Zagrożenia i bezpieczeństwo komputerów i danych

Agnieszka Nowak -Brzezińska

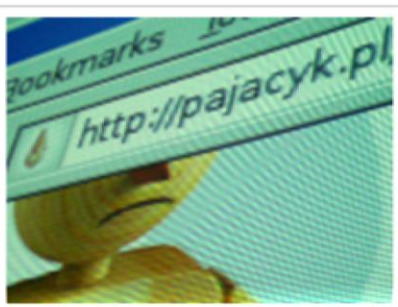
Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

Pytanie: Czy czujesz się bezpiecznie surfując w sieci Internet?

Większość z Nas odpowie:

- A ja tylko przeglądam znane strony:
  - Wp
  - Onet
  - Pajacyk

Zagrożenie na www.pajacyk.pl - jednak malware, a nie reklama



W niedzielę 22 lutego na kilku forach internetowych pojawiły się wypowiedzi zaniepokojonych internautów informujące, że ich programy antywirusowe wykrywają złośliwe oprogramowanie na stronie www.pajacyk.pl (na przykład *Avast* identyfikował je jako *VBS:Malware-gen*). Przeprowadzona przez nas analiza potwierdziła zagrożenie – jak się okazało do kodu strony Pajacyka został doklejony skrypt *JavaScript* przekierowujący na inną stronę infekującą internautów trojanem *ZBot*. Fragment źródła strony z przekierowującym skryptem (zapamiętany przez nas około godziny 10:00 w poniedziałek 23 lutego) wyglądał następująco:

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

WWW.PAJACYK.PL

- Niedziela 22 lutego programy antywirusowe wykrywają złośliwe oprogramowanie na stronie www.pajacyk.pl (na przykład Avast identyfikował je jako VBS:Malware-gen)
- Zagrożenie zostało usunięte dopiero w poniedziałek około godziny 10:30
- Według statystyk umieszczonych na www.pajacyk.pl, tylko w niedzielę witrynę odwiedziło prawie 100 tysięcy osób.

Źródło: http://www.cert.pl/news/1571

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Plan zajęć

- Zagrożenia
- Bezpieczeństwo
- Metody zapewnienia poufności
- Metody zabezpieczeń komputera i sieci
- Hasła
- Podsumowanie

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

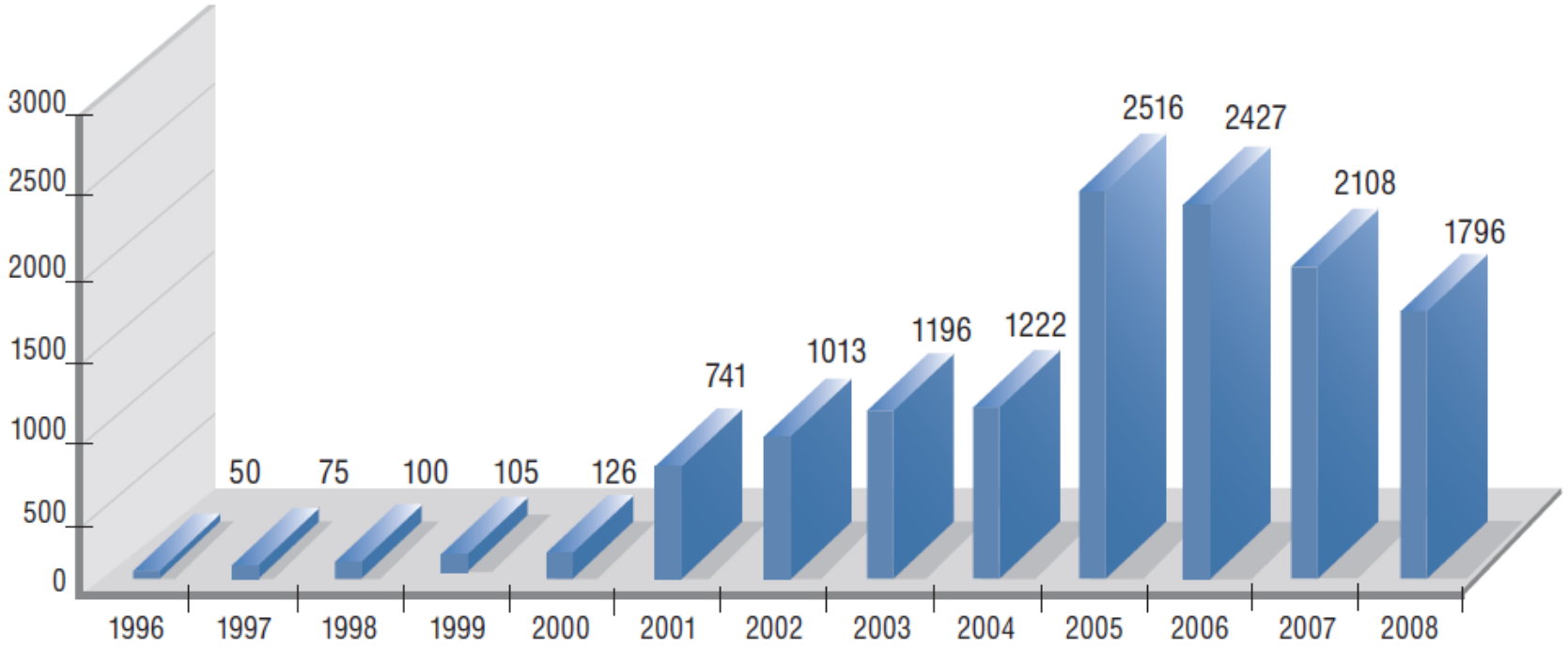
ZAGROŻENIA

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Liczba incydentów w latach 1996 – 2008



Źródło: www.cert.pl

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Rozkład procentowy typów incydentów

Oszustwa komputerowe	10
Nieuprawnione wykorzystanie zasobów	5
Naruszenie praw autorskich	316
Kradzież tożsamości, podszycie się (w tym phishing)	400

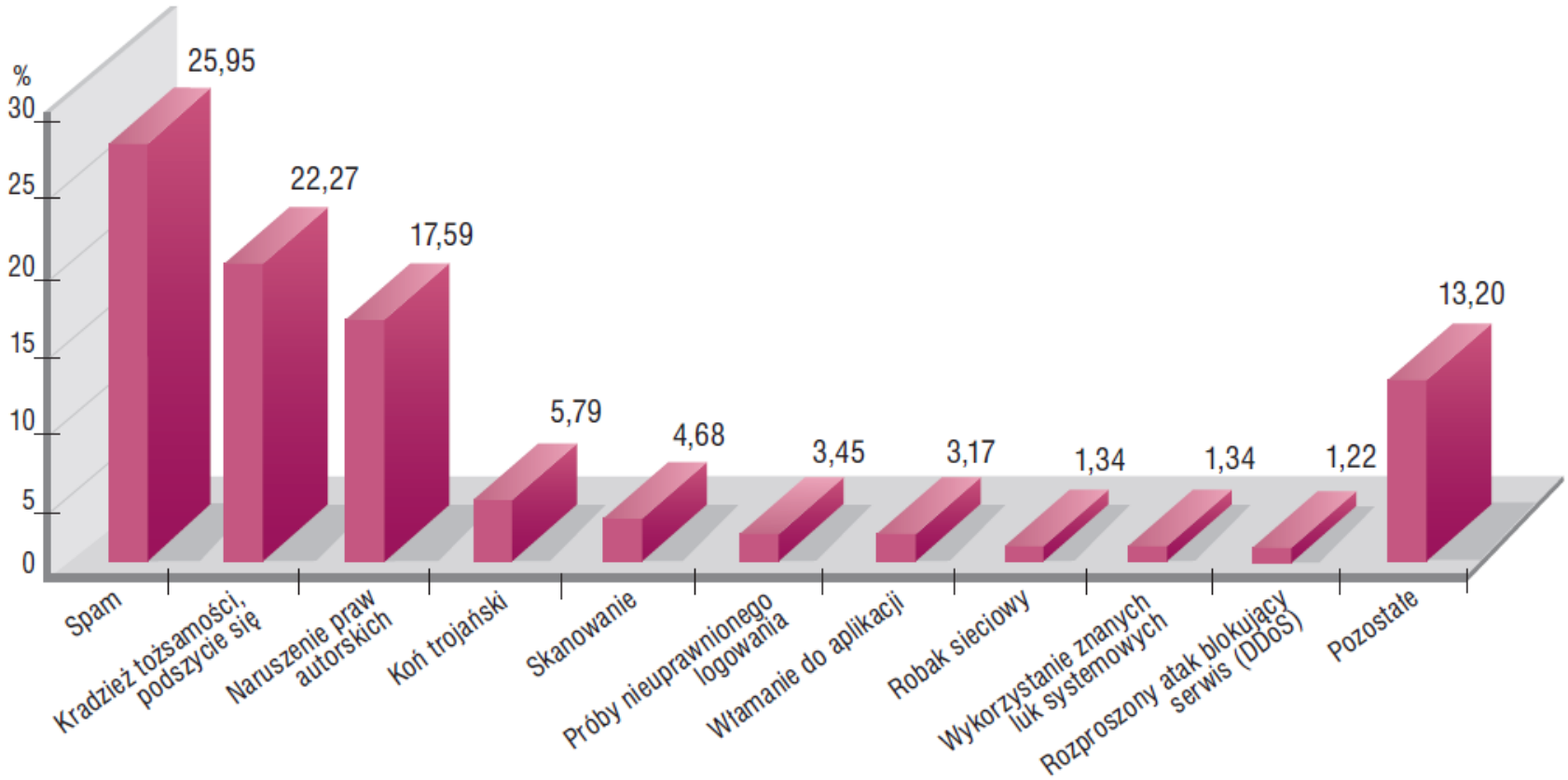
Obraźliwe i nielegalne treści	0
Spam	466
Dyskredytacja, obrażanie	8
Pornografia dziecięca, przemoc[3]	8

Złośliwe oprogramowanie	143
Wirus	3
Robak sieciowy	24
Koń trojański	104
Oprogramowanie szpiegowskie	2
Dialer	0

Rozkład procentowy typów incydentów

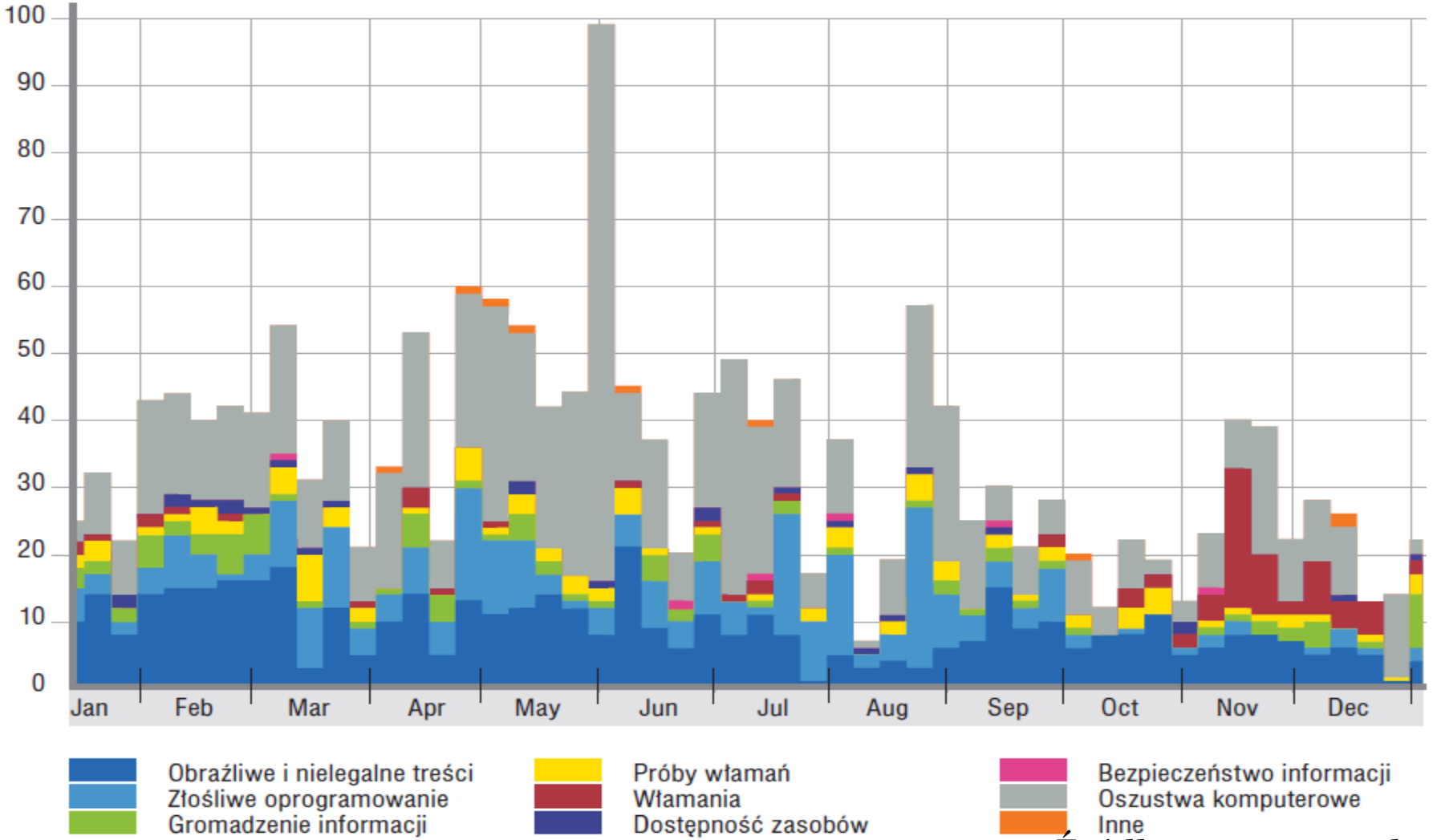
Źródło: www.cert.pl

Rozkład procentowy podtypów incydentów



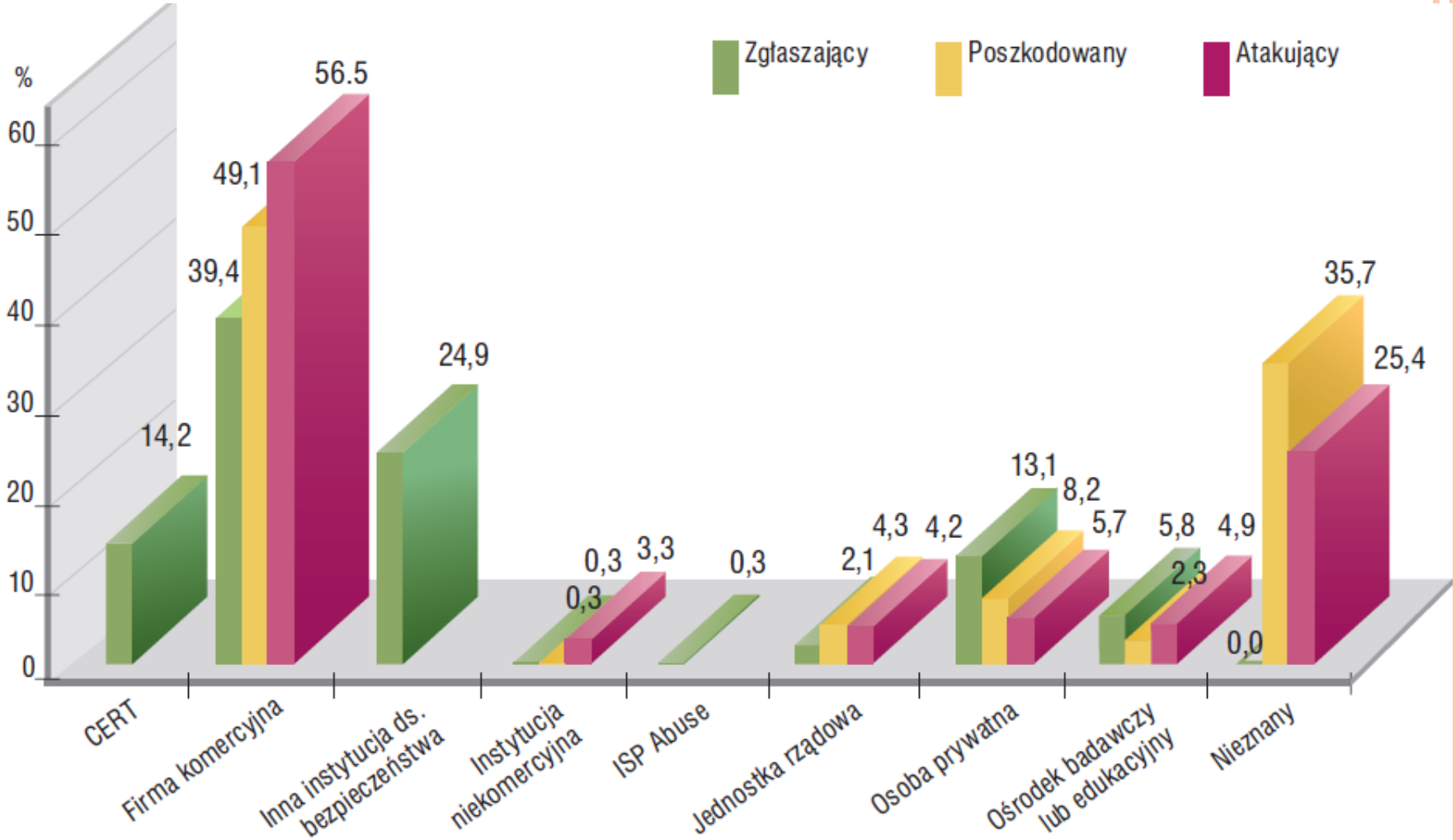
Źródło: www.cert.pl

Liczba incydentów zgłaszanych tygodniowo w 2008



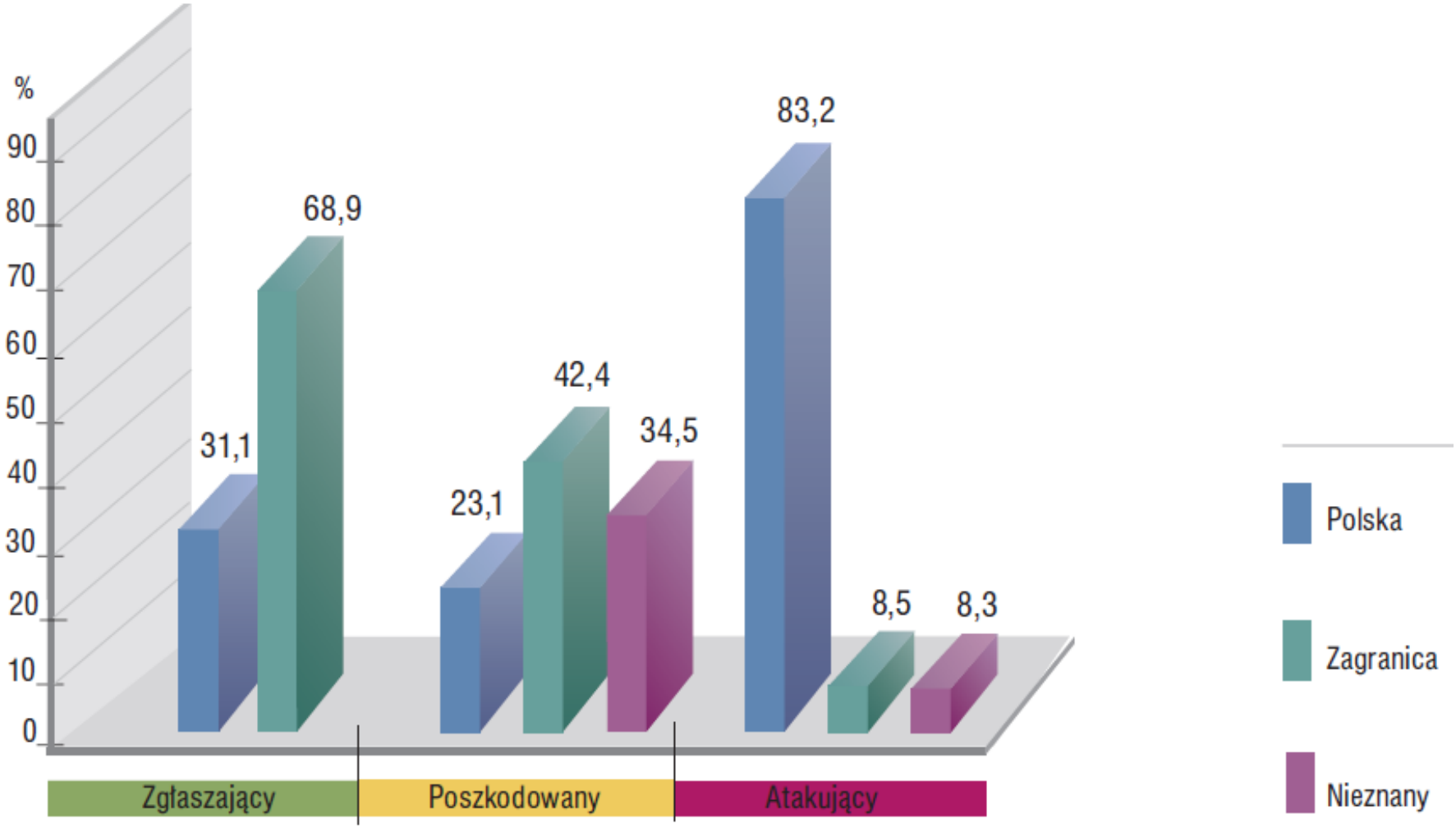
Źródło: www.cert.pl

Źródła zgłoszeń, ataków i poszkodowani



Źródło: www.cert.pl

Pochodzenie zgłaszającego, poszkodowanego i atakującego



Źródło: www.cert.pl

Zagrożenia

- Systemy komputerowe narażone są na dwojakiego rodzaju niebezpieczeństwa:
  - Oprogramowania - Związane z danymi (ujawnianie, przetwarzanie, zniekształcanie, utrata) lub z oprogramowaniem (jego uszkodzeniem bądź wykorzystaniem do celów sprzecznych z prawem)
  - Sprzętowe - dotyczące zniszczeń samego sprzętu. Przestępstwa komputerowe (działanie umyślne) stanowią tu część całości zagrożeń systemów komputerowych, do których zaliczyć można również zachowania nieświadome, powodujące awarie systemu (działania niedoświadczonych użytkowników, zdarzenia losowe, wpływ otoczenia).

