Watchdog ID Documentation

Release 0.1

Adam Dobrawy

Dec 02, 2017

Contents

CHAPTER 1

Wstęp

Często w obrębie jednej instytucji funkcjonuje wiele niezależnych aplikacji sieciowych. Każda z nich posiada własne mechanizmy identyfikacji i uwierzytelniania użytkowników, które są oparte na systemie haseł.

Aby zagwarantować bezpieczne uwierzytelnianie w dużej liczbie niezależnych systemów, warto ten proces przenieść do dedykowanego, funkcjonalnego, wysoce dostępnego systemu komputerowego, który będzie gwarantować jednolity, wysoki poziom bezpieczeństwa, a także zagwarantuje możliwość skutecznych audytów bezpieczeństwa, wczesnego wykrywania nadużyć i odpowiedzi na nowe oczekiwania w zakresie nowoczesnych form uwierzytelniania, w tym uwierzytelniania wieloskładnikowego.

Brak odpowiedniego, dedykowanego otwartoźródłowego systemu, który mógłby zostać wdrożony w organizacji, spowodował potrzebę stworzenia własnego, który będzie wspomagać inne aplikacje w procesie rejestracji i uwierzytelniania użytkowników, stanowiąc dedykowany *Identify Provider* zapewniając mechanizm *Single sign-on*.

1.1 Cel pracy

Celem prezentowanej pracy było stworzenie otwartego i elastycznego systemu centralnego uwierzytelniania użytkownika, jak również ich rejestracji. Nowy proces logowania ma być jednolity w obrębie różnych systemów, a także wzbogacony o dodatkowe formy uwierzytelniania.

System ten ma przejąć zadanie uwierzytelniania z systemów dotychczas działających w organizacji, a wspierających tylko prymitywne formy uwierzytelniania, powstałych w oparciu o rozbieżne technologie tworzące indywidualne bazy tożsamości i danych uwierzytelniających. Aby zapewnić jego rzeczywiste wykorzystanie system winien być łatwy i wygodny w integracji z dotychczas istniejącymi systemami, a - zważywszy na wygodę użytkownika - powinien mieć formę aplikacji internetowej. Powinien mieć charakter modularny w zakresie form uwierzytelniania, aby umożliwiał łatwe dodawanie nowych form uwierzytelniania wraz z pojawiającymi się zagrożeniami, potrzebami i możliwości.

Praca uwzględnia także przygotowanie komponentów do dotychczas funkcjonujących systemów, które umożliwią przeniesienie procesu uwierzytelniania do centralnego systemu. Stanowić to będzie potwierdzenie skuteczności protokołu integracji, a także spełnienia jego wymagań w zakresie prostoty i wygody.

Idea centralnej aplikacji wynika z analizy potrzeb Stowarzyszenie Sieć Obywatelska - Watchdog Polska, które chciałoby - w celu poprawy swojego bezpieczeństwa - stworzyć możliwość utworzenia zintegrowanego konta użytkownika dla członków zespołu, ale także dla odbiorców swoich działań (wolontariuszy, aktywistów itp.). Podstawowym celem

wdrożenia systemu jest podniesienie poziomu bezpieczeństwa rozproszonych systemów komputerowych i zapewnienie w możliwie wielu aplikacjach bezpiecznych form uwierzytelniania.

1.2 Tworzenie projektu

Koncepcja systemu została opracowane przez autora na podstawie osobistych doświadczeń[1] podczas pełnienia funkcji Administratora Bezpieczeństwa Informacji (ABI) w Stowarzyszeniu Sieć Obywatelska - Watchdog Polska.

Autor rozpoczął opracowanie projektu od analizy formy uwierzytelniania (*Uwierzytelnianie*), a następnie rozpatrzył dotychczasowe standardowych form delegacji uwierzytelniania (*Protokoły integracji*). Rozpatrzone zostały wymagania prawne mogące mieć wpływa na sposób funkcjonowania aplikacji (*Uwarunkowania prawne*). Po wnikliwej analizie sformował główne założenia aplikacji (*Wymagania systemu*).

Główny komponent aplikacji zrealizowano w języku Python z wykorzystaniem frameworka Django (https://djangoproject.com/). Podczas pracy został wykorzystano liczne narzędzia wspomagające prace. Do zarządzania projektem wykorzystano GitHub (https://www.github.com/), który zapewniał także hosting dla wykorzystanego systemu kontroli wersji Git. Systemy te były z sobą zintegrowane. Z systemem kontroli wersji był zintegrowany także system ciągłej integracji Travis CI (https://travis-ci.org/). W przypadku środowiska testowego został wykorzystany hosting Heroku (http://heroku.com/), który zapewnił możliwość weryfikację współpracy komponentów w sieci Internet z wykorzystaniem różnych aplikacji klienckich.

[1] Wpis Karola Breguła na portalu Facebook z dnia 3 grudnia 2016 roku (https://www.facebook.com/adam.dobrawy/posts/592261217627776)

CHAPTER 2

Uwierzytelnianie

W tym rozdziale opiszemy formy uwierzytelniania, z szczególnym uwzględnieniem dwuskładnikowego uwierzytelniania. Założenia leżące u jego podstaw, korzyści, ryzyko, ograniczenia, a także przeanalizujemy formy dwuskładnikowego dokonując analizy ich słabych i mocnych stron.

W tym rozdziale zostaną także przedstawine doświadczenia autora uzyskane w ramach projektu Koła Naukowego Programistów polegającej na stworzeniu i rozwoju strony internetowej Dwa-Skladniki.pl (https://dwa-skladniki.pl/). Zostaną one przedstawione w formie analizy dotychczas wykorzystywanych w Polsce form uwierzytelniania. Zostanie przedstawiona analiza odnosząca się do sektora publicznego, jak również prywatnego, w tym perspektyw rozwoju w sektorze bankowości, który - obecnie - wytycza trendy.

Todo

Zapoznać się z:

- https://pages.nist.gov/800-63-3/sp800-63b.html DRAFT NIST Special Publication 800-63B Digital Authentication Guideline
- wyjaśnić hasło "Bring Your Own Authentication (BYOA)""
- https://sekurak.pl/kompendium-bezpieczenstwa-hasel-atak-i-obrona/
- Materiały reklamowe Google - https://www.google.com/landing/2step/
- Karty chipowe z kluczami kryptograficznymi
- Trusted Platform Module - przeanalizować znaczenie dla przechowywania kluczy publicznych

2.1 Kontrola dostępu

Aplikacje zakładające interakcję z użytkownikiem wymagają przeprowadzenia logowania (ang. *logging in* lub *signing in*), czyli procesu składającego się zasadniczo z trzech etapów[2]:

[2] Tomasz Mielnicki, Franciszek Wołowski, Marek Grajek, Piotr Popis, Identyfikacja i uwierzytelnianie w usługach elektronicznych, Przewodnik Forum Technologii Bankowych przy Związku Banków Polskich, Warszawa, 2013, http://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/

- identyfikacji (ang. *identification*) użytkownika, czyli uzyskania od użytkownika deklaracji co do swojej tożsamości np. w postaci nazwy użytkownika, w sposób umożliwiający zidentyfikowanie tożsamości użytkownika w danym środowisku,
- uwierzytelnienia (ang. *authentication*) użytkownika, czyli dostarczenia dowodów, że użytkownik jest właśnie tą zidentyfikowaną osobą (nikt się nie podszywa), a dane uzyskane w etapie identyfikacji są autentyczne,
- autoryzacji (ang. *authorization*), czyli przyznaniu przez system komputerowy dostępu do określonego zasobu po pozytywnym uwierzytelnieniu lub potwierdzenie woli realizacji czynności w postaci elektronicznej przez uwierzytelnionego użytkownika za pomocą dodatkowych danych.

Proces ten przeprowadzony łącznie na potrzeby indywidualnej sesji jest nazywany logowaniem. Jednakże może być także wykorzystywany do dodatkowego potwierdzenia akcji o szczególnej wrażliwości np. zlecenie przelewu w systemach bankowych. Każdy z tych etapów może być przeprowadzony w odmienny sposób w zależności od wymogów systemu komputerowego. Najpopularniejszą formą identyfikacji i uwierzytelniania użytkowników w systemach komputerowych jest wykorzystanie nazwy użytkownika (ang. *login*) i hasła. Jednak tradycyjne podejście nie jest wystarczająco bezpieczne w dzisiejszym świecie, w którym co dzień zdarzają się ataki szkodliwego oprogramowania i inne formy kradzieży haseł wykazujące słabość tego mechanizmu.

2.2 Wygoda użytkowania a bezpieczeństwo

Największym wyzwaniem w projektowaniu procesu logowania w systemach komputerowych pracujących w sieci Internet wydaje się być uwierzytelnianie. Musi ono zapewnić adekwatny do charakteru systemu komputerowy poziom bezpieczeństwa systemu komputerowego przy zachowaniu użyteczność (ang. *usability*) akceptowalnej przez użytkownika. Dwie te wartości pozostają niezwykle często w napięciu.

Jeśli mechanizmy bezpieczeństwa są zbyt skomplikowane w obsłudze, użytkownicy często wybierają, aby nie używać ich w ogóle, albo poszukują metod na ich obejście.

Przykładowo uwierzytelnienie z wykorzystaniem hasła wymaga współdzielonego pomiędzy użytkownikiem i systemem komputerowym sekretu. Dane te powinny zostać zapamiętane przez użytkownika w umyśle. Jednak nieprawidłowe wymogi odnośnie takiego sekretu skłaniają użytkowników do ich zapisywania narażając poufność sekretu (zob. *Polityki haseł*). Wymaga to ostrożnego doboru sposobów (form) w jakich uwierzytelnianie ma przebiegać. Nieprawidłowy dobór, nawet mechanizmów, które technicznie zapewniają wyższy poziom bezpieczeństwa - ze względu na niezrozumienie i nie stosowanie się do zasad bezpieczeństwa przez użytkowania (czynnik ludzki) - może paradoksalnie zwiększać zagrożenie dla systemu informatycznego.

Todo

Rozbudować sekcje i bibliografie:

- Google hasła “Security and Usability”
- publikacja Lorrie Faith Cranor; Simson Garfinkel, “Security and Usability : Designing Secure Systems that People Can Use.”, O’Reilly Media, Inc.

2.3 Formy uwierzytelniania

Wykorzystanie hasła nie jest jedyną możliwą formą uwierzytelniania, która może zostać wykorzystana w systemie komputerowym, aczkolwiek najpopularniejszą. Ponadto możliwe jest złożenie wielu form w ramach jednego procesu uwierzytelniania, co szczegółowo zostało omówione w rozdziale *Dwuskładnikowe uwierzytelnienie*.

technologie_bankowe/publikacje/Przewodnik_Identyfikacja_i_uwierzytelnianie_strona_FTB.pdf [dostęp 23 grudnia 2016 roku]

W dalszych rozważaniach będzie wykorzystywana następująca klasyfikacja podstawowych form uwierzytelniania:

- coś co wiesz (*something you know*) – informacja będąca w wyłącznym posiadaniu uprawnionego podmiotu, na przykład hasło lub klucz prywatny;
- coś co masz (*something you have*) – przedmiot będący w posiadaniu uprawnionego podmiotu, na przykład generator kodów elektronicznych (token), telefon komórkowy (kody SMS, połączenie autoryzacyjne) lub klucz analogowy,
- coś czym jesteś (*something you are*) – metody biometryczne.

