



# **Główne wyzwania ochrony prywatności wobec trendów rozwojowych informatyki**

**Wojciech Cellary**

Katedra Technologii Informacyjnych  
Uniwersytet Ekonomiczny w Poznaniu

Mansfelda 4, 60-854 Poznań  
cellary@kti.ue.poznan.pl  
www.kti.ue.poznan.pl



# Prywatność

**Istotą prywatności jest tajemnica**

- ⇒ Świadome **dopuszczenie** kogoś **do tajemnicy** ma na celu osiągnięcie pewnych **korzyści**
  - korzyści racjonalne
  - korzyści emocjonalne
- ⇒ **Naruszenie tajemnicy**
  - ktoś nieuprawniony wszedł w posiadanie tajemnicy – **naruszenie ochrony**
  - osoba dopuszczona do tajemnicy ujawniła ją – **zdrada**, czyli naruszenie zaufania; lub **wyłudzenie** tajemnicy



# Tajemnica w wersji elektronicznej

- ⇒ **Każdy bit może być skopiowany z doskonałą jakością**
  - w trakcie przechowywania
  - w trakcie transmisji
- ⇒ **Samo skopiowanie bitu nie zostawia żadnego śladu**
- ⇒ **Jeśli do skopiowania jest użyte pewne oprogramowanie, to to oprogramowanie może zarejestrować fakt skopiowania**



# Trzy poziomy naruszenia ochrony

## ⇒ Informatyczny

- znalezienie niechronionej luki w systemie
- podszycie się pod osobę uprawnioną

## ⇒ Elektroniczny

- przełożenie dysku
- atak na kopie zapasowe

## ⇒ Fizyczny

- antena – rejestracja fal radiowych, nasłuch magnetyczny kabli
- kamera – rejestracja obrazów
- drgania – rejestracja dźwięków



# Środki ochrony

## ⇒ Informatyczna autoryzacja dostępu

- unikalny, tajny ciąg bitów pamiętany lub generowany: hasła, klucze programowe i sprzętowe, biometria, profile
- wielokanałowość identyfikacji

## ⇒ Szyfrowanie

## ⇒ Rozproszenie

## ⇒ Fizyczna autoryzacja dostępu do pomieszczeń

- strażnicy, zamki, kamery

## ⇒ Ekranowanie

- pokoje bez okien
- puszki Faraday'a



# Zależność użyteczności od ochrony

⇒ **Im większa ochrona, tym mniejsza użyteczność**

- mniejsza wydajność
- mniejsza przyjazność
- mniejszy zasięg
- mniejszy efekt synergii

**Maksymalna ochrona = zerowa użyteczność**  
**Najbezpieczniejszy samolot to taki, który nie lata**



# Tajemnica a korzyść

⇒ **Fundamentalne pytanie:**

**Czy korzyść przyniesie zachowanie tajemnicy,  
czy dopuszczenie do niej wybranych osób?**

⇒ **Wybrane osoby:**

- znajomi
- sprzedawcy/usługodawcy
- urzędnicy
- pośrednio – personel techniczny

**Skrajnym przypadkiem jest  
otwartość,  
czyli ujawnienie tajemnicy  
wszystkim –  
– zatem i dobrym, i złym**



# Straty wynikające z utraty prywatności

- ⇒ **Dyskomfort** wynikający ze zmiany relacji społecznych – ocena przez innych
- ⇒ Zwiększona podatność na **ataki biznesowe** (np. agresywny marketing, odmowa zawarcia pewnych umów lub zmiana ich warunków)
- ⇒ Zwiększone prawdopodobieństwo **ataków kryminalnych**
- ⇒ Podatność na **kradzież tożsamości**



# Zaufanie

## do osób dopuszczonych do tajemnicy

### ⇒ **Znajomi**

- osobista znajomość i zbudowane relacje
- obdarzenie zaufaniem (powierzenie tajemnicy) prowadzi do pogłębienia relacji i/lub rozwiązania problemów