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

KLASYFIKACJA ZAGROŻEŃ

- Wskutek różnorodności wykształca się poniższa klasyfikacja zagrożeń
  - zewnętrzne wynikające ze szkodliwego wpływu otoczenia systemu i niewłaściwych zabezpieczeń fizycznych (zamki, drzwi, blokady),
  - zagrożenia wewnętrzne (wg. różnych statystyk, to pracownicy powodują ponad połowę (czasami mówi się o 80%) incydentów związanych z bezpieczeństwem),
  - zagrożenia ze strony sieci komputerowej, w szczególności sieci Internet.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Zagrożenia w sieci komputerowej

- Podsłuchiwanie informacji przekazywanej w sieci komputerowej (Sniffing)
- Przechwytywanie danych w celu ich modyfikacji przed dostarczeniem do odbiorcy (Hijacking)
- Podszywanie się pod inną osobę/urządzenie i wysłanie w jej imieniu (Spoofing)
- Nieuprawniony dostęp do danych zgromadzonych w pamięci dyskowej lub chronionych zasobów informacyjnych, np. WWW
- Przejmowanie uprawnień właścicieli kont internetowych (Phishing)
- Blokowanie dostępu do usług - Denial of Sevice (DoS)
- Przesyłanie niechcianej poczty (Spam)
- Terroryzm sieciowy (cyberterrorism)
- Wirusy/Trojany/Robaki
- System Echelon – National Security Agency

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Echelon

- System Echelon to wspólne przedsięwzięcie USA, Wielkiej Brytanii, Kanady, Australii oraz Nowej Zelandii.
- Stanowi m.in. zespół kilkunastu anten rozsianych po całym świecie i skierowanych w satelity.
- Jego zadaniem jest śledzenie wszystkich rozmów telefonicznych, faksów i danych przesyłanych drogą satelitarną. System w wiadomościach poszukuje ustalonych słów kluczowych. Działa bez zgody sądu i prokuratora.

ECHELON

- Echelon znany jest jako największy **system szpiegowski** na świecie. Kontrolowana przez NSA (National Security Agency, Agencja Bezpieczeństwa Narodowego USA o której pisaliśmy w pierwszym artykule o teoriach spiskowych) sieć urządzeń pozwala na odczytywanie znacznej ilości danych przekazywanych przez systemy telekomunikacyjne takie jak Internet czy sieć GSM. Z przechwyconych informacji wywiad wyłuskuje zwroty związane z terroryzmem i światowym bezpieczeństwem.
- System ten gromadzi i analizuje wszelkie przekazy elektroniczne z całego świata - faksy, e-maile, transfery plików, a nawet zwykłe rozmowy telefoniczne. Szacuje się, że system gromadzi i przetwarza ok. 3 miliardy przekazów elektronicznych na dobę. Zebrane lokalnie informacje z całego świata przesyłane są do centrali w Fort Meade, gdzie znajduje się też główna siedziba NSA. Superkomputery dokonują analizy materiału, dostosowanej do regionu: język, słownik haseł i stanu materiału: kompresja, szyfr.

Nie można zaprzeczyć, że działalność NSA zapobiegła wielu przestępstwom, a wokół niej narosły setki mitów. Niestety, obecna postać agencji prowokuje do podejrzeń i zarzutów o zbyt dużą władzę. Fakty takie jak utajnienie kryptoanalizy różnicowej, backdoor w powszechnie używanym standardzie czy szyfrowanie wiadomości użytkowników biznesowych kluczem publicznym agencji mogą budzić sprzeciw. Jest on wzmacniany ukrywaniem informacji np. o Echelonie i zakresie działania NSA. Czy wymienione sytuacje to tylko teorie spiskowe, czy może rzeczywiste zagrożenie? To pytanie pozostanie otwarte przez długi czas

Ściśle tajne

•Akt powołujący NSA był ściśle tajny. Przez kilkadziesiąt lat rząd USA nie potwierdził jej istnienia, a pracownikom zakazano mówić gdzie pracują.

•Statut agencji do dziś nie został ujawniony.

•Cywilni pracownicy NSA mogą korzystać wyłącznie z usług dentystów zatwierdzonych przez agencję.

•Fort Meade, siedziba NSA, jest uznawany za największe skupisko matematyków na świecie.

•W siedzibie NSA działa wytwórnia mikroprocesorów dla parku komputerowego agencji.

•NSA tłumaczy się żartobliwie jako No Such Agency (ang. nie ma takiej agencji).

•W latach 80. sieć obsługująca Echelon była większa od ówczesnego Internetu.

SZKODLIWE PROGRAMY

Czym są szkodliwe programy – jakie są ich rodzaje i funkcje, jak się przed nimi bronić?

Szkodliwe oprogramowanie *(ang. Malware - malicious software)* to termin, który stosuje się w odniesieniu do każdego rodzaju niebezpiecznych aplikacji. W skład malware wchodzą zatem między innymi wirusy, trojany, robaki czy spyware. Są to terminy, z którymi można spotkać się najczęściej.

Wirus – jest to szkodliwy kod, który dołącza się do zdrowych, niezarażonych plików. Podobnie jak wirus biologiczny w naturze, tak i wirus komputerowy potrzebuje nosiciela, dzięki któremu może się powielać. Jego działanie często jest destrukcyjne dla zainfekowanych programów.

Robak – jest bardzo podobny do wirusa, jednak podstawową różnicą jest brak nosiciela jako czynnika wymaganego do reprodukcji – robak potrafi się sam powielać. Główną „przestrzenią" życiową robaków jest Internet, jednak przenoszą się także przez pamięci przenośne. Niektóre robaki internetowe potrafią pobierać z Internetu dodatkowe składniki.

Trojan, inaczej koń trojański, jak sama nazwa wskazuje, nawiązuje do mitologii greckiej. Jest to program, który udaje pożyteczną aplikację (np. grę komputerową). Użytkownik instaluje taki program, będąc nieświadomym jego destrukcyjnego charakteru. Działanie trojana zależy wyłącznie od jego twórcy - może on kasować określone pliki systemowe, przechwytywać wpisywane poprzez klawiaturę informacje lub wykorzystać komputer do wysyłania spamu.

Spyware – grupa programów szpiegujących działanie użytkownika. Ich głównym zadaniem jest wykradanie danych takich jak hasła, loginy, numery kart kredytowych oraz przechwytywanie wpisywanych przez klawiaturę informacji .

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Potencjalne ataki

- Przerwanie przesyłania danych – informacja nie dociera do odbiorcy

- Przechwycenie danych – informacja dochodzi do odbiorcy, ale odczytuje ją również strona trzecia

- Modyfikacja danych – informacja zostaje przejęta, zmodyfikowana i w fałszywej postaci dostarczona do odbiorcy

- Sfabrykowanie danych – odbiorca dostaje informację, której nadawca jest nieprawdziwy

WIRUS, ROBAK I KOŃ TROJAŃSKI

- Wirus – to program, który przyłącza się do innych programów i jest wraz z nimi przenoszony pomiędzy komputerami.
  - Obecnie znane są tysiące odmian i rodzajów wirusów.
  - Może powodować różnorodne szkody: zmieniać lub uszkadzać dane, zakłócać komunikację, wyświetlać komunikaty, przechwytywać informacje, spowalniać pracę systemu, zmieniać ustawienia komputera
- W sieciach pojawiły się również tzw. robaki, infekujące kolejne systemy komputerowe. "Robaki" rozmnażają się i przemieszczają.
- Koń trojański – program, który podszywa się pod aplikacje i zawiera dodatkową niepożądaną funkcjonalność (np. spyware, backdoor)

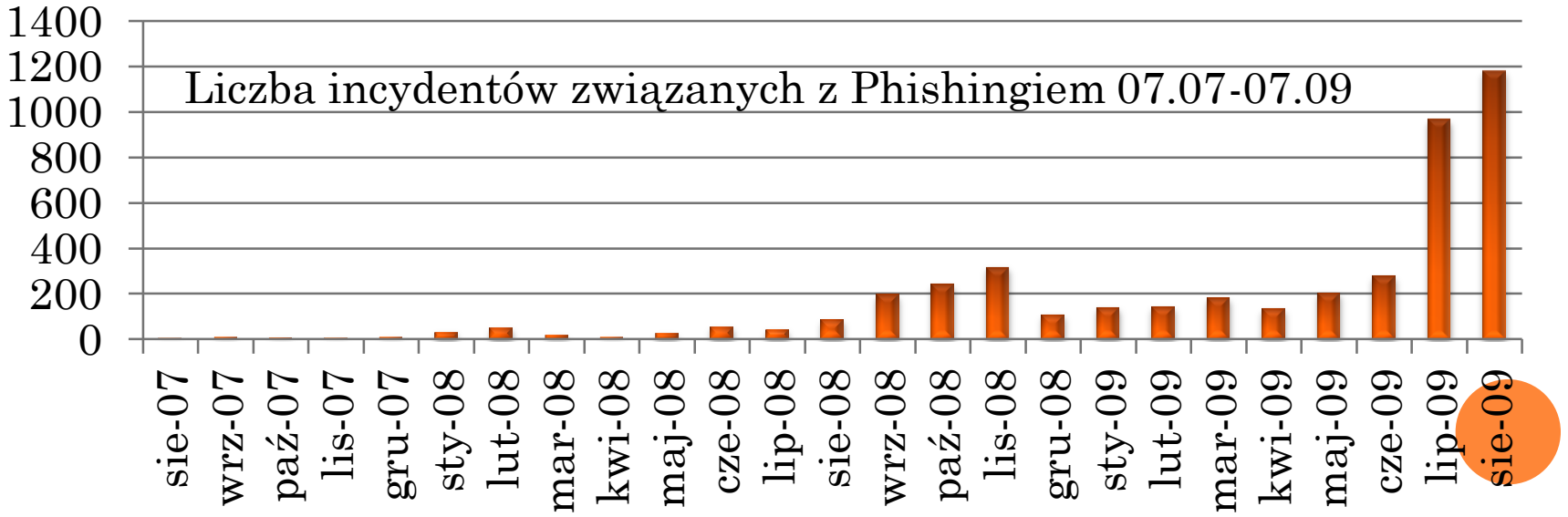
KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Phishing

- wyłudzanie poufnych informacji osobistych przez podszywanie się pod godną zaufania osobę lub instytucję, której te informacje są pilnie potrzebne. Jest to rodzaj ataku opartego na inżynierii społecznej.



http://www.phishtank.com

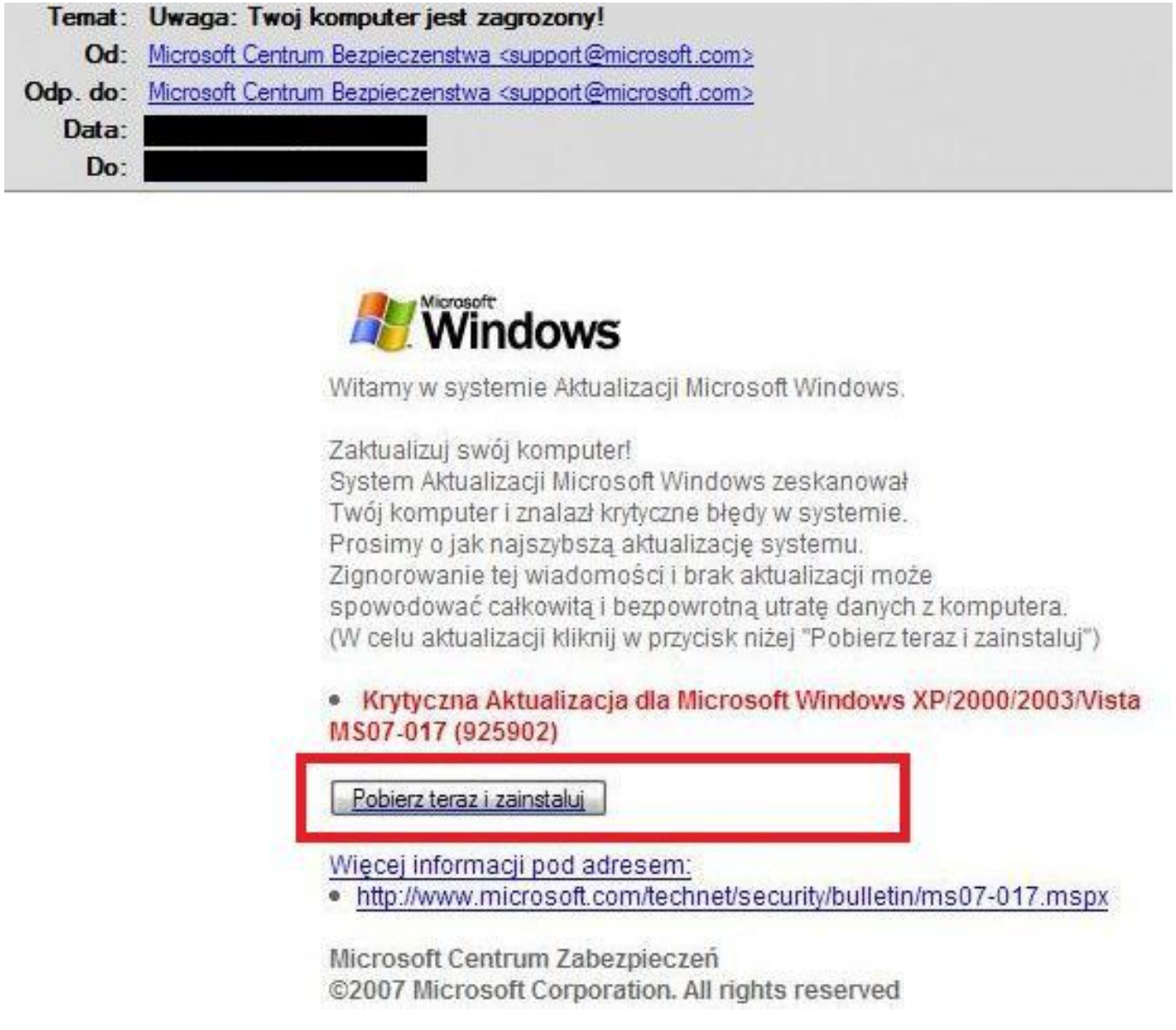
Na czym polega phishing – jak rozpoznać fałszywą wiadomość?

Nazwa ta pochodzi od angielskiego słowa *fishing* – wędkować, łowić. Metoda łączy w sobie najczęściej próbę manipulacji użytkownikiem i skłonienia go do określonych działań oraz infekcji komputera ofiary programem szpiegującym lub trojanem.
Phishing to wiadomość wysyłana za pomocą komunikatora internetowego lub e-maila, która zachęca do kliknięcia umieszczonego w niej odnośnika, przenosząc nas na fałszywą stronę jakiejś organizacji (najczęściej są to banki). Tam proszeni jesteśmy o podanie swoich danych osobowych lub o pobranie jakiegoś oprogramowania, które okazuje się być trojanem. Atakujący stara się skomponować całość tak, abyśmy byli niemalże pewni autentyczności wiadomości.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Temat: **Uwaga: Twoj komputer jest zagrozony!**
Od: Microsoft Centrum Bezpieczenstwa <support@microsoft.com>
Odp. do: Microsoft Centrum Bezpieczenstwa <support@microsoft.com>
Data: [redacted]
Do: [redacted]

Microsoft Windows

Witamy w systemie Aktualizacji Microsoft Windows.

