DynAuth

System uwierzytelniania dynamicznego

Otoczenie rynkowe (1/5)

Wymogi prawne

NIS 2 - Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii Europejskiej.

Art. 3 Podmioty kluczowe i ważne - wykaz załącznik
do dnia 17 kwietnia 2025 r.

Art. 34. ust. 4 i ust. 5 - kary do 10,000,000 EUR

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.

Art. 8 ust. 3 Do dnia 18 września 2015 r. - minimalne techniczne specyfikacje, standardy i procedury dla: niski, średni i wysoki poziom bezpieczeństwa dla środka identyfikacji elektronicznej.

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. Załącznik 2.3. Uwierzytelnianie

Średni	Jak przy poziomie niskim oraz:
1.	**Uwolnienie danych identyfikujących osobę jest poprzedzone wiarygodną weryfikacją środka identyfikacji elektronicznej oraz jego ważności za pomocą uwierzytelniania dynamicznego.**

ISO/IEC 29115
rekomendacje kryptografii OTP

zastąpione przez

„uwierzytelnianie dynamiczne"

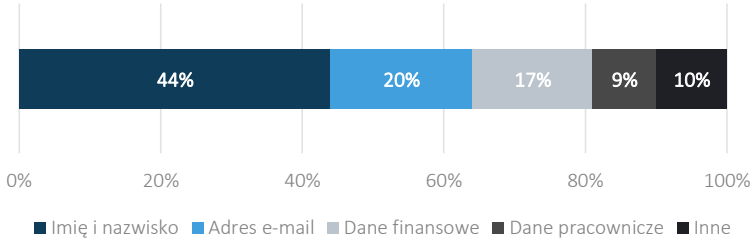
Otoczenie rynkowe (2/5)

Zagrożenia – do incydentów dochodzi w co drugiej organizacji

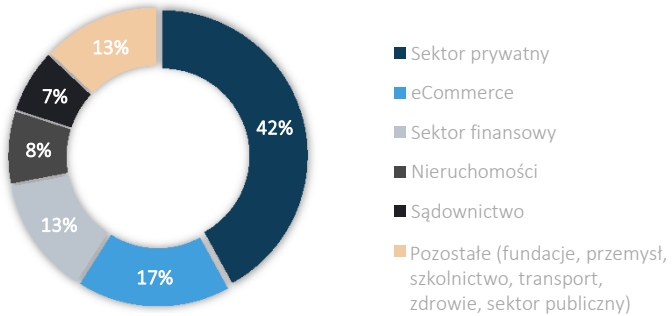
0,46 Średnia liczba incydentów przypadających na jedną organizację

