

13

Incident Preparation, Response, and Investigation

In this you will learn about two different subjects. The first is Access Control, or ensuring that users and devices only access the resources they are authorized to access. The chapter then moves to a discussion of how you should respond to security incidents which includes a discussion of forensics or investigating incidents to determine what occurred.

Objectives

At the end of this module, you will be able to:

1. Define Access Control.
2. Compare and contrast Mandatory Access Control and Discretionary Access Control.
3. Explain the steps in preparing for a cybersecurity incident.
4. Describe how to respond in an incident.
5. List the steps in an incident investigation.
6. List the steps in the forensics investigation process.
7. Create an incident response plan for your own computing device(s).
8. Configure Microsoft's User Access Control.
9. List the benefits and drawbacks of the various UAC settings.
10. Find and recover files and information that have been recycled or deleted.
11. Locate and read meta data in Microsoft Office files.

Section Content

One of the disappointing realities of cyber security is that even if you've done everything possible to protect your systems they can still be attacked, and data may be stolen. Attackers may take advantage of new vulnerabilities that haven't been patched yet, take advantage of your users, get in through one of your suppliers, or you may be attacked by one of the company's own employees. So, even though you don't think you'll be attacked part of information assurance is ensuring that have plans in place if an attack occurs, whether it's successful or not. This is especially important if an attack is successful as the costs can be significant if you don't know how to respond or respond improperly. This is like having fire drills with the people you live with. You don't want to plan on burning down your house, but you should practice how everyone will escape a fire if one does occur before one happens. If you wait until after the fire starts to figure out escape routes it may be too late, and people could be severely injured or die. In business there are lots of cases where an organization has been attacked and didn't know how to respond. The response includes the technical response to stop the attack and figure out what the attackers did, as well as communicating with employees, the public, the media, and law enforcement. In this section you'll be introduced to the planning and preparation that should occur, the steps that should be taken to respond if an attack is detected, and to computer forensics which is the process used to look for evidence about computer crimes.

You'll also learn about access control, which is based on the concept that there are typically different levels of authorization and access on any computer system. That is, there is typically an administrator account which can do anything, read or delete any file, manage users, etc., and normal or user accounts which will have permission to run certain programs or access certain files, but can't do everything like the admin account. Access control refers to the process of ensuring that non-admin accounts can only access the programs and data they need to do their jobs and that they can't elevate their level of privilege to gain access to any other programs or data.

Keep in mind that this is just an introduction and that there's lots more to learn about these subjects.

The Incident Response Plan

In this section you'll start to look at security from a business perspective, and incident response which includes the processes an organization should have in place just in case an attack does occur.

While no one plans to have a security incident, you should have a plan of what you're going to do if one occurs. You can think of it as being similar to planning for a fire in your home. No one wants to have a fire, but it's crucial to have a plan in case one occurs. You'll need to have an exit plan for every member of your family, and a safe place outside the house where you can meet. It's also important to practice your plan, to both find any kinks or problems in the plan, and to make sure that everyone knows and can carry out their parts during the heat of the moment. No pun intended. You might be able to imagine the confusion that would occur during a fire, and the importance of knowing what to do when every second counts. The time to figure out what to do is before an emergency occurs when you have time to calmly think through what steps should be taken. If you wait until a fire occurs, when a delay could be fatal, you don't have time to stop and think about the best course of action. With this in mind you should create a house fire plan for your family that includes exit routes for everyone to get out of the house and a place to meet up once everyone is outside and of danger.

Once you create a plan it's just as important to test it to ensure it's workable, you didn't leave anything out, and to test the plan to make sure everyone knows what to do and they can actually perform the steps. If you wait until there's a fire and you find flaws in the plan it will be too late to prevent problems. For example, by testing your plan you might find that it's not a

good idea to require grandpa Tony to jump out of the second-floor bathroom window and land in the swimming pool.¹

In the case of a business, everyone needs to know what to do if the company's computers are attacked. A good plan will allow the organization to respond both technically and from a legal/business perspective. For example, how does the company respond if an attacker is able to encrypt all of its data using ransomware. Or what should happen if you discover that an attacker has been able to penetrate the network and access sensitive customer information. You don't want to wait and try to figure out what you need to during a time of crisis, you want everyone to know what to do before the crisis occurs.