Zaktualizuj swój komputer!
System Aktualizacji Microsoft Windows zeskanował
Twój komputer i znalazł krytyczne błędy w systemie.
Prosimy o jak najszybszą aktualizację systemu.
Zignorowanie tej wiadomości i brak aktualizacji może
spowodować całkowitą i bezpowrotną utratę danych z komputera.
(W celu aktualizacji kliknij w przycisk niżej "Pobierz teraz i zainstaluj")

- **Krytyczna Aktualizacja dla Microsoft Windows XP/2000/2003/Vista MS07-017 (925902)**

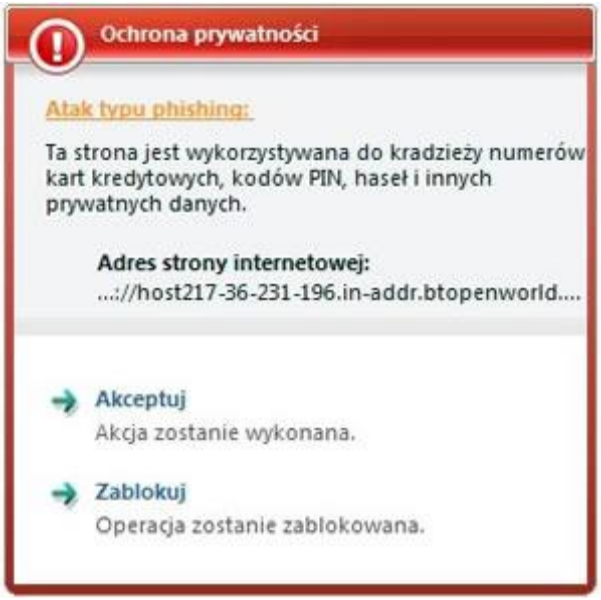
Pobierz teraz i zainstaluj

Więcej informacji pod adresem:
- http://www.microsoft.com/technet/security/bulletin/ms07-017.mspx

Microsoft Centrum Zabezpieczeń

KASPERSKY VS. PHISHING

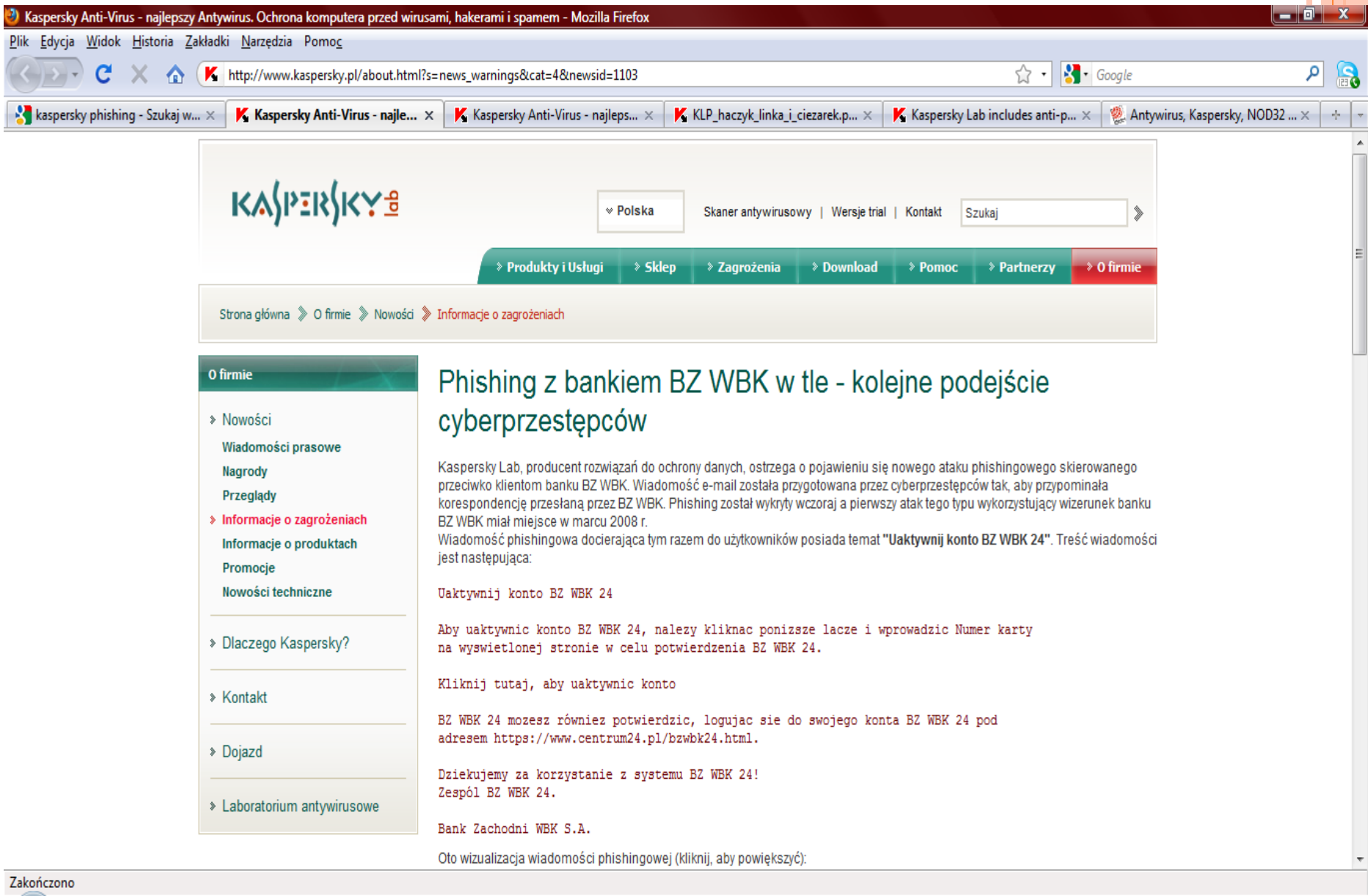
Technologie wbudowane w *Kaspersky Internet Security* także pomagają rozpoznać próby wyłudzenia informacji. Użytkownik ostrzegany jest przed takim zagrożeniem jeszcze zanim przejdzie na sfałszowaną witrynę, dzięki czemu ma szanse zareagować w porę i zablokować szkodliwe działanie.



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY


Kaspersky Anti-Virus - najlepszy Antywirus. Ochrona komputera przed wirusami, hakerami i spamem - Mozilla Firefox
Plik Edycja Widok Historia Zakładki Narzędzia Pomoc
http://www.kaspersky.pl/about.html?s=news_warnings&cat=4&newsid=1103
Google
kaspersky phishing - Szukaj w...
Kaspersky Anti-Virus - najle...
Kaspersky Anti-Virus - najleps...
KLP_haczyk_linka_i_ciezarek.p...
Kaspersky Lab includes anti-p...
Antywirus, Kaspersky, NOD32 ...
KASPERSKY lab
Polska
Skaner antywirusowy | Wersje trial | Kontakt
Szukaj
Produkty i Usługi
Sklep
Zagrożenia
Download
Pomoc
Partnerzy
O firmie
Strona główna
O firmie
Nowości
Informacje o zagrożeniach
O firmie
Nowości
Wiadomości prasowe
Nagrody
Przeglądy
Informacje o zagrożeniach
Informacje o produktach
Promocje
Nowości techniczne
Dlaczego Kaspersky?
Kontakt
Dojazd
Laboratorium antywirusowe
Phishing z bankiem BZ WBK w tle - kolejne podejście cyberprzestępców
Kaspersky Lab, producent rozwiązań do ochrony danych, ostrzega o pojawieniu się nowego ataku phishingowego skierowanego przeciwko klientom banku BZ WBK. Wiadomość e-mail została przygotowana przez cyberprzestępców tak, aby przypominała korespondencję przesłaną przez BZ WBK. Phishing został wykryty wczoraj a pierwszy atak tego typu wykorzystujący wizerunek banku BZ WBK miał miejsce w marcu 2008 r.
Wiadomość phishingowa docierająca tym razem do użytkowników posiada temat "Uaktywnij konto BZ WBK 24". Treść wiadomości jest następująca:
Uaktywnij konto BZ WBK 24
Aby uaktywnic konto BZ WBK 24, nalezy kliknac ponizsze lacze i wprowadzic Numer karty na wyswietlonej stronie w celu potwierdzenia BZ WBK 24.
Kliknij tutaj, aby uaktywnic konto
BZ WBK 24 mozesz również potwierdzic, logujac sie do swojego konta BZ WBK 24 pod adresem https://www.centrum24.pl/bzwbk24.html.
Dziekujemy za korzystanie z systemu BZ WBK 24!
Zespól BZ WBK 24.
Bank Zachodni WBK S.A.
Oto wizualizacja wiadomości phishingowej (kliknij, aby powiększyć):
Zakończono

From: bzwbk@bzwbk.pl
Subject: **Uaktywnij konto BZ WBK 24**
Date: May 14, 2008 2:12:43 AM GMT+02:00
To:
Reply-To: bzwbk@bzwbk.plz

Uaktywnij konto BZ WBK 24

Aby uaktywnic konto BZ WBK 24, nalezy kliknac ponizsze lacze i wprowadzic Numer karty na wyswietlonej stronie w celu potwierdzenia BZ WBK 24.

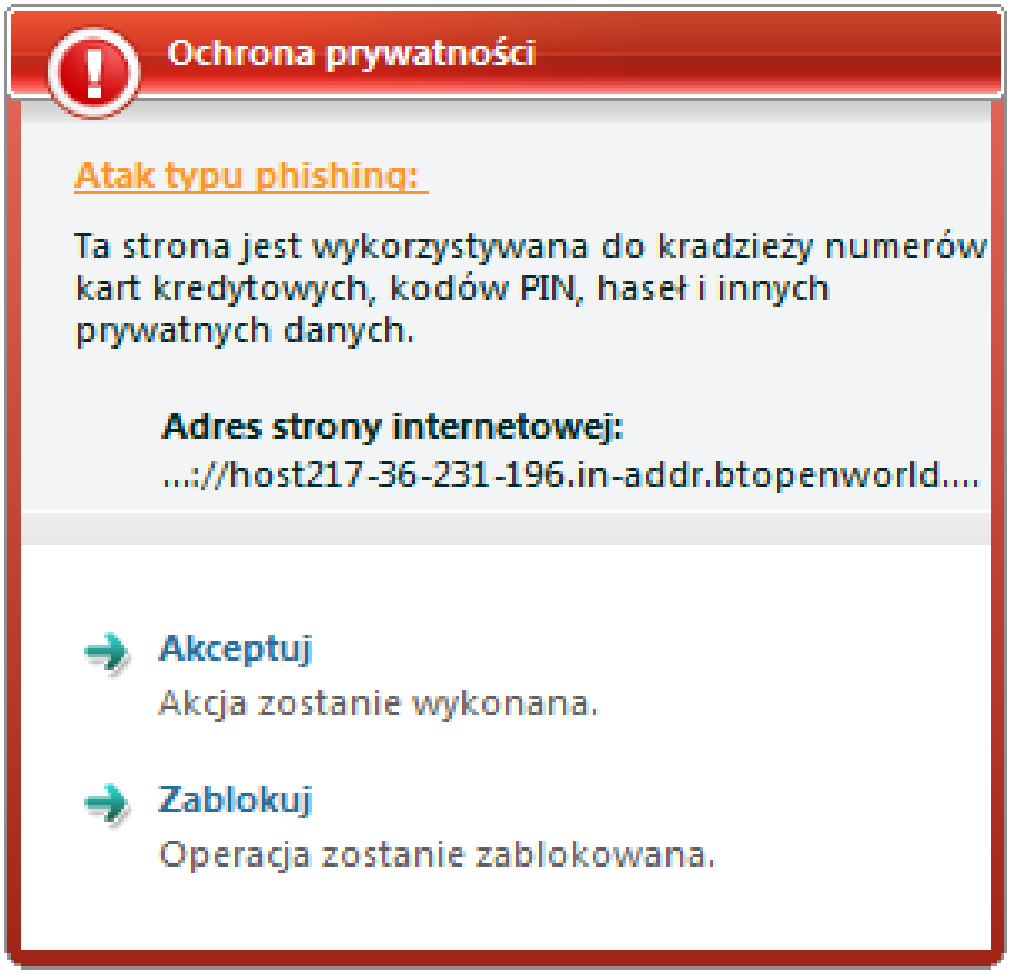
Kliknij tutaj, aby uaktywnic konto

BZ WBK 24 mozesz równiez potwierdzic, logujac sie do swojego konta BZ WBK 24 pod adresem https://www.centrum24.pl/bzwbk24.html.

Dziekujemy za korzystanie z systemu BZ WBK 24!
Zespól BZ WBK 24.

Bank Zachodni WBK S.A.

- Po kliknięciu pierwszego odsyłacza znajdującego się w treści wiadomości użytkownik trafi na sfałszowaną stronę zawierającą formularz, w którym cyberprzestępca przygotował miejsce na wprowadzenie numeru karty płatniczej.
- Oprogramowanie Kaspersky Lab wykrywa ten atak phishingowy. Po kliknięciu odsyłacza ze sfałszowanej wiadomości na ekranie chronionego komputera pojawi się następujący komunikat:
-


Ochrona prywatności
Atak typu phishing:
Ta strona jest wykorzystywana do kradzieży numerów kart kredytowych, kodów PIN, haseł i innych prywatnych danych.
Adres strony internetowej:
...://host217-36-231-196.in-addr.btopenworld....
Akceptuj
Akcja zostanie wykonana.
Zablokuj
Operacja zostanie zablokowana.

- Phishing jest formą cyberprzestępstwa lub oszustwa opartego na socjotechnice. Nazwa jest świadomym błędem w pisowni terminu 'fishing' oznaczającego łowienie ryb. Termin "phishing" odnosi się do procesu zbierania (kradzieży) danych przez przestępców.
- W typowym ataku phishingowym cyberprzestępca tworzy prawie idealną replikę strony WWW dowolnej instytucji lub portalu. Następnie rozpoczyna się "phishing": przy użyciu technik spamowych wysyłane są wiadomości e-mail imitujące prawdziwą korespondencję wysyłaną przez różne instytucje. Hakerzy mogą wykorzystywać prawdziwe logo firmy, nienaganny styl korespondencji handlowej, a nawet prawdziwe nazwiska osób należących do zarządu.
- Wszystkie takie wiadomości mają jeden cel: nakłonienie odbiorców do kliknięcia zawartego w liście odsyłacza. Stworzone przez phisherów odsyłacze kierują użytkowników bezpośrednio do fałszywej strony WWW, na której "schwytana ryba" wprowadza poufne informacje dotyczące numerów kont bankowych, kart kredytowych, haseł dostępu itp. lub pobiera szkodliwy kod, który następnie instalowany jest w systemie.

erprzestępców - Biznes - Informacje - portal TVN24.pl - 20.06.2008 - Mozilla Firefox

Zakładki Narzędzia Pomoc

http://www.tvn24.pl/12692,1554369,0,1,klienci-ipko-na-celowniku-cyberprzestepcow,wiadomosc.html

Google

yberprzes...

TVN24.pl WIDEO ZUMI

SZUKAJ

FAKTY

oglądaj w internecie »

INFORMACJE | WIDEO | FOTO | FAKTY | NA ŻYWO | PROGRAM | TERAZ MY | FORUM | KONTAKT TVN24

+ startuj z nami

Najważniejsze | Najnowsze | Polska | Świat | Sport | Biznes | Meteo | Michałki | Kultura | więcej

Kontakt TVN24

Autobus spłonął w Katowicach

16.01 | Kolejny pożar autobusu komunikacji miejskiej,...

Sople spadły na kobietę

13.01| Wielka bryła lodu spadła z budynku wprost na...

Biznes

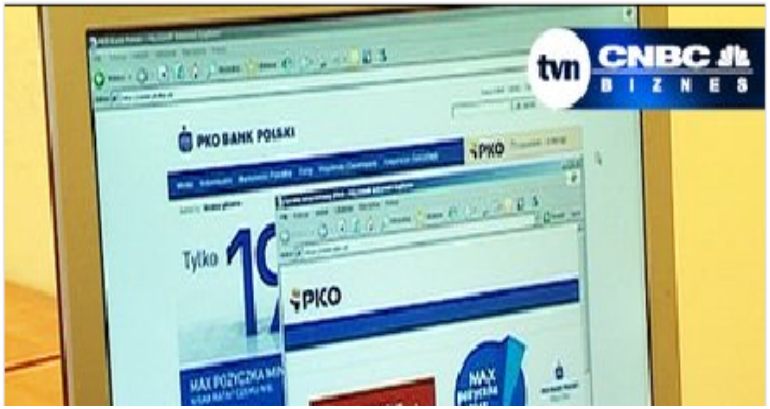
Kanały RSS RSS

02:55, 20.06.2008 /TVN CNBC Biznes, di.com.pl

Tagi: pieniądze, internet, przestępczość, banki

Klienci iPKO na celowniku cyberprzestępców

NOWA, BARDZIEJ WYRAFINOWANA METODA E-NAPADÓW



15:30 Giełdowa relacja TVN CNBC Biznes

Internet według Google

Obejrzyj wywiad TVN CNBC Biznes

czytaj »

Polskie stocznie na wyprzedaży

czytaj »

PKO - Najnowsze informacje - Informacje - portal TVN24.pl - 01.12.2009 - Mozilla Firefox

akładki Narzędzia Pomoc

http://www.tvn24.pl/0,1631455,0,1,wyludzacze-poluja-na-klientow-ipko,wiadomosc.html

w iPKO ...

TVN24.pl WIDEO ZUMI

INFORMACJE WIDEO FOTO FAKTY NA ŻYWO PROGRAM TERAZ MY FORUM K

Najważniejsze | Najnowsze | Polska | Świat | Sport | Biznes | Met

Kontakt TVN24

Autobus spłonął w Katowicach

16.01 | Kolejny pożar autobusu komunikacji miejskiej,...

Sople spadły na kobietę

13.01| Wielka bryła lodu spadła z budynku wprost na...

Najnowsze informacje

Kanały RSS RSS

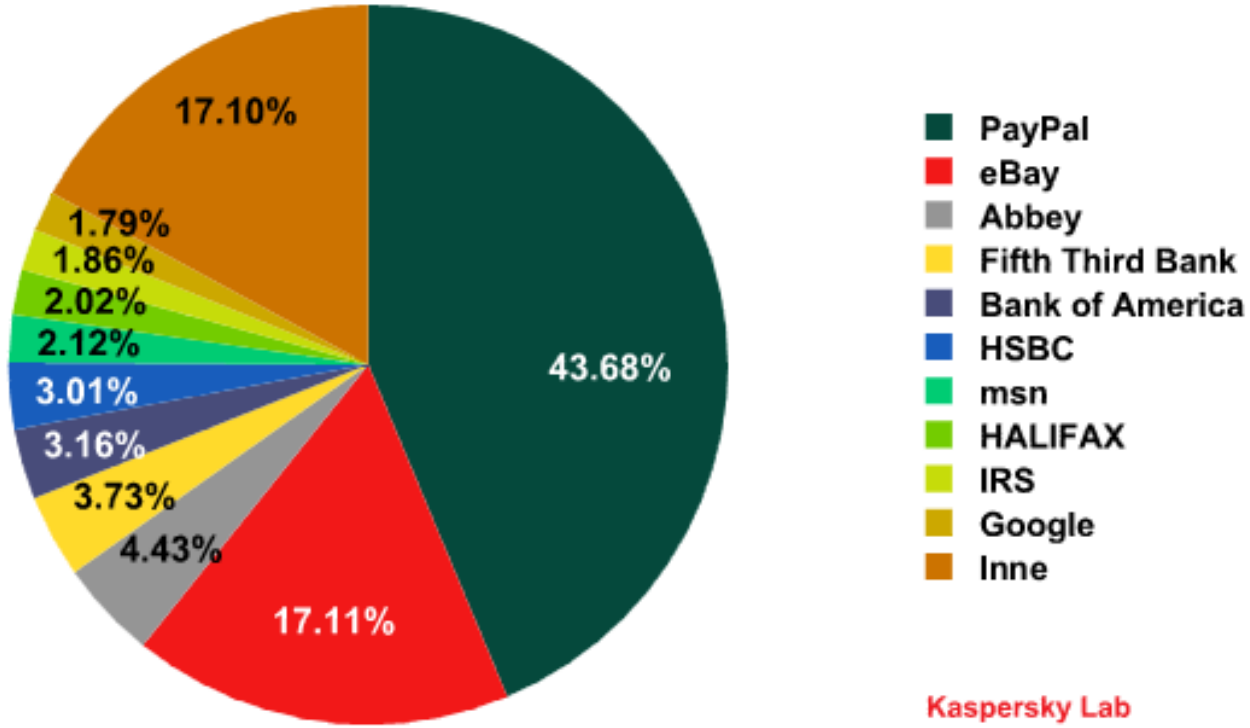
11:51, 01.12.2009 /tvn24.pl, Kontakt TVN24