76% Incydentów zakończyło się poinformowaniem zainteresowanych o naruszeniu

Najczęściej naruszane kategorie danych | %

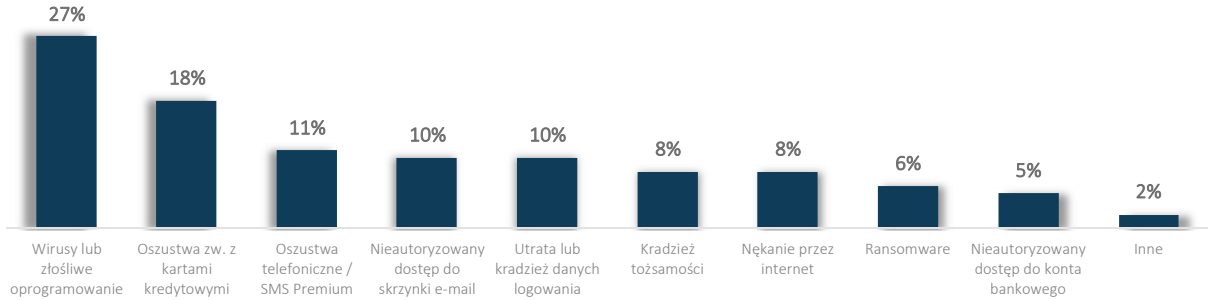


Branże w których dochodziło do incydentów | %

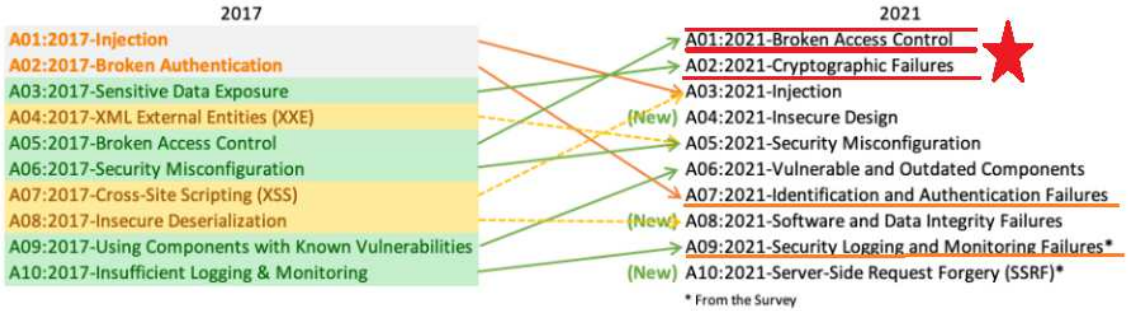


Źródło: Badanie przeprowadzone przez Związek Firm Ochrony Danych Osobowych od 05.2018 do 05.2019 w którym objęto 277 organizacji

Najczęstsze incydenty naruszenia bezpieczeństwa | %



TOP10 zagrożeń bezpieczeństwa aplikacji internetowych | %



Otoczenie rynkowe (3/5)

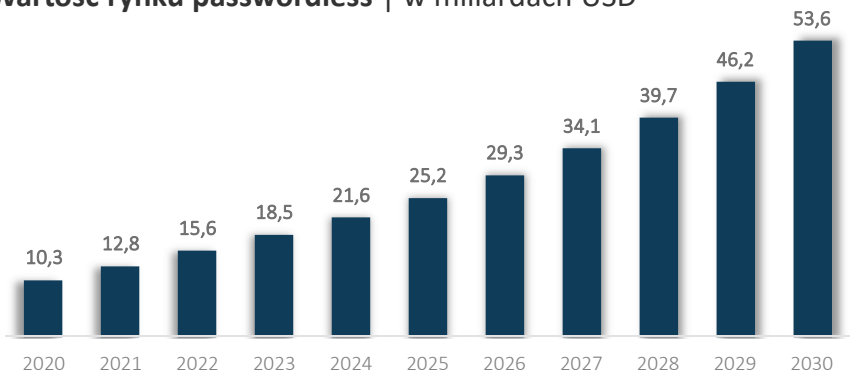
Rozwój i cyfryzacja

Rozwijający się świat daje duże możliwości rozwoju, a z drugiej strony daje nowe narzędzia cyberprzestępcom.

Cyberprzęstpcy wykorzystują AI do identyfikacji celów:

- skanują internet w poszukiwaniu podatnych systemów na atak,
- tworzą AI-boty w celu naśladowania ludzkich zachowań, aby skuteczniej unikać wykrycia przez systemy bezpieczeństwa,
- generują ukierunkowane e-maili phishingowe za pomocą AI, być może przygotowane na podstawie wielu zestawów danych zdobytych w Dark Web, tak aby zawierały wiarygodne szczegóły, które pomogą zwabić cel i zbudować zaufanie,
- tworzą coraz bardziej wyrafinowane złośliwe oprogramowania, np. wykorzystując sztuczną inteligencję do znajdowania możliwych do wykorzystania wzorców w systemach bezpieczeństwa i tworzą złośliwe oprogramowanie, które jest specjalnie zaprojektowane w celu uniknięcia wykrycia.

Wartość rynku passwordless | w miliardach USD



Źródło: Statista 2023

Wartość rynku „uwierzytelniania passwordless" w roku **2021 wyniosła 12,7 MLD USD**.