2.3.1 Współdzielony sekret

W przypadku wielu systemów komputerowych do uwierzytelniania wykorzystywane jest wyłącznie współdzielony sekret potocznie określony hasłem. Jest to najpopularniejszą forma uwierzytelniania. Stanowi ona formę uwierzytelniania typu *coś co wiesz*.

Ten proces uwierzytelniania wymaga wcześniejszego zindywidualizowanej dla każdego użytkownika inicjalizacji polegającej na wymianie hasła (współdzielonego sekretu) pomiędzy użytkownikiem a systemem komputerowym. W zależności od decyzji projektanta systemu współdzielone hasło może zostać wygenerowane przez system komputerowy, albo być wprowadzane przez użytkownika. W przypadku dużej części aplikacji internetowych wymiana współdzielonego hasła ma miejsce podczas rejestracji. Jednocześnie powszechnie tworzone są dedykowane formularze służące do zmiany haseł i odzyskania zdolności do uwierzytelniania ("Przypomnij hasło"). Proces wymiany współdzielonego hasła wymaga, aby uprzednio użytkownik został zidentyfikowany w inny sposób, jeżeli uwierzytelnianie ma odwoływać się do innych tożsamości. Podstawowym warunkiem bezpieczeństwa tej formy uwierzytelniania jest zachowanie w poufności współdzielonego sekretu. W przypadku wykorzystania wyłącznie tej formy uwierzytelnianie polega ona na wprowadzeniu hasła użytkownika i wymiany komunikatów zgodnie z przedstawionym schematem:

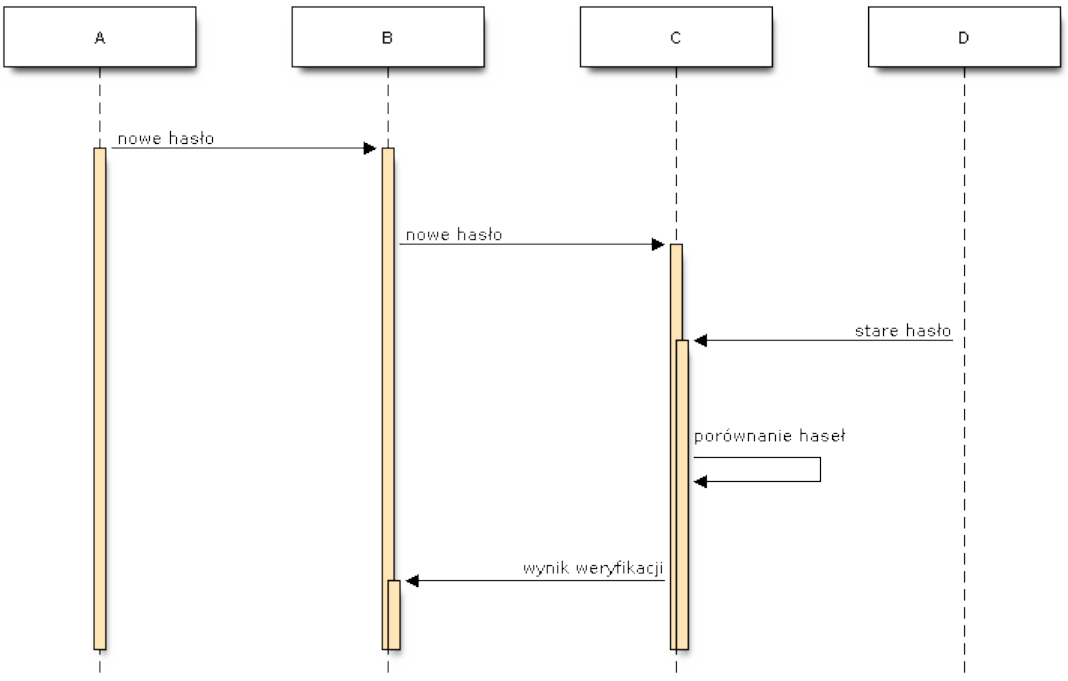

Fig. 2.1: Podstawowe uwierzytelnienie hasłem

Name	Description
A	użytkownik
B	przeglądarka
C	aplikacja
D	baza danych

W związku z ograniczonym bezpieczeństwem tej formy uwierzytelniania wdrażane są liczne rozwiązania, które mają ograniczyć jej słabość. Mają one charakter organizacyjny i techniczny.

Funkcje skrótu

Wartym odnotowania mechanizmem usprawnienia mechanizmu uwierzytelniania z wykorzystaniem współdzielonego sekretu o charakterze technicznym jest tzw. *hashowanie* haseł. Polega ono na ograniczeniu dostępności w systemie komputerowym hasła w postaci jawnej poprzez zapisanie wyłącznie danych stanowiących wynik jednokierunkowej funkcji skrótu kryptograficznego tzw. *hash*. Bezpieczne funkcje hashujące h(x) = hash są funkcjami hashującymi z następującymi właściwościami[8]:

- jednokierunkowość – na podstawie wyjścia funkcji (hash) nie możemy w żaden sposób określić wejścia (x),
- duża zmienność wyjścia – efekt lawinowy objawiający się w dużej różnicy wyjść (hash1, hash2) wygenerowanych nawet przez bardzo podobne wejścia (x1, x2),
- wysoka odporność na kolizje – kosztowne wygenerowanie tego samego wyjścia (hash) przy użyciu dwóch różnych wejść (x1, x2).

W przypadku zastosowania takiego rozwiązania proces uwierzytelniania polega na porównaniu danych stanowiących wynik funkcji skrótu krytograficznego. Można go przedstawić z wykorzystaniem następującego schematu:

Name	Description
A	użytkownik
B	przeglądarka
C	aplikacja
D	baza danych

Dzięki wykorzystaniu funkcji skrótu zostało ograniczone ryzyko, że po włamaniu do bazy danych użytkownik będzie od razu zagrożony[7]. Wykorzystanie takich danych wymaga odnalezienie słabości funkcji hashującej np. kolizji, co zazwyczaj wymaga zaangażowania znacznych mocy obliczeniowych. W wielu wypadkach zastosowanie funkcji skrótu zwiększa zasoby wymaganie do wykorzystania danych, ale tego nie uniemożliwia. Może to jednak być wystarczające, aby zneutralizować zagrożenie.

Projektowane są dedykowane algorytmy funkcji skrótu kryptograficznego, które przeznaczeniem jest hashowania haseł statycznych, a nie dowolnych danych binarnych. Określane są one mianem PKF (ang. *key derivation function*). Do najbardziej znaczących należą PBKDF2, bcrypt i scrypt. Oferują one m. in. mechanizm *key stretching* stanowiącą konfigurowalną wartość wpływającą na złożoność obliczeniową funkcji zapewniając opór dla prawa Moore'a, a także elastyczność wobec ataków wymyślonym w przyszłości (future-proof)[#citation_needed]_.

Uwierzytelnienie wyzwanie-odpowiedź

Hasło musi stanowić sekret znany wyłącznie przez użytkownika i system komputerowy, a więc zagrożeniem dla uwierzytelniania hasłem jest m. in. przesyłanie go w postaci jawnej poprzez sieć. W celu ograniczenia tego zagrożenia wykorzystywane są odpowiednie mechanizmy. Warto w tym miejscu zwrócić uwagę na grupę algorytmów wyzwanie-odpowiedź, które zapewniają ochronę przed prostym podsłuchaniem hasła podczas komunikacji sieciowej. Proces uwierzytelniania można wówczas przedstawić z wykorzystaniem następującego diagramu:

[8] Adrian Vizzdoom Michalczyk, Kompendium bezpieczeństwa haseł – atak i obrona (część 1.), Sekurak.pl 1 lutego 2013 roku, https://sekurak.pl/kompendium-bezpieczenstwa-hasel-atak-i-obrona/ (dostęp: 27 stycznia 2017 roku)

[7] Devdatta Akhawe, How Dropbox securely stores your passwords, Dropbox Tech blog, https://blogs.dropbox.com/tech/2016/09/how-dropbox-securely-stores-your-passwords/ [dostęp 2 stycznia 2016 roku]

