Komputery, Internet, Sztuczna Inteligencja — zagrożenia nowoczesnej technologii

Witold Paluszyński
Instytut Cybernetyki Technicznej
Politechniki Wrocławskiej
Witold.Paluszynski@ict.pwr.wroc.pl

Internet

Powstał w latach 80-tych XX wieku jako sieć komputerowa łącząca największe amerykańskie uniwersytety, ośrodki badawcze, oraz ośrodki wojskowe. Internet powstał na bazie ARPANET-u, czyli sieci stworzonej przez wojsko i na potrzeby wojska amerykańskiego.

Znaczenia ogólnoświatowej sieci wymiany informacji zaczął nabierać od początku lat 90-tych, po wprowadzeniu standardu WWW, czyli udostępniania i wymiany informacji w formacie HTML, łączącym początkowo tekst z obrazami, a później z dźwiękiem, i obrazami ruchomymi, czyli filmem, animacjami, dynamicznie generowaną grafiką, itp.

Obecnie trudno wyobrazić sobie świat bez Internetu, a przecież Internet nadal intensywnie się rozwija, i nabiera coraz większego znaczenia w życiu codziennym. Czy to jest dobra wiadomość? Czy powinniśmy się cieszyć akceptując coraz szybsze i bardziej przepustowe łącza komunikacyjne, coraz potężniejsze i tańsze komputery, coraz więcej możliwości załatwienia różnych spraw przez Internet, takich jak: zakupy, rozrywka, czyli dostępność muzyki, filmów, i gier, oraz nauka, i praca?

Jasne, że TAK!!

Ale nie do końca!

Przecież w naszym skomputeryzowanym świecie zdarzają się pomyłki, błędy, i wypadki, a także nadużycia, oszustwa, i kradzieże, spowodowane, i zawinione właśnie przez wykorzystanie komputerów i Internetu. Przyjrzyjmy się różnym schematom oszustw bankowych.

Karty kredytowe

Obiektem zainteresowania oszustów i złodziei internetowych są karty kredytowe i płatnicze, ponieważ zapewniają one dostęp do posiadanych przez ludzi pieniędzy, podobnie jak obiektem zainteresowania oszustów i złodziei tradycyjnych są portfele i sejfy, ponieważ w nich przechowywane są (coraz rzadziej) pieniądze w formie gotówkowej.

„Phishing” czyli złodzieje wybierają się na ryby

Złodzieje i oszuści internetowi stosują szeroki asortyment wymyślnych forteli, żeby wydobyć od użytkowników Internetu numery i dane ich kart kredytowych, ale nie tylko, również inne cenne informacje takie jak: numery i dane kont bankowych, numery PESEL, nazwy kont internetowych i hasła, itp.

Wiele z tych sztuczek ma charakter pułapek z przynętą, które oszuści zastawiają na naiwnych użytkowników, i potem czekają aż coś, albo ktoś się w taką pułapkę złapie. Dlatego powstało w języku angielskim nowe słowo na określenie takich oszustw: *phishing* kojarzące się z łowieniem ryb (ang. *fishing*).

Najprostsza pułapka polega na przysłaniu klientowi banku, korzystającego z usług bankowych przez Internet, komunikatu e-mail proszącego go o podłączenie się do banku w celu:

- zaktualizowania swoich danych osobistych pod groźbą zablokowania konta
- skorzystania z promocji z losowaniem darmowego wyjazdu na Karaiby
- ...

W komunikacie zawarty jest odnośnik WWW, na który wystarczy kliknąć, aby uzyskać połączenie z serwerem bankowym. Jednak w rzeczywistości, zamiast połączyć się z bankiem, łączymy się z serwerem oszustów, który do złudzenia przypomina znaną nam i budzącą zaufanie witrynę banku.

To connect with Citibank click here: 

http://www.yahoo.com/anonim357/login.php

Najprostsza pułapka polega na przysłaniu klientowi banku, korzystającego z usług bankowych przez Internet, komunikatu e-mail proszącego go o podłączenie się do banku w celu:

- zaktualizowania swoich danych osobistych pod groźbą zablokowania konta
- skorzystania z promocji z losowaniem darmowego wyjazdu na Karaiby
- ...

W komunikacie zawarty jest odnośnik WWW, na który wystarczy kliknąć, aby uzyskać połączenie z serwerem bankowym. Jednak w rzeczywistości, zamiast połączyć się z bankiem, łączymy się z serwerem oszustów, który do złudzenia przypomina znaną nam i budzącą zaufanie witrynę banku.

To connect with Citibank click here: citi http://www.yahoo.com/anonim357/login.php

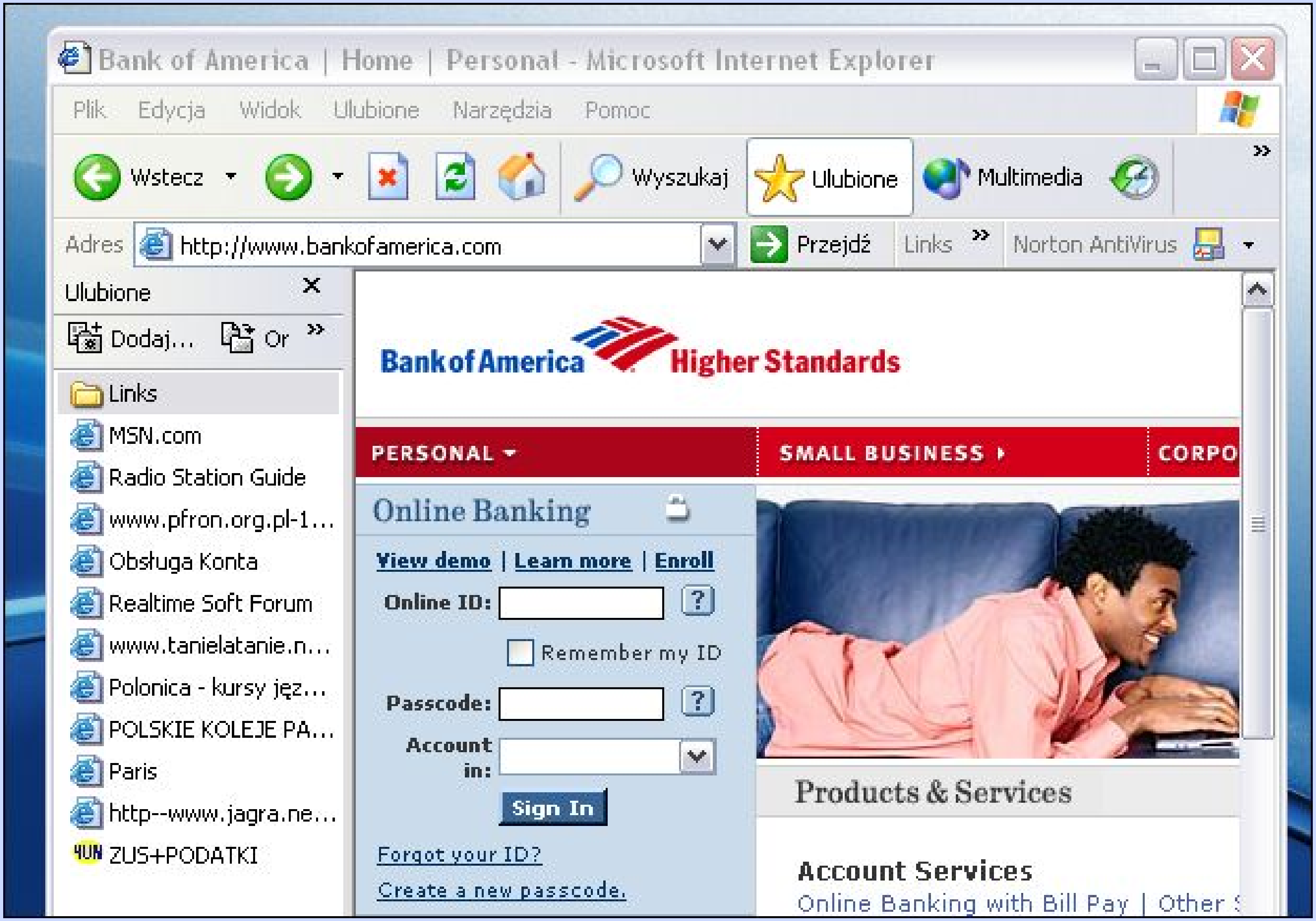
Kto złapie się na tak prymitywną przynętę?