Szacowane jest, że w roku **2030 będzie to około 53.6 MLD USD**.

Źródło: Microsoft fights phishing with passwordless authentication for Azure AD on iOS and Android (venturebeat.com)

Ustawa o aplikacji mObywatel wchodzi w życie. Czy Twoje dane będą bezpieczne?

W rządowym serwisie moje.gov.pl wykryto poważną lukę bezpieczeństwa lub błąd w oprogramowaniu, który pozwalał dowolnej osobie mieć wgląd do naszych danych w paszporcie.

Otoczenie rynkowe (4/5)

Rozwiązania konkurencyjne, ale czy na pewno?

1 **Uwierzytelnianie dwuskładnikowe (2FA)**: bank kontroluje certyfikat i kod SMS -> możliwe przejęcie i podsłuchanie.

Uwierzytelnianie to nie daje bezpieczeństwa przed pozyskaniem danych ze strony cyberprzestępców w ataku phishing.

Nie spełnia wymogu „uwierzytelnianie dynamiczne”

2 **YubiKey (certyfikat z kluczem prywatnym na Tokenie):** klucz publiczny przekazywany do np. banku -> możliwe skopiowanie lub złamanie Certyfikatu YubiKey.

Ważność oraz czas życia „Certyfikatu”, a więc również klucza kryptograficznego, określa producent i nie jest to „Certyfikat” spełniający wymagania kryptografii z kluczami jednorazowymi oraz nie jest jasne czy ten „Certyfikat” służy jednemu urządzeniu czy też wielu „użytkownikom”.

Źródło: https://www.sirt.pl/czy-uwierzytelnianie-dwuskladnikowe-2fa-zabezpieczy-przed-phishingiem/

Otoczenie rynkowe (5/5)

Rozwiązania konkurencyjne, ale czy na pewno?

3 **Google Authenticator (GA):** umożliwia kopiowanie lub klonowanie urządzenia realizującego uwierzytelnianie, np. poprzez współdzielony kod startowy otrzymany jako hasło od „GA" -> oznacza to, że jest możliwe uwierzytelnianie poprzez duplikat np. „wykradzionego" kodu startowego otrzymanego od „GA" w momencie startu aplikacji.

Zatem to „Goog[illegible] w „czyimś imieniu". Co oznacza, że to kon[illegible].

Ponadto „GA" pobrana na np. smartfon synchronizuje się poprzez generowanie „tego samego" sześciocyfrowego kodu, zatem jest możliwość skopiowania również metody czyli algorytmu generowania kodu (ponieważ ta sama wartość „sześciocyfrowa" [illegible] stanowi zaufaną trzecią stronę zarządzającą „cyfrowymi kodami dostępu".

Nie spełnia wymogu „uwierzytelnianie dynamiczne"

Ponadto, sześciocyfrowe kody dostępu są ważne przez 30 sekund i nie spełniają właściwości kodów jednorazowych i unikatowych chociażby ze względu na powtarzalność 1/999999. Dodatkową podatnością jest korzystanie z „plików" np. „cooki" w realizacji usługi definiowania „urządzenia zaufanego" mającego możliwość uwierzytelniania się przez więcej niż jedno urządzenia w tym samym okresie, zatem nie są spełnione założenia unikalnych kodów uwierzytelniających i możliwy jest proces w którym kilka różnych „urządzeń" może w tym samym czasie się uwierzytelniać nawet bez wiedzy i zgody „właściciela".

4 **DynAuth:** klucze jednorazowe generowane są przez „użytkownika" i bank nie ma możliwości podszycia się pod użytkownika -> nie jest możliwe skopiowanie ani też odgadnięcia klucza jednorazowego.

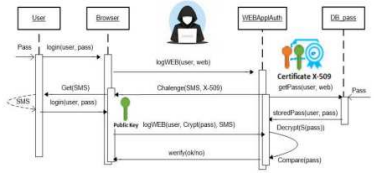
Rozwiązanie (1/4)

DynAuth – co oznacza i kiedy musi być stosowane?

