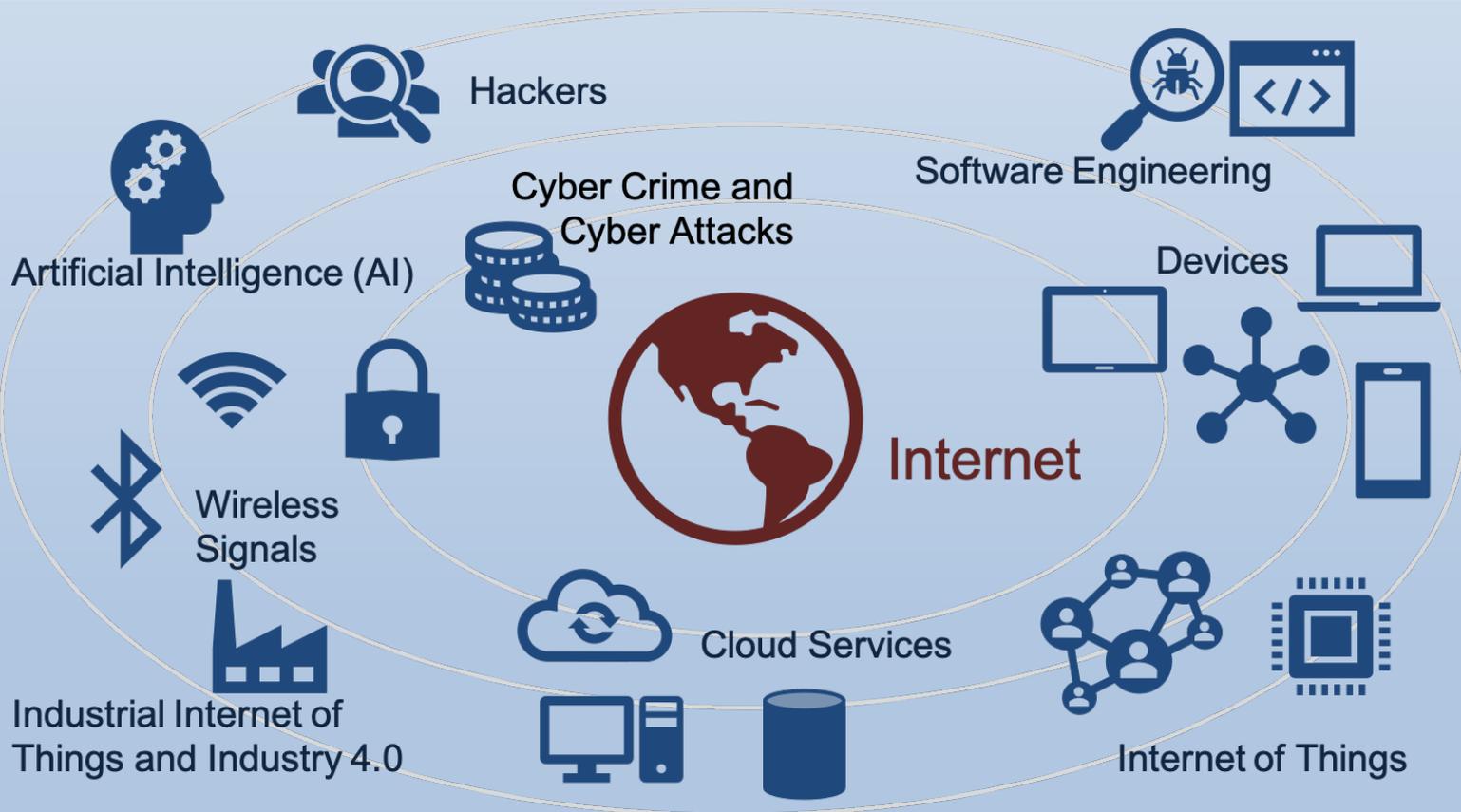




Cyber Security

Hans-Petter Halvorsen



<https://www.halvorsen.blog>

Cyber Security

Cyber Security, Data Security, GDPR and Data Privacy
with focus on Practical Implementations

Hans-Petter Halvorsen - 2021

Table of Contents

Table of Contents	2
Preface	6
Contents	6
Part 1 : Introduction	7
1. Your Digital Life	8
1.1 Introduction	8
1.2 Internet	9
1.3 Internet of Things	10
2. What is Cyber Security?	12
2.1 Hacking and Cyber Attacks	12
2.2 Types of Cyber Security threats	12
2.2.1 Ransomware.....	12
2.2.2 Malware	13
2.2.3 Social Engineering	13
2.2.4 Phishing	13
2.3 Spam	13
2.4 How to be Secure?	14
2.4.1 Firewall	14
2.4.2 Antivirus and Antimalware Software	14
2.4.3 Access Control	14
2.4.4 VPN.....	15
2.4.5 Wi-Fi Network	15
2.4.6 Education.....	15
Part 2 : Cyber Attacks	16
3. Types of Cyber Attacks	17
3.1 Malware	17
3.2 Phishing	17
3.3 Man-in-the-middle attack (MitM)	17
3.4 Denial-of-service attack (DoS)	18
3.4.1 Botnet.....	18
3.5 SQL injection	18
3.6 Zero-day exploit	18
4. Malware	19

4.1	Virus	19
4.2	Worms	19
4.3	Trojan Viruses	19
4.4	Spyware	20
4.5	Adware	20
4.6	Ransomware	20
4.6.1	WannaCry Ransomware Attack	20
4.6.2	Norsk Hydro	20
4.6.3	Cryptojacking/Cryptomining Malware	21
5.	SQL Injection	22
5.1	Introduction	22
5.2	Examples	22
5.3	Other Resources	24
5.3.1	Python Resources	24
5.3.2	ASP.NET Resources	24
6.	How to be Secure?	25
6.1	Passwords	25
6.2	Firewall	25
6.2.1	Web Application Firewall (WAF)	25
6.3	Antivirus and antimalware software	26
6.4	Access Control	26
6.4.1	Two-factor Authentication	26
6.5	VPN	27
6.6	Web Hosting Providers	27
6.7	Wi-Fi Network	27
6.8	Operating System	27
6.9	Education	27
	Part 3 : Data Privacy	28
7.	Introduction to Data Privacy	29
8.	GDPR	30
	Part 4 : Data Security	31
9.	Data Security	32
10.	Antivirus Software	33
10.1	Operating Systems	33
10.1.1	Windows 10	33
10.1.2	macOS	33

11.	<i>User Identity and Login</i>	34
11.1	<i>Password Security</i>	34
11.1.1	<i>Encryption and Decrypting</i>	34
11.1.2	<i>Hashing</i>	35
11.1.3	<i>Rainbow Tables</i>	36
11.1.4	<i>Salting</i>	37
	<i>Part 5 : Internet of Things and Cyber Security</i>	39
12.	<i>Internet of Things (IoT)</i>	40
13.	<i>IoT and Cyber Security</i>	42
13.1	<i>Security of Things</i>	42
14.	<i>Industrial Internet of Things and Industry 4.0</i>	43
14.1	<i>Industry 4.0</i>	43
14.2	<i>SCADA Systems</i>	44
15.	<i>IEC 62443</i>	46
	<i>Part 6 : Cloud Systems</i>	47
16.	<i>Cloud Systems</i>	48
17.	<i>Microsoft Azure</i>	49
	<i>Part 7 : Database Systems</i>	50
18.	<i>Database Systems</i>	51
19.	<i>SQL Server</i>	52
19.1	<i>Introduction</i>	52
19.2	<i>Authentication</i>	52
19.3	<i>Create Logins in SQL Server</i>	53
20.	<i>Microsoft Azure</i>	56
	<i>Part 8 : Web Platforms</i>	57
21.	<i>Web Platforms</i>	58
22.	<i>ASP.NET Core</i>	59
23.	<i>PHP</i>	60
	<i>Part 9 : ASP.NET Core</i>	61
24.	<i>Introduction to ASP.NET Core</i>	62
25.	<i>User Identity and Login</i>	63
25.1	<i>Introduction</i>	63
25.2	<i>Microsoft.AspNetCore.Identity</i>	63
25.2.1	<i>PasswordHasher<TUser> Class</i>	63
25.3	<i>Session State in ASP.NET Core</i>	64

25.4	Demo Application.....	64
25.4.1	Login	65
25.4.2	Create User	66
25.4.3	Update User Information	66
25.4.4	More Features	67
26.	<i>ASP.NET Core Identity.....</i>	68
26.1	Introduction.....	68
26.1.1	Scaffold Identity in ASP.NET Core Projects.....	68
26.2	Demo Application.....	69
26.2.1	Create Project in Visual Studio with Identity Enabled.....	69
26.2.2	Create Identity Database.....	71
26.2.3	Register New Account and Log In.....	73
26.2.4	2 Factor Authentication.....	75
26.2.5	Start Creating your Application	77
26.2.6	Scaffolding.....	79
26.3	Additional Resources.....	83
	<i>Part 10 : Software Security Testing.....</i>	84
27.	<i>Software Security Testing</i>	85
27.1	Introduction.....	85
27.2	Test Standards	85
27.2.1	ISO/IEC 27001.....	85
27.3	Test Tools.....	85
27.4	OWASP	85
27.5	Test Platforms.....	85
28.	<i>OWASP.....</i>	86
	<i>Part 11 : Machine Learning and Artificial Intelligence.....</i>	87
29.	<i>Introduction.....</i>	88
	<i>References.....</i>	89

Preface

In this textbook an overview of Cyber Security, Data Security, GDPR and Data Privacy will be given.

Why should we know about these things? This textbook will give you the answers.

The focus will be very practical, with many examples.

Cyber Security Web Site:

https://www.halvorsen.blog/documents/technology/cyber_security/

Here you will find lots of resources regarding Cyber Security in context of Internet of Things (IoT) systems, Industry 4.0, Cloud systems, Web Technology and Software Engineering.

You will in addition find lots of useful resources on my Website/Blog:

<https://www.halvorsen.blog>

Contents

This textbook consists of the following Parts:

- Part 01 - Introduction
- Part 02 - Cyber Attacks
- Part 03 - Data Privacy
- Part 04 - Data Security
- Part 05 - Internet of Things (IoT)
- Part 06 - Cloud Systems
- Part 07 - Database Systems
- Part 08 - Web Platforms
- Part 09 - ASP.NET Core
- Part 10 - Software Security Testing
- Part 11 - Machine learning and Artificial Intelligence

Part 1 : Introduction

This part gives a short introduction to topics covered in this textbook.

1. Your Digital Life

1.1 Introduction

Figure 1-1 shows an overview of Cyber Security Issues.

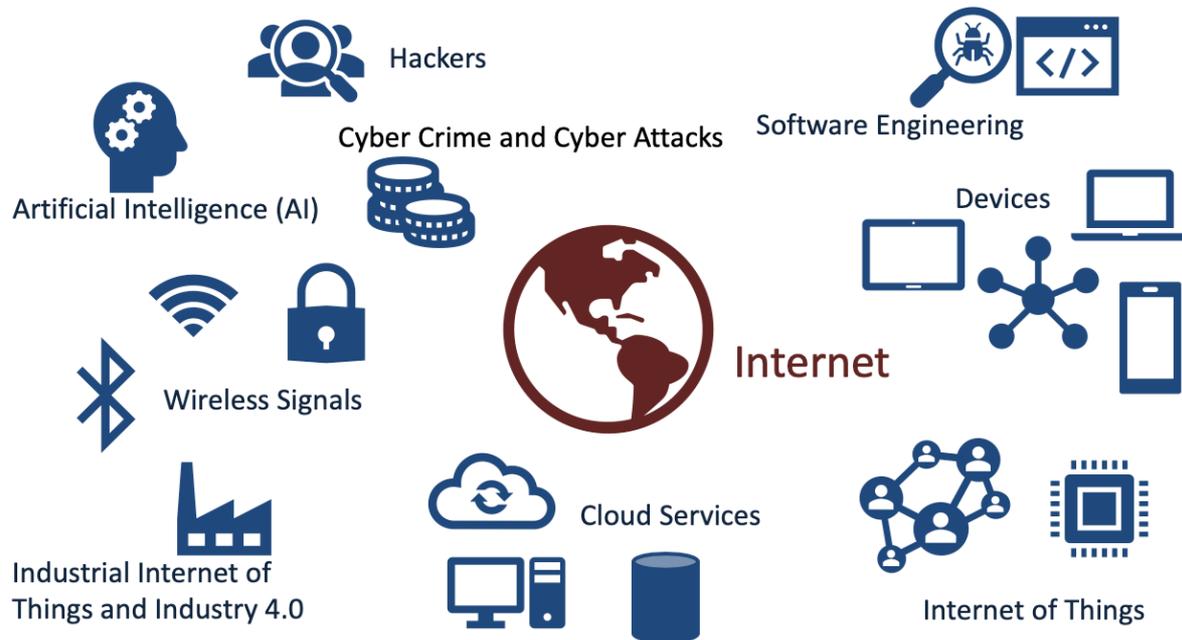


Figure 1-1: An overview of Cyber Security Issues

Facebook – Social Network founded by Mark Zuckerberg, 2.2 billion monthly active users.

You probably use hundreds of different Internet services. Are your personal data safe within these companies?

- Is the data well protected (from hackers)?
- Is the data sold to other companies (advertising purposes)?
- Can you get an overview of the information stored on you?
- Is it possible to delete it?

Data Security: Protect digital data (e.g., data in a database) from destructive forces and from the unwanted actions of unauthorized users (e.g., hackers, etc.).

Data Privacy: Issues regarding your personal data stored.

Cyber Security is the practice of protecting systems, networks, and programs from digital attacks.

Cybersecurity, or computer security, is a catchall term for any strategy for protecting one's system from malicious attacks aimed at stealing money, personal information, system

resources (cryptojacking, botnets), and a whole host of other bad things. The attack might occur on your hardware or software, or through social engineering.

GDPR: General Data Protection Regulation. EU directive. Purpose: Protect the privacy and the data stored, i.e., protection of your digital life

The “Facebook/Cambridge Analytica” Issue:

- Facebook shared your personal data with Cambridge Analytica.
- Cambridge used the data in the US election.
- About 87 million people affected by the scandal.

WannaCry: The WannaCry ransomware attack was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.

References:

<https://www.malwarebytes.com/antivirus/>

1.2 Internet

With the good, comes the bad. Since Internet connected all devices together a new era of our life was a fact.

Internet is great for many things, but it is also a great place for criminals.

Figure 1-2 we see the evolution of computers and internet from the early begging and until today.

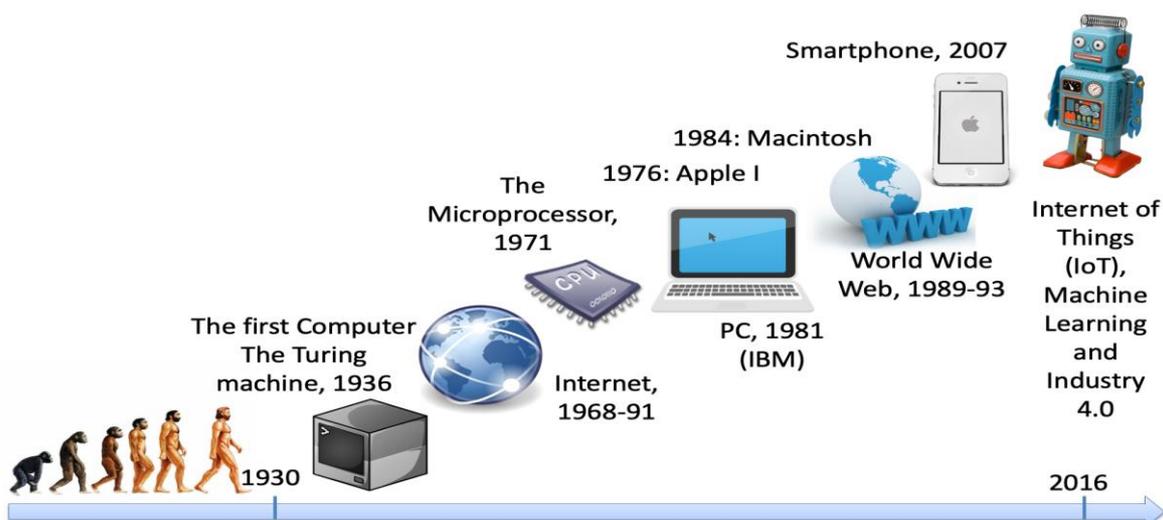


Figure 1-2: The Evolution of Computers and Internet

1.3 Internet of Things

With Internet of Things (IoT) everything is connected and share information via Internet and are online 24-7. The Internet of Things (IoT) is a network of physical objects and items, such as devices, vehicles, buildings, etc. which are embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data.