### ⇒ **Sprzedawcy/usługodawcy**

- naruszenie zaufania odbija się bezpośrednio na interesach przedsiębiorstwa
- utrata reputacji = utrata klientów, czyli przychodów

### ⇒ **Urzędnicy**

- słaby element w odniesieniu do zaufania
- brak osobistych relacji
- odległy interes korporacyjny – reputacja państwa
- utrata reputacji nie oznacza utraty interesariuszy – monopol państwa na obsługę administracyjną



# Personel techniczny

## ⇒ Prywatność najłatwiej naruszyć personelowi technicznemu

- administratorzy sieci, serwerów, baz danych, aplikacji mają duże (często nieograniczone) uprawnienia dostępu
- mają dostęp do danych na najniższym poziomie informatycznym oraz na poziomie elektronicznym i fizycznym – kopiowanie bez śladu
- są bardzo trudni do skontrolowania przez przełożonych, którzy nie mają wiedzy technicznej



# Kluczowy problem zaufania do państwa

## Ochrona czy prywatność?

⇒ Czy wyżej stawiamy **ochronę** nas obywateli przez państwo przed zagrożeniami:

- atakami terrorystycznymi
- atakami kryminalnymi
- nadużyciami, np. niepłaceniem podatków

zgadzając się na przekazanie funkcjonariuszom państwowym więcej informacji prywatnych?

⇒ Czy wyżej stawiamy **prywatność** bojąc się bardziej jej naruszenia przez funkcjonariuszy państwowych?



# Demagogia

- ⇒ Często podnoszony **argument**, że uczciwy obywatel nie ma nic do ukrycia, jest **demagogiczny**
- ⇒ **Uczciwość** obywatela nie chroni go bowiem przed wytypowaniem go do **ataku kryminalnego** na podstawie ujawnionych informacji prywatnych



# Zdrada

- ⇒ **Prewencyjnego zabezpieczenia** technicznego przed zdradą, czyli nadużyciem zaufania, **właściwie nie ma**
- można jedynie **wykryć** nadużycie po fakcie i próbować ograniczyć rozpowszechnianie danych prywatnych
  - należy **karać** na drodze prawnej za ujawnianie lub wykorzystanie danych prywatnych
  - należy poszukiwać najlepszych metod **wykrywania**, kto jest źródłem wycieku danych prywatnych
  - należy **ograniczyć** dostęp urzędnika/pracownika do minimalnego podzbioru danych prywatnych
- ⇒ **Niestety – raz opublikowana informacja elektroniczna jest praktycznie wieczna**
- każdy może skopiować opublikowaną daną
  - kopiowanie dla celów technicznych (kopie zapasowe)



# Źródła danych prywatnych

- ⇒ Podawanie danych prywatnych przez interesariusza/klienta w celu załatwienia sprawy
  - ⇒ Generowanie danych prywatnych interesariusza/klienta przez usługodawcę (np. lekarza)
  - ⇒ Podawanie danych prywatnych z powodów społecznych – serwisy społecznościowe
  - ⇒ Automatyczne zbieranie danych
  - ⇒ Ekstrakcja i eksploracja wiedzy
- Jawne zbieranie danych**
- Niejawne zbieranie danych**



# Dane zbierane jawnie

- ⇒ Podawanie danych prywatnych przez interesariusza/klienta lub ich generowanie przez usługodawcę w celu **załatwienia sprawy**
  - niebezpieczeństwo wykradzenia danych
  - niebezpieczeństwo ujawnienia danych
- ⇒ Podawanie danych prywatnych z powodów społecznych – **serwisy społecznościowe**
  - kwestia świadomości znaczenia ochrony prywatności
  - ewoluująca definicja korzyści wynikających z opublikowania danych prywatnych
  - praktyczna niemożność usunięcia danych elektronicznych



