

# Ukryte funkcjonalności w oprogramowaniu i urządzeniach elektronicznych

mgr inż. Paweł Koszut

# Ukryte funkcjonalności w oprogramowaniu i urządzeniach elektronicznych

Zamiast wstępu :

Inspiracja

# GSM w Grecji



The image is a screenshot of the BBC News website. At the top, there is a navigation bar with the BBC logo and links for Home, News, Sport, Radio, TV, Weather, and Languages. Below this, there are radio buttons for 'UK version' and 'International version', with 'International version' selected. The main header features the 'BBC NEWS' logo on the left and a 'WATCH One-Minute World News' button on the right, accompanied by a globe icon. The page is dated 'Last Updated: Thursday, 2 February 2006, 14:22 GMT'. There are links for 'E-mail this to a friend' and 'Printable version'. The main headline is 'Greek government's phones tapped'. The sub-headline reads: 'Greek Prime Minister Costas Karamanlis and several ministers had their mobile phones tapped for more than a year, the government has confirmed.' To the right of the text is a portrait of Costas Karamanlis. Below the portrait is a caption: 'Costas Karamanlis and other ministers were tapped'. On the left side of the page, there is a 'News Front Page' section with a world map and a list of regional categories: Africa, Americas, Asia-Pacific, Europe (highlighted), Middle East, South Asia, UK, Business, Health, and Science/Nature.

BBC

Home News Sport Radio TV Weather Languages

UK version  International version | About the versions

BBC NEWS

WATCH One-Minute World News

Last Updated: Thursday, 2 February 2006, 14:22 GMT

[E-mail this to a friend](#) [Printable version](#)

## Greek government's phones tapped

**Greek Prime Minister Costas Karamanlis and several ministers had their mobile phones tapped for more than a year, the government has confirmed.**

A spokesman said an investigation had been opened, but had not yet discovered who was conducting the surveillance.



Costas Karamanlis and other ministers were tapped

News Front Page

Africa  
Americas  
Asia-Pacific  
**Europe**  
Middle East  
South Asia  
UK  
Business  
Health  
Science/Nature

# GSM w Grecji

BBC

Home News Sport Radio TV Weather Languages

UK version  International version | About the versions

**BBC NEWS**

WATCH One-Minute World News

News Front Page

Last Updated: Friday, 24 March 2006, 08:31 GMT

[E-mail this to a friend](#) [Printable version](#)

## Death muddies Greek spy probe

By Richard Galpin  
BBC News, Athens

**A senior aide to the Greek prime minister is expected to be the next person to testify before a parliamentary committee investigating what is believed to be the worst espionage scandal in the country's history.**

Last month, the government admitted that the mobile phones of the prime minister, the most senior members of the cabinet and top security officials had all been tapped in 2004 - the year Athens hosted the Olympic Games.



Costas Tsalikidis: Did he help set up the phone-tapping?

Africa  
Americas  
Asia-Pacific  
**Europe**  
Middle East  
South Asia  
UK  
Business  
Health  
Science/Nature  
Technology  
Entertainment  
Also in the news

Video and Audio

# Prosty przykład XOR


```
function xor (int a,b) {  
    if (a≠b) return 1 else return 0;  
}
```

# Prosty przykład XOR

```
function xor (int a,b) {  
    if (a≠b) return 1 else return 0;  
  
}
```

# Prosty przykład XOR

```
function xor (int a,b) {  
  
    if (a≠b) return 1 else return 0;  
  
}
```

 - part of source code which implements normal functionality

 - part of source code which implements hidden functionality


# Prosty przykład XOR


```
int secret_sequence[] = {t0, t1, t2, t3, ..., tn};  
int secret_counter = 0;
```

```
function xor (int a,b) {
```

```
    // until triggering condition occurs behave normally  
    if (a≠b) return 1 else return 0;
```

```
}
```


 - part of source code which implements normal functionality


 - part of source code which implements hidden functionality



# Prosty przykład XOR

```
int secret_sequence[] = {t0, t1, t2, t3, ..., tn};  
int secret_counter = 0;  
  
function xor (int a,b) {  
  
    // until triggering condition occurs behave normally  
    if (a≠b) return 1 else return 0;  
  
    //check how many consecutive bits match the secret_sequence  
    if (a==secret_sequence[secret_counter]) { secret_counter++; }  
    else { secret_counter=0; }  
  
}
```

