Nowe możliwości identyfikacji użytkowników systemów informatycznych

Adrian Kapczyński

adrian@pti.katowice.pl
adrian@posterus.it
adrian@polsl.pl

Plan wystąpienia

- Wprowadzenie
- Bezpieczeństwo teleinformatyczne
- Aktualne możliwości identyfikacji użytkowników
- Nowe możliwości identyfikacji użytkowników
- Podsumowanie

Wprowadzenie

13.06.2005r., Politechnika Śląska, Gliwice

10 Doktorat Honoris Causa
Prof. Ryszarda Tadeusiewicza

Wykład mistrzowski:

„Internet jako źródło przemian cywilizacyjnych”

(wojna na bity)

11.03.2015r., Oko Miata, Katowice

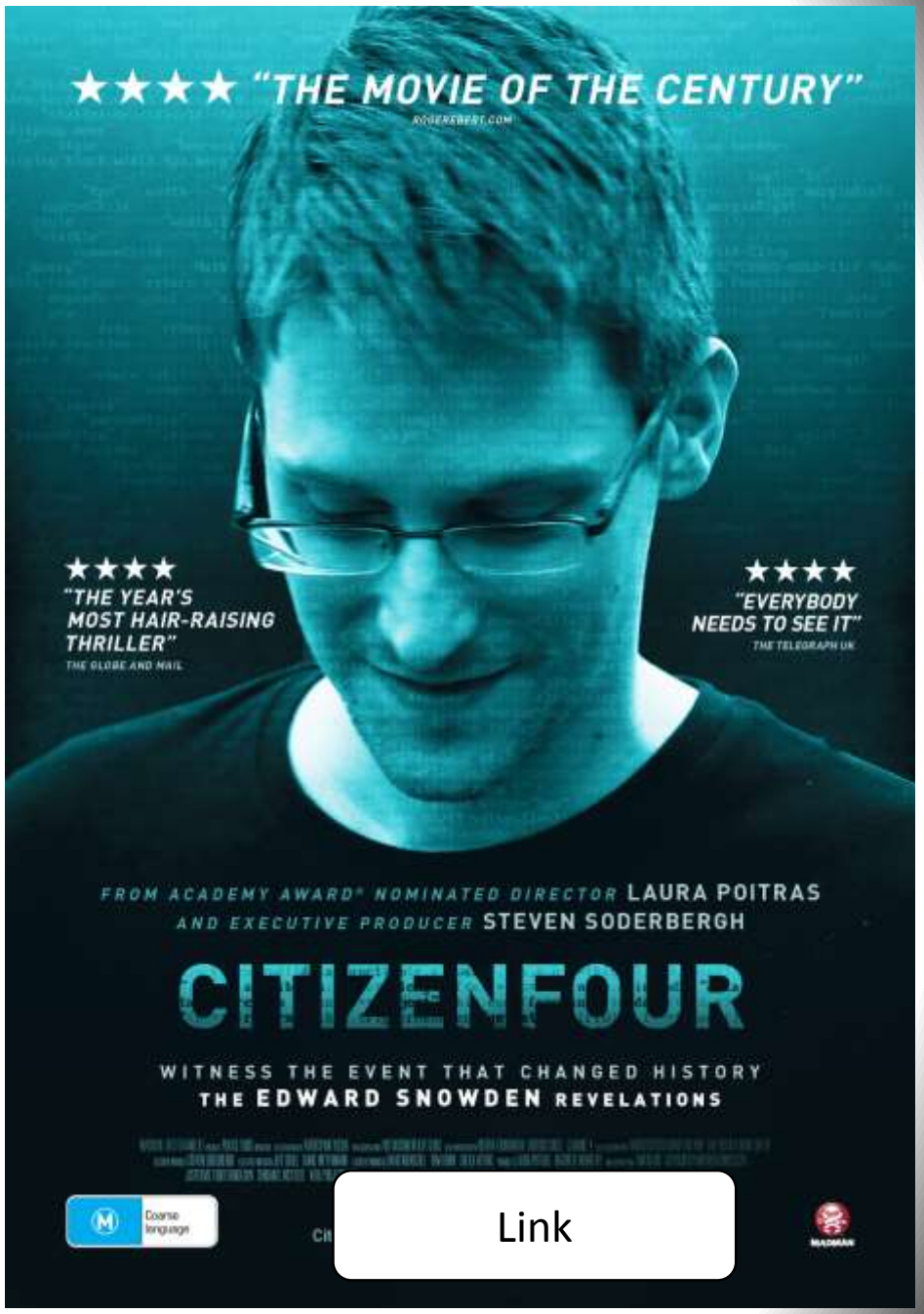
Śląska Kawiarnia Naukowa

Wykład:

„Człowiek (w) przyszłości”

(cyberwojna)

Link


★★★★ "THE MOVIE OF THE CENTURY"
★★★★
"THE YEAR'S MOST HAIR-RAISING THRILLER"
THE GLOBE AND MAIL
★★★★
"EVERYBODY NEEDS TO SEE IT"
THE TELEGRAPH UK
FROM ACADEMY AWARD® NOMINATED DIRECTOR LAURA POITRAS
AND EXECUTIVE PRODUCER STEVEN SODERBERGH
CITIZENFOUR
WITNESS THE EVENT THAT CHANGED HISTORY
THE EDWARD SNOWDEN REVELATIONS

Link

WANTED
BY THE FBI

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering

EVGENIY MIKHAILOVICH BOGACHEV

Multimedia: Images

Aliases:
Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

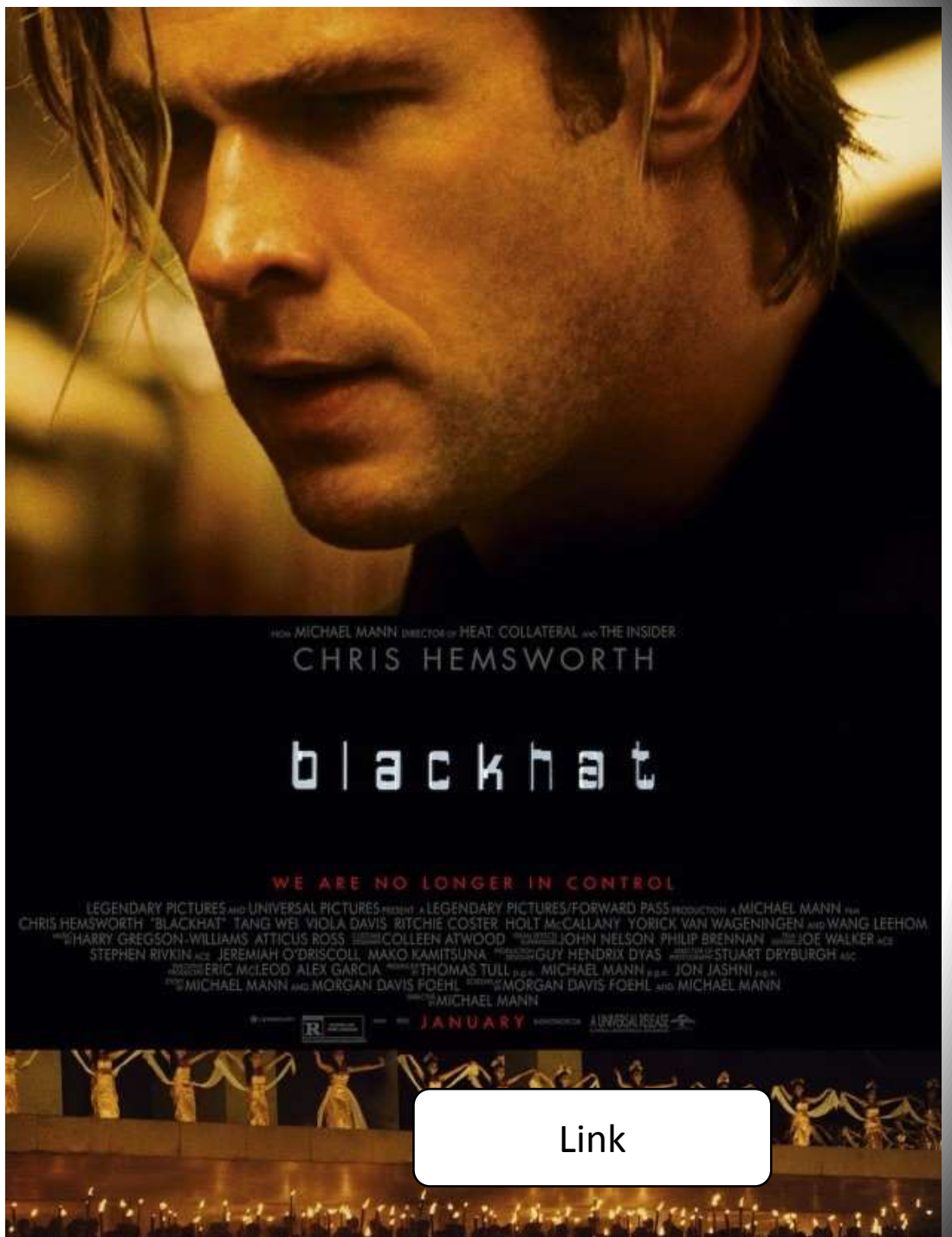
DESCRIPTION

Date(s) of Birth Used:	October 28, 1983	**Hair:**	Brown (usually shaves his head)
Height:	Approximately 5'9"	**Eyes:**	Brown
Weight:	Approximately 180 pounds	**Sex:**	Male
NCIC:	W890989955	**Race:**	White
Occupation:	Bogachev works in the Information Technology field.		

Remarks: Bogachev was last known to reside in An[illegible]d may travel to locations along the Black Sea in his boat.

Yevgeniy Bogachev, Evgeniy Mikhaylovich Bog[illegible]ollingsoon". Source:

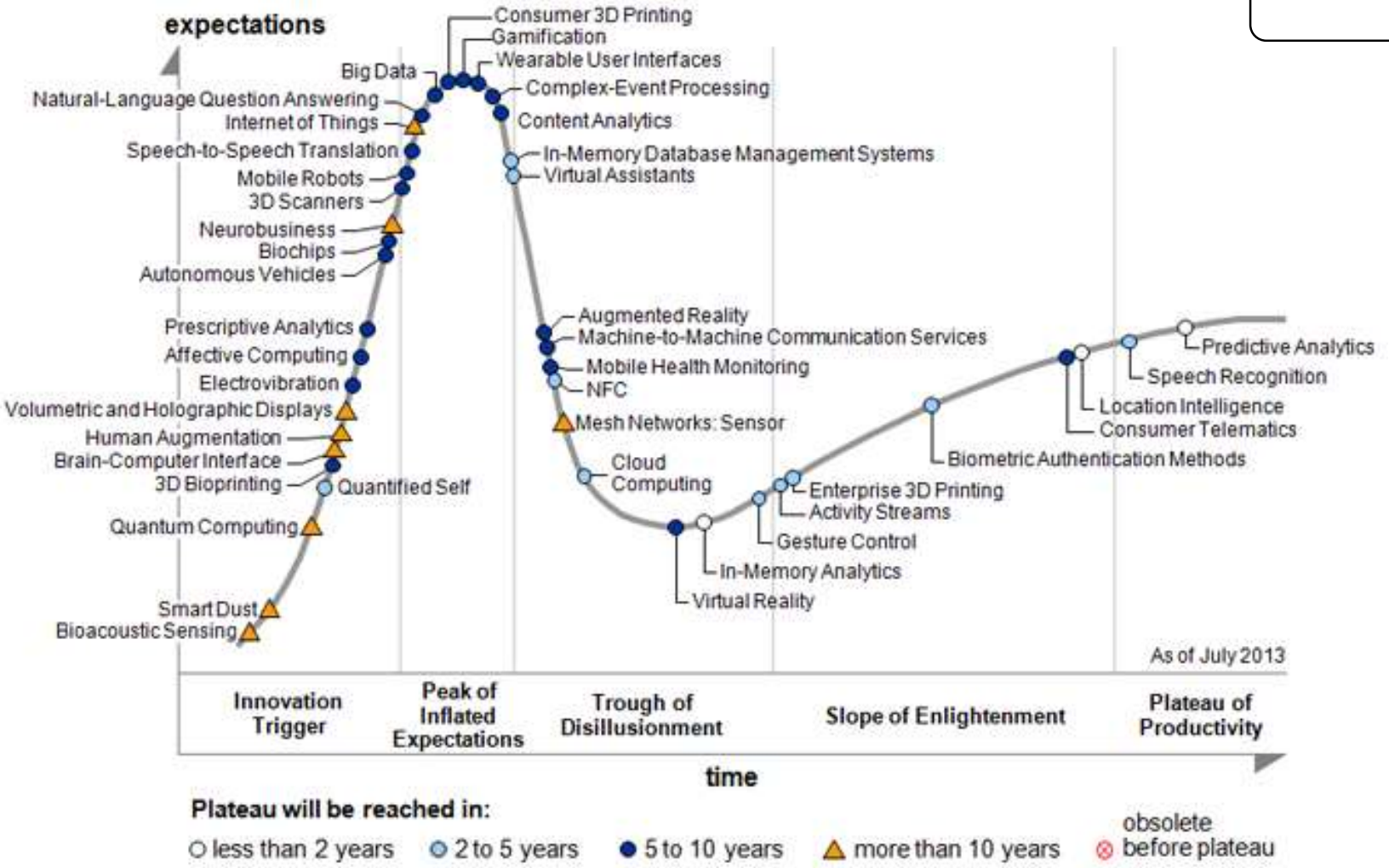
Link



Link

Świat pełen cyfrowych możliwości...