http://www.bankofamerica.com zxhghw.zz/

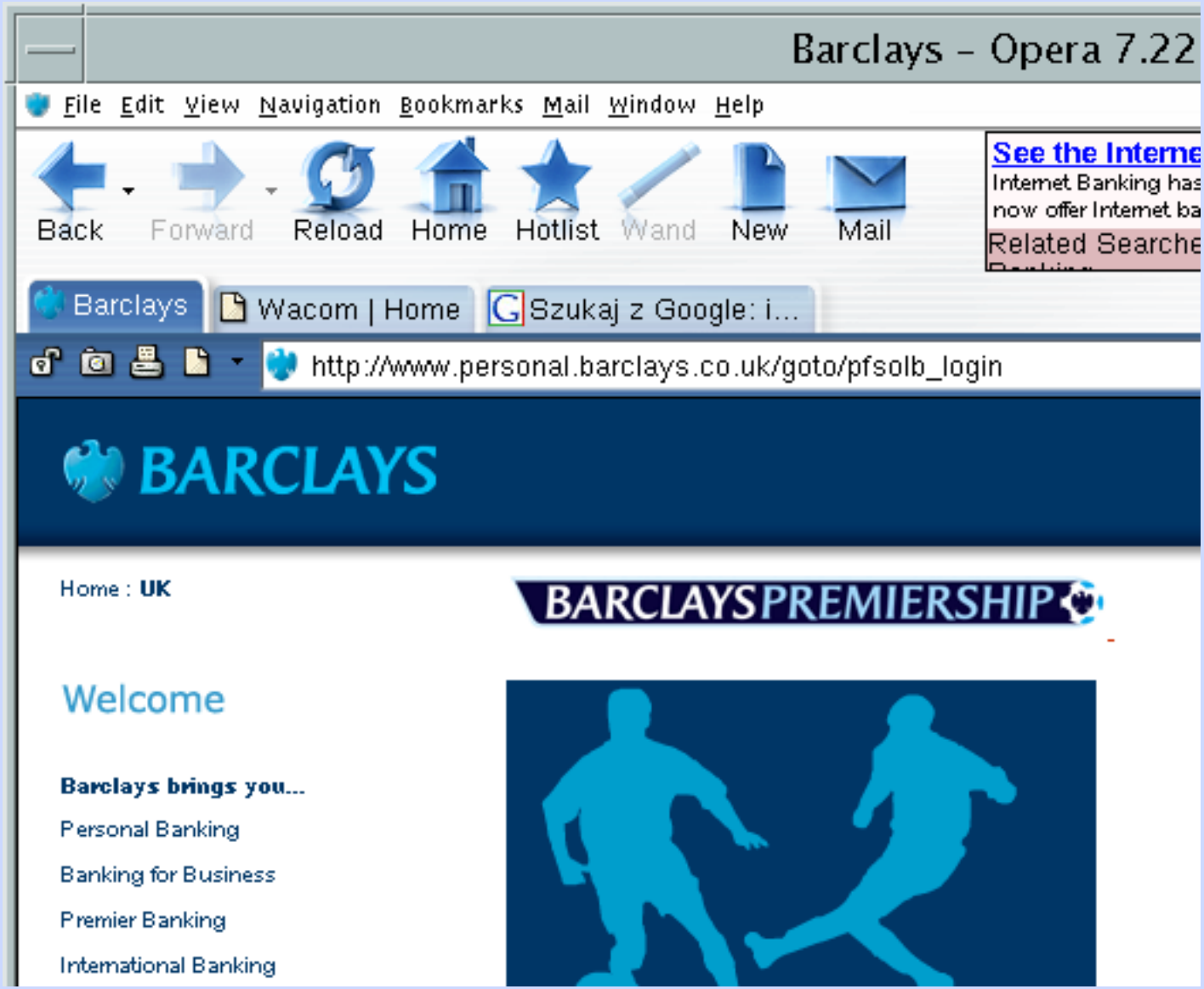
http://www.bankofamerica.com zxhghw.zz/

http://www.bankofamerica.com%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20zxhghw.zz/

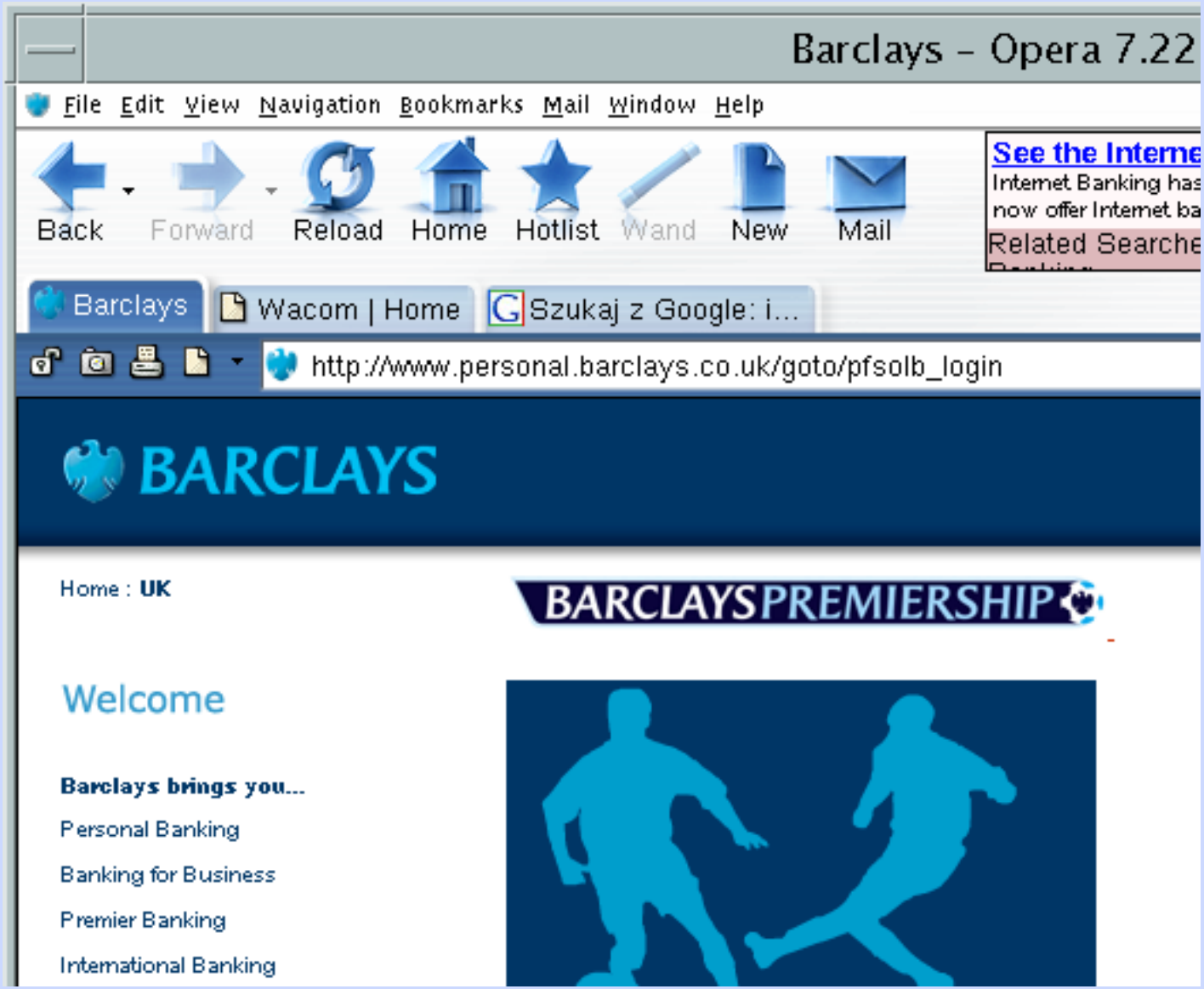
http://www.bankofamerica.com%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20zxhghw.zz/



http://www.personal.barclays.co.uk/goto/pfsolb_login



http://www.personal.barclays.co.uk/goto/pfsolb_login



http://www.personaI.barcIays.co.uk/goto/pfsoIb_Iogin

Jeszcze inny fortel stosowany przez oszustów polega na wykorzystaniu zwykłych błędów popełnianych przez ludzi. Wiedząc, że istnieje duży bank z witryną internetową o adresie **http://www.citibank.com/** złodzieje mogą stworzyć szereg identycznych witryn pod adresami:
http://www.ctibank.com/
http://www.citbank.com/
http://www.citybank.com/
http://www.cytibank.com/
http://www.vitibank.com/
i tak dalej, i wiedząc, że ludzie robią czasami pomyłki, spokojnie czekać aż jakaś rybka połknie haczyk.

Czy powinniśmy ograniczyć korzystanie z banków przez Internet i systemy komputerowe, czy raczej doprowadzić do opracowania lepszych i bezpieczniejszych sposobów z nich korzystania?

Odpowiedź wydaje się oczywista, bo czy ktoś chciałby wrócić do starych, bezpiecznych systemów bankowych, gdy wszelkie operacje finansowe wymagały osobistego kontaktu, i czekania w kolejkach przed kasami bankowymi?

Co więc możemy zrobić?

Wykorzystanie podpisu

Stosujemy go by potwierdzić, że transakcji dokonuje uprawniony klient banku, właściciel konta. Problem polega jednak na tym, że o ile złodziej ma utrudnione zadanie sfałszowania podpisu, to jednak gdy mu się uda, i zdobędzie sposób uwiarygodnienia transakcji wykradzionym podpisem prawowitego właściciela, to temu ostatniemu będzie niezwykle trudno udowodnić swoją rację, ponieważ dla banku to on właśnie dokonał transakcji, co potwierdza podpis.