1. **Stosowane definicje**

3) „uwierzytelnianie dynamiczne" oznacza proces elektroniczny z zastosowaniem kryptografii lub innych technik służący dostarczeniu na żądanie elektronicznego dowodu, iż podmiot podlegający uwierzytelnieniu jest w posiadaniu danych identyfikacyjnych lub dane te znajdują się pod jego kontrolą, oraz który ulega zmianie z każdym uwierzytelnieniem zachodzącym między podmiotem podlegającym uwierzytelnieniu a systemem weryfikacji tożsamości danego podmiotu;

Authenticate - now …
PBKDF2, JWT …

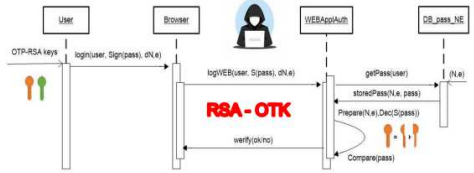


Phishing, Replay attack,
Atak Man In The Middle,
Atak Man In The Browser,
Quantum Computing

stay secure, use

Dynamic Authenticate - future

the first solution in that meets the requirements of QuantumResists base at Pat. 218339 …



~~Phishing, Replay attack,~~ Atak Man In The Middle, Atak Man In The Browser, ~~Quantum Computing~~

RSA-OTKeys and QuantumResists key „excange protocol", meeting the requirements defined in ISO/IEC29115 and "dynamic authentication" in UE 1502/2015

Poziom zaufania	Wymagane elementy
Średni	Jak przy poziomie niskim oraz: 1. Uwolnienie danych identyfikujących osobę jest poprzedzone wiarygodną weryfikacją środka identyfikacji elektronicznej oraz jego ważności za pomocą uwierzytelniania dynamicznego. 2. Mechanizm uwierzytelniania jest sposobem realizacji kontroli zaufania na potrzeby weryfikacji środków identyfikacji elektronicznej, dzięki któremu jest mało prawdopodobne, aby takie działania jak zgadywanie, podsłuchiwanie, odtwarzanie lub manipulowanie komunikacji przez atakującego o umiarkowanym potencjale ataku mogło zachwiać mechanizmami uwierzytelniania.
Wysoki	Jak przy poziomie średnim oraz: mechanizm uwierzytelniania jest sposobem realizacji kontroli zaufania na potrzeby weryfikacji środków identyfikacji elektronicznej, dzięki któremu jest mało prawdopodobne, aby takie działania jak zgadywanie, podsłuchiwanie, odtwarzanie lub manipulowanie komunikacji przez atakującego o wysokim potencjale ataku mogło zachwiać mechanizmami uwierzytelniania.

DynAuth

sprawia, że utrata danych osobowych czy danych logowania nie zagrozi bezpieczeństwu użytkownika.

Rozwiązanie (2/4)

DynAuth – co oznacza i kiedy musi być stosowane?

