

Everything Needs to be Secured

Introduction to the Internet of Things v2.0



Sections & Objectives

- Security in the Digitized World
 - Explain why security is important in the digitized world.
 - Explain the need for security in the digitized world.
 - Explain how to help secure the corporate world.
 - Explain how to secure personal data and devices.

Security in the Digitized World

Why is Security so Important?

Types of Data

PII	Informational
Social security number	Rain gauge value
Email address	Number of cars through an intersection
Bank account numbers	Hospital emergency use per state
Student tuition bill	Average plane capacity
Credit rating	House thermometer reading
Debit card number	Census data
Fingerprints	Immigration values
Birth date	Average potato crops per province
Username/password	Next train time per station
Vehicle identification number (VIN)	Average gas consumption per flight
Mortgage information	
Home address	
Facebook photographs	

- The quantity, volume, variety, and immediacy of generated data has changed.
- Personally identifiable information (PII) or sensitive personal information (SPI) is data relating to a living individual that can be used on its own or with other information to identify, contact, or locate a specific individual.
- Informational data can also contain sensitive information concerning corporate secrets, new product patents, or national security.

Why is Security so Important?

Lab – Types of Data



Lab – Types of Data (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. This lab can be done as independent work by a student or as a group discussion.

Objectives

Select 3 or 4 "non-traditional" objects or places that could now contain sensors. List the types of data that could be collected by the sensors. Determine if any of the collected data is sensitive.

Background / Scenario

It is important to recognize where sensors are being used in our world today and what types of data they are collecting. We need to determine if the collected data is sensitive in nature. If it is sensitive, is it PII or who might benefit from stealing it?

Required Resources

- none

Step 1: Select 1 or 2 more objects or places that already (or could) contain sensors.

1> car GPS

2> fitness wristband (eg. FitBit)

3> _____

4> _____

Step 2: List types of data that could be collected from entry 1 or 2, and entry 3 or 4 of the sensors from above

Sensor	Type of Data	Sensitive? PII?	Useful to: Hackers Companies Government Cities

Why is Security so Important?

Who Wants our Data?



- **The Good Guys**
 - Legitimate companies that have an agreement in place to use the collected data about you.
 - We agree to this in “Terms and Conditions” or “Terms of Service and Agreements”
 - White hat hackers who test security to help protect data.
- **The Bad Guys**
 - Black hat hackers, want access to collected data for many nefarious reasons:
 - To access user IDs and passwords to steal identities
 - To access data to commit a crime.
 - To sell the information to a third party.
 - To modify the data or disable functionality on a device.
 - To disrupt or to damage the image of a legitimate company.
 - To create political unrest or to make a political statement.

Why is Security so Important?

Data in the Wrong Hands

- Login credentials and other personal data for more than one Million Yahoo and Gmail accounts are reportedly being offered for sale on the dark web.
- Cybercriminals penetrated Equifax (EFX), one of the largest credit bureaus, in July 2017 and stole the personal data of 145 million people
- A breach of MyFitnessPal affected 150 million users.
- Ransomware attackers stole 57 million drivers and rider accounts from Uber.



Why is Security so Important?

Lab – Internet Fingerprint



Lab 5.1.1.5 – Internet Fingerprint

Instructor Note: Red font color indicates text that appears in the instructor copy only.

Objectives

The purpose of this lab is to introduce the aspect of “fingerprinting” an individual using the worldwide web. The objective is to introduce various methods to extract as much information as possible using only the internet browser and various sites effectively.

Part 1: Obtain as much information about yourself using the Internet Edge, Google Chrome and Firefox through the use of the Google search engine.

Part 2: Use various sites to augment the information gathered using the Google search engine.

Part 3: Compare and contrast the information collected using the google search engine and the various sites stipulated.

Part 4: Create an internet fingerprint of yourself using all the information gathered and evaluate what information you would not want made public.