Szyfrowanie

- zapewnia poufność przekazywanych informacji
- daje pewność, że komunikujemy się z właściwym partnerem, np. bankiem
- dzięki często zmienianym kluczom szyfrowania zabezpiecza przed „siłowym” łamaniem szyfru

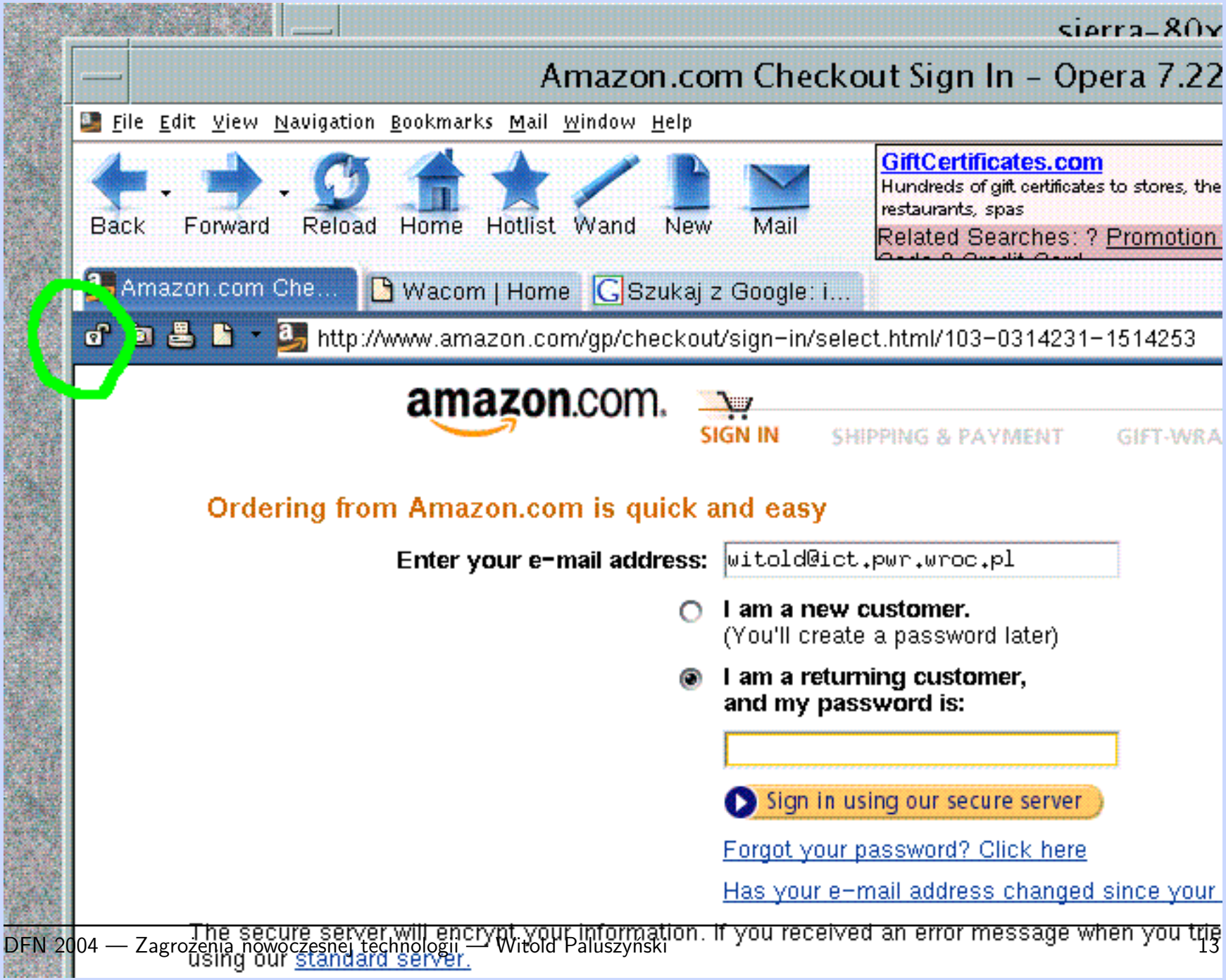
Podpis elektroniczny

+ pozwala na bezpieczne i skuteczne szyfrowanie przekazywanych elektronicznie informacji
+ pozwala na **uwierzytelnianie**, czyli potwierdzenie, że nadawcą przesyłki elektronicznej jest na pewno osoba posiadająca podpis elektroniczny
– musi być chroniony, ponieważ dostęp oszusta do podpisu elektronicznego daje mu wszystkie możliwości prawowitego posiadacza
– dla bezpieczeństwa musi być co jakiś czas wymieniany na nowy