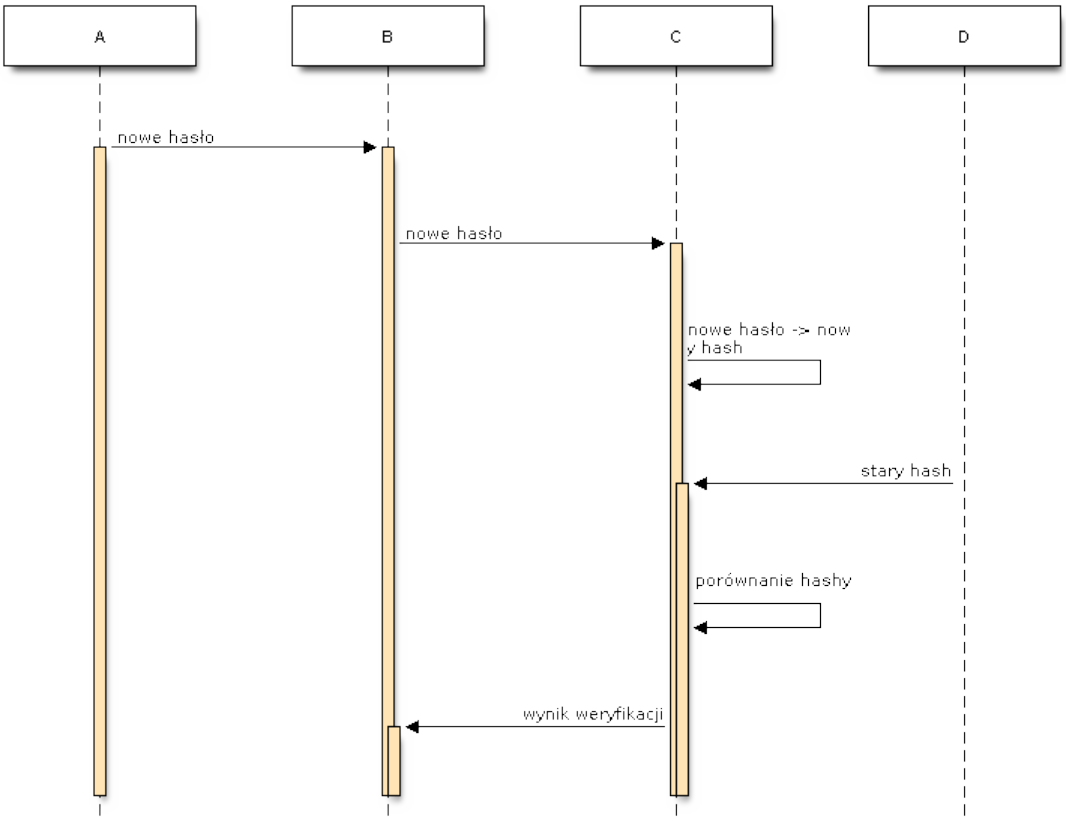

Fig. 2.2: Uwierzytelnianie hasłem z wykorzystaniem funkcji skrótu

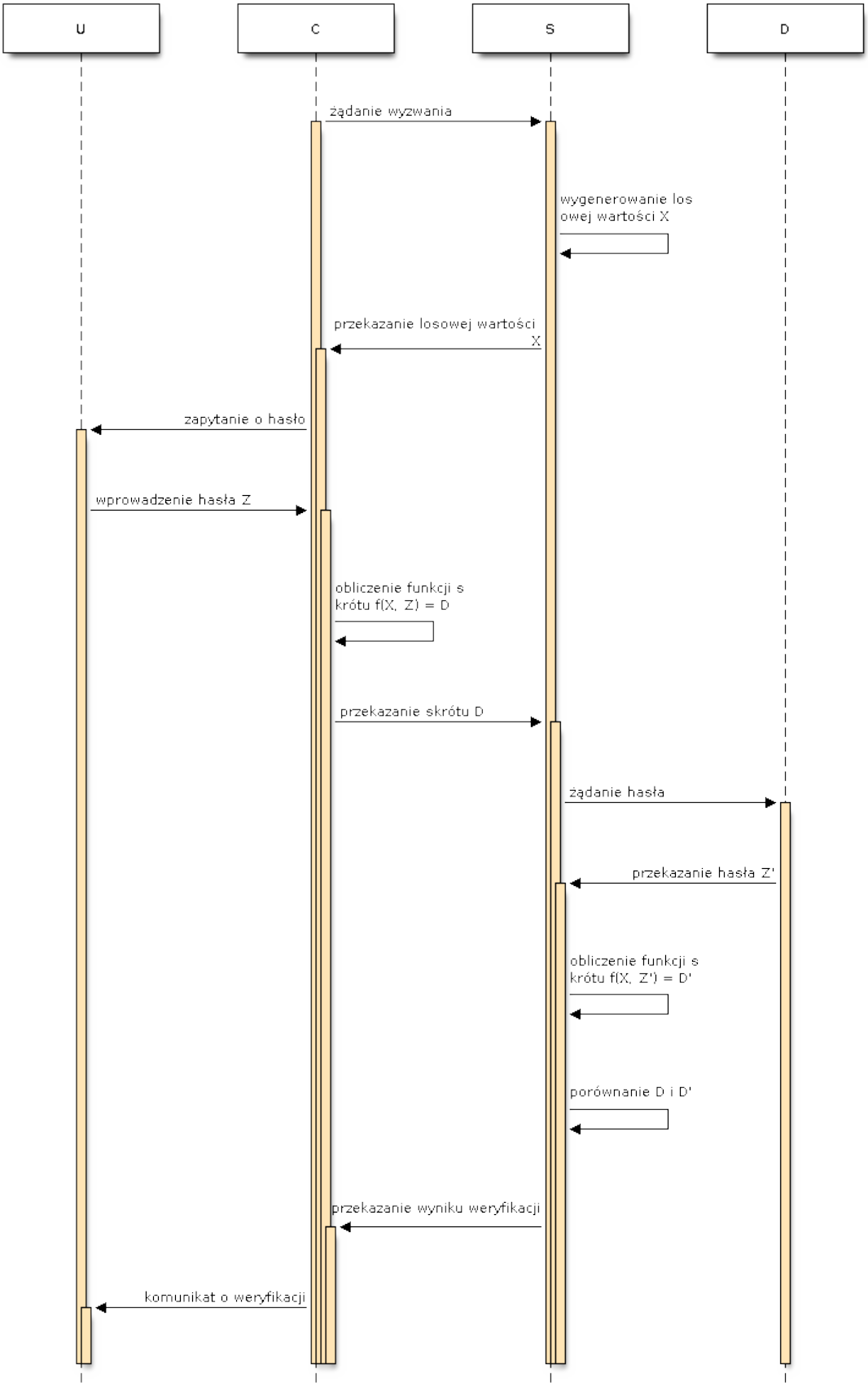

Fig. 2.3: Uwierzytelnianie z wykorzystaniem mechanizmu wyzwanie-odpowiedź

Name	Description
U	użytkownik
C	klient
S	serwer
D	baza danych

Należy objaśnić, że sam mechanizm wyzwania ma na celu ochronę przed atakiem powtórzenia (ang. *replay attack* lub *playback attack*), który polega na skopiowaniu komunikatu i powtórki go do jednego lub większej liczby stron. Ochrona jest zapewniona, ponieważ w przypadku ponownej próby uwierzytelniania zostanie wykorzystanie inne wyzwanie (wartość X na diagramie), która lawinowo zmieni wartość kryptograficznej funkcji skrótu f(X,Z) (zob. *hashing*).

Zbliżony mechanizm stanowi podstawę dla uwierzytelniania z wykorzystaniem kryptografii asymetrycznej, gdzie wyzwaniem jest opatrzenie zadanej wiadomości kluczem prywatnym, co - po zweryfikowaniu z wykorzystaniem klucza publicznego - pozwala na potwierdzenie tożsamości.

Phishing

Phishing to forma ataku internetowego, który stanowi istotne zagrożenie dla procesu uwierzytelniania z wykorzystaniem współdzielonego sekretu.

Atak ten polega na nakłonieniu użytkownika do wprowadzenia osobistych danych na fałszywej stronie. Do nakłonienia do chodzi na skutek zastosowania przez agresora różnorodnych metod socjotechnicznych. Jedną z częstszych jest przesłanie wiadomość, która próbuje zachęcić odbiorcę, aby z określonego powodu niezwłocznie zaktualizował swoje poufne informacje, bo w przeciwnym razie dotkną go niekorzystne konsekwencje. Taka wiadomość zazwyczaj zawiera odnośnik, który stanowi odwołanie do fałszywej strony internetowej, która złudnie przypomina swój oryginał, a której celem jest przechwycenie osobistych danych ofiary.

Ataki phishingowe mogą obejmować liczne metody, które mają na celu zwiększenie swojej skuteczności poprzez zmniejszenie prawdopodobieństwa zorientowania się co do fałszywości wiadomości lub strony internetowej. Przykładowo typosquatting, homoglyph, punycode, bitsquatting, Right-to-Left override[23]. Wykorzystywane są także certyfikaty SSL dla uwiarygodnienia fałszywych stron, w szczególności wobec zwiększonej dostępności bezpłatnych certyfikatów[24].

Ochrona przed atakami tego rodzaju przede wszystkim polega na budowaniu świadomości użytkownika odnośnie posługiwania się poufnymi wiadomościami, uwierzytelnianiu komunikacji poczty elektronicznej i innych komunikatów technicznych[1].

W przypadku masowych kampanii istotnym zabezpieczeniem są mechanizmy czarnych list[25] . Jednakże skuteczność rozwiązań wbudowanych w konkretne przeglądarki jest zróżnicowana. Z pewnością istotnym wyzwaniem w tym zakresie jest fakt, że prawie 20 % stron phishingowych istnieje tylko 3 godziny, a większość nie jest dostępna już po dwóch dniach[26].

Inne środki techniczne wzmocnienia uwierzytelniania hasłem

Coraz większą popularnością cieszą się algorytmy szyfrowania całej komunikacji w architekturze klient-serwer np. HTTPS (ang. *Hypertext Transfer Protocol Secure*). Przy spełnieniu pewnych warunków zabezpieczają one hasło (a także całą komunikacje sieciową) przez podsłuchem. Ogólne dostępne statystyki użytkowania przeglądarki Chrome

[23] Artur Czyż, Nietypowe metody wykorzystywane w atakach phishingowych, Sekurak, 27 marca 2017 roku, https://sekurak.pl/nietypowe-metody-wykorzystywane-w-atakach-phishingowych/ (dostęp 29 marca 2017 roku)

[24] Catalin Cimpanu, 14,766 Let's Encrypt SSL Certificates Issued to PayPal Phishing Sites, bleepingcomputer.com, 24 marca 2017 roku, https://www.bleepingcomputer.com/news/security/14-766-lets-encrypt-ssl-certificates-issued-to-paypal-phishing-sites/ (dostęp 29 marca 2017 roku)

[1] Potrzebne źródło

[25] How does built-in Phishing and Malware Protection work?, Mozilla Support, https://support.mozilla.org/t5/Protect-your-privacy/How-does-built-in-Phishing-and-Malware-Protection-work/ta-p/9395 (dostęp 29 marca 2017 roku)

[26] Cyren, The Phishing Issue – A Deep Dive Into Today's #1 Security Threat, sierpień 2016, s. 17, http://pages.cyren.com/rs/944-PGO-076/images/CYREN_2016Q3_Phishing_Threat_Report.pdf (dostęp 29 marca 2017 roku)

wskazują, że 14 marca 2015 roku na platformie Windows 39% stron była wczytywana z wykorzystaniem HTTPS. Natomiast 1 października 2016 roku wskaźnik ten przekroczył 50% i wciąż systematycznie rośnie[9].

Należy w tym miejscu zwrócić także uwagę na presje płynącą z strony twórców przeglądarek internetowych. Od stycznia 2017 roku w przeglądarce Chrome w przypadku formularza zawierającego pole hasła i transmisji nieszyfrowej wyświetlane jest ostrzeżenie, a presja ta ma być rozszerzana także na inne sytuacje komunikacji nieszyfrowanej[10]. Podobne mechanizmy są wdrażane w aktualnych wydaniach przeglądarki Firefox[11]

Należy zaznaczyć, że szyfrowanie komunikacji klient-serwer nie zabezpiecza przed przypadkami, gdy hasło zostanie podsłuchane pomiedzy użytkownikiem, a przeglądarką np. na skutek wykorzystania *keyloggerów* lub innego złośliwego oprogramowania pracujące na komputerze użytkownika.

W aspekcie technicznym podejmowane są działania, które mogą ograniczyć skuteczność keyloggerów. Należą w tym zakresie m. in. hasła maskowane, które polegają na oczekiwaniu od użytkownika jednorazowo tylko wybranych znaków z hasła i z każdą zmianą zmienianie tego zestawu znaków. W takiej sytuacji nie jest wystarczające jednorazowe podsłuchanie wprowadzonych danych, gdyż podczas kolejnego uwierzytelniania wymagane będzie inny zestaw znaków. Taki mechanizm został wdrożony w usługach T-Mobile Usługi-bankowe, co zostało zaprezentowane na poniższym diagramie:

Fig. 2.4: Przykładowy ekran uwierzytelniania z wykorzystaniem hasła maskowanego (T-Mobile Usługi bankowe, styczeń 2017 roku) (opr. własne)

[9] Transparency Report, Google, https://www.google.com/transparencyreport/https/metrics/?hl=en (dostęp: 4 lutego 2017 roku)

[10] Emily Schechter, Moving towards a more secure web, Google Security Blog 8 września 2016 roku, https://security.googleblog.com/2016/09/moving-towards-more-secure-web.html (dostęp: 4 lutego 2017 roku)

[11] Tanvi Vyas, Peter Dolanjski, Communicating the Dangers of Non-Secure HTTP, Mozilla Security Blog, https://blog.mozilla.org/security/2017/01/20/communicating-the-dangers-of-non-secure-http/ (4 lutego 2017 roku)

Polityki haseł

W zakresie organizacyjnym, który często wspierany jest także odpowiednimi rozwiązaniami technicznymi wprowadzone są polityki haseł. Obejmują one najczęściej zagadnienia dotyczącego ponownego wykorzystania tych samych haseł w różnych systemach komputerowych, złożoność haseł i częstotliwość ich zmiany.

Warto w tym miejscu dostrzec, że nieadekwatna polityka haseł może prowadzić do ograniczenia bezpieczeństwa, a nie jego poprawy. Moim zdaniem dotyczy to w szczególności wymogu częstej zmiany haseł bez wdrożenia alternatywnych rozwiązań. Częsta zmiana haseł rodzi kilka zasadniczych problemów. Nie wszyscy posiadają zdolność zapamiętania złożonych haseł, co prowadzi do ponownego używania haseł w wielu miejscach lub stosowania haseł schematycznych z wykorzystaniem prostych transformacji. W takim wypadku zbyt skomplikowane i często zmieniane hasła prowadzą do zapisywania ich w jawnej formie, co może narażać na ich kradzież.