Background / Scenario

Whenever a person browses the internet, your various details like your background, politics, ethnicity, preferences, etc. are gathered by the various sites one visit. As you visit sites small “cookies” are planted into your PC in relation to the web browser and sites visited. These cookies contain small pieces of data based on your browsing patterns and sites visited. The social media sites gather a vast volume of your personal data prior to allowing you access to use the sites. All this personal information can be mined by anyone who may choose to do so. Thus browsing the internet is like leaving a sprinkling trail of cookie crumbs that will lead to a more detailed picture of yourself available to anyone searching the internet about you.

Note: Please ensure the PC is running windows 8 or 10 with access to the latest version of Microsoft Edge and Google Chrome or Mozilla Firefox. The PC must have access to the internet.

Note: Please ensure windows enhanced security is turned off on the PC prior to commencing. If you are unsure please contact your instructor.

Required Resources

- One PC running windows 8 or 10 with internet access

Note: PC must have the latest version of Microsoft Edge, Google Chrome and Mozilla Firefox pre-installed. Enhanced internet security must be turned off on the respective PC

1: Use Mozilla Firefox to gather information about yourself

- Open up Mozilla Firefox and navigate to the <https://google.com> site.
- Enclose the first and last name of the person you’re searching for in quotes when you enter it into the search box (like “John Smith”). In this lab the person you are gathering data on is yourself.
- You can include other relevant words, like your profession, employer, location, or even a screen name that you may have used.
- If the person you’re searching for is likely to appear on a particular web site—like a school—search only that site using the site: URL operator (like [site:centennialcollage.com](https://www.centennialcollage.com) “John Smith”).
- You can also search for people by face, search for them on Google Images to get a quick visual—especially useful for people with common names, or to determine the gender of a name you never heard before. Search all the social media sites that are exposed linked to your search.
- Document all the information you have gathered from this search.

Why is Security so Important?

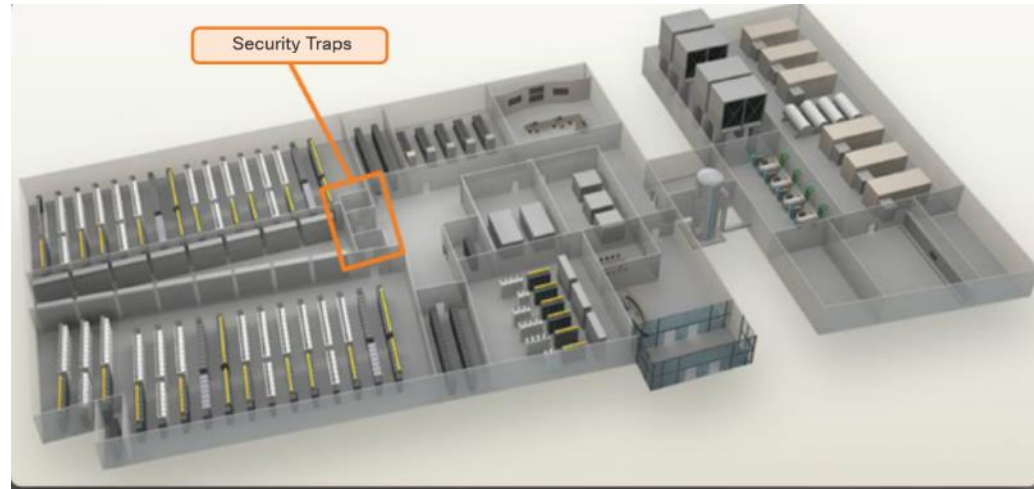
Security Best Practices

Security Best Practices	
Perform Risk Assessment	Regularly Test Incident Response
Create a Security Policy	Implement a Network Monitoring, Analytics and Management Tool
Physical Security Measures	Implement Network Security Devices
Human Resource Security Measures	Implement a Comprehensive Endpoint Security Solution
Perform and Test Backups	Educate Users
Maintain Security Patches and Updates	Encrypt data
Employ Access Controls	

Protecting the Corporate World

Physical Security

- **Outside perimeter security** - on-premise security officers, fences, gates, continuous video surveillance, and security breach alarms.
- **Inside perimeter security** - continuous video surveillance, electronic motion detectors, security traps, and biometric access and exit sensors.



