Szanowny Czytelniku, okazuje się, że obok zwykłego świata, znanego wszystkim nam od dziecka, istnieje też świat alternatywny, w którym jest zanurzone studiowanie i ogół pracy wielu polskich uczelni. Co więcej, świat ten pozwala na teleportację do analogicznych światów stowarzyszonych z uczelniami innych krajów. Ten **alternatywny świat to USOS.**

Wiemy, że USOS dla wielu jest równie egzotyczny jak tolkienowskie krainy i, podobnie jak one, tajemniczy i groźny. Dlatego często nie chcą o niego pytać, zarówno by nie ujawnić swojej niewiedzy, jak by nie dowiedzieć się o swoich względem niego powinnościach, wreszcie by nie wpaść w kompleksy, gdy odpowiedź okaże się niezrozumiała.

Z tego powodu poprosiliśmy Twórców USOS-a o reportaże ze stworzonego przez nich świata. I – aby tak nas, jak naszych Czytelników nie wpędzać w kompleksy – zasugerowaliśmy, by owe reportaże były ucharakteryzowane na listy do młodego badacza, na początku cyklu – kandydata na studia.

Spodziewamy się jedenastu listów – oto pierwszy z nich, poprzedzony stosowną preambułą.

Redakcja

Ze świata USOS

Pewno nie wiesz, co to USOS. Dokładniej pewno ***jeszcze*** *nie wiesz, co to USOS, bo jeśli planujesz studia na polskiej uczelni, to z dużym prawdopodobieństwem (rzędu 2/5, o ile to będzie uczelnia publiczna) poznasz USOS, a – co może ważniejsze – USOS pozna Ciebie i umożliwi Ci surfowanie po uczelnianym świecie wirtualnym. No dobrze, USOS to nickname (czyli ksywka)* ***Uniwersyteckiego Systemu Obsługi Studiów*** *– systemu informatycznego, który wspiera studentów, nauczycieli akademickich i uczelnianą administrację we wszystkim, co się wiąże z dydaktyką, od drukowania elektronicznych legitymacji studenckich, po rejestrację na zajęcia, pełnienie roli elektronicznego indeksu, archiwizowanie prac dyplomowych i wydawanie dyplomów ukończenia studiów. USOS to złożony twór, o rozbudowanej, rozproszonej architekturze, zaawansowanych mechanizmach komunikacji i synchronizacji danych, napisany w różnych technologiach, implementujący wiele ciekawych algorytmów, skalowalny, będący bogatym źródłem danych nie tylko dla uczelnianej administracji, lecz także dla statystyków, socjologów, psychologów czy speców od zarządzania. O takich systemach mówi się czasem, że stanowią zintegrowaną platformę informatyczną – zintegrowaną (gdyż potrafią się ze sobą porozumieć i wymienić dane) z innymi systemami informatycznymi, które wspierają funkcjonowanie uczelni wyższej.*

USOS powstaje na Wydziale Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego, rękoma pracowników i studentów, informatyków i matematyków. My – twórcy USOS – chcemy Wam zdradzić trochę sekretów kuchni. W kolejnych odcinkach opowiemy o tym, co, naszym zdaniem, w USOS-ie jest ciekawe, ambitne, co stanowi prawdziwe wyzwanie i dzięki czemu praca przy nim jest taką frajdą.

Zapraszamy do świata USOS.

Janina MINCER-DASZKIEWICZ z zespołem

Część 1 – Skąd USOS mnie zna i jakie są moje prawa, czyli o zarządzaniu tożsamością

Załóżmy, że dałeś się przekonać do studiowania na Uniwersytecie Warszawskim, na Wydziale Matematyki, Informatyki i Mechaniki (bądź dowolnym innym wydziale dowolnej innej z USOS-owych uczelni).

Dziewczyny też u nas studiują, a jakże, ale na potrzeby przykładu załóżmy, że mowa o studencie płci męskiej.

Zakładasz sobie konto w systemie *Internetowej Rekrutacji Kandydatów* (o wdzięcznej nazwie IRKa, `http://irk.uw.edu.pl`), podając swój PESEL (który będzie pełnił rolę identyfikatora konta) i wymyślone przez siebie hasło (to ważne, bo – jak się zaraz okaże – będzie Ci ono służyć długo i lepiej, żeby nikt inny go nie poznał). Możesz zresztą skorzystać ze swojego konta na platformie ePUAP (ale to całkiem inna historia, o której może napiszemy później).

ePUAP to elektroniczna *Platforma Usług Administracji Publicznej*, która umożliwia (między innymi) wiarygodną weryfikację tożsamości. Żeby założyć konto w ePUAP, trzeba poświadczyć tożsamość w przeznaczonym do tego urzędzie administracji państwowej. Niektóre aplikacje internetowe, takie jak np. IRKa, uwierzytelniają użytkownika za pomocą jego identyfikatora i hasła w ePUAP.