Link



Źródło: Gartner 19.08.2013

Hype Cycle for Emerging Technologies Maps Out Evolving Relationship Between Humans and Machines

Neurosky

Link

Muse

Link

… oraz wyzwań

Międzynarodowa operacja Europolu i Eurojustu - w sumie zatrzymano 49 cyberprzestępców

Wczoraj na terenie województwa małopolskiego [...] do aresztu trafiło pięć osób, w tym mężczyzna, który organizował przestępczy proceder na terenie Polski.

Policjanci Centralnego Biura Śledczego Policji zabezpieczyli ponad 160 tysięcy złotych pochodzących z phishingu.

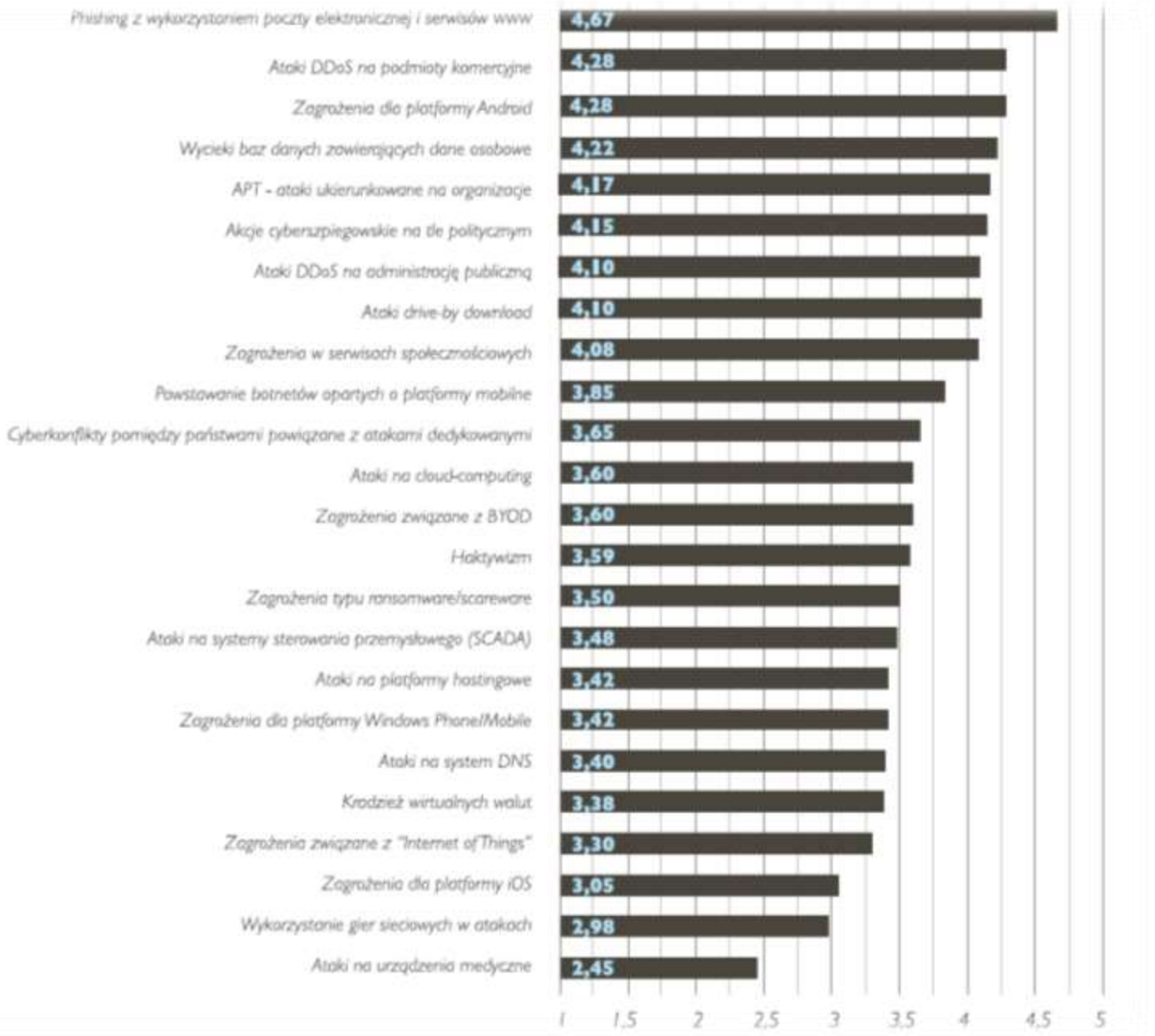
Link

NAJWIĘKSZE ZAGROŻENIA DLA BEZPIECZEŃSTWA W INTERNECIE W 2015 ROKU

GŁOS POLSKICH EKSPERTÓW

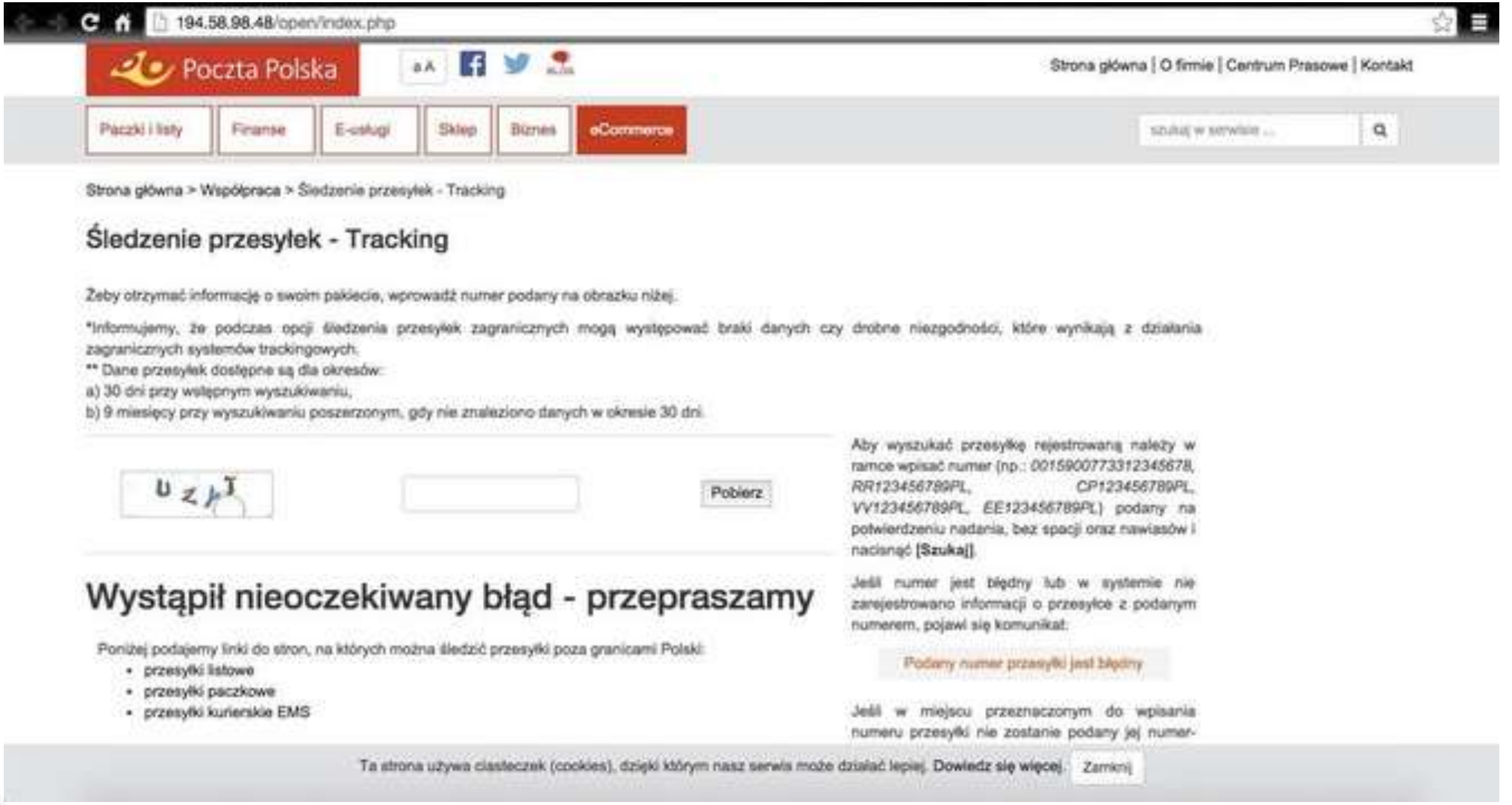
Link

RAPORT


Phishing z wykorzystaniem poczty elektronicznej i serwisów www
4,67
Ataki DDoS na podmioty komercyjne
4,28
Zagrożenia dla platformy Android
4,28
Wycieki baz danych zawierających dane osobowe
4,22
APT - ataki ukierunkowane na organizacje
4,17
Akcje cyberszpiegowskie na tle politycznym
4,15
Ataki DDoS na administrację publiczną
4,10
Ataki drive-by download
4,10
Zagrożenia w serwisach społecznościowych
4,08
Powstawanie botnetów opartych o platformy mobilne
3,85
Cyberkonflikty pomiędzy państwami powiązane z atakami dedykowanymi
3,65
Ataki na cloud-computing
3,60
Zagrożenia związane z BYOD
3,60
Haktywizm
3,59
Zagrożenia typu ransomware/scareware
3,50
Ataki na systemy sterowania przemysłowego (SCADA)
3,48
Ataki na platformy hostingowe
3,42
Zagrożenia dla platformy Windows Phone/Mobile
3,42
Ataki na system DNS
3,40
Kradzież wirtualnych walut
3,38
Zagrożenia związane z "Internet of Things"
3,30
Zagrożenia dla platformy iOS
3,05
Wykorzystanie gier sieciowych w atakach
2,98
Ataki na urządzenia medyczne
2,45
1
1.5
2
2.5
3
3.5
4
4.5
5

Zdaniem ekspertów (Raport FBC)

- Personalizowane ataki na klientów bankowości elektronicznej
- Ataki socjotechniczne (bardziej wysublimowane niż tylko phishing)
- Spear phishing
- Ataki na stacje robocze
- Niekompetencja administratorów
- Ataki ransomware (w stylu cryptolocker) na urządzenia mobilne
- Koordynowane ataki na PC i mobile obniżające wartość popularnej dwuskładnikowej autentykacji
- Nadużycia wewnętrzne (nielegalny dostęp do danych)
- Kradzież danych przez użytkowników uprzywilejowanych


194.58.98.48/open/index.php
Poczta Polska
Strona główna | O firmie | Centrum Prasowe | Kontakt
Paczki i listy
Finanse
E-usługi
Sklep
Biznes
eCommerce
Strona główna > Współpraca > Śledzenie przesyłek - Tracking
Śledzenie przesyłek - Tracking
Żeby otrzymać informację o swoim pakiecie, wprowadź numer podany na obrazku niżej.
*Informujemy, że podczas opcji śledzenia przesyłek zagranicznych mogą występować braki danych czy drobne niezgodności, które wynikają z działania zagranicznych systemów trackingowych.
** Dane przesyłek dostępne są dla okresów:
a) 30 dni przy wstępnym wyszukiwaniu,
b) 9 miesięcy przy wyszukiwaniu poszerzonym, gdy nie znaleziono danych w okresie 30 dni.
Pobierz
Aby wyszukać przesyłkę rejestrowaną należy w ramce wpisać numer (np.: 00159007733312345678, RR123456789PL, CP123456789PL, VV123456789PL, EE123456789PL) podany na potwierdzeniu nadania, bez spacji oraz nawiasów i nacisnąć [Szukaj].
Wystąpił nieoczekiwany błąd - przepraszamy
Jeśli numer jest błędny lub w systemie nie zarejestrowano informacji o przesyłce z podanym numerem, pojawi się komunikat:
Podany numer przesyłki jest błędny
Poniżej podajemy linki do stron, na których można śledzić przesyłki poza granicami Polski:
przesyłki listowe
przesyłki paczkowe
przesyłki kurierskie EMS
Jeśli w miejscu przeznaczonym do wpisania numeru przesyłki nie zostanie podany jej numer-
Ta strona używa ciasteczek (cookies), dzięki którym nasz serwis może działać lepiej. Dowiedz się więcej.
Zamknij

Link

12.06.2015 - odwołanie Pana prelekcji - Wiadomość (zwykły tekst)

PLIK | WIADOMOŚĆ | PDF Architect 2 Creator

Usuwanie: Usuń
Odpowiadanie: Odpowiedz | Odpowiedz wszystkim | Prześlij dalej
Szybkie kroki: ! | Do kierownika | Wiadomość e-...
Przenoszenie: Przenieś
Znaczniki: Oznacz jako nieprzeczytane | Kategoryzuj | Flaga monitująca
Edytowanie: Przetłumacz
Powiększenie: Powiększ
Evernote: Add to Evernote 5