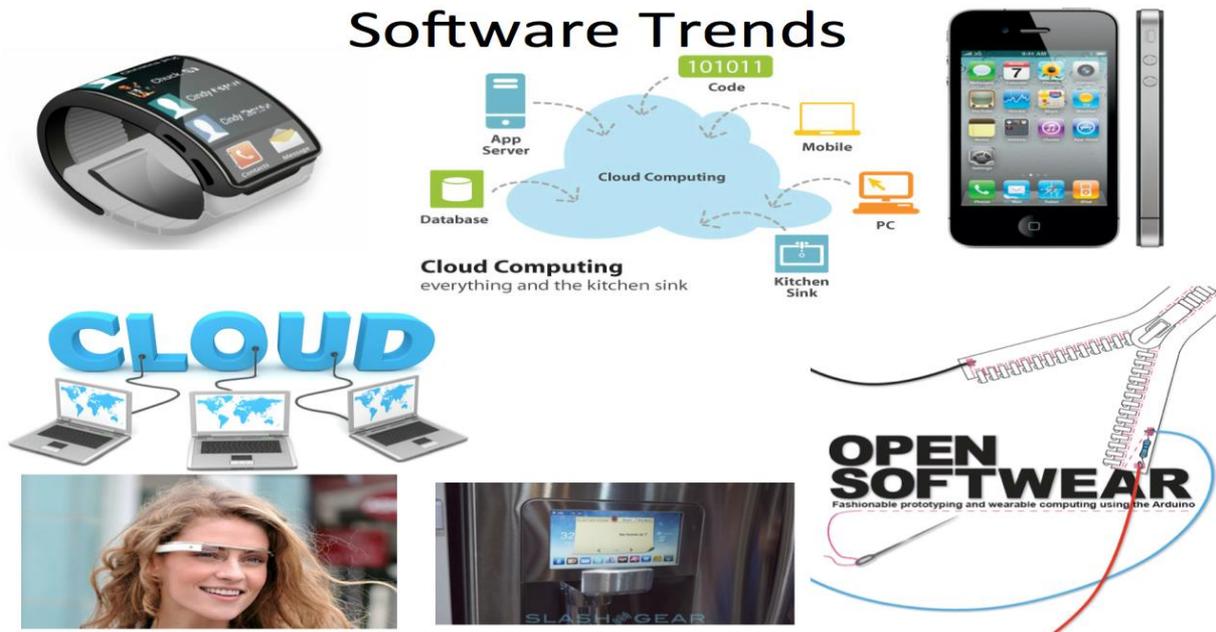


Figure 1-3: Modern Software Trends

Figure 1-4 shows the complexity of software development and different components that are involved.

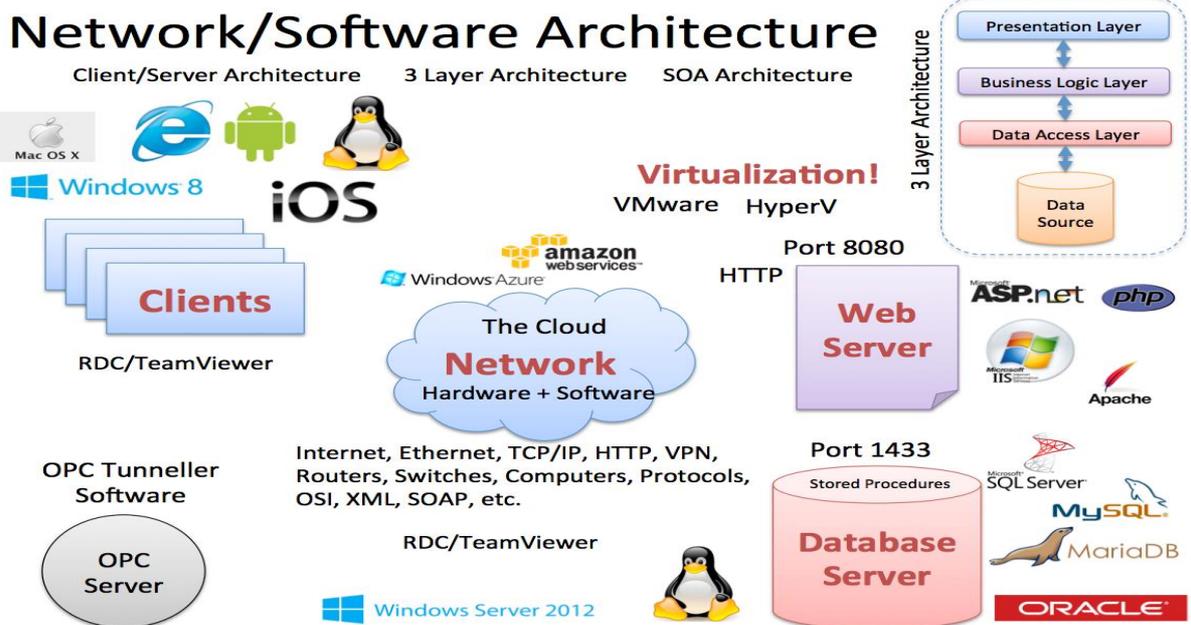


Figure 1-4: The Complexity of modern Software

For more information about creating modern software, please see my textbook "**Software Development - A Practical Approach!**".

Web:

https://www.halvorsen.blog/documents/programming/software_engineering/

2. What is Cyber Security?

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.

These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information, extorting money from users, or interrupting normal business processes.

References:

<https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html>

2.1 Hacking and Cyber Attacks

What are Cyber Attacks?

What is Hacker? Who is hacking?

Private persons, professional organizations and even countries. The main goal is to make money or get information from other countries.

What is the goal with hacking?

2.2 Types of Cyber Security threats

Different types of Cyber Security threats:

- Ransomware
- Malware
- Social engineering
- Phishing

These will be discussed more in detail below.

2.2.1 Ransomware

Ransomware is a type of malicious software. It is designed to extort money by blocking access to files or the computer system until the ransom is paid.

These include, e.g., email phishing and malvertising (malicious advertising). After it is distributed, the ransomware encrypts selected files and notifies the victim of the required payment.

Paying the ransom does not guarantee that the files will be recovered, or the system restored.

The most "famous" Ransomware is the WannaCry Ransomware.

2.2.2 Malware

Malware is a type of software designed to gain unauthorized access or to cause damage to a computer. Malware is short for “malicious software”.

Examples of common malware includes viruses, worms, Trojan viruses, spyware, adware, and ransomware.

2.2.3 Social Engineering

Social engineering is a tactic that adversaries use to trick you into revealing sensitive information. They can solicit a monetary payment or gain access to your confidential data. Social engineering can be combined with any of the threats listed above to make you more likely to click on links, download malware, or trust a malicious source.

2.2.4 Phishing

Phishing is the practice of sending fraudulent emails that resemble emails from reputable sources.

The aim is to steal sensitive data like credit card numbers and login information, or to install malware on the victim’s machine.

Phishing is the most common type of cyber-attack.

You can help protect yourself through education (teach them not to click on links, etc. from untrusted sources) or a technology solution that filters malicious emails.

Types of phishing attacks:

- **Deceptive phishing** - Deceptive phishing is the most common type of phishing. In this case, an attacker attempts to obtain confidential information from the victims. Attackers use the information to steal money or to launch other attacks. A fake email from a bank asking you to click a link and verify your account details is an example of deceptive phishing.
- **Spear phishing** - Spear phishing targets specific individuals instead of a wide group of people. Attackers often research their victims on social media and other sites. That way, they can customize their communications and appear more authentic. Spear phishing is often the first step used to penetrate a company’s defenses and carry out a targeted attack.
- **Whaling** - When attackers go after a “big fish” like a CEO, it’s called whaling.
- **Pharming** - pharming sends users to a fraudulent website that appears to be legitimate. However, in this case, victims do not even have to click a malicious link to be taken to the bogus site.

2.3 Spam

Spam is unsolicited and unwanted junk email sent out in bulk to an indiscriminate recipient list. Typically, spam is sent for commercial purposes. It can be sent in massive volume by botnets, networks of infected computers.

Often, spam email is sent for commercial purposes. While some people view it as unethical, many businesses still use spam. The cost per email is incredibly low, and businesses can send out mass quantities consistently. Spam email can also be a malicious attempt to gain access to your computer.

Spam email can be difficult to stop, as it can be sent from botnets. **Botnets** are a network of previously infected computers. As a result, the original spammer can be difficult to trace and stop.

Spam email can be dangerous. It can include malicious links that can infect your computer with malware (see What is malware?). Do not click links in spam. Dangerous spam emails often sound urgent, so you feel the need to act.

2.4 How to be Secure?

Here are some examples:

- Firewall
- Antivirus and antimalware software
- Access control
- VPN
- Wi-Fi Network
- Education

These will be discussed more in detail below.

2.4.1 Firewall

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Firewalls are the first line of defense in network security.

A firewall can be hardware, software, or both.

2.4.2 Antivirus and Antimalware Software

“Malware”, short for “malicious software”, includes viruses, worms, Trojans, ransomware, and spyware. Sometimes malware will infect a network but lie dormant for days or even weeks. The best antimalware programs not only scan for malware upon entry, but also continuously track files afterward to find anomalies, remove malware, and fix damage.

2.4.3 Access Control

Not every user should have access to your network. To keep out potential attackers, you need to recognize each user and each device.

Two Factor Authentication.

2.4.4 VPN

A virtual private network encrypts the connection from an endpoint to a network, often over the Internet.

2.4.5 Wi-Fi Network

Use only secure Wi-Fi networks, not open Wi-Fi network that do not need password, etc.

2.4.6 Education

By learning more about cyber security threats and how you can protect yourself as a private person or a company is crucial.

Part 2 : Cyber Attacks

This part gives an overview common types of Cyber Attacks in our software-based world.

3. Types of Cyber Attacks

A cyberattack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization.

Usually, the attacker seeks some type of benefit from disrupting the victim's network.

Common types of cyber-attacks:

- Malware
- Phishing
- Man-in-the-middle attack (MitM)
- Denial-of-service attack (DoS)
- SQL injection
- Zero-day exploit

These will be discussed more in detail below.

3.1 Malware

Malware is a term used to describe malicious software, including spyware, ransomware, viruses, and worms.

Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software.

3.2 Phishing

Phishing is the practice of sending fraudulent emails that resemble emails from reputable sources.

The aim is to steal sensitive data like credit card numbers and login information, or to install malware on the victim's machine.

It's the most common type of cyber-attack.

3.3 Man-in-the-middle attack (MitM)

Man-in-the-middle (MitM) attacks, also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data.

Two common points of entry for MitM attacks:

- On unsecure public Wi-Fi, attackers can insert themselves between a visitor's device and the network. Without knowing, the visitor passes all information through the attacker.
- Once malware has breached a device, an attacker can install software to process all of the victim's information.

3.4 Denial-of-service attack (DoS)

A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests.

Attackers can also use multiple compromised devices (Botnet) to launch this attack. This is known as a distributed-denial-of-service (DDoS) attack.

3.4.1 Botnet

A botnet is a network of devices that has been infected with malicious software, such as a virus. Attackers can control a botnet as a group without the owner's knowledge with the goal of increasing the magnitude of their attacks. Often, a botnet is used to overwhelm systems in a distributed-denial-of-service attack (DDoS) attack.

3.5 SQL injection

A Structured Query Language (SQL) injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not.

An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box.

[\[https://www.cisco.com/c/en/us/about/security-center/sql-injection.html\]](https://www.cisco.com/c/en/us/about/security-center/sql-injection.html)

3.6 Zero-day exploit

A zero-day exploit hits after a network vulnerability is announced but before a patch or solution is implemented. Attackers target the disclosed vulnerability during this window of time.

4. Malware

Malware is a type of software designed to gain unauthorized access or to cause damage to a computer.

Malware is a contraction for “malicious software” (Norsk: skadelig programvare).

Examples of common malware includes viruses, worms, Trojan viruses, spyware, adware, and ransomware.

Types of malware:

- Virus
- Worms
- Trojan virus
- Spyware
- Adware
- Ransomware
- Cryptojacking or Cryptomining malware

These will be discussed more in detail below.

References:

<https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html>

4.1 Virus

A virus is malicious software attached to a document or file that supports macros to execute its code and spread from host to host. Once downloaded, the virus will lay dormant until the file is opened and in use.

4.2 Worms

Worms are a malicious software that rapidly replicates and spreads to any device within the network.

4.3 Trojan Viruses

Trojan viruses are disguised as helpful software programs. But once the user downloads it, the Trojan virus can gain access to sensitive data and then modify, block, or delete the data.

4.4 Spyware

Spyware is malicious software that runs secretly on a computer and reports back to a remote user. Rather than simply disrupting a device's operations, spyware targets sensitive information and can grant remote access to predators.

Spyware is often used to steal financial or personal information.

A specific type of spyware is a keylogger, which records your keystrokes to reveal passwords and personal information.

4.5 Adware

Adware is malicious software used to collect data on your computer usage and provide appropriate advertisements to you.

While adware is not always dangerous, in some cases adware can cause issues for your system.

Adware can redirect your browser to unsafe sites, and it can even contain Trojan horses and spyware.

4.6 Ransomware

Ransomware is malicious software that gains access to sensitive information within a system, encrypts that information so that the user cannot access it, and then demands a financial payout for the data to be released.

The most "famous" Ransomware is the WannaCry Ransomware.

4.6.1 WannaCry Ransomware Attack

The WannaCry ransomware attack was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.

References:

https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

4.6.2 Norsk Hydro

In the beginning of 2019 Norway's Norsk Hydro was hit by ransom cyber-attack.

Norwegian aluminum maker Norsk Hydro may have lost more than \$40 million in the week that followed a cyber-attack that paralyzed parts of its operations, and a full recovery of IT systems.

4.6.3 Cryptojacking/Cryptomining Malware

Cryptojacking (also called malicious cryptomining) is an emerging online threat that hides on a computer or mobile device and uses the machine's resources to "mine" forms of online money known as cryptocurrencies.

Cryptocurrencies are forms of digital money that exist only in the online world, with no actual physical form. They were created as an alternative to traditional money, and gained popularity for their forward-looking design, growth potential, and anonymity.

Two words, "cryptography" and "currency"—combine to form "cryptocurrency," which is electronic money, based on the principles of complex mathematical encryption. All cryptocurrencies exist as encrypted decentralized monetary units, freely transferable between network participants.

One of the earliest, most successful forms of cryptocurrency is Bitcoin.

Now also Facebooks together with others created a new cryptocurrency called Libra.

References:

<https://www.malwarebytes.com/cryptojacking/>

5. SQL Injection

SQL Injection is a type of attack by which cybercriminals exploit software vulnerabilities in web applications for the purpose of stealing, deleting, or modifying data, or gaining administrative control over the systems running the affected applications.

References:

<https://www.malwarebytes.com/sql-injection/>

5.1 Introduction

A Structured Query Language (SQL) injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not.

An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box.

Structured Query Language (SQL) is used to query, operate, and administer database systems such as Microsoft SQL Server, Oracle, or MySQL. The general use of SQL is consistent across all database systems that support it.

Database systems are commonly used to provide backend functionality to many types of web applications. In support of web applications, user-supplied data is often used to dynamically build SQL statements that interact directly with a database. A SQL injection attack is an attack that is aimed at subverting the original intent of the application by submitting attacker-supplied SQL statements directly to the backend database.

References:

<https://www.cisco.com/c/en/us/about/security-center/sql-injection.html>

5.2 Examples

Below you find some basic SQL Injection examples.