# Dane zbierane niejawnie (1)

## ⇒ **Automatyczne zbieranie danych**

- płaćenie kartami
- śledzenie położenia telefonów komórkowych
- śledzenie odwiedzanych stron WWW
- rozpoznawanie obrazów z kamer
- śledzenie w Internecie Rzeczy
- automatyczne kopie zapasowe

⇒ W większości przypadków, automatyczne śledzenie jest **warunkiem koniecznym** świadczenia usług



# Dane zbierane niejawnie (2)

## ⇒ Ekstrakcja i eksploracja wiedzy

- wiedza wynika z kojarzenia faktów i wyciągania wniosków
- wiedza może mieć charakter deterministyczny lub probabilistyczny – oba rodzaje są użyteczne
- w warunkach dostępności różnych baz danych zawierających opisy ogromnej liczby faktów jest możliwa automatyczna:
  - ekstrakcja wiedzy – wydedukowanie faktów, które nie są jawnie zapisane w bazach danych
  - eksploracja danych i wiedzy – poznanie nowych zależności między faktami i praw rządzących ich ewolucją



# Dane

## zbierane niejawnie (3)

### Ekstrakcja i eksploracja wiedzy

- ⇒ Ten sam **dylemat**: czy naruszenie prywatności przez ekstrakcję i eksplorację wiedzy jest z **korzyścią** czy **stratą** dla obywateli?
- ⇒ Bez prawa do tworzenia nowej wiedzy ludzkość przestanie się rozwijać
  - badania medyczne
  - badania ekonomiczne
  - badania społeczne
- ⇒ Pewnym rozwiązaniem jest **anonimizacja** danych, ale ona może być złamana



# Rozproszenie danych

⇒ W konflikcie:

**Zdolność do eksploracji wiedzy versus prywatność**

⇒ istotną rolę odgrywa

**Integracja danych versus rozproszenie danych**

⇒ **Integracja** danych umożliwia większą **eksplorację** wiedzy w łatwy sposób

⇒ **Rozproszenie** danych zwiększa ich **ochronę** i zmniejsza możliwość zdrady, ze względu na wielostopniową weryfikację dostępu do danych



# Najważniejsze tendencje rozwojowe współczesnej informatyki

- ⇒ **Multimedia**
- ⇒ **Współpraca**
- ⇒ **Semantyka**

**Wszystkie te tendencje mają na celu  
podniesienie jakości życia**

**Niestety wszystkie niosą zwiększone  
zagrożenie dla prywatności**



# Multimedia

## Kierunki badawcze

- ⇒ Automatyczne **rozpoznawanie** treści multimedialnych,
- ⇒ Prezentacja za pomocą technik **wirtualnej, wzbogaconej i mieszanej** rzeczywistości,
- ⇒ Przetwarzanie na urządzeniach **mobilnych**



# Zagrożenia dla prywatności

- ⇒ W ekstremalnym przypadku – zarejestrowanie obrazu **całego życia** każdego człowieka
  - **realnie** – zarejestrowanie obrazu każdego człowieka pojawiającego się w przestrzeni publicznej, w szczególności w dużych miastach
  - **automatyczne** rozpoznawanie obrazów (twarzy, postaci) i łączenie ich z wielu źródeł (kamer)
- ⇒ Naruszenie prywatności **awatarów** w wirtualnych światach
  - skutki społeczne i emocjonalne
  - skutki ekonomiczne



# Współpraca

- ⇒ Współpraca przedsiębiorstw i urzędów z informatykami – **przetwarzanie w chmurze** (ang. Cloud Computing)
- ⇒ Współpraca wzajemna przedsiębiorstw i urzędów – **architektura usługowa SOA** (ang. Service Oriented Architecture)
- ⇒ Współpraca ludzi – **serwisy społecznościowe** (ang. social networks)
- ⇒ Współpraca urządzeń – **Internet rzeczy** (ang. Internet of Things)



# **Przetwarzanie w chmurze**

**Przetwarzanie w chmurze  
jest modelem biznesowym oferowania zasobów  
i aplikacji informatycznych zdalnie przez Internet**