Któregoś dnia logujesz się do IRKi i bingo! Zostałeś przyjęty. Musisz raz odbyć osobistą wycieczkę do dziekanatu, żeby złożyć papiery, ale potem jedziesz wreszcie na zasłużone wakacje. We wrześniu chciałbyś jednak poznać swój plan zajęć, wyczytałeś też w USOSowni (to taki portal informacyjny dla studentów UW, `http://usosownia.uw.edu.pl`), że wkrótce ruszają rejestracje na wuefy i oguny (przedmioty ogólnouniwersyteckie). Wchodzisz na stronę USOSweba

(wirtualnego dziekanatu), logujesz się, używając danych konta z IRKi i znowu bingo! Nie tylko logowanie się powiodło, ale system wyświetlił Twoje imię i nazwisko, Twój plan zajęć, harmonogram rejestracji na zajęcia dodatkowe, a nawet zdjęcia profesorów i kolegów z grupy. Wchodzisz na centralny serwer pocztowy UW – to samo, do portalu uczelnianego i wydziałowego – to samo, rozpoznaje Cię system biblioteczny, Moodle (czyli platforma zdalnego nauczania), lokalne laboratorium komputerowe i wiele innych uczelnianych serwisów. Nawet nie musisz się po raz drugi logować, PESEL i hasło z IRKi okazują się być magicznym kluczem do wirtualnego świata. Na dodatek jeśli jakąkolwiek aplikację odwiedzasz niezalogowany, to zawsze jesteś odsyłany na tę samą stronę z budzącym zaufanie uniwersyteckim orzełkiem.

Chciałbyś wiedzieć, kto za tym stoi? Mówiąc w skrócie, IRKa, USOS, CAS, SSO i LDAP. IRKę już znasz. To IRKa w procesie zwanym *elektroniczną immatrykulacją* przekazała wszystkie Twoje dane do USOS. Także PESEL i hasło. Nie martw się, hasło jest odpowiednio zaszyfrowane, postać niezaszyfrowaną hasła znasz tylko Ty. A z postaci zaszyfrowanej tak łatwo odszyfrować się go nie da, bo stoi za tym kawał solidnej matematyki.

Dokładniej, jest to funkcja jednokierunkowa (ang. *one-way function*), czyli funkcja f o takiej własności, że dla danego y (zaszyfrowanego hasła), takiego, że $f(x) = y$, wyznaczenie x (czyli hasła przed zaszyfrowaniem) jest bardzo trudne. Najpopularniejsze funkcje w jedną stronę to SHA-1 i MD5, ale ponieważ ostatnio okazało się, że w ich przypadku „bardzo trudne" nie jest „wystarczająco trudne" z praktycznego punktu widzenia, więc trwają poszukiwania ich dobrych następców.

Poza tym USOS to hasło od razu wysyła dalej, do centralnego repozytorium danych o kontach i rolach. A kto i jak może stamtąd te dane pobrać? Tylko CAS, który potrafi czytać dane z tego repozytorium, korzystając z protokołu LDAP (ang. *Lightweight Directory Access Protocol*). To CAS (ang. *Central Authentication Service*), czyli **Centralny System Uwierzytelniania** jest tutaj głównym motorniczym. Wszystkie serwisy, z których chcesz skorzystać, podczas procedury logowania przekierowują Cię na stronę logowania CAS (tę z orzełkiem). Tam jesteś proszony o wprowadzenie identyfikatora i hasła. CAS szyfruje hasło, które wprowadzasz (wspomnianą funkcją jednokierunkową) i porównuje z tym, co jest trzymane w repozytorium haseł. Jeśli wynik wyjdzie inny, to logowanie się nie powiedzie. Jeśli ten sam, to otwiera się przed Tobą brama do wirtualnego świata uczelni.

CAS po zakończonym sukcesem uwierzytelnieniu przekazuje Twojej przeglądarce specjalne ciasteczko (ang. *ticket granting cookie*). Przeglądarka przechowuje je do zamknięcia i używa do uwierzytelniania, nie tylko w tym serwisie, z którego właśnie chcesz skorzystać, ale także wszystkich innych, które współpracują z CAS. To dzięki temu, przechodząc na strony innych serwisów, nie musisz ponownie wprowadzać identyfikatora i hasła, bo CAS po ciasteczku rozpoznaje, że już wcześniej zweryfikował Twoje dane. To jest tzw. **zasada pojedynczego logowania**, czyli SSO (ang. *single sign-on*).