Web Site:

```
<form action="/cgi-bin/login" method=post>
  Username: <input type=text name=username>
  Password: <input type=password name=password>
<input type=submit value=Login>
```

SQL query executed by the web site for getting the user information:

```
select * from Users where (username = 'submittedUser' and password = 'submittedPassword');
```

SQL Injection Example #1:

For example, if an application accepts and processes user-supplied data without any validation, an attacker could submit a maliciously crafted username and password. Consider the following string sent by an attacker:

```
username=admin%27%29+--+&password=+
```

The SQL query executed by the web site for getting the user information will be:

```
select * from Users where (username = 'admin') -- and password = ' ');
```

In this example, an attacker could successfully log in to the application using the admin account without knowledge of the password to that account.

Note that the string of two dash characters (--) indicates to the database server that the remaining characters in the SQL statement are a comment and should be ignored.

SQL Injection Example #2:

A hacker might get access to user names and passwords in a database by simply inserting " OR ""="" into the user name or password text box:

User Name:

Password:

The SQL query executed by the web site for getting the user information will be:

```
select * from Users where Name ="" or ""="" AND Pass ="" or ""=""
```

The SQL above is valid and will return all rows from the "Users" table, since OR ""="" is always TRUE.

References:

https://www.w3schools.com/sql/sql_injection.asp

5.3 Other Resources

Here are some other resources regarding SQL injection:

https://www.owasp.org/index.php/SQL_Injection

https://en.wikipedia.org/wiki/SQL_injection

https://www.w3schools.com/sql/sql_injection.asp

5.3.1 Python Resources

Python is an open-source and cross-platform programming language, that has become increasingly popular over the last ten years. Below you find some useful Python resources for implementing database communication.

Web:

<https://www.halvorsen.blog/documents/programming/python/>

Videos:

Python and SQL Server: <https://youtu.be/pMGW353gauo>

5.3.2 ASP.NET Resources

ASP.NET is an open-source web framework, created by Microsoft, for building web apps and services using the .NET Framework or the .NET Core. We have both ASP.NET and ASP.NET Core. ASP.NET Core is the new approach built on .NET Core.

Below you find some useful ASP.NET resources for implementing database communication.

Web:

<https://www.halvorsen.blog/documents/programming/web/aspnet>

Videos:

ASP.NET Core - Database Communication: <https://youtu.be/0Ta3dQ3rxzs>

ASP.NET Core - Database CRUD Application: <https://youtu.be/k5TCZDwTYcE>

6. How to be Secure?

How can you avoid cyber-attacks in general?

What can you do as a company or a private person?

Here are some examples:

- Passwords
- Firewall
- Antivirus and antimalware software
- Access control
- VPN
- Wi-Fi Network
- Education

These will be discussed more in detail below.

6.1 Passwords

Make sure to use secure passwords, don't use the same password for all your services and software systems.

6.2 Firewall

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Firewalls are the first line of defense in network security.

A firewall can be hardware, software, or both.

6.2.1 Web Application Firewall (WAF)

A web application firewall (WAF) is an application firewall for HTTP applications. It applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection.

The WAF software (or hardware) is installed on the server that runs the web applications or web sites.

A WAF is used for protection of a specific web application or set of web applications.

A WAF creates a shield between the web application and the Internet, which can avoid many common attacks.

A WAF helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others.

Most professional hosting platforms offers some kind of WAF, like Amazon Web Services. In addition, there are many WAF software you can buy and use, e.g., Imunify360.

References:

<https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/>

https://www.owasp.org/index.php/Web_Application_Firewall

https://en.wikipedia.org/wiki/Web_application_firewall

6.3 Antivirus and antimalware software

“Malware”, which is short for “malicious software”, includes viruses, worms, Trojans, ransomware, and spyware. Sometimes malware will infect a network but lie dormant for days or even weeks. The best antimalware programs not only scan for malware upon entry, but also continuously track files afterward to find anomalies, remove malware, and fix damage.

The Windows 10 operating system has built in antivirus software called "Windows Defender".

The name “Antivirus” software is a little old, because viruses are just one kind of malware in today’s world of cyber threats. Though viruses still exist, there are other forms of malware that are more common these days, as mentioned in an earlier chapter.

6.4 Access Control

Not every user should have access to your network. To keep out potential attackers, you need to recognize each user and each device.

6.4.1 Two-factor Authentication

Two-factor authentication (also known as 2FA) is a type, or subset, of multi-factor authentication.

It is a method of confirming users' claimed identities by using a combination of two different factors: 1) something they know, 2) something they have, or 3) something they are.

A good example of two-factor authentication is the withdrawing of money from an ATM; only the correct combination of a bank card (something the user possesses) and a PIN (something the user knows) allows the transaction to be carried out.

All the large providers of internet services, like Facebook, Google, Apple, etc. offers Two-factor authentication, you just need to turn it on.

References:

https://en.wikipedia.org/wiki/Multi-factor_authentication

6.5 VPN

A virtual private network encrypts the connection from an endpoint to a network, often over the Internet.

6.6 Web Hosting Providers

Make sure to use professional Web hosting companies for your web sites.

You have the large Cloud platform providers like Amazon Web Services (AWS), Microsoft Azure, Oracle Cloud and Google Cloud Platform.

These large providers have a high level of security, they continuously update the systems with new security patches, etc.

6.7 Wi-Fi Network

Use only secure Wi-Fi networks, not open Wi-Fi network that do not need password, etc.

6.8 Operating System

Make sure your PC and the operating system is up to date.

6.9 Education

By learning more about cyber security threats and how you can protect yourself as a private person or a company is crucial.

Part 3 : Data Privacy

You store lots of information about yourself when you use different devices, web sites and services. Can you trust that the data is safe?

7. Introduction to Data Privacy

Data security is about protect digital data (e.g., data in a database) from destructive forces and from the unwanted actions of unauthorized users (e.g., hackers, etc.). Data privacy deals with issues regarding your personal data stored.

Facebook – Social Network founded by Mark Zuckerberg, 2.2 billion monthly active users. You probably use hundreds of different Internet services. Are your personal data safe within these companies when it comes to:

- Is the data well protected (from hackers)?
- Is the data sold to other companies (advertising purposes)?
- Can you get an overview of the information stored on you?
- Is it possible to delete it?

GDPR, or General Data Protection Regulation, is an EU directive. The purpose is to protect the privacy and the data stored, i.e., protection of your digital life.

Example: The “Facebook/Cambridge Analytica” Issue:

- Facebook shared your personal data with Cambridge Analytica
- Cambridge used the data in the US election
- About 87 million people affected by the scandal

8. GDPR

GDPR: General Data Protection Regulation

EU regulation. All countries and companies within EU need to follow the regulation. Also, outside EU if the company save data about EU citizens.

Purpose:

- Protect the privacy and the data stored, i.e., protection of your digital life.
- Better control of your personal data
 - What kind of data is stored?
 - It should be able to delete the data
 - etc.

What is GDPR about? GDPR is about data protection and privacy. The main concepts are as follows:

1. You decide what kind of data that should be stored and what the data should be used for
2. Privacy statements: It should be clear what you say yes to
3. It should be possible to later delete the information stored about you.

References:

https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

Part 4 : Data Security

An overview of different Data Security aspects.

9. Data Security

Data Security: Protect digital data (e.g., data in a database) from destructive forces and from the unwanted actions of unauthorized users (e.g., hackers, etc.).

Antivirus Software

User Identity and Login

10. Antivirus Software

The name “Antivirus” software is a little old, because viruses are just one kind of malware in today’s world of cyber threats.

Though viruses still exist, there are other forms of malware that are more common these days.

All computers should have Antivirus Software today. Windows 10 (and other Operating Systems) has a built-in Antivirus/antimalware Software and E-mail software also have Antivirus/antimalware/Spam Software.

10.1 Operating Systems

10.1.1 Windows 10

10.1.2 macOS

References:

<https://www.malwarebytes.com/mac-antivirus/>

11. User Identity and Login

Here we will give an overview of user identity and login features in modern applications.

The concepts will be exemplified using web technology and the ASP.NET Core web framework from Microsoft.

ASP.NET is an open-source web framework, created by Microsoft, for building web apps and services using the .NET Framework or the .NET Core. We have both ASP.NET and ASP.NET Core. ASP.NET Core is the new approach built on .NET Core.

In this chapter we will see how we can create and use login functionality in your ASP.NET Core Web Applications.

Typically, you need to create functionality for User Registration, Login, etc. Here you will see how this can be done from scratch. If you do it from scratch, you will have full control of your code.

If you use something called “ASP.NET Core Identity” (which will be explained and demonstrated in the next chapter) lots of “magic” happens behind the curtains. If something not working, it may be more complicated to figure out why.

Below you find some useful ASP.NET resources.

<https://www.halvorsen.blog/documents/programming/web/aspnet>

11.1 Password Security

Keeping your passwords safe is important and all software systems should take this seriously.

Password security mechanism:

- Encryption and Decrypting
- Hashing
- Salting
- 2 Factor Authentication
- Etc.

These password security mechanisms will be described in more detail below.

11.1.1 Encryption and Decrypting

Encryption is the practice of scrambling information in a way that only someone with a corresponding key can unscramble and read it.

Encryption is a two-way function. When you encrypt something, you are doing so with the intention of decrypting it later.

To encrypt data, you use an algorithm. Many different encryption algorithms do exist

Figure 11-1 gives an overview of the concepts of Encryption and Decryption.

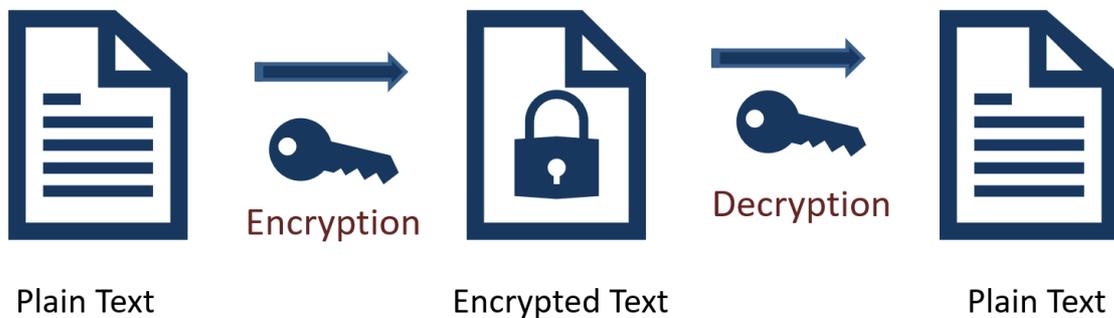


Figure 11-1: Encryption and Decryption

When should encryption be used? Here are some examples:

- Encryption is a two-way function.
- You encrypt information with the intention of decrypting it later.
- Examples when to use encryption:
 - Protecting Files and Information on your Computer
 - Protecting your Cloud data
 - Transmitting Data between 2 Computers
 - Etc.

The key is that Encryption is reversible. Hashing is not.

11.1.2 Hashing

Hashing is the practice of using an algorithm to map data of any size to a fixed length. Encryption is a two-way function. Hashing is a one-way function.

While it is technically possible to reverse-hash something, the computing power required makes it unfeasible. Hashing is one-way. See Figure 11-2.

Encryption is meant to protect data in transit, hashing is meant to verify that a file or piece of data has not been altered—that it is authentic. In other words, it serves as a checksum. Every hash value is unique.

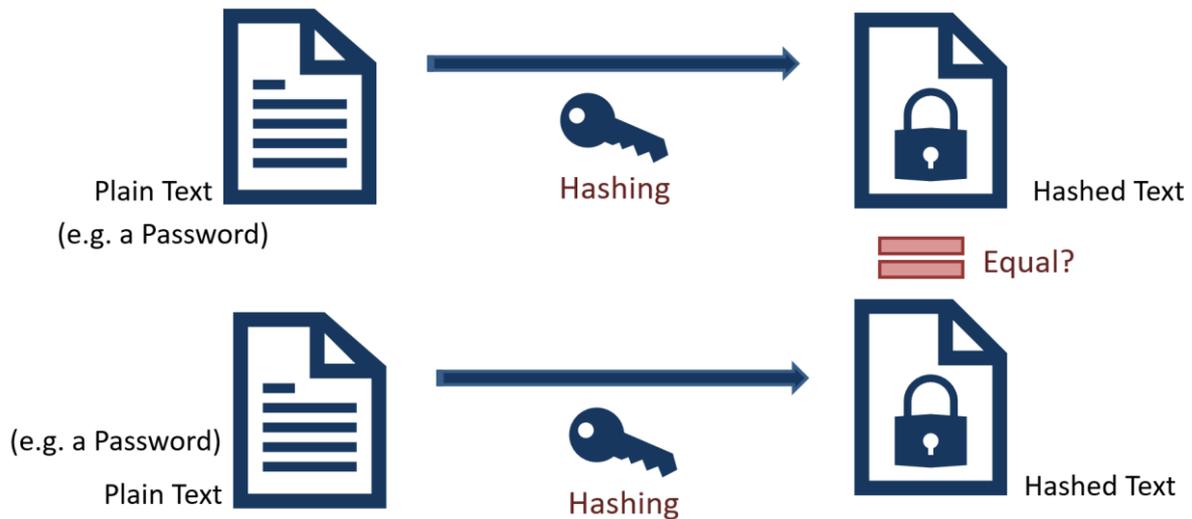


Figure 11-2: Hashing

11.1.3 Rainbow Tables

Is it possible for a hacker to get access to Hashed Passwords?

By using something called “Rainbow Table” the hacker can get access to your hashed password, see Figure 11-3.

Password Table for System X

UserName	HashedPassword
Mike	4420d1918bbc7
Bob	73fb51a0c9be7d
Peter	4420d1918bbc7

If a Hacker gets access to this Database, he can see that Mike and Peter have the same password. But he does not know the actual password

Password	HashedPassword
tesla	4420d1918bbc7
friendship	73fb51a0c9be7d
bicycle	7420e1618abc6

If the Hacker has access to so-called “Rainbow table” (which is essentially a pre-computed database of hashes), he may also be able to find the Password (as seen here)

Rainbow table

If you have a complicated password, it is less likely that your password is in such a Rainbow table

Figure 11-3: Using Rainbow Table for Hacking your Hashed Password

If a hacker gets access to this Database, he can see that Mike and Peter have the same password, but he does not know the actual password. If the Hacker has access to a so-called “Rainbow table” (which is essentially a pre-computed database of hashes), he may also be able to find the Password, as seen in Figure 11-3. If you have a complicated password, it is less likely that your password is in such a Rainbow table.

11.1.4 Salting

Salting is a technique typically used for Password Hashing. It is a unique value that can be added to the end of the password to create a different hash value. The additional value is referred to as a “salt”. This is done to make it even more secure. Typically, the Hashing Algorithm uses a Random salt. This prevents an attacker from seeing whether users have the same password. See Figure 11-4.

```
password = "Password123"  
salt = "Tesla"  
  
passwordHashed = HashPassword(password, salt);
```

Typically, Salting is built into the Hashing Algorithm and it is changed every time

```
password = "Password123"  
  
ph1 = HashPassword(password);  
ph2 = HashPassword(password);
```

ph1 \neq ph2

This means if 2 different Users use the same Password, the Hashed Password will be different!

Figure 11-4: Salting

Is it possible to hack “Hashing with Salt”?

Assume Mike and Peter use the same Password, see Table 11-1. If a hacker gets access to this database, he cannot see that Mike and Peter have the same password. This is because a random Salt has made these 2 Hashed Passwords different!

Table 11-1: Examples of Hashed Passwords with Salt

User Name	Hashed Password with Salt
Mike	4420d1918bbcf7
Bob	73fb51a0c9be7d
Peter	4520d1818cbcf7

Figure 11-5 shows a typical Flow when Creating User and Login.

Create User and Login

Create User

Name:

E-Mail:

Password:

Information given by User



```
passwordHashed = HashPassword(userName, password);
```



Store Hashed Password in the Database

Login

Enter UserName and Password in order to get access to the system.