Pt 2015-06-12 06:21

Mariusz Andryszak [redacted]@gmail.com>

12.06.2015 - odwołanie Pana prelekcji

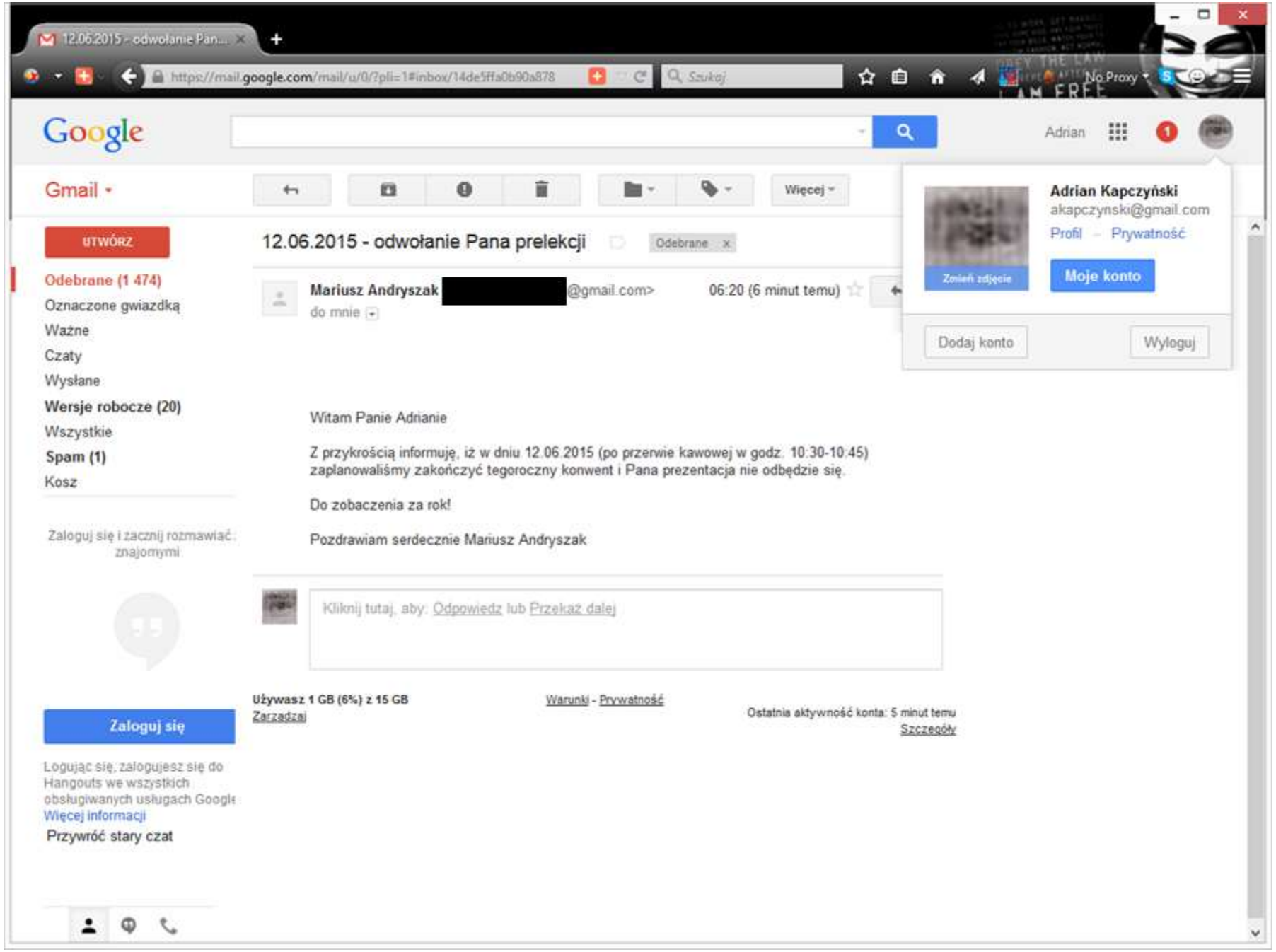
Do akapczynski@gmail.com

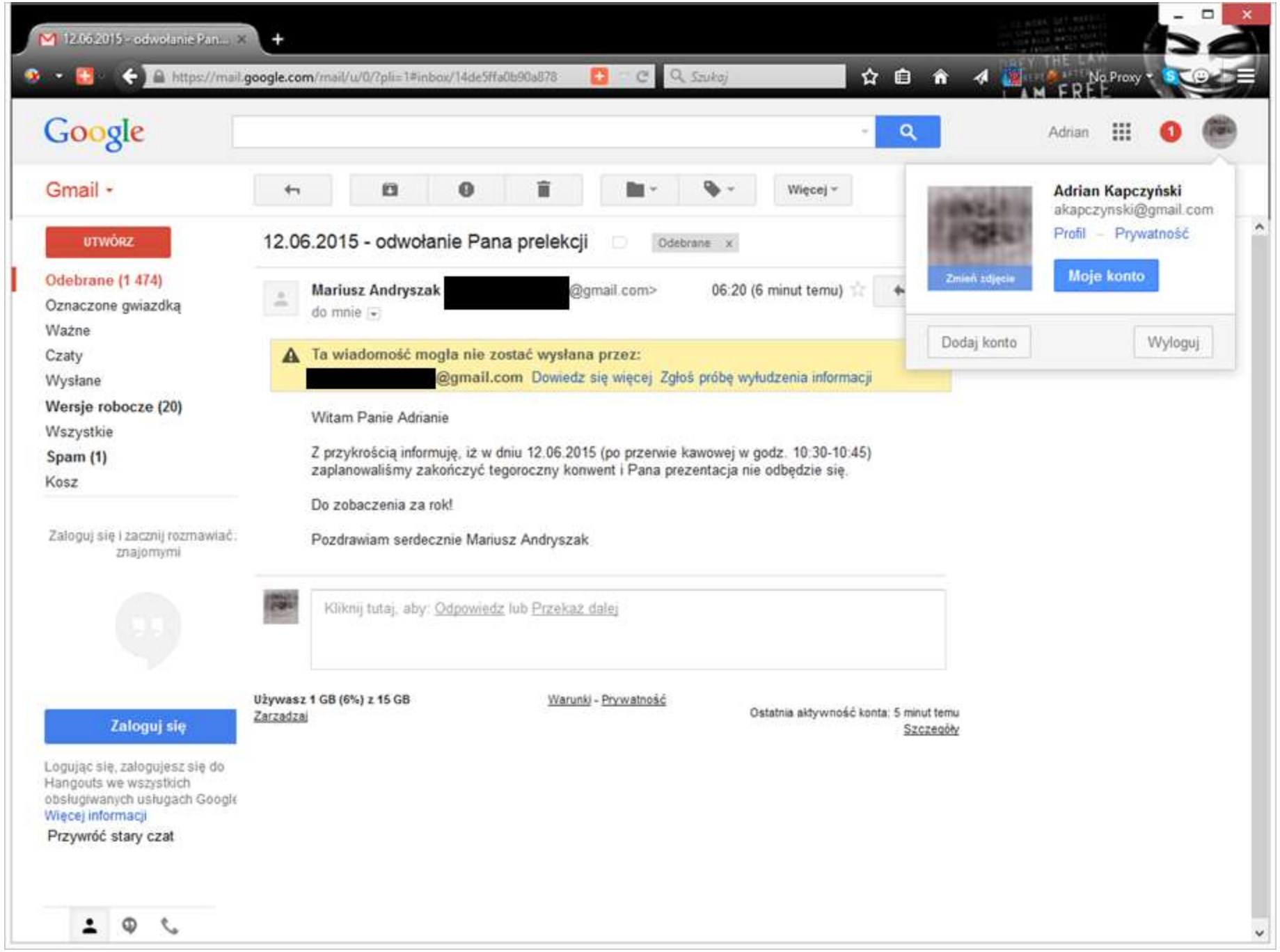
Witam Panie Adrianie

Z przykrością informuję, iż w dniu 12.06.2015 (po przerwie kawowej w godz. 10:30-10:45) zaplanowaliśmy zakończyć tegoroczny konwent i Pana prezentacja nie odbędzie się.

Do zobaczenia za rok!

Pozdrawiam serdecznie Mariusz Andryszak


12.06.2015 - odwołanie Pan...
https://mail.google.com/mail/u/0/?pli=1#inbox/14de5ffa0b90a878
Szukaj
No Proxy
Google
Adrian
Gmail
Więcej
UTWÓRZ
Odebrane (1 474)
Oznaczone gwiazdką
Ważne
Czaty
Wysłane
Wersje robocze (20)
Wszystkie
Spam (1)
Kosz
Zaloguj się i zacznij rozmawiać ze znajomymi
Zaloguj się
Logując się, zalogujesz się do Hangouts we wszystkich obsługiwanych usługach Google
Więcej informacji
Przywróć stary czat
12.06.2015 - odwołanie Pana prelekcji
Odebrane
Mariusz Andryszak [redacted]@gmail.com>
06:20 (6 minut temu)
do mnie
Witam Panie Adrianie
Z przykrością informuję, iż w dniu 12.06.2015 (po przerwie kawowej w godz. 10:30-10:45) zaplanowaliśmy zakończyć tegoroczny konwent i Pana prezentacja nie odbędzie się.
Do zobaczenia za rok!
Pozdrawiam serdecznie Mariusz Andryszak
Kliknij tutaj, aby: Odpowiedz lub Przekaż dalej
Używasz 1 GB (6%) z 15 GB
Zarządzaj
Warunki - Prywatność
Ostatnia aktywność konta: 5 minut temu
Szczegóły
Adrian Kapczyński
akapczynski@gmail.com
Profil
Prywatność
Zmień zdjęcie
Moje konto
Dodaj konto
Wyloguj


12.06.2015 - odwołanie Pan...
https://mail.google.com/mail/u/0/?pli=1#inbox/14de5ffa0b90a878
Szukaj
No Proxy
Google
Adrian
Gmail
Więcej
UTWÓRZ
Odebrane (1 474)
Oznaczone gwiazdką
Ważne
Czaty
Wysłane
Wersje robocze (20)
Wszystkie
Spam (1)
Kosz
Zaloguj się i zacznij rozmawiać ze znajomymi
Zaloguj się
Logując się, zalogujesz się do Hangouts we wszystkich obsługiwanych usługach Google
Więcej informacji
Przywróć stary czat
12.06.2015 - odwołanie Pana prelekcji
Odebrane
Mariusz Andryszak [redacted]@gmail.com>
06:20 (6 minut temu)
do mnie
Ta wiadomość mogła nie zostać wysłana przez:
[redacted]@gmail.com Dowiedz się więcej Zgłoś próbę wyłudzenia informacji
Witam Panie Adrianie
Z przykrością informuję, iż w dniu 12.06.2015 (po przerwie kawowej w godz. 10:30-10:45) zaplanowaliśmy zakończyć tegoroczny konwent i Pana prezentacja nie odbędzie się.
Do zobaczenia za rok!
Pozdrawiam serdecznie Mariusz Andryszak
Kliknij tutaj, aby: Odpowiedz lub Przekaż dalej
Używasz 1 GB (6%) z 15 GB
Zarządzaj
Warunki - Prywatność
Ostatnia aktywność konta: 5 minut temu
Szczegóły
Adrian Kapczyński
akapczynski@gmail.com
Profil – Prywatność
Zmień zdjęcie
Moje konto
Dodaj konto
Wyloguj

Delivered-To: akapczynski@gmail.com
Received: by 10.96.92.197 with SMTP id co5csp326810qdb;
Thu, 11 Jun 2015 21:20:45 -0700 (PDT)
X-Received: by 10.180.37.200 with SMTP id a8mr2818995wik.11.1434082844779;
Thu, 11 Jun 2015 21:20:44 -0700 (PDT)
Return-Path: <zaczernilem.alias@gmail.com>
Received: from emkei.cz (emkei.cz. [46.167.245.72])
by mx.google.com with ESMTP id ei5si1114909wid.118.2015.06.11.21.20.44
for <akapczynski@gmail.com>;
Thu, 11 Jun 2015 21:20:44 -0700 (PDT)
Received-SPF: softfail (google.com: domain of transitioning zaczernilem.alias@gmail.com does not designate 46.167.245.72 as permitted sender) client-ip=46.167.245.72;
Authentication-Results: mx.google.com;
spf=softfail (google.com: domain of transitioning zaczernilem.alias@gmail.com does not designate 46.167.245.72 as permitted sender) smtp.mail=zaczernilem.alias@gmail.com;
dmarc=fail (p=NONE dis=NONE) header.from=gmail.com
Received: by emkei.cz (Postfix, from userid 33)
id 4C73AD5391; Fri, 12 Jun 2015 06:20:41 +0200 (CEST)
To: akapczynski@gmail.com
Subject: 12.06.2015 - =?UTF-8?B?b2R3b8WCYW5pZSBQYW5hIHByZWxla2NqaQ==?=
From: "Mariusz Andryszak" <zaczernilem.alias@gmail.com>
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: zaczernilem.alias@gmail.com
Reply-To: zaczernilem.alias@gmail.com
Content-Type: text/plain; charset=utf-8
Message-Id: <20150612042041.4C73AD5391@emkei.cz>
Date: Fri, 12 Jun 2015 06:20:41 +0200 (CEST)

ISACA Katowice Chapter Meeting
"Phishing w dwóch odsłonach: Part 2 Kraków"

Link

Bezpieczeństwo teleinformatyczne

Inspiracja (1 z 2)