# Zalety przetwarzania w chmurze

- ⇒ **Uwolnienie środków na inwestycje**
- ⇒ **Redukcja kosztów przetwarzania danych**
- ⇒ **Redukcja ryzyka biznesowego**
- ⇒ **Uwolnienie od konieczności zapewnienia obsługi technicznej i pielęgnacji sprzętu i oprogramowania**
- ⇒ **Uniformizacja e-usług w skali całego kraju**
- ⇒ **Sensowne wykorzystanie (przyszłej) infrastruktury telekomunikacyjnej w kraju**



# Zagrożenia dla prywatności

- ⇒ Dane są przechowywane w „chmurze”, czyli centrach danych, które są **poza kontrolą** właściciela danych
  - możliwość **niewykrywalnego** kopiowania danych
  - możliwość **nieautoryzowanego** przetwarzania danych
- ⇒ Ponieważ niektóre centra danych mogą być w innych krajach, to powstaje problem **ochrony prawnej** prywatności w różnych krajach
- ⇒ Rozwiązaniem są **chmury prywatne**, czyli dedykowane dla zamkniętej grupy odbiorców



# Architektura usługowa SOA

SOA jest architekturą umożliwiającą wzajemną interakcję tych, którzy mają **możliwości**, z tymi, którzy mają **potrzeby**



# SOA

- ⇒ Punktem wyjścia do opracowania **architektury usługowej SOA** jest **podejście procesowe** i **ukierunkowanie na klienta**, niezależnie od implementacji
- ⇒ To oznacza konieczność **dynamicznej kompozycji usług** świadczonych przez **komputery** i przez **ludzi** z różnych, rozproszonych i różnorodnych jednostek organizacyjnych, zarówno z sektora **publicznego**, jak i **prywatnego**



# Znaczenie architektury usługowej SOA

- ⇒ Poszerzenie gamy e-usług o usługi **zintegrowane, mieszane i dodane**, których sam sektor publiczny lub sam sektor prywatny nigdy by nie wytworzył
- ⇒ Lepsza i bardziej efektywna obsługa klientów (obywateli i przedsiębiorstw), którzy realizują swoje **całościowe procesy**, a nie załatwiają poszczególne sprawy w odrębnych urzędach i przedsiębiorstwach
- ⇒ Otwarcie **nowych rynków e-usług** opartych na wiedzy, a tym samym tworzenie wartościowych miejsc pracy



# Zagrożenia dla prywatności

- ⇒ Na **stykach** różnorodnych systemów informatycznych współpracujących ze sobą w architekturze SOA najłatwiej o **luki** bezpieczeństwa i naruszenie prywatności
  - niekompatybilne systemy bezpieczeństwa
- ⇒ Współpraca oznacza **przekazanie** praw dostępu do swoich danych współpracującej, niezależnej jednostce. Dane te mogą być niewykrywalnie skopiowane i wykorzystane, również po zakończeniu współpracy
- ⇒ **Generalnie** – im więcej współpracujących jednostek, tym większe zagrożenie dla prywatności



# Serwisy społecznościowe

**Forma życia społecznego  
realizowana za pomocą  
komunikacji elektronicznej**

**Kiedyś:** migracja ludzi ze wsi do miast

**Obecnie:** migracja ludzi z realu do wirtualu



# Motywacja

- ⇒ Obok tradycyjnych **wspólnot terytorialnych** – dzięki Internetowi funkcjonują nowe **wspólnoty treściowe**
- ⇒ Główną motywacją do udziału w serwisach społecznościowych jest uzyskanie **akceptacji społecznej** i zdobycie **wyższej pozycji społecznej**, nawet jeśli słowo „społecznej” odnosi się do bardzo małego kręgu ludzi