E-Mail:

Password:

Compare Hashed Password stored in the Database with Password given by User in Login Page

```
valid = VerifyHashedPassword(userName, passwordDB, password);
```

Figure 11-5: Typical Flow when Creating User and Login

Part 5 : Internet of Things and Cyber Security

IoT or Internet of Things and Cyber Security Issues

12. Internet of Things (IoT)

The Internet of Things (IoT) is the network of physical objects or “things” embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data. The Internet of Things allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration between the physical world and computer-based systems, and resulting in improved efficiency, accuracy, and economic benefit.

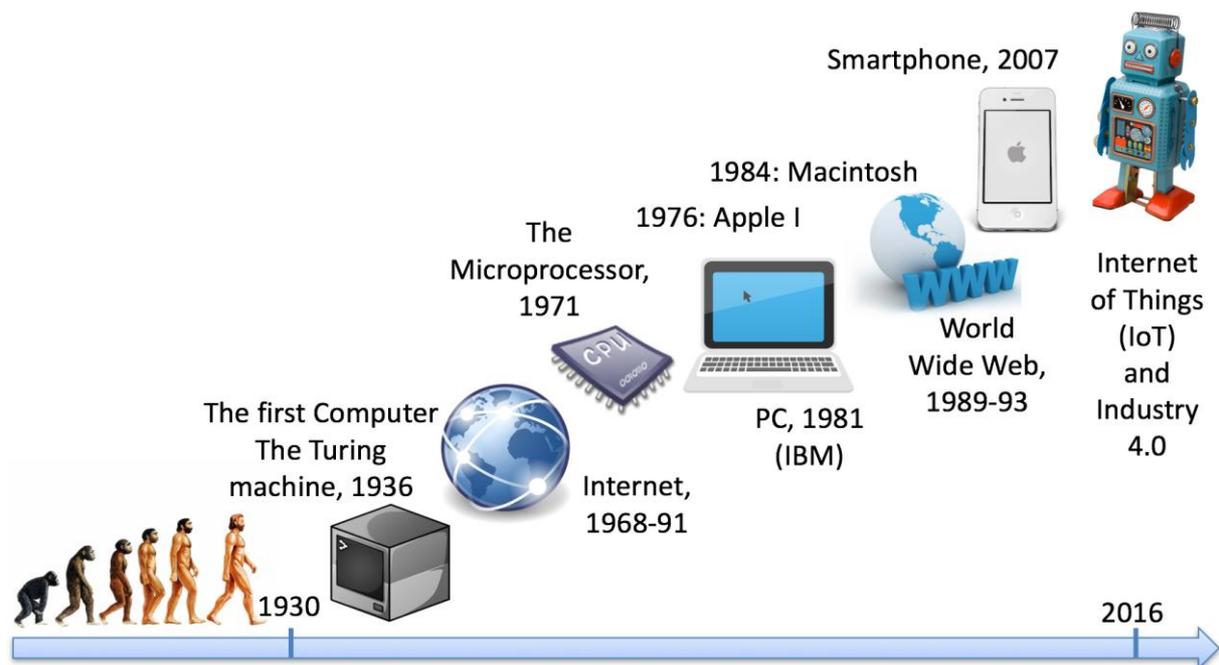


Figure 12-1: The New Era of Internet of Things

References:

https://en.wikipedia.org/wiki/Internet_of_Things

It is expected that all kinds of things will be connected to the Internet (Figure 12-2), e.g., lights, heating system, even the fridge.

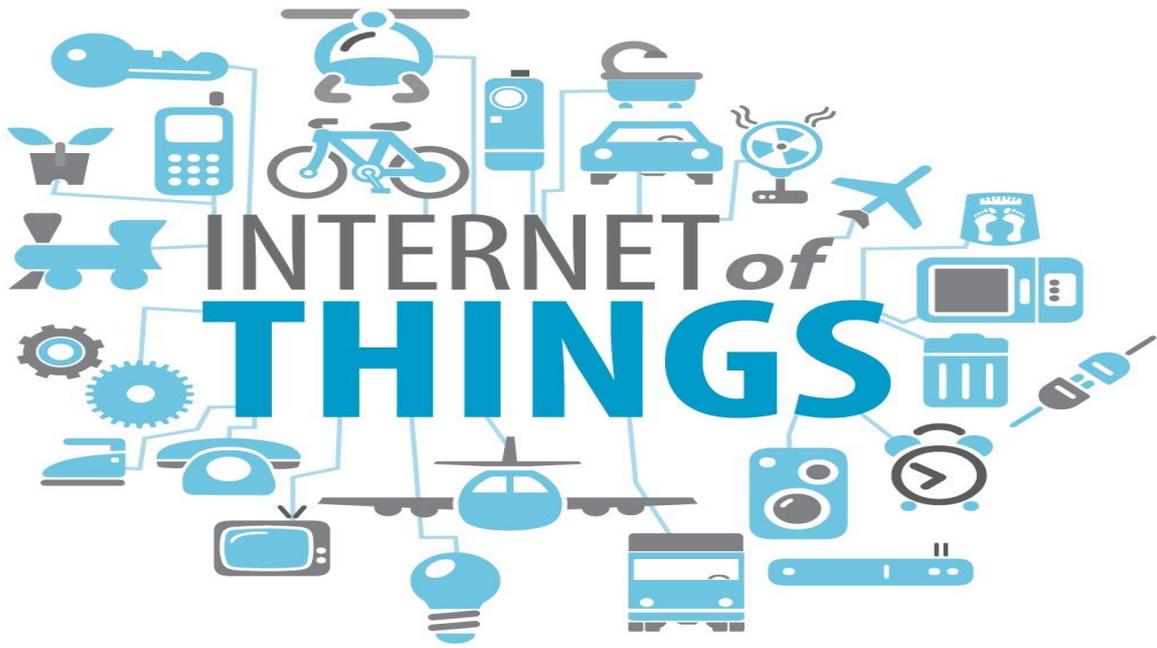


Figure 12-2: Internet of Things (IoT)

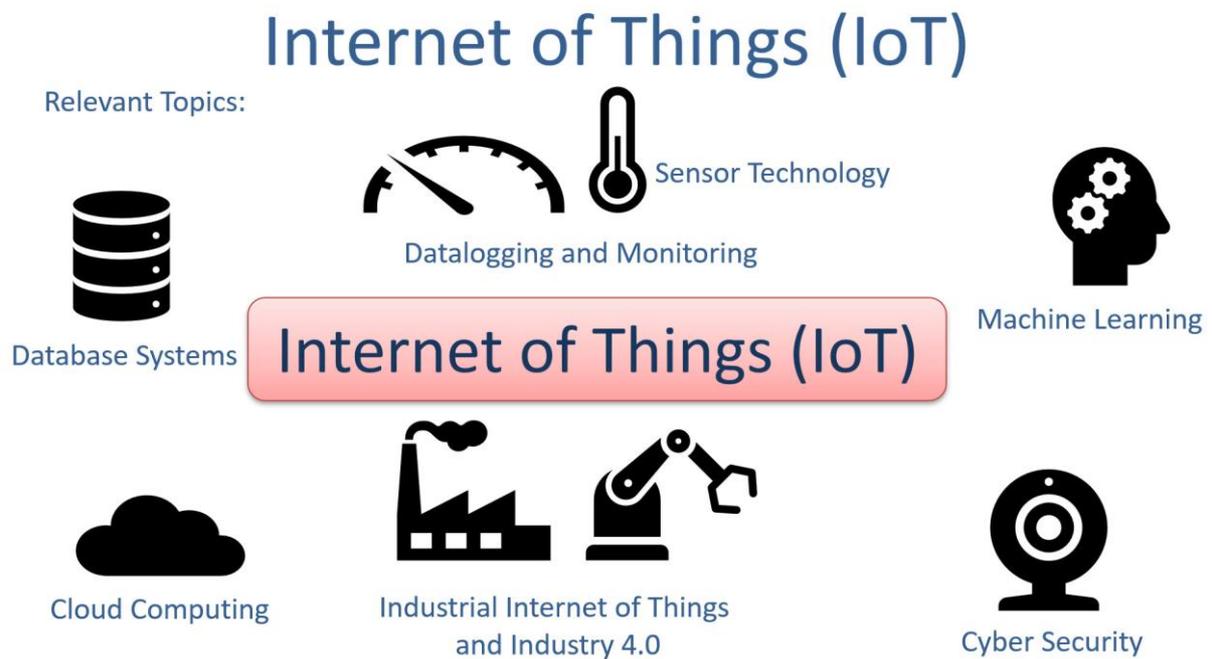


Figure 12-3: Internet of Things (IoT)

Web:

<https://www.halvorsen.blog/documents/technology/iot/>

13. IoT and Cyber Security

IoT solutions and Data Security? How can we make sure our applications and data are safe? Security is crucial in IoT/IIoT Applications. See

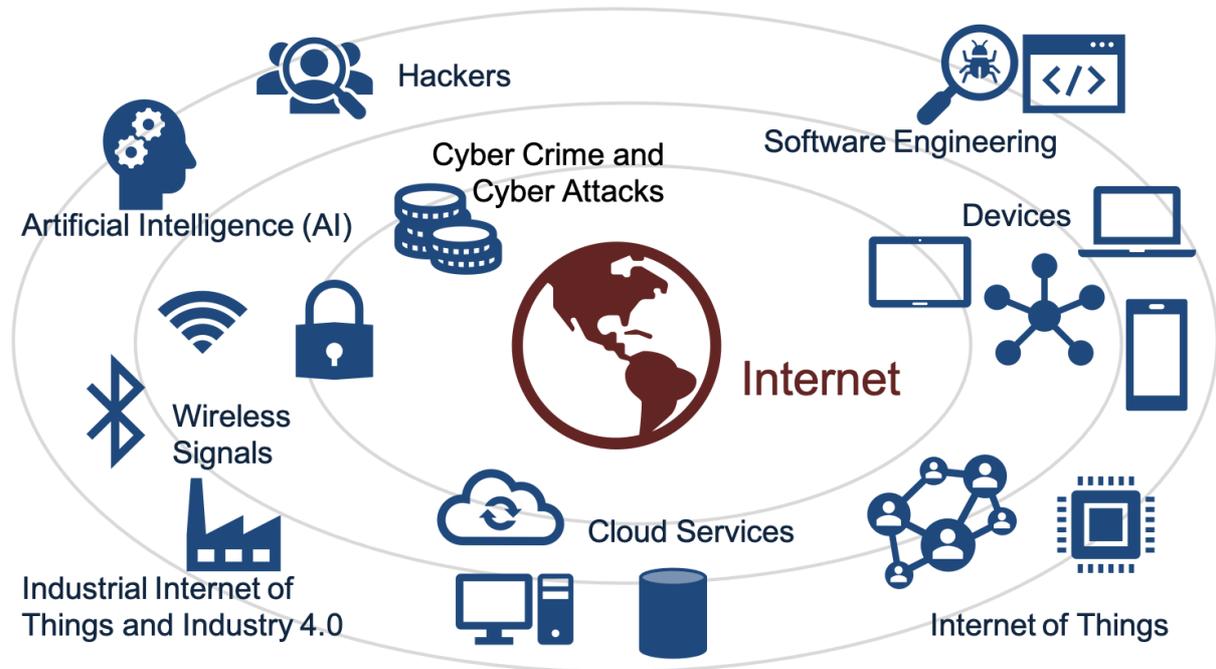


Figure 13-1: IoT and Cyber Security

13.1 Security of Things

Maintaining a high level of security is critical when transporting the data around the IoT network. Information transmitted through this network can be anything from temperature sensor data in production machines to patient data recorded by X-ray machines in hospitals.

Business-critical information is often collected and reported in a central database located somewhere in the cloud or a local data center. When we have IoT devices containing so much sensitive data, security is essential for developers who want to take advantage of the benefits offered by IoT technology.

14. Industrial Internet of Things and Industry 4.0

Industrial Internet of Things (IIoT) is another word for Industry 4.0. Security is crucial in IIoT applications.

IoT – Consumer oriented, Smart Home Solutions, etc.

IIoT – Industrial use of IoT Technology.

IoT often focuses on consumer-oriented products and solutions, while IIoT focuses industrial use of IoT technology.

More about: IEC 62443:

https://en.wikipedia.org/wiki/IEC_62443

14.1 Industry 4.0

Industry 4.0 is the new buzzword for the combination of industry, automation, and the current Internet of Things (IoT) technology.

IIoT – Industrial use of IoT Technology. Industrial Internet of Things (IIoT) is another word for Industry 4.0. You could say that IoT is consumer oriented with applications like Smart Home, Home Automation, etc., while IIoT has more industrial focus and applications.

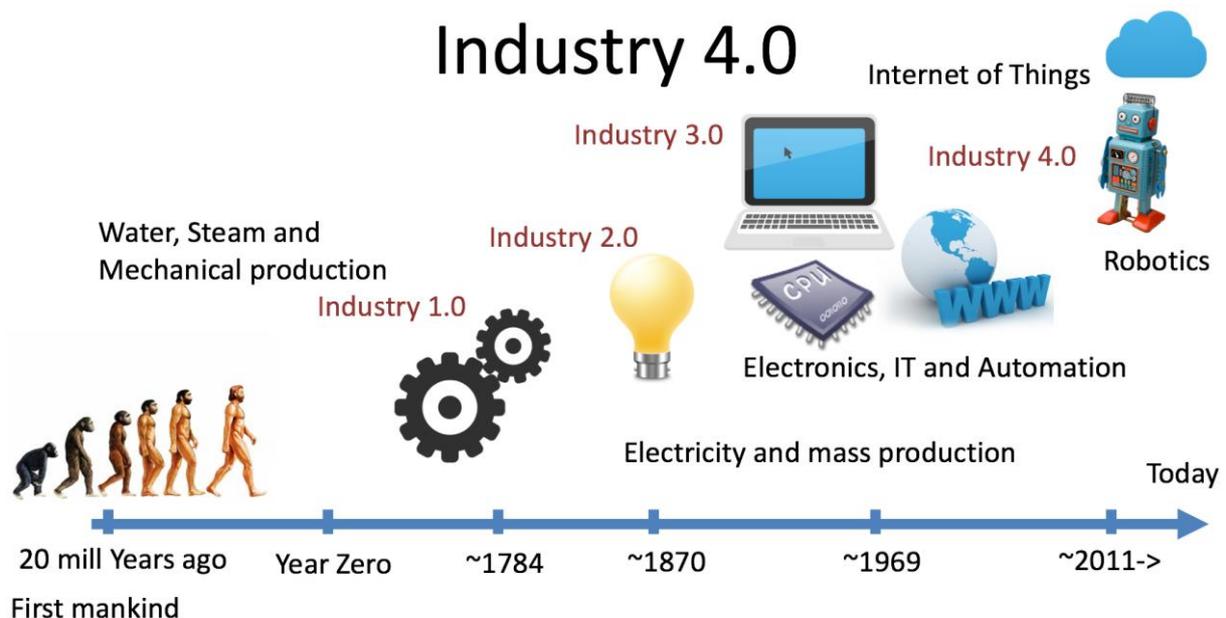


Figure 14-1: Industry 4.0

The term "Industrie 4.0" was first used in 2011 in Germany.

Industry 4.0 is also called the fourth industrial revolution, where:

- Industry 1.0: Mechanization of production using Water and Steam Power.
- Industry 2.0: Mass production with the help of Electric Power.
- Industry 3.0: The Digital Revolution. From Analog to Digital Devices and Signals. Use of Electronics and IT to further Automate Production.
- Industry 4.0 The combination of industry, automation, digitalization, and the current Internet of Things (IoT) technology.

Industry 4.0 is the "Next Generation Industry".

