


Introduction and Security Trends: The Computer Security Problem

Slide 1



The image shows the cover of a book titled "Principles of Computer Security, Fifth Edition". The cover features a dark red header with the title in white. Below the header, the main title "Introduction and Security Trends" is displayed in large black font. Underneath the title is a square image of a person in a dark hoodie standing in front of a background of green digital code. Below the image, the subtitle "The Computer Security Problem" is written in a smaller black font. At the bottom of the cover, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

Howdy, in this video we're going to talk about the computer security problem.



Principles of Computer Security, Fifth Edition


The Computer Security Problem (1 of 2)

- Fifty years ago companies did not conduct business across the Internet.
- Today millions of people perform online transactions every day.
- Companies rely on the Internet to operate and conduct business.
- Vast amounts of money are transferred via networks, in the form of either bank transactions or simple credit card purchases.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Fifty years ago, companies did not conduct business across the internet because the internet didn't really exist 50 years ago. However, today millions of people use the internet to shop to conduct a business, and companies rely on the internet for their daily operations.

Lots of money is transferred over the internet either as bank transactions or credit card purchases or cryptocurrency and wherever there are vast amounts of money there are people and organizations who will try to take advantage of that and get some of it for themselves through various shady means. In 2019 the e-commerce market was valued at over 4 trillion dollars and it's growing at about 10 per year. So this is a lot of money out there on the internet and it's all secured by computers and computer security.




Principles of Computer Security, Fifth Edition

The Computer Security Problem (2 of 2)

- There are many different ways to attack computers and networks.
- Identity theft is so common today that most everyone knows somebody who's been a victim of such a crime, if they haven't been a victim themselves.
- There are many other types of cyber-criminal activity and all are on the rise.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

There are many different ways that you can attack computers and networks. One of the common attacks is identity theft where your personal information is obtained by an attacker and they can masquerade as you or they can sell it for others to masquerade as you and use for example your credit in order to take out loans and they get the money and you get the debt. It's a very common crime, pretty much everybody has either been a victim or they know someone who's been a victim. There are many other ways that cyber criminals operate. Pretty much every single cyber crime is increasing in prevalence.




Principles of Computer Security, Fifth Edition

Definition of Computer Security (1 of 2)

- **Computer security** is not a simple concept to define.
- If one is referring to a computer, then it can be considered secure when the computer does what it is supposed to do and only what it is supposed to do.
- However, the security emphasis has shifted from the computer to the information being processed.
- **Information security** is defined by the information being protected from unauthorized access or alteration and yet is available to authorized individuals when required.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

So what is computer security? Turns out that it's not so simple to define what computer security is anymore. With respect to just a computer we might consider that computer to be secure when it does all and only what it is supposed to do. However, with the advent of networks and the internet computers being connected to each other the thing that is even more valuable than the computer itself is what is in the computer: the data that is stored that is processed that is transmitted between computers. So rather than computer security we talk a lot more now about information security and we try to protect that information from unauthorized access from unauthorized alteration and make sure it's available when it's needed to be used. This refers to what's known as the CIA triad confidentiality integrity and availability as you learn more about security you're going to see these three concepts and a few others pop up quite often these are the big security goals keeping things confidential maintaining integrity and maintaining availability.



Principles of Computer Security, Fifth Edition


Definition of Computer Security (2 of 2)

- When one begins considering the aspects of information, it is important to realize that information is stored, transferred between machines, and processed, and all of these different states require appropriate protection schemes.
- **Information assurance** is a term used to describe not just the protection of information, but a means of knowing the level of protection that has been accomplished.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

So when we're thinking about information security there are three different places that we need to be thinking about securing information that's in storage in transit and in use so at rest in transit and in use. It is difficult to protect information while it is being used but advances are being made to keep information secure even while it's being used. Keeping things secure when they're at rest, when they're in storage, typically uses cryptography; keeping the information obscured so only certain authorized parties can access it. Same thing for being transferred between machines. Cryptography is the typical mechanism used so that anybody who sees the information while it's being transmitted can't read it.

When talking about information security you'll also hear the word information assurance; this refers to the level of security so information security and computer security uh talk about the things that we do to improve and maintain security. That is like what can I do to make my system more secure. Information assurance takes everything we've done to make the system secure and ask the question how secure is it? What's the level of protection that we can say that this system provides for the data and for the users?




Principles of Computer Security, Fifth Edition

Historical Security Incidents (1 of 3)

- Electronic crime can take a number of different forms, but the ones we will examine here fall into two basic categories:
 - Crimes in which the computer was the target
 - Incidents in which a computer was used to perpetrate the act (bank fraud)
- Virus activity existed prior to 1988, having started in the early 1980s.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Let's now take a look at some historical security incidents. We're going to do this so that we can better understand the threats and the security issues that computer and network systems deal with today. Electronic crime can take many different forms. The ones we look at here fall into either the category of the computer being the target or the computer was used to attack the target. You may have heard about viruses; viruses have been around prior to 1988 which was about the first time the world heard of viruses or worms, but prior to that time criminal activity was chiefly centered on getting access to computer systems. A lot of these were owned by the telephone companies so you could get free calls or things like that.




Principles of Computer Security, Fifth Edition

Historical Security Incidents (2 of 3)

- The Morris Worm (November 1988)
- Citibank and Vladimir Levin (June–October 1994)
- Kevin Mitnick (February 1995)
- Worcester Airport and “Jester” (March 1997)
- The Melissa Virus (March 1999)
- The Love Letter Virus (May 2000)

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

We're not going to talk about all of these you can read more about them in the textbook and online; they are really really cool. But I do want to talk about just one of them: The Morris worm. It's named after a person Robert Morris who at the time was a graduate student at Cornell and in 1988 he released what has been become known as the internet worm or the Morris Worm. It infected roughly ten percent of the machines that were connected to the internet at that time which was about six thousand, so there were maybe sixty thousand machines on the internet of which ten percent of them were affected by the Morris Worm. It had no malicious payload uh the program was obviously a work in progress. If I recall correctly he said that he was simply trying to count the number of systems on the internet. Seems reasonable when there's only 60,000 of them, not a big number, but unfortunately it had some bad behavior. It continually reinfected computer systems until they could no longer run programs its replication strategy was flawed and it failed to recognize when it had already infected the machine and then it swamped the hosts and pretty soon they were unable to do any more work.



Principles of Computer Security, Fifth Edition


Historical Security Incidents (3 of 3)

- The Code Red Worm (2001)
- The Slammer Worm (2003)
- Cyberwar? (2007)
- Operation Bot Roast (2007)
- Conficker (2008–2009)
- U.S. Electric Power Grid (2009)
- Fiber Cable Cut (2009)

Copyright © 2015 by McGraw-Hill Education. All rights reserved.