SN: TT11719795
500MHz H61.4.1/128MB/CD48x

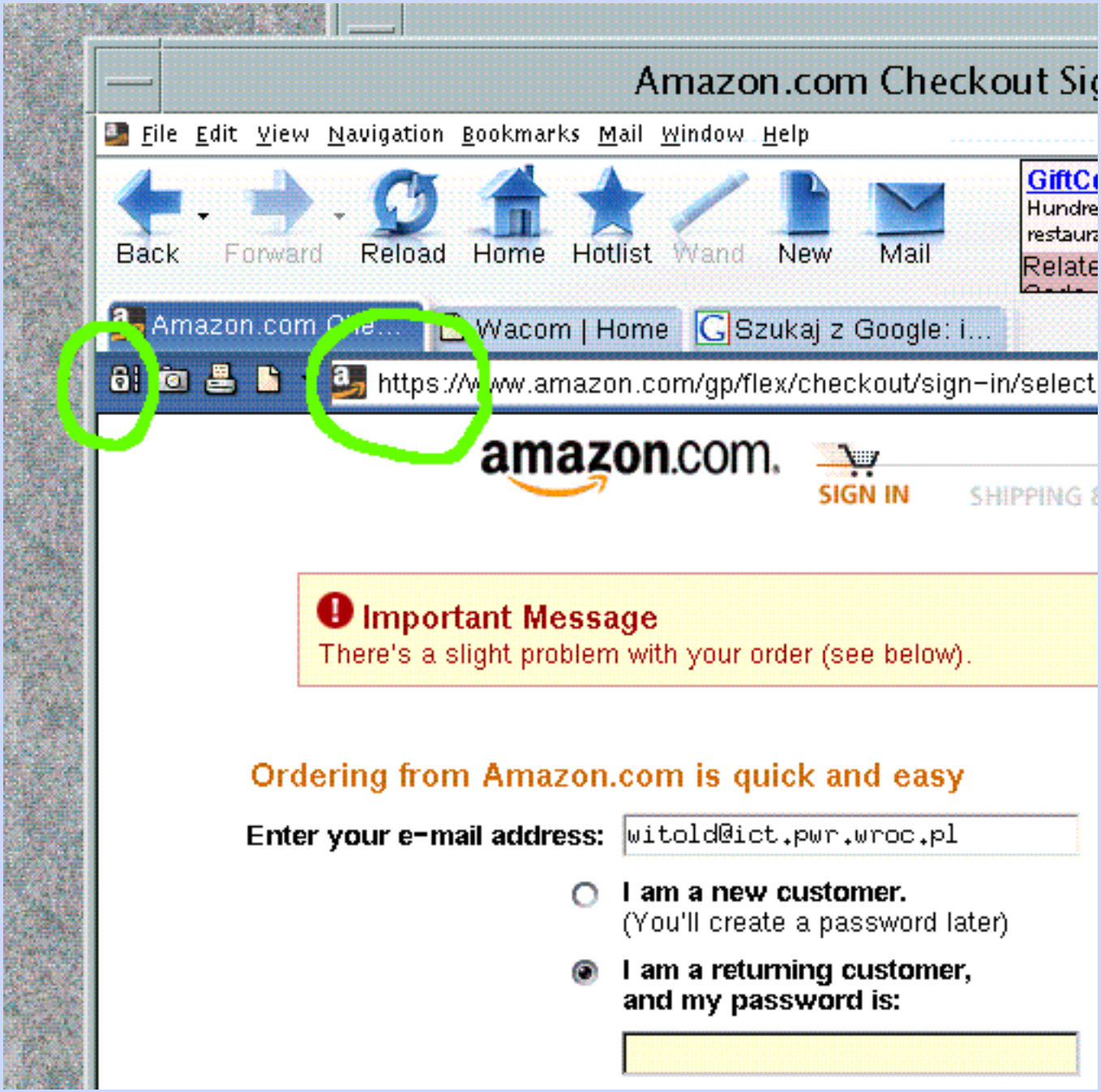

GEMPLUS
Sun
microsystems

Transakcje finansowe w Internecie



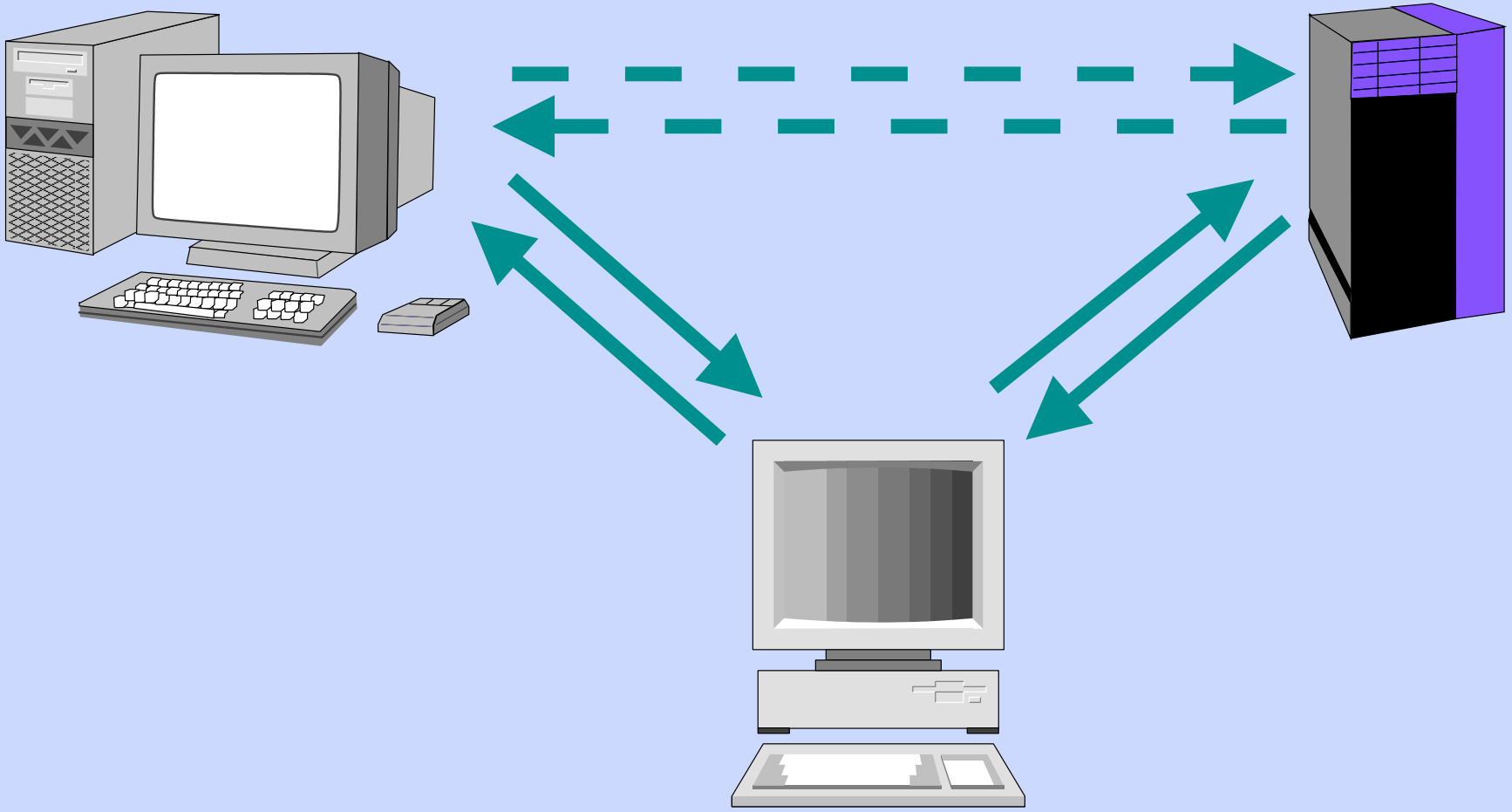
☺ Użycie protokołu https i symbol kłódki wyświetlany przez przeglądarki internetowe wskazują, że komunikacja ze zdalnym serwerem jest szyfrowana, i że nikt nie może przechwycić wpisywanych przez nas informacji.

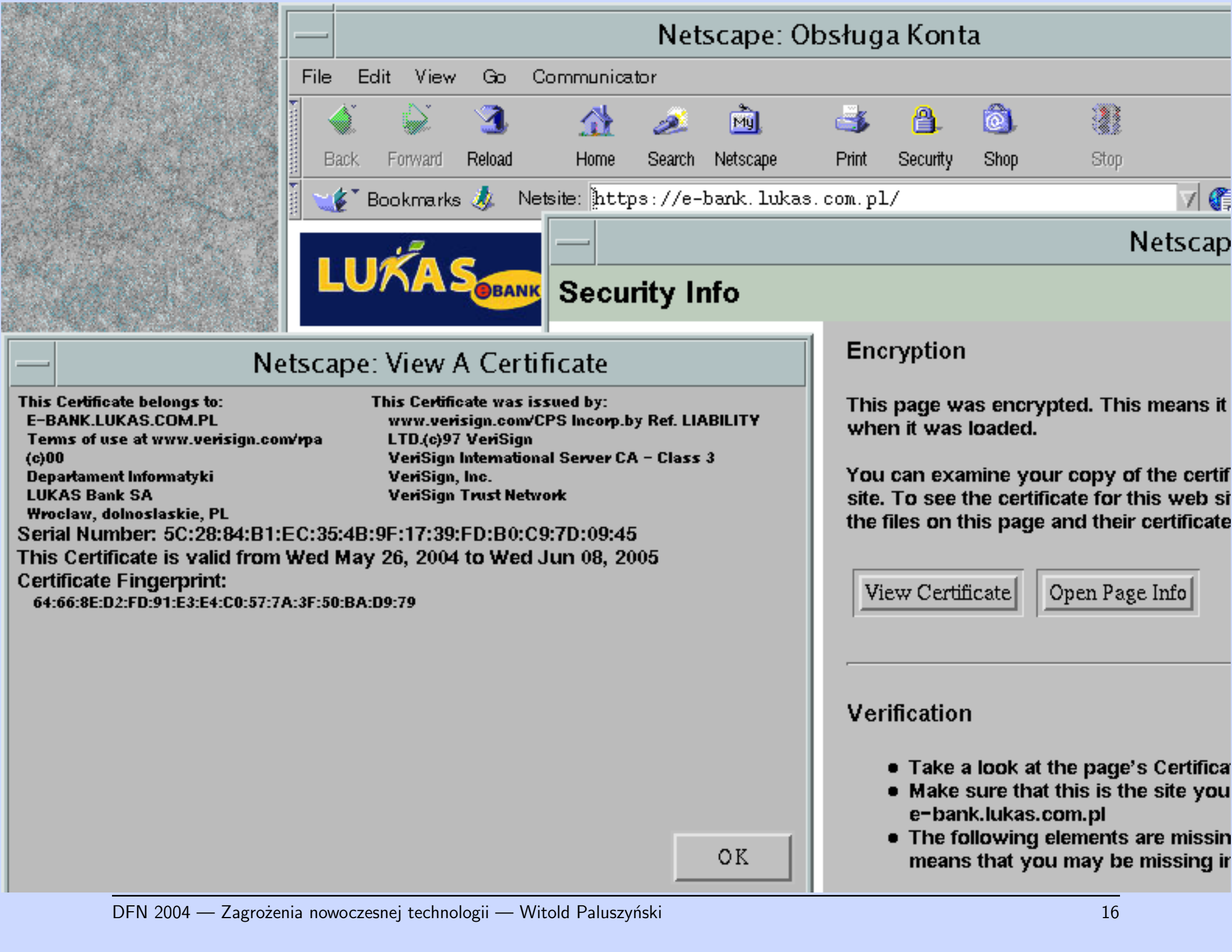
☹ Niestety, nie jest to jeszcze gwarancja bezpiecznej transakcji.