Odnośnie schematycznych haseł warto w tym miejscu dostrzec uwagi Lorrie Cranor z amerykańskiej Federalnej Komisji Handlu (FTC), która opisała na stronie FTC badania przeprowadzone na University of North Carolina (w Chapel Hill). Badacze pozyskali ponad 51 tys. hashy haseł do 10 tys. nieaktywnych kont studentów i pracowników, na których wymuszano zmianę hasła co 3 miesiące. Po ich analizie stwierdzono, że dla 17% kont znajomość poprzedniego hasła pozwalała na zgadnięcie kolejnego hasła w mniej niż 5 próbach[4][5].

Podobne wątpliwości co do skuteczności polityki zmiany haseł wyrażono w badaniach tego problemu przeprowadzonych na Carleton University[6] . Dostrzeżono w nich, że w przypadku wielu ataków jednorazowy dostęp do systemu umożliwia natychmiastowe pozyskanie plików docelowych, założenie tylnych drzwi, zainstalowanie oprogramowania typu keylogger lub innego trwałego, złośliwego oprogramowania, które późniejsze zmiany hasła uczyni nieskutecznymi. Autorzy nawet stawiają tezę, że prawdziwe korzyści z wymuszania zmiany haseł nie rekompensują związanych z tym uciążliwości.

Sytuacja ta oznacza, że nie można wprowadzić generalnej reguły, która uzasadniałaby określoną politykę haseł, wymaga to każdorazowo indywidualnej analizy ze strony administratora systemu komputerowego.

Powyższa analiza pokazuje tylko niektóre z słabości uwierzytelniania z wykorzystaniem haseł i uzasadnia konieczność poszukiwania bezpieczniejszych form uwierzytelniania w celu zrealizowania współcześnie procesu uwierzytelniania na adekwatnym poziomie. Utrata poufności haseł - związana zarówno z atakimi po stronie użytkownika i serwera, a także procesu samej komunikacji - stanowią codzienność.

2.3.2 Uwierzytelnianie z wykorzystaniem tokenów

Jedną z popularniejszych form wdrożenia tokenów dwuskładnikowego uwierzytelniania są jednorazowe kody oparte na zdarzeniu bazujące na RFC4225 tzw. HOTP oraz oparte na czasie bazujące na RFC6238 tzw. TOTP. W generalnym ujęciu są one do siebie bardzo zbliżone.

Oba z tych algorytmów bazują na współdzielonym sekrecie, który złączony z licznikiem dla HOTP lub z TOTP aktualnym wskazaniem zegara poddawany jest odpowiedniej transformacji funkcji kryptograficznej w celu uzyskania krótkoterminowego / jednorazowego tokenu. Operacja ta jest wykonywana przez obie strony procesu uwierzytelniania, co stanowi dowód, że podmiot podlegający uwierzytelnieniu jest w posiadaniu danych identyfikacyjnych lub dane te znajdują się pod jego kontrolą.

Sekret o odpowiedniej sile jest generowany przez serwer i prezentowany z wykorzystaniem kodów QR, które są odczytywane przez użytkownika i w bezpieczny sposób przechowywane w aplikacjach takich jak Google Authenticator lub Authy[1].

[4] Lorrie Cranor, Time to rethink mandatory password changes, 2 marca 2016 roku, Federalna Komisja Handlu, ftc.gov, https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes [dostęp 16 marca 2016 roku]

[5] Brian Barrett, Want Safer Passwords? Don't Change Them So Often, Wired.com 3.10.2016, http://www.wired.com/2016/03/want-safer-passwords-dont-change-often/ [dostęp 16 marca 2016 roku]

[6] Sonia Chiasson, P. C. van Oorschot, Quantifying the security advantage of password expiration policies, Designs, Codes and Cryptography, 2015, Volume: 77, Issue 2-3, 401-4

2.3.3 Uwierzytelnienie odrębnym kanałem

Uwierzytelnianie może także opierać się na wykorzystaniu odrębnego kanału, co opiera się wówczas na uwierzytelnianiu typu *coś co masz*, gdyż weryfikowany jest wówczas dostęp do alternatywnego kanału komunikacji. Forma ta obejmuje przede wszystkim sytuacje jednorazowych haseł wymagających wprowadzenia w celu uwierzytelniania operacji na stronie internetowych przekazanych z wykorzystaniem kodów SMS, lecz możliwe jest także wykorzystanie połączeń telefonicznych, a także autoryzacji operacji bezpośrednio za pomocą odrębnego kanału komunikacji.

Istnieją zróżnicowane warianty tej formy uwierzytelniania, jednak podstawą cechą wyróżniającą cechą jest zaistnienie komunikacji odrębnym kanałem. Przykładowo w systemie ePUAP uwierzytelnianie polega na przesłaniu hasła z wykorzystaniem kodu SMS, a następnie oczekiwaniu na wprowadzenie go na stronie internetowej[29]. Natomiast Amazon AWS - co ustalono poprzez badanie w realnym środowisku - realizuje uwierzytelnianie, gdzie użytkownikowi w przeglądarce prezentowany jest kod, który ma wprowadzić podczas automatycznie wyzwolonego połączenia telefonicznego przychodzącego do użytkownika. Odwrotnie postępuje Google, które jako jedną formę uwierzytelniania przewiduje połączenie telefoniczne w trakcie którego użytkownikowi odczytywany jest przez lektora kod, który użytkownik ma wprowadzić na stronie internetowej[27]. Tymczasem mBank wykorzystuje powiadomienia push w aplikacji mobilnej, które odnoszą się do autoryzacji indywidualnej operacji i nie wymagane jest przepisanie dodatkowych kodów[28].

Proces uwierzytelniania z wykorzystaniem haseł jednorazowych przekazanych za pomocą komunikacji SMS można przedstawić z wykorzystaniem następującego diagramu:

Name	Description
U	użytkownik
C	klient
S	serwer
D	
O	operator GSM
P	telefon komórkowy

Podstawowym warunkiem bezpieczeństwa tej formy uwierzytelniania jest brak nieautoryzowanego dostępu do alternatywnego kanału komunikacji. Kluczowym zatem jest dobór takiego kanału komunikacji, który będzie zapewniał odporność systemu na ingerencje agresora. Istnieją udokumentowane ataki odnoszące się do tej formy uwierzytelniania w przypadku np. wykorzystania komunikacji GSM.

Zagrożenie istnieje ze strony protokołu GSM. Należy dostrzec, że były one projektowane z uwzględnieniem ograniczonego bezpieczeństwa, ze względu na wymogi państw i nie był projektowany z przeznaczeniem wykorzystania ich do uwierzytelniania. Istnieją udokumentowane ataki obejmujące zdalne przejęcie komunikacji obranego telefonu komórkowego[30].

Możliwe jest zagrożenie z powodu słabości organizacyjnych operatora GSM. Naciski socjotechniczne na operatorów, błąd w logice biznesowej operatorów np. podczas odzyskiwania karty, zlecenie przekierowania usług, czy nacisków rządów na operatorów GSM mogą prowadzić do ujawnienia kodu za pośrednictwem samego operatora GSM. Przykładowo w przypadku ataku UGNazi vs. Cloudflare w 2012 nakłoniono operatora od przekierowania poczty głosowej[42] , w ataku na @Deray z 2016 roku nakłoniono operatora do przekierowania wiadomości[31]. Natomiast w analizie ataku na uwierzytelnianie usługi Telegram przeprowadzonym w 2016 roku sugeruje się uległość operatora wobec rządu[32]. W 2016 roku operator Play w Polsce uruchomił usługę TelePlay. Umożliwiała ona odbiór

[29] Rozporządzenie Ministra Cyfryzacji w sprawie profilu zaufanego elektronicznej platformy usług administracji publicznej, Dz.U. z 2016 r. poz. 1633

[27] Google, Google 2-Step Verification, online: https://www.google.com/intl/en-US/landing/2step/features.html (dostęp 17 czerwca 2017 roku)

[28] mBank, Mobilna autoryzacja, https://www.mbank.pl/indywidualny/uslugi/uslugi/mobilna-autoryzacja/ (dostęp 17 czerwca 2017 roku)

[30] Mobile network security report: Poland, Security Research Labs, Berlin, February 2015, online: http://gsmmap.org/assets/pdfs/gsmmap.org-country_report-Poland-2015-02.pdf

[42] Piotr Konieczny, Jak można było podmienić stronę Niebezpiecznika? Czyli błąd w dwuskładnikowym uwierzytelnieniu Google i atak na Cloudflare, Niebezpiecznik.pl 5 czerwca 2012 roku, online: https://niebezpiecznik.pl/post/jak-mozna-bylo-zhackowac-niebezpiecznika/

[31] Emily Dreyfuss, @Deray's Twitter Hack Reminds Us Even Two-Factor Isn't Enough, Wired, 6.10.2016,

[32] Frederic Jacobs, How Russia Works on Intercepting Messaging Apps, online: https://www.bellingcat.com/news/2016/04/30/russia-telegram-hack/, bellingcat 2016

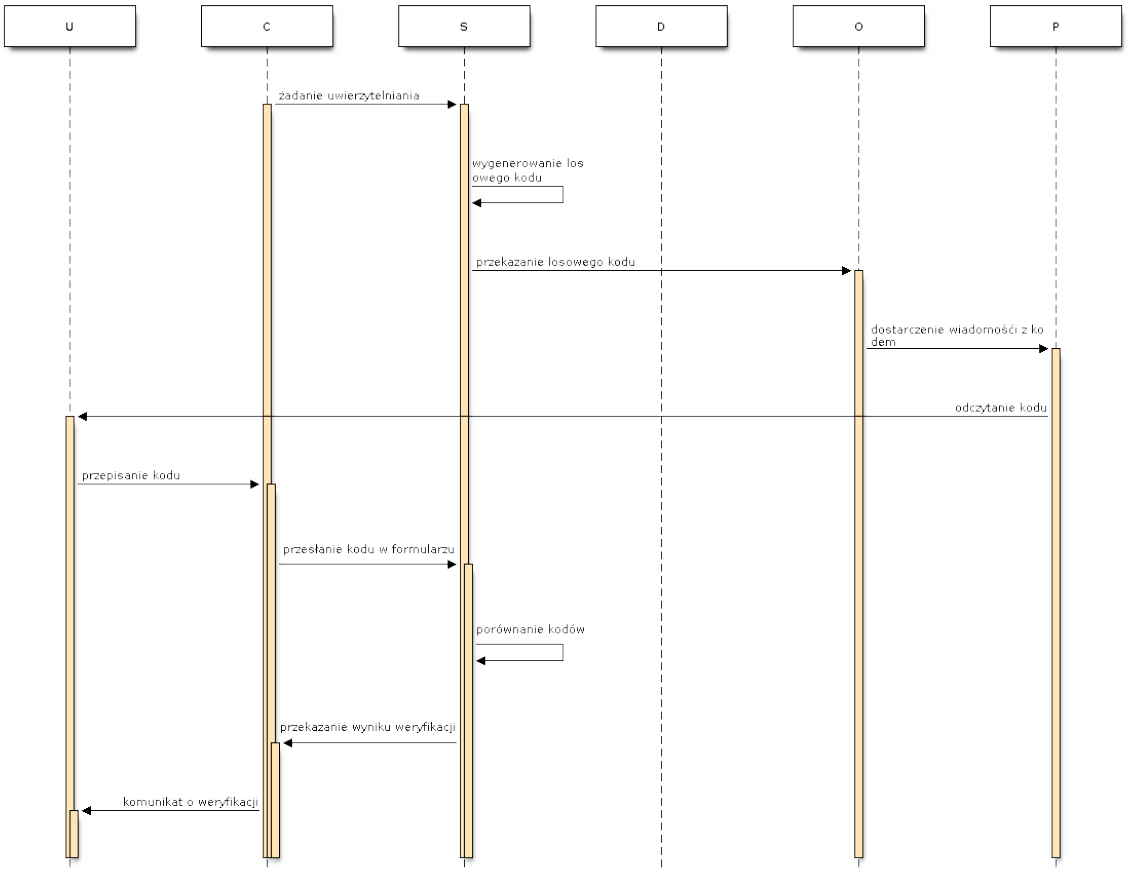

Fig. 2.5: Uwierzytelnianie z wykorzystaniem mechanizmu haseł jednorazowych

połączeń i wiadomości SMS z wykorzystaniem strony internetowej. Słabość form uwierzytelniania portalu internetowego została wykorzystania do wykradania kodów jednorazowych do innych usług[33].