Challenges of Securing IoT Devices



- **Increasing Number of Devices** - The number of interconnected sensors and smart devices is growing exponentially, increasing the opportunity for attacks.
- **Non-Traditional Location of Devices** - Some connected IoT devices are able to interact with the physical world.
- **Lack of Upgradeability** - IoT sensor-enabled devices may be located in remote and/or inaccessible locations where human intervention or configuration is almost impossible.

Protecting the Corporate World

Safe Wi-Fi Usage

Steps to Help Protect Your Company Wireless Network

Change the default administrator password



Configure the wireless router to use WPA2-AES encryption



Change the network service set identifier (SSID)



Keep the wireless router's firmware updated



Do not advertise the SSID name



Use Media Access Control (MAC) Address Filtering



Create a Guest Wireless Network



Disable your wireless router's remote management feature



Enable the built-in firewall



Physically secure the wireless router



Protecting the Corporate World

Protecting Devices


- **Keep the Firewall On**
- **Manage Your Operating System and Browser**
- **Protect All Your Devices**
- **Use Antivirus and Antispyware**



Protecting devices



Packet Tracer – Secure a Wireless Router

 Cisco Networking Academy® Mind Wide Open™

Packet Tracer – Secure a Wireless Router (Instructor Version)

Objectives

- Create a home network with a secure wireless router

Introduction

In this activity, you will configure a wireless router to:

- Modify the default password.
- Modify the default SSID and do not broadcast
- Use WPA2 Personal as security method.
- Rely on MAC filtering to increase security.
- Disable remote management.

Step 1: Load the .pkt file

- a. Load the 5.1.2.6 Packet Tracer – Configure Wireless Security.pkt file.
- b. Press the **power** button on Laptop1 to turn it off.
- c. Drag the **Ethernet** port to the **Modules** list to remove it.
- d. Drag the **WPC300N** module to the empty slot on **Laptop1** and press the **power** button to boot **Laptop1**.

Step 2: Modify the default password.

- a. Click on the wireless router and select the **GUI** for configuration.
- b. Click **Administration > Management**
- c. Modify the router password to a stronger one. Change the password to **aCompAny3**. Note that the new password has 8 characters with upper and lower case digits and some of the vowels have been changed to numbers. Select **Save Settings** at the bottom of that screen.

Step 3: Modify the default SSID name and disable the broadcast feature.

- a. Click **Wireless** and modify the SSID name to **aCompany**.
- b. Select **SSID Broadcast** and click **Disabled**. Click **Save Settings** at the bottom of that screen.

Check the topology. Has Laptop0 lost connectivity with the wireless router? If so, why?

Yes - Because Laptop0 has not been configured with the new SSID name.

Step 4: Configure WPA2 security on the wireless router.

- a. Return to the wireless router GUI tab. Click **Wireless > Wireless Security**. Change Security Mode to **WPA2 Personal**. **AES** is currently the strongest encryption protocol available. Leave it selected.
- b. Configure the passphrase as **aCompWiFi**. Scroll to the bottom of the window and click **Save Settings**.