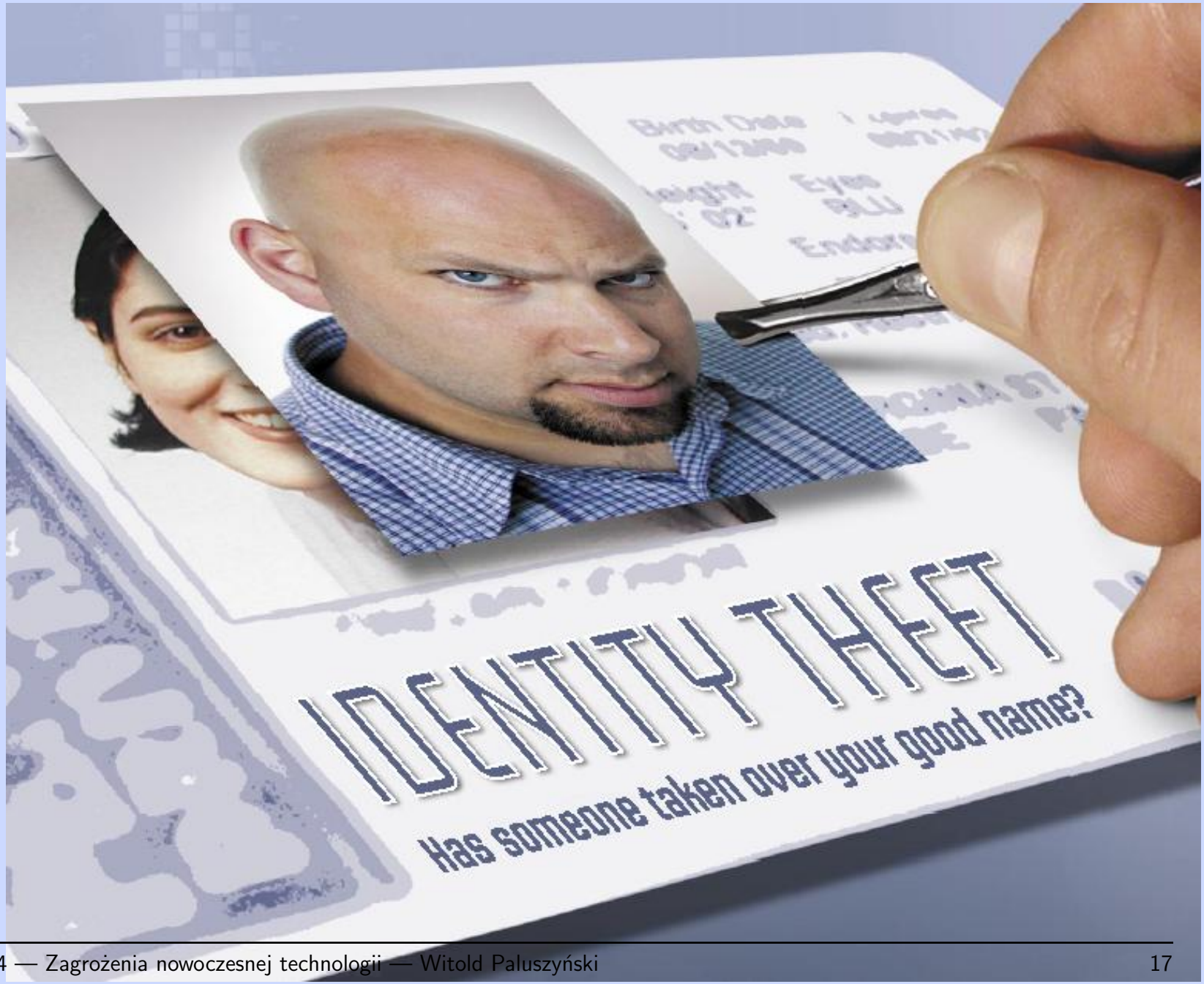
Niepożądani pośrednicy

Nawet jeśli stosujemy szyfrowanie i dbamy o bezpieczne łączenie się z serwerami internetowymi, to nie daje nam to automatycznej gwarancji bezpieczeństwa przed wszystkimi rodzajami ataków internetowych. Niezwykle przewrotnym rodzajem ataku jest tzw. atak z pośrednikiem (ang. *man-in-the-middle attack*).




Netscape: Obsługa Konta
File Edit View Go Communicator
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Netsite: https://e-bank.lukas.com.pl/
LUKAS eBANK
Netscap
Security Info
Encryption
This page was encrypted. This means it
when it was loaded.
You can examine your copy of the certif
site. To see the certificate for this web si
the files on this page and their certificate
View Certificate
Open Page Info
Verification
Take a look at the page's Certifica
Make sure that this is the site you
e-bank.lukas.com.pl
The following elements are missin
means that you may be missing ir
Netscape: View A Certificate
This Certificate belongs to:
E-BANK.LUKAS.COM.PL
Terms of use at www.verisign.com/rpa
(c)00
Departament Informatyki
LUKAS Bank SA
Wroclaw, dolnoslaskie, PL
This Certificate was issued by:
www.verisign.com/CPS Incorp.by Ref. LIABILITY
LTD.(c)97 VeriSign
VeriSign International Server CA - Class 3
VeriSign, Inc.
VeriSign Trust Network
Serial Number: 5C:28:84:B1:EC:35:4B:9F:17:39:FD:B0:C9:7D:09:45
This Certificate is valid from Wed May 26, 2004 to Wed Jun 08, 2005
Certificate Fingerprint:
64:66:8E:D2:FD:91:E3:E4:C0:57:7A:3F:50:BA:D9:79
OK

Kradzież tożsamości



Złodziej, który ukradł naszą tożsamość, może w naszym imieniu:

- założyć kartę kredytową lub płatniczą, i korzystać z niej do momentu, aż bank upomni się o zapłatę
- wystąpić wprost o pożyczkę gotówkową z banku
- otworzyć zwykły rachunek w banku, i wykorzystać go do robienia różnych płatności o charakterze kredytu, na przykład wystawiając czeki
- otworzyć rachunek telefoniczny i korzystać z niego "nabijając" nam koszty
- zaprenumerować inne usługi realizowane w dobrej wierze na podstawie danych wiarygodnego klienta (czyli nas)

Jakie mogą być konsekwencje, gdy ktoś ukradnie i wykorzysta naszą wiarygodną dotychczas tożsamość:

- natychmiastowa utrata wiarygodności finansowej, utrata dostępu do kredytów
- zablokowanie kart kredytowych
- wymówienie posiadanych kredytów, np. na dom, samochód
- w konsekwencji postępowanie komornicze i utrata dóbr
- tymczasowe aresztowanie za niepopełnione przestępstwa
- utrata pracy i/lub szans na zatrudnienie
- utrata klientów w biznesie, bankructwo
- uciążliwe postępowanie wyjaśniające

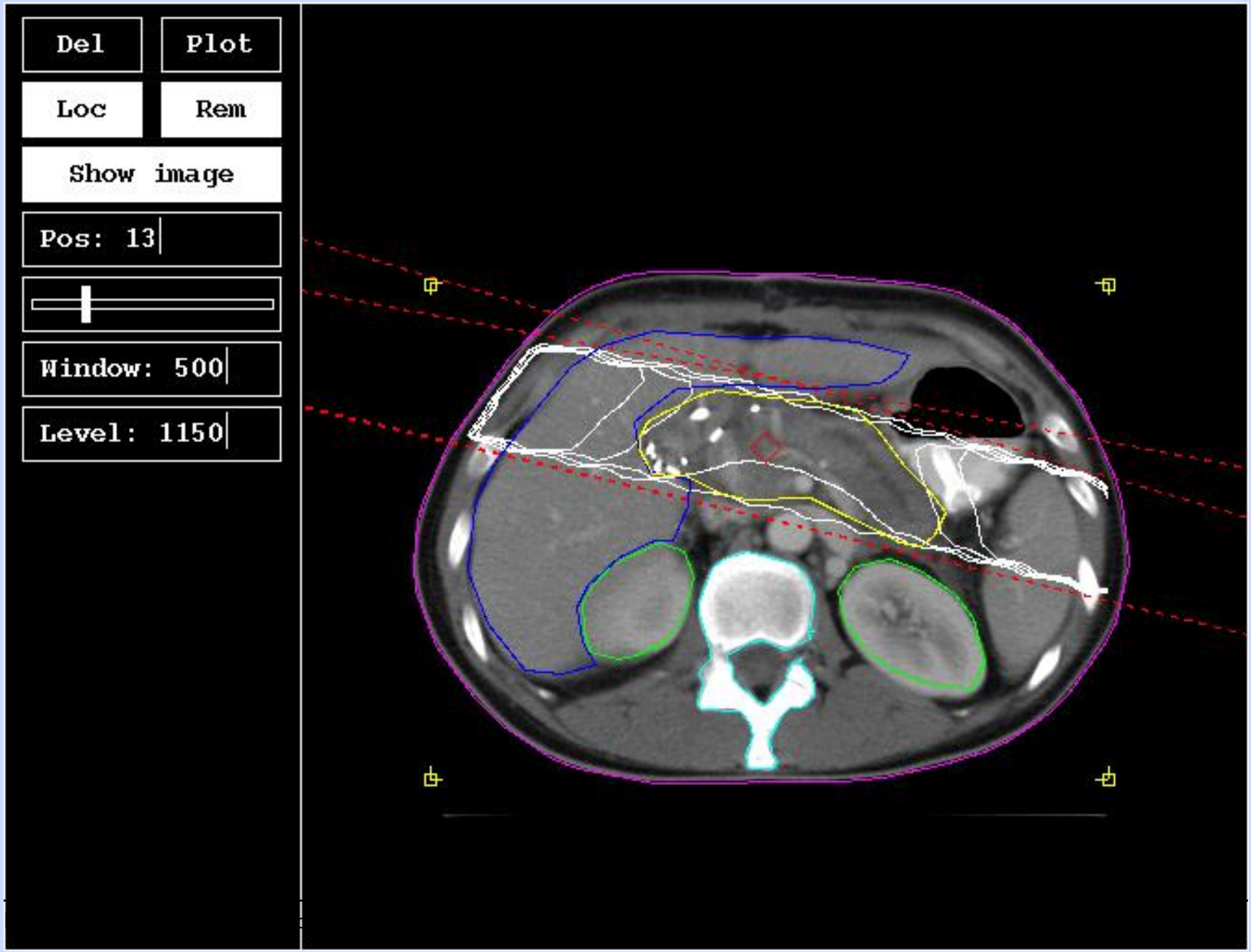
Ocenia się, że w roku 2002 w Stanach Zjednoczonych ofiarą kradzieży tożsamości padło ogółem 10 milionów obywateli. Spośród 162 tysięcy zarejestrowanych w tym roku przypadków kradzieży tożsamości średnia wartość strat w U.S.A. wynosiła 2,000 US$.

