Co-funded by the Erasmus+ Programme of the European Union

Data protection: Passwords
Ochrona danych: hasła

English	Polski
Data Access	**Dostęp do danych**
When you store information electronically you are leaving information on resources that are easily accessible. Restricting access to non-authorised persons is vital when it comes to your data. It does not really matter what data you store, what is important is that access to the information is only granted to you (or whoever is supposed to have access). The authentication mechanism works based on 3 (most usually) elements - A user identification or piece of information that will identify the user as part of the system to access. This is usually referred to as the login or user id. It is also common to have the email of the user substitute a login due to the uniqueness of this information. - A user secret value or key (commonly referred to as password) that is used to authenticate the person attempting access. - An algorithm that somehow combines the user id with the password and produces a unique piece of information (that no other combination can produce). This information is stored in the protecting entity database and is used to verify the identity of the person attempting access. Here is how it works. When the original user created the account they selected (or were assigned) a user name and a password. The algorithm generated the unique value and it was stored. Later, for the user to gain access, they need to enter their user id and password. The protecting entity reads in the information and, using the algorithm, generates a unique value. The generated unique value is then compared with the unique value stored in the database. If the two values match, the user is authenticated and access is granted. If the two values do not match then access is denied.	Kiedy przechowujesz informacje w formie elektronicznej, pozostawiasz informacje o zasobach, które są łatwo dostępne. Ograniczenie dostępu osobom nieupoważnionym jest niezbędne, jeśli chodzi o Twoje dane. Nie ma znaczenia, jakie dane przechowujesz, ważne jest to, że dostęp do informacji masz tylko Ty (lub ktokolwiek ma mieć dostęp). Mechanizm uwierzytelniania najczęściej działa w oparciu o 3 elementy: - Identyfikacja użytkownika lub informacja, która będzie identyfikować użytkownika jako część systemu do dostępu. Jest to zwykle określane jako login lub identyfikator użytkownika. Często zdarza się, że e-mail użytkownika zastępuje login ze względu na wyjątkowość tych informacji. - Tajna wartość lub klucz użytkownika (powszechnie nazywany hasłem) używany do uwierzytelniania osoby próbującej uzyskać dostęp. - Algorytm, który w jakiś sposób łączy identyfikator użytkownika z hasłem i generuje unikalną informację (której nie da żadna inna kombinacja). Informacje te są przechowywane w bazie danych podmiotów chronionych i służą do weryfikacji tożsamości osoby próbującej uzyskać dostęp. Oto jak to działa. Kiedy pierwotny użytkownik utworzył konto, wybrał (lub został przypisany) nazwę użytkownika i hasło. Algorytm wygenerował unikalną wartość, została ona zapisana. Później, aby użytkownik uzyskał dostęp, musi wprowadzić swój identyfikator użytkownika i hasło. Jednostka zabezpieczająca wczytuje informacje i za pomocą algorytmu generuje unikalną wartość. Wygenerowana unikalna wartość jest następnie porównywana z unikalną wartością przechowywaną w bazie danych. Jeśli te dwie wartości są zgodne, użytkownik jest uwierzytelniany i udzielany jest mu dostęp. Jeśli te dwie wartości nie są zgodne, następuje odmowa dostępu.
The importance of the password	**Znaczenie hasła**
In everyday usage of technology we have to authenticate ourselves in order to gain access to our data. Unlocking your mobile phone (code, fingerprint, and face recognition); logging onto windows (code,	W codziennym korzystaniu z technologii musimy się uwierzytelniać, aby uzyskać dostęp do naszych danych. Odblokowywanie telefonu komórkowego (kod, odcisk palca i rozpoznawanie twarzy); logowanie do okien