Tagi: internet, banki

Wyłudzacze polują na klientów iPKO

NIE DAJ SIĘ NABRAĆ CYBERPRZESTĘPCOM

Główne cele ataków phishingowych

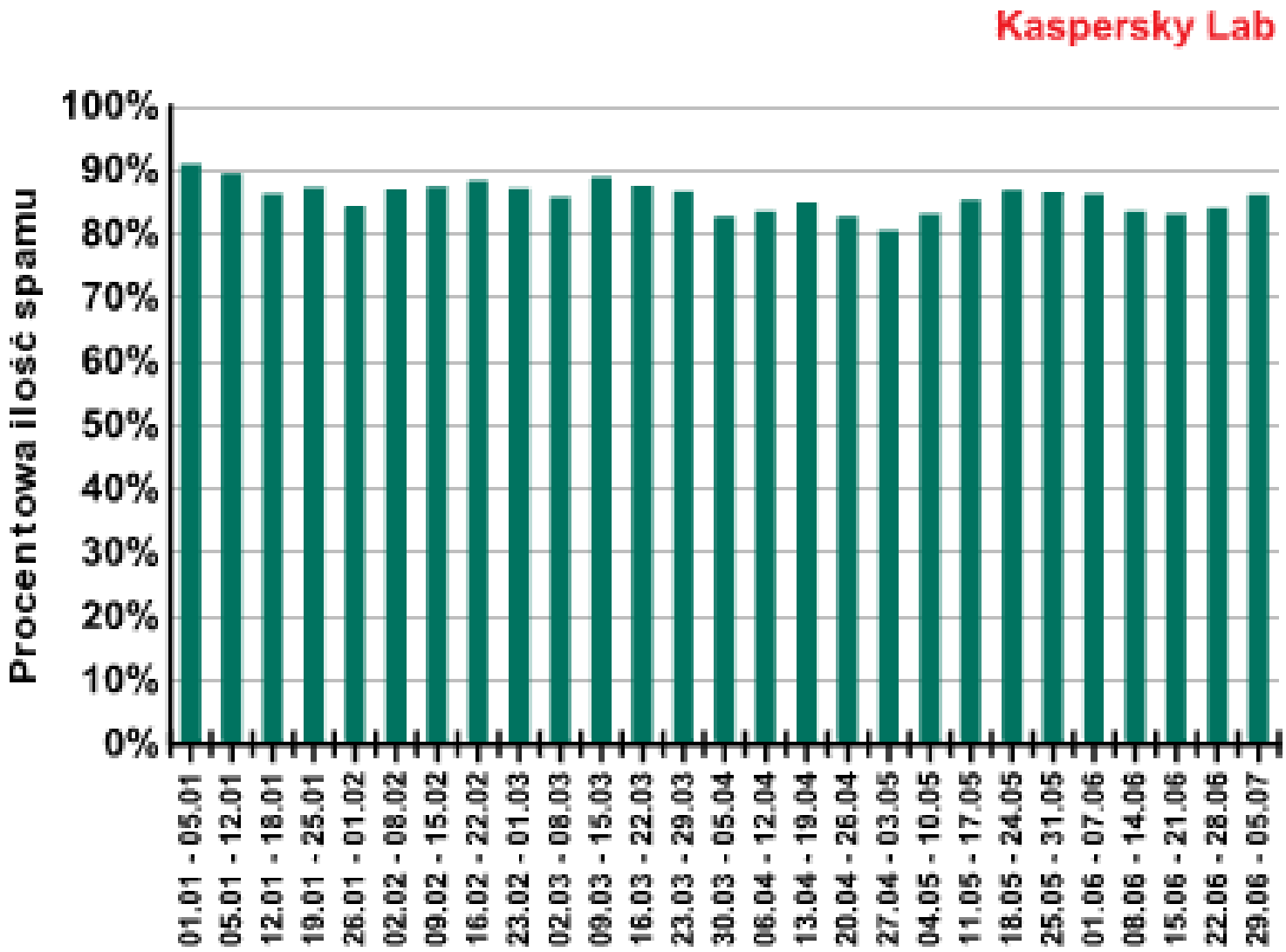


KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Spam w ruchu pocztowym



SPAM

Zjawisko spamu zaistniało dawno temu, praktycznie już na samym początku sieci komputerowych. Pierwszy został odnotowany 1 maja 1978 roku, kiedy to niejaki Einar Stefferud wysłał 1000 maili z zaproszeniami na swoje urodziny. Niepożądane wiadomości, których treść nie jest związana z tożsamością odbiorcy, stały się prawdziwą plagą Internetu. Całkowita liczba spamu w ciągu roku sięga miliardów. Niosą one za sobą wiele szkód: zwalniają pracę serwerów, zatykają łącza, zaśmiecają skrzynkę odbiorczą, często szerzą wiadomości o obraźliwych i niemoralnych treściach (np. pornografia), utrudniają pracę z pocztą elektroniczną, mogą służyć do rozpowszechniania złośliwego oprogramowania.

Najważniejsze środki do zwalczania niechcianej poczty e-mail:

1. filtry blokujące spam,
2. stosowanie odpowiednich narzędzi programów pocztowych,
3. umiejętność czytania nagłówków oraz różne techniki blokowania spamu.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Odróżnianie spamu od prawdziwych wiadomości

Spam wyróżnia się takimi cechami, jak bałamutny temat, podejrzany (nieistniejący) adres czy dziwna treść. Programy filtrujące blokują wiadomości, gdy znajdą w nich takie składniki. Podstawę wszystkich filtrów antyspamowych stanowi sortowanie wiadomości e-mail według kategorii. Prawdziwe wiadomości, niestety, również są omyłkowo blokowane, gdyż często posiadają składniki, którymi charakteryzuje się spam. Istnieje sześć podstawowych typów wiadomości. Pierwsze to wiadomości osobiste, które są bezpośrednio do nas zaadresowane. Program może je przez pomyłkę zablokować, kiedy w treści wystąpią zwroty spotykane w spamach - emotikony ("buźki"), dziwne ciągi znaków itp.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Drugą kategorię stanowią wiadomości osobiste, które nie są do nas bezpośrednio zaadresowane. Nasz adres w tym przypadku znajduje się w polu DW (do wiadomości) albo UDW (ukryte do wiadomości). Filtry często traktują wiadomości z polem UDW jako spam. Następne są to listy skierowane do grupy, której jesteśmy członkami. One z reguły także nie są bezpośrednio zaadresowane, przez co mogą być blokowane. Kolejnym typem są wiadomości handlowe, które chcemy otrzymywać. Z tą kategorią filtry mają dużo problemów, ponieważ trudno jest im odróżniać usługi pożądane i niechciane. Następną kategorią są właśnie niechciane wiadomości promocyjne. Skoro nie chcemy ich otrzymywać, traktowane są jako spam. Ostatnim typem są niechciane listy pochodzące z nieznajomego lub anonimowego źródła. Do tej kategorii należy większość spamów: łańcuszki szczęścia, reklamy witryn dla dorosłych i inne dokuczliwe wiadomości.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Techniki blokowania spamu

- **Wycofaj się z niechcianej korespondencji**
- **Do niepewnych operacji używaj oddzielnego adresu**
- **Wybierz dobry program pocztowy**
- **Stosuj filtry (również do tworzenia wyjątków dla wiadomości)**

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

CRC (Cyclic Redundancy Check–cykliczny kod nadmiarowy)

- Jest to ciąg kontrolny wykorzystywany do wykrywania

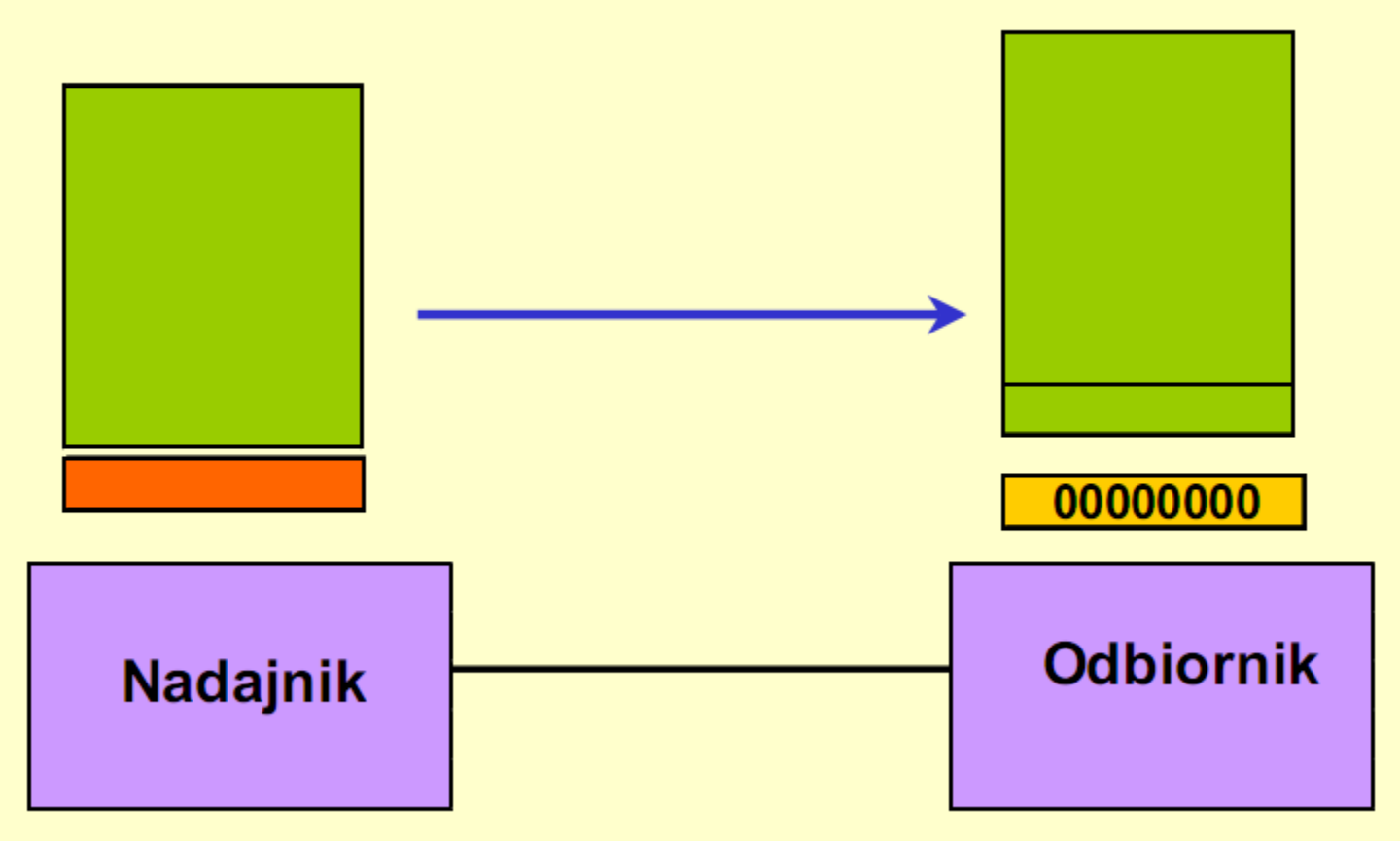
uszkodzonych danych binarnych

- Sekwencja CRC jest obliczana w nadajniku na podstawie zawartości przesyłanego pakietu danych
- Wyznaczony kod CRC jest dodawany do przesyłanego pakietu
- Odbiornik realizuje ten sam algorytm obliczenia dla całego bloku danych z uwzględnieniem dołączonej sekwencji kontrolnej CRC
- Wynikiem wykonania tych obliczeń powinna być sekwencja zerowa, co sygnalizuje poprawną transmisję

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

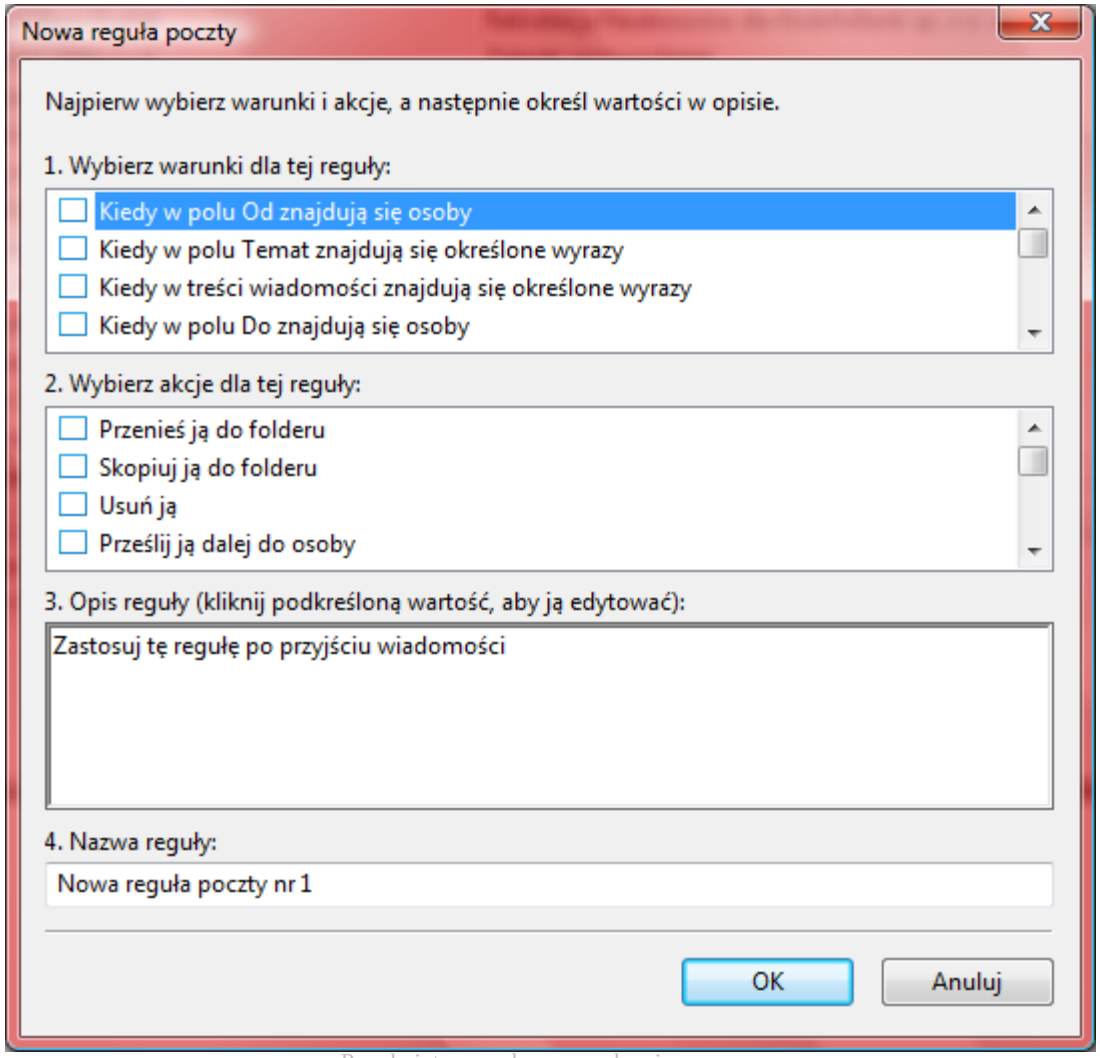
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

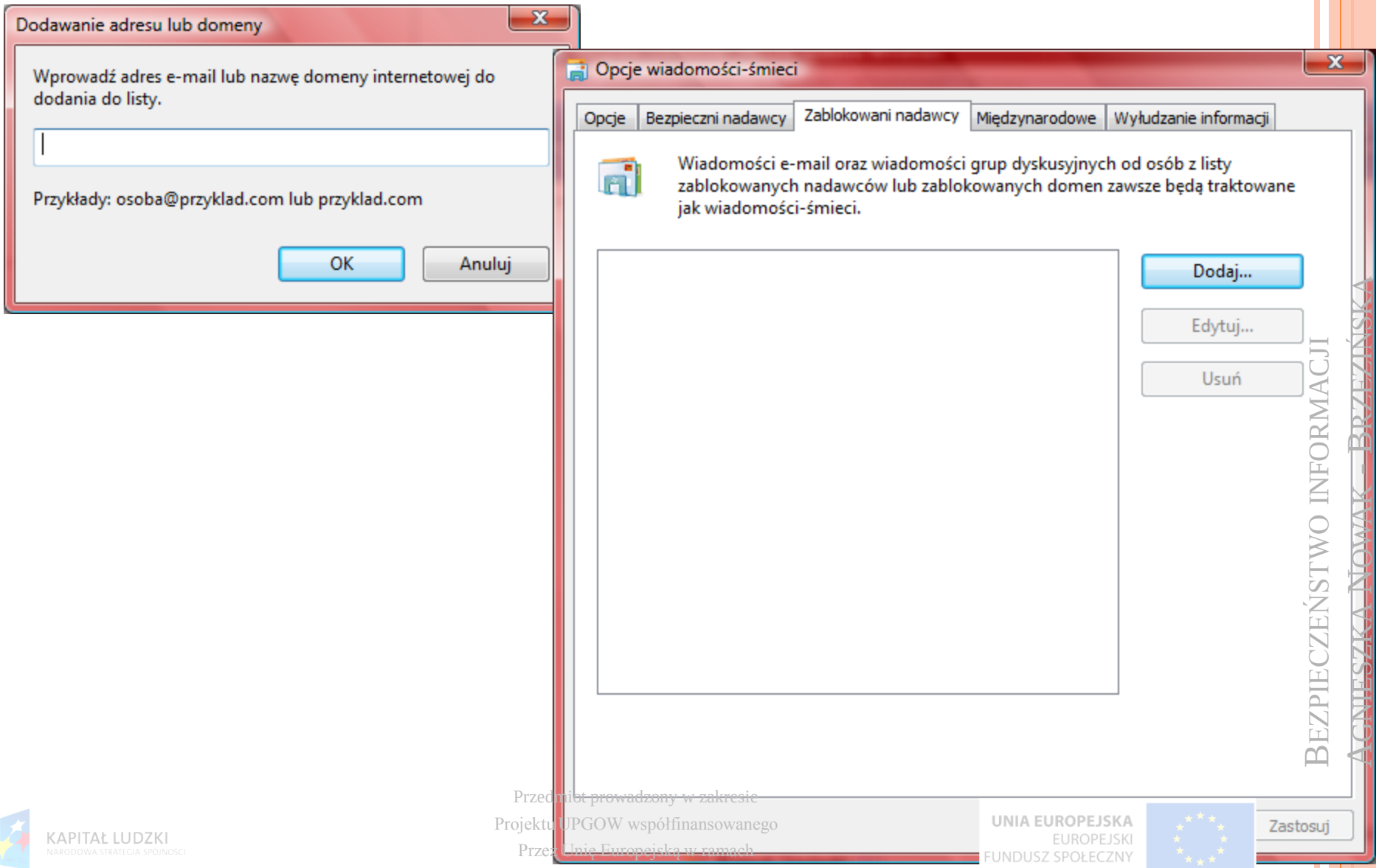
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

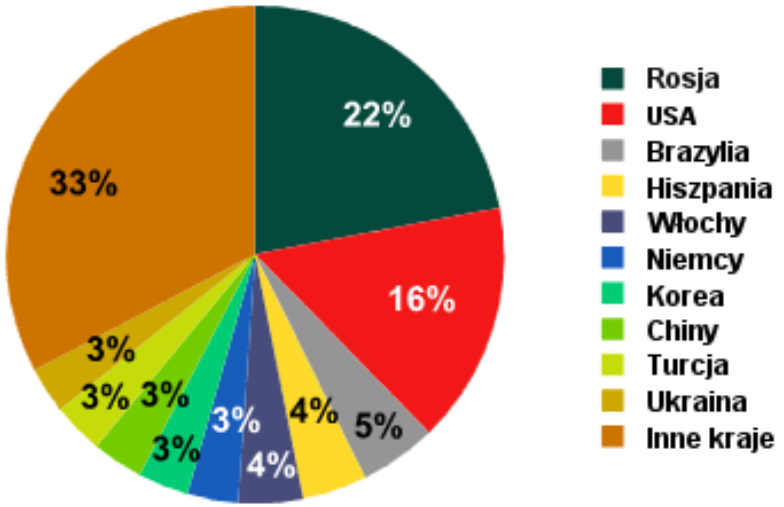


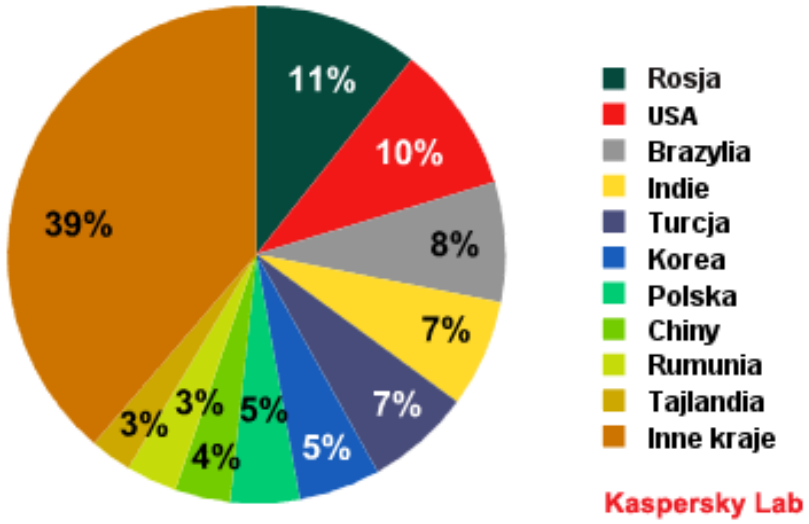
KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

SPAMU (II POŁOWA 2008 R.; I POŁOWA 2009 R.)