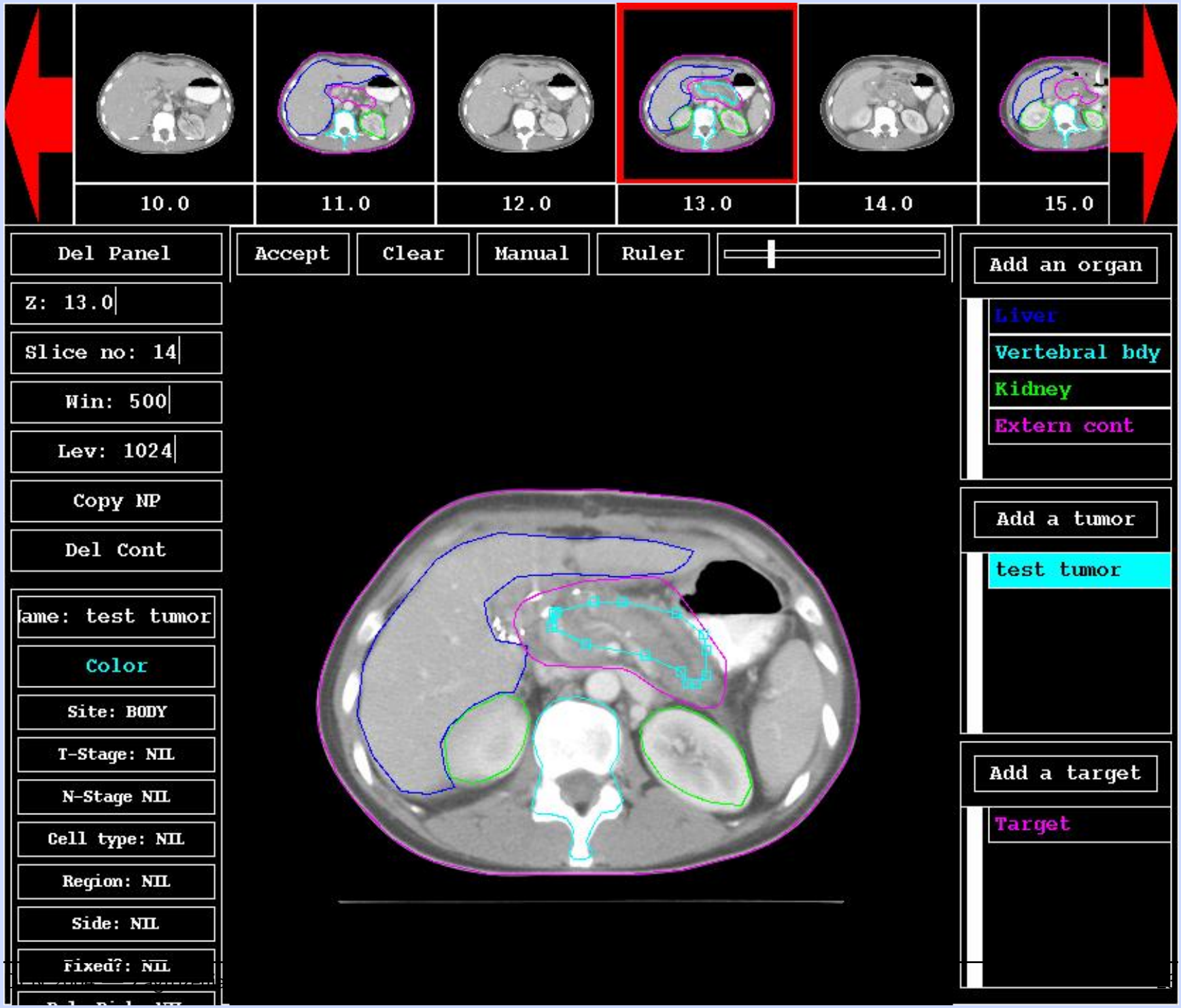
Główne sposoby pozyskiwania danych osobowych przez złodziei tożsamości:

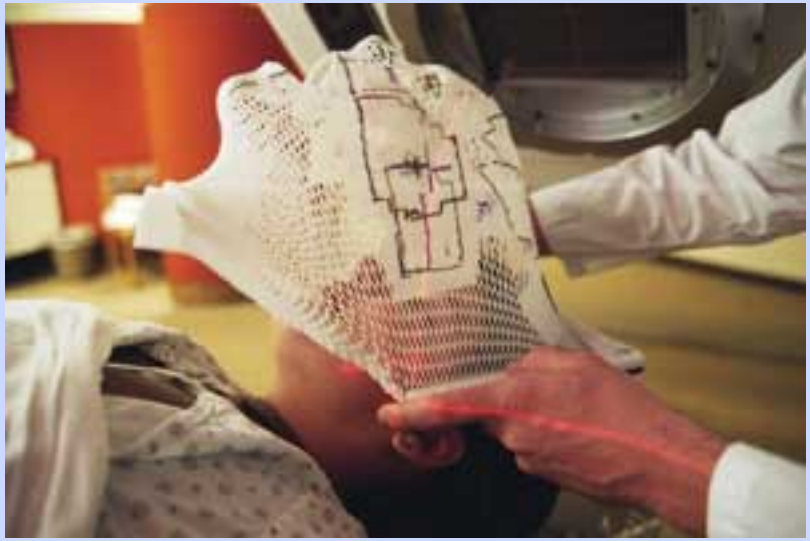
- pułapki internetowe (phishing)
- podczytywanie danych w trakcie dokonywania transakcji przez internet lub przez bankomat
- włamanie do systemów komputerowych naszego pracodawcy, banków, operatorów telekomunikacyjnych, providerów internetowych, innych firm świadczących powszechne usługi, organów administracji, itd.
- przekupienie pracownika ww. instytucji
- grzebanie w śmietnikach ww. instytucji
- omyłkowe ujawnienie do publicznej wiadomości baz danych przez ww. instytucje
- zwykła kradzież dokumentów, z torebki lub z domu
- kradzież poczty ze skrzynki pocztowej, np. zestawień bankowych, albo ofert wydania kart kredytowych
- wywiad telefoniczny


varian
NOMOS
B R T

Komputerowe systemy wspomagają planowanie terapii radiacyjnej oparte na obrazach CT (tomografii komputerowej) i NMR (rezonansu magnetycznego).




10.0
11.0
12.0
13.0
14.0
15.0
Del Panel
Accept
Clear
Manual
Ruler
Z: 13.0
Slice no: 14
Win: 500
Lev: 1024
Copy NP
Del Cont
ame: test tumor
Color
Site: BODY
T-Stage: NIL
N-Stage NIL
Cell type: NIL
Region: NIL
Side: NIL
Fixed?: NIL
Add an organ
Liver
Vertebral bdy
Kidney
Extern cont
Add a tumor
test tumor
Add a target
Target



Ciało pacjenta musi być unieruchomione w tym samym położeniu na każdą z np. 25 dziennych dawek promieniowania.

Sterowany komputerowo akcelerator liniowy może skierować wytworzoną wiązkę promieniowania o wielkiej energii, np. 25 MeV, w ciało pacjenta pod różnymi kątami.

Wypadki poparzeń promieniowaniem

- lata 80-te XX wieku: wypadki z akceleratorem Therac-25 (AECL Canada)
  - w roku 1985 trzech pacjentów ciężko poparzonych;
    nie podjęto poważniejszych działań w celu zapobieżenia dalszym wypadkom
  - w roku 1986 dwa kolejne ciężkie poparzenia (pacjenci zmarli), dopiero po drugim wypadku, po którym pacjent zmarł 3 tygodnie później, zatrudniony w ośrodku fizyk przeprowadził serię eksperymentów z maszyną, i wykrył trudny do powtórzenia błąd w oprogramowaniu operatora;
    rozpoczyna się śledztwo rządowe i poszukiwanie błędu
  - w roku 1987 producent znalazł w końcu i usunął błąd w oprogramowaniu;
    w międzyczasie jednak nastapił kolejny wypadek, po którym pacjent zmarł
- 2001: wypadki z akceleratorem Cobalt-60 (Multidata Systems International)
  - 28 wypadków poparzeń, 6 pacjentów zmarło w Panamie;
    w tym przypadku oprogramowanie nie miało błędu, jednak było tak skomplikowane, że operatorzy wprowadzali niepoprawne dane

Przykłady zagrożeń: katastrofy lotnicze

- błędy systemów automatycznej nawigacji (CFIT=*Controlled Flight into Terrain*)
- utrata kontroli nad samolotem w wyniku błędu oprogramowania
  - Airbus A320 Lufthansy w Warszawie w 1992; system sterowania samolotu opóźnił o 9 sekund włączenie hamulców przez pilota
  - Airbus A300 China Airlines rozbił się w 1994 w Nagoya; omyłkowo włączony przez drugiego pilota w czasie lądowania autopilot chwilowo walczył z pilotami o kontrolę nad samolotem
  - Mars Polar Lander na Marsie w 2000; system wyłączył silniki 40 metrów nad Marsem
- omyłkowe zestrzelenia
  - samoloty wojskowe — wiele przypadków
  - cywilne samoloty pasażerskie
    * 1985: koreański Boeing 747 KAL007 — 269 ofiar
    * 1988: irański Airbus A300 IR655 — 290 ofiar
    * 1996: amerykański Boeing 747 TWA800 — 230 ofiar (oficjalna wersja: wybuch na pokładzie)
    * 2001: rosyjski Tupolew Tu-154 SB1812 — 78 ofiar

Katastrofy lotnicze: omyłkowe zestrzelenia

System Patriot

Miał służyć do obrony przeciwko atakom rakietowym.

Wyposażony w radar, rakiety, oraz system automatycznego rozpoznania celu i naprowadzania nań rakiet w czasie lotu.