Przeczytaj uważnie treść strony informacyjnej CAS (`http://logowanie.usos.edu.pl/info/pl`). Ważne są aspekty bezpieczeństwa opisanego tutaj procesu. Znane są przypadki tzw. wykradania tożsamości (ang. *phishing*). Jednokrotne logowanie do wielu serwisów jest wygodne, ale też potencjalnie ryzykowne. Pamiętaj, żeby hasło wprowadzać tylko na stronie z orzełkiem, upewniwszy się wcześniej, że strona korzysta z szyfrowanego protokołu (adres zaczyna się od `https://`, a nie od `http://`) i CAS przedstawia się poprawnym, rozpoznawalnym certyfikatem.

Certyfikat serwera to taki dowód tożsamości wydawany przez upoważnione do tego zaufane instytucje, które swoim autorytetem poświadczają wiarygodność certyfikowanego serwisu.

A jeśli zapomnisz hasła? Czy jak poprosisz, to prześlą nowe mailem? Przecież żeby się zalogować do uczelnianego systemu pocztowego, potrzebujesz tego samego hasła, więc kółko się zamyka. To może szybko założyć konto w jednym z darmowych serwisów pocztowych? To nic nie da, żaden znający się na rzeczy administrator nie wyśle otwartym tekstem hasła, które chroni dostępu do Twojej uczelnianej tożsamości. Procedura odzyskiwania hasła będzie, niestety, bolesna, za to stuprocentowo bezpieczna. Na stronie CAS możesz wpisać nowe hasło, które będzie chronione krótkim kodem aktywacyjnym (jest jednorazowy i ma kilkudniowy okres ważności). Z kodem aktywacyjnym musisz się udać do dziekanatu. Pracownik dziekanatu sprawdzi Twoją tożsamość i wprowadzi do USOS-a kod aktywacyjny. USOS wyśle kod do CAS, a CAS automatycznie aktywuje konto. No tak, uciążliwe, nie da się tego zrobić zdalnie, ale za to Twoje nowe hasło jest całkowicie bezpieczne – nikomu nie musisz go ujawniać, nie poznał go nawet pracownik dziekanatu, któremu udostępniasz tylko krótki i prosty do podyktowania kod aktywacyjny.

CAS jest podstawowym narzędziem stosowanym do **zarządzania tożsamością** (ang. *identity management*). Zarządzanie tożsamością obejmuje dwa ważne procesy:

- **uwierzytelnianie** (ang. *authentication*) – proces weryfikowania tożsamości osoby ubiegającej się o dostęp do serwisu,
- **autoryzację** (ang. *authorization*) – proces określania rodzaju dostępu przyznawanego użytkownikowi.

Proces uwierzytelniania już poznałeś. Autoryzacja sprowadza się do rozpoznania, że jesteś studentem, studiujesz (przykładowo) matematykę na Wydziale

MIM, jesteś członkiem samorządu studenckiego. Występujesz na uczelni w określonych **rolach**, a każda taka rola daje Ci konkretne uprawnienia. Jako student możesz zabierać głos na forum dyskusyjnym w USOSowni i wypożyczać książki w systemie bibliotecznym, jako student MIM masz dostęp do portali z licencjonowanym oprogramowaniem, jako członek samorządu studenckiego możesz wysyłać maile do studentów MIM. Widać, że rola decyduje o Twoich **uprawnieniach**. Jak powstają role? Na szczęście w pełni automatycznie (to eliminuje ludzką pomyłkę) – jeśli tylko w USOS pojawia się informacja, że zostałeś przyjęty na studia, USOS buduje odpowiednią rolę i wysyła ją do repozytorium, z którego korzysta CAS.

Rola to nic innego jak **widok** (ang. *view*) w bazie danych, zbudowany automatycznie na podstawie danych przechowywanych w jednej lub kilku tabelach.

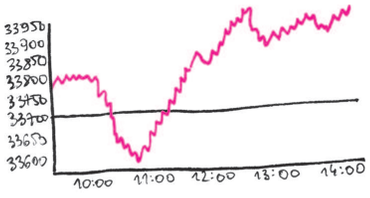
CAS dowiaduje się, że zacząłeś występować w roli studenta. Zadziała to także całkowicie automatycznie w odwrotnym przypadku – gdy skończysz studia i przestaniesz być studentem. Nagle – niestety – uniwersyteckie serwisy przestaną Ciebie rozpoznawać i serdecznie witać. Wtedy jednak będziesz już absolwentem i inne problemy będą zaprzątały Twoją głowę.

