someone who's not authorized that the hacker or whoever else, they're really breaching confidentiality of the data, because it gets disclosed to an unauthorized party.

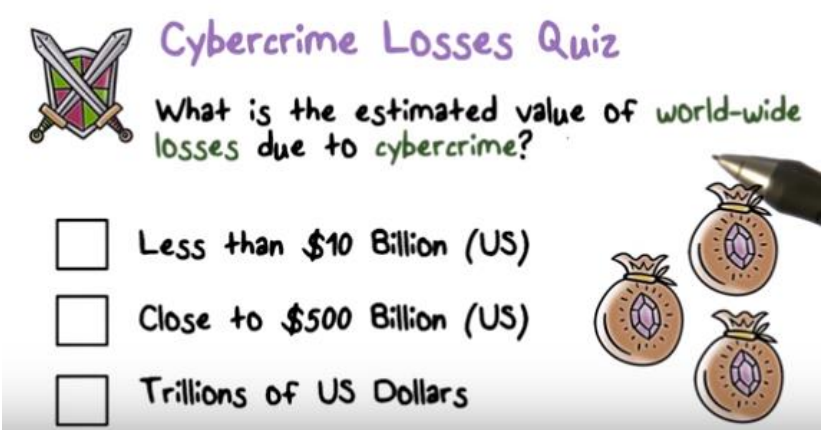


Talk about another perspective, in terms of what the good guys have to do.

- First of all, we have to worry about what we call prevention. Prevention really is keeping the bad guys out of our systems. The bad guys are the threat sources, they're going to try to attack our system. If we can keep them out, that is prevention.
- Unfortunately, prevention is not going to be 100%. If that happens, we want to detect the compromise as quickly as possible. People talk about advanced persistent threats, APTs that go undetected for a long time. That means we don't have good systems to detect that kind of malicious activity.
- Well, if we find out that they have breached our systems or compromised them, then we have to respond to that. So response comes next, and what do we need to do as part of the response? We need to recover from whatever that has happened. If data was corrupted, maybe we have to restore it and things like that.
- And then remediation basically has to be that the same attack should not happen again.

All these things is what good guys have to do so there are really two parts. Sort of, how do you do that? How do you do detection? How do you do remediation? And what exactly needs to be done? So mechanism is sort of the how part. You want to have a flexible set of mechanisms. So policy is always what is the way in which we're going to address something and what's done is through this whole spectrum.

Cyber security, again, you're not going to be 100% secure ever but that doesn't mean that we leave the door wide open, so that's what good guys have to do.



So what is the estimated value of world-wide losses due to cybercrime? These criminals could include potentially nation states. Think about all that is due to essentially criminal activity no matter where it comes from. So what is sort of the rough estimate of that? We look at the world-wide losses in the year 2014.

Instructor Notes - Losses Due to Cyber Crime

So this report actually has an estimate of losses. Worldwide it's close to $500 billion or half a trillion US Dollars. So I think the take away here is that this number is pretty significant. Cyber security is big business.

What is that we should be doing to address cyber security? How is the task of securing our system, it is going to be addressed by us? What are the things that are available to us?

So one way you can reduce vulnerability is by basically following some design principles that are good for security. And when they're more secure, there are fewer vulnerabilities, and less likely to be compromised.

The complexity is always the enemy. The well-established studies that show whether it's bugs or performance related things, or whatever it is. Those increase with the complexity or size of lines of code for example. So one way to reduce vulnerabilities is, what we call this economy of mechanism. Should be a small set of mechanisms that your system fundamentally relies on. So avoid complexity. Keep it simple keep it small. Chances are that you are going to have fewer vulnerabilities then.

Now the design principle is fail safe defaults. Fail safe defaults always say when somebody may or may not need access to some sensitive data you deny it. If they really need it at that point you can allow it. So default should be denied and fail safety fault is that the thing is protected. Access is controlled.

Complete mediation says your system should never allow someone to bypass that monitor. The monitor has to mediate before someone is able to gain access to the resource. The idea is that someone who's there to enforce that accesses are those allowed by policy you have in place then you can bypass it and that's the complete mediation requirement.