Focus on Next Generation Industry

We will learn the latest technology and terms used in the industry today and tomorrow

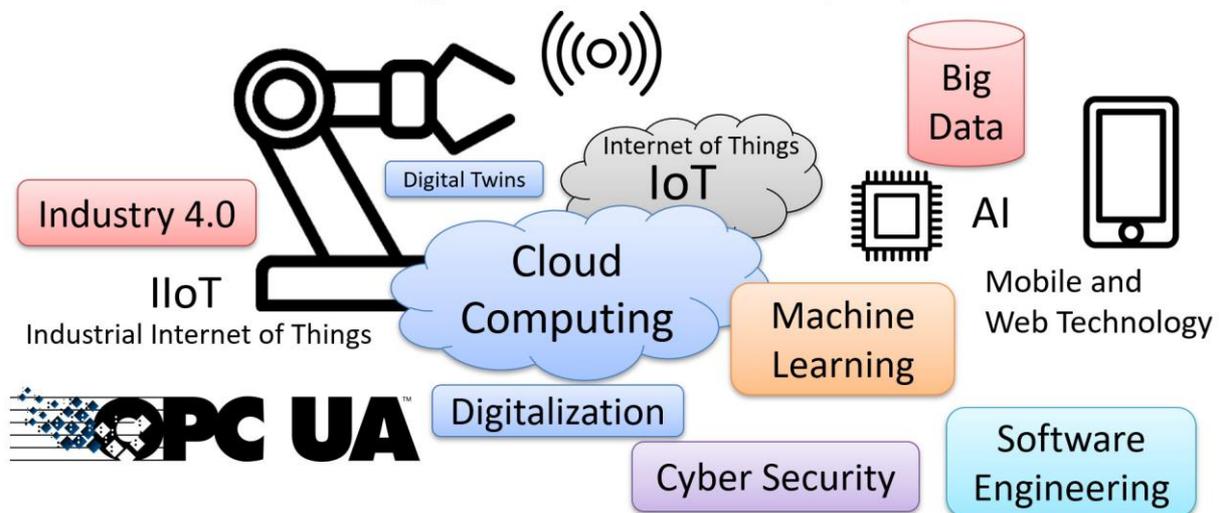


Figure 14-2: Next Generation Industry

Web:

<https://www.halvorsen.blog/documents/technology/industry40>

Video:

Industry 4.0 | <https://youtu.be/LeqKtr5Luv8>

14.2 SCADA Systems

SCADA (Supervisory Control and Data Acquisition) is a type of Industrial Control System (ICS). Industrial Control Systems (ICS) are computer-controlled systems that monitor and control industrial processes that exist in the physical world.

Industrial Control Systems, like PLC (Programmable Logic Controller), DCS (Distributed Control System) and SCADA (Supervisory Control and Data Acquisition) share many of the same features.

Next Generation Control and Automation Systems/SCADA systems are closely related to Industrial Internet of Things (IIoT) and Industry 4.0.

15. IEC 62443

IEC 62443 is an international series of standards on "Industrial communication networks - IT security for networks and systems". The standard is divided into different sections and describes both technical and process-related aspects of industrial cybersecurity.

A new standard in the series, is ISA-62443-4-2, which deals with Security for Industrial Automation and Control Systems.

References:

https://en.wikipedia.org/wiki/IEC_62443

Part 6 : Cloud Systems

An overview of Security in Database Systems.

16. Cloud Systems

Many Cloud Computing and Hosting Providers do exist today, such as Amazon Web Services (AWS), Google Cloud Platform (GCP) and Microsoft Azure.

Here you can rent Cloud based services like Virtual Machines (Computers with OS running in the Cloud), Web Server, Database Systems, etc. based on a monthly fee.

Web:

<https://www.halvorsen.blog/documents/technology/cloud/>

17. Microsoft Azure

With the product “Microsoft Azure” Microsoft is one of the largest cloud providers today.

You could say Microsoft Azure is "Windows running in the Cloud".

Video:

Microsoft Azure: <https://youtu.be/Ee8gANKc1Pc>

Part 7 : Database Systems

An overview of Security in Database Systems.

18. Database Systems

A Database is a structured way to store lots of information. The information is stored in different tables.

Some of the most popular Database Systems today are:

- SQL Server
- MySQL
- MariaDB

A database can be installed locally, on a server within a company or in a cloud platform.

We will take a closer look at SQL Server and the Cloud platform Microsoft Azure.

Resources:

Video:

Introduction to Database Systems: <https://youtu.be/n75iPNrzN-o>

Web:

<https://www.halvorsen.blog/documents/technology/database>

19. SQL Server

19.1 Introduction

SQL Server is a Database System from Microsoft. SQL Server comes in different editions, for basic, personal use

SQL Server Express is recommended because it is simple to use, and it is free.

Web:

https://www.halvorsen.blog/documents/technology/database/sql_server.php

Videos:

Introduction to SQL Server: <https://youtu.be/SIR4KOhAG1U>

SQL Server Express Installation: <https://youtu.be/hhhggAlUYo8>

19.2 Authentication

SQL Server has 2 different types of authentication:

- Windows Authentication
- SQL Server Authentication

Using "Windows Authentication" the Connection String looks like this:

```
DATA SOURCE=<SQL Server Name>;DATABASE=<Database Name>;Integrated Security = True;
```

Using "SQL Server Authentication" the Connection String looks like this:

```
DATA SOURCE=<SQL Server Name>;DATABASE=<Database Name>;UID=sa;PWD=<Your Password>;
```

Replace <SQL Server Name> with the name of your SQL Server, typically "<YourComputerName>\SQLEXPRESS" if you are using SQL Server Express.

UID is a SQL Server user, here you can create your own SQL Server user inside SQL Server Management Studio or use the built-in sa user (sa=System Administrator). During the setup of SQL Server, you need to select "Mixed Mode" and enter the password for your sa user.

It may look something like this:

```
DATA SOURCE=HPPCWORK\\SQLEXPRESS;DATABASE=MEASUREMENTS;UID=sa;PWD=Password123;
```

You can also turn on “SQL Server Authentication” in SQL Server Management Studio (SSMS) after installation of SQL Server. See Figure 19-1.

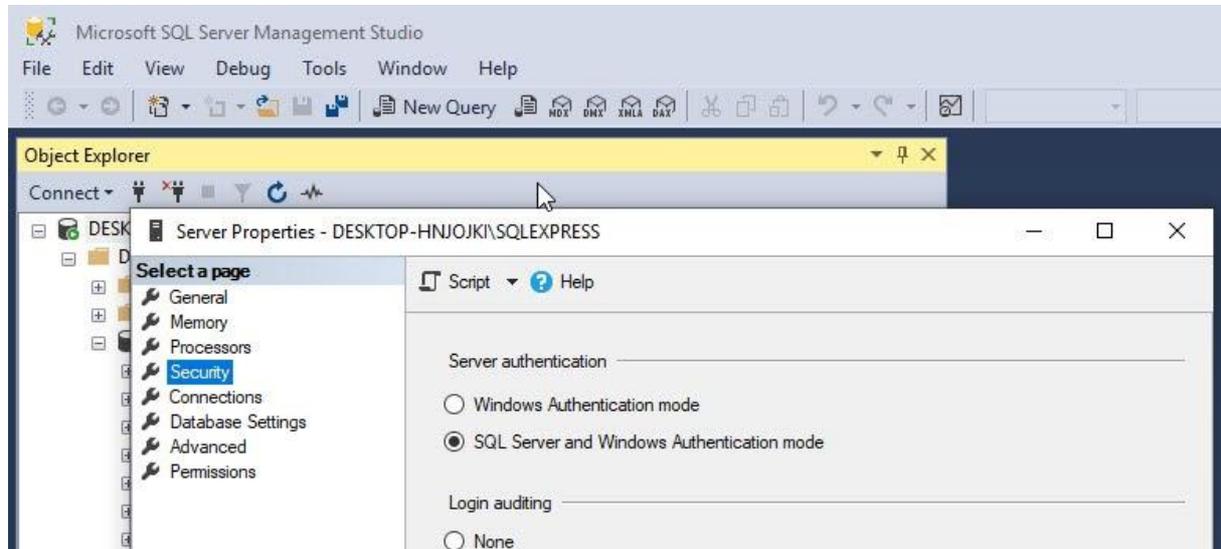


Figure 19-1: SQL Server Authentication

To change security authentication mode, do the following steps:

- In SQL Server Management Studio Object Explorer, right-click the server, and then click Properties.
- On the Security page, under Server authentication, select the new server authentication mode, and then click OK.
- In the SQL Server Management Studio dialog box, click OK to acknowledge the requirement to restart SQL Server.
- In Object Explorer, right-click your server, and then click Restart. If SQL Server Agent is running, it must also be restarted. Or just restart your computer.

19.3 Create Logins in SQL Server

“sa” (short for System Administrator) is a built-in Login in SQL Server. You can also create your own SQL Server Logins. Normally you should do that rather than using the “sa” login. “sa” have access to “everything” and in context of Data Security that is unfortunate. In general, you should make your own Logins that have access to only what is strictly necessary. See Figure 19-2.

Create Logins in SQL Server

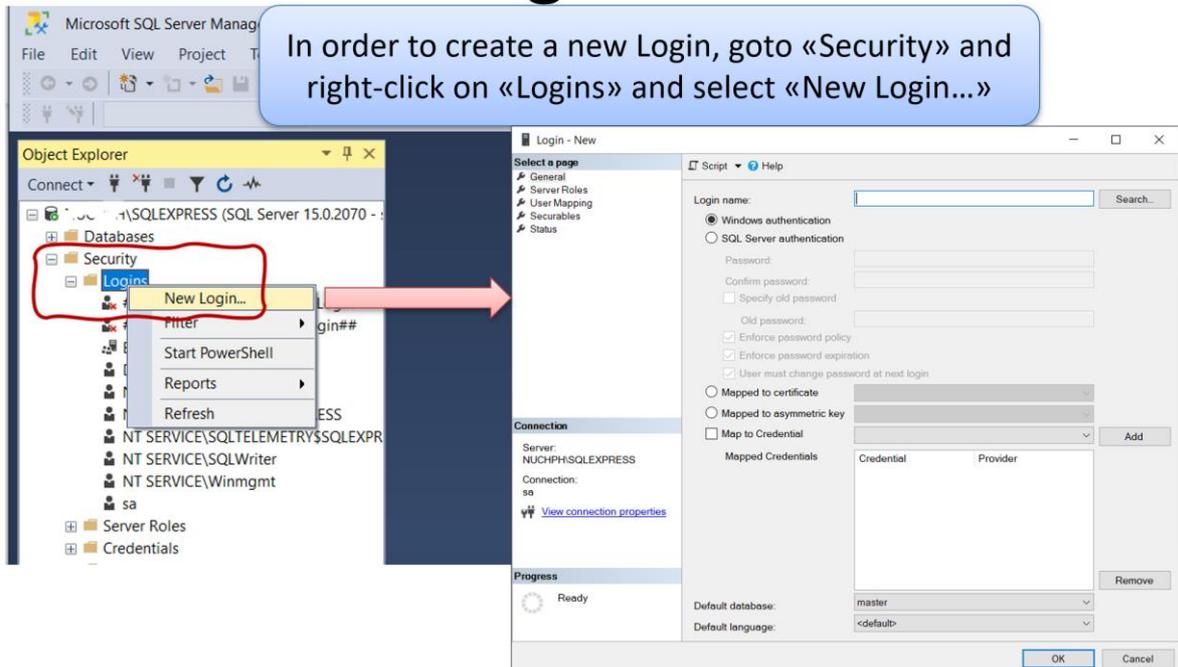


Figure 19-2: Create Logins in SQL Server

We can select login type, see Figure 19-3.

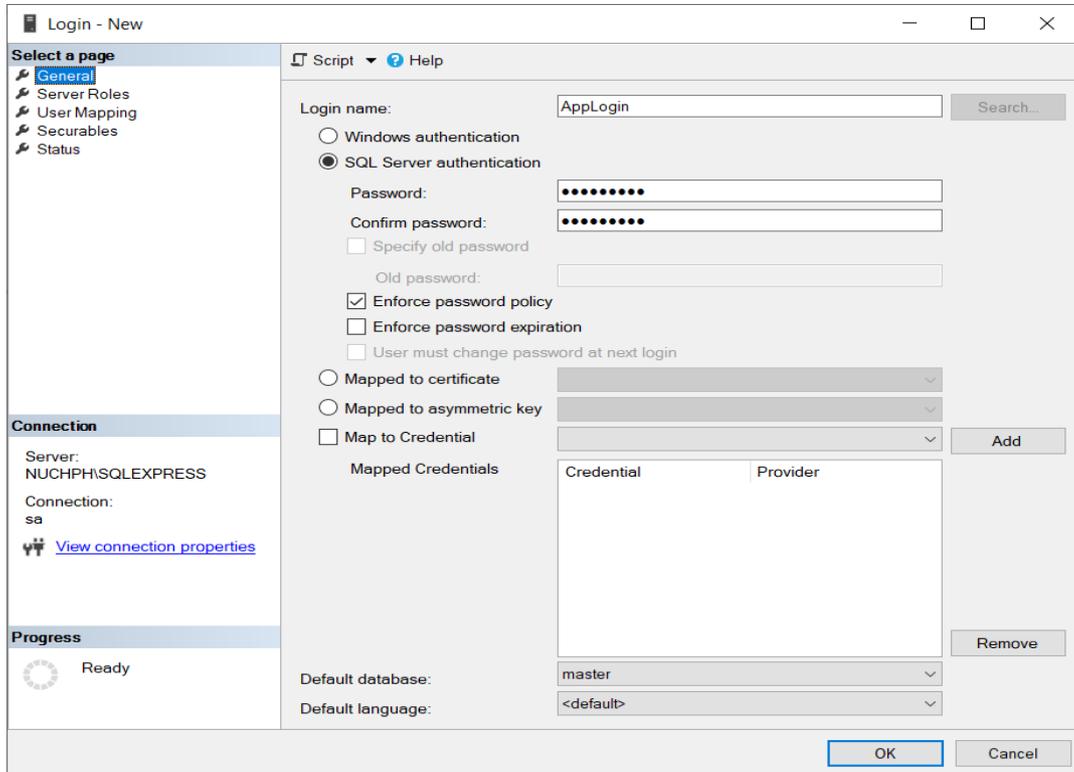


Figure 19-3: New Login

Select access levels, see Figure 19-4.

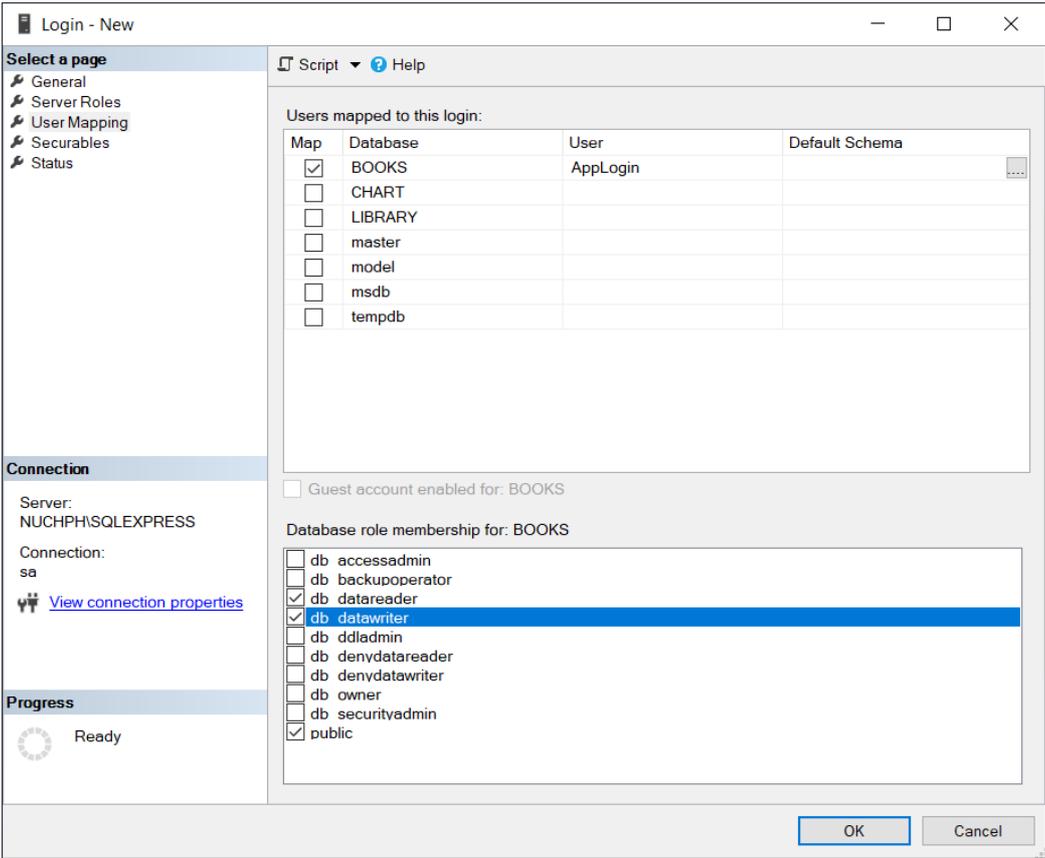


Figure 19-4: Login - Select Access Level

20. Microsoft Azure

Microsoft Azure is a Cloud Computing and Hosting Platform from Microsoft. You could say Microsoft Azure is "Windows running in the Cloud".