Baterie Patriot były używane w czasie wojny „Pustynna Burza” w 1991 przeciwko irackim rakietom SCUD, ale okazały się mało skuteczne.

- W czasie wojny „Pustynna Burza” w Iraku w 1991 systemy Patriot były stosowane przeciwko irackim rakietom SCUD, ale okazały się nieskuteczne, 10 wysoce prawdopodobnych zestrzeleń na 85 wystrzałów.

- Przez 10 lat prowadzono intensywne prace nad zwiększeniem skuteczności.

- 23 marca 2003 bateria Patriot zainstalowana na granicy Kuwejtu omyłkowo namierzyła i zestrzeliła samolot RAF Tornado GR-4 wracający znad Iraku. Zginęło dwóch brytyjskich pilotów.

- 24 marca 2003 inna bateria Patriot zainstalowana niedaleko miasta Nadżaf w Iraku namierzyła amerykański F-16 i przygotowywała się do zestrzelenia. Pilot natychmiast wystrzelił superszybką rakietę HARM i zniszczył baterię ratując się przed zestrzeleniem. Szczęśliwie nikt nie zginął ponieważ obsługa baterii schowała się w schronie, pozostawiając Patriota w trybie ognia automatycznego.

  Dowództwo wszczęło śledztwo w sprawie niesłusznego otwarcia ognia przez ... pilota, i zniszczenia mienia państwowego!

Omyłkowe zestrzelenia: USS Vincennes

USS Vincennes, 3 lipca 1988

- wojna Iranu z Irakiem, ataki irańskie na tankowce przepływające przez Zatokę Perską
- flota amerykańska wysłana w celu ochrony statków przed atakami irańskimi; Amerykanie w przyjaźni z Irakiem i Saddamem Husajnem
- wzajemne zaczepki małych łodzi irańskich i okrętów wojennych U.S.A.
- krążownik floty amerykańskiej USS Vincennes wyposażony w najnowocześniejszy system uzbrojenia Aegis (aegis w mitologii greckiej: tarcza Zeusa), zaplanowany do pracy w pełni automatycznej, od rozpoznania do zniszczenia przeciwnika
  - system silnie nasycony techniką informatyczną i sztuczną inteligencją
  - radar AN/SPY o mocy 4 MW
  - rakiety przeciwlotnicze Standard SM-2

Amerykański kapitan, wbrew rozkazom dowództwa, wpływa na wody terytorialne Iranu. Ścigając małe kutry irańskie zapomina o regularnym sprawdzaniu otoczenia, np. rozkładu lotów linii lotniczych. Wierzy w niezawodność systemów automatycznego rozpoznania i ostrzegania.

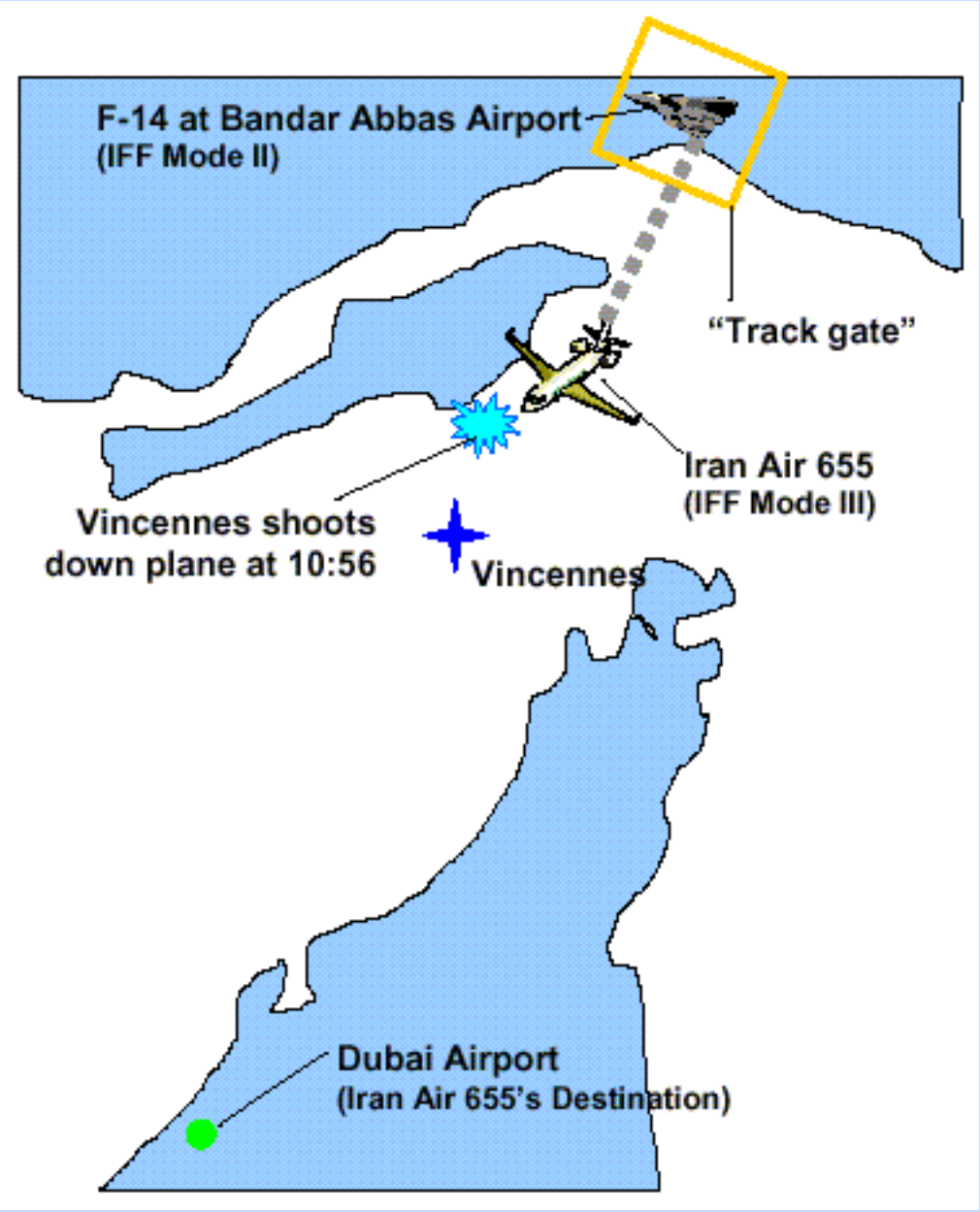

CHINA AIRLINES
(c) Frank Schaefer - A.300B4-622R B-1816 China A/l - HKG OCT 1991

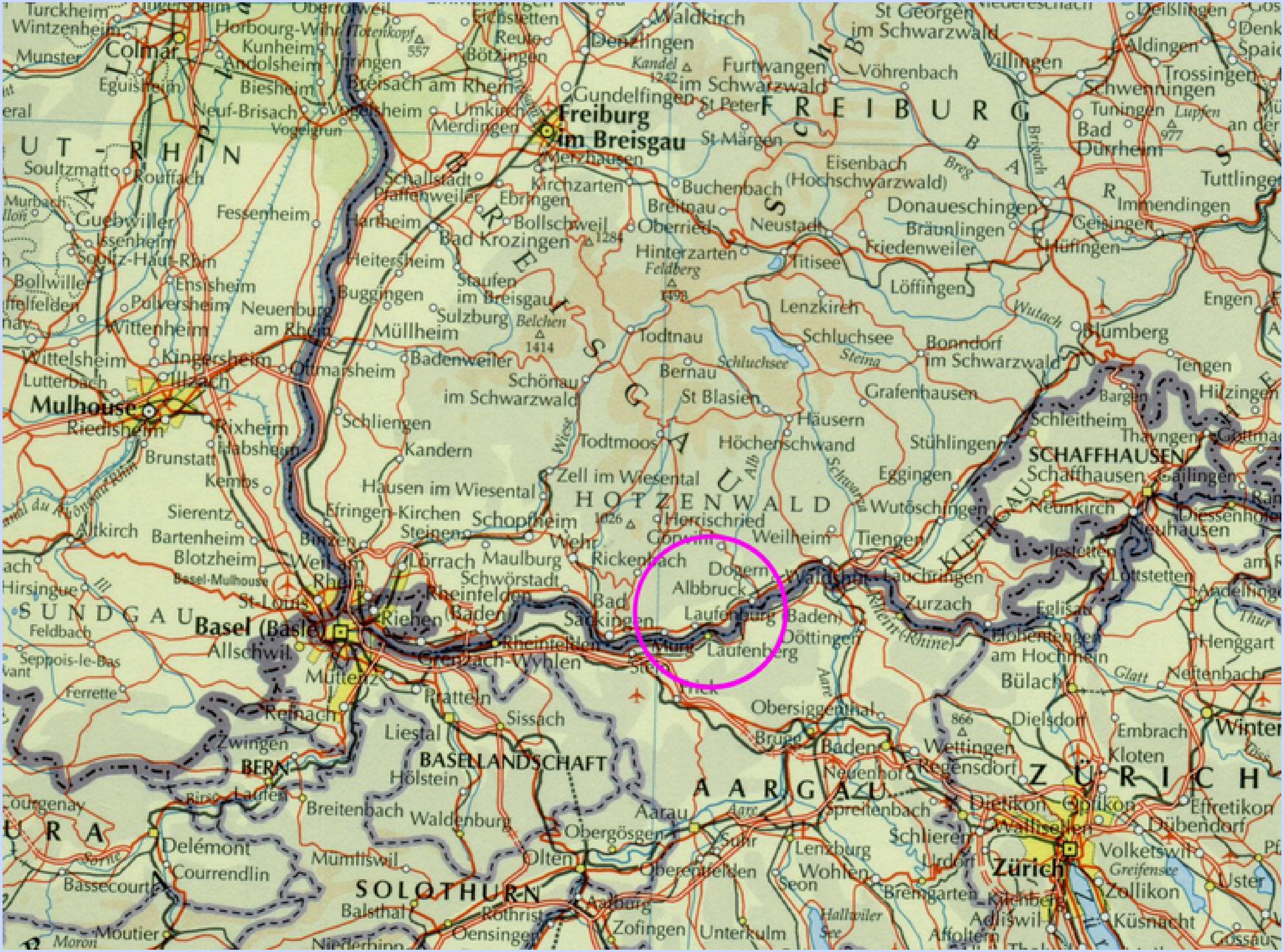

49

Wskutek błędnego projektu systemu komputerowego i szeregu pomyłek obsługa stanowiska dowodzenia nabiera przekonania, że w stronę okrętu leci irański myśliwiec F-14.