I also want to talk about the slammer worm. In 2003 this is early 2003 the slammer worm was released into the wild it exploited what's called a buffer overflow vulnerability and we'll learn more about that later. The particular buffer overflow exploited was in Microsoft's SQL server which is a database this vulnerability was not new; it had been discovered and a patch was released in the previous year in 2002, but that patch was not universally applied. Too many systems go unpatched, and this is a problem so within the first 24 hours of slammer's release the worm had infected at least 120 000 hosts and caused network outages and disruption of airline flights, elections, and ATMs at its peak slammer infected hosts were generating one terabyte of worm-related activity every second.

The worm doubled its number of infected hosts every eight seconds and it's estimated that it took less than 10 minutes to reach global proportions, and in fact 90% of the possible hosts it could infect. So, this thing spread really really fast, and it generated a lot of internet traffic, and it brought down a lot of systems. So, it did a lot of damage in a very short amount of time it was a wake-up call for the cyber community.



Principles of Computer Security, Fifth Edition


The Current Threat Environment (1 of 2)

- As time has gone on, more organized elements of cybercrime have entered the picture along with nation-states.
- From 2009 and beyond, the cyber threat landscape became considerably more dangerous, with new adversaries with various goals, including:
 - Deny the use of your computer systems
 - Use systems for financial gain including theft of intellectual property or financial information including personally identifiable information

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

So how do things look now? Well as time has gone on these attacks have become more sophisticated; there are organizations getting higher levels of sophistication, so not just hacker groups. You could think criminal organizations but also nation states so country level activity over the last 10 years the fiber the cyber threat landscape has become much more dangerous with many new adversaries some of them very powerful and they have various goals including simply denial of service so taking systems down uh or financial gain trying to steal intellectual property or personally identify information to sell or use for a quick profit but also you could think nation states might want to find out what other nation states are doing in terms of secret research. So these adversaries can have any number of goals when they go after computer systems.

So while in the past the threats were smaller and quite targeted and they were mostly a nuisance; nowadays, these threats can be very broad and they can do a lot of damage and they are way more than just a nuisance, they can really do some damage.



Principles of Computer Security, Fifth Edition


The Current Threat Environment (2 of 2)

- Advanced Persistent Threats (APTs)
- GhostNet (2009)
- Operation Aurora (2009)
- Stuxnet, Duqu, and Flame (2009–2012)
- Sony (2011)
- Saudi Aramco (Shamoon) (2012)
- Data Breaches (2013–present)
- Nation-State Hacking (2013–present)

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Again, there's a lot to talk about here I'm not going to talk about all of it but I'm going to mention a few things in particular APTs: advanced persistent threats. There's been numerous claims as to when APTs began and who first coined the term however it's important to note that APTs represent over the last 10 years or so. A new breed of attack pattern that the three words are important advanced refers to the use of advanced techniques such as spearfishing as a vector into the target persistent refers to the attacker's goal of establishing a long-term hidden position on a system.

Many APTs can go for years without being noticed and threats refer to the other objective exploitation. If an adversary invests the resources to achieve an APT attack they're doing it for some form of long-term advantage. APTs are not a specific type of attack but rather the new means by which highly resourced adversaries target systems, so nation states or organizations, as components of nation states or other possibly even corporations can comprise APTs and these APTs can attack systems with the goal of establishing long-term presence for future exploitation.




Principles of Computer Security, Fifth Edition

Summary

- Computer security – In general terms, the methods, techniques, and tools used to ensure that a computer system is secure, i.e. does all and only what it should do and information is kept available to authorized users and safe from unauthorized access and modification.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

So in summary what is computer security? In general terms computer security refers to the methods, techniques, and tools used to ensure that a computer system is secure that is that it does all and only what it should do and that information is kept confidential that it has integrity and is available.



Principles of Computer Security, Fifth Edition

Attribution

- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and I'll see you in the next video.


Introduction and Security Trends: Threats to Security

Slide 1



The image shows the cover of the book "Principles of Computer Security, Fifth Edition". The top part of the cover is a dark red banner with the title "Principles of Computer Security, Fifth Edition" in white serif font. Below this, the main title "Introduction and Security Trends" is written in a large, bold, black sans-serif font. Underneath the title is a square image of a person in a dark hoodie standing in front of a background of green digital code. Below the image, the subtitle "Threats to Security" is written in a smaller, grey sans-serif font. At the very bottom of the cover, there is a small line of text: "Copyright © 2018 by NoStarch-HEducation. All rights reserved."

Howdy! In this video we're going to talk about threats to security.




Principles of Computer Security, Fifth Edition

Threats to Security

- External versus Internal
- Level of Sophistication
 - “Script kiddies” to “elite hackers”
- Level of Organization
 - Unstructured to Highly Structured

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

There are a number of different ways that we can break down the various threats. One way is to categorize them by external versus internal. Another way is to look at the level of sophistication of the attack. A third way is to look at the level of organization of the various threats or attacks. All of these are valid approaches and, in fact, they overlap each other.



Principles of Computer Security, Fifth Edition

Intruders (1 of 3)


- The act of deliberately accessing computer systems and networks without authorization is generally referred to as **hacking**, with individuals who conduct this activity being referred to as **hackers**.
- The term **hacking** also applies to the act of exceeding one's authority in a system.
- Hacking does not live up to the Hollywood hype.
- Intruders are extremely patient.
 - Process takes persistence and determination

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The act of deliberately accessing computer systems or networks without authorization is generally referred to as hacking, and the individuals who do this are referred to as hackers. Hacking includes authorized users who attempt to gain access to files they aren't permitted to access or who attempt to obtain permissions that they have not been granted.

The term hacking can also apply to the act of exceeding one's authority in a system.

However, hacking does not live up to the Hollywood hype; real hackers are extremely patient as the process takes time and patience and determination. Usually the attacker will conduct many pre-attack activities in order to obtain the information needed to determine which attack will be most successful. Typically, by the time an attack is launched the attacker will have gathered enough information to be very confident that the attack will succeed.