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology

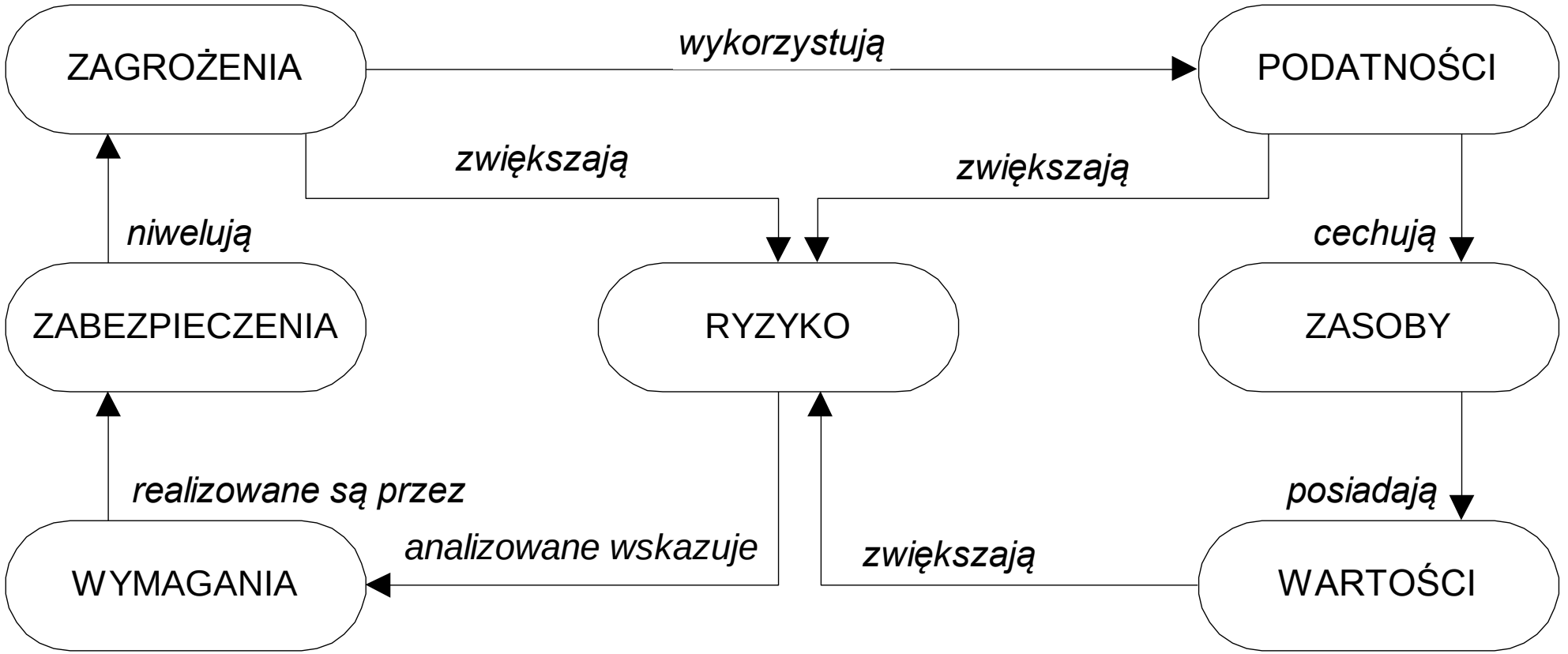
Bruce Schneier

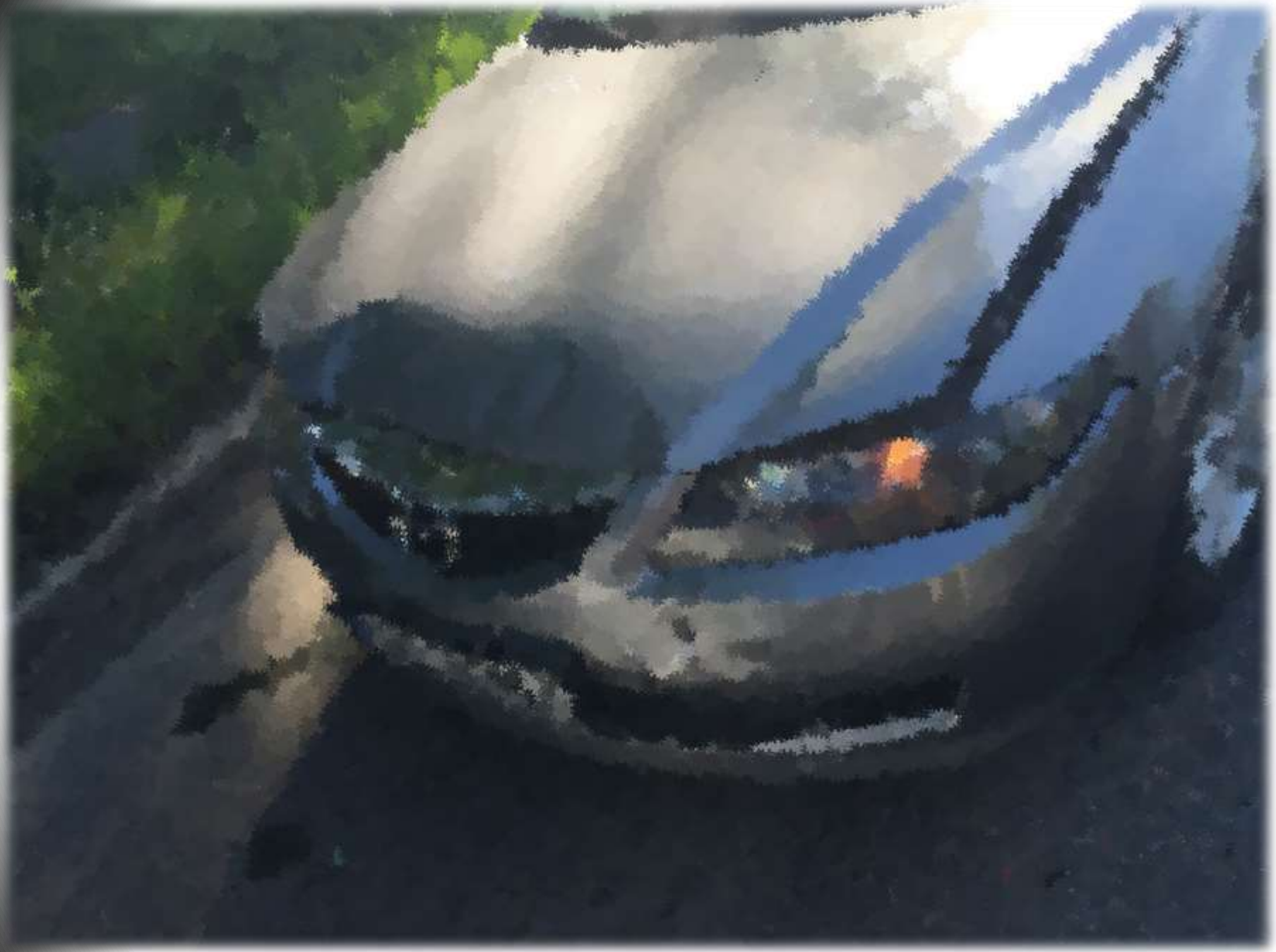
Inspiracja (2 z 2)

Feeling Model Reality

Feeling Model Reality

Feeling Model Reality





Reality

Ryzyko

Identyfikacja użytkowników (#1)

Wiarygodność AMA została potwierdzona

458

wykop

[AMA] Policyjny informatyk

@kyrre wykop.pl #ama #pytanie #komputery #informatyka #internet #ciekawostki

Witam ! Byłem pracownikiem cywilnym w Komendzie Miejskiej Policji na stanowisku Inspektora Łącznośc i Informatyki, chętnie odpowiem na Wasze pytanie, naturalnie nie każdą rzecz mogę zdradzić, ale ze spraw czysto administracyjnych jak najbardziej. Postaram się odpowiadać na pytania dziś i jutro.

KOMENTARZE (725) : **najstarsze** najnowsze najlepsze AMA

RozrywkowyMateusz 3 dni temu +28

czy policyjna sieć z której korzystają kryminalni jest fizycznie połączona z internetem czy może jest to osobna sieć bez dostępu z "zewnątrz"

kyrre 3 dni temu +173

@RozrywkowyMateusz: Zupełnie osobna sieć.

caa2 3 dni temu -6

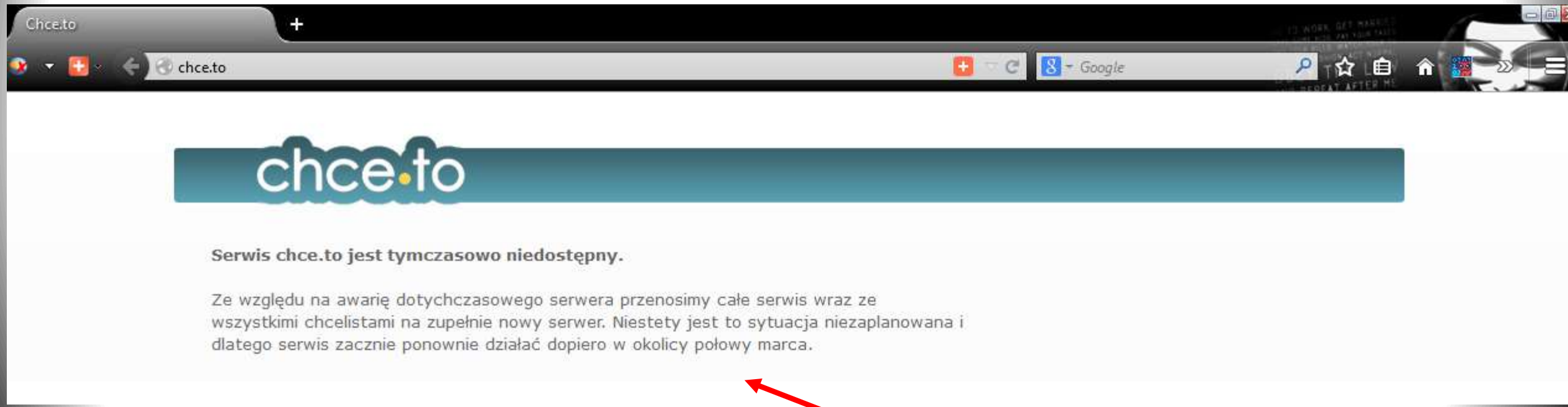
@kyrre: Jak to jest uzasadnione w obecnych czasach? To sieć dzielona z wojskiem, jest oddzielny kabel?

kyrre 3 dni temu +94

@caa2: Oddzielna sieć na calej Polsce, dzierżawiona od dostawcy. Wojsko ma swoją.

Link

http://chce.to


Chce.to
chce.to
Google
chce.to
Serwis chce.to jest tymczasowo niedostępny.
Ze względu na awarię dotychczasowego serwera przenosimy całe serwis wraz ze wszystkimi chcelistami na zupełnie nowy serwer. Niestety jest to sytuacja niezaplanowana i dlatego serwis zacznie ponownie działać dopiero w okolicy połowy marca.

Identyfikacja użytkowników (#2)

Kapczyńscy

Identyfikacja użytkowników (#3)


DERMALOG
BIOMETRICS
DERMALOG
DERMALOG
Not identified!
DERMALOG

How Old Do I Look?

how-old.net/#

Szukaj

No Proxy

How-Old.net

HOW OLD DO I LOOK? #HowOldRobot

Search Faces...

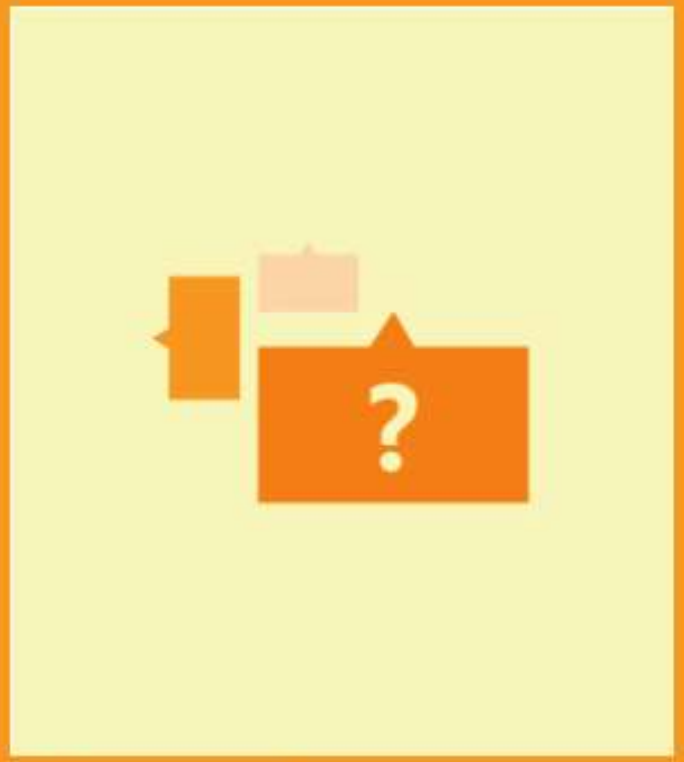
Use This Photo

Use your own photo

P.S. We don't keep the photo

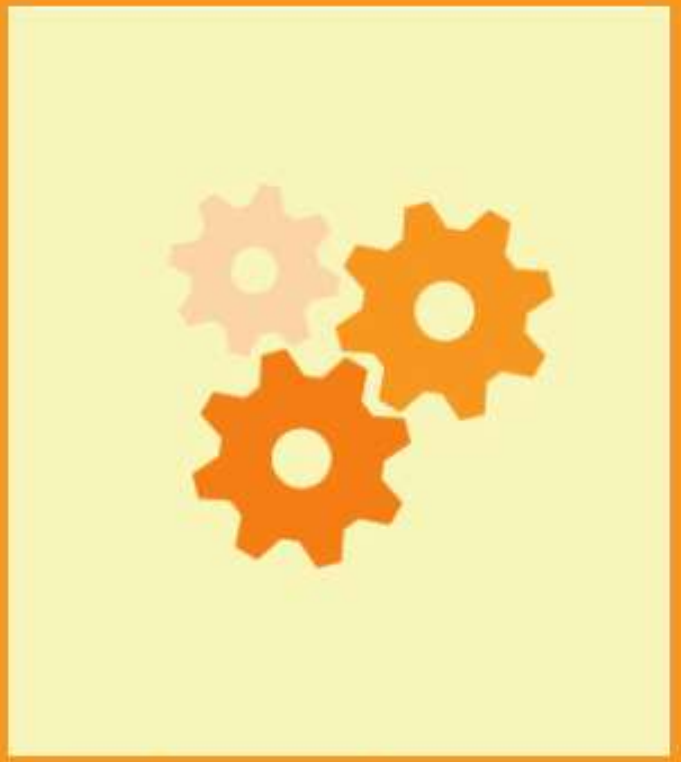
How-Old.net

HOW OLD DO I LOOK? #HowOldRobot



Discover the story behind How Old?