On the technical side you'll need to know how to first contain and stop an attack, and then how to restore normal business functions. For example, if it's a ransomware attack do you pay the ransom or not. Then how do you discover how the attack occurred so you can ensure the attackers won't be able to start the attack again after you've restored your operations. Or how do you proceed if you find an attacker has gained access to the data in one of your databases. Do you lock everything down immediately, which would alert the attacker that you know of the attack, or do you watch the attacker to see what they're doing? And what do you do if you decide to lock everything down but law enforcement asks you to let the attack continue so they can monitor the attacker's moves? Just like with a home fire, you'll need to know what to do immediately, and won't have time to start formulating plans or calling managers and lawyers to get opinions on the best way to proceed.

On the legal and business end the organization needs to know how to report the incident to law enforcement and how to work with them to gather evidence, how to report the incident to their customers, the press, and shareholders, and what steps they may be legally required to do

¹ https://www.youtube.com/watch?v=gO8N3L_aERg – Don't let Dwight from the Office plan your fire drills

to mitigate the problem(s) before resuming operations. These steps are more in the realm of Business and Law School, but if you have a career in cyber security you should be aware of the steps, especially if you work for smaller businesses. That is, if you work for a large business, they will have attorneys and business executives who should be responsible for this part of the planning. But if you work for a small company, they might be so focused on their product that they have no idea that they should be making these types of plans and you can help guide them through the planning process.

This type of plan is called an Incident Response Plan, and for a business or organization having and practicing an Incident Response Plan can be crucial to remaining in business. Missteps during an attack can cost precious time, and lead to additional costs and legal problems further down the road.

Luckily, plenty of companies have experienced cyber attacks and equipment failures, so there are plenty of examples to learn from. This obviously wasn't lucky for the companies that were attacked, but it was lucky for anyone who can learn from their mistakes and misfortune. In later classes you'll study cases involving different attacks and how companies responded in successful ways, as well as the less than successful responses that you want to avoid.

Forensics

Another subject covered in this chapter is forensics, or figuring out what is happening during an attack. This is critical as you need to know what happened to make sure you've actually stopped the attack, and to make sure it doesn't happen again.

Just like other forensics fields, digital forensics is the science of looking at evidence to determine exactly what occurred. At this point in time there are some fairly sophisticated digital forensics programs to assist you in making sense of the mountains of digital data. But these tools won't just pull up all the evidence you need with the touch of a button like in the movies or on TV. In some cases, where the attacker or criminal has technical skills, finding and

deciphering the evidence will require a solid knowledge of hardware, networking protocols, encryption, combined with some Sherlock Holmes level deduction skills.

To be a good forensics investigator you'll need to know where to look for evidence, how to decipher data, and how to get past anti-forensics techniques such as hiding files or using encryption that an attacker might use. You'll also need to learn how to find data in places that most people don't know even know exist. You'll get a small taste of this in the Hands-On exercises for this chapter.

If you find forensics interesting, you're also in luck as you can learn much more in my Digital Forensics class.

Access Control

This section should really be called preparing to not have an incident. And while you've already learned several important actions you should take to prevent an incident, such as installing patches and updates, this section introduces one more important action which is Access Control.

The book describes several methods of Access Control but doesn't do the best job at explaining what Access Control is, and what it does. To help ensure you understand what Access Control is we'll talk about it here, plus you'll have an exercise where configure and test different settings for Access Control in Windows. You'll also be doing a lot more with Access Control in your Windows and Linux Administration classes.

Ok ... so what is Access Control. The book definition of Access Control states that it is " ... the granting or denying approval to use specific resources". But what does this mean? Let's start out by defining the problem Access Control is meant to solve.

If you've only used your own personal computer Access Control probably won't make much sense because you're allowed to do anything to any file or connected device. You can create new files and folders anywhere you want, run any program you want, add and remove devices like printers or thumb drives, delete any files you want, you can even delete the entire system and reinstall if you want. But imagine that you become a system administrator or network administrator and you're now responsible for setting up systems that will have multiple users. Do you see where it would be a problem if every user on a shared device had the same rights as they did on their own personal computer? For example, say you have a file server that all your users can use to store and backup their files. Would it be an issue if every user could delete any of the files on the server? Or, say you get a job in the IT department at the college, and you're placed in charge of the computers in the Computer Science labs and it's your responsibility to ensure the computers are always ready for use by any student. Would you want anyone who uses those computers to be able to install or remove any software applications they wanted at any time?