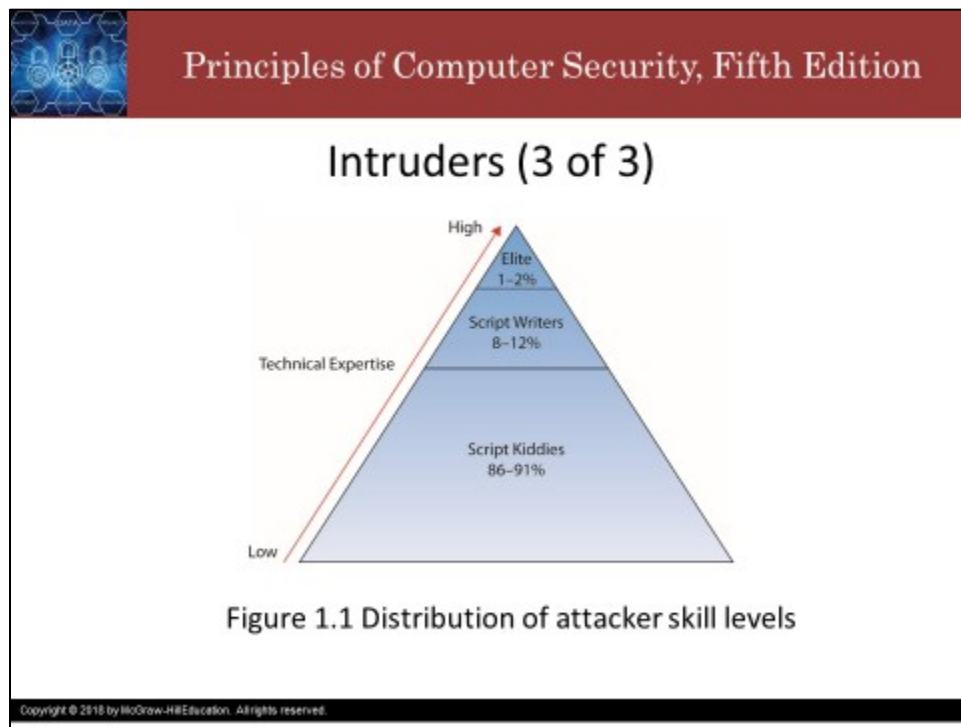
Principles of Computer Security, Fifth Edition

Intruders (2 of 3)


- Generally, attacks by an individual or even a small group of attackers fall into the **unstructured threat** category.
- Attacks at this level generally are conducted over short periods of time (lasting at most a few months), do not involve a large number of individuals, have little financial backing, and are accomplished by insiders or outsiders who do not seek collusion with insiders.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Generally, attacks by an individual or even a small group fall into the unstructured threat category; attacks at this level are generally conducted over a short period of time, usually not more than a few months, do not involve a large number of individuals, have little financial backing, and are accomplished either by insiders, or outsiders who do not have collusion with insiders.



Intruders definitely come in many different varieties and have varying degrees of sophistication. At the low end technically are what are referred to as script kitties: individuals who do not have the technical expertise to develop scripts or discover new vulnerabilities in software but who have just enough understanding of computer systems to be able to download and run scripts that others have developed. These individuals generally are not interested in attacking specific targets but instead simply want to find any organization that may not have patched the newly discovered vulnerability for which the script kitty has located a script to exploit the vulnerability. At the next level are those people who are capable of writing scripts to exploit known vulnerabilities; these individuals are much more technically competent than script kitties and account for an estimated 8 to 12 percent of malicious internet activity. At the top end of this spectrum are those highly technical individuals, often referred to as elite hackers, who not only have the ability to write scripts that exploit vulnerabilities, but also are capable of discovering new vulnerabilities. This group is the smallest of the lot, however, and is responsible for at most only about 1 to 2 percent of intrusive activity.




Principles of Computer Security, Fifth Edition

Insiders

- Insiders are more dangerous than outside intruders.
 - Insiders have the access and knowledge necessary to cause immediate damage to an organization.
 - Insiders frequently have knowledge of the security systems in place and are better able to avoid detection.
- Also, anyone with physical access.
 - Custodial crews, contractors, or partners

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Most security is designed to protect against outside intruders and thus lies at the boundary between the organization and the rest of the world. Insiders may actually already have all the access they need to perpetrate criminal activity such as fraud attacks by insiders are often the result of employees who have become disgruntled with their organization and are looking for ways to disrupt operations. It is also possible that an attack by an insider may be an accident and not intended as an attack at all. An example of this is the time in 1997 when a Pixar employee accidentally deleted 90 of Toy Story 2 from Pixar's servers. Another concern is anyone with physical access, including custodial crews, contractors, or other partners. An example of this would be Edward Snowden, who leaked highly classified information from the NSA in 2013 while he was a subcontractor.



Principles of Computer Security, Fifth Edition


Criminal Organizations

- Criminal activity on the Internet is basically no different from criminal activity in the physical world.
- One difference is the level of organization that criminal elements employ in their attack.
- Attacks by criminal organizations usually fall into the **structured threat** category.
 - Characterized by a greater amount of planning, a longer period of time to conduct the activity, more financial backing to accomplish it, and possibly corruption of, or collusion with, insiders

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

As businesses become increasingly reliant upon computer systems and networks and as the amount of financial transactions conducted via the internet increase, it is inevitable that criminal organizations would eventually turn up to the electronic world as a new target to exploit.

Fraud, extortion, theft, embezzlement, and forgery can all take place in an electronic environment. Criminal groups typically have more money to spend on accomplishing the criminal activity and are willing to spend extra time accomplishing the task provided the level of reward at the conclusion is great enough. With the tremendous amount of money that is exchanged via the internet on a daily basis the level of reward for a successful attack is high enough to interest criminal elements. These attacks typically fall into the structured category.



Principles of Computer Security, Fifth Edition


Nation-States, Terrorists, and Information Warfare (1 of 3)

- Many nations today have developed to some extent the capability to conduct **information warfare**.
 - Warfare conducted against the information and information processing equipment used by an adversary
- Information warfare falls into the **highly structured threat** category.
 - Characterized by a much longer period of preparation (years is not uncommon), tremendous financial backing, and a large and organized group of attackers.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

As nations have increasingly become dependent on computer systems and networks, the possibility that these essential elements of society might be targeted by organizations or nations determined to adversely affect another nation has become a reality.

Many nations today have developed some extent the capability to conduct information warfare, which is warfare conducted against the information and information processing equipment used by an adversary. This would fall into the highly structured threat category; these kinds of attacks typically take much longer to prepare. A number of years is not uncommon, they take lots of financial backing and they require many people to be involved. In practice, this is a much more complicated subject because information may not only be the target of an adversary, but also may be used as a weapon. The threat may include attempts not only to subvert insiders, but also to plant individuals inside of a potential target in advance of a planned attack.



Principles of Computer Security, Fifth Edition

Nation-States, Terrorists, and Information Warfare (2 of 3)

- An interesting aspect of information warfare is the list of possible targets available.
- Military forces are still a key target in information warfare.
- **Critical infrastructures** are those whose loss would have severe repercussions on the nation.
 - Water, electricity, oil and gas refineries and distribution, banking and finance, telecommunications
 - Dependent on computer systems

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

An interesting aspect of information warfare is the list of possible targets available.