Możliwe jest także zagrożenie ze strony samego użytkownika. Na smartfony powstały i są aktywnie wykorzystywane złośliwe aplikacje, których celem jest przejęcie jednorazowych kodów w celu narażenia uwierzytelniania systemów finansowych[34].

Ta forma uwierzytelniania nie wyklucza możliwości przeprowadzenia ataku phishingowego, gdyż przez cały proces strona phishingowa może pośredniczyć w komunikacji do pożądanej strony, aby pozyskać od niej odpowiednie identyfikatory sesji lub uzyskać fałszywą operacje autoryzacji[39] . Dlatego podczas procesu uwierzytelnienie strony internetowej musi zostać przeprowadzone w inny sposób.

Nie można też pominąć, że w maju 2016 roku NIST opublikował wytyczne zalecające wygaszenie wykorzystania SMS jako czynnik uwierzytelniania[40]. Oznacza to, że przyszłe systemy informatyczne administracji federalnej Stanów Zjednoczonej mogą zostać zmuszone do rezygnacji z tego kanału uwierzytelniania.

Należy wskazać, że uwierzytelnianie z wykorzystaniem kodu SMS lub połączenia telefonicznego może stanowić ingerencje w prywatność użytkownika, gdyż wymagane jest ze strony użytkownika ujawnienie usłudze internetowej jego indywidualnego numeru telefonu. Praktycznie każdy może jednocześnie użytkować ograniczoną ilość numerów telefonu, zatem ten identyfikator identyfikuje użytkownika nie tylko w danej usłudze, ale także będzie współdzielony w innych usługach. Taka sytuacja może budzić opór niektórych użytkowników, a w niektórych społecznościach stanowić wręcz nieakceptowalną ingerencje w prywatnościach. Taka forma nie występuje w pozostałych przedstawionych formach uwierzytelniania.

2.3.4 Kryptografia asymetryczna

Dość powszechnie - stosowane zarówno w środowisku przemysłowym i domowym - zwłaszcza w środowisku systemu operacyjnego Linux jest uwierzytelnianie z wykorzystaniem klucza publicznego. Polega ono na przedstawieniu podpisanej cyfrowo wiadomości.

Ten rodzaj uwierzytelniania został zastosowany m .in . w protokole SSH2, którego specyfikacja wymaga implementacji tej formy uwierzytelniani[12]. Uwierzytelnienie klienta odbywa się po negocjacji warunków połączenia i uwierzytelnienie serwera. Polega na przesłaniu pakietu o następującej strukturze:

```
byte      SSH_MSG_USERAUTH_REQUEST
string    user name
string    service name
string    "publickey"
boolean   TRUE
string    public key algorithm name
string    public key to be used for authentication
string    signature
```

Zawarty podpis cyfrowy składany jest na następującej wiadomości:

```
string    session identifier
byte      SSH_MSG_USERAUTH_REQUEST
```

[33] Adam Haertle, Jak złodzieje okradali konta bankowe klientów sieci Play, ZaufanaTrzeciaStrona.pl, 8 marca 2016 roku, https://zaufanatrzeciastrona.pl/post/jak-zlodzieje-okradali-konta-bankowe-klientow-sieci-play/

[34] Brian Krebs, A Closer Look: Perkele Android Malware Kit, https://krebsonsecurity.com/2013/08/a-closer-look-perkele-android-malware-kit/, Krebs on Security Blog, 19 kwietnia 2013 roku, online: https://krebsonsecurity.com/2013/08/a-closer-look-perkele-android-malware-kit/

[39] Zulfikar Ramzan, Phishing and Two-Factor Authentication Revisited, Symantec Official Blog 17 maj 2007 roku, online: https://www.symantec.com/connect/blogs/phishing-and-two-factor-authentication-revisited

[40] Paul A. Grassi, Michael E. Garcia, James L. Fenton, DRAFT NIST Special Publication 800-63B Digital Authentication Guideline, National Institute of Standards and Technology, online: https://pages.nist.gov/800-63-3/sp800-63-3.html

[12] "The only REQUIRED authentication 'method name' is "publickey" authentication. All implementations MUST support this method; however, not all users need to have public keys, and most local policies are not likely to require public key authentication for all users in the near future." (Public Key Authentication Method: "publickey" [w:] T. Ylonen, RFC 4252 - The Secure Shell (SSH) Authentication Protocol)

```
string    user name
string    service name
string    "publickey"
boolean   TRUE
string    public key algorithm name
string    public key to be used for authentication
```

Po odebraniu tak sformułowanego pakietu serwer musi zweryfikować czy przedstawiony klucz publiczny jest właściwy do uwierzytelnia dla danego użytkownika, co najczęściej odbywa się poprzez weryfikacje bazy uprawnionych kluczy zawartej w pliku `.ssh/authorized_keys` w katalogu domowym użytkownika. Jak również serwer musi zweryfikować czy złożony podpis jest prawidłowy.

Należy objaśnić, że przedstawiony identyfikator sesji (`session identifier`) został ustalony podczas wcześniejszych etapów negocjacji połączenia. Wartość ta ulega zmianie wraz z każdym połączeniem lub częściej. Dzięki czemu ten jeden pakiet stanowi całą komunikacje uwierzytelniania, która jest odporna na atak powtórzenia. Jednak generalnie idee uwierzytelniania z wykorzystaniem kryptografii asymetrycznej można przedstawić w formie następującego schematu:

Name	Description
U	użytkownik
C	klient
S	serwer
D	baza danych

Klucz prywatny jest składowany często na komputerze użytkownika, co oznacza że ten sposób uwierzytelniania należy sklasyfikować jako oparty na "czymś co masz" (*authentication_form*). Należy od razu jednak podkreślić, że klucz prywatny może przechowywany w formie zaszyfrowanej i wówczas wymagane jest wprowadzenia hasła przed tym jak wygenerowanie podpisu cyfrowego stanie się możliwe.

Ta forma uwierzytelniania nie jest wrażliwa na sytuacje, gdy poufność klucza prywatnego użytkownika zostanie naruszona. Może to mieć miejsce w sytuacji ataku złośliwego oprogramowania na komputer użytkownika. Niedostateczne w takim przypadku może okazać się szyfrowanie hasła, gdyż podczas próby użycia klucza hasło lub sam klucz może zostać przejęta przez złośliwe oprogramowanie z pamięci komputera.

Jest ona natomiast pozbawione zagrożenia, że użycie tych samych danych dostępowych stanowić będzie zagrożenie dla samego użytkownika. Nie ma zatem konieczności - analogicznie do współdzielonego sekretu - wprowadzenia rozwiązań, które chroniłyby poufność kluczy po stronie system uwierzytelniającego, a w szczególności przechowanie danych z wykorzystaniem funkcji skrótu (*Funkcje skrótu*).

Istotne jest jedynie zagwarantowanie integralności bazy uprawnionych kluczy, gdyż jego modyfikacja, w szczególności dopisanie kluczy obcych może prowadzić do obejścia zabezpieczeń.

Universal 2nd Factor

Jedną z form ochrony kluczy prywatnych wykorzystywanych do uwierzytelniania przed atakom złośliwego oprogramowania może stanowić wykorzystanie do tego celu dedykowanych układów elektronicznych, które stanowić będą sprzętowe zabezpieczenie przed naruszeniem poufności zawartego w układzie klucza prywatnego. Wykorzystanie ich jednak wymaga odpowiedniego sprzętu, oprogramowania (sterowników), a w przypadku aplikacji działających w przeglądarce także wsparcie z strony przeglądarki internetowej.

W ostatnim czasie rosnącą popularność zyskuje otwarty standard *Universal 2nd Factor* (U2F), który to realizuje. Opisuje sposób komunikacji stron internetowych z dedykowanym tokenem (kluczem sprzętowych) podłączonym z wykorzystaniem powszechnie dostępnego w komputerach portu USB bez wykorzystania dodatkowych sterowników za pośrednictwem przeglądarki w celu przeprowadzenia procesu uwierzytelniania. Stanowi zatem kompleksowe rozwiązanie umożliwiające przechowywanie kluczy kryptograficznych w sprzętowym tokenie i wykorzystanie ich w aplikacjach działających w przeglądarce internetowej wymagających uwierzytelnienia.

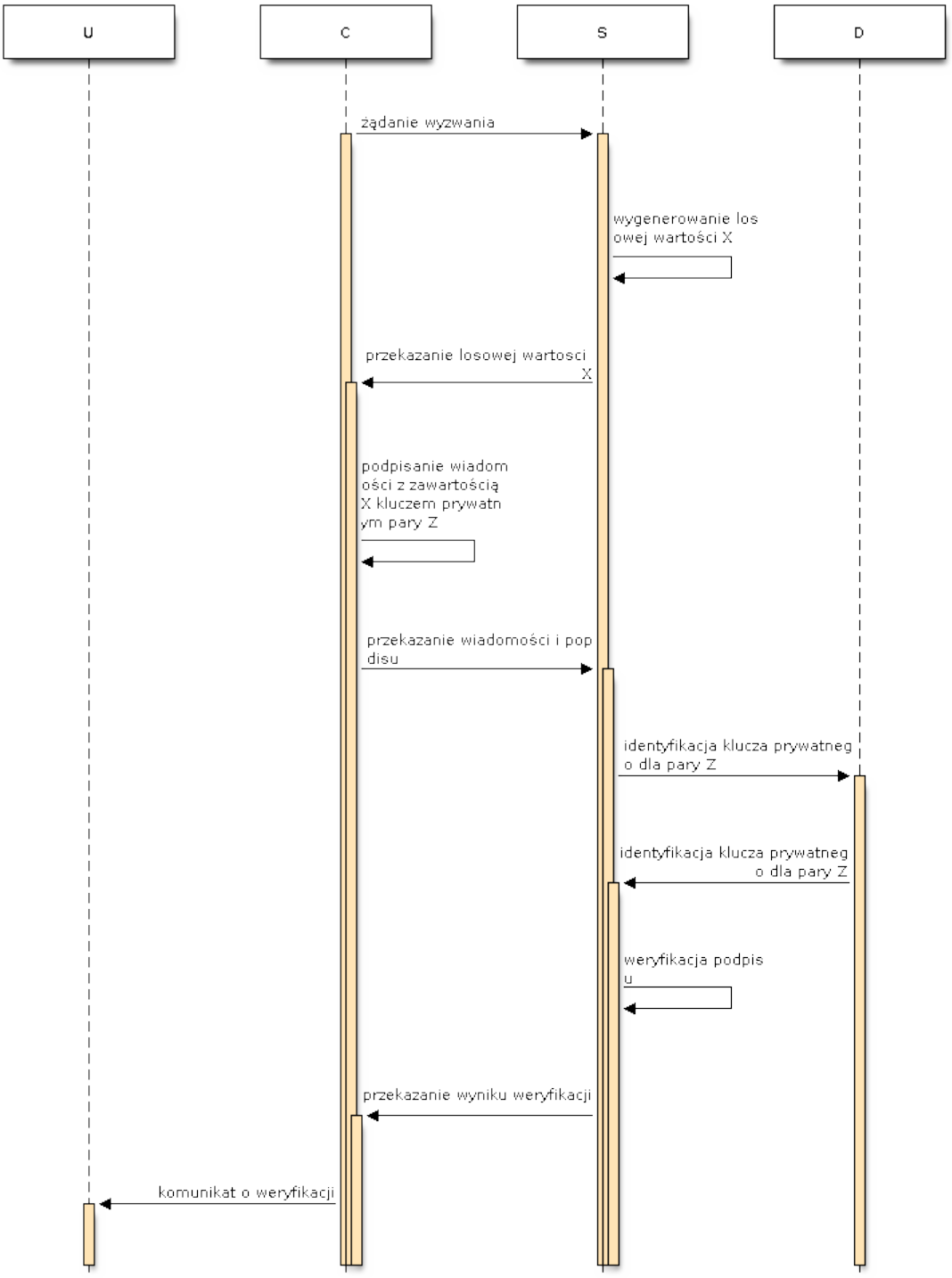

Fig. 2.6: Uwierzytelnianie z wykorzystaniem kryptografii asymetrycznej

Standard ten został zapoczątkowany przez firmę Google i jest teraz zarządzany przez FIDO (Fast Identity Online) Alliance. Członkami FIDO Alliance są także m. in. Microsoft, Mastercard, Visa, PayPal, Discover, Samsung i BlackBerry[13].