So, the various Access Control methods are meant to provide a way to control what users can do on a system. This is done not only to ensure data is secure, but also to prevent users from messing things up or breaking things.

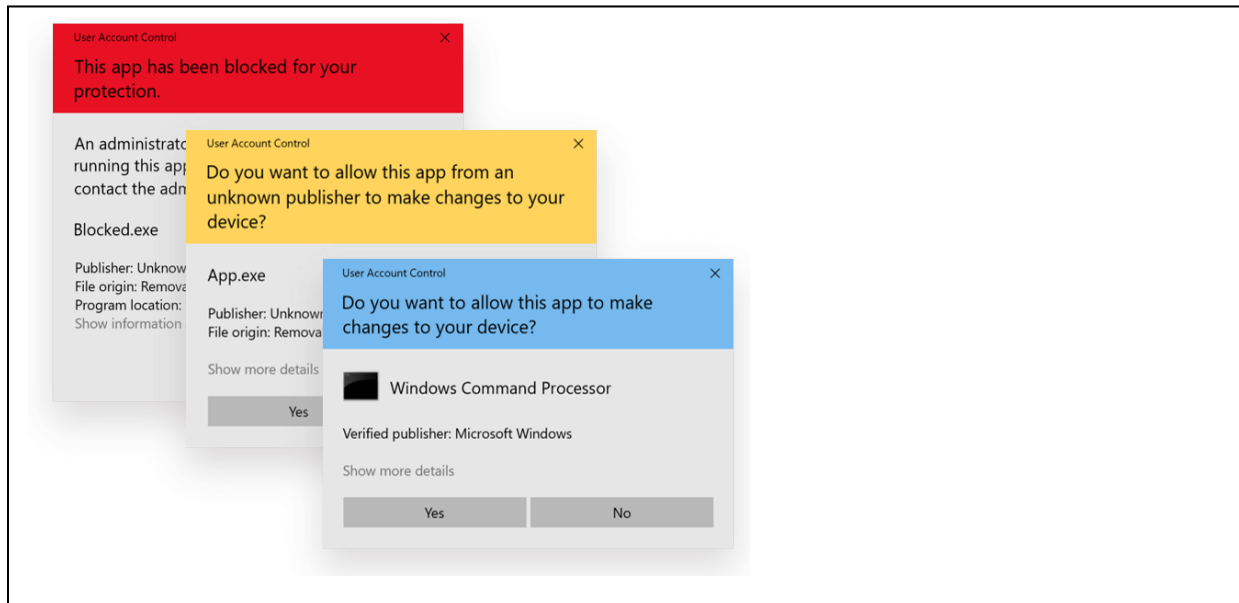
When you learn about Access Control models, most of the permissions or restrictions are fairly straightforward, and should be easy to understand. For example, a user may be given permission to access certain files or run specific programs, but denied permission to read other files or do things like create new user accounts. If you become a system administrator you'll spend some time learning how to grant permissions to individuals and groups.

There are also a few permissions that are not so straightforward, but will make sense with a little explanation. These are the permissions or restrictions that are not placed on a user, but those that are placed on programs that a user might run. If you have a smart phone you'll be able to relate to this, as you see this every time you install a new app and the phone OS asks if

you want to give the new app permission to access your cameras, or phone book, or data, etc. In this case, you have permission to install apps, but those apps won't have any permission unless you authorize them first.

You also may know that with Android phones and iPhones, you the owner, don't have administrative privileges. The Access Control model on the phones gives you some permissions, but not all permissions like Windows. You can gain administrative privileges on your phone by jailbreaking or rooting the phone, but this opens your phone up to some new security issues.

With Windows, even on single user systems like your home system, there is a concern that an application you run may contain malware that will try to do something you're not aware of. This is why Microsoft developed the User Account Control (UAC) model, where you can have Windows ask you for permission before certain actions such as installing a new application are performed. You may have experienced this already when you start to install a new program and Windows asks if you want to let the install program makes changes to your system. While you might have seen this before, it's easy to miss what's happening if you're not aware of what Access Control is and how Windows is trying to protect your system. In any case, one of the Hands-On Projects will walk you through configuring and testing UAC.