You may have grown accustomed to the idea that during war, military forces will target opposing military forces but will generally attempt to destroy as little civilian infrastructure as possible; that is no longer true. Military forces are still the key target in information warfare, however, pretty much everything is on the table, including critical infrastructure, which includes things like water, electricity, oil and gas refineries and distribution, banking, finance, telecommunications. All of these are dependent on computer systems. With countries relying so heavily on these critical infrastructures, it is inevitable that they will be viewed as valid targets during conflict. Given how dependent these infrastructures are on computer systems and networks, it is also inevitable that these same computer systems and networks will be targeted for a cyber-attack in an information war.



Principles of Computer Security, Fifth Edition


Brand Names

- Energetic Bear
- Sandworm
- Shadow Brokers
- Equation Group
- Regin
- Cozy Bear and Fancy Bear
- Vault7
- Lazarus Group
- Comment Crew

Learn More: <https://attack.mitre.org/groups/>

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

In some cases, the names associated with attacks groups or techniques come from the computer security industry where the firm that first discovers them gives them a code name. Here are just a few that you may have heard of, and I'll point out just three of these and tell you a bit about them. First is the Sandworm Team, which is a destructive Russian threat group that has been attributed to the Russian Gru unit 74455 by the US Department of Justice and the UK National Cyber Security Center. Sandworm Team's most notable attacks include the 2015 and 2016 targeting of the Ukrainian electrical companies, and 2017's Nopecha attacks. Sandworm Team has been active since at least 2009. Vault 7 is a series of documents that Wikileaks published in 2017 that detail activities and capabilities of the United States Central Intelligence Agency to perform electronic surveillance and cyber warfare. The files include details on the agency's ability to compromise cars, smart TVs, web browsers, and the operating systems of most smartphones and computers. And finally Comment crew also known as PLA unit 61398, or Comment Panda, they are a military unit of the People's Liberation Army of China. They were one of the first advanced persistent threats to be identified publicly. They have the name apt-1 in certain attack group naming systems.




Principles of Computer Security, Fifth Edition

Summary

- Threats to security can be classified in several, overlapping ways:
 - Internal vs. External
 - Level of Sophistication
 - Level of Organization
- Information warfare is a highly structured threat that has a wide range of targets that includes critical infrastructure
- Some groups or attacks are notorious enough to have public code names

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

So in summary, we can categorize threats in several ways, either internal or external based, on their level of sophistication, and based on the level of organization of the group or the threat. Information warfare is a highly structured threat that has a wide range of targets that includes critical infrastructure, and some groups or attacks are notorious enough to have public code names associated with them, That's all for this video. Thank you for your attention and I'll see you next time.



Principles of Computer Security, Fifth Edition

Attribution

- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.


Introduction and Security Trends: Attributes of Actors

Slide 1



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. Below the header, the title "Introduction and Security Trends" is displayed in large black font. Underneath the title is a square image of a person in a dark hoodie with their hood up, set against a background of green digital code. Below the image, the subtitle "Attributes of Actors" is written in a smaller black font. At the bottom left of the slide, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

Howdy! In this video, we talk about differentiating threat actors based on their attributes.



Principles of Computer Security, Fifth Edition

Attributes of Actors

- **Internal:** have access to system
- **External:** need to gain access to system
- **Level of Skill/Sophistication**
 - As skill level goes up so does use of minimal methods
 - Surprising number of old attacks using old vulnerabilities
- **Resources/Funding:** criminal organizations and nation-states have big budgets, big teams
- **Intent/Motivation:** ranging from script kiddies to APT threat actors

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

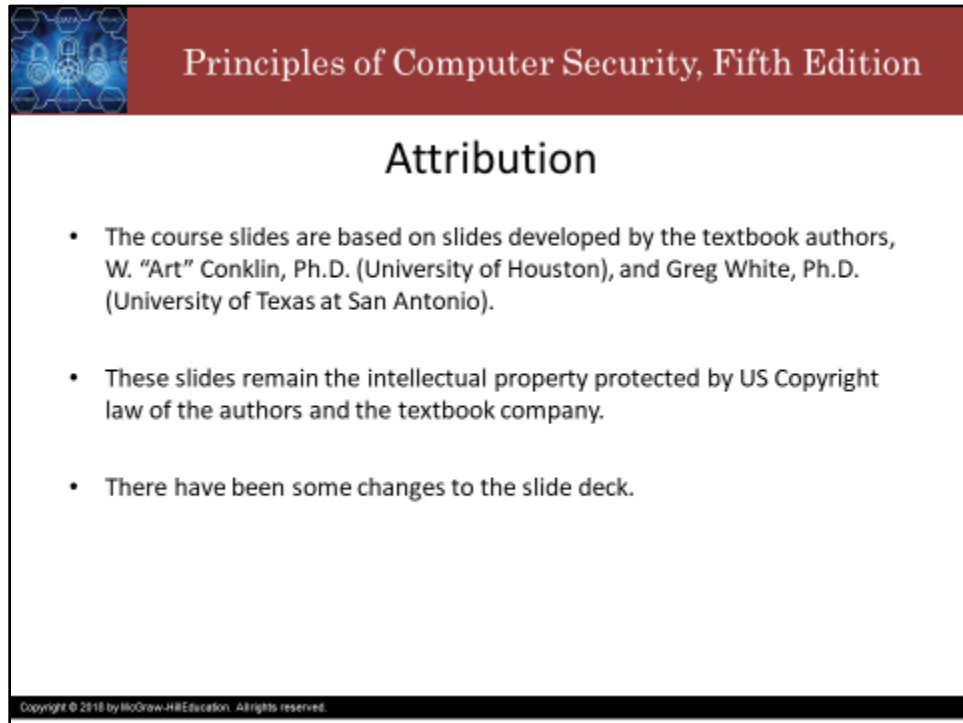
Threat actors can be divided into groups based on their location, level of skill, resources, and motivation. Internal actors have a key advantage over external actors' access to the system. Even if that access is limited, it still provides the opportunity to pursue an attack. External actors first have to gain access to the system before they can pursue the attack.