BEZPIECZEŃSTWO INFORMACJI
AGNIESZKA NOWAK - BRZEZIŃSKA

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Hacker

- Haker (z ang. hacker) to osoba o dużych praktycznych umiejętnościach w sprawach związanych z komputerami. Doskonale zna języki programowania i systemy operacyjne.
- Nie ma ścisłej definicji hakera i o tym czy dana osoba jest czy też nie jest hakerem decyduje przede wszystkim reputacja wśród innych hakerów.
- Posługuje się specyficznym językiem http://www.catb.org/~esr/jargon/

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Więcej z historii hackowania

- Angielskie słowo hacker pochodzi od hack, co znaczy poprawka, mała modyfikacja. Słowa 'hack' zaczęto używać na Massachusetts Institute of Technology w latach 60-tych do określenia żartów płatanych przez studentów, takich jak np. owinięcie górującej nad kampusem uniwersyteckim kopuły folią odbijającą promienie świetlne. Aby zasłużyć na to określenie żarty musiały się wyróżniać szczególną pomysłowością i stylem.
- Miano hackera nadawali sobie wzajemnie niektórzy członkowie Tech Model Railroad Club działającego na tej uczelni. Część z nich przeniosła później swoje zainteresowanie na komputery - ich możemy nazwać pierwszymi hakerami.

Kto jest naszym wrogiem

- Cracker (włamywacz) włamuje się lub w inny sposób narusza bezpieczeństwo komputer zdalnego. Po uzyskaniu nieautoryzowanego dostępu niszczy kluczowe dane, zamyka dostęp prawowitym użytkownikom i ogólnie przyczynia się do powstawania problemów. Krakera jest łatwo poznać: kierują nim złe pobudki.
- Phracker - Osoba zajmująca się kradzieżami programów umożliwiających bezpłatne korzystanie z usług telekomunikacyjnych lub mająca komputery i bazy danych firm oferujących takie usługi.
- Phreaker - osoba korzystająca z ukradzionych informacji dotyczących połączeń telefonicznych takich jak numery kart lub numery abonentów w celu uzyskania dostępu do innych komputerów

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Przestępstwo komputerowe

- Definiuje się jako bezprawne, nieetyczne i nieupoważnione działania wpływające na proces przetwarzania i/lub przekazywania danych.
- W świetle prawa przestępstwa komputerowego dopełnia się sprawca, który korzysta z komputera jako narzędzia służącego do popełniania przestępstwa lub działania sprawcy są skierowane przeciwko urządzeniom komputerowym.
- Przestępstwo komputerowe można również popełnić sprowadzając niebezpieczeństwo dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach poprzez zakłócenie, uniemożliwienie lub wpływanie w inny sposób na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji, nie wspominając już o szpiegostwie komputerowy.

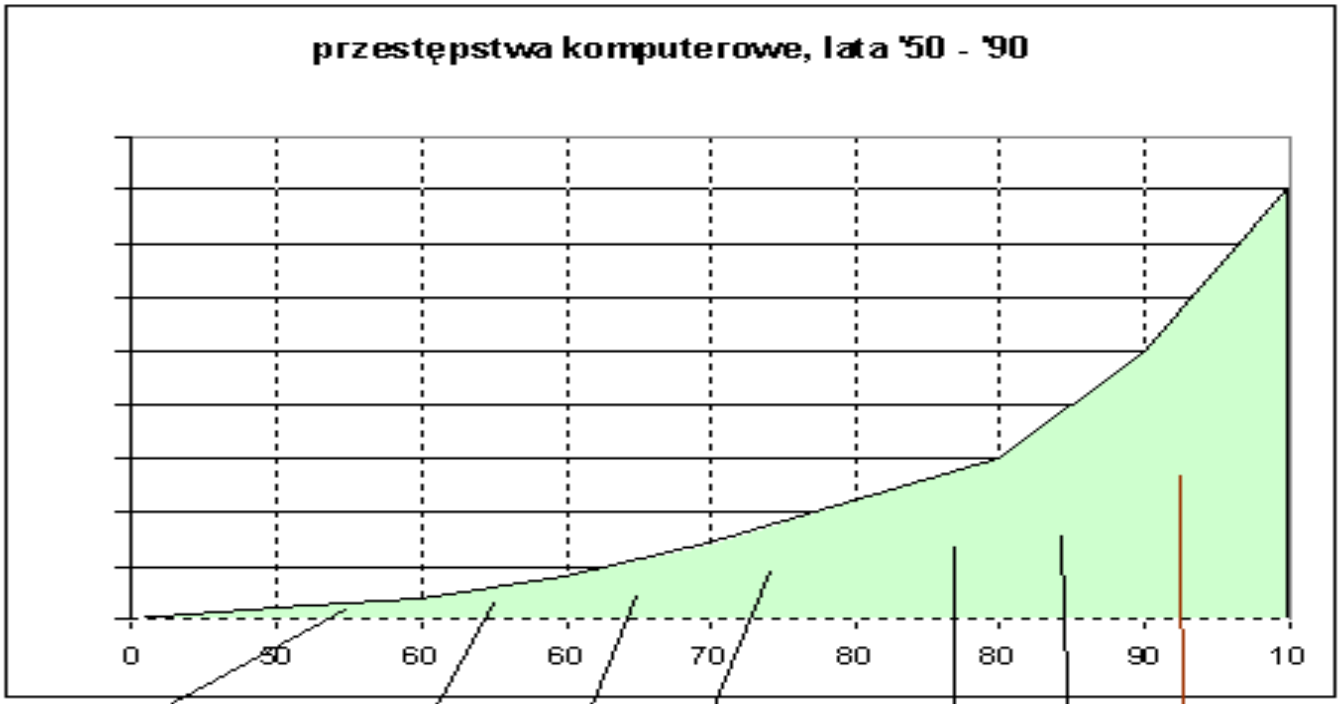
KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

KARNOPRAWNE ASPEKTY PRZESTĘPSTW KOMPUTEROWYCH

- Kwestie dotyczące postępowania w przypadku przestępstw komputerowych reguluje przede wszystkim Kodeks Karny w ustawie z 6 czerwca 1997 r. (Dz.U. nr 88, poz. 553), w kilku osobnych rozdziałach:
  - rozdział XXXIII – Przestępstwa przeciwko ochronie informacji (art. 267 § 1 i 2, art. 268 § 2 oraz art. 296 § 1 i 2 kk);
  - rozdział XXXV – Przestępstwa przeciwko mieniu (art. 278 § 2 i 5, art. 285 § 1, art. 287 § 1 oraz art. 293 § 1 kk);
  - rozdział XX – Przestępstwa przeciwko bezpieczeństwu powszechnemu (art. 165 § 1 ust. 4, art. 165 § 2 i art. 167 § 2 kk);
  - rozdział XVII – Przestępstwa przeciwko Rzeczypospolitej Polskiej (art. 130 § 2 i 3 oraz art. 138 § 2 kk);
  - rozdział XXXIV – Przestępstwa przeciwko wiarygodności dokumentów (art. 270 § 1 kk).
  - jak również w niewielkim stopniu Kodeks Cywilny (np. co do ochrony korespondencji - art.25 oraz 415 kc).



Wykorzystanie komputerów do rutynowych prac w administracji

Pierwsze wypadki

Tworzenie masowych baz danych i ograniczenie praw dostępu do nich traktowane jako zagrożenie praw

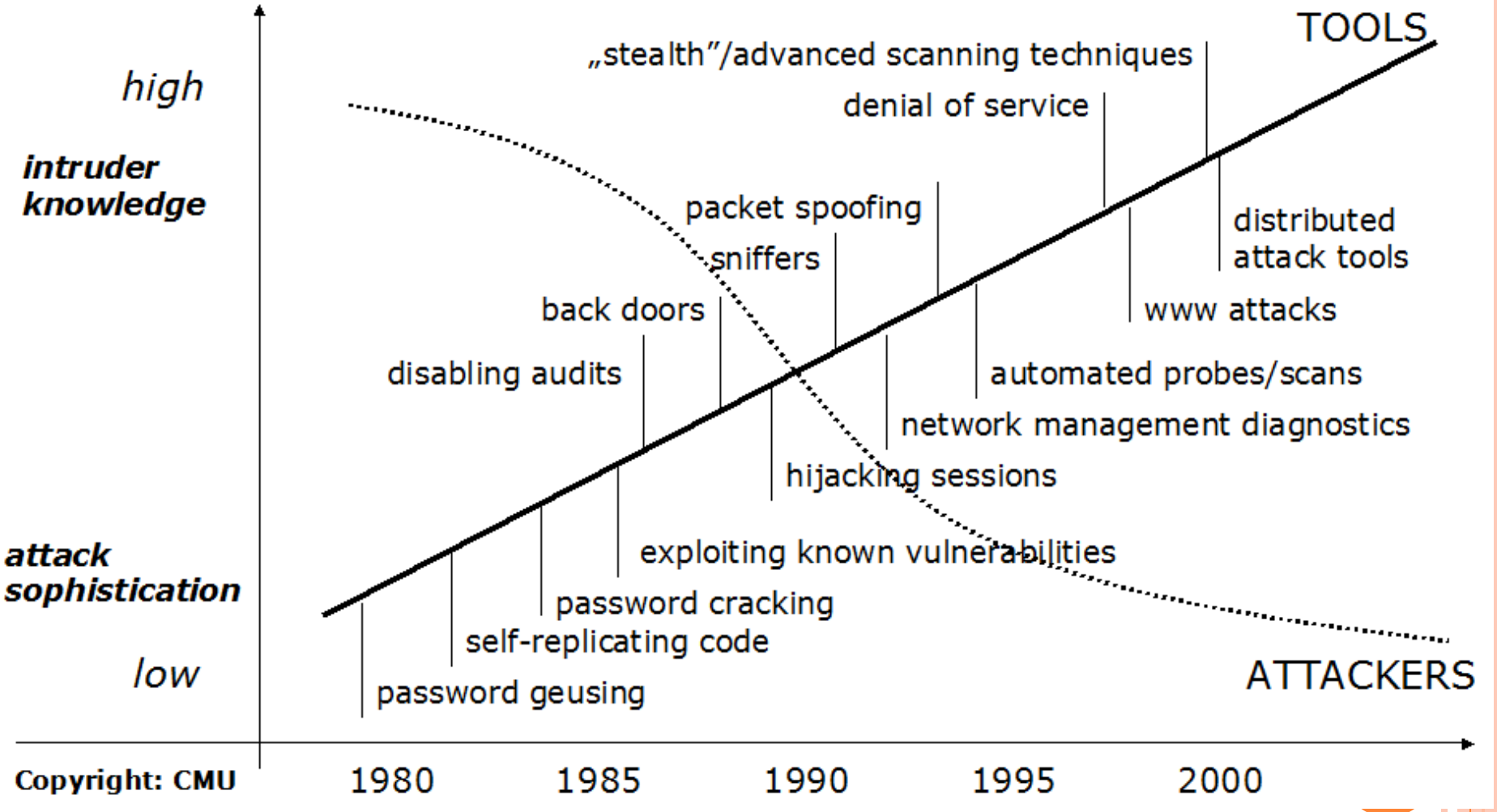
poważniejsze wypadki oszustw, sabotażu, a także szpiegostwa gospodarczego z wykorzystaniem

Rozwój PC-tów, masowe zjawisko sporządzania pirackich kopii programów

rozwinięcie sieci bankomatów ➔ nadużycia za pomocą kart magnetycznych

Zorganizowane grupy przestępcze, zarówno kryminalne, jak i gospodarcze; Dalszy rozwój technologiczny

Złożoność ataków a wiedza atakujących



Dla hakera narzędzi jest wiele

EWOLUCJA ZAGROŻEŃ

źródło: Symantec

BEZPIECZEŃSTWO

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

BEZPIECZEŃSTWO INFORMACJI
AGNIESZKA NOWAK - BRZEZIŃSKA

Bezpieczeństwo

Bezpieczeństwo jest to stan systemu informatycznego, w którym poziom ryzyka jego aplikacji jest zredukowany do akceptowalnego poziomu, poprzez zastosowanie odpowiednich środków

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Bezpieczeństwo teleinformatyczne

Bezpieczeństwem teleinformatycznym nazywamy wszystkie zagadnienia związane z bezpieczeństwem systemów i sieci teleinformatycznych w których wytwarzane, przetwarzane, przechowywane lub przesyłane są informacje

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Czego oczekujemy

- Prywatność (poufność) danych
  - Alicja wysyła wiadomość do Pawła. Kuba przechwytuje ją … ale nie może jej odczytać
- Integralność danych
  - Alicja wysyła wiadomość do Pawła, Kuba przechwytuje i zmienia wiadomość … ale Paweł może to sprawdzić
- Użyteczność systemów i danych
  - Alicja musi podać 100 haseł do systemu zanim będzie go mogła użyć
  - Aby pobrać plik podaj 25-te hasło ☺

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Co należy zapewnić

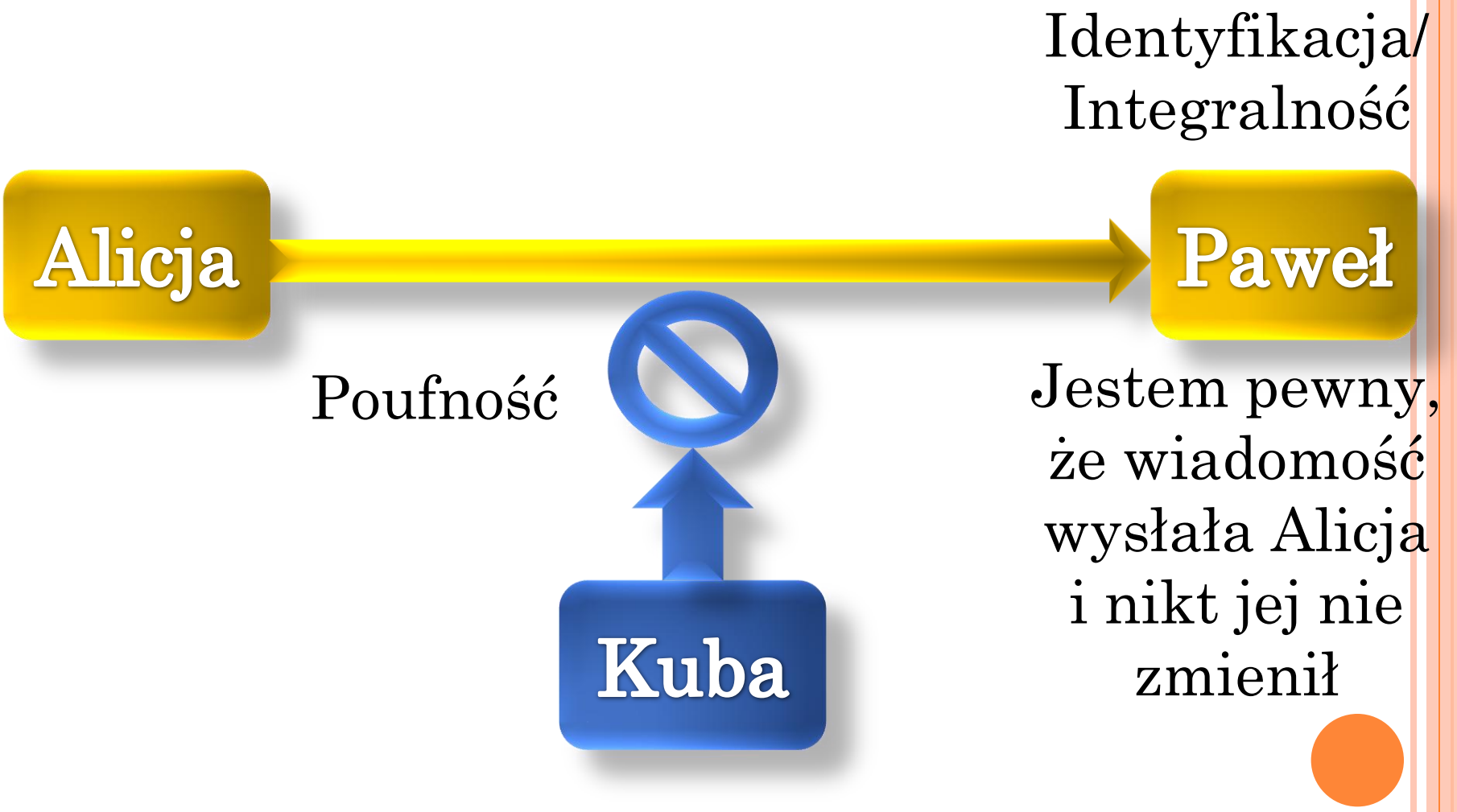
- Identyfikacja – kim jest użytkownik
  - Cześć nazywam się Kubuś Puchatek
  - Udowodnij to!
- Autoryzacja – kto może co zrobić
  - Uzbroić głowice nuklearne!
  - …?
- Niezaprzeczalność – kto jest autorem, kto i kiedy ktoś wysłał/otrzymał
  - Nigdy nie wysłałem tego maila
  - Nigdy nie otrzymałem tego maila

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Schemat działania!



METODY ZAPEWNIENIA POUFNOŚCI

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

BEZPIECZEŃSTWO INFORMACJI
AGNIESZKA NOWAK - BRZEZIŃSKA

Metody zapewnienia poufności

- Steganografia
  - Ukrycie faktu istnienia wiadomości
  - z greckiego steganos+ graphein przykryte (ukryte) pismo
- Kryptografia
  - Konwersja wiadomości do formatu, który dla osób postronnych jest nieczytelny
  - z greckiego kryptos + graphein => ukryte pismo

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Steganografia

STEGANOGRAFIA - PRZYKŁAD

- Fishing freshwater bends and saltwater coasts rewards anyone feeling stressed. Resourceful anglers usually find masterful leapers fun and admit swordfish rank overwhelming anyday.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

STEGANOGRAFIA - PRZYKŁAD

- Fishing freshwater bends and saltwater coasts rewards anyone feeling stressed. Resourceful anglers usually find masterful leapers fun and admit swordfish rank overwhelming anyday.