fingerprint scan); accessing online banking (code, 2-way verification); we are entering password after password in order to open machines, start applications or access services and/or resources. Choosing, using and safely keeping your multiple passwords is very important.	(kod, skan linii papilarnych); dostęp do bankowości internetowej (kod, weryfikacja dwukierunkowa); wprowadzamy hasło za hasłem w celu otwierania maszyn, uruchamiania aplikacji lub dostępu do usługi/ lub zasobów. Wybór, używanie i bezpieczne przechowywanie wielu haseł jest bardzo ważne.
<u>Choosing a password</u>	<u>Wybór hasła</u>
Many systems can generate and supply a password (usually difficult to remember) or they will allow you to select your own but can request that the selected password must meet certain requirements. Usual restrictions include: - Length of the password. The longer the password the more difficult it is to guess. A usual restriction is a minimum of 8 characters - Including lower as well as uppercase letters. Passwords are **always** case sensitive so using lowercase and uppercase complicates the password more - Including at least one digit. Mixing letters and digits further complicates the password, thus making guessing more difficult - Including symbols (like !, _, @, #, %, &,), (, [etc.). Incorporating (one or more) symbols complicates the password more. Choosing a password is important. Combining letters (upper and/or lower case) and digits and symbols ensure a high complexity password. The more complicated the password is the more difficult it is for it to be guessed / discovered.	Wiele systemów może generować i dostarczać hasło (zwykle trudne do zapamiętania) lub pozwalają wybrać własne, ale mogą zażądać, aby wybrane hasło spełniało określone wymagania. Typowe ograniczenia obejmują: - Długość hasła. Im dłuższe hasło, tym trudniej je odgadnąć. Zwykłe ograniczenie to minimum 8 znaków - W tym małe i duże litery. W hasłach jest zawsze rozróżniana wielkość liter, więc używanie małych i wielkich liter jeszcze bardziej komplikuje hasło - Zawiera conajmniej jedną cyfrę. Mieszanie liter i cyfr dodatkowo komplikuje hasło, co utrudnia jego odgadnięcie - W tym symbole (takie jak: !, _, @, #,%, &,), (, [, itp.). Włączenie (jednego lub więcej) symboli bardziej komplikuje hasło. Wybór hasła jest ważny. Połączenie liter (wielkich i/lub małych) oraz cyfr i symboli zapewnia hasło o wysokim stopniu złożoności. Im bardziej skomplikowane hasło, tym trudniej je odgadnąć/odkryć.
<u>Using passwords</u>	<u>Korzystanie z haseł</u>
It is a fact that in modern society users are required to remember and use a considerable number of passwords. It is tempting to use and reuse the same password(s) for a number of applications and services. However, such a practice is not advisable. If your password is discovered then your accounts are in danger. Modern computer systems and browsers can store your passwords and use them when you visit specific pages. This is something that can be used but only if you are the only one using the computer. If you are using a shared computer in a lab or an office then you should not allow any application to store your passwords. One more approach is to write down your passwords either in a hard copy file (on paper) or in electronic format and save it in a location that you are aware. Both these approaches are **not advisable** since the information can be compromised.	Faktem jest, że we współczesnym społeczeństwie od użytkowników wymaga się zapamiętania i używania znacznej liczby haseł. Kuszące jest używanie i ponowne używanie tego samego hasła (haseł) w wielu aplikacjach i usługach. Jednak taka praktyka nie jest wskazana. Jeśli Twoje hasło zostanie odkryte, Twoje konta są w niebezpieczeństwie. Nowoczesne systemy komputerowe i przeglądarki mogą przechowywać Twoje hasła i używać ich podczas odwiedzania określonych stron. To jest coś, czego można użyć, ale tylko wtedy, gdy jesteś jedyną osobą korzystającą z komputera. Jeśli używasz wspólnego komputera w laboratorium lub biurze, nie powinieneś zezwalać żadnej aplikacji na przechowywanie haseł. Jeszcze jedno podejście polega na zapisaniu haseł w pliku papierowym (na papierze) lub w formacie elektronicznym i zapisaniu go w miejscu, które znasz. Oba te podejścia **nie są zalecane**, ponieważ informacje mogą zostać naruszone.

Safe keeping passwords	Bezpieczne przechowywanie haseł
Due to the number of passwords that must be remembered, a common approach to use is to install some password management software application. Applications like these give you the ability to save as many passwords as you like in a database and look them up whenever you need them. Password management applications use what is called a 'master' password, which is needed in order to start up the application and access the database (and remaining passwords). One other, a little bit more manual approach, is to create a file to store your passwords and then either encrypt the file using some encryption application or add the file to a compress archive and use a password to protect the file.	Ze względu na liczbę haseł, które należy zapamiętać, typowym podejściem jest zainstalowanie aplikacji do zarządzania hasłami. Aplikacje takie jak te umożliwiają zapisywanie w bazie danych dowolnej liczby haseł I wyszukiwanie ich w dowolnym momencie. Aplikacje do zarządzania hasłami używają tak zwanego hasła „głównego”, które jest potrzebne do uruchomienia aplikacji i uzyskania dostępu do bazy danych (i pozostałych haseł). Innym, nieco bardziej ręcznym podejściem, jest utworzenie pliku do przechowywania haseł, a następnie zaszyfrowanie pliku za pomocą jakiejś aplikacji szyfrującej lub dodanie pliku do archiwum kompresji i użycie hasła do ochrony pliku.