Actors may have varying levels of skill, ranging from script kitty to elite. When working in groups, there may be a mix of skill levels with more experienced individuals leading or directing less experienced individuals. The attacks themselves can also range in sophistication; an interesting note is that as the skill level of the attacker increases, the less likely it is they resort to highly sophisticated attacks. Instead, the most experienced, and therefore most skilled, attackers use the minimum amount of technical force required to achieve their goal. This follows the classic principle of security called economy of mechanism, or, you may know it as the kiss principle: keep things as simple as possible. Once a new weapon is revealed, countermeasures will be developed, and the attacker will eventually lose the advantage, so it makes sense to use the simplest methods, especially old attacks, against unpatched systems whenever possible in order to save the good stuff for when it really matters. But also, we must realize that attackers with sufficiently high levels of sophistication have the skills to remain undetected for some time.

It is possible that a system is attacked in such a way that the attack goes undetected, and therefore the methods employed are not discovered, and therefore countermeasures and patches are not developed or deployed. Actors also have different levels of access to resources and funding. The larger the attacking team and the longer the attack persists, the more expensive it is to maintain long-lived attacks (like those of APTs) typically have large technical and personnel budgets. But even lone-wolf hackers can be well resourced. Finally, actors can have different motivations for their attacks. Some actors are out

for fun; some are out for financial gain; some are out to wreak havoc and mayhem; some are out to make a statement often called hacktivism; some are out for several reasons that may change over time. Typically, the more skilled the actor, the more specific and focused their motivation. APTs have at least three goals; persistent access, stealth, and the acquisition of something valuable on the system like information or intellectual property. Basically, APTs don't spend all their time and money just to crash a system. Sophisticated attacks often have many phases and facets. A system crash may seem like an end, but it may only be part of a larger plan to achieve a more valuable objective. It is important to take a step back and try to see the whole picture, considering the different attributes of threat actors can help with understanding and responding to attacks.

Slide 3



The slide features a dark red header with a blue and white geometric pattern on the left. The title 'Principles of Computer Security, Fifth Edition' is centered in the header. Below the header, the word 'Attribution' is centered in a large, bold, black font. The main content area contains three bullet points. At the bottom of the slide, there is a small copyright notice.

Principles of Computer Security, Fifth Edition

Attribution

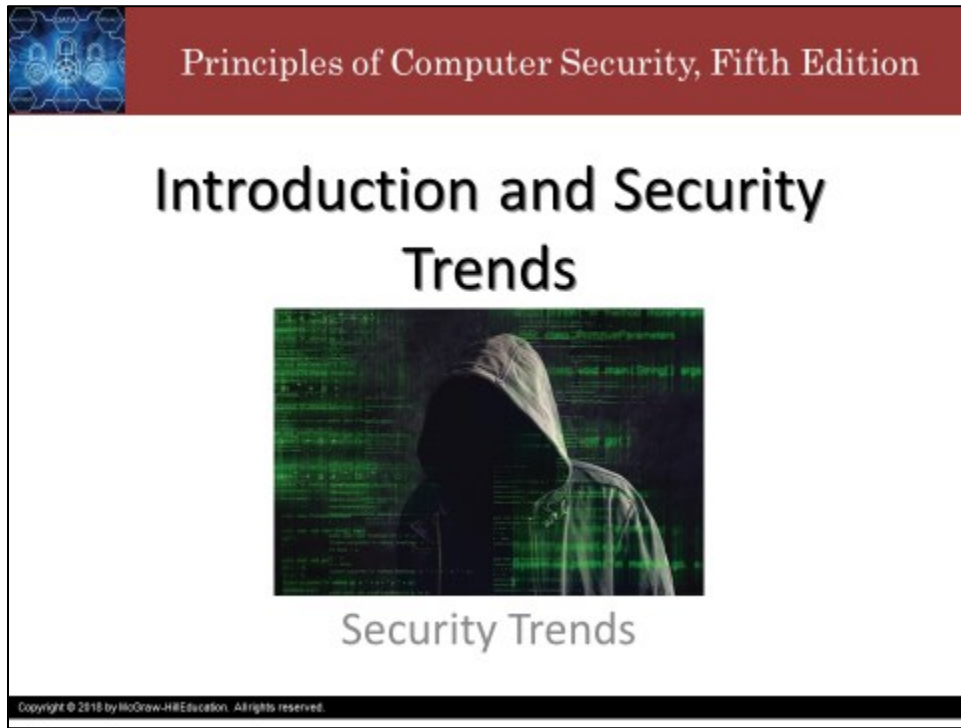
- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you for watching, take care.


Introduction and Security Trends: Security Trends

Slide 1



Principles of Computer Security, Fifth Edition


Introduction and Security Trends



Security Trends

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video we discuss some changes in the computer security landscape.




Principles of Computer Security, Fifth Edition

Security Trends

- Transformation from few large mainframes to many small systems
- Switch from closed operating environment to remote access
- Security is more complicated now

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The biggest change affecting computer security has been that the computing environment has transformed from large mainframes to a highly interconnected network of smaller systems. This interconnected network is what is called the internet. There is a switch from closed operating environments to one in which access to a computer can occur from almost anywhere on the planet. This has, for obvious reasons, greatly complicated the job of the security. Professional security is not a Boolean condition, where a system is either secure or it isn't. Absolute security is not practically feasible. Instead, practitioners focus on risk management and achieving enough security.



Principles of Computer Security, Fifth Edition

Security Trends

- Attackers more focused on gain over notoriety.
- Most attacks are financially motivated.
- Large number of targets, high reward, low risk

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The type of individual who attacks a computer system or network has also evolved. Today, computer attacks are used to steal and commit fraud and other crimes in the pursuit of monetary enrichment. Computer crimes are big business today, not just because it is hard to catch the perpetrators, but also because the number of targets is large, and the rewards greater than robbing a local store.



Principles of Computer Security, Fifth Edition

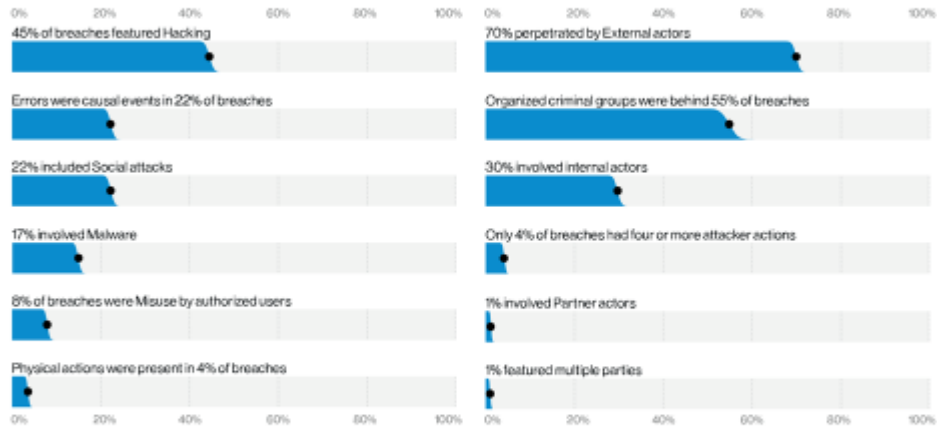



Figure 2. What tactics are utilized? (Actions)

Figure 3. Who's behind the breaches?