Standard ten został wdrożony przez czołowych dostawców usług sieciowych, a jego popularność rośnie. Google ogłosiło jego obsługę w październiku 2014 roku[15], w sierpniu 2015 roku Dropbox[16], w październiku 2015 roku GitHub[17], w czerwcu 2016 roku BitBucket[18], w lutym 2017 roku Facebook[19]. Można zatem przyjąć, że staje się fakycznie standardem.

Dostępne są liczne urządzenia o niewygórowanych cenach. Koszt indywidualnej sztuki wynosi około 70 zł[14]. Samodzielny montaż pozwala skonstruowanie urządzenia w cenie poniżej 25 zł / sztuka, co zostało zweryfikowane przez autora podczas samodzielnego montażu urządzenia[#u2f_uph]_.

Zapewniona jest także odpowiednia obsługa z strony popularnych przeglądarek internetowych - Google Chrome w wersjach 38 i Opera od wersji 40 domyślnie. Natomiast Firefox wymaga dedykowanej wtyczki[20], a wbudowana obsługa jest zaplanowana na 1 kwartał 2017 roku[21].

Ta forma uwierzytelniania zapewnia odporność wobec ataku phishingowych, gdyż wykorzystany mechanizm wyzwanie-odpowiedź zabezpiecza przed wielokrotnym użyciem odpowiedzi (*replay attack*), a weryfikacja kluczy jest dokonywana przez przeglądarkę[35].

Wykorzystywanie uwierzytelniania z wykorzystaniem tokenu U2F może obecnie stanowić jednak wyzwanie ze względu na ograniczoną dostępność tokenów sprzętowych w Polsce. Przykładowo zapytanie o "U2F" w najpopularniejszej platformie aukcyjnej i e-commerce Allegro.pl nie zwróciło żadnych tokenów. A także podczas uwierzytelniania na urządzeniach mobilnych, gdzie dopiero kształtują się odpowiednie rozwiązania i standardy komunikacji.

2.3.5 Dwuskładnikowe uwierzytelnienie

W nowoczesnych systemach komputerowych przed uzyskaniem dostępu często stosuje się uwierzytelniani wieloskładnikowe (*multi-factor authentication*), w szczególności dwuskładnikowe (*two-factor authentication*), czyli łączące dwie różne metody uwierzytelniania. W takich systemach bezpieczeństwo uwierzytelniania opiera się zatem na łącznej skuteczności różnych tych form. W przypadku zawiedzenia wszystkich z form może dojść do zjawisk niepożądanych typu kradzież tożsamości.

Każda forma uwierzytelniania nie jest doskonałe, dla każdej istnieją określone skuteczne wektory ataków, więc dążeniem projektanta, a następnie administratora systemu winno być stałe zapewnienie maksymalnej sprawności ich obu.

Jest to praktykowane, ponieważ w komunikacji elektronicznej stosowanie samego hasła wiąże się z różnego rodzaju ryzykiem, a wykorzystanie kilku form uwierzytelnienia może ograniczać skutki przechwycenia (keylogger), albo podsłuchania (sniffer) hasła po którym przestaje ono być wówczas znane wyłącznie osobie uprawnionej, zaś kradzież

[13] Tony Bradley, How a USB key drive could remove the hassles from two-factor authentication, PCWorld 21 październik 2014 roku, http://www.pcworld.com/article/2836692/how-the-fido-alliances-u2f-could-simplify-two-factor-authentication.html (dostęp 4 luty 2017 roku)

[15] Nishit Shah, Strengthening 2-Step Verification with Security Key, Google Security Blog, 21 październik 2014 roku, https://security.googleblog.com/2014/10/strengthening-2-step-verification-with.html (dostep 4 luty 2017 roku)

[16] Patrick Heim, Jay Patel, Introducing U2F support for secure authentication, Dropbox Blog 12 sierpnia 2015 roku, https://blogs.dropbox.com/dropbox/2015/08/u2f-security-keys/ (dostęp 4 luty 2017 roku)

[17] Ben Toews, GitHub supports Universal 2nd Factor authentication, GitHub Blog, https://github.com/blog/2071-github-supports-universal-2nd-factor-authentication (dostęp 4 luty 2017 roku)

[18] TJ Kells, Universal 2nd Factor (U2F) now supported in Bitbucket Cloud, 22 czerwca 2016, Bitbucket Blog, https://blog.bitbucket.org/2016/06/22/universal-2nd-factor/ (dostęp 4 luty 2017 roku)

[19] Brad Hill, Security Key for safer logins with a touch, Facebook Security, https://www.facebook.com/notes/facebook-security/security-key-for-safer-logins-with-a-touch/10154125089265766 (dostęp 4 luty 2017 roku)

[14] Cena urządzenia FIDO U2F Security Key na Yubico Store, https://www.yubico.com/store/, dostęp 4 luty 2017 roku)

[20] Bug 1065729 - Implement the FIDO Alliance u2f javascript API, Mozilla Bugzilla, https://bugzilla.mozilla.org/show_bug.cgi?id=1065729 (online: 4 luty 2017 roku)

[21] Jcjones, Security/CryptoEngineering, Mozilla Wiki, https://wiki.mozilla.org/index.php?title=Security/CryptoEngineering&oldid=1159535 (dostęp 4 luty 2017 roku)

[35] tylerl, Reply to question "How secure are the FIDO U2F tokens", StackExchange.com, 27 października 2014, https://security.stackexchange.com/a/71704

może pozostać niezauważona. Ryzyko to można ograniczyć, wprowadzając dodatkowy składnik uwierzytelniania wykorzystując kilka form autoryzacji jednocześnie.

Najpopularniejszym rozwiązaniem jest - łącznie z hasłem - wykorzystanie m. in.:

- sprzętowego tokenu istniejącego w jednym, unikatowym egzemplarzu, więc jego użycie wymaga fizycznego dostępu lub kradzieży, która zostanie zauważona (cecha coś co masz),
- jednorazowych kodów generowanych programowo (TOTP), a także przesłanych z użyciem alternatywnego kanału komunikacji (SMS, połączenia, e-mail).

W ostatnich latach zauważalna jest popularność takich rozwiązań w powszechnych usługach internetowych. Obsługę dla wieloskładnikowego uwierzytelniania zapewnia usługa poczty Gmail i Outlook.com, serwisy społecznościowe Facebook i Google+, a nawet platformy gier Battle.net i Steam. Istnieją dedykowane strony internetowe, których celem jest popularyzacja takich rozwiązań - TwoFactorAuth.org (http://TwoFactorAuth.org) i Dongleauth.info (http://www.dongleauth.info/) . Po pierwsze, poprzez promocję wśród konsumentów witryn internetowych, które wspierają bezpieczne formy uwierzytelniania. Po drugie, mają wywierać presję na dostawców usług internetowych, aby wdrożyli oni w optymalny sposób bezpieczne formy uwierzytelniania.

W Polsce dostępność takich rozwiązań rośnie. Analiza witryny Dwa-Skladniki.pl przeprowadzona wskazuje, że żaden krajowy dostawa usług pocztowych nie oferuje takich form uwierzytelniania. Ani Interia, ani O2.pl, ani WP.pl, ani Onet.pl nie oferują takich rozwiązań. Zainteresowane osoby zmuszone są do korzystania z usług w/w zagranicznych gigantów. Natomiast spośród firm hostingowych jakąkolwiek formę dwuskładnikowego uwierzytelniania zapewnia wyłącznie MyDevil.net. Jeżeli chce się mieć bezpieczny hosting w Polsce – należy samemu nim zarządzać. Wówczas można skorzystać z usług OVH, Oktawave lub e24cloud[22].

Warto zwrócić uwagę, że standardy regulacyjne dotyczące dostępu do systemów rządu federalnego USA wymagają używania uwierzytelniania wieloskładnikowego, aby uzyskać dostęp do krytycznych zasobów IT, na przykład podczas logowania do urządzeń sieciowych podczas wykonywania zadań administracyjnych oraz przy dostępie do uprzywilejowanego konta. Również publikacja „The Critical Security Controls for Effective Cyber Defense", wydana przez instytut SANS, przygotowana przez rządowe agencje i komercyjnych ekspertów śledczych i d/s bezpieczeństwa stanowczo zaleca wykorzystanie takich rozwiązań[3].

Unia Europejskiej podejmuje działania na rzecz harmonizacji środków identyfikacji elektronicznej na potrzeby kontaktów z organami publicznymi w celu zapewnienie wzajemnego uznawania elektronicznej identyfikacji i uwierzytelniania[#rozp_EIDAS]_. Rozporządzenie wykonawcze Komisji (UE) 2015/1502[38] określa minimalne specyfikacje techniczne oraz procedury identyfikacji elektronicznej i usług zaufania. W motywie 7 preambuły tego rozporządzenia wskazano, że należy "zachęcać do korzystania z większej liczby czynników uwierzytelniania, zwłaszcza należących do różnych kategorii, w celu zwiększenia bezpieczeństwa procesu uwierzytelniania". Natomiast dla określenia cech charakterystycznych i konstrukcji środków identyfikacji elektronicznej dla poziomu zaufania średniego sformułowano wymaganie "Środek identyfikacji elektronicznej wykorzystuje co najmniej dwa czynniki uwierzytelniania należące do różnych kategorii.".

Todo

Zadać Ministerstwu Cyfryzacji pytanie czy i dlaczego uznaje, że kody SMS spełniają wymaganie: "Środek identyfikacji elektronicznej jest zaprojektowany w taki sposób, że można zakładać, iż jest on stosowany jedynie przez osobę, do której należy, lub pod jej kontrolą.".