A lot of people don't believe that you can get security by obscurity. So if someone says well we are secure because no one knows how we do something. Well don't count on that. Perhaps somebody smart can reverse engineer and learn most of it. So Open Design is good because we're not counting on somebody in not finding out how we do things.

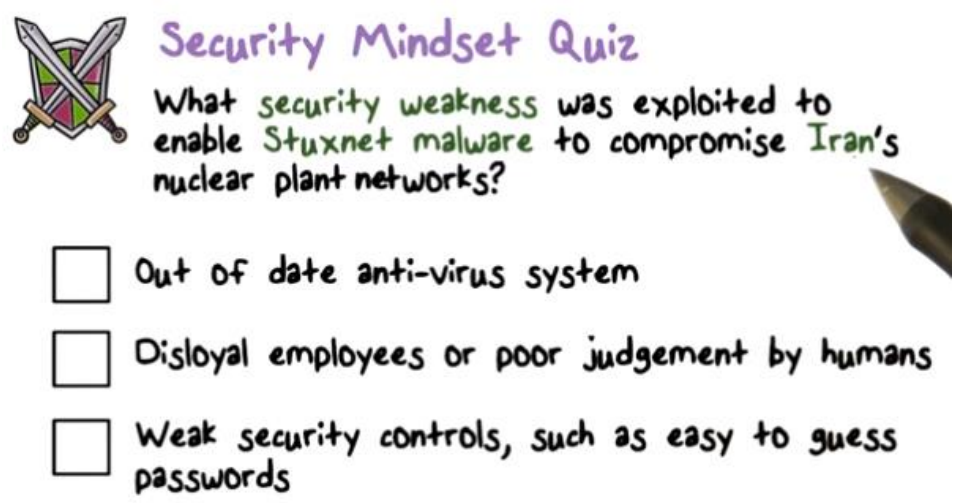
An extremely important design principle is what's called least privilege. So in systems at any time, essentially when you're running an application or a program, you have the privilege to be able to access a set of resources. Least privilege says you should only have privileges for resources that you absolutely need, and nothing more. It's a damage containment idea. If something were to go wrong, what you can harm is the set of resources for which you hold privileges.

We said people are the weak link when it comes to security. And that is because we perhaps expect people to do something and that doesn't come naturally to them. Psychological acceptability says don't ask people to do that doesn't put excessive burden on them.

So there are a number of these design principles. Actually they come from a classical paper called design principles for secure systems. You'll have a link to that paper. At least read the design principle section out of that paper. And for each of these principles we should understand how does it enhance or improve cyber security.

Instructor Notes

- Design Principles for Secure Systems
- Computer Security in the Real World
- Protection of Information in Computer Science



What security weakness was exploited for this malware to be able to compromise the computers that controlled the centrifuges and so on?

Instructor Notes

Stuxnet: How It Infects PLCs

Stuxnet, we're going to talk about when we talk of malware, exploited some zero day or vulnerabilities that were not known at the time. So the exploit zero day of course in every system is not going to help you. So it's not the first case. It's not easy to guess passwords, because you can't remotely access it you had to physically get into the plant. So it has to be the second option here. It was an isolated network, so the only way you can breach the air gap is through a humans helping you do that. So either its poor judgement by an employee or an employee who was a spy of somebody else. So you really had to breach the air gap to access the computers and that requires that people participated in this.

Instructor Notes

The Real Story of Stuxnet
Kobayashi Maru

Security Mindset
Lesson Summary

- **Cyber Security:**
  - HUGE problem for people, governments, companies, etc
  - Enhance the **level of assurance** of systems
- **Security mindset** requires we know:
  - **threats**
  - **actors/motivations**
  - how they **successfully attack**

The Security Mindset helps us understand why cyber security is such a big concern for governments, companies and people like you and me. We also discuss the design principles that help us deal with some of the threats that we face and the vulnerabilities that exist in our systems.