<https://enterprise.verizon.com/resources/reports/dbir/>

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Over the past several years, a wide range of computer industry firms have begun issuing annual security reports; among these firms is Verizon, which has issued its annual data breach investigations report DBIR since 2008. The 2020 DBIR was based on over 157 thousand security incidents, and 3009 confirmed data breaches in 81 countries. Perhaps the most valuable aspect of the DBIR is its identification of common details that result in a data breach. It's a very interesting report, and I highly encourage you to check it out when you get a chance.



Principles of Computer Security, Fifth Edition

Attribution

- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you, and take care.


Introduction and Security Trends: Targets and Attacks

Slide 1



The image shows the cover of a book titled "Principles of Computer Security, Fifth Edition". The cover features a dark red header with the title in white. Below the header, the main title "Introduction and Security Trends" is displayed in large black font. Underneath the title is a central image of a person in a dark hoodie standing in front of a background of green digital code. Below the image, the subtitle "The Computer Security Problem" is written in a smaller black font. At the bottom of the cover, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

Howdy, in this video we will discuss targeted attacks, targets of opportunity, and some steps to take to minimize attack surface.



Principles of Computer Security, Fifth Edition

Targets and Attacks

- Reasons why a particular system is attacked
 - Specific Target
 - Opportunistic Target

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

There are two general reasons a particular system is attacked:

- It is specifically targeted by the attacker, or
- It is an opportunistic target.



Principles of Computer Security, Fifth Edition

Specific Target

- Targeted Attack
- Attacker a *specific* reason for attacking
- Examples
 - Nation state interference
 - Hacktivism
 - Cyberterrorism
 - Electronic fraud

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

An attack on a specific target is called a targeted attack.

The attacker has chosen the target not because of the hardware or software the organization is running but for another reason, perhaps a political reason.

For example, an individual in one country attacking a government system in another, or the attacker targeting the organization as part of a **hacktivist** attack. For example, defacing a website because the attacker is politically, ethically, or otherwise opposed to the content or authorship of the website, or an attacker targeting critical infrastructure to cause economic damage, or for personal (possibly financial) gain.



Principles of Computer Security, Fifth Edition

Opportunistic Target

- Target of Opportunity
- Target is vulnerable to a specific exploit.
 - Any target will do.
- Might be targeting a specific type of organization
 - E.g. financial data, medical data, infrastructure
- Less difficult and faster than targeted attacks
 - “like catching fish in a barrel”

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

An attack against a target of opportunity is conducted against a system that has software that is vulnerable to a specific exploit.


The attackers are not targeting the organization. Rather, they know about a vulnerability and are simply looking for an organization with this vulnerability that they can exploit.

An attacker might be targeting a specific type of organization and looks for a target of opportunity that matches that profile.

For example, an attacker may want credit card or other personal information and will seek out any exploitable system which stores or processes that kind information in order to carry out the attack.

Targeted attacks are more difficult and take more time than attacks on a target of opportunity.

Attacks on targets of opportunity rely simply on the fact that any piece of widely distributed software will almost always be used by someone (or some organization) in an unsafe way, like improperly applying security patches, or applying them late, or worse, not patching at all.



Principles of Computer Security, Fifth Edition

Minimizing Possible Avenues of Attack

- Attack Surface
- A key element of defense: minimize the attack surface
 - Patch early, patch often
 - Malware loves unpatched systems
 - Harden. That. System.
 - Least Privilege – only use what is absolutely necessary
 - Economy of Mechanism – small and simple = fewer possibilities for vulnerabilities, easier maintenance
- Impossible to prevent or defend from all possible attacks
 - Security Is Risk Management.

Copyright © 2019 by McGraw-Hill Education. All rights reserved.

Understanding the steps an attacker will take enables you to limit the exposure of your system and minimize those avenues an attacker might possibly exploit.


The attack surface of a system is composed of all of the different points (also called attack vectors) that an attacker could use to attack the system.

There are multiple elements to a solid computer defense, but two of the key elements involve minimizing the attack surface.

The first step an administrator can take to reduce possible attacks is to ensure that all patches for the operating system and applications are installed. Many security problems that we read about, such as viruses and worms, exploit known vulnerabilities for which patches exist. The reason such malware caused so much damage in the past was that administrators did not take the appropriate actions to protect their systems.

The second step an administrator can take is system hardening, which involves limiting the services that are running on the system. Only using those services that are absolutely needed does two things: it limits the possible avenues of attack (those services with vulnerabilities that can be exploited), and it reduces the number of services the administrator has to worry about patching in the first place. This is one of the most important steps any administrator should take (and review periodically) to establish and maintain a secure computer system.

While there are no iron-clad defenses against attack, or guarantees that an attack won't be successful, you can take steps to reduce the risk of an attack. This is the basis for a change in strategy from "defend all the things" to one of risk management, which is more like "defend the important things the most."



Principles of Computer Security, Fifth Edition

Attribution

- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.