While the UAC messages might seem annoying, they can save you from situations like when an attacker adds code to their website that will download malware on the computer of anyone that visits the site. That is, you think you're just using your web browser and surfing the Internet, but when you load a page from the attacker's website it tries to sneak some malware onto your computer. If you're running UAC at the correct level, you'll get the message that something is trying to change your device, which is a tip off that something shady is going on. If you're not running UAC the malware can be installed without you knowing that anything happened.

Access Control Models

Another way to think about Access Control and the Access Control models is to use the securing a physical building analogy again, and think of the difference between a hotel and your home. In this comparison the hotel uses a Mandatory Access Control model because almost everything in a hotel is locked by default. The guest rooms are locked, the recreation and pool area is behind a locked door, most of the exterior doors are locked, the business office is locked, etc. The only place non-paying visitors can access is the lobby which is "guarded" by the check-in

desk. If you're a guest at the hotel you'll be given a key that will provide you access to one room and the public areas like the pool, but it won't give you access to everything. This is much like the Mandatory Access Control model, where everything is locked by default, and if a user is given access, it's only to specific resources.

The Discretionary Access Control model is probably much more like what you use in your home. That is, everything is unlocked and available to anyone that you allow in the house. You might have a few locked items in your house, maybe a safe or gun safe, and maybe a few doors that can be locked for privacy purposes, like on the bathroom doors, but overall everything in the house can be accessed by anyone in the house.

Applying What You've Learned to Your Home System(s)

There are a few things you can take from this chapter and apply to your life and your devices. The first is that you should have a plan for home emergencies. The main one we all should have is a plan for a home fire, but there may be others depending on your situation and circumstances. That is, there is some statistical chance of home fire, but you may also want to plan for other emergencies like an earthquake, or flood, or tornado, depending on where you live. You might also want to have plans for medical emergencies if you have nut allergies or diabetes, etc. The other thing you want to do after developing a plan is to practice it a few times. The more you practice the easier it will be to perform the steps if an emergency actually does occur, plus practicing will expose any weaknesses or flaws in your plan. And it's important to identify any problems with the plan before an emergency actually strikes, at which point it will be too late to make any changes.

As far as applying the lessons from this chapter to your tech devices, the one thing you can do is check your access control. If you have a Windows computer, you can set (or disable) UAC. I strongly urge you to set it, so you'll know anytime important changes are being made to your system. And, if you have a smart phone, you can check the permissions you're giving away to your applications and ensure that the permissions you're allowing are all necessary.

The other item in this section that may apply to your personal life is regarding computer forensics. One of the big things you should takeaway is that you shouldn't do computer crimes. I hope you don't need me to tell you to not be a criminal. But if you do anything naughty with your computer, you need to be aware that you're leaving digital evidence all over the place and a good forensic investigator can get your computer to give up all your secrets. You might think you're covering your tracks and deleting any evidence of your crimes, but the odds are very high that you're unknowingly leaving behind clues and evidence that can be used to discover what you've been doing.

Ways to Check Your Comprehension

The test over this chapter, Test 3, won't happen until after you finish all the remaining Modules. If you want check your comprehension you can use the review questions at the end of the chapter or the Practice Test. I don't have the review questions loaded in Canvas, so you'll have to just read them and figure out your answers on your own. Or you could try and connect with some other students in the class and drill each other using these questions.

If you want to use the Practice Test, look in the Test 3 Module in Canvas for the link to a Practice Test 3. You can take the Practice Test as few or as many times as you want. You're not required to take the practice test, but it's also a good way to check your comprehension and prepare for the "real" test.

The Activities for This Section

There are four activities for this section, Hands-On Projects 13-1, 13-2 and 13-4, and a Case Project (writing assignment). Hands-On Projects 13-2 and 13-3 have been designed to provide you with a taste of computer forensics, and provide experience finding data that most users

don't know exists, while 13-4 provides you experience with Microsoft's User Account Control (UAC) which is a part of the Access Control process used by Windows.