Zaufana strona, klient - ma "portfel" o ustalonej w pierwszym kontakcie "zawartości" początkowej X np. 1024 bitowa wartość. Druga strona "ufająca" np. bank znając poprzez uzgodnienie ze stroną „zaufaną" w procesie pierwszego kontaktu ustalili "wartości X portfela" np. Gotówki. Strona „ufająca" wie kim jestem i jaka jest wartość X. Następnie ja jako strona zaufana wykonując transakcję np. 100 PLN, inicjuję czyli formułuję/zlecam transakcję i ją uwierzytelniam, np. informując stronę ufającą (bank) jawnie, że chcę przekazać kwotę 100 PLN, zatem mój portfel będzie miał wartość X–100, a następnie tą X–100 wartość używam jako klucz do potwierdzenia transakcji. Czyli X–100 jest użyte jako "jednorazowy klucz uwierzytelniający". Strona „ufająca" - np. bank dostał ode mnie „ID" oraz zlecenie transakcji na 100 PLN podpisaną kluczem o wartości X–100, zatem tylko np. bank jest w stanie "odszyfrować" podpisaną transakcję, ponieważ tylko strona ufająca – bank znał wartość X. Po udanej transakcji ja aktualizuję swój klucz do wartości X–100, która będzie nowym kluczem. W tej metodzie, nawet bank znający wartość X nie jest w stanie wykonać transakcji w moim imieniu, a jeśli by spróbował to zrobić to ja łatwo udowodnię, że takiej transakcji nie zlecałem, bo np. mam historię ostatnich transakcji, czyli kluczy kryptograficznych, a nawet bank nie ma dostępu do mojej tożsamości, czyli "mojego nośnika danych o wartości portfela" i tutaj rozwiązań może być wiele, mogę pamiętać ostatnią kwotę, czy też mieć zapisaną na "pendrive„, a może zapisaną na personalnym "chipie" itp.

Wykonanie transakcji jest potwierdzone kluczem jednorazowym będącym pod kontrolą lub w posiadaniu jedynego użytkownika tożsamości cyfrowej, którą otrzymał w momencie wydania środka identyfikacji elektronicznej jako unikatową wartość np. rozmiaru 1024 bity (lub dowolny rozmiar). W związku z tym, tylko użytkownik może ten jednokrotnego użycia klucz zmieniać, ponieważ tylko użytkownik ma pod kontrolą lub posiada wartość klucza kryptograficznego, którą to wartością „uwierzytelnia transakcję". Zatem „haker" nawet znając wszystkich dane np. kredytobiorcy, nie będzie mógł wykonać „uwierzytelnienia" tej transakcji ponieważ nie posiada „jednorazowego klucza kryptograficznego umożliwiającego uwierzytelnienie tej transakcji", nawet jeśli zna wszystkie dane (np. NIP, pesel, itd.) oraz zna lub wie o poprzednich transakcjach (bo ma np. ich kopie), to i tak nie uwierzytelni tej transakcji, ponieważ usiałby zgadnąć jaką jednorazową wartość rozmiaru 1024 bitów (lub większego rozmiaru, bo rozwiązanie jest skalowalne) wygeneruje posiadacz danej "tożsamości" – jako metoda np. to co mam z One Time Pad. **Zgadnięcie wartości np. 1024 bitów nie jest możliwe nawet z zastosowaniem komputerów kwantowych. To jest jedna, ale nie jedyna z przewag konkurencyjnych rozwiązania DynAuth nad wszystkimi innymi oferowanymi rozwiązaniami.** Co więcej, nawet druga strona przyjmująca transakcję nie wie jaką wartością „zmieniającego się z każdą transakcją klucza kryptograficznego związanego tylko z jedną wartością - tożsamości z użyciem, której dokument zostanie uwierzytelniony – podpisana transakcja".

Rozwiązanie (3/4)

DynAuth – zalety na tle innych dostępnych rozwiązań

Istniejące rozwiązania

Existing encryption types - pre & post quantum

Name	Function	pre-quantum security level	post-quantum security level
Symmetric cryptography			
AES-128	bloc-cypher	128	64
AES-256	block-cypher	256	128
Salsa20	stream cypher	256	12
GMAC	MAC	128	128
Poly1305	MAC	128	128
SHA-256	hash-function	256	128
SHA-3	hash function	256	128
Public-key cryptography			
RSA-3072	encryption	128	broken
RSA-3072	signature	128	broken
DH 3072	key exchange	128	broken
DSA-3072	signature	128	broken
256-bit ECDH	key exchange	128	broken
256-bit ECDSA	signature	128	broken

Source: University of Illinois, Bernstein & Lange

Wady innych rozwiązań

MFA w tym 2FA: uwierzytelnianie dwuskładnikowe –> atak powtórzeniowy „przejęcie”.