Introduction to Security Trends: Approaches to Computer Security

Slide 1



Principles of Computer Security, Fifth Edition

Introduction and Security Trends

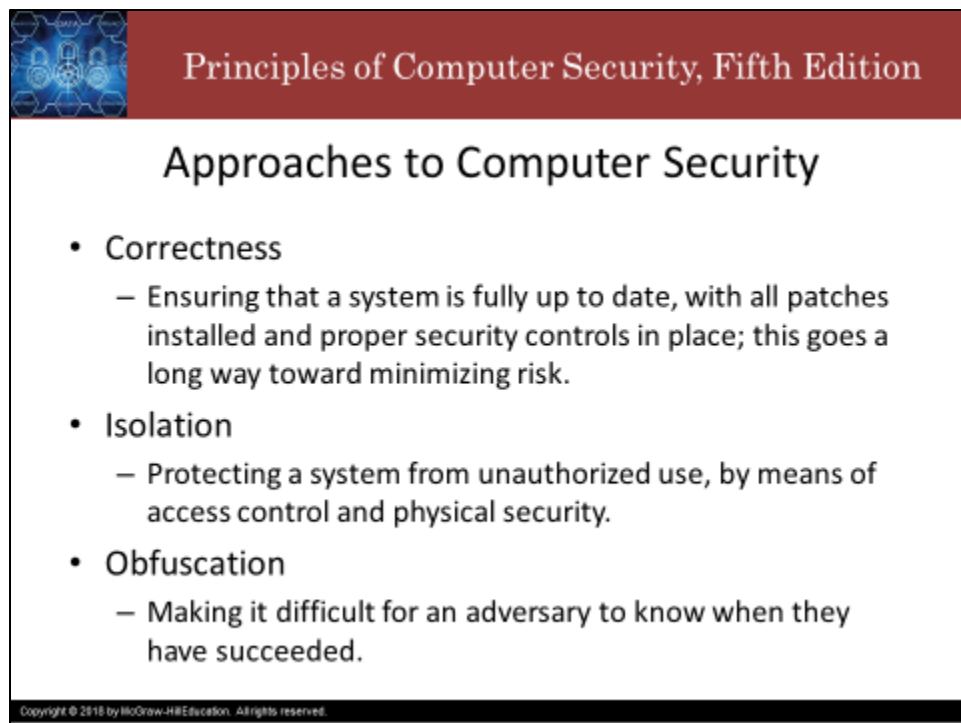


Approaches to Computer Security

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we will discuss some strategies for establishing and maintaining system security.

Slide 2



Principles of Computer Security, Fifth Edition

Approaches to Computer Security

- **Correctness**
 - Ensuring that a system is fully up to date, with all patches installed and proper security controls in place; this goes a long way toward minimizing risk.
- **Isolation**
 - Protecting a system from unauthorized use, by means of access control and physical security.
- **Obfuscation**
 - Making it difficult for an adversary to know when they have succeeded.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.


In addition to taking steps to defend against specific types of attacks, there are also more general means of securing systems. There are three important strategies to consider: correctness, isolation, and obfuscation. Supporting security through correctness demands consideration at all stages of system development and operation, including using a secure development life cycle, applying system hardening in patches, and employing sound security operation practices.

Cyber physical isolation of systems, and even of components within a system, is another powerful technique for securing systems. It's hard to attack something that you can't interact with. One may even argue that the only secure system is an unusable system, so by protecting systems from unauthorized access both physically and digitally, we make it hard for attacks to succeed. Isolation is part of several security principles, least privilege, least common mechanism, and economy of mechanism. Least privilege says to give users and processes the least privilege they need to do their job. Least common mechanism says that the components used to access resources should not be shared in order to mitigate the risk of information leaks and covert channels. And economy of mechanism says that components should be kept simple to reproduce both the complexity and the attack surface, and make defense and maintenance easier.

Isolation involves infrastructure access, control physical security, and even cryptography. You may have heard the mantra that security by obscurity is no security at all. What that means is that we shouldn't rely solely on secrecy for security; secrets will always be found out eventually. It does not mean that obfuscation is not worthwhile for security. On the contrary, we would expect that an obfuscated system would be harder to attack than a non-obfuscator system all other things being equal. Vis-a-vis the security posture one application of security with obscurity is the practice of obfuscating binary executables which includes, but is not limited to, encryption.

So a vulnerability in an obfuscated service is harder to find and exploit than the same vulnerability in the same but unobfuscated service. Whereas, correctness and isolation help to reduce the attacker's probability of success, obfuscation reduces the attacker's ability to recognize success given that many attacks consist of several steps, each a prerequisite for the ones that follow. Not being able to know when you've succeeded at each step leaves you in the dark as to how to progress the attack.

Obfuscation fits into several security principles, most prominently open design and work factor. Open design says that system security design should not depend on the design being kept a secret. Assume the adversary knows the system and base your security on things like cryptographic keys, process isolation, access control, etc. Work factor simply says that we should make the attacker's job as hard as possible. While each approach has its own inherent weaknesses, when applied together they provide a strong foundation of system security. This is part of a security principle called defense in depth. A successful attack must defeat many layers of security which makes attacks more difficult, less likely to succeed, and less likely to cause major damage, and therefore the risk of attack can be significantly reduced.



Principles of Computer Security, Fifth Edition

Approaches to Computer Security

- **Cyberattack Kill chain**
 - Step-by-step process that attacks follow to target and achieve results on victim systems
- **Threat Intelligence**
 - Actionable information about malicious actors and their tools
 - **ISACs** and **ISAOs**
- **Open Source Threat Intelligence**
 - Processes used to collect **threat intelligence** information

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

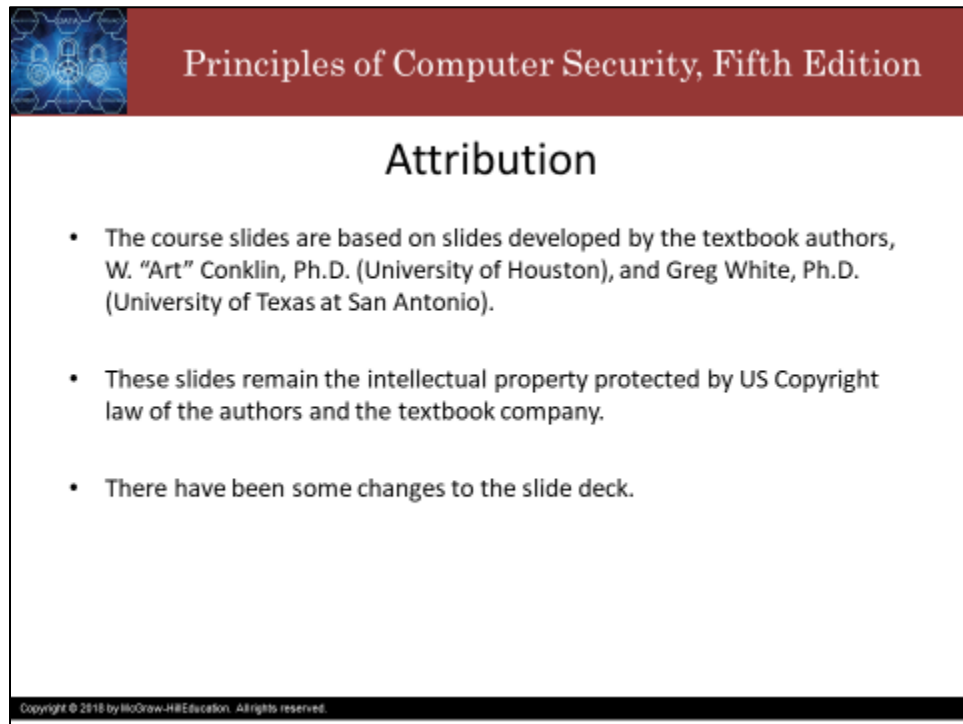
One modern method for modeling attacks is the cyber attack kill chain. The kill chain lays out the steps that attackers take to achieve their goal in attacking a system the idea is to detect and respond to attacks as early as possible and to break the attack before any, or any more, damage is done. This is part of a theme I hope you will find common throughout all of security theory and practice, which is the sooner the better, the earlier you take action the better for security. Security has to be taken into account from day zero, and must be designed, built in, and maintained throughout the life cycle of this system; an ounce of prevention is worth a pound of cure. Also sometimes a good defense requires a good offense. Some cyberkill chains include options for the defense to return fire and attack the attackers'.