1. Hands-On Project 13-1: Entering and Viewing Metadata

The purpose of this assignment is to demonstrate one of the places that a forensics specialist can look for "hidden" information that may serve as evidence in an investigation. In this case you'll be looking for information associated with Microsoft Word, or any Microsoft Office documents, that isn't displayed directly in the document itself. This information isn't exactly hidden from a technical perspective, but most users don't know it exists and it's been used to solve many actual criminal cases including the capture of the infamous BTK killer in 2005².

Microsoft occasionally changes the Word interface, so if you're using an older or newer edition/version of Word you may have to look around a little bit to find the meta information. Once again, if you needed to do this for your job your employer would expect you to be able to problem solve and find where it's stored, so if you are using a different version than the book this will be good practice for you. If you can't use the Internet to find the meta data in your version of Word you can check below where I've added the steps for finding the meta data in Word 2019, version 1808., or you can email me and ask for help.

What to submit for Project 13-1:

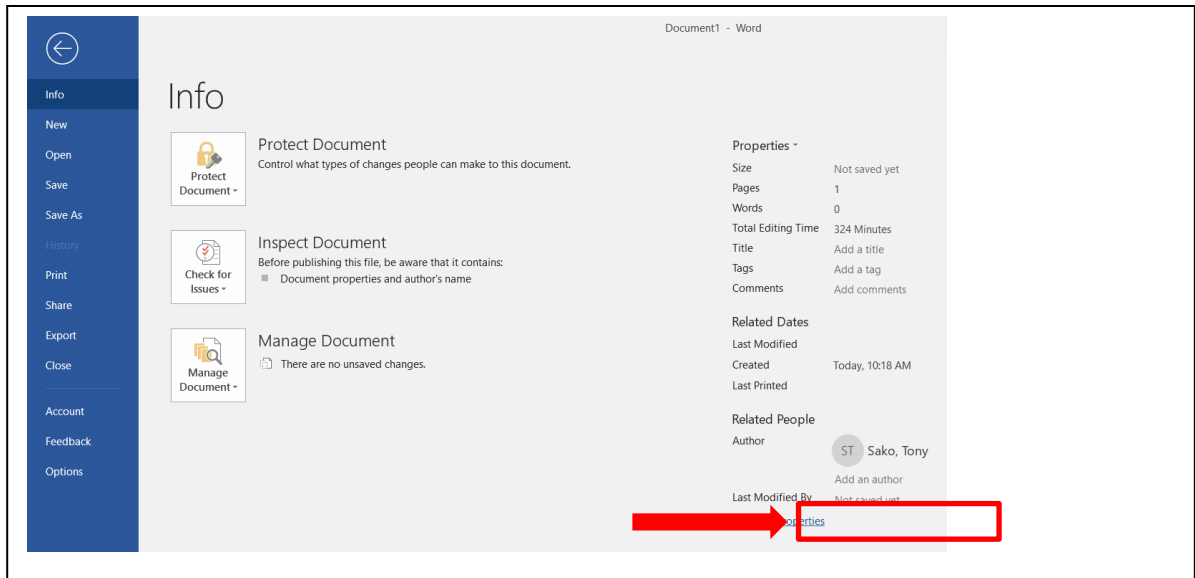
- Take a screen shot after steps 4, 14, and 20.
- Answer the questions in steps 9 and 21.

Locating Word Meta Data in Word 2019

To locate the meta data in Word 2019 do the following:

² <https://www.goodhousekeeping.com/life/entertainment/a28859869/btk-killer-dennis-rader/>

1. Select the **File** menu from the main Word menu, then select **Info**. You should see something similar to the following figure. You can see and edit some of the meta in the right column.



2. To see the advanced properties, or all of the meta data click the **Show All Properties** link at the bottom of the **Properties** column, which is the right-hand column.

3. This will display the entire list of meta data for this document. Some of the meta data items can be changed. To do this, simply click on data area. For example, to change the Title, click on the text that says **Add a title**.