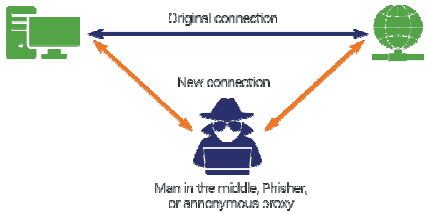
YubiKey: certyfikat z kluczem prywatnym na Tokenie -> kto wystawcą, wiele kopii, kryptoanaliza.

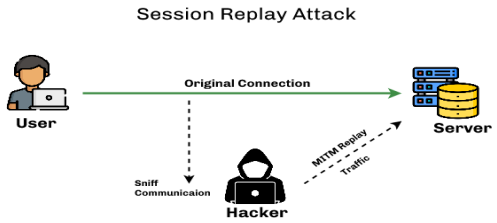
Google Authenticator (GA) -> przejęcie SMS, atak man-in-the middle zgodnie z podatnościami wskazanymi po prawej stronie.

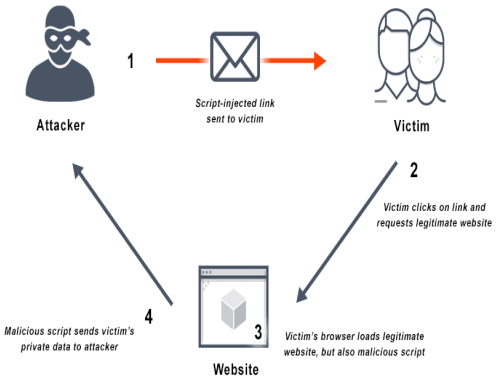
Co wyróżnia DynAuth?

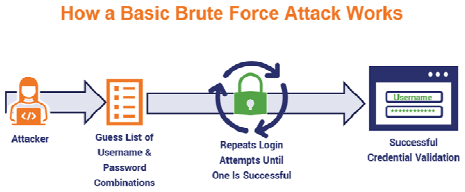
DynAuth jest oparty na OTP, dowód bezwzględnego bezpieczeństwa C. Shannon 1949. Jedyny proponowany system uwierzytelniania z OTP z kluczami jednorazowymi generowanymi po stronie zaufanej – klienta. Odporny na znane metody ataków i znane podatności:

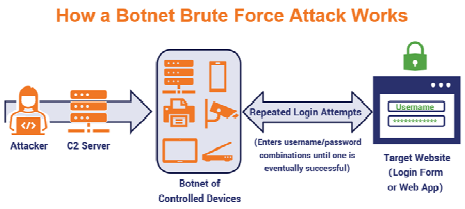
- **klucze jednorazowe niemożliwe do powtórzenia**, a przejęcie „użytego” już klucza nie stanowi zagrożenia,
- **jeden ważny klucz kryptograficzny**,
- **wystawcą klucza jest strona zaufana – nikt poza stroną zaufaną nie zna klucza który zostanie użyty do kolejnej transakcji**,
- **komputer kwantowy** może odgadnąć mnóstwo np. 2^1024 możliwych kluczy, ale **nie potrafi wskazać, który z nich został użyty**.

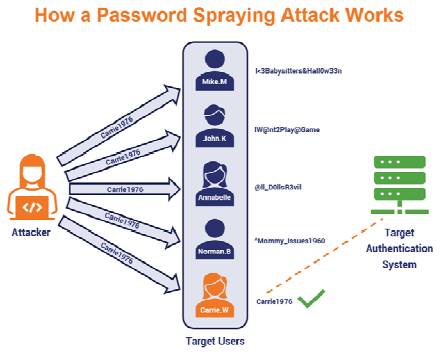












Rozwiązanie (4/4)

DynAuth – opinia dotycząca systemu uwierzytelniania DynAuth

Wrocław, 13 kwietnia 2022

dr hab. inż. Janusz Biernat,
em. prof. Politechniki Wrocławskiej,
email: janusz.biernat@op.pl

Opinia o koncepcji systemu uwierzytelniania
autorstwa dra inż. Janusza Jabłońskiego

Zasadniczą cechą proponowanej koncepcji jest całkowita zmiana filozofii uwierzytelniania, a istotnym jej elementem jest zapewnienie bezpiecznego przesyłania unikatowych kluczy.