---

[22] Analiza została przeprowadzona w dniu 4 lutego 2017 roku poprzez przegląd całości treści opublikowanych na stronie Dwa-Skladniki.pl

[3] CIS Controls for Effective Cyber Defense Version 6.0, SANS Institute, https://www.cisecurity.org/critical-controls.cfm [dostęp 16 marca 2016 roku]

[38] Rozporządzenie wykonawcze Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym

2.3.6 Inne formy uwierzytelniania

W niniejszym opracowaniu zostały pominięte formy uwierzytelniania, które nie cechują się dostateczną rozpoznawalnością w Polsce np. nie zostały wdrożone w żadnej powszechnej usłudze lub nie są adekwatne do sytuacji prawnej w Polsce np. brak otwartego państwowego dostawcy tożsamości lub nie są praktyczne do zastosowania w aplikacji webowej np. biometria.

2.3.7 Dobór form uwierzytelniania adekwatny do ryzyka

Analizy ryzyka bezpieczeństwa informacji oparta winna być na ocenie zasobów, zagrożeń, zabezpieczeń i podatności systemów informatycznych organizacji, a następnie na analizie ryzyka, w tymm określenie ryzyka akceptowalnego i szczątkowego, co pozwala na skuteczne zarządzanie bezpieczeństwem informatycznym i zaprojektowanie systemu ochrony[41].

Wdrożenie dwuskładnikowego uwierzytelniania w otwartej usłudze wymaga dużej uwagi i działań promocyjnych takich rozwiązań, ze względu na brak świadomości społecznej. W wielu usługach użytkownicy wciąż nie korzystają z dwuskładnikowego uwierzytelniania, nawet gdy są one dostępne. Chociaż z drugiej strony w realiach polskich brak jest odpowiedniej kultury w IT, co przejawia się nieoferowaniem użytkownikom takich rozwiązań. Niska popularność takich rozwiązań wpływa na ograniczenie wsparcie dla wdrożenia takich rozwiązań np. brak dostawców tokenów SMS lub telefonicznych nastawionych na rynek polski, co wymaga samodzielnej implementacji w oparciu o ogólne API, co powoduje wzrost kosztu takich rozwiązań. W przypadku gdy uwierzytelnianie wymaga dedykowanego sprzętu występuje dla niego ograniczona dostępność, co wymaga poczynienia nakładów na samodzielny montaż lub import.

Dopuszczalne formę uwierzytelniania winna być adekwatna do wartości chronionych zasobów i zagrożeń, a także uwzględniać czynniki społeczne np. związane z prawem do prywatności i dotychczasową dostępność tokenów U2F. Inne wymagania mogą zostać wykorzystywane w zakresie administracyjnego dostępu do systemu bankowego, a inne w przypadku powszechnego dostępu użytkowników bez szczególnych uprawnień, gdzie narażenie konta użytkownika stanowi zagrożenie wyłącznie dla jego własnych danych.

Stowarzyszenie Sieć Obywatelska - Watchdog Polska jest organizacją strażniczą dla której istotną, zapisaną w samym organizacji statucie jest poszanowanie prawa człowieka do prywatności. Podejmuje także działania kontrolne wobec służb i naczelnych organów państwa, co stwarza potencjalne zagrożenie wykorzystaniem uprawnień państwa do ingerencji w systemy informatyczne Stowarzyszenia, także w porozumieniu z potencjalnie zaufaną trzecią. Obniża to w istotny sposób uwierzytelnianie wykorzystujące bezpieczny kanał komunikacji w postaci sieci GSM, gdyż jego bezpieczeństwo jest w takich sytuacjach wątpliwe. Ograniczone grono pracowników dysponuje własnymi telefonami komórkowymi, a w tym zakresie dominuje podejście - z własnego wyboru pracowników - BYOP (bring your own phone), a więc ich wykorzystanie w procesie uwierzytelniania stanowi ingerencje w prywatność, która może zostać niezaakceptowana.

Wywołuje to przeświadczenie o adekwatności trójstopniowej polityki wrażliwości kont użytkownika:

- Wysoki poziom wrażliwości charakteryzowany dla kont użytkownika o administracyjnych uprawnieniach co najmniej w jednym systemie komputerowym Stowarzyszenia.
- Średni poziom wrażliwości odnosi się do kont użytkownika, które posiadają wyższe niż przeciętne uprawnienia w co najmniej jednym systemie informatycznym Stowarzyszenia, w szczególności dla kont z uprawnieniami redakcyjnymi serwisy internetowe.
- Niski poziomi wrażliwości odnosi się do kont użytkownika, które nie posiadają żadnych szczególnych uprawnień w żadnym systemie informatycznym.

Dla każdego z poziomów wrażliwości kont użytkownika możliwe jest przyporządkowanie minimalnych form uwierzytelniania:

- wysoki poziom wrażliwości - dwuskładnikowe uwierzytelnianie oparte o współdzielone hasło i token U2F,

[41] dr Jan Madej, Strategie analizy ryzyka w opracowywaniu polityki bezpieczeństwa systemu informatycznego, Nierówności Społeczne a Wzrost Gospodarczy 2011, z. nr 22, s. 196 - 198

- średni poziom wrażliwości - dwuskładnikowe uwierzytelnianie oparte o współdzielone hasło i tokenem TOTP lub formy uwierzytelniania właściwe dla kont z wysokim poziomem wrażliwości,
- współdzielone hasło lub jedna z powyższych form - jednoskładnikowe uwierzytelnianie oparte o współdzielone hasło lub formy uwierzytelniania właściwe dla kont z wysokim lub średnim poziomem wrażliwości.

CHAPTER 3

Protokoły integracji

W tym dokumencie zostanie przedstawiona analiza porównwcza form delegacji uwierzytelniania. Przedstawione zostaną założenia protokołów, wskazane krytyczne punkty, analiza bezpieczeństwa, a także elastyczność, w tym formy alternatywnych przepływów integracji. Jak również zostaną przedstawione istniejące rozwiązania SSO, które mogą stanowić bazę dla szerszego wdrożenia. Zostaną one krótko przedstawione ich założenia, ich zakres, słabe i mocne strony.

W szczególnośći zostaną przedstawione takie mechanizmy jak:

- tradycyjne podejście z LDAP-em - Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach,
- single sign-on (SSO)
  - SAML
  - OAuth 1.0
  - OAuth 2.0
  - OpenID 2.0
  - OpenID Connect

3.1 Usługi zintegrowane

W tym dokumencie opiszemy usługi zintegrowane z zaproponowaną forma uwierzytelniania. Zostanie przedstawiona konfiguracja integracji, a także jej ograniczenia.

CHAPTER 4

Uwarunkowania prawne

W tym dokumencie opiszę uwarunkowania prawne związane z realizacją projektu. Zostaną przedstawione wymagania odnośnie bezpieczeństwa systemów, wymagane dzienniki, a także kwestie dotyczące ochrony danych osobowych. W zakresie ochrony danych osobowych zostanie w szczególności przeanalizowany stan obecny, a także perspektywa zmian i rozwoju. Przedstawione zostaną zarówno rozwiązania z zakresu twardego prawa (ang. *hard law*), jak również miekkie prawo (ang. *soft law*), w szczególności środowiska bezpieczeństwa informatycznego i organizacji pozarządowych zajmujących się prawem do prywatności.

Wdrożenie centralnego uwierzytelniania przez użytkowników może mieć wpływ na ich prawo do prywatności. Uważam, że konieczne jest we współczesnym świecie uwzględnienie ochrony danych osobowych, a szerzej wpływu na prawa do prywatności użytkowników już na etapie projektowania aplikacji, które mogą mieć na tą prywatność wpływ.

4.1 Prawo do prywatności

Postęp techniczny stwarzał i nadal stwarza nowe wyzwania dla skutecznej ochrony prywatności i danych osobowych. Zwraca się w literaturze, że łatwo można wykazać, iż niektóre specyficzne właściwości sieci komputerowych niejako z natury rzeczy wywołują nieznane wcześniej zagrożenia dla dóbr osobistych, skłaniając do poszukiwań środków zaradczych[1].

Wobec ingerencji w prawo do prywatności należy zwrócić uwagę, że prawo do prywatności zostało w sposób wyraźny zagwarantowane w międzynarodowych aktach prawnych dotyczących ochrony praw człowieka (art. 12 Powszechnej Deklaracji Praw Człowieka, art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych oraz art. 8 Europejskiej Konwencji Praw Człowieka). Prawo do ochrony prawnej życia prywatnego zostało zagwarantowane w art. 47 Konstytucji, a niektóre uprawnienia szczegółowe składające się na treść tego prawa – ponadto w innych przepisach konstytucyjnych.

W kontekście tego projektu należy w szczególności zwrócić uwagę na autonomię informacyjną jednostki, którą gwarantuje przede wszystkim art. 51 Konstytucji. W myśl art. 51 ust. 1, nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym (art.

[1] Janusz Barta, Paweł Fajgielski, Ryszard Markiewicz, Ochrona danych osobowych. Komentarz, wyd. V

51 ust. 2). Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa (ust. 5). Zgodnie z ust. 3, każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa. Z kolei art. 51 ust. 4 stanowi, że każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.

W literaturze zwraca się, że polski system prawny przyjmuje zasadę (prawo do) samodzielnego decydowania każdej osoby o ujawnianiu dotyczących jej informacji. Zasada ta odnosi się do wszelkich tego rodzaju informacji, w szczególności nie została zawężona do informacji szczególnego charakteru albo dotyczących szczególnych kwestii[2].

Użyte w analizowanych normach określenie "informacje dotyczące osoby" może być uznane za synonim pojęcia danych osobowych[3].

4.2 Ochrona danych osobowych

U podstaw ustawy o ochronie danych osobowych z 1997 r. (dalej: u.o.d.o.)[4] leży koncepcja, iż przetwarzanie danych dopuszczalne jest tylko w przypadkach i na warunkach wskazanych przez ustawę, równocześnie wykorzystanie danych osobowych nie może być zabronione, o ile odbywa się z poszanowaniem ustawy.

Ustawa wprowadza dwie podstawowe kategorie danych osobowych - tzw. dane zwykłe i dane sensytywne (wrażliwe), których ujawnienie lub inne wykorzystanie może w sposób szczególnie dotkliwy naruszać prawa i wolności jednostki, określone w art. 27 u.o.d.o. Przetwarzanie w określonym systemie komputerowym danych sensytywne podnosi znacząco wymogi bezpieczeństwa wymagane od systemu informatycznego.

W przypadku systemu centralnego uwierzytelniania bezpośrednio w nim nie będą przetwarzane dane sensytywne. Mogą natomiast one stanowić bramę wejścia do systemu komputerowego, w którym takie dane mogą być przetwarzane.

Ustawa zawiera delegację do wydania rozporządzenia przez ministra właściwego do spraw administracji w porozumieniu z ministrem właściwym do spraw informatyzacji, które określi podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, uwzględniając zapewnienie ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną, a także wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzanych danych (art. 39a u.o.d.o.).

Delegacja została spełniona poprzez rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004 r.[5]

W rozporządzeniu - uwzględniając kategorie przetwarzanych danych oraz zagrożenia wprowadza się poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym wprowadził trzy poziomy bezpieczeństwa - podstawowy, podwyższony i wysoki. Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną. Zważywszy że aplikacja ma służyć także do uwierzytelniania także odbiorców Stowarzyszenia należy - podczas projektowania aplikacji - przyjąć konieczność spełnienia wymogów bezpieczeństwa na najwyższym poziomie bezpieczeństwie tj. poziomie wysokim.