Machine Learning Blog



Check out other amazing Machine Learning APIs

Azure Machine Learning

Create your own Machine Learning Model

Azure Machine Learning

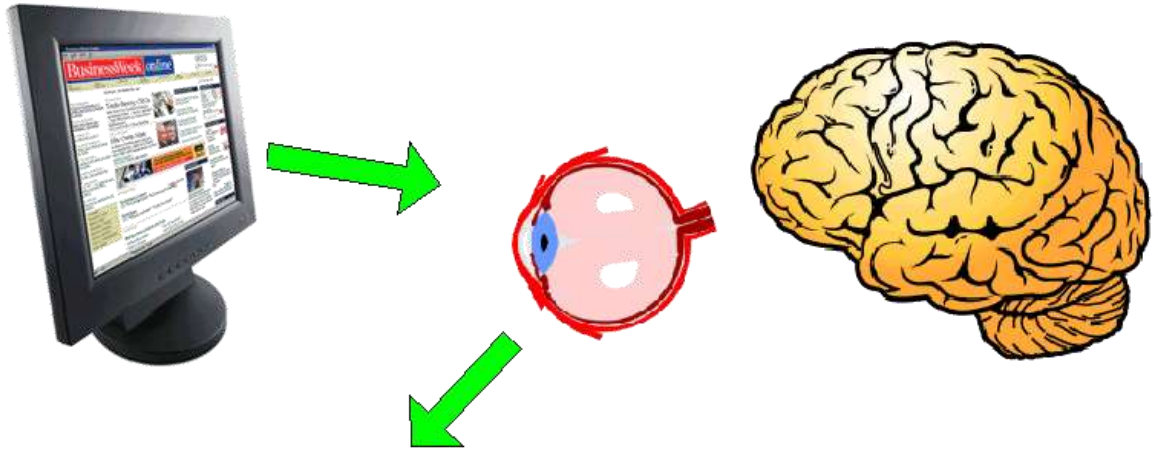
Identyfikacja użytkowników (#4)


WINCOR
NIXDORF
BANKNOTY

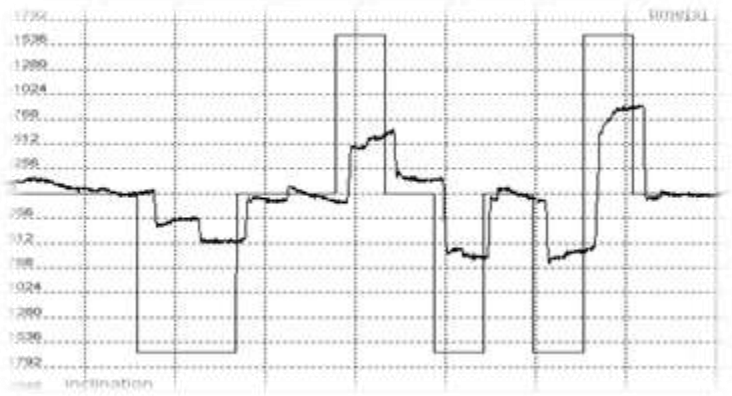
Aktualne możliwości identyfikacji użytkowników

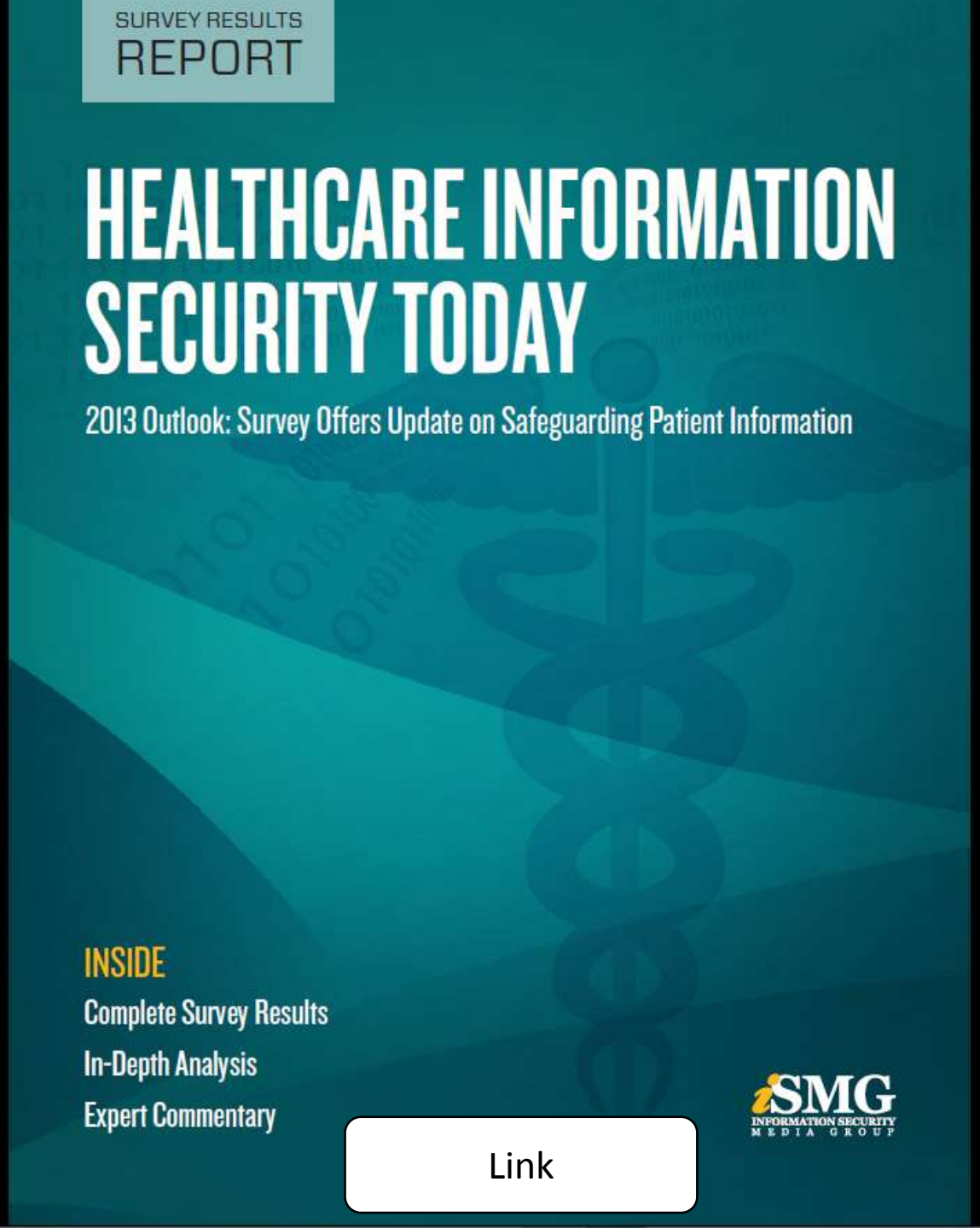
Biometria tęczówki oka

Biometria dynamiki ruchu gałki ocznej

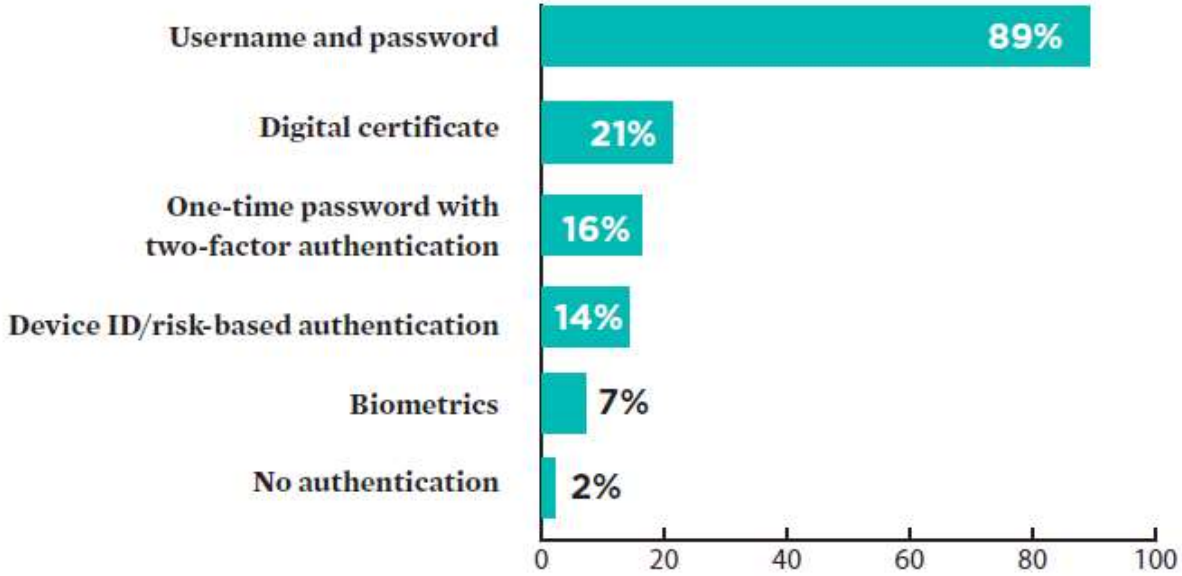


OBER2 Measuring System



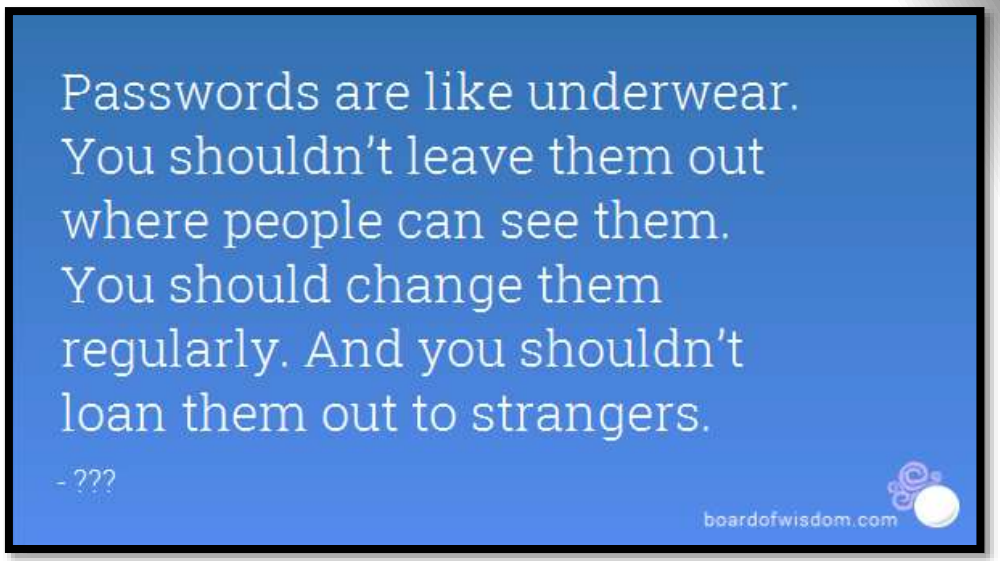

SURVEY RESULTS
REPORT
HEALTHCARE INFORMATION SECURITY TODAY
2013 Outlook: Survey Offers Update on Safeguarding Patient Information
INSIDE
Complete Survey Results
In-Depth Analysis
Expert Commentary
ISMG
INFORMATION SECURITY
MEDIA GROUP
Link

To guard against inappropriate access to electronic health records, what type of authentication does your organization require for users to gain access while they are on the job at one of your facilities?



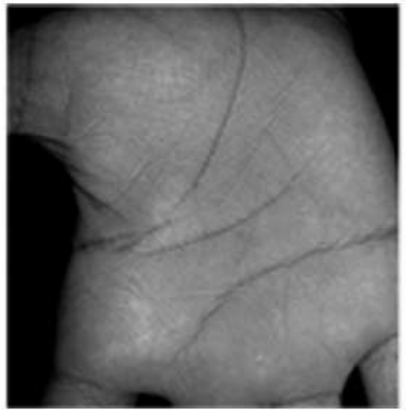
Wiedza użytkownika

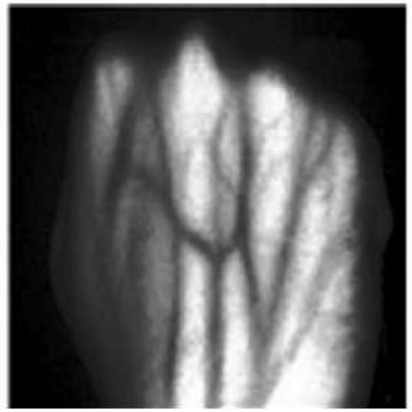
- Hasła są jak...