The screenshot shows a 'Properties' panel with the following data:

Property	Value
Size	Not saved yet
Pages	1
Words	0
Total Editing Time	324 Minutes
Title	Add a title
Tags	Add a tag
Comments	Add comments
Template	Normal.dotm
Status	Add text
Categories	Add a category
Subject	Specify the subject
Hyperlink Base	Add text
Company	Columbia Basin College

Related Dates

Last Modified	
Created	Today, 10:18 AM
Last Printed	

Related People

Manager	Specify the manager
Author	ST Sako, Tony
	Add an author

Last Modified By: Not saved yet

[Show Fewer Properties](#)

2. Hands-On Project 13-2: Viewing Windows Slack and Hidden Data

Theoretically this assignment provides you with some forensics experience by displaying data hidden in file slack. This requires a basic understanding of what file slack is to be an effective exercise. If you don't know what file slack is you should watch the following video as it provides a brief explanation.

<https://tonysako.com/home/cs150-introduction-to-computer-security/cs150-explanation-of-slack-space/> - Slack space explanation.

I've also made two other videos to help you complete the exercise. There are a few steps in the book that don't tell you what you really need to do, and the main steps in the exercise don't

really show you what they say they show you. That is, they say you will see some data hidden in file slack, when in reality you're just looking at normal file data. To help you with this, I've made two other videos. You should watch both before starting the exercise, or as you go through the exercise yourself. Also note that there have been a couple changes since I created the video. When I originally made the video, we were using a different version of the book and the exercise had a different number. Also, the user interface for Directory Snoop has changed a little, but I think you should be able to adapt and figure out which buttons to press.

<https://tonysako.com/home/cs150-introduction-to-computer-security/cs150-using-directory-snoop-part-1/> - Using Directory Snoop Part 1

<https://tonysako.com/home/cs150-introduction-to-computer-security/cs150-using-directory-snoop-part-2/> - Using Directory Snoop Part 2

What to submit for Project 13-2:

- Take a screen shot after steps 7 and 19.
- Answer the questions in steps 8 and 19.

3. Hands-On Project 13-4: Exploring User Account Control

Note that I strongly suggest that you watch the following videos on UAC before doing 13-4. The videos will provide an explanation of what UAC is, how it should behave, and what the Group Policy editor is. The videos will also explain why UAC it won't work with Windows Home and what you should do if you have Windows Home on your computer. If you have the Home version of Windows you must use your cloud VM to complete the assignments, or one of the computers in the CBC Comp Science labs if they're available. Also note that if you use the VM in the CBC Cloud, UAC will not function as expected. If you're using the VM make sure and watch the last video for details on what you need to do to complete the assignment.

<https://tonysako.com/home/cs150-introduction-to-computer-security/cs150-microsoft-window-user-access-control-uac/> - An overview of UAC

<https://tonysako.com/home/cs150-introduction-to-computer-security/cs150-using-uac/> - Using UAC

<https://tonysako.com/home/cs150-introduction-to-computer-security/intro-to-computer-security-incident-prep-response-investigation-group-policy-editor-and-uac/> - Changing UAC settings with the Windows Group Policy editor.

<https://tonysako.com/home/cs150-introduction-to-computer-security/intro-to-computer-security-incident-prep-response-investigation-uac-on-the-vm/> - Completing the UAC Hands-On Project on the class VM

What to submit for Project 13-4:

Before submitting your Hands-On Projects, add all the information for all the assignments into a single document. Make sure that this document has the proper header information (your name, project number, date) and well as the project and step number for each item in the document.

If you are able to run this on your home computer, submit the following:

- Take a screen shot on step 7 before you click OK.
- Answer the question in step 12.
- Take a screen shot or upload the file in step 18

If you are unable to run this on your home computer and do this on the CBC VM, submit the following:

- Log in as Administrator
- Take a screen shot after step 2 where you set UAC to the highest level, before you click OK.

- Take a screen shot after step 26, before you click Apply or OK.

Note – the following steps are not in the book.

1. Ensure UAC is still set at the highest level
2. Log out as Administrator and login as a normal user.
3. Try to install some software. Any software program will do.
4. Create a screenshot of the UAC warning.

Case Project Homework (Writing Assignment)

Choose one of the following Case projects located at the end of chapter 13: 13-3 or 13-6.

Make sure and include the proper header with the required information, and any web sites that you use as references using the APA format. If you don't remember what's required you can refer to the Written Project Guidelines document for details on how your paper/report will be graded. You can find the document at:

<https://tonysako.com/writingprojectguidelines2021/>