Opis środków bezpieczeństwa stosowany na poziomach określa załącznik do rozporządzenia, który jest cytowany poniżej:

1. Środki bezpieczeństwa na poziomie podstawowym

I

[2] Janusz Barta, Paweł Fajgielski, Ryszard Markiewicz, Ochrona danych osobowych. Komentarz, wyd. V
[3] Janusz Barta, Paweł Fajgielski, Ryszard Markiewicz, Ochrona danych osobowych. Komentarz, wyd. V
[4] Dz.U. 1997 Nr 133, poz. 883 t.j. Dz.U. z 2016 r. poz. 922
[5] Dz.U. Nr 100, poz. 1024

1. Obszar, o którym mowa w § 4 pkt 1 rozporządzenia, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.
2. Przebywanie osób nieuprawnionych w obszarze, o którym mowa w § 4 pkt 1 rozporządzenia, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

II

1. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych.
2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:

1. w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;
2. dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

III

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed: 1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego; 2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

IV

1. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
2. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 6 znaków.
3. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.
4. Kopie zapasowe:

1. przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
2. usuwa się niezwłocznie po ustaniu ich użyteczności.

V

Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, o którym mowa w § 4 pkt 1 rozporządzenia, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

VI

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do: 1) likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie; 2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie; 3) naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

VII

Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego.

2. Środki bezpieczeństwa na poziomie podwyższonym

VIII

W przypadku gdy do uwierzytelniania użytkowników używa się hasła, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

IX

Urządzenia i nośniki zawierające dane osobowe, o których mowa w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, przekazywane poza obszar, o którym mowa w § 4 pkt i rozporządzenia, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

X

Instrukcja zarządzania systemem informatycznym, o której mowa w § 5 rozporządzenia, rozszerza się o sposób stosowania środków, o których mowa w pkt IX załącznika.

XI

Administrator danych stosuje na poziomie podwyższonym środki bezpieczeństwa określone w części A załącznika, o ile zasady zawarte w części B nie stanowią inaczej.

3. Środki bezpieczeństwa na poziomie wysokim

XII

1. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
2. W przypadku zastosowania logicznych zabezpieczeń, o których mowa w ust. 1, obejmują one:

1. kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną;
2. kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.

XIII

Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

XIV

Administrator danych stosuje na poziomie wysokim środki bezpieczeństwa, określone w części A i B załącznika, o ile zasady zawarte w części C nie stanowią inaczej.

Todo

Uzupełnić numery strony w #f1 i #f2 na podstawie wydania papierowego.

Wskazać należy także na częściową uzasadnioną krytykę powyższych regulacji, których nieprawidłowe odczytanie może prowadzić do wręcz do ograniczenia bezpieczeństwa. W przywołanym zaączniku określono dla poziomu B i C, że jeśli do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. W poszczególnych przypadkach określono wymogi co do złożoności haseł.

Przepisy te bywają odczytywane jako wprowadzające bezwzględny wymóg cyklicznego zmienia hasła, jeżeli tylko formą uwierzytelniania jest hasło[6]. Takie odczytanie tych przepisów okazuje się jednak, że mógłoby prowadzić do ograniczenia bezpieczeństwa systemów informatycznych (zob. *Polityki haseł*).

[6] Adam Dobrawy, O potrzebie wzmocnienia ochrony danych osobowych, Blog Dobrawego, 30 marca 2016 roku, https://ochrona.jawne.info.pl/2016/03/30/o-potrzebie-zmian-ochronie-danych-osobowych/ [dostep 22 grudnia 2016 roku]

Wobec pojawiających się wątpliwości stanowisko w tym zakresie - w 2016 roku kilkukrotnie - przedstawiała Minister Cyfryzacji, która jest obecnie odpowiedzialna za ewentualną zmianę rozporządzenia. Należy w tym zakresie zwrócić szczególną uwagę na pismo Minister Cyfryzacji z dnia 12 maja 2016 roku[7]:

> Wymóg cyklicznej zmiany hasła w praktyce zwiększa poziom zabezpieczenia i ochrony danych osobowych. Jeżeli stosowana jest zmiana hasła co 30 dni, to dostęp do konkretnego systemu czy zbioru danych osobowych jest możliwy jedynie przez ww. okres. W przypadku, gdy system informatyczny nie wymusza zmiany hasła w określonych odstępach czasu, wówczas uzyskanie hasła przez osoby nieuprawnione może oznaczać uzyskanie permanentnego dostępu do danego systemu. W odpowiedzi na sugestię zawartą w petycji, zgodnie z którą przepisy prawa powszechnie obowiązującego powinny przewidywać możliwości autoryzacji wieloskładnikowej zamiast wymogu częstej zmiany haseł albo że wymóg zmiany haseł powinien przynajmniej zostać ograniczony w przypadku wprowadzenia takiej formy autoryzacji pragnę uprzejmie wyjaśnić, że przepisy rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, wprowadzają obowiązek cyklicznej zmiany haseł i ustanawiają jedynie minimalny poziom zabezpieczenia systemów informatycznych. Wymogi określone w załączniku do ww. rozporządzenia odnoszące się do haseł (w pkt Iy.2 oraz w pkt VIII), poprzedzone są zastrzeżeniem: *w przypadku gdy do uwierzytelniania użytkowników używa się hasła....* Przyjęcie takiego rozwiązania nie wyklucza zatem innych sposoby uwierzytelniania, jeżeli zapewniają odpowiednie środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych oraz zostały opisane w Polityce bezpieczeństwa, o której mowa w 4 ust. 5 ww. rozporządzenia. W związku z powyższym, w celu ochrony systemów informatycznych możliwe jest stosowanie bardziej złożonych zabezpieczeń, w tym autoryzacji wieloskładnikowej. Zaznaczyć należy, że bardziej zaawansowane formy uwierzytelniania są w Polsce już obecnie powszechnie stosowane zarówno w sektorze prywatnym, jak i publicznym. Pragnę również podkreślić, że w 2018 roku wejdzie w życie rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Powyższe stanowisko przemawiają dodatkowo za zasadnością wdrożonych alternatywnych form uwierzytelniania, których szczegółowa analiza została przedstawioan (*Dwuskładnikowe uwierzytelnienie*).

[7] pismo Minister Cyfryzacji znak BM-WSKN.053.5.2016 z dnia 12 maja 2016 roku stanowiące odpowiedź na petycje autora niniejszego opracownaia, http://mc.bip.gov.pl/skargi-wnioski-petycje/petycja-o-uwzglednienie-dwuskladnikowej-autoryzacji.html [dostęp 22 grudnia 2016 roku]

CHAPTER 5

Wymagania systemu

System ma zostać zaprojektowany w taki sposób, aby możliwe było jego wdrożenie przez różne podmioty. Jednak jego podstawowym odbiorcą jest Stowarzyszenie Sieć Obywatelska - Watchdog Polska. Jest ona niezależna organizacją społeczną, która aktywnie wykorzystuje w swojej pracy nowoczesne technologie. Posiada rozproszoną strukturę, gdzie podstawową komunikacji stanowią różnorodne aplikacje internetowe. Autor niniejszej publikacji jest jej członkiem. Stowarzyszenie swoje cele działania określa jako:

> Pilnujemy, żeby ludzie wiedzieli, co robi władza. Uczymy mieszkańców, że mogą pytać urzędy o to, dlaczego zlikwidowano szkołę, ile wydano na festyn czy gdzie planowana jest budowa wiatraków. Udzielamy tysięcy porad i setki razy chodzimy do sądu. Dzięki temu coraz więcej ludzi wie, że ma prawo pytać urzędy, te zaś wiedzą, że muszą odpowiadać.

Ze względu na dotychczasowy stan, który musi być uwzględniony w projektowaniu niniejszej aplikacji przyjęto, że architektura aplikacja będzie składać się z kilku komponentów. Jeden z nich będzie miał charakter centralny, a pozostałe będą uzupełniać dotychczas funkcjonujące aplikacje wzbogacając je o dodatkowe formy uwierzytelniania.

Centralny moduł uwierzytelniania i zarządzania użytkownikami stanowić będzie odrębną usługę Watchdog.ID (https://github.com/watchdogpolska/watchdog-id). Usługa ta będzie bazować na frameworku Django w języku Python 3.5. Pełnić będzie funkcje dostawcy tożsamości tak jak jest dla wielu stron Facebook (“Zaloguj przez Facebooka”). Jednak o wiele lepiej cel odzwierciedla odwołanie się do konta Google, które raz utworzone jest dostępne w szeregach systemów firmy Google w sposób niemal niezauważalny.

Ze względu na praktyczne wdrożenie aplikacji równie istotne co centralny moduł uwierzytelniania jest zapewnienie integracji z zewnętrznymi komponentami. Stowarzyszeniu wykorzystuje aplikacje w różnych technologiach. Są to m. in. aplikacje PHP, w tym m. in. ownCloud, liczne instancje Wordpressów. Jak również autorskie aplikacje Python z wykorzystaniem frameworka Django, które są otwarto źródłowe. Należy dla nich opracować integracje z Watchdog.ID.

System Watchdog.ID wymaga prac, aby zapewnić adekwatny poziom zabezpieczeń, wygląd i przyjazność dla użytkownika. Adekwatny poziom zabezpieczeń wynika w szczególności z wykorzystania systemu do kontroli dostępu do danych osobowych. W tym celu w szczególności mają być wdrożone formy dwuskładnikowego uwierzytelniania. Przystępny wygląd i przyjazność dla użytkownika wynika z otwartego charakteru systemu, który będzie wykorzystywany także przez odbiorców działań Stowarzyszenia. Konieczne jest zatem zapewnienie, że każda osoba zainteresowana działaniami Stowarzyszenia będzie mogła skutecznie uwierzytelnić swoje konto w systemie Watchdog.ID. Szczegółowe wymagania w zakresie bezpieczeństwa w związku z ochroną danych osobowych zostały przeanalizowane w rozdziale *Uwarunkowania prawne*.

5.1 Wymagania funkcjonalne

5.2 Wymagania niefunkcjonalne

CHAPTER 6

Opis wykorzystanych technologii

6.1 Python

6.2 Framework Django

6.2.1 Informacje ogólne

6.2.2 Struktura aplikacji

6.2.3 MVT

Model

Widok

Szablon

6.2.4 Formularze

6.2.5 URL dispatcher

6.2.6 Panel administracyjny

Kontrola dostępu

6.2.7 Inne właściwości

6.3 Heroku

6.3.1 Uzasadnienie wyboru platformy

6.3.2 Zdalne administrowanie platformą

6.4 Baza danych PostgreSQL

CHAPTER 7

Architektura zrealizowanego systemu

7.1 Koncepcyjna struktura

7.1.1 Podział na moduły

7.1.2 Architektura web

7.2 Implementacyjna struktura

7.3 Struktura modułu centralnego

7.3.1 Wykorzystane biblioteki

7.4 Struktura komponentów uzupełniających

CHAPTER 8

Szczegóły implementacyjne zrealizowanego modułu centralnego

CHAPTER 9

Instrukcja użytkowania systemu

CHAPTER 10

Podsumowanie

10.1 Wnioski końcowe

W ramach niniejszej pracy inżynierskiej został zaprojektowany, zaimplementowany, a także wdrożony system centralnego uwierzytelniania. Aplikacja ta jest otwarta na rozwój. Wykorzystuje wyłącznie biblioteki i technologie udostępniane jako darmowe oprogramowanie Open Source. Samodzielnie stanowi również takie oprogramowanie.

Dzięki wykorzystania języka Python, który jest językiem stosunkowo popularnym i łatwym do nauki możliwe jst łatwe wdrożenie do projektu nowego osób. Zapewniona dokumentacja również przyczynia się do zwiększenia zainteresowania projektem.

CHAPTER 11

Indeksy i tabele

- genindex
- modindex
- search