 © 2018 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public. Page 1 of 3

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 14

Securing Personal Data and Devices

Smart Homes

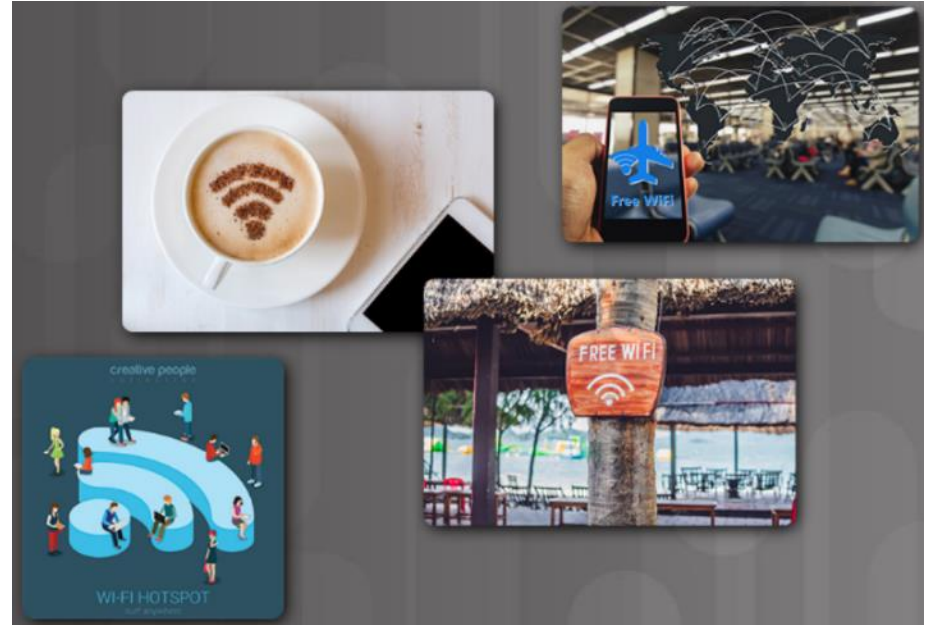


- Smart sensors in our homes increase the potential for security issues.
- The sensors could provide a way for hackers to get into our home network and gain access to any PCs and data that are connected to it.
- Before purchasing home security systems, it is very important to research the developer and the security and encryption protocols that are in place for its products.

Securing Personal Data and Devices

Public Hotspots

- Safety rules to follow when using a public or unsecure Wi-Fi hotspot:
 - Do not access or send any sensitive personal information
 - Verify that your computer is configured with file and media sharing, and that it requires user authentication with encryption.
 - Use encrypted virtual private network (VPN) tunnels and services.
- Bluetooth can be exploited by hackers to eavesdrop on some devices, establish remote access controls, distribute malware, and drain batteries.
 - Turn off when not in use.



Securing Personal Data and Devices

Setting up a VPN on Smartphones

How to manually set up a VPN from the Android settings

- Step 1 • Unlock your phone.
- Step 2 • Open the **Settings** app.
- Step 3 • Under the **Wireless & networks** section, select **More**.
- Step 4 • Select **VPN**.
- Step 5 • At the top-right corner you will find a plus sign (+), tap it.
- Step 6 • Your network administrator will provide you with all your VPN information. Simply select your desired protocol and enter all the information.
- Step 7 • Tap **Save**.
- Step 8 • You can connect by going back to the VPN settings and selecting your VPN of choice. You will be asked to enter a username and password.

How to manually set up a VPN on your iPhone or iPad

- Step 1 • Launch **Settings** from your Home screen.
- Step 2 • Tap **General**.
- Step 3 • Tap **VPN**.
- Step 4 • Tap **Add VPN Configuration**. If you have one already configured, select the **VPN client** you want to use and toggle the **Status** switch on.
- Step 5 • Tap **Type**.
- Step 6 • Select your **VPN type** from IKEv2, IPSec, or L2TP.
- Step 7 • Tap **Add Configuration** in the upper left corner to go back to the previous screen.
- Step 8 • Enter the **VPN settings information** including description, server, and remote ID.
- Step 9 • Enter your **authentication login** including your username (or certificate), and password.
- Step 10 • If you use a proxy, enable it by tapping **Manual** or **Auto**, depending on your preferences.
- Step 11 • Tap **Done**.