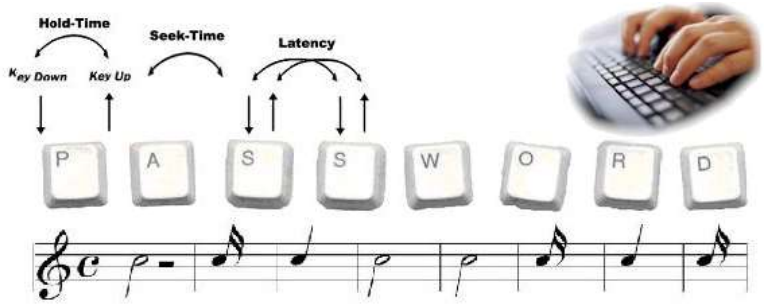


Przedmiot posiadany przez użytkownika

Cechy anatomii i zachowania użytkownika

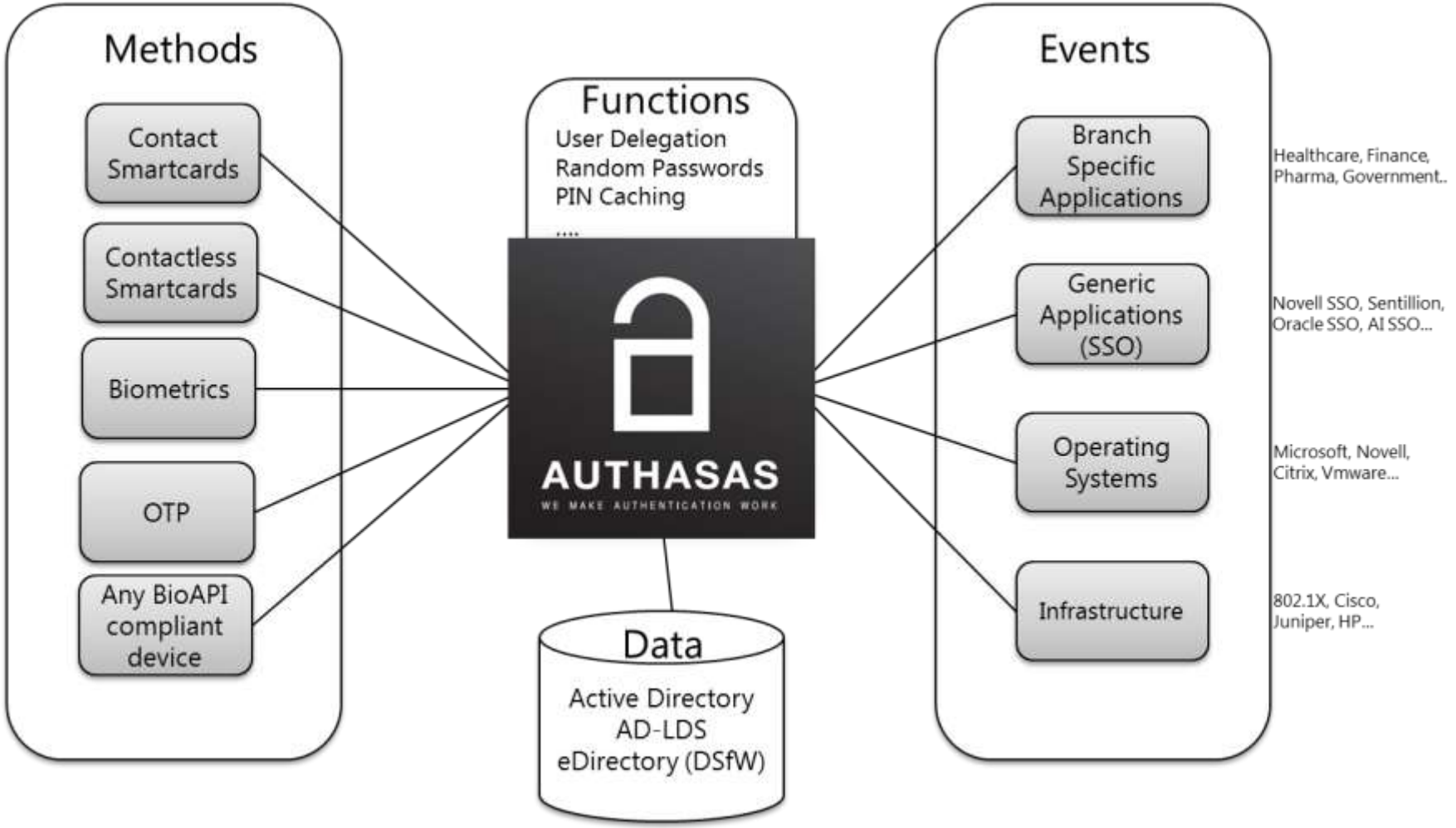




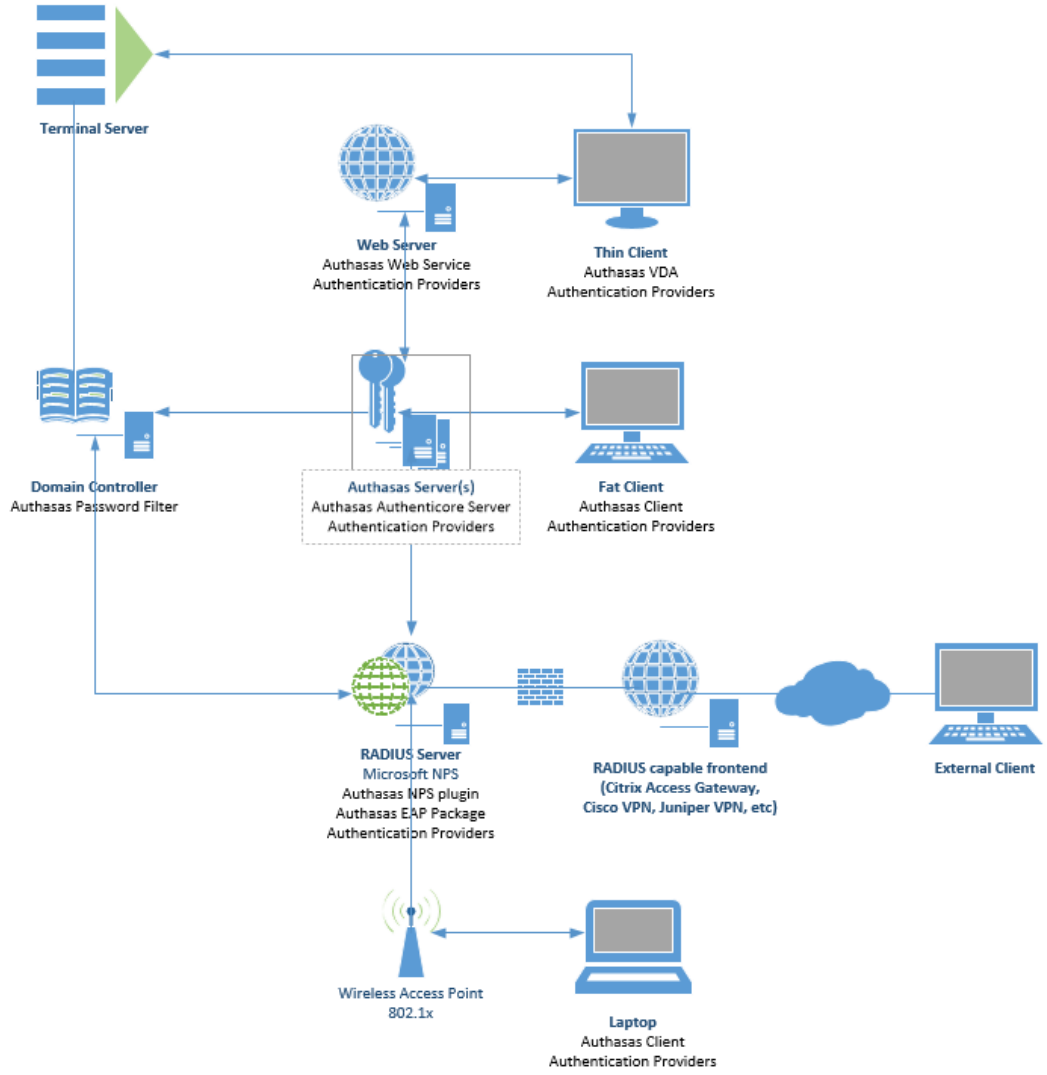
Uwierzytelnianie w sieci

- Authenticator (https://github.com/google/google-authenticator)
- OpenID 2 → OpenID Connect (http://openid.net)
- Shibboleth (https://shibboleth.net)
- OneLogin (https://www.onelogin.com)
- Authasas (http://www.authasas.com)
- LiveEnsure (https://liveensure.com)
- Rublon (http://www.rublon.com)

Przykładowe rozwiązanie (1/2)



Przykładowe rozwiązanie (2/2)




CHALLENGERS
LEADERS
SafeNet
EMC (RSA)
Gemalto
TeleSign
SecurEnvoy
SecureAuth
Entrust Datacard
Authentify
CA Technologies
Vasco Data Security
neXus
Symantec
HID Global
PointSharp
Duo Security
SMS Passcode
Microsoft
Deepnet Security
NICHE PLAYERS
VISIONARIES
ABILITY TO EXECUTE
COMPLETENESS OF VISION
As of December 2014

BRK2324

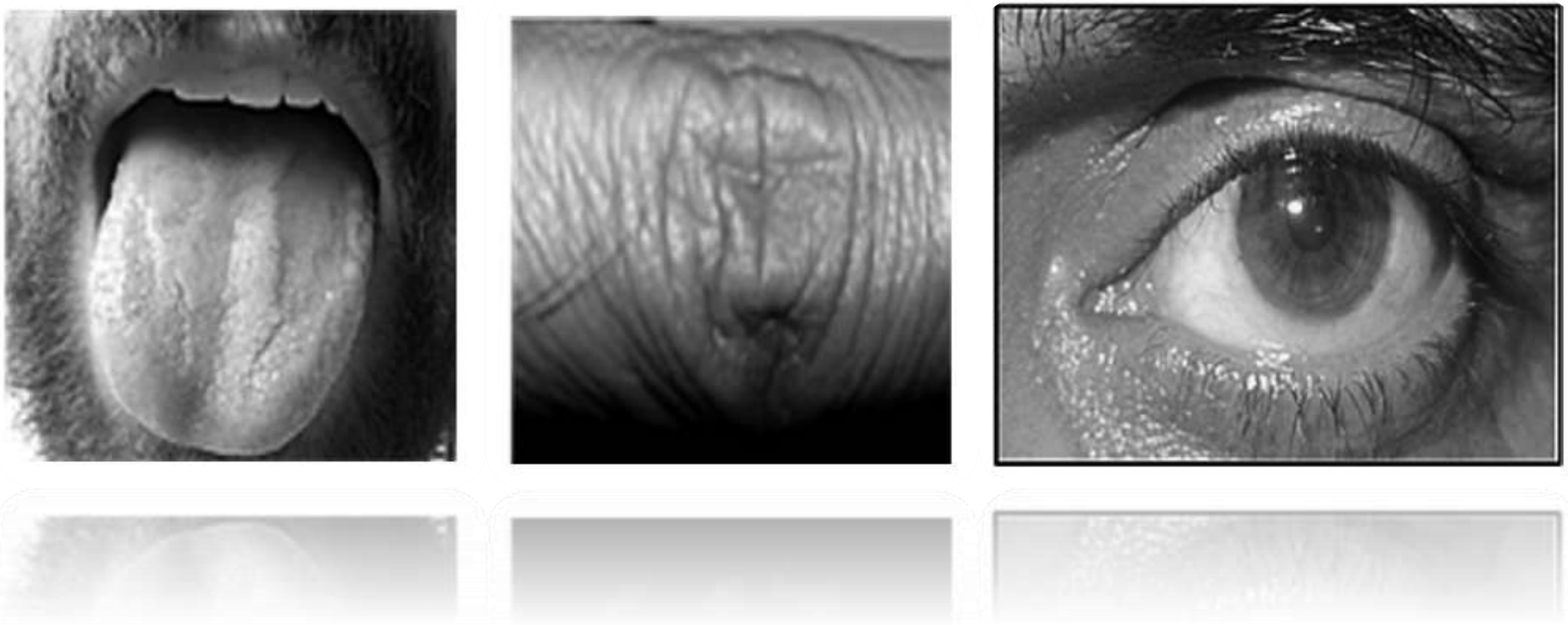
Secure Authentication with Windows Hello