- **Send lawyers, guns, and money.**

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Inne metody steganografii

- II wojna światowa – mikrokropki
- Mleko lub cytryna
- Ukrywanie wiadomości w plikach graficznych – wykorzystywanie najmniej znaczących wartości kolorów
- Ukrywanie wiadomości w plikach dźwiękowych

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

- Można wysłać list zawierający na pierwszy rzut oka cytat z Koranu, a w rzeczywistości wezwanie do świętej wojny - z dumą tłumaczył dziennikarzowi "USA Today" przedstawiciel Hezbollahu. Jak ukryć tajemny przekaz w niewinnym obrazku?
- Wrześniowy atak terrorystyczny na budynki World Trade Center był możliwy między innymi dzięki zastosowaniu przez terrorystów nowoczesnych technologii powszechnie dostępnych w internecie, takich jak steganografia - ukrywanie wiadomości tekstowych w plikach zawierających obrazy i dźwięk.
- Zaczerpnięty z greki termin "steganografia" można przetłumaczyć jako "ukryte pismo". Choć steganografia znana jest od wielu stuleci, to powszechnie dostępna i popularna stała się dopiero od kilku lat. Dlaczego? Bo pojawiły się również jej współczesne odmiany wykorzystujące technologie cyfrowe, niezwykle trudne do wykrycia i łatwe do zastosowania.
- Amerykańskie służby specjalne są przekonane, że terroryści używają różnych zaawansowanych metod kryptograficznych już od ponad pięciu lat. Co najmniej trzech złapanych w ostatnich latach terrorystów używało komputerów i miało na nich zaszyfrowane pliki dotyczące zamachów na różne cele na całym świecie.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

- Steganografia polega na ukryciu informacji tak, aby ktoś, kto przechwyci wiadomość, nie wiedział o istnieniu zaszyfrowanego przekazu. Ponad 5 tys. lat temu w starożytnym Egipcie i Chinach w powszechnym użyciu było pisanie tzw. atramentem sympatycznym - cieczą, której ślad pokazuje się na papierze dopiero po wykonaniu pewnych ściśle określonych czynności, np. po ogrzaniu lub potraktowaniu papieru specyficznym odczynnikiem chemicznym. Jako atrament sympatyczny można wykorzystać wiele związków organicznych - chociażby niektóre soki owocowe (szczególnie popularna jest cytryna) lub mleko.

- Niektóre metody naprawdę zaskakują pomysłowością. Oto w niemieckiej gazecie ukazuje się ogłoszenie z życzeniami dla cioci Helgi od kochających siostrzeńców. Przeciętny czytelnik sądzi, że to normalne życzenia. Prawdziwe informacje z tych pozornie nic nieznaczących życzeń potrafili odczytać agenci, łącząc ze sobą np. pierwsze litery każdego ze słów. W efekcie otrzymywali informacje o terminie czy miejscu zrzutu lub kontaktu z innymi agentami.
- Powszechny strach przed użyciem przez wroga różnych metod stenograficznych wywoływał zarówno dawniej, jak i dziś kuriozalne reakcje władz cywilnych i wojskowych. W czasie wojny cenzura wojskowa żądała zakazu publikacji krzyżówek, gdyż mogły one stanowić doskonały sposób ukrycia przekazu. W Związku Radzieckim i Stanach Zjednoczonych dokładnie przeglądano listy, a nawet naklejone na nich znaczki pocztowe.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Instrukcje dla uśpionych

- Powszechną cechą współczesnej steganografii jest wykorzystanie publicznych, ogólnodostępnych mediów do przesłania wiadomości. Dzisiejszy szpiedzy czy terroryści nie przenoszą już wiadomości na wytatuowanych głowach. Rzadko też drukują ogłoszenia w gazetach. Zwykle przekazują informacje za pomocą ogólnie dostępnych mediów - takich jak np. radio, telewizja czy internet. Stąd zaniepokojenie amerykańskich służb specjalnych wypowiedziami Osamy ben Ladena, które publikowała katarska telewizja, a za nią wszystkie główne dzienniki na świecie. Specjaliści obawiali się, że Osama w swoim płomiennym przemówieniu może używać metod steganograficznych do instruowania uśpionych na całym świecie agentów al Kaidy (choć nie było na to dowodów).
- Ben Ladena i jego organizację już przed zamachami podejrzewano o wykorzystywanie zaawansowanych metod szpiegowskich. Na początku roku amerykański tygodnik Time przedstawił artykuł, w którym powołując się na źródła wywiadowcze, dowodzono o stosowaniu przez przyjaciół ben Ladena steganografii w internecie.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

TAKIE SAME, A JEDNAK INNE

- Sieć wydaje się idealnym wprost narzędziem dla szpiegów. Miliony anonimowych internautów, niezliczona ilość informacji, strony WWW, które pojawiają się i za chwilę znikają - wszystko to tworzy chaos, w którym nikt nigdy nie będzie w stanie znaleźć ukrytej wiadomości.
- Szybko pojawiła się też cyfrowa forma znanego od tysięcy lat atramentu sympatycznego. Dziś już nikt nie będzie bazgrał cytryną po kartce papieru. Współcześni wykorzystają do ukrycia wiadomości nowoczesne oprogramowanie, które pozwala wpleść dowolną treść do cyfrowego zdjęcia. Wystarczy później taką fotografię umieścić na stronie internetowej poświęconej np. naszej ostatniej wycieczce w Tatry Najbardziej nawet spostrzegawcze osoby nie odkryją ukrytej treści.
- Dlaczego? Bo wiadomość zakodowana jest w bardzo subtelnych różnicach barwy poszczególnych punktów (pikseli) obrazu. A punktów jest mnóstwo. Obraz 410x270 pikseli, taki jak w galerii fotograficznej portalu Gazeta.pl, to ponad 110 tys. punktów. Jeśli zmienimy po jednym bicie każdego punktu, to mamy miejsce na 13 tys. znaków. Tak właśnie działają programy steganograficzne - ukrywają wiadomość, zmieniając po jednym bicie każdego punktu obrazu. W praktyce punkt ten staje się "nieco" mniej czerwony, zielony czy niebieski, co jest niezauważalne dla oglądającego obraz na ekranie.
- Stosując tę technikę, można wręcz w dowolnym zdjęciu ukryć inne, mniejsze zdjęcie, tekst czy jakąkolwiek zapisaną w postaci elektronicznej informację - teoretycznie nawet wirusa. Podobną metodą ukryjemy informacje w plikach dźwiękowych czy wideo!

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

TERROR W OBRAZKACH

- Pierwsze informacje sugerujące używanie przez terrorystów steganografii w internecie pojawiły się na początku bieżącego roku. Od tego momentu Niels Provos i Peter Honeyman z Uniwersytetu stanu Michigan rozpoczęli prace, których celem jest przeszukanie internetu, znalezienie i rozszyfrowanie plików graficznych zawierających ukryte wiadomości. Przedsięwzięcie podzielono na dwa etapy:
- Przeszukanie stron WWW pod kątem obrazków,
- Przeszukanie grup dyskusyjnych.

Przeszukuje się strony WWW, gdyż w nich bowiem najprawdopodobniej terroryści ukrywają steganograficzne obrazki. Najwięcej obrazków zawierających ukryte informacje znaleziono na serwerze aukcyjnym eBay. Co prawda nie jest pewne, czy ich autorami są terroryści. Jest to jednak dowód na to, że praktycznie można w ten sposób przesyłać informacje. Swoistym testem możliwości systemu stworzonego przed dwóch naukowców był eksperyment przeprowadzony przez telewizję ABC. Na stronach jej serwisu internetowego przedstawiono grafikę komputerową z ukrytym zdjęciem samolotów B-52. Stworzony przez Nielsa Provosa program do wykrywania steganograficznych obrazów potrzebował zaledwie jednej sekundy, aby zidentyfikować grafikę, w której ukryto zdjęcie, rozszyfrować ją i "wydobyć" sam obraz.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Listing 1: Kodowanie kolejnych bitów w pikselach obrazu

```
for m_bit in message_bits:
    pos = pix[random.randint(0, len(pix)-1)]
    pix.remove(pos)
    cr, cc = pos/img.width, pos - (pos/img.width)*img.width
    img[cr, cc] = (img[cr, cc] & 0xFE) + m_bit
```

Rysunek 1: Ilustracja skali zmian wprowadzonych przez ukrycie wiadomości w obrazie. Od lewej: obraz oryginalny, obraz zmieniony, ilustracja miejsc zmian.

- Obecnie obaj naukowcy skupili się na drugim etapie prac, czyli przeszukiwaniu plików w grupach dyskusyjnych USENET. Szczególnie skrupulatnie sprawdzono popularne grupy poświęcone problematyce seksu (podobnie jest w przypadku zdjęć na stronach WWW). Według cytowanych przez dziennik "USA Today" ekspertów amerykańskich terroryści najczęściej przekazują sobie instrukcje przez internet, wykorzystując popularne czaty sportowe lub strony pornograficzne. Przedstawiciele radykalnych organizacji islamskich wcale zresztą nie kryją się z tym, że stosują nowoczesne metody szyfrowania informacji - w tym przede wszystkim steganografię.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

W dużym powiększeniu kolory sąsiednich pikseli mają zupełnie różne kolory, ale oko nie potrafi tego rozróżnić. To zjawisko jest wykorzystywane w steganografii. Inną metodą ukrywania danych w tekście jest zastępowanie pojedynczych liter. W najprostszej wersji, pochodzącej z "ery przedkomputerowej", wystarczyło znaleźć w tekście np. wszystkie litery "k" i podnieść je trochę do góry, aby zaznaczyć jedynkę, a pozostawić na miejscu dla oznaczenia zera. Metoda ta jest podobna do poprzedniej, ale kontener ma większą pojemność - maks. ok. 4 procent, w zależności od wybranej litery i użytego alfabetu, a co za tym idzie częstotliwości występowania tego znaku.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

http://www.spychecker.com/program/stools.html

Darmowy program S-Tools pozwala na ukrywanie informacji w polikach dźwiękowych i graficznych, zabezpieczając je dodatkowo jednym z 4 popularnych algorytmów szyfrujących. Wiadomo, że jeden obraz mówi tyle, co sto słów. W steganografii jest jeszcze lepiej - nawet w małym zdjęciu można ukryć całą książkę.

Umożliwia on ukrycie danych w plikach graficznych i dźwiękowych. Tajnym przekazem może być tekst, obraz i dźwięk. Dzięki temu możliwe jest np. ukrycie w pliku dźwiękowym obrazu, który z kolei zawiera tajny tekst.

Program działa na zasadzie opisanej w poprzednich akapitach, z dwoma ulepszeniami: ukrywane dane są zabezpieczane hasłem i szyfrowane, a wybrane do celów steganograficznych próbki lub piksele są rozrzucane mniej lub bardziej chaotycznie po całym pliku.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Każdy użytkownik komputera mniej więcej orientuje się w strukturze plików graficznych. Są to zwykle bardzo długie ciągi danych, które zawierają dokładne informacje o każdym pikselu (punkcie) obrazu. W najczęściej wykorzystywanym modelu barwnym RGB dowolny kolor uzyskuje się poprzez mieszanie w odpowiednich proporcjach barw podstawowych, tj. czerwonego (Red), zielonego (Green) i niebieskiego (Blue). Każdy piksel musi być zatem opisany trzema wartościami, które określają nasycenie poszczególnych składowych barwnych. W kolorowych obrazkach, których pełno w Internecie, do zapisania każdej z tych wartości potrzeba 8 bitów, czyli jednego bajta. Jednemu pikselowi odpowiadają więc 24 bity - 3 bajty. Stąd już łatwo obliczyć, że typowe, nieskompresowane zdjęcie z taniego cyfrowego kompaktu o rozdzielczości 5 megapikseli stanowi kontener liczący sobie (w zaokrągleniu) 15 MB, czyli 120 milionów bitów.

W jaki sposób dane są ukrywane? Wykorzystywana jest ułomność ludzkiego wzroku - na 24 bitach możemy opisać aż 16 milionów kolorów, podczas gdy odróżniamy ich jedynie kilkadziesiąt tysięcy. Na przykład, jeden z odcieni niebieskiego opisany jest zestawem liczb 78, 131, 244 (binarnie: 01001110 10000011 11110100). Zmieniając pierwszą składową z 78 (01001110) na 79 (01001111) możemy ukryć jeden bit informacji bez widocznej zmiany na zdjęciu - dużo większe szumy niż jeden bit powodują przypadkowe błędy powstałe w trakcie wykonywania zdjęcia. Aby się o tym przekonać, wystarczy zrobić zbliżenie zdjęcia jednolitej powierzchni, np. czystego nieba i pobrać wartości dwóch sąsiednich pikseli - różnica będzie na co najmniej kilku bitach, a i tak jest dla nas niezauważalna.

I tak tego nie widać...

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Dane możemy też ukryć w plikach dźwiękowych. Nieskompresowane formaty, takie jak np. WAV pozwalają na uzyskanie prawie 19-procentowej pojemności kontenera. Zasada pozostaje ta sama: dla każdej próbki sygnału dźwiękowego zastępujemy najmniej znaczące bity tajną informacją. Zwykle jedna próbka składa się z 16 bitów, a bezpieczną ilością podmienianych danych są 3 bity. Warto dodać, że dla konkretnych rodzajów dźwięku (np. rozmowa, dźwięki ulicy) wartość tę można znacznie zwiększyć.

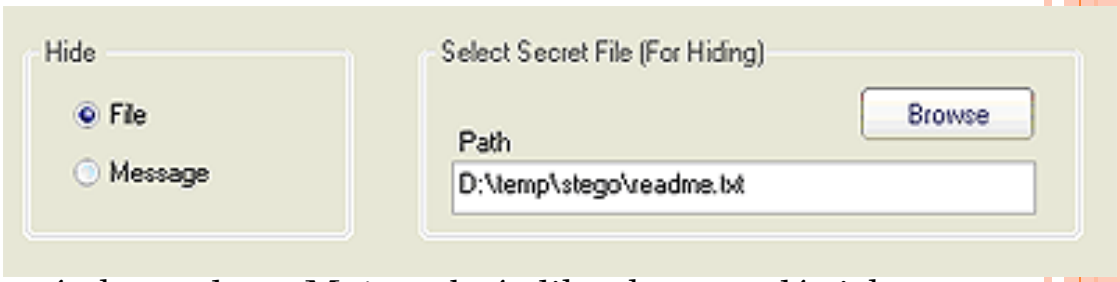
Wydaje się, że pojemność dźwięku jest mniejsza niż obrazu, ale nie zawsze jest to prawdą. 19% to pojemność jednej próbki, których liczba wynosi zazwyczaj ponad 44 tysiące na sekundę. Pozwala to na umieszczenie 1 MB danych w audycji trwającej ledwo minutę. Sygnał dźwiękowy ma dodatkowo tę zaletę, że może być nadawany przez radio i odbierany (analogowo) przez urządzenia czulsze niż ludzki słuch, które są w stanie wychwycić niesłyszalne dla nas zmiany na niższych bitach.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

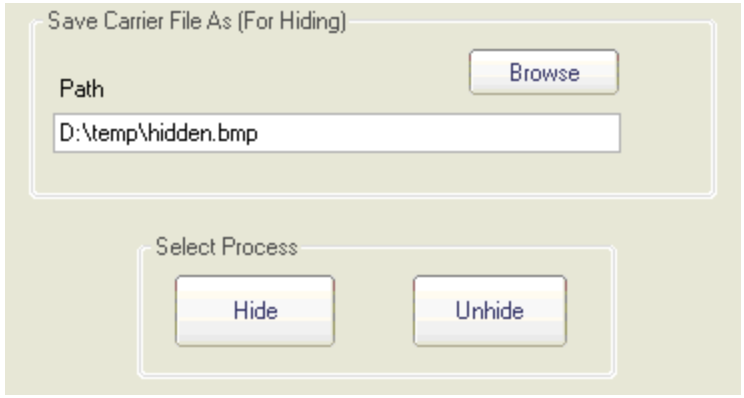
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

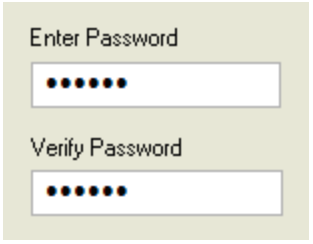
Na początek wybieramy czy chcemy ukryć plik czy wiadomość oraz podajemy ścieżkę w przypadku pliku:



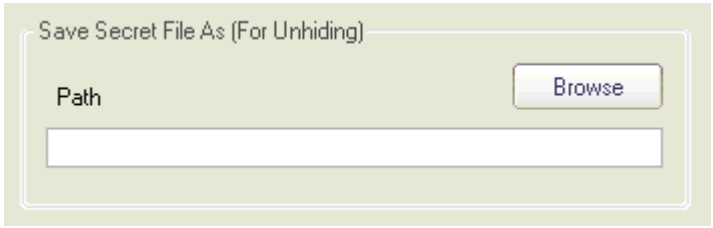
Następnie określamy plik, w którym mają zostać ukryte dane. Może to być plik tekstowy, dźwiękowy (tylko WAV) lub grafika (tylko w formacie BMP).

Podajemy hasło dostępu do ukrytych danych:Na koniec określamy gdzie i pod jaką nazwą zapisany będzie plik wynikowy oraz klikamy *Hide*.





Procedura jest niemalże identyczna w przypadku wydobywania ukrytej informacji z pliku, z tą tylko różnicą, że podajemy ścieżkę zapisu dla pliku ukrytego



StegoMagic 1.0

http://programy.onet.pl/74,50,11107,programy.html

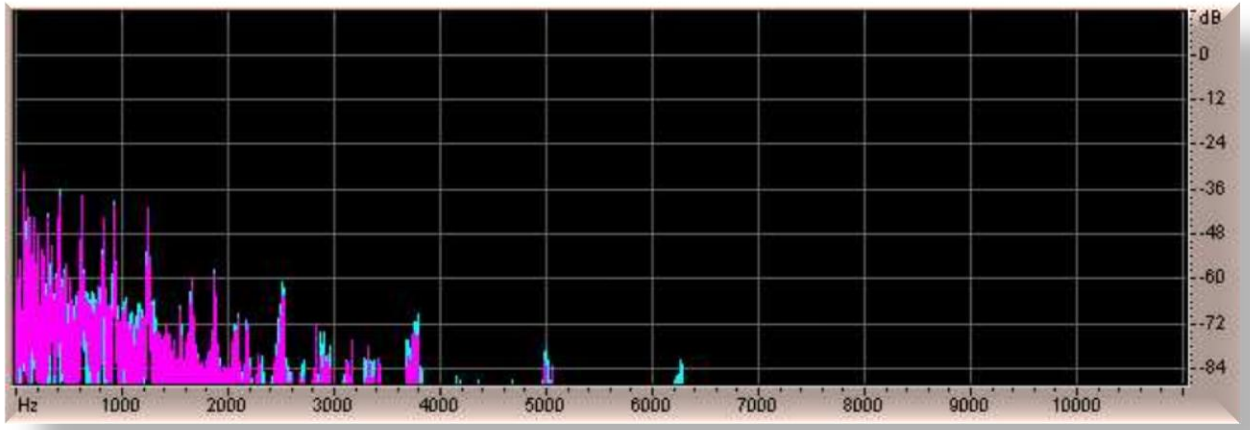
KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

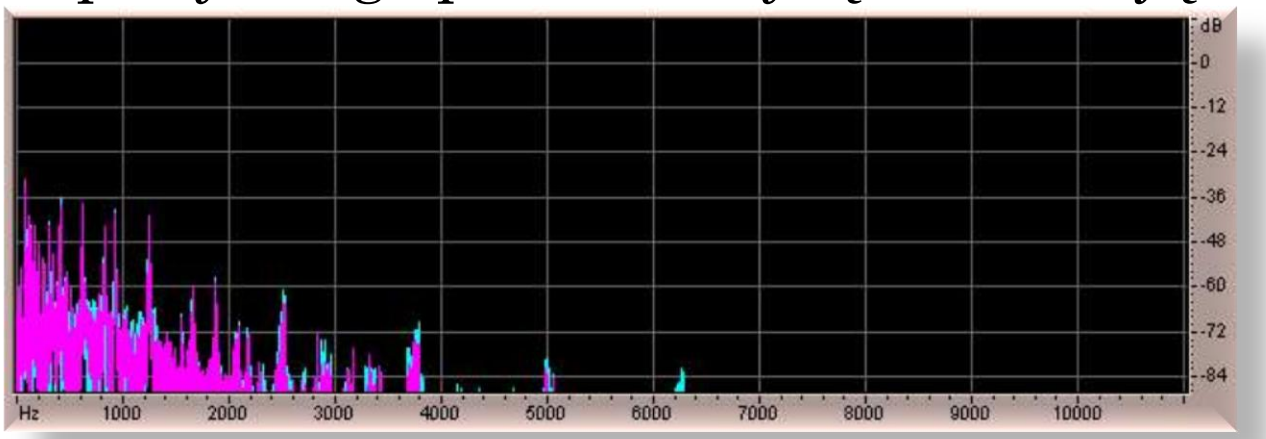
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Charakterystyki częstotliwościowe

dla pliku oryginalnego 44kHz/16bit



dla powyższego pliku z ukrytą informacją



Źródło: Analiza i implementacja metod steganograficznych w plikach ultimedialnych (audio) Dariusz Kosicki

Co z bezpieczeństwem?