Videos:

Microsoft Azure: <https://youtu.be/Ee8gANKc1Pc>

ASP.NET Core - Azure Deployment: <https://youtu.be/xw1yNHWkKaw>

Part 8 : Web Platforms

An overview of Security in development and use of Web Technology.

21. Web Platforms

Today, almost everything is based on Internet and Web technology.

Web:

<https://www.halvorsen.blog/documents/programming/web/>

It all started with Internet (1960s) and the World Wide Web - WWW (1991). The first Web Browser, Netscape, came in 1994. This was the beginning of a new era, where everything is connected on internet, the so called Internet of Things (IoT).

Learning Web Technology is essential today because Internet has become the number one source to information, and many of the traditional software applications have become Web Applications. Web Applications have become more powerful and can fully replace desktop application in most situations.

That is why you need to know basic Web Programming, including HTML, CSS and JavaScript. To create more powerful Web Sites and Web Applications you also need to know about Web Servers, Database Systems and Web Frameworks like PHP, ASP.NET, etc.

Videos:

Web Programming Overview: <https://youtu.be/pIRBYKbQSuE>

Create Web Pages with HTML and CSS: <https://youtu.be/DUEHx7I5a3Y>

22. ASP.NET Core

ASP.NET is an open-source web framework, created by Microsoft, for building web apps and services using the .NET Framework or the .NET Core. We have both ASP.NET and ASP.NET Core. ASP.NET Core is the new approach built on .NET Core.

Below you find some useful ASP.NET resources for implementing database communication.

Web:

<https://www.halvorsen.blog/documents/programming/web/aspnet>

Videos:

ASP.NET Core - Hello World: <https://youtu.be/lcQsWYgQXK4>

ASP.NET Core – Introduction: <https://youtu.be/zkOtiBcwo8s>

ASP.NET Core - Database Communication: <https://youtu.be/0Ta3dQ3rxzs>

ASP.NET Core - Database CRUD Application: <https://youtu.be/k5TCZDwTYcE>

23. PHP

PHP is a server-side scripting language for web development. It is used to make dynamic and interactive web pages. PHP is an old and well-known technology, but it is still very popular and easy to learn. PHP is open source (free) and cross-platform. Especially, the combination of PHP and MySQL is a powerful combination used to create rich, dynamic web pages.

Part 9 : ASP.NET Core

An overview of the ASP.NET Core Web Development Framework with respect to
Development of Secure Web Applications

24. Introduction to ASP.NET Core

Textbook:

Web Programming | ASP.NET Core

<https://halvorsen.blog/documents/programming/web/aspnet>

Videos:

ASP.NET Core - Introduction | <https://youtu.be/zkOtiBcwo8s>

25. User Identity and Login

25.1 Introduction

Here we will see how user identity and login features can be implemented in modern web applications. The concepts will be exemplified using web technology and the ASP.NET Core web framework from Microsoft.

In this chapter we will see how we can create and use login functionality in your ASP.NET Core Web Applications.

Typically, you need to create functionality for User Registration, Login, etc. Here you will see how this can be done from scratch. If you do it from scratch, you will have full control of your code.

For more details, please see the following:

<https://halvorsen.blog/documents/programming/web/aspnet>

If you use something called "ASP.NET Core Identity" (which will be explained and demonstrated in the next chapter) lots of "magic" happens behind the curtains. If something not working, it may be more complicated to figure out why.

25.2 Microsoft.AspNetCore.Identity

This Namespace contains different Classes and Methods for Identity handling. We will use the **PasswordHasher<TUser>** Class.

25.2.1 PasswordHasher<TUser> Class

Namespace: Microsoft.AspNetCore.Identity

2 important Methods:

- **HashPassword**(TUser, String)

Returns a hashed representation of the supplied password for the specified user.

- **VerifyHashedPassword**(TUser, String, String)

Returns a PasswordVerificationResult indicating the result of a password hash comparison.

Example:

```
using Microsoft.AspNetCore.Identity;
...
string username; //UserName given by user when creating a User
```

```
string passwordHashed;

PasswordHasher<string> pw = new PasswordHasher<string>();

passwordHashed = pw.HashPassword(userName, password);
```

25.3 Session State in ASP.NET Core

We need to store information whether the User is logged in or not. We can use Session variables to share that information between multiple web pages.

Session management in ASP.NET Core is not enabled by default.

- You need to install the **Microsoft.AspNetCore.Session** NuGet Package in order to use Session state.
- You need to **enable Session State** in the **Startup.cs** file
- You need to include the Namespace using **Microsoft.AspNetCore.Http**;

25.4 Demo Application

Here we will demonstrate how we can create a web application (see Figure 25-1) with “Login”, including “Create New User”, “Update User Information”.

Figure 25-1 shows the main page of the “Login” application.

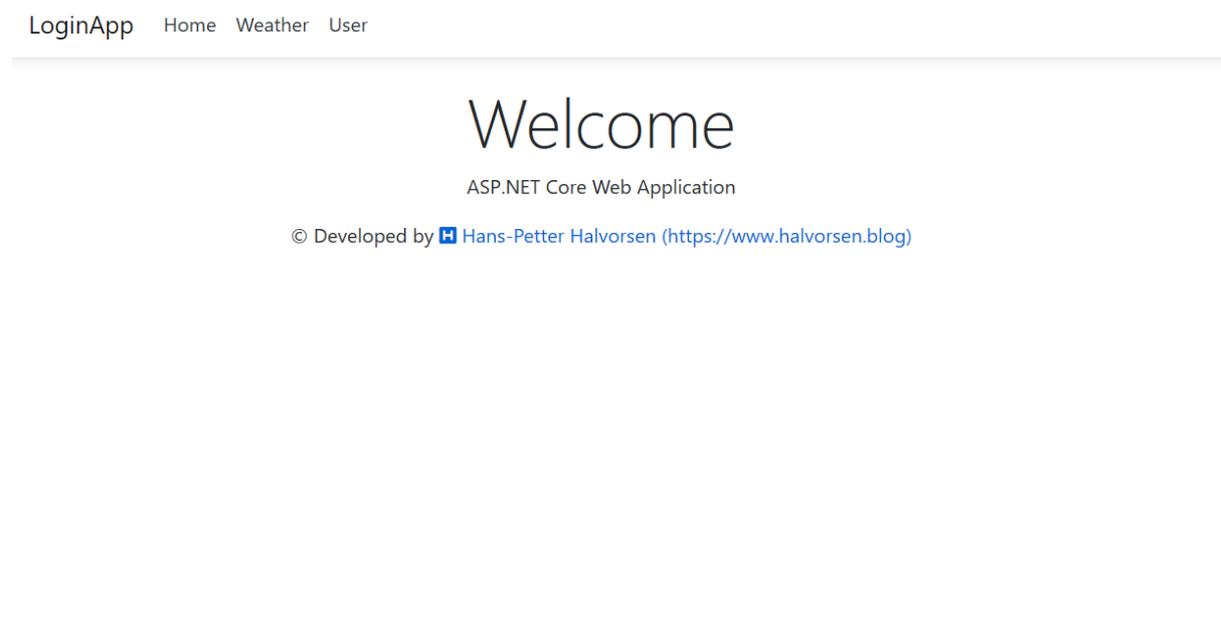


Figure 25-1: Login App - Welcome Web Page

...

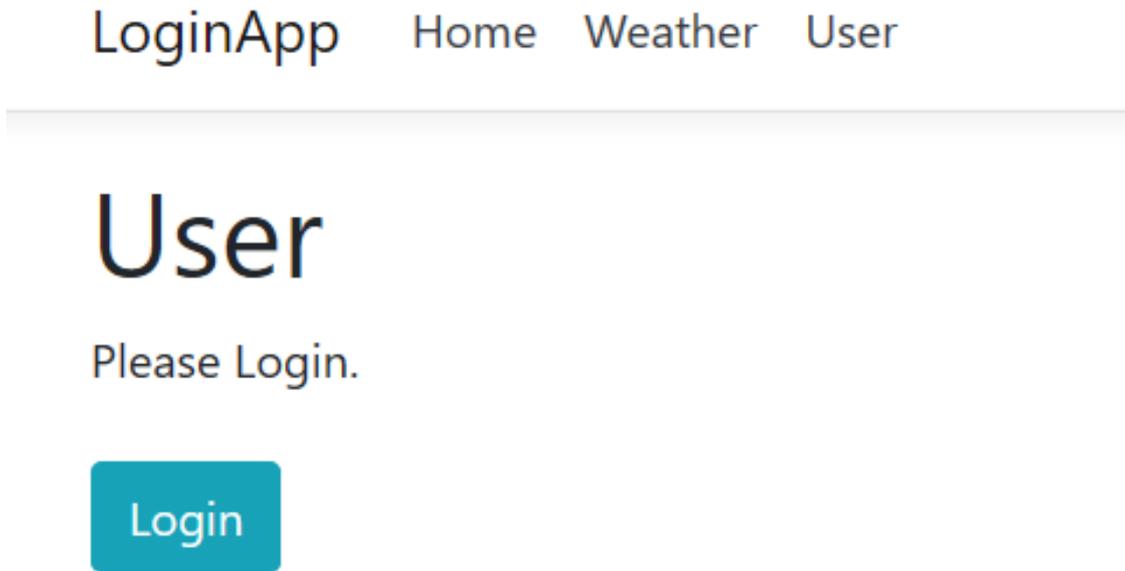


Figure 25-2: User needs to Login before he can see Information

25.4.1 Login

See Figure 25-3.

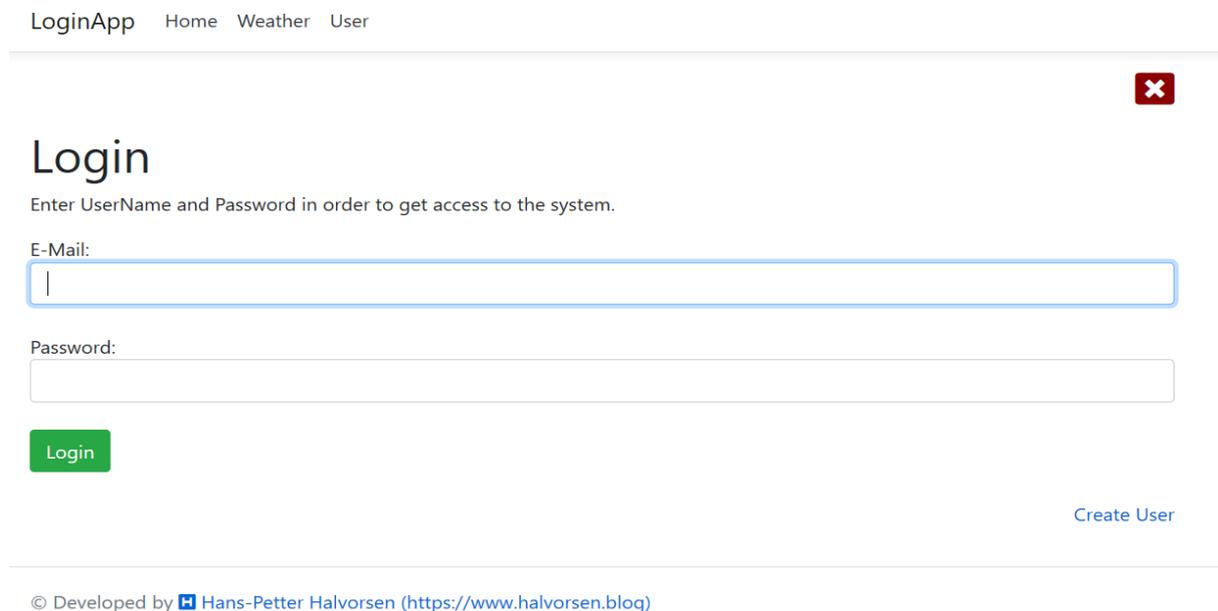


Figure 25-3: Login Web Page

25.4.2 Create User

See Figure 25-4.

LoginApp Home Weather User



Create User

The Password will be hashed before it is stored in the database. This means that no one can find your password even if the database was hacked.

Name:

E-Mail:

Password:

© Developed by  [Hans-Petter Halvorsen \(https://www.halvorsen.blog\)](https://www.halvorsen.blog)

Figure 25-4: Create User Web Page

25.4.3 Update User Information

See Figure 25-5.

LoginApp Home Weather User



Update User Information

Name:

E-Mail:

Password:

The Password will be hashed before it is stored in the database. This means that no one can find your password even if the database was hacked.

Figure 25-5: Update User Information Web Page

25.4.4 More Features

The web application presented is very basic and only to illustrate the basic principles.

All modern systems offer what we call “2 Factor Authentication”. This means in addition to enter the password, the user needs to enter a one-time password received on E-Mail or SMS.

An alternative is to use an Authenticator App like “Google Authenticator” or “Microsoft Authenticator” available on iPhone and Android.

Another basic feature is “Forgot Password?”. Today we have lots of accounts on different systems. It is recommended that we use different Passwords for these accounts, and it is easy to forget the password for one or more of these accounts. Because of that we need to have “Forgot Password” functionality. This means that the user needs to enter his e-mail address and then the system should send an email (or SMS or similar) with a new temporary Password that the user needs to change once he is able to logon to the system again.

To increase security, it is also normal to have some kind of keyword (what is your nickname? what is your favorite pet?, etc.) that the user needs to remember before he can receive a new password.

26. ASP.NET Core Identity

26.1 Introduction

We will use ASP.NET Core Identity for creating an Application with built-in Authentication that has the following features:

- User Registration
- User Login
- Check if User is Authenticated/Logged into your Application
- 2FA

ASP.NET Core Identity is an API that supports user interface (UI) login functionality out of the box. You can manage users, passwords, roles, email confirmation, 2FA, and more.

Users can create an account with the login information stored in Identity or they can use an external login provider.

Supported external login providers include Facebook, Google, Microsoft Account, and Twitter.

ASP.NET Core Identity offers GUI for creating Users and User Login, 2FA, etc. If you need to change the layout and behaviors of those “out of the box” provided GUIs, you need to use “Scaffolding”. Scaffolding is explained below in more detail.

26.1.1 Scaffold Identity in ASP.NET Core Projects

What is Scaffolding?

In general, Scaffolding, also called scaffold or staging is a temporary structure used to support a work crew and materials to aid in the construction, maintenance, and repair of buildings, etc.

<https://en.wikipedia.org/wiki/Scaffolding>

Scaffolding, as used in computing, refers to one of two techniques: The first is a code generation technique related to database access in some model–view–controller frameworks; the second is a project generation technique supported by various tools.

[https://en.wikipedia.org/wiki/Scaffold_\(programming\)](https://en.wikipedia.org/wiki/Scaffold_(programming))

Scaffold Identity in ASP.NET Core Projects

Applications that include Identity can apply the scaffolder to selectively add the source code contained in the Identity Razor Class Library (RCL).

You might want to generate source code so you can modify the code and change the behavior. For example, you could instruct the scaffolder to generate the code used in login or registration.

Generated code takes precedence over the same code in the Identity RCL.

26.2 Demo Application

Below an ASP.NET Core Web Application implementing and using ASP.NET Core Identity will be presented.

26.2.1 Create Project in Visual Studio with Identity Enabled

We start by creating an ordinary ASP.NET Core Web Application, see Figure 26-1.