Nelly Porter
Principal Program Manager Lead
OS Security

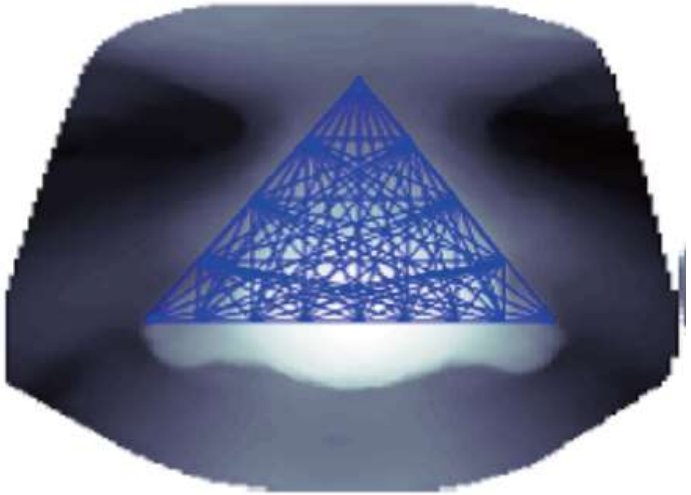
Link

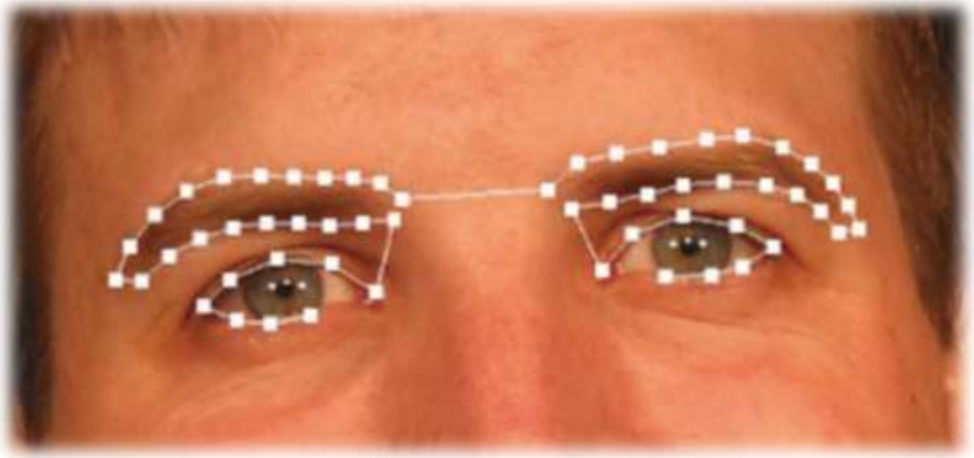
Nowe możliwości identyfikacji użytkowników

Cechy anatomii

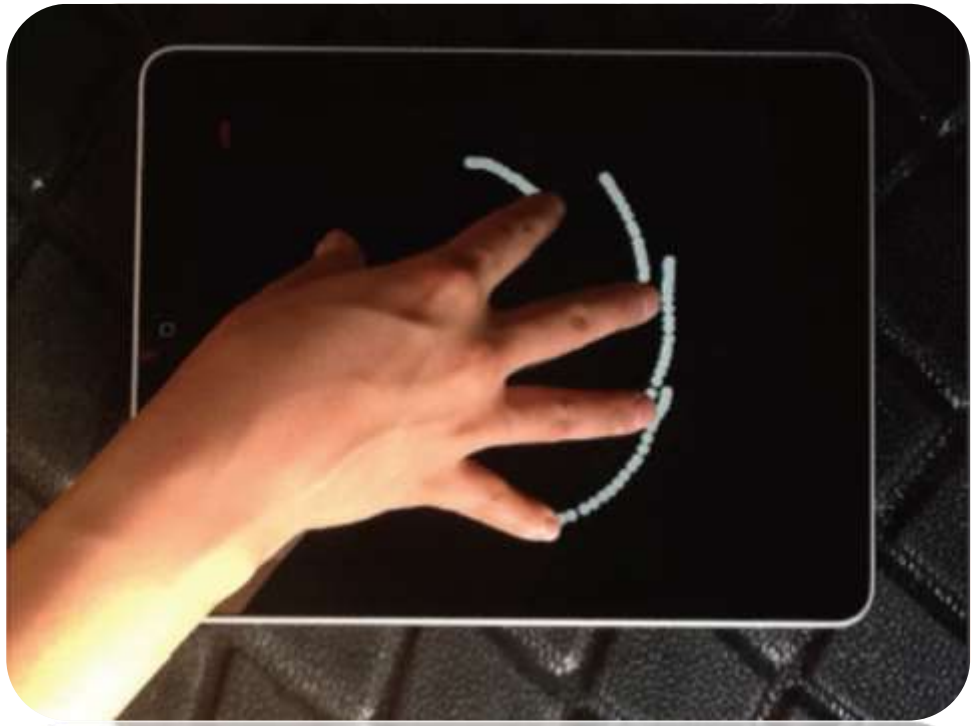


Cechy anatomii





Cechy zachowania



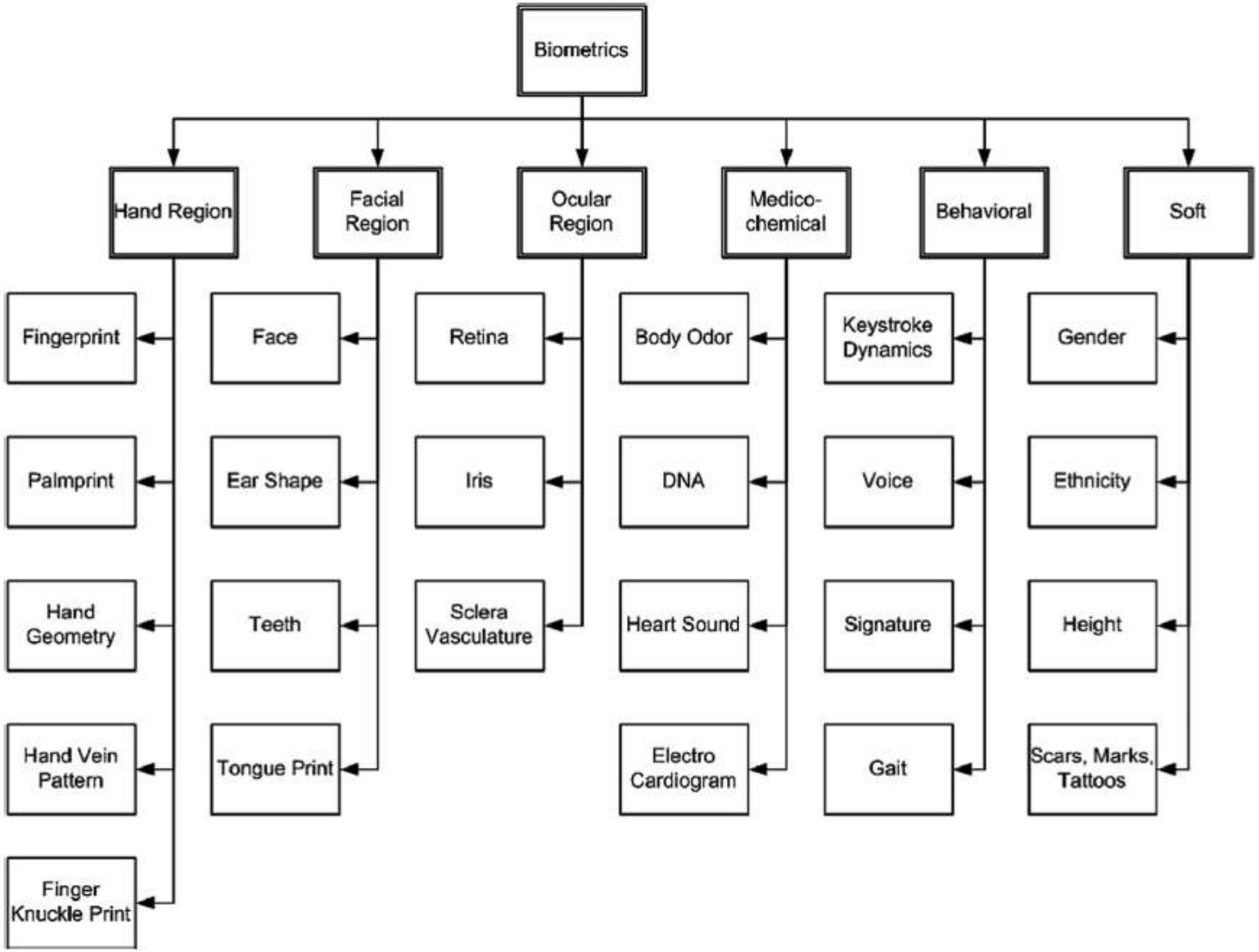
27.11.2014, Planet Biometrics

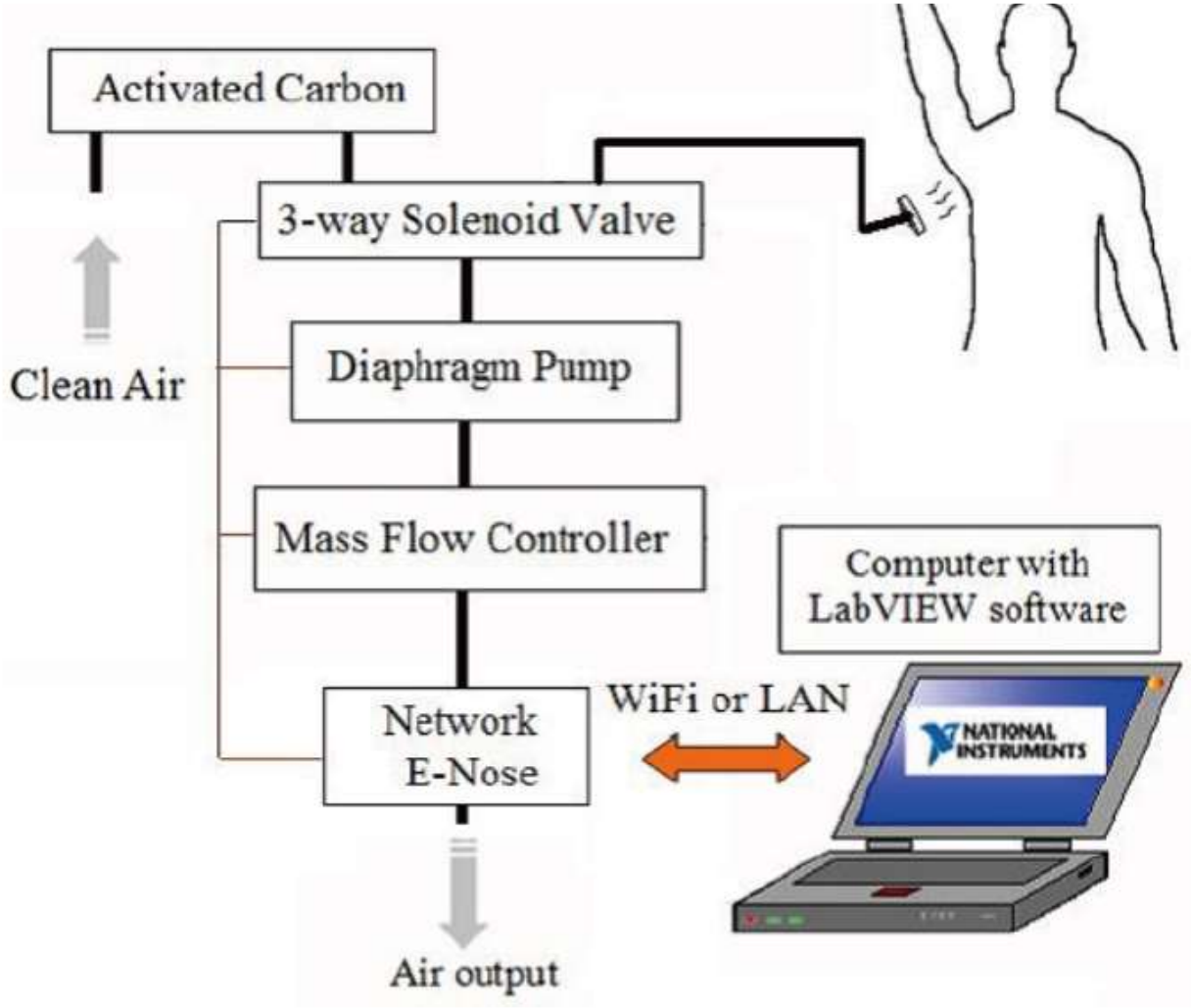
- In October 2014, **Goode Intelligence** predicted that wearable technology will drive a “second wave” of adoption of biometric authentication.

- The **Arki** wrist band, which this week reached a **$100,000** Kickstarter goal, measures a user’s walking pattern so that it can become a password.

- **Bionym** plans to launch the **Nymi** wristband later this year, which uses cardiac rhythms to validate the user.

Bionym is working with the Royal Bank of Canada on a pilot:
“RBC PayBand”


Biometrics
Hand Region
Facial Region
Ocular Region
Medico-chemical
Behavioral
Soft
Fingerprint
Palmprint
Hand Geometry
Hand Vein Pattern
Finger Knuckle Print
Face
Ear Shape
Teeth
Tongue Print
Retina
Iris
Sclera Vasculature
Body Odor
DNA
Heart Sound
Electro Cardiogram
Keystroke Dynamics
Voice
Signature
Gait
Gender
Ethnicity
Height
Scars, Marks, Tattoos



C. Wongehoosuk, M. Lutz, T. Puntheeranurak, T. Youngrod, H. Phetmung, and T. Kerdeharoen. Identification of people from armpit odor region using networked electronic nose. In *IEEE Defense Science Research Conference and Expo (DSR)*, 2011.