Aby sposób zapisu danych został uznany za bezpieczny, muszą być spełnione następujące warunki: poufność, dostępność i integralność informacji. Niestety, steganografia nie spełnia tego ostatniego warunku. Dane są ukrywane w postaci niezaszyfrowanej, a to oznacza, że możliwe jest ich przechwycenie, sfałszowanie i ponowne umieszczenie w kontenerze bez pozostawienia jakiegokolwiek śladu. Innymi słowy, **nie ma żadnej gwarancji, że to co odczytujesz jest tym co zostało ukryte i nie ma możliwości, żeby to sprawdzić**. Oczywiście nic nie stoi na przeszkodzie, aby ukrywany tekst poddać uprzednio szyfrowaniu i tak się zwykle robi. Wymienione wyżej oprogramowanie wręcz zmusza użytkownika do zaszyfrowania przekazu jednym z kilku popularnych algorytmów.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Kryptografia pojęcia

- Tekst jawny (plain text) – tekst, który będzie podlegał szyfrowaniu
- Tekst zaszyfrowany (szyfrogram) – tekst będący wynikiem szyfrowania
- Szyfrowanie – proces zmiany tekstu jawnego na tekst zaszyfrowany
- Deszyfrowanie – proces odwrotny do szyfrowania, w wyniku którego otrzymujemy tekst jawny
- Algorytm kryptograficzny – funkcja użyta do szyfrowania
- Klucz jest ciągiem bitów użytym w metodzie

Algorytmy kryptograficzne

- Przestawieniowe - polegające na zmianie porządku znaków według pewnego schematu, tzw. Figury
- Podstawieniowe - polegające na zamianie bitów, znaków lub ciągów znaków ich odpowiednimi zamiennikami
- Symetryczne – (z kluczem prywatnym)
- Asymetryczne – (z kluczem publicznym)

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Przykład szyfru przestawieniowego

- Przestawienie kolumnowe

Przykład.
tekst jawny: KRYPTOGRAFIA
macierz: 3x4
klucz: 2-4-1-3

1	2	3	4
K	R	Y	P
T	O	G	R
A	F	I	A

tekst zaszyfrowany:
ROFPRAKTAYGI

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Przykład szyfru podstawieniowego

- Szyfr Cezara – każda litera tekstu jawnego jest zamieniana w inną literę z przesunięciem 3 (czyli A=D, B=E,… X=A, Y=B, Z=C)

Przykład

tekst jawny: KRYPTOGRAFIA

tekst zaszyfrowany: NUBSWRJUDILD

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Szyfrowanie kluczem symetrycznym (Symmetric Key Encryption)

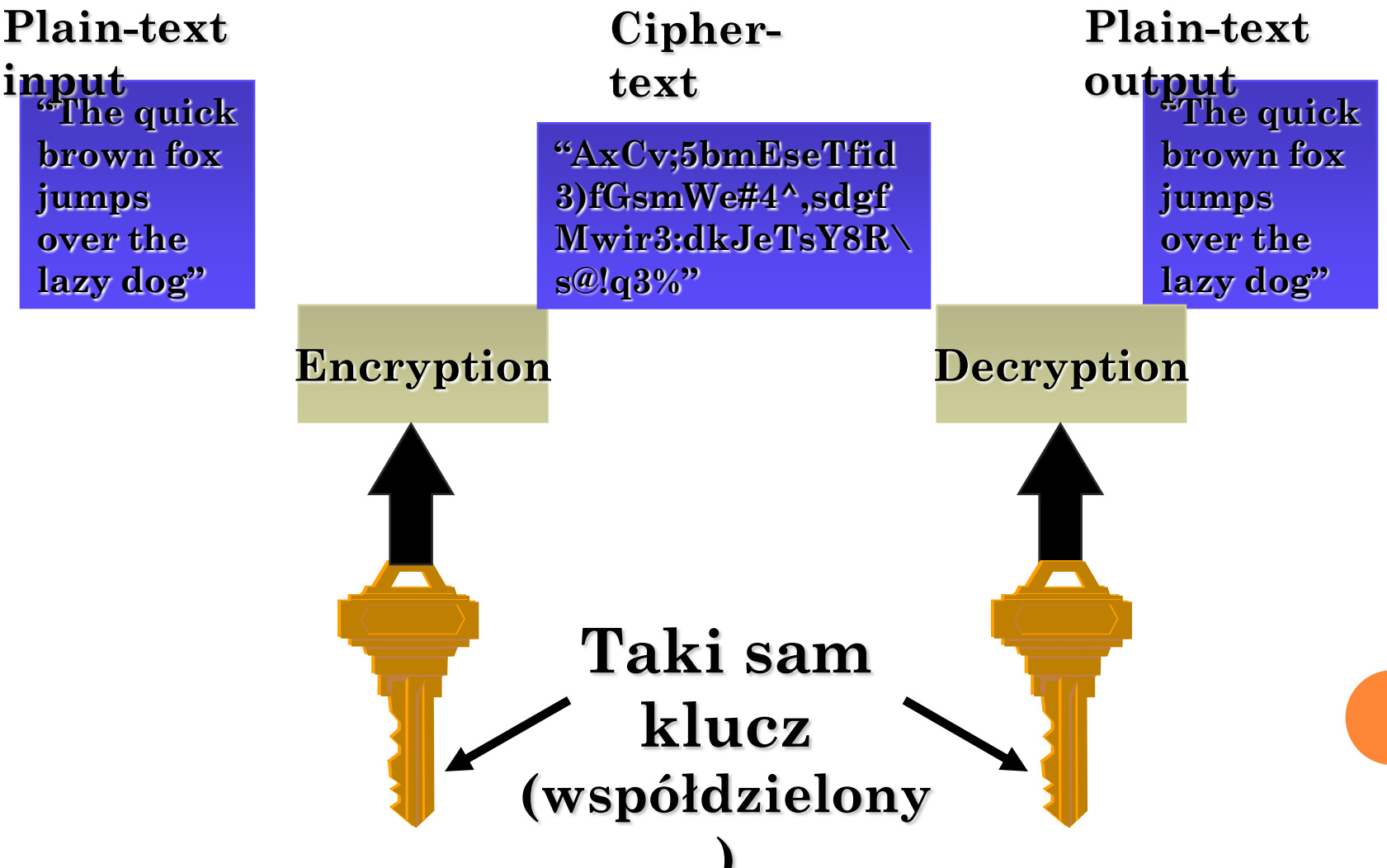
- Obie strony używają jednego klucza do kodowania i odkodowania
- Kiedy osoba A wysyła wiadomość do B
- A koduje kluczem K, B odkodowuje tym samym kluczem
- Kiedy osoba B wysyła wiadomość do A
- B koduje kluczem K, A odkodowuje tym samym kluczem
- Wystarczająco szybkie nawet dla długich wiadomości

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Kryptografia symetryczna



Kryptografia symetryczna

- Zalety:
  - stosunkowo mały kod programu implementującego algorytm
  - duża szybkość pracy (rzędu dziesiątków megabajtów na sekundę), dobra wydajność (możliwość implementacji w układach scalonych)
- Wady
  - wymianę danych musi poprzedzić przekazanie klucza, które powinno odbyć się niezależną, bezpieczną drogą
  - wyjątkowo uciążliwe jest nawiązanie bezpiecznej komunikacji z nieznanym partnerem
  - stosunkowo proste złamanie szyfru

łności związane z rozbudową usługi

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
projektu Rozwój Wyższego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Szyfrowanie asymetryczne

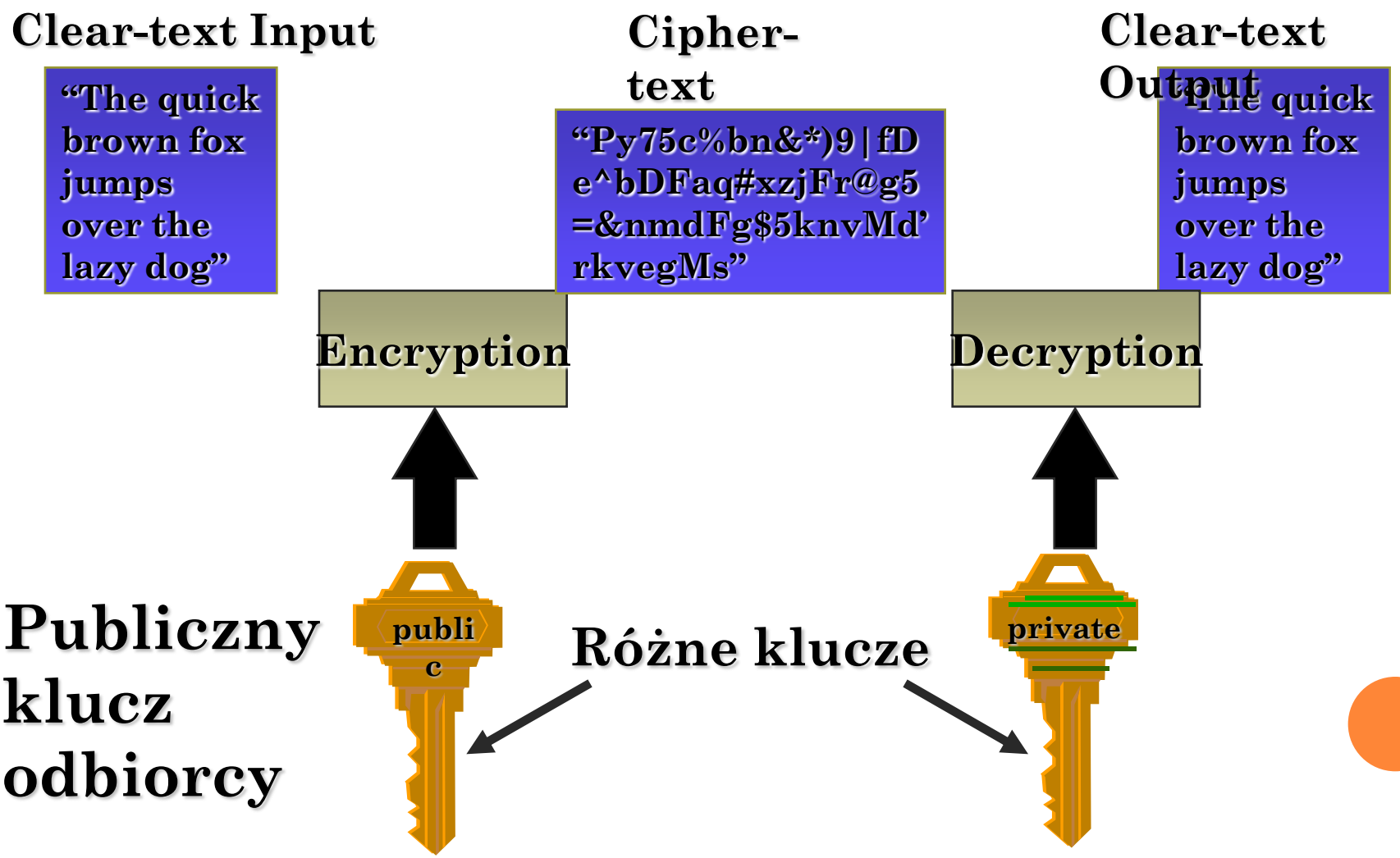
- Wiedza o kluczu szyfrującym nie pozwala (?) odgadnąć klucza odszyfrowującego
- Odbiorca informacji generuje parę kluczy
  - klucz publiczny – publikuje
  - klucz prywatny jest kluczem tajnym
- Zatem każdy może przysyłać jemu zaszyfrowane dane

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Szyfrowanie asymetryczne



Szyfrowanie asymetryczne

- Różne klucze do kodowania i odkodowania
  - Szyfrowanie za pomocą klucza publicznego odbiorcy
  - Deszyfrowanie za pomocą klucza prywatnego odbiorcy
  - Po zdekodowaniu nadawca nie może odkodować szyfru nie ma prywatnego klucza odbiorcy
- Każdy ma klucz prywatny i publiczny
  - Klucz prywatny powinien być zabezpieczony
  - Klucz publiczny może zostać rozpowszechniony dla wszystkich
- Wtedy każdy może zakodować wiadomość do odbiorcy przy użyciu klucza publicznego
- Ale tylko odbiorca może odczytać wiadomość

Szyfrowanie asymetryczne

- Potrzeba 4 kluczy dla komunikacji w dwie strony
  - Każda ze stron posiada klucz prywatny i klucz publiczny
  - Każdy wysyła klucz publiczny do innych niekodowany
  - Szyfrowanie odbywa się kluczem publicznym drugiej strony
  - Deszyfracja odbywa się za pomocą klucza prywatnego
  - Nigdy nie należy odwoływać się do klucza publicznego lub prywatnego, bez informacji do kogo należy ten klucz
- Nie ma potrzeby na generowanie osobnych kluczy dla każdego z partnerów
  - Uproszczenie zarządzania kluczami

Wady

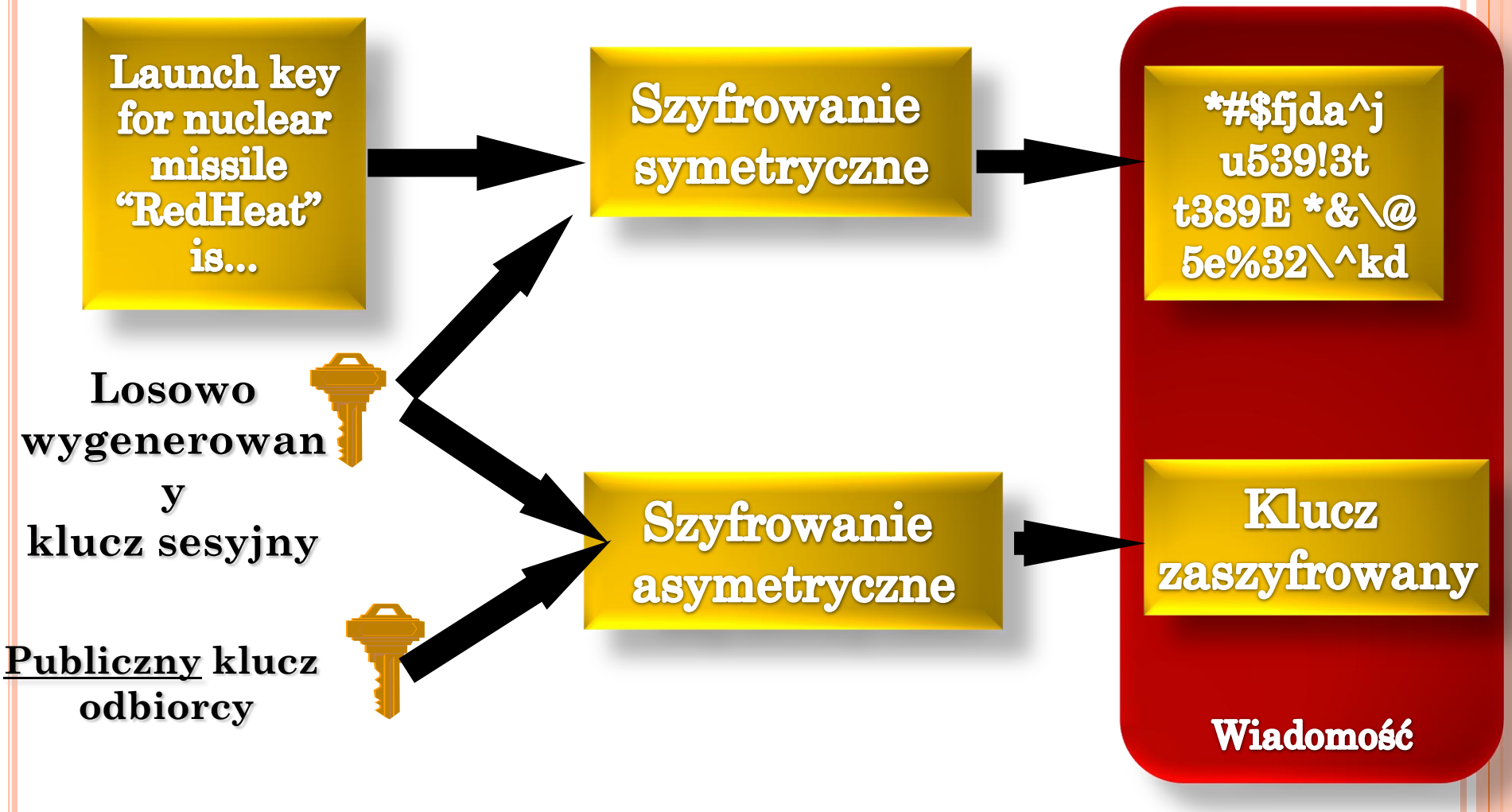
- Niestety metody są bardzo wolne
  - 100 razy wolniejsze od kodowania symetrycznego
  - można zakodować tylko krótkie wiadomości

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Połączenie szyfrowania symetrycznego i asymetrycznego



Podpis cyfrowy

- Zapewnia potwierdzenie autorstwa wiadomości
- Umożliwia sprawdzenie integralności wiadomości

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Podpis cyfrowy

- Przed wysłaniem wiadomości nadawca tworzy skrót wiadomości (message digest) – krótki ciąg binarny obliczony na podstawie wszystkich bitów w wiadomości

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Podpis cyfrowy

- Sposób tworzenia skrótu wiadomości
  - Użycie procesu zwanego haszowaniem (hashing)
  - Dla wiadomości dowolnej długości, algorytm dzieli ją na mniejsze fragmenty o jednakowej długości (MDA: 128 bitów, SHA-1:160 bit)
- Haszowanie
  - Nie ma operacji odwrotnej
  - Nie można odtworzyć wiadomości oryginalnej na podstawie jej haszu
  - Używane w celu zmniejszenia ilości informacji dla kodowania asymetrycznego

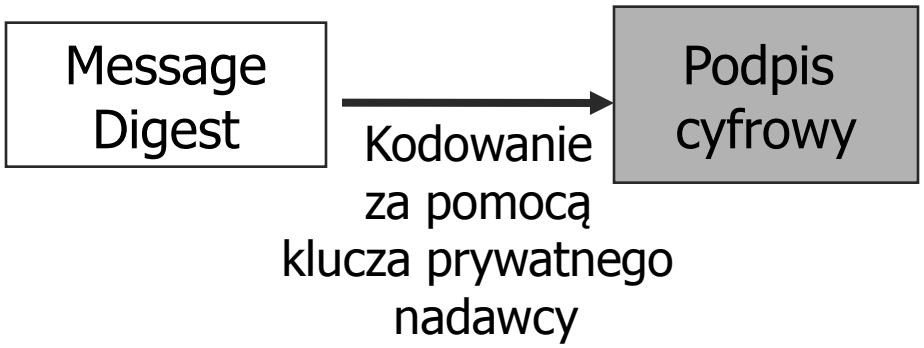
KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Podpis cyfrowy

- Następnie ze skrótu wiadomości tworzony jest podpis cyfrowy
  - Kodowanie skrótu wiadomości prywatnym kluczem nadawcy, co może zrobić jedynie posiadacz tego klucza
  - Skrót wiadomości jest krótki, więc kodowanie asymetrycznie nie jest problemem



Podpis cyfrowy

- Następnie algorytm łączy podpis z wiadomością i tak przygotowaną wiadomość nadawca może wysłać