Lab - Discover Your Own Risky Online Behavior



Lab – Discover Your Own Risky Online Behavior (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Objectives

Explore actions performed online that may compromise your safety or privacy.

Background / Scenario

The Internet is a hostile environment, and you must be vigilant to ensure your data is not compromised. Attackers are creative and will attempt many different techniques to trick users. This lab helps you identify risky online behavior and provide tips on how to become safer online.

Part 1: Explore the Terms of Service Policy

Answer the questions below with honesty and take note of how many points each answer gives you. Add all points to a total score and move on to Part 2 for an analysis of your online behavior.

- a. What kind of information do you share with social media sites? _____
 - 1) Everything; I rely on social media to keep in touch with friends and family. (3 points)
 - 2) Articles and news I find or read (2 points)
 - 3) It depends; I filter out what I share and with whom I share. (1 point)
 - 4) Nothing; I do not use social media. (0 points)
- b. When you create a new account in an online service, you: _____
 - 1) Re-use the same password used in other services to make it easier to remember. (3 points)
 - 2) Create a password that is as easy as possible so you can remember it. (3 points)
 - 3) Create a very complex password and store it in a password manager service. (1 point)
 - 4) Create a new password that is similar to, but different from, a password used in another service. (1 point)
 - 5) Create an entirely new strong password. (0 points)
- c. When you receive an email with links to other sites: _____
 - 1) You do not click the link because you never follow links sent to you via email. (0 points)
 - 2) You click the links because the email server has already scanned the email. (3 points)
 - 3) You click all links if the email came from a person you know. (2 points)
 - 4) You hover the mouse on links to verify the destination URL before clicking. (1 point)
- d. A pop-up window is displayed as you visit a website. It states your computer is at risk and you should download and install a diagnostics program to make it safe: _____
 - 1) You click, download, and install the program to keep your computer safe. (3 points)
 - 2) You inspect the pop-up windows and hover over the link to verify its validity. (3 points)
 - 3) Ignore the message, making sure you don't click it or download the program and close the website. (0 points)
- e. When you need to log into your financial institution's website to perform a task, you: _____

Chapter Summary

Chapter Summary

Summary

- The quantity, volume, variety, and immediacy of generated data has changed.
- Personally identifiable information (PII) or sensitive personal information (SPI) is data relating to a living individual that can be used on its own or with other information to identify, contact, or locate a specific individual.
- Informational data can also contain sensitive information concerning corporate secrets, new product patents, or national security.
- White hat hackers test security to help protect data.
- Black hat hackers, want access to collected data for many nefarious reasons.
- **Outside perimeter security** - on-premise security officers, fences, gates, continuous video surveillance, and security breach alarms.
- **Inside perimeter security** - continuous video surveillance, electronic motion detectors, security traps, and biometric access and exit sensors.

Summary (Cont.)

- Challenges of securing devices on the IoT:
 - **Increasing Number of Devices** - The number of interconnected sensors and smart devices is growing exponentially, increasing the opportunity for attacks.
 - **Non-Traditional Location of Devices** - Some connected IoT devices are able to interact with the physical world.
 - **Lack of Upgradeability** - IoT sensor-enabled devices may be located in remote and/or inaccessible locations where human intervention or configuration is almost impossible.
- Know the steps to protect your company's wireless network.
- Steps for protecting your own devices:
 - Keep the Firewall On
 - Manage Your Operating System and Browser
 - Protect All Your Devices
 - Use Antivirus and Antispyware

Summary (Cont.)

- Smart sensors in our homes increase the potential for security issues.
- Safety rules to follow when using a public or unsecure Wi-Fi hotspot:
 - Do not access or send any sensitive personal information
 - Verify that your computer is configured with file and media sharing, and that it requires user authentication with encryption.
 - Use encrypted virtual private network (VPN) tunnels and services.
- Set up a VPN on your smart phone.