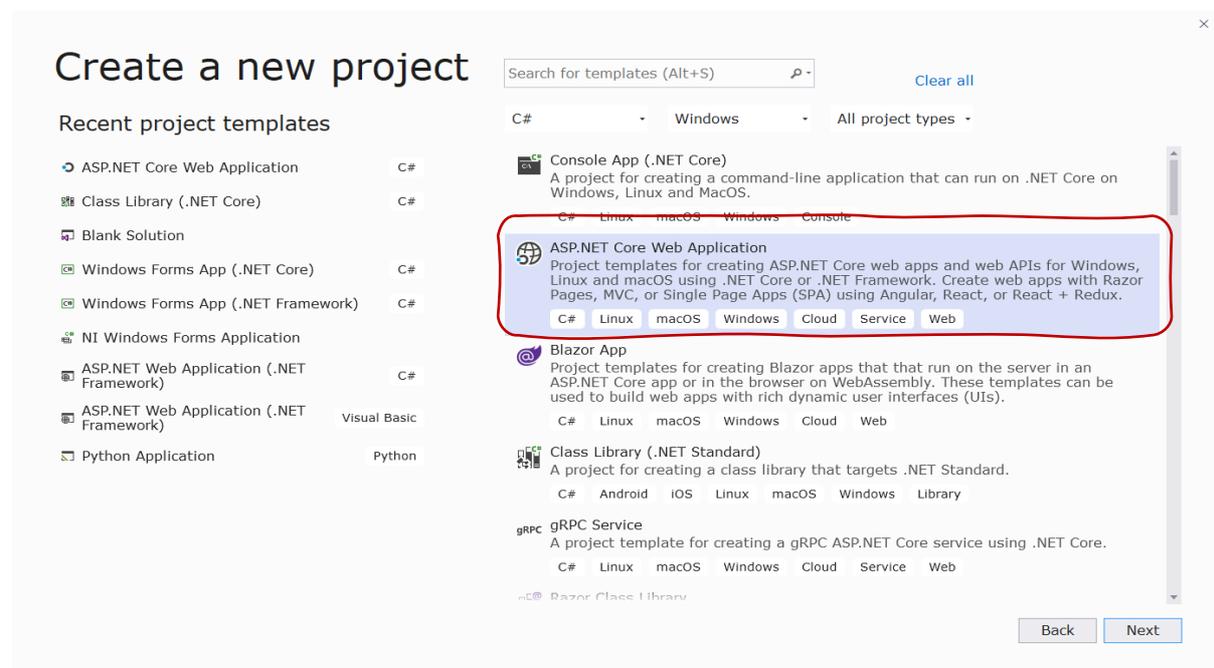


Figure 26-1: ASP.NET Core Web Application Template

Select Authentication:

Then, in the next window (see Figure 26-2) you need to select "Authentication".

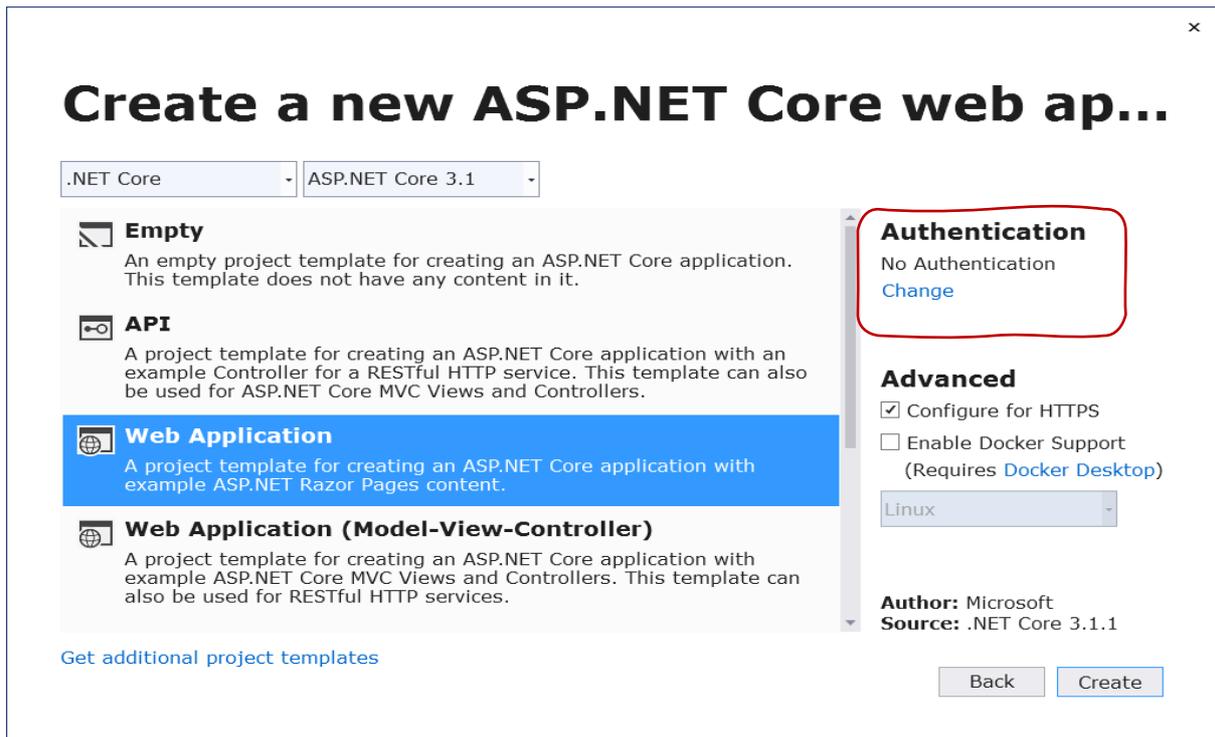


Figure 26-2: Select Authentication in ASP.NET

Change Authentication:

When you click “Authentication” in Figure 26-2, the “Change Authentication” window appears (see Figure 26-3). Here you then should typically select “Individual User Accounts”.

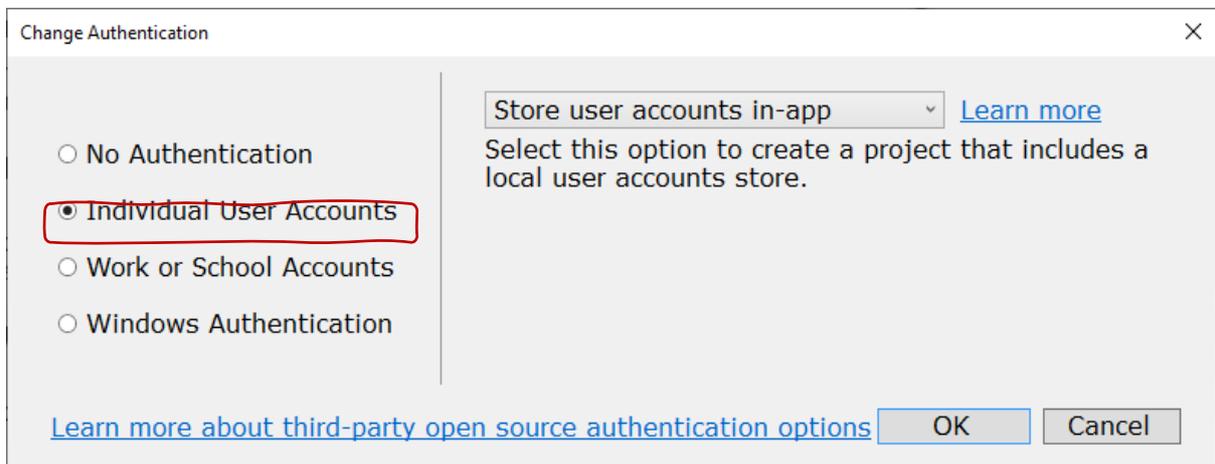


Figure 26-3: Change Authentication

Solution Explorer:

When you have selected proper authentication, your project and files will be created for you, see Figure 26-4. Lots of new stuff has been created for us that are used by the Identity features we have enabled.

26.2.3 Register New Account and Log In

Create New Account:

IdentityApp Home Privacy Register Login

Register

Create a new account. Use another service to register.

Email

Password

Confirm password

© 2020 - IdentityApp - [Privacy](#)

There are no external authentication services configured. See [this article](#) for details on setting up this ASP.NET application to support logging in via external services.

Figure 26-7: Create New Account

Confirm Registration:

IdentityApp Home Privacy Register Login

Register confirmation

This app does not currently have a real email sender registered, see [these docs](#) for how to configure a real email sender. Normally this would be emailed: [Click here to confirm your account](#)

© 2020 - IdentityApp - [Privacy](#)

Figure 26-8: Confirm Registration

Login:

IdentityApp [Home](#) [Privacy](#) [Register](#) [Login](#)

Log in

Use a local account to log in.

Email

Password

Remember me?

[Log in](#)

[Forgot your password?](#)

[Register as a new user](#)

Use another service to log in.

There are no external authentication services configured. See [this article](#) for details on setting up this ASP.NET application to support logging in via external services.

Figure 26-9: Login

IdentityApp [Home](#) [Privacy](#) Hello [hans.p.halvorsen@usn.no!](#) [Logout](#)

Welcome

Learn about [building Web apps with ASP.NET Core](#).

© 2020 - IdentityApp - [Privacy](#)

Figure 26-10: You are Logged In

Manage your Account:

Manage your account

Change your account settings

Profile

Email

Password

Two-factor authentication

Personal data

Profile

Thank you for confirming your email. ×

Username

hans.p.halvorsen@usn.no

Phone number

Save

Figure 26-11: Manage your Account

26.2.4 2 Factor Authentication

All modern systems offer what we call “2 Factor Authentication”, or 2FA.

This means in addition to enter the password, the user needs to enter a one-time password received on E-Mail or SMS.

An alternative is to use an Authenticator App like “Google Authenticator” or “Microsoft Authenticator” available on iPhone and Android.

Start using 2FA:

Manage your account

Change your account settings

Profile

Email

Password

Two-factor authentication

Personal data

Configure authenticator app

To use an authenticator app go through the following steps:

1. Download a two-factor authenticator app like Microsoft Authenticator for [Android](#) and [iOS](#) or Google Authenticator for [Android](#) and [iOS](#).

2. Scan the QR Code or enter this key  into your two factor authenticator app. Spaces and casing do not matter.

[Learn how to enable QR code generation.](#)

3. Once you have scanned the QR code or input the key above, your two factor authentication app will provide you with a unique code. Enter the code in the confirmation box below.

Verification Code

Verify

Figure 26-12: Configure 2FA

...

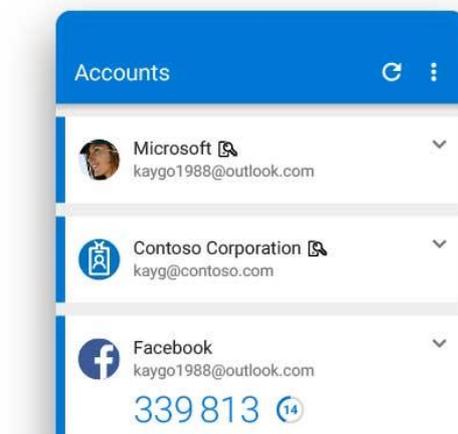


Figure 26-13: Microsoft Authenticator App for 2FA

Microsoft Authenticator App

<https://www.microsoft.com/en-us/account/authenticator>

Log In using 2FA:

Enter Code from Authentication App

Two-factor authentication

Your login is protected with an authenticator app. Enter your authenticator code below.

Authenticator code

Remember this machine

Log in

Don't have access to your authenticator device? You can [log in with a recovery code](#).

Figure 26-14: Log In using 2FA

26.2.5 Start Creating your Application

When the Identity features are installed, configured, and set up, you can start creating the rest of your application.

Typically, you need to check in your different web pages if the user is logged in (authenticated) or not.

@User.Identity

Typically, you want to use the following:

- @User.Identity.IsAuthenticated
- @User.Identity.Name

Check if you are Logged In or not in your Code:

Welcome

ASP.NET Core Identity Example Application

Is Authenticated: False

UserName:

Figure 26-15: Check if you are Logged In or not in your Code

Welcome

ASP.NET Core Identity Example Application

Is Authenticated: True

UserName: hans.p.halvorsen@usn.no

Figure 26-16: User are Logged In

Razor Code:

```
@page
@model IndexModel
@{
    ViewData["Title"] = "Home page";
}
<div>
```

```

<h1>Welcome</h1>
<p>ASP.NET Core Identity Example Application</p>
<p>Is Authenticated: @User.Identity.IsAuthenticated</p>
<p>UserName: @User.Identity.Name</p>
</div>

```

Typically, we want to use “@User.Identity.IsAuthenticated” for checking if Logged In or not and then show, e.g., data from the database, if the user are logged in.

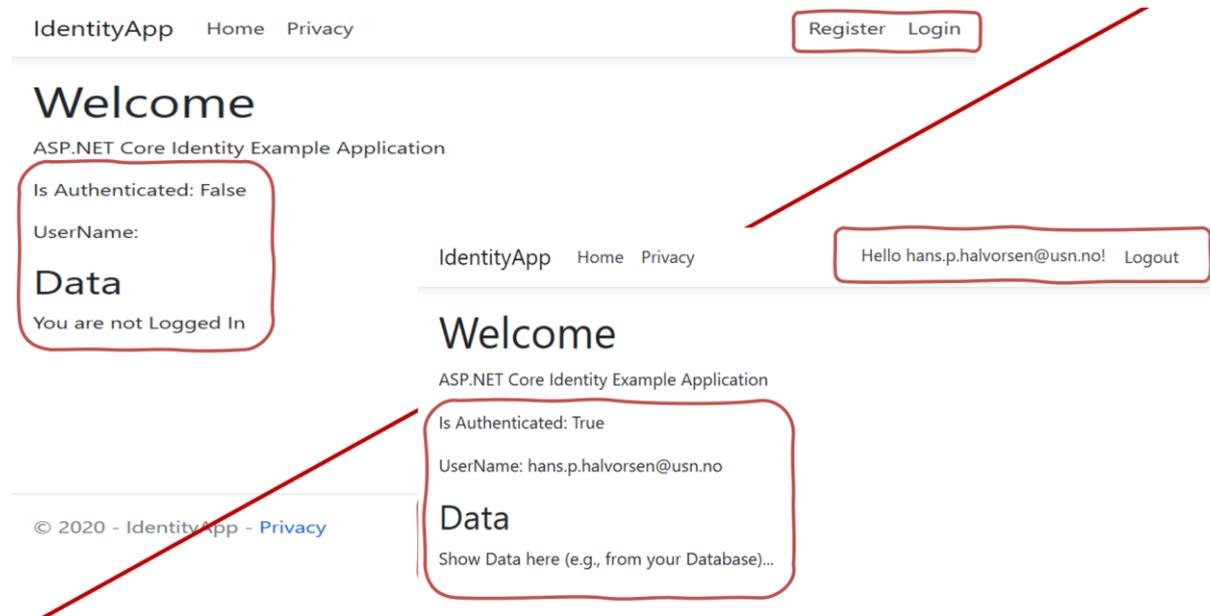


Figure 26-17: Authenticated/Not Authenticated

Razor Code:

```

<div>
  <h2>Data</h2>
  @if (User.Identity.IsAuthenticated)
  {
    <p>Show Data here (e.g., from your Database)...</p>
  }
  else
  {
    <p>You are not Logged In</p>
  }
</div>

```

26.2.6 Scaffolding

If you are not happy with the default Layout of the different Identity web pages (Register, Login, etc.) You can override the default Scaffolding and modify these web pages, so they fit your needs.