Threat Intelligence is the actionable information about malicious actors and their tools, infrastructure, and methods. Several forms of threat intelligence are provided and used by organizations; the largest and most comprehensive are the information sharing and analysis centers, or ISACS, and information sharing and analysis organizations, or ISAOS, that are created and that are created to share information about attacks and attackers between the members of the center or organization. ISACS and ISAOS are typically big budget operations with cost and result sharing between members.

Another form of threat intelligence is open source intelligence, which is the gathering or thing or synthesis of threat intelligence from public sources; these sources can include anything from news articles to blogs government reports and even search engines and social networks. This is in contrast to unqualified threat intelligence which can include information from non-public sources like security consultants and ISACS and ISAOS. Threat intelligence is very important information because it is critical for risk management that resources be put where they can do the most good. The attacks which are the most likely should be the ones which get the most attention from the security team; also the attacks which might cause the most damage.

By sharing threat intelligence, organizations can help each other to respond more quickly and more effectively to a rapidly changing threat landscape.

Slide 4



The slide features a dark red header with the title "Principles of Computer Security, Fifth Edition" in white serif font. On the left side of the header is a small blue graphic with a network of nodes and lines. The main content area is white with the title "Attribution" in bold black font. Below the title is a bulleted list of three items. At the bottom of the slide is a thin black footer containing the copyright text.

Principles of Computer Security, Fifth Edition

Attribution

- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you, and take care.

Introduction and Security Trends: Ethics

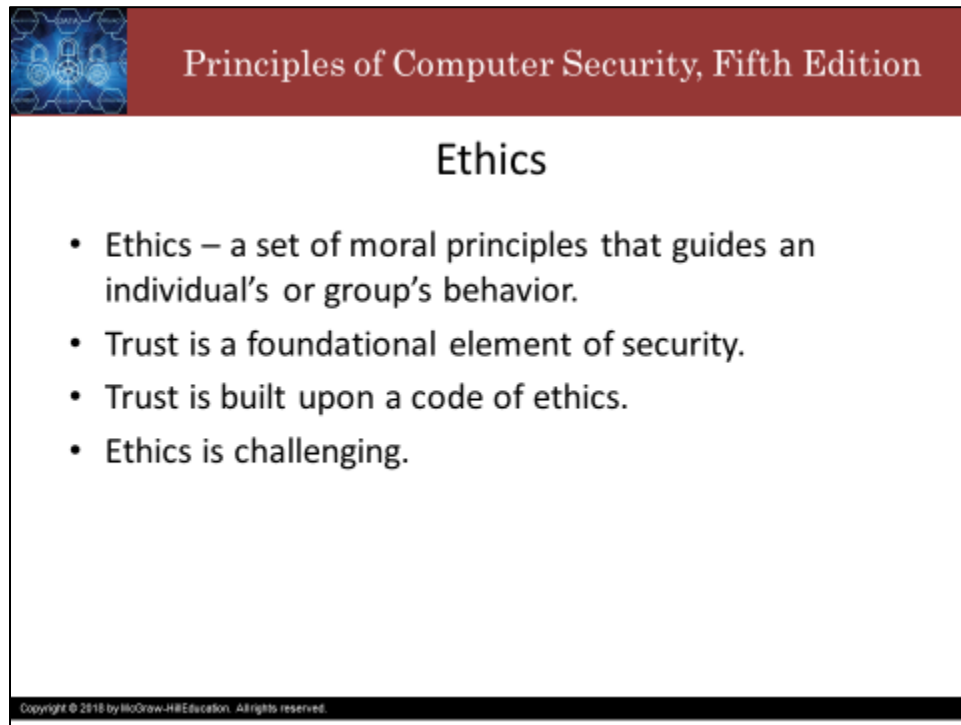
Slide 1



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. Below the header, the main title "Introduction and Security Trends" is displayed in a large, bold, black font. Underneath the title is a central image of a person in a dark hoodie standing in front of a background of green digital code. Below the image, the word "Ethics" is written in a large, black font. At the bottom left of the slide, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

Howdy! In this video, we introduce the topic of ethics. Ethics is a very important topic, and I want you to be thinking about ethics from the start. Ethics and security are inseparable in many ways, and not least because they must both be constantly considered throughout the life cycle of a system, from design through implementation and operation, and even after decommissioning. The importance of ethics in security cannot be understated; any meaningful discussion about operational aspects of information security must include the topic of ethics. There are several different ethical frameworks that can be applied to making a decision, and these are covered in another module dedicated to legal and ethical issues within the context of the practice of security.

Slide 2



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. To the left of the header is a small graphic of blue gears and a padlock. The main content area is white with the title "Ethics" centered at the top. Below the title is a bulleted list of four points. At the bottom of the slide, there is a small copyright notice.

Principles of Computer Security, Fifth Edition

Ethics


- Ethics – a set of moral principles that guides an individual's or group's behavior.
- Trust is a foundational element of security.
- Trust is built upon a code of ethics.
- Ethics is challenging.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Ethics means a set of principles of conduct governing an individual or a group. Most, if not all, professional organizations have a code of ethics that their members are expected to uphold; for example, the Certified Information Systems Security Professional certification or CISSP has a code of ethics that must be followed as a condition of certification. Violation of that code results in revocation of the certification, which might, in turn, mean losing your job, if not your entire career, as a security professional. Trust is very important in security.

People are also very important in security. Information security efforts frequently involve trusting people to keep secrets that could cause harm if revealed and to generally conduct their actions in order to safeguard the safety and welfare of society and the common good, but also to represent the high standards of the profession. Therefore, trust is founded in part on the codes of ethics to which practitioners and participants are expected to adhere. Ethics is a difficult topic. Separating right from wrong may be easy in many cases, but in other cases, can be quite difficult; for example, writing a virus that damages a system is clearly bad behavior but is writing a worm that goes out and patches systems even without the user's permission right or wrong? Does the end justify the means? Questions like these are the basis of ethical discussions that define the challenges faced by security personnel on a regular basis.

Slide 3



Principles of Computer Security, Fifth Edition

Attribution

- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you, and take care.