# Zagrożenia dla prywatności

- ⇒ **Prywatne dane** uczestnika serwisu społecznościowego udostępnione zamkniętemu kręgowi odbiorców mogą **rozpowszechniać się** poza jego kontrolą
- ⇒ Dla zdobycia **wyższej pozycji społecznej** (forma osoby publicznej), uczestnik serwisu społecznościowego jest gotowy udostępniać swoje prywatne dane **nieznanym** sobie i **nieaufanym** osobom
- ⇒ Problem pojawia się, gdy **zmieni zdanie**
  - dorośnie
  - wycofa się z pewnych form działalności
- ⇒ i nie pretenduje już do tej pozycji społecznej natomiast pragnie **powrócić do prywatności**
- ⇒ Polityki portali społecznościowych
  - naruszenie prywatności **generuje ruch**, a zatem zyski
  - **wydobywanie** danych prywatnych pod pretekstem usług



# Internet rzeczy (IoT)

**Światowa sieć połączonych,  
identyfikowalnych obiektów  
bazująca na standardowych  
protokołach komunikacyjnych**

**Obiekty:**

- ⇒ sensory
- ⇒ przetworniki
- ⇒ efektory

wbudowane w **rzeczy**



# Inteligentne środowiska

- ⇒ **Internet rzeczy** pozwala na tworzenie inteligentnych środowisk,
- ⇒ w których **rzeczy własne** człowieka
- ⇒ samodzielnie komunikują się z
- ⇒ **rzeczami** stanowiącymi wyposażenie jego **chwilowego otoczenia** (ciche przetwarzanie)



# Motywacja

⇒ Tworzenie inteligentnych środowisk w miejscach ważnych dla ludzi:

- **budynkach** (domach, szkołach, szpitalach, fabrykach, biurach itp.)
- **drogach** (przejeździach, ulicach, autostradach, drogach wodnych, powietrznych itp.)
- **miejscach zgromadzeń** (placach, stadionach, plażach itp.)
- **miejscach wpływających na środowisko przyrodnicze** (dopływy rzek, lodowce, wulkany itp.)

⇒ Celem tych inteligentnych środowisk jest:

- poprawa **jakości** życia
- poprawa **bezpieczeństwa**
- zmniejszenie **zużycia energii**
- zmniejszenie **obciążenia** środowiska przyrodniczego



# Zagrożenia dla prywatności

- ⇒ Możliwość **inwigilacji** na ogromną skalę
- ⇒ Możliwość jednoznacznej **identyfikacji** osób w dowolnych miejscach i przy wykonywaniu dowolnych działań
- ⇒ Możliwość **rejestrowania** wszelkich działań człowieka i ich parametrów
- ⇒ Możliwość **wpływan**a na działania człowieka przez ingerencję w zachowanie rzeczy, które go otaczają



# Semantyka

## Kierunki badawcze

- ⇒ **Reprezentacja** wiedzy i **wnioskowanie**
- ⇒ Automatyczna **ekstrakcja** semantyki
- ⇒ **Infrastruktura** semantyczna
- ⇒ Inteligentne **interfejsy** użytkownika
- ⇒ Semantyczne przetwarzanie **społecznościowe**

**Chcemy, aby komputery  
nie tylko wykonywały nasze rozkazy,  
ale aby nas rozumiały**



# Zagrożenia dla prywatności

- ⇒ Eksploracja danych i wiedzy pozwala na **profilowanie** zachowań ludzi
- ⇒ Jeśli komputery będą nas **rozumiały**, to będą też w stanie **wpływać** na nasze zachowanie



## **Wnioski (1)**

**Internet niczego nie zapomina,  
a na pewno niczego nie przebacza**

**Wszystko co zapiszesz (dasz zapisać) o sobie  
w postaci elektronicznej,  
może być wykorzystane przeciwko Tobie**



## **Wnioski (2)**

**Nie ma technicznych środków ochrony przed zdradą**

**Jedyną skuteczną ochroną prywatności jest etyka wspomagana prawem karnym**



**Dziękuję**

**Wojciech Cellary**