Znane protokoły uwierzytelniania są oparte na jednej z dwóch koncepcji:

1. Stroną aktywną w procedurze uwierzytelniania jest **serwer**, świadczący usługę o którą ubiega się **klient**. **Serwer** w celu weryfikacji uprawnień **klienta** sprawdza jego tożsamość.
2. Strony procedury uwierzytelniania korzystają z usługi **zaufanego autorytetu**, który wydaje klientowi **certyfikat** uznawany przez serwer.

W ramach obu koncepcji wymiana informacji następuje w trybie kryptografii asymetrycznej (np. RSA),gdzie strona uwierzytelniana (klient) szyfruje swoją tożsamość. Zasadniczą wadą obu koncepcji jest, jakkolwiek mało prawdopodobna, możliwość nieuczciwego posłużenia się tożsamością klienta po stronie serwera.

W koncepcji dra Jabłońskiego stroną aktywną procedury uwierzytelniania jest **klient**, który kontroluje wykonanie procedury, co uniemożliwia nieuczciwe użycie jego tożsamości.

Aby zapewnić bezpieczeństwo dystrybucji klucza, dr Jabłoński proponuje wykorzystanie szyfrowania w trybie RSA z użyciem nowych kluczy w każdej transakcji. W tym trybie odkrycie klucza deszyfrującego przy znajomości klucza szyfrującego jest skrajnie trudne. Zmiana klucza szyfrującego następuje przez przesyłanie informacji o powiązaniu kolejnych kluczy zamiast tych kluczy. Poświadcza to jednocześnie tożsamość wysyłającego, bo tylko on jest w stanie wygenerować poprawną informację o nowym kluczu.

Proponowane rozwiązanie jest odporne na zakłócenie transmisji, bo przesyłane do drugiej strony dane nowego klucza szyfrującego są zawsze odnoszone do klucza użytego w ostatniej poprawnej transakcji. Skutkiem zakłócenia transmisji jest zidentyfikowanie niepoprawnej informacji, co gwarantuje wykrycie błędu. W takiej sytuacji następuje wysłanie powiązania odniesionego do poprzednio użytego poprawnego klucza.

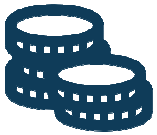
W razie intensywnych sesji, ostatnio użyty klucz mógłby służyć do identyfikacji klienta, co wymagałoby modyfikacji bazy klientów. Identyfikacja może być jednak zrealizowana za pomocą dowolnego protokołu *„challenge-and-response"*.

Proponowane **innowacyjne** rozwiązanie zapewnia nie gorszy poziom bezpieczeństwa niż rozwiązania obecnie używane, a z perspektywy klienta jest bardziej godne zaufania. Może być użyte zarówno jako część protokołu komunikacyjnego, jak też realizowane niezależnie w innych kontekstach internetowej wymiany informacji.

Janusz Biernat

Potencjał (1/2)

Szeroki zakres branż w których rozwiązanie DynAuth może być stosowane to (UE)255/2022 - ”Usługi kluczowe”, ale nie tylko



Instytucje finansowe

Sektor publiczny

Sektor zdrowotny

Firmy energetyczne

Media

Sektor zbrojeniowy

eCommerce

Szkolnictwo i edukacja

Przemysł

TMT

Potencjał (2/2)

DynAuth może znaleźć zastosowanie dla bezpieczeństwa także poza siecią

Rozwiązanie DynAuth może być stosowane np. w branży automotive integrując „uwierzytelnianie dynamiczne” z oprogramowaniem komputera sterującego pojazdem np. zamkiem samochodu, który realizuje bezpieczny dostęp do pojazdu.