Podsumowanie

Dziękuję

Rozszerzenie

Uwierzytelnianie

- **Uwierzytelnianie użytkowników systemów komputerowych** to proces sprawdzania tożsamości użytkowników w systemie komputerowym, do którego zasobów, podejmowana jest próba dostępu

Uwierzytelnianie

- **Proces uwierzytelniania** realizowany jest w oparciu o przedstawione przez użytkowników:
  - uprzywilejowane informacje
  - materialne znaczniki
  - posiadane cechy biologiczne

Uwierzytelnianie

- Środek ochrony przed nieuprawnionym dostępem w systemach teleinformatycznych
- Środek ograniczania dostępu logicznego do informacji

Uwierzytelnianie

- Inne środki ograniczania dostępu logicznego:
  - nadawanie praw dostępu zgodnie z zasadami *minimalnego środowiska pracy*
  - uruchamianie narzędzi programowych do detekcji oraz blokowania prób nieuprawnionego dostępu do zasobów
- Wymienione środki są komplementarne względem środków ograniczających fizyczny dostęp do elementów systemu komputerowego

Uwierzytelnianie

- Pojęcia:
  - uwierzytelnianie
  - autoryzacja (upoważnianie)
  - ewidencjonowanie
- Usługi te we współczesnych systemach komputerowych, często są realizowane przez dedykowany element infrastruktury sieciowej, tzw. serwer AAA (ang. *Authentication, Authorization, Accounting*)

Uwierzytelnianie

- **Autoryzacja** (ang. *authorization*) to zapewnianie procesowi, programowi lub użytkownikowi dostępu do zasobów systemu zgodnie z prawami dostępu
- Procesy uwierzytelniania oraz autoryzacji składają się na podjęcie decyzji o udzieleniu dostępu do chronionych zasobów
- Uwierzytelnianie stanowi warunek wstępny autoryzacji

Uwierzytelnianie

- **Ewidencjonowanie** (ang. *auditing*) polega na bieżącym monitorowaniu aktywności użytkowników oraz rejestracji zdarzeń zgodnie z przyjętym algorytmem selekcji, przykładowo zdarzeń związanych z realizacją uwierzytelniania czy autoryzacji

Uwierzytelnianie

- Warunkiem koniecznym realizacji procedury uwierzytelniania (użytkownika lub systemu), jest przedstawienie **identyfikatora** stanowiącego niepowtarzalną nazwę lub numer przypisany danemu obiektowi

Uwierzytelnianie

- Przedłożona informacja - najczęściej hasło
- Wymagania procedur uwierzytelniania są najistotniejsze z punktu widzenia użytkownika:
  - liczba znaków do wprowadzenia
  - wysiłek umysłowy
  - sposób postępowania w wypadku popełnienia błędu przy wprowadzaniu danych uwierzytelniających
- Bardziej skomplikowane metody niż metoda prostych haseł, z uwagi na niską wygodę stosowania przez użytkownika, mogą okazać się niepraktyczne, mimo zapewnienia wyższego stopnia bezpieczeństwa

Uwierzytelnianie

- Kluczowe zadanie - znalezienie odpowiedniego kompromisu:
  - między wysokim poziomem bezpieczeństwa
  - a dogodnością używania systemu oraz innymi potrzebami użytkowników

Uwierzytelnianie

- Oprócz uwierzytelniania użytkowników przed systemem komputerowym - uwierzytelnianie systemu komputerowego przed użytkownikiem
- Użytkownik przed rozpoczęciem przekazywania określonych informacji musi być pewny, iż uzyskał połączenie i rozpoczyna współpracę z właściwym elementem systemu, a nie podszywającym się pod dany adres intruzem (ang. S*hadow station, shadow server*)

Uwierzytelnianie

- Realizacja procesu **uwierzytelniania** na różnych poziomach:
  - uwierzytelnianie bezpośrednie w ramach systemu operacyjnego stacji roboczej
  - uwierzytelnianie pośrednie w ramach sieciowego systemu operacyjnego czy też Intersieci.

Metody uwierzytelniania użytkowników

- Metody uwierzytelniania oparte o
  - Wiedzę użytkowników (ang. *Something You Know, SYK*)
  - Materialne identyfikatory (ang. *Something You Have*, *SYH*)
  - Cechy biologiczne (ang. *Something You Are, SYA*)
  - Działanie (ang. *Something You Do, SYD*)

Metody uwierzytelniania użytkowników

- Metody oparte o wiedzę - sprawdzenie znajomości przez użytkownika pewnej poufnej (uprzywilejowanej) informacji
  - hasła
  - PIN-u
- Poufna informacja - ciąg znaków (cyfr, liter, znaków specjalnych), który winien być tajny oraz odpowiednio skomplikowany

Metody uwierzytelniania użytkowników

- Istota użycia hasła jako weryfikatora tożsamości użytkownika sprowadza się do porównania hasła podawanego przez użytkownika w odpowiedzi na żądanie systemu, z hasłem zapisanym w repozytorium
- Jeśli hasła są zgodne, system uznaje wiarygodność tożsamości użytkownika

Metody uwierzytelniania użytkowników

- Hasło – kryteria do spełnienia
  - Podstawowe – bezpieczeństwo
    - Ciąg znaków powinien być tajny oraz odpowiednio skomplikowany utrudniając realizację ataków słownikowych oraz pełnego przeglądu
  - Dodatkowe - funkcjonalność
    - Minimalny wysiłek umysłowy (ciąg znaków łatwy do zapamiętania) i fizyczny użytkowników (wprowadzanie hasła, możliwe omyłki)

Metody uwierzytelniania użytkowników

- Metoda prostych haseł
  - najpopularniejsza
  - użytkownik sam wybiera hasło, które jest z jednej strony łatwe do zapamiętania, a z drugiej strony nie jest zbyt oczywiste
- Metody automatycznej generacji i nadawania użytkownikom haseł
  - hasła tworzone przez system są skomplikowane w odgadnięciu jak i zapamiętaniu

Metody uwierzytelniania użytkowników

- Poziom bezpieczeństwa hasła:
  - proporcjonalny do liczby znaków w alfabecie hasła
    - od mocy alfabetu (N) oraz długości hasła (L) zależy złożoność ataku metodą brutalną (przeglądu zupełnego) – liczba możliwych haseł to N^L
  - proporcjonalny do czasu używania hasła
  - proporcjonalny do długości hasła

Metody uwierzytelniania użytkowników

- Wady hasła
  - podatność (mimo szyfrowania z użyciem funkcji jednokierunkowych) na ataki słownikowe
  - możliwość ich użycia bez wiedzy prawowitych użytkowników
  - konieczność zapamiętania
  - ryzyko, że hasło zostanie gdzieś zapisane przez użytkownika, a następnie wykorzystane przez osobę niepowołaną

Metody uwierzytelniania użytkowników

- Podniesienie poziomu bezpieczeństwa hasła
  - zaleca się korzystanie z łączy komunikacyjnych zabezpieczonych przed podsłuchem
  - hasła winny być szyfrowane
  - często przechowywane są w postaci otrzymanej w wyniku przekształcenia jednokierunkową funkcją skrótu

Metody uwierzytelniania użytkowników

- Podniesienie poziomu bezpieczeństwa hasła
  - tworzenie rejestru historii haseł lub regularne badania mające na celu wyszukanie haseł łatwych do odgadnięcia
  - skracanie czasu używania hasła
  - zaleca się używanie haseł co najmniej 8 znakowych, wykorzystujących małe i duże litery, cyfry i znaki specjalne
  - limitowanie prób błędnego dostępu

Metody uwierzytelniania użytkowników

- **Metoda haseł jednorazowych** (ang. *One-time-password, OTP*)
  - zakłada że istnieje lista N haseł, która jest w posiadaniu użytkownika
  - lista jest przechowywana w postaci zaszyfrowanej w zasobach systemu
  - lista może być wygenerowana losowo przez system lub też wygenerowana przez użytkownika i zatwierdzana przez system

Metody uwierzytelniania użytkowników

- **Metoda haseł jednorazowych**
  - Po wykorzystaniu przez użytkownika hasła z pozycji *p* listy, kolejnym, które będzie oczekiwane przy próbie weryfikacji tożsamości jest hasło z pozycji *p+1*
  - w przypadku przejęcia przez intruza hasła z pozycji *p*, nie będzie ono aktualne
  - zastosowanie: bankowość elektroniczna

Metody uwierzytelniania użytkowników

- W celu zabezpieczenia przechowywanej listy haseł jednorazowych, stosowane są kryptograficznie bezpieczne algorytmy mieszające, posiadające dwie własności:
  - danych wejściowych nie można odtworzyć z danych wyjściowych
  - prawdopodobieństwo, że różne dane wejściowe dadzą takie same dane wyjściowe, jest bardzo niskie

Metody uwierzytelniania użytkowników

- Wady metody haseł jednorazowych
  - użytkownik musi mieć przy sobie (lub pamiętać) listę haseł w tym hasło aktualne
  - w razie fizycznej utraty listy może być ona przejęta przez intruza
  - w niektórych systemach gdy wystąpi błąd w transmisji, użytkownik nie wie czy należy podać ponownie to samo hasło, czy też następne

Metody uwierzytelniania użytkowników

- Wady metody haseł jednorazowych
  - przy źle zabezpieczonej linii komunikacyjnej, intruz w wyniku symulowanego błędu komunikacyjnego oraz wysłania żądania o podanie następnego hasła z listy może zdobyć wiedzę niezbędną przy kolejnej próbie uwierzytelniania użytkownika
  - pomimo zastosowania zaawansowanych algorytmów kryptograficznych możliwe są ataki metodą brutalnej siły (ang. *Brute force attack*) bądź ataki słownikowe (ang. *Dictionary attack*)

Metody uwierzytelniania użytkowników

- Metody oparte o materialne identyfikatory polegają na sprawdzeniu posiadania przez użytkownika *charakterystycznego przedmiotu*
  - fizycznego klucza
  - materialnego identyfikatora
  - znacznika

Metody uwierzytelniania użytkowników

- Metody oparte o materialne identyfikatory
  - *Proces uwierzytelniania polega na odczytaniu informacji zawartej w identyfikatorach przez czytnik kontaktowy lub bezkontaktowy*

Metody uwierzytelniania użytkowników

- Czytniki
  - czytniki kontaktowe wykorzystują w komunikacji
    - styki elektryczne
    - odczyt magnetyczny
    - odczyt optyczny
  - czytniki bezkontaktowe wykorzystują
    - fale radiowe
    - fale podczerwone
    - sprzężenia indukcyjne i pojemnościowe

Metody uwierzytelniania użytkowników

- **Charakterystyczne przedmioty** (ang. *Handheld authentication devices, HHAD)*
  - to przenośne urządzenia posiadające możliwość lokalnego przechowywania i/lub przetwarzania informacji

Metody uwierzytelniania użytkowników

- Charakterystyczne przedmioty - cechy
  - użytkownik fizycznie posiada charakterystyczny przedmiot
  - przedmiot jest trudny do podrobienia
  - duplikacja charakterystycznego przedmiotu wymaga określonych środków finansowych i technologicznych
  - utrata przedmiotu może być wykryta relatywnie łatwo i szybko

Metody uwierzytelniania użytkowników

- Identyfikatory:
  - plastykowe karty dziurkowane
  - karty z kodem paskowym
  - żetony (pastylki) uwierzytelniające
  - karty magnetyczne
  - karty elektroniczne z pamięcią półprzewodnikową
  - karty wyposażone w mikroprocesor (ang. *Smart card*)
  - karty superinteligentne, wyposażone dodatkowo w miniaturowy ekran oraz klawiaturę alfanumeryczną

Metody uwierzytelniania użytkowników

- Żetony (pastylki) uwierzytelniające
  - urządzenia posiadające unikatowy, 64-bitowy numer seryjny oraz specjalizowane układy elektroniczne zapewniające realizację funkcji materialnego identyfikatora użytkownika systemu komputerowego

Metody uwierzytelniania użytkowników

- Karty magnetyczne
  - wykorzystywane są najczęściej przy uwierzytelnianiu użytkownika podczas fizycznej kontroli dostępu
  - rzadziej są stosowane w metodach przy kontroli dostępu do systemu komputerowego
  - relatywnie tanie
  - podatne na uszkodzenia (wrażliwość kart magnetycznych na zewnętrzne pola magnetyczne)
  - stosunkowo łatwe do podrobienia

Metody uwierzytelniania użytkowników

- Karty elektroniczne z pamięcią półprzewodnikową
- Karty wyposażone w mikroprocesor (ang. *Smart card*)
- Karty superinteligentne, wyposażone dodatkowo w miniaturowy ekran oraz klawiaturę alfanumeryczną

Metody uwierzytelniania użytkowników

- Karty elektroniczne
  - w tym głównie karty mikroprocesorowe, dzięki wbudowanemu mikroprocesorowi, trwałości karty, trwałości zapisu oraz odporności na zewnętrzne pola magnetyczne i elektryczne, znalazły szerokie zastosowanie jako materialne dowody tożsamości użytkowników

Metody uwierzytelniania użytkowników

- Metody biometryczne
  - Metody oparte o cechy biologiczne użytkowników
  - Metody oparte o działania użytkowników
  - Wykorzystują unikatowość wybranych cech anatomicznych oraz behawioralnych

Metody uwierzytelniania użytkowników

- Uzupełnienie przedstawionych rodzajów metod uwierzytelniania
  - uwierzytelnienie oparte o geodezyjną (fizyczną) lokalizację
  - uwierzytelnianie oparte o logiczną lokalizację
    - mogą znaleźć zastosowanie we wspomaganiu procesów uwierzytelniania realizowanych przez Internet