Scaffold Identity in ASP.NET Core Projects:

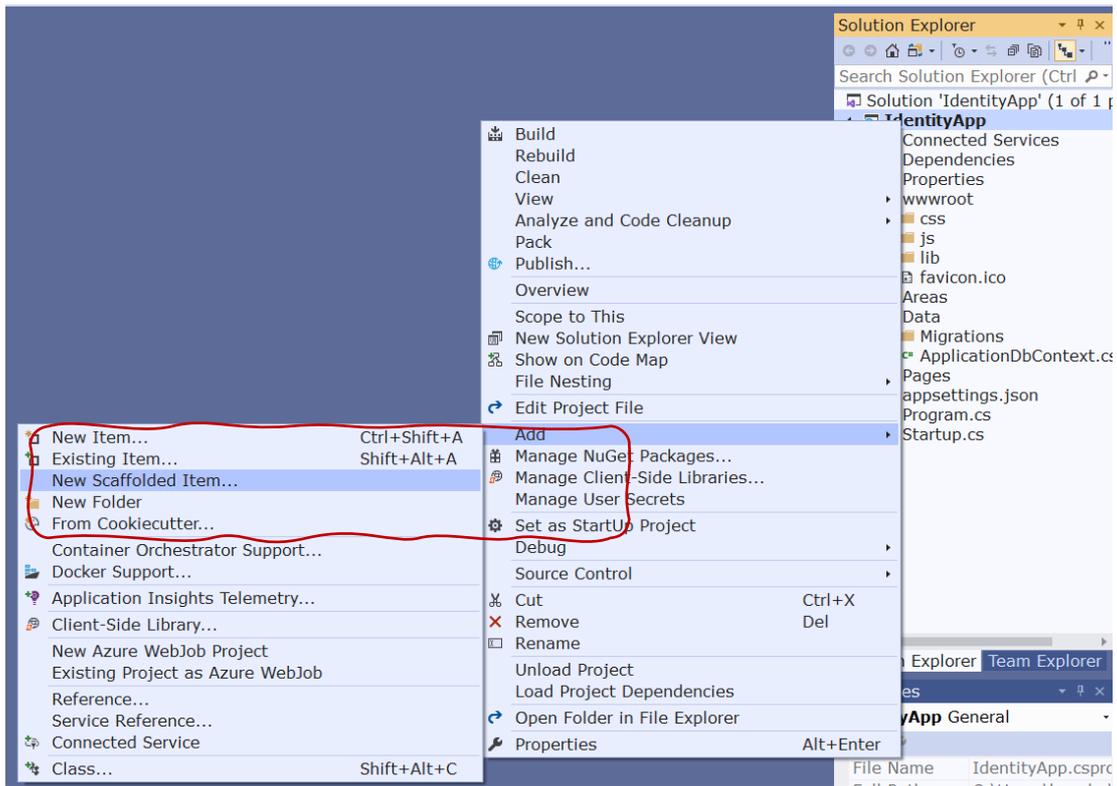


Figure 26-18: Scaffolding

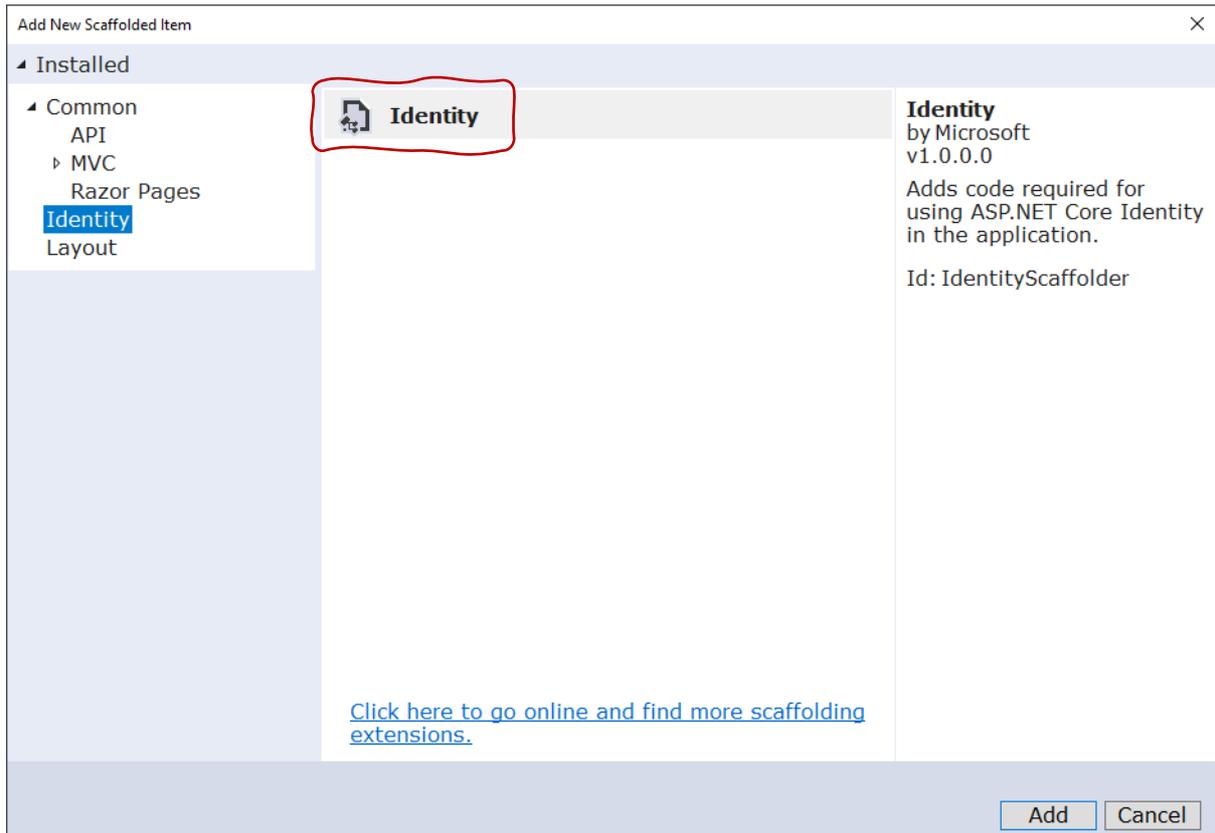


Figure 26-19: Add New Scaffolding Item

Select the Identity page(s) you want to override:

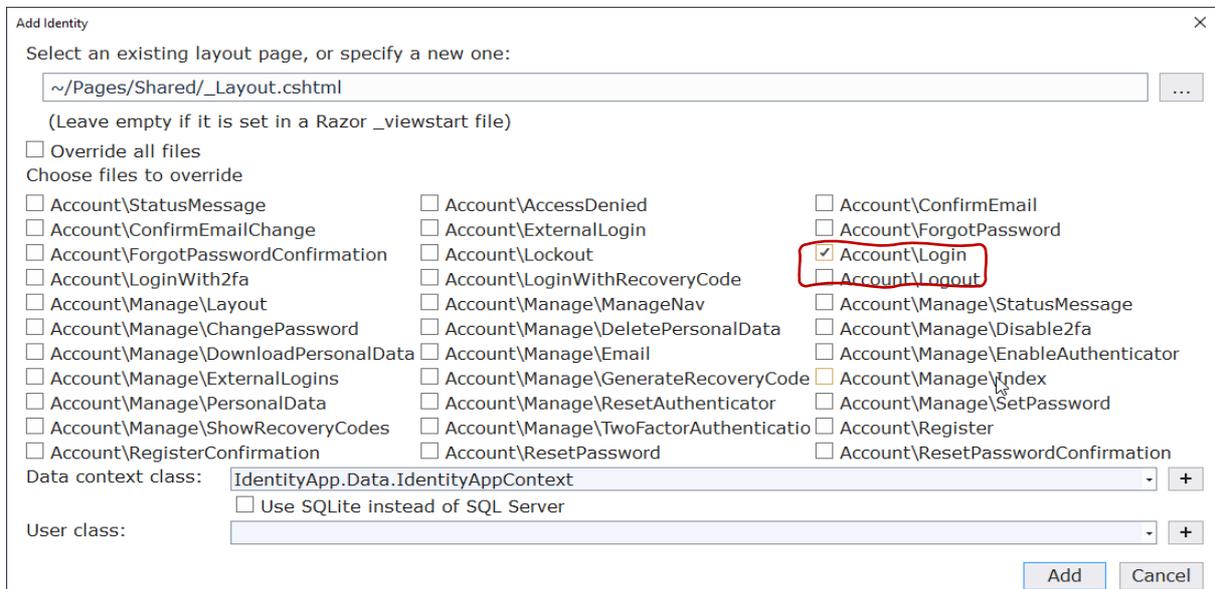


Figure 26-20: Overriding

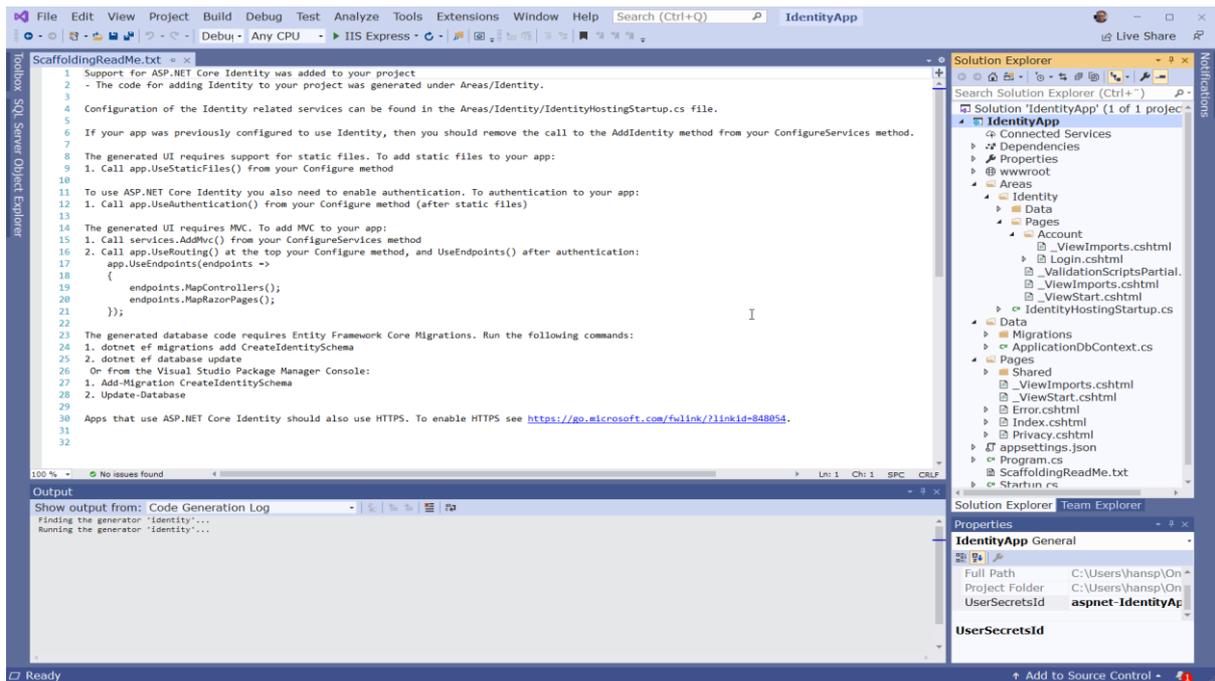


Figure 26-21: Solution Explorer

Existing Login.cshtml:

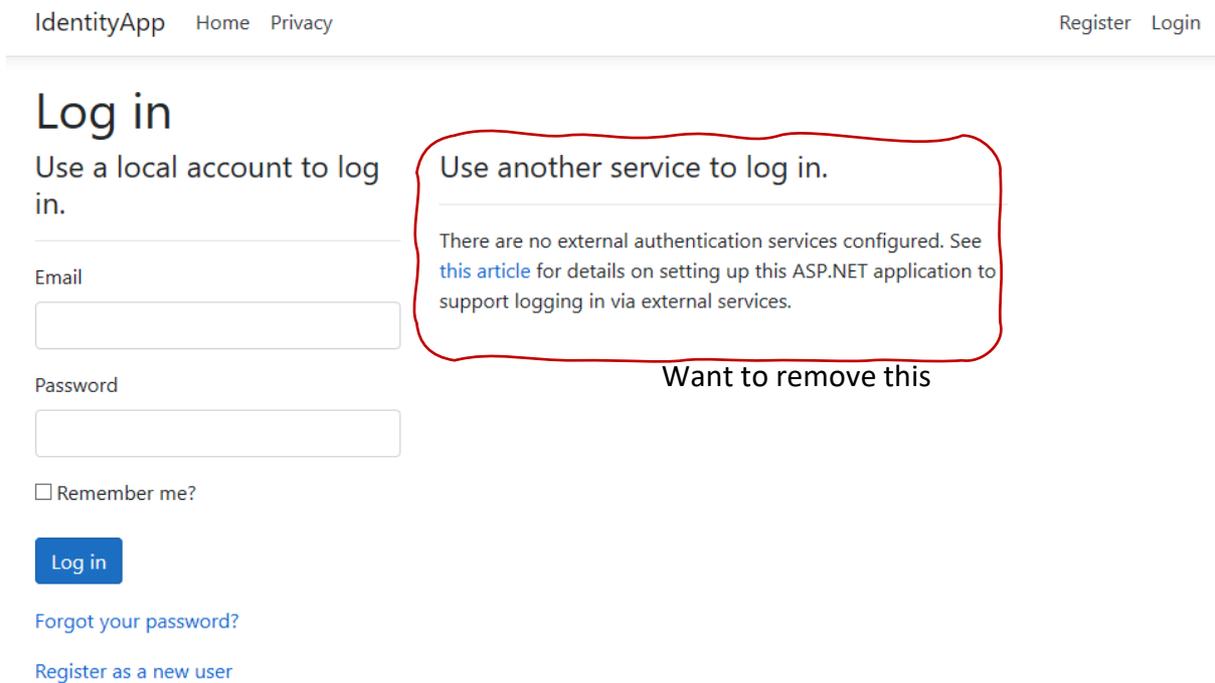


Figure 26-22: Login Page

Updated Login.cshtml:

Log in

Use a local account to log in.

Email

Password

Remember me?

Log in

[Forgot your password?](#)

[Register as a new user](#)

Figure 26-23: Updated Login Page

26.3 Additional Resources

Here are some additional resources if you want to dig deeper into ASP.NET Core Identity:

- Introduction to Identity on ASP.NET Core: <https://docs.microsoft.com/en-us/aspnet/core/security/authentication/identity>
- Scaffold Identity in ASP.NET Core projects: <https://docs.microsoft.com/en-us/aspnet/core/security/authentication/scaffold-identity>

Account confirmation and password recovery in ASP.NET Core:

<https://docs.microsoft.com/en-us/aspnet/core/security/authentication/acconfirm>

Part 10 : Software Security Testing

An overview of Software Security Testing.

27. Software Security Testing

27.1 Introduction

Penetration Testing

27.2 Test Standards

ISO/IEC 27001

27.2.1 ISO/IEC 27001

ISO/IEC 27001 provides requirements for information security management system (ISMS). An ISMS is a systematic approach to managing sensitive company information so that it remains secure.

27.3 Test Tools

27.4 OWASP

The Open Web Application Security Project (OWASP) is an organization focused on improving the security of software.

Web Site:

<https://www.owasp.org>

27.5 Test Platforms

28. OWASP

The Open Web Application Security Project (OWASP) is an organization focused on improving the security of software.

Web Site:

<https://www.owasp.org>

Part 11 : Machine Learning and Artificial Intelligence

Machine Learning and Artificial Intelligence are increasingly used both by hackers and by those who wants to prevent cyber-attacks

29. Introduction

Machine Learning and Artificial Intelligence are increasingly used both by hackers and by those who want to prevent cyber-attacks.

References

- Cyber Security: <https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html>
- Data Security: https://en.wikipedia.org/wiki/Data_security
- GDPR: <https://gdpr-info.eu>
- GDPR - Wikipedia: https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
- What is Cyber Security? <https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html>
- MitM: https://en.wikipedia.org/wiki/Man-in-the-middle_attack
- Eavesdropping: <https://en.wikipedia.org/wiki/Eavesdropping>
- WannaCry: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
- Introduction to Identity on ASP.NET Core: <https://docs.microsoft.com/en-us/aspnet/core/security/authentication/identity>
- Scaffold Identity in ASP.NET Core projects: <https://docs.microsoft.com/en-us/aspnet/core/security/authentication/scaffold-identity>
- Account confirmation and password recovery in ASP.NET Core: <https://docs.microsoft.com/en-us/aspnet/core/security/authentication/acconfirm>



Cyber Security