- Odbiorca rozdziela wiadomość i podpis
- Dekoduje podpis kluczem publicznym nadawcy – otrzymuje prawdziwy skrót wiadomości
- Następnie tworzy skrót wiadomości, tak, jak nadawca
- Porównuje skrót otrzymany z przesłanym

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Problem z podpisem

- Podszywanie się pod osobę
  - Osoba prawdziwa ma klucz prywatny i publiczny, ale
  - Osoba udająca ma je również
- Osoba udająca wysyła klucz publiczny do weryfikacji (krytyczny krok!)
- Jeśli osoba weryfikująca zaakceptuje ten klucz PROBLEM!!!
- Wniosek
  - Kodowanie ma sens tylko gdy istnieje 3 zaufana strona i ona podpisuje (autoryzuje) prawdziwość klucza

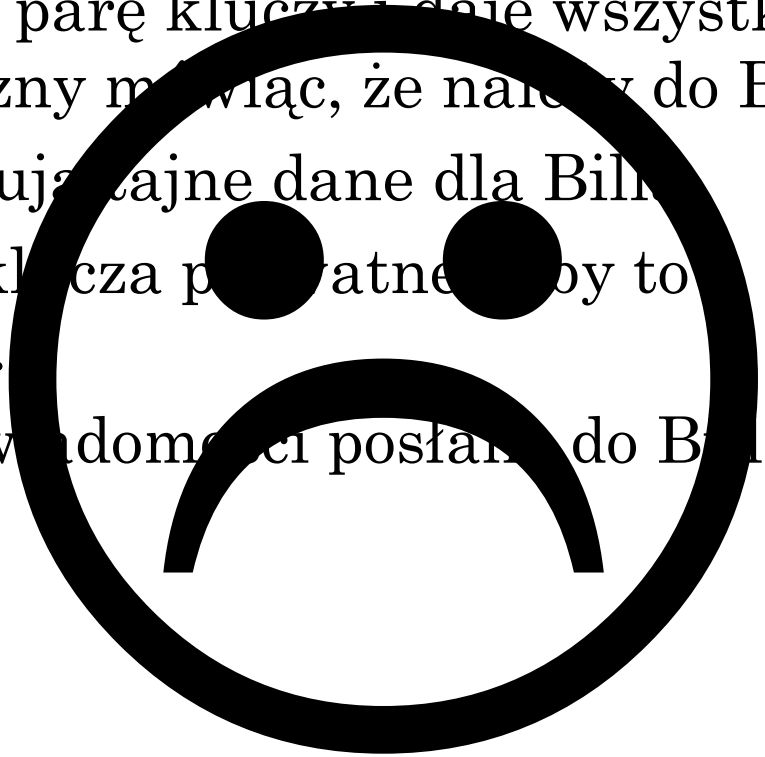
KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Przykład

- Scott tworzy parę kluczy i daje wszystkim swój klucz publiczny mówiąc, że należy do Billa
- Ludzie szyfrują tajne dane dla Billa
- Bill nie ma klucza prywatnego aby to odszyfrować.
- Scott czyta wiadomości posłane do Billa



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Algorytm Luhna

Jeden z najczęściej wykorzystywanych algorytmów służących do sprawdzania poprawności wpisania danej liczby. Jest on używany m.in. do walidacji numerów kart kredytowych, ciągów liczbowych, itd. Nazwa algorytmu pochodzi od nazwiska niemieckiego naukowca Hansa Petera Luhna (1896–1964).

Na końcu liczby doklejana jest cyfra kontrolna określająca, czy poprzedzający ją ciąg cyfr jest wpisany poprawnie.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

- Algorytm ten wygląda następująco:
- Dla każdej pozycji cyfry określone zostają wagi (mnożniki). Najczęściej jest to 2 dla pozycji nieparzystych, 1 dla parzystych.
- Każdą cyfrę liczby mnożymy przez odpowiadającą jej wagę.
- Jeśli w wyniku mnożenia otrzymamy liczbę dwucyfrową, dodajemy cyfry do siebie otrzymując liczbę jednocyfrową.
- Dodajemy wszystkie otrzymane liczby do siebie.
- Wykonujemy operację mod 10 na otrzymanej sumie (pozostawiamy jedynie cyfrę jedności).
- Następnie, jeśli otrzymana cyfra nie równa się 0, odejmujemy ją od 10. Otrzymujemy cyfrę kontrolną, która jest "doklejana" do liczby.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Przykład

- Mamy liczbę 92480.
- Wykonujemy mnożenie przez odpowiednie wagi:
- $9 \cdot 2 = 18$
- $2 \cdot 1 = 2$
- $4 \cdot 2 = 8$
- $8 \cdot 1 = 8$
- $0 \cdot 2 = 0$
- Cyfry liczby 18 (jako dwucyfrowej) dodajemy do siebie, otrzymując 9.
- Otrzymane liczby dodajemy do siebie: $9 + 2 + 8 + 8 + 0 = 27$.
- Wykonujemy operację mod 10: $27 \bmod 10 = 7$.
- $7 <> 0$, więc wykonujemy operację $10 - 7 = 3$.
- Cyfrę kontrolną 3 "doklejamy" do liczby, otrzymując 924803

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Szyfrowanie – nr PESEL

Dla numeru PESEL algorytm obliczenia cyfry kontrolnej przebiega następująco: każdej z pozycji cyfr numeru nadany został stały współczynnik zwany wagą pozycji. Każdą cyfrę numeru mnoży się przez odpowiednią wagę i sumuje się wynik mnożenia. Otrzymany wynik dzieli się modulo 10 i odejmuje od 10

Jak łatwo zauważyć odjęcie wyniku od 10 nic w zasadzie nie zmienia ale widocznie twórcy systemu PESEL (Powszechy Elektroniczny System Ewidencji Ludności) dostali rozkaz (*a były to lata siedemdziesiąte*) aby trochę utrudnić rozszyfrowanie tego systemu zachodnim szpiegom **:-)**.
Ale z doniesień czytelnika tej strony wynika, że cały system PESEL, chyba nawet z komputerami, był kupiony od Szwedów, więc o tajemnicy nie ma mowy. **:-(**
Ale ... w Szwecji *personnummer*, odpowiednik numeru PESEL ma tylko 10 cyfr, cyfrę kontrolną oblicza się według metody Luhn'a, algorytmu, w którym mnożnikami są przemiennie 1 i 2. Wspólnymi cechami z systemem szwedzkim są: sześciocyfrowy zapis daty urodzenia, oznaczenie płci w numerze i położenie cyfry kontrolnej na końcu numeru.

CIEKAWOSTKI W KODOWANIU NUMERU PESEL

- Dwie pierwsze cyfry oznaczają ostatnie dwie cyfry w roku urodzenia. Dla przykładu osoba urodzona w roku 1966 ma w numerze PESEL 66mmddxxxxk.
- Cyfra trzecia i czwarta oznaczają miesiąc urodzenia.
- Ale jeśli dana osoba urodziła się przed rokiem 1900, ale po roku 1800 to do liczby miesiąca dodaje się 80. Dla przykładu: osoba urodzona 1 grudnia 1898 ma numer PESEL 989201xxxxk
- Osoby urodzone w roku 2000 i później będą miały powiększony numer miesiąca o liczbę 20. Dla przykładu osoba urodzona 1 grudnia 2000 będzie miała numer PESEL 003201xxxxk
- Cyfry piąta i szósta oznaczają dzień urodzenia.
- W cyfrach siódmej, ósmej, dziewiątej i dziesiątej zakodowany jest numer seryjny :-) danego osobnika.
- W dziesiątej cyfrze PESEL zakodowana jest jednocześnie płeć osoby: nieparzysta oznacza mężczyznę, a parzysta kobietę. Ciekawostka: w wielu podobnych do PESELa numerów nadawanych w krajach europejskich nieparzysta cyfra oznacza mężczyznę a parzysta kobietę.
- W jedenastej jest oczywiście słynna cyfra kontrolna.
- Na razie brak danych do rozkodowania innych informacji tam zawartych. Nie wiadomo, na przykład, co decyduje czy dana kobieta jako kod płci dostanie 0, 2, 4, 6 czy 8. . . . badania trwają

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

W JAKI SPOSÓB TWORZY SIĘ NUMER PESEL?

Numer PESEL jest to 11–cyfrowy, stały symbol numeryczny, jednoznacznie identyfikujący określoną osobę fizyczną. Jego postać przedstawia rysunek

0	4	0	5	1	4	0	1	4	5	8
1	2	3	4	5	6	7	8	9	10	11

gdzie:

- na pozycji 1-2 umieszczone są dwie ostatnie cyfry roku urodzenia,
- na pozycji 3-4 umieszczone są dwie cyfry miesiąca urodzenia,
- na pozycji 5-6 umieszczone są dwie cyfry dnia urodzenia,
- na pozycji 7-10 umieszczony jest liczba porządkowa z oznaczeniem płci,
- na pozycji 11 umieszczona jest liczba kontrolna.

- **Sposób obliczania liczby kontrolnej w numerze ewidencyjnym PESEL**

1. każdą pozycję numeru PESEL mnoży się przez odpowiednią wagę: 1-3-7-9-1-3-7-9-1-3;
2. utworzone iloczyny sumuje się (przy tradycyjnym obliczaniu liczby kontrolnej stosowanie „modulo 10" nie wymaga dodawania pełnych iloczynów wchodzących w skład sumy, lecz tylko ostatnich jego cyfr, co jest oczywistym ułatwieniem, szczególnie przy „wyższych" wagach);
3. wartość ostatniej otrzymanej liczby należy odjąć od 10 (dopełnienie 10); wynik odejmowania stanowi liczbę kontrolną danego numeru PESEL.

Np.: numer PESEL ma postać: 0207080362 – dotyczy więc osoby urodzonej 8 lipca 1902 roku, płci żeńskiej (parzysta końcówka numeru z serii – 0362).
Obliczenie liczby kontrolnej:
1.
0207080362
x 1379137913
0603040766

http://www.pko.pl/f/pesel.htm

2. 0+6+0+3+0+4+0+7+6+6=32

3. 10-2=8
Liczba kontrolna=8

Pełny numer PESEL ma więc postać: 02070803628

Przykład dla numeru PESEL 49040501580

1 3 7 9 1 3 7 9 1 3 --> wagi

X X X X X X X X X X Y --> cyfry nr PESEL (Y- cyfra kontrolna)

czyli:

1 3 7 9 1 3 7 9 1 3

* 4 9 0 4 0 5 0 1 5 8

---

suma=(1*4+3*9+7*0+9*4+1*0+3*5+7*0+9*1+1*5+3*8)=

=(4+ 27+ 0+ 36+ 0+ 15+ 0+ 9+ 5+ 24)= 120

120 mod 10 = 0

10 - 0 = 10 ----> cyfra kontrolna ?

korekta: dla wyniku 10 ----> cyfra kontrolna = 0

Uzyskany wynik jest cyfrą kontrolną numeru, który w naszym przypadku ma postać: 49040501580 i dotyczy kobiety urodzonej: 5 kwietnia 1949 roku. W przypadku wprowadzenia błędnego numeru PESEL, komputer po obliczeniu cyfry kontrolnej może ten błąd wykryć, gdyż np: jeśli pomylimy się i zamiast 49040501580 podamy 46040501580 to otrzymamy:

1 3 7 9 1 3 7 9 1 3

* 4 6 0 4 0 5 0 1 5 8

---

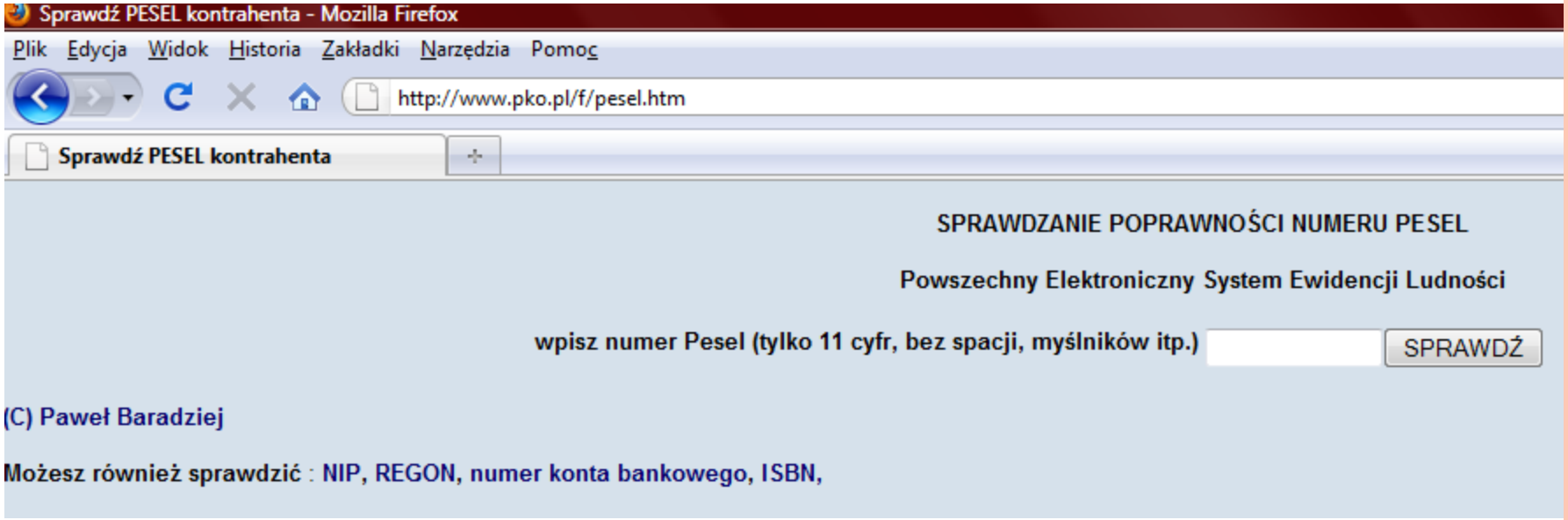
suma=(1*4+3*6+7*0+9*4+1*0+3*5+7*0+9*1+1*5+3*8)=

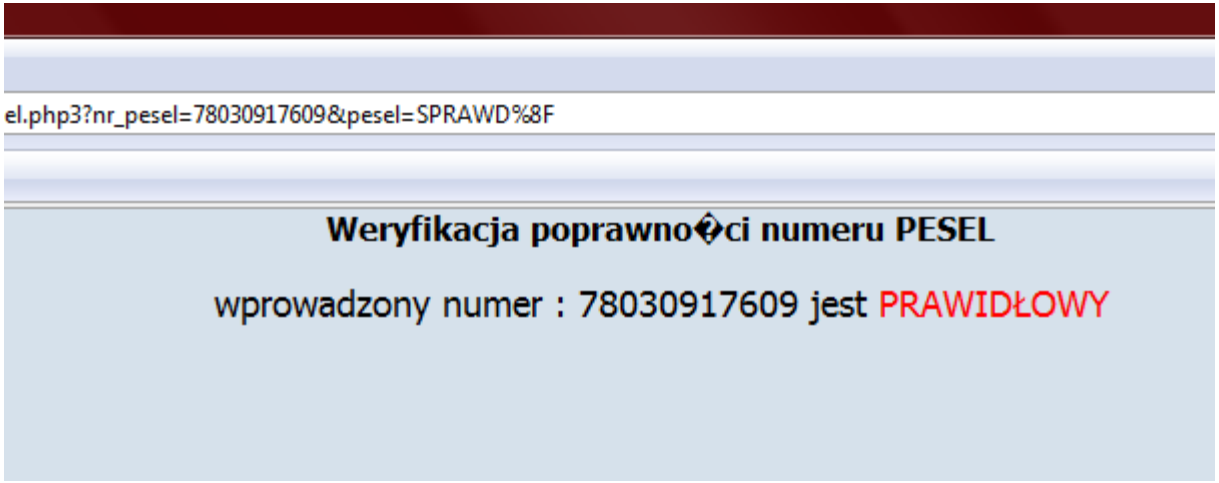
=(4+ 18+ 0+ 36+ 0+ 15+ 0+ 9+ 5+ 24)= 111

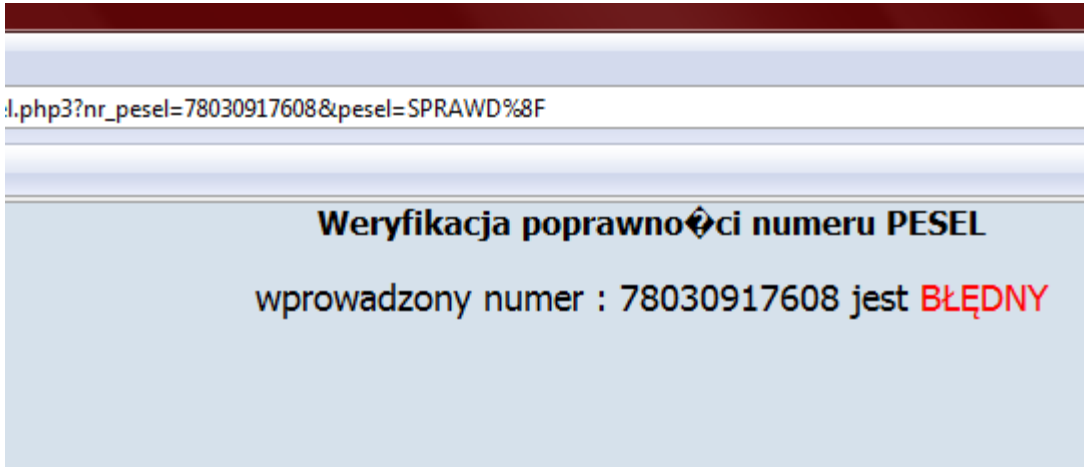
111 mod 10 = 1

10 - 1 = 9

Obliczona cyfra kontrolna to 9, podczas gdy prawidłowa cyfra to 0. Oczywiście może nastąpić przypadek błędnego wprowadzenia także ostatniej cyfry.
W tym przykładzie łatwo sie pomylić gdyż na formularzu drukowanym na drukarce igłowej cyfra 0 jest podobna do cyfry 8. Wtedy algorytm przepuści błędne dane.


Sprawdź PESEL kontrahenta - Mozilla Firefox
Plik Edycja Widok Historia Zakładki Narzędzia Pomoc
http://www.pko.pl/f/pesel.htm
Sprawdź PESEL kontrahenta
SPRAWDZANIE POPRAWNOŚCI NUMERU PESEL
Powszechny Elektroniczny System Ewidencji Ludności
wpisz numer Pesel (tylko 11 cyfr, bez spacji, myślników itp.)
SPRAWDŹ
(C) Paweł Baradziej
Możesz również sprawdzić : NIP, REGON, numer konta bankowego, ISBN,


el.php3?nr_pesel=78030917609&pesel=SPRAWD%8F
Weryfikacja poprawno&#65533;ci numeru PESEL
wprowadzony numer : 78030917609 jest PRAWIDŁOWY



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Przedmiot prowadzony w zakresie
Projektu UPGOW współfinansowanego
Przez Unię Europejską w ramach
Europejskiego Funduszu Społecznego

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Liczba kontrolna i sprawdzanie poprawności numeru

- Jedenasta cyfra jest cyfrą kontrolną, służącą do wychwytywania przekłamań numeru. Jest ona generowana na podstawie pierwszych dziesięciu cyfr. Aby sprawdzić czy dany PESEL jest prawidłowy należy, zakładając, że litery *a*-*k* to kolejne cyfry numeru od lewej, obliczyć wyrażenie
- a + 3*b + 7*c + 9*d + e + 3*f + 7*g + 9*h + i + 3*j + k
- Jeśli otrzymany wynik nie jest podzielny przez *10*, to znaczy, że numer zawiera błąd.
- Przykład dla numeru PESEL 44051401358:
- 4*1 + 4*3 + 0*7 + 5*9 + 1*1 + 4*3 + 0*7 + 1*9 + 3*1 + 5*3 + 8 = 109
- Liczba 109 nie jest podzielna przez *10*, więc numer zawiera błąd.