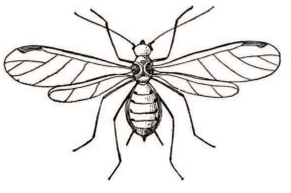
Jak widzisz, proces zarządzania tożsamością decyduje o Twoim istnieniu w wirtualnym świecie macierzystej uczelni. I – potencjalnie – wielu innych. Duża grupa uczelni europejskich, opierając się na wzajemnym zaufaniu, zbudowała federację na bazie swoich lokalnych systemów uwierzytelniania. Takie **federacyjne zarządzanie tożsamością** (ang. *federated identity management*) polega na tym, że gdy logujesz się w systemie informatycznym innej uczelni, jesteś przekierowywany do strony logowania CAS macierzystej uczelni (znowu znajomy orzełek) i jeśli Twój CAS Ciebie rozpozna, to logowanie się powiedzie. Na podobnej zasadzie działa **eduroam** (ang. ***edu**cation **roam**ing*), czyli sieć umożliwiająca bezpieczny roaming użytkowników jednostek naukowych oraz szkolnictwa wyższego. W praktyce oznacza to, że jeśli odpowiednio skonfigurujesz dostęp do eduroam z prywatnego laptopa czy komórki w swojej uczelni, to bez żadnych dodatkowych zmian w ustawieniach logowania będziesz się mógł podłączyć do sieci w pozostałych uczelniach z federacji. I surfować za darmo.

Dasz się poznać USOS-owi, a otworzą się przed Tobą drzwi nie tylko wirtualnego świata Twojej uczelni, ale także wiele innych. Oj, warto żyć z USOS-em w przyjaźni.

Informatyk gra na giełdzie

Tomasz IDZIASZEK





Nasz znajomy informatyk zdecydował się zainwestować część swoich oszczędności na giełdzie papierów wartościowych. Jak na informatyka przystało, do grania na giełdzie postanowił zaprząc komputer. W tym celu, korzystając z najnowszych trendów sztucznej inteligencji, napisał program, który na podstawie przeszłych notowań giełdowych przewiduje, jak kurs akcji będzie się zmieniał w przyszłości, i podejmuje decyzje o kupnie bądź sprzedaży. Nasz znajomy przetestował program, uruchamiając go na dużym zbiorze archiwalnych notowań. Zastanawia się teraz, jak dobrze jego program sobie poradził – stanął zatem przed problemem wyznaczenia najlepszej możliwej gry na giełdzie, jeśli znamy wszystkie notowania.

Model gry na giełdzie będzie następujący. Mamy daną tablicę $A[0..n]$ z notowaniami giełdowymi w kolejnych dniach: $A[i]$ oznacza cenę jednej akcji w i-tym dniu (dla uproszczenia przyjmiemy, że mamy tylko jeden rodzaj akcji). Na początku dysponujemy kwotą P i możemy wykonać nie więcej niż m operacji kupna-sprzedaży akcji (zakładamy, że możemy kupować ułamkową liczbę akcji). Zauważmy, że nie potrzebujemy wykonywać operacji równolegle (tzn. przed każdym kupnem opłaca się nam najpierw sprzedać wszystkie posiadane akcje). Ponadto warto też kupować akcje za całą dostępną kwotę. Z tego wynika, że jeśli pierwszą operację kupna przeprowadzimy w dniu k_1, a odpowiadającą jej sprzedaż w dniu s_1, to po tej operacji będziemy mieli kwotę $P \cdot A[s_1]/A[k_1]$. Naszym celem jest zmaksymalizowanie kwoty po wszystkich m operacjach, czyli iloczynu

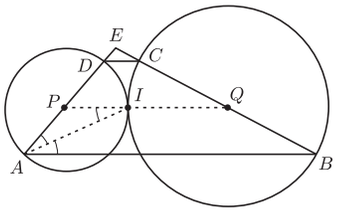
$$P \cdot \prod_{1 \leqslant i \leqslant m} \frac{A[s_i]}{A[k_i]}.$$

Możemy pozbyć się mnożeń i dzieleń, logarytmując powyższy wzór. Innymi słowy, równoważnie możemy zmaksymalizować sumę

$$\log P + \sum_{1 \leqslant i \leqslant m} (\log A[s_i] - \log A[k_i]).$$

W końcu jeśli wprowadzimy pomocniczą tablicę $a[0..n-1]$, która zawierać będzie zmiany zlogarytmowanych notowań, tzn. $a[i] = \log A[i+1] - \log A[i]$, to

Rozwiązanie zadania M 1399.
Niech P i Q będą odpowiednio środkami ramion AD i BC.



Połączmy je odcinkiem. Jest on równoległy do podstawy AB i zawiera punkt I. Dlatego $\sphericalangle BAI = \sphericalangle AIP = \sphericalangle PAI$, więc I leży na dwusiecznej kąta EAB. Analogicznie I leży na dwusiecznej kąta ABE, więc przechodzi przez niego także trzecia dwusieczna trójkąta ABE.