Wysłane zostają ostrzeżenia drogą radiową, lecz skierowane są do ... irańskiego myśliwca. Załoga rejsowego samolotu nie odpowiada.

Załogi innych amerykańskich statków w rejonie obserwują sytuację, lecz nie ingerują w przebieg wydarzeń wierząc, że najnowocześniejszy system Vincennes'a nie może się mylić.


F-14 at Bandar Abbas Airport
(IFF Mode II)
"Track gate"
Iran Air 655
(IFF Mode III)
Vincennes shoots
down plane at 10:56
Vincennes
Dubai Airport
(Iran Air 655's Destination)



Colmar
Freiburg im Breisgau
Waldkirch
Denzlingen
Gundelfingen
St Georgen im Schwarzwald
Furtwangen im Schwarzwald
Vöhrenbach
Villingen
Schwenningen
Trossingen
Bad Dürrheim
F R E I B U R G
Breisach am Rhein
Neuf-Brisach
Kirchzarten
Buchenbach
Hinterzarten
Titisee
Neustadt
Donaueschingen
Bräunlingen
Hüfingen
Löffingen
Lenzkirch
Schluchsee
Bonndorf im Schwarzwald
Blumberg
Engen
Tuttlingen
Immendingen
Bad Krozingen
Staufen im Breisgau
Müllheim
Badenweiler
Todtnau
Bernau
St Blasien
Schönau im Schwarzwald
Todtmoos
Höchenschwand
Häusern
Grafenhausen
Stühlingen
Schleitheim
SCHAFFHAUSEN
Schaffhausen
Neunkirch
Neuhausen
Mulhouse
Riedisheim
Rixheim
Habsheim
Brunstatt
Kembs
Sierentz
Altkirch
Bartenheim
Blotzheim
Hirsingue
S U N D G A U
Basel (Basle)
Allschwil
Muttenz
Riehen
Lörrach
Weil am Rhein
Schopfheim
Zell im Wiesental
H O T Z E N W A L D
Herrischried
Görwihl
Weilheim
Tiengen
Wutöschingen
Rickenbach
Wehr
Bad Säckingen
Albbruck
Dogern
Laufenburg (Baden)
Laufenburg
Waldshut
Lauchringen
Zurzach
Döttingen
Rheinfelden (Baden)
Rheinfelden
Grenzach-Wyhlen
Schwörstadt
Maulburg
Kandern
Schliengen
Pratteln
Liestal
Sissach
BASELLANDSCHAFT
Hölstein
Reinach
Zwingen
BERN
Laufen
Breitenbach
Waldenburg
Delémont
Courrendlin
Bassecourt
Moutier
SOLOTHURN
Balsthal
Mümliswil
Olten
Aarau
A A R G A U
Brugg
Baden
Wettingen
Regensdorf
Dietikon
Schlieren
Lenzburg
Wohlen
Bremgarten
Zürich
Z Ü R I C H
Kloten
Bülach
Dielsdorf
Embrach
Winterthur
Effretikon
Dübendorf
Volketswil
Uster
Zollikon
Küsnacht
Zofingen
Unterkulm
Aarburg
Oensingen
Rothrist
Obergösgen
Eglisau
Hohentengen am Hochrhein
Henggart
Neftenbach
Jestetten
Lottstetten
Tengen
Hilzingen
Thayngen
Feldberg

Historia mostu w Laufenberg

Nowo wybudowany most na Renie między szwajcarską miejscowością Laufenberg, a niemiecką miejscowością Laufenburg, wypadł dzielnym budowniczym, ku ich wielkiemu zdziwieniu, całe 54 centymetry powyżej poziomu drogi zbudowanej po niemieckiej stronie (po szwajcarskiej stronie droga zgodziła się z mostem).

Przebudowa okazała się bardzo kosztowna i opóźniła oddanie mostu do użytku o wiele miesięcy.

http://www.laufenburg.ch/

Dlaczego 54 centymetry?

Wszystko było precyzyjnie, z milimetrową dokładnością zaprojektowane przy użyciu komputerów, mierząc od poziomu morza. Projekt był wielokrotnie sprawdzany, a następnie most wykonany zgodnie z projektem z iście niemiecką dokładnością.

Więc dlaczego? Skąd wziął się taki błąd?

W Szwajcarii pomiary wysokości wykonuje się od poziomu Morza Śródziemnego, położonego o 27 centymetrów wyżej niż Morze Północne, od którego poziomu mierzą w Niemczech. To wiedzą wszyscy budowlańcy realizujący projekty w Europie Środkowej. Skąd więc wzięła się różnica poziomów aż o 54 centymetry?

Dlaczego 54 centymetry?

Wszystko było precyzyjnie, z milimetrową dokładnością zaprojektowane przy użyciu komputerów, mierząc od poziomu morza. Projekt był wielokrotnie sprawdzany, a następnie most wykonany zgodnie z projektem z iście niemiecką dokładnością.

Więc dlaczego? Skąd wziął się taki błąd?

W Szwajcarii pomiary wysokości wykonuje się od poziomu Morza Śródziemnego, położonego o 27 centymetrów wyżej niż Morze Północne, od którego poziomu mierzą w Niemczech. To wiedzą wszyscy budowlańcy realizujący projekty w Europie Środkowej. Skąd więc wzięła się różnica poziomów aż o 54 centymetry?

Czyżby...

Dlaczego 54 centymetry?

Wszystko było precyzyjnie, z milimetrową dokładnością zaprojektowane przy użyciu komputerów, mierząc od poziomu morza. Projekt był wielokrotnie sprawdzany, a następnie most wykonany zgodnie z projektem z iście niemiecką dokładnością.

Więc dlaczego? Skąd wziął się taki błąd?

W Szwajcarii pomiary wysokości wykonuje się od poziomu Morza Śródziemnego, położonego o 27 centymetrów wyżej niż Morze Północne, od którego poziomu mierzą w Niemczech. To wiedzą wszyscy budowlańcy realizujący projekty w Europie Środkowej. Skąd więc wzięła się różnica poziomów aż o 54 centymetry?

Czyżby... Uuuups!!!

Dlaczego 54 centymetry?

Wszystko było precyzyjnie, z milimetrową dokładnością zaprojektowane przy użyciu komputerów, mierząc od poziomu morza. Projekt był wielokrotnie sprawdzany, a następnie most wykonany zgodnie z projektem z iście niemiecką dokładnością.

Więc dlaczego? Skąd wziął się taki błąd?

W Szwajcarii pomiary wysokości wykonuje się od poziomu Morza Śródziemnego, położonego o 27 centymetrów wyżej niż Morze Północne, od którego poziomu mierzą w Niemczech. To wiedzą wszyscy budowlańcy realizujący projekty w Europie Środkowej. Skąd więc wzięła się różnica poziomów aż o 54 centymetry?

Czyżby... Uuuups!!!
Tak, niestety, różnica poziomów morza została w programie komputerowym użytym do zaprojektowania mostu odjęta zamiast dodana, i wyszło za mało.

Zagrożenia nowoczesnych technologii

■ nadużycia, wykorzystanie technologii przeciwko ludziom

- nadużycia i przestępstwa w systemach komputerowych
- zagrożenia prywatności jednostki
- zagrożenia własności intelektualnej

■ zagrożenia wynikające z niepoprawnego posługiwania się technologią

- trudności z projektowaniem rzeczywiście niezawodnych systemów komputerowych, niedocenianie złożoności oprogramowania, lekceważenie dostatecznego testowania,
- lekceważenie jednostkowych incydentów, zwalanie winy na „błąd człowieka”
- problemy z przystosowaniem się ludzi do pracy w ważnych działach w warunkach nadmiernego nasycenia techniką, nadmiaru informacji, wzrostu szybkości i presji podejmowania decyzji
- błędy popełniane przez ludzi w wyniku nadmiernego zaufania do systemów komputerowych
- możliwość powierzania ważnych decyzji komputerom