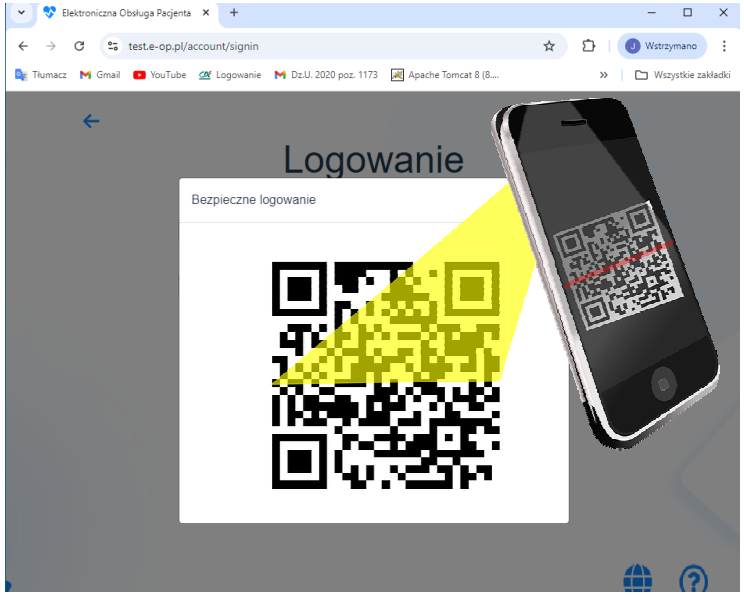
Podobnie jak w przypadku DynAuth, aplikacja połączona z tym "sterownikiem" jest sterowana z aplikacji na smartfonie. Realizując uwierzytelnianie dostępu do dowolnego "chronionego fizycznym urządzeniem np. zamkiem czy drzwiami".

Użycie takiego zabezpieczenia "uodparnia" np. pojazd na wszelkie znane dziś podatności i systemy włamaniowe czy to "transmiter" jako przekaźnik sygnału z kluczyka czy też inne znane i dziś stosowane.

Podobne rozwiązanie mogą być stosowane do pomieszczeń z kontrolą dostępu do procesów w Przemysł 4.0 czy też do infrastruktury Internetu lub „Cloud”

Zespół wdrożeniowy DynAuth

Wynalazca i doświadczony zespół programistów



„Uwierzytelnianie dynamiczne” spełnia wymogi (UE)2022/2555 – NIS2 – dla (UE)2014/910 art. 8. 3 minimalne specyfikacje techniczne implementowane przez (UE)2015/1502, ponadto proponowane rozwiązanie spełnia wymogi:

„PasswordLess” i „PostQuantum” jako jedyne w kraju, UE i na świecie …

Oparte na „kryptografii z kluczami jednorazowymi” przeciwdziała, kradzieży tożsamości, podszywaniu się, podstawianiu fałszywych stron internetowych …

Przykład pokazuje integrację z RFC7519 JSON Web Token dla AWS i Cognito

dr inż. Janusz Jabłoński

Wynalazca „DynAuth”

Pracownik AGH: Wydział Informatyki, Elektroniki i Telekomunikacji - Cyberbezpieczeństwo

Członek Rady do Spraw Cyfryzacji w latach 2016 - 2018

Laureat Konkursu Polskiej Agencji Przedsiębiorczości pt. „Polski Produkt Przyszłości” w roku 2014

W zakresie kryptologii posiadacz patentów w Polsce, UE i USA

Transakcje na rynku uwierzytelniania

Wybrane przejęcia z obszaru zarządzania tożsamością cyfrową oraz bezpiecznym uwierzytelnianiem

Inwestor	Target	EV	Data	HQ	WWW
THOMABRAVO	PingIdentity	2,796 USDm	08.2022	US	Ping Identity
THOMABRAVO	SailPoint	7,062 USDm	04.2022	US	SailPoint
CISCO	DUO	2,350 USDm	08.2018	US	Duo Security

Źródło: Capital IQ