 - part of source code which implements normal functionality

 - part of source code which implements hidden functionality

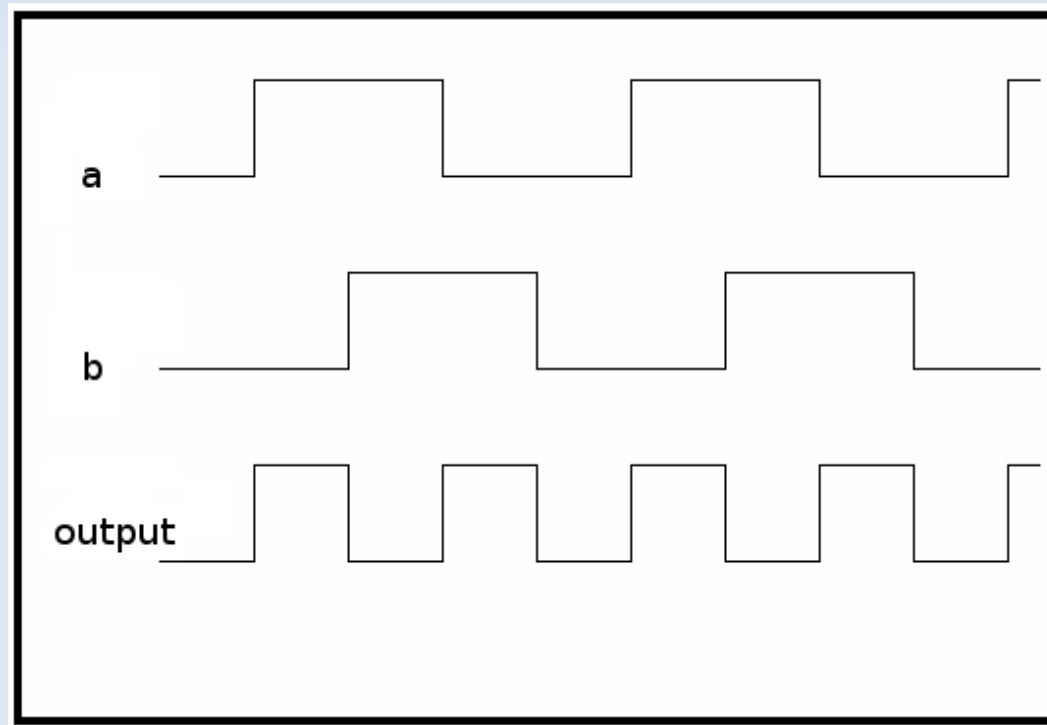
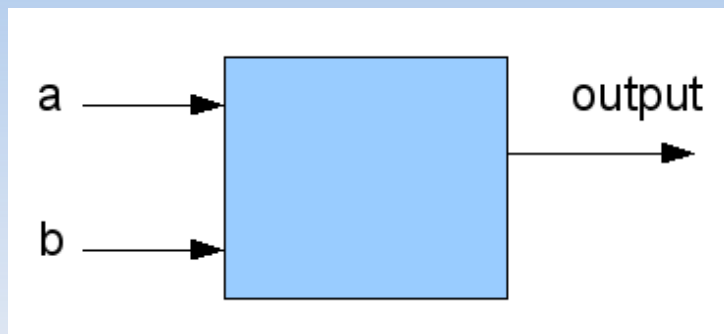
# Prosty przykład XOR

```
int secret_sequence[] = {t0, t1, t2, t3, ..., tn};  
int secret_counter = 0;  
  
function xor (int a,b) {  
  
    // until triggering condition occurs behave normally  
    if (a≠b) return 1 else return 0;  
  
    //check how many consecutive bits match the secret_sequence  
    if (a==secret_sequence[secret_counter]) { secret_counter++; }  
    else { secret_counter=0; }  
  
    //after complete secret_sequence is recognized, call triggered_action  
    if (secret_counter>n) { triggered_action(); }  
  
}
```

- part of source code which implements normal functionality

- part of source code which implements hidden functionality

# Prosty przykład XOR



# Prosty przykład XOR

It is important to take notice of the following :

- The length  $n$  of secret triggering sequence `secret_sequence[ ]` can be long enough to effectively prevent `triggered_action( )` from being called unintentionally;
- The triggering strategy presented above is only an example - an adversary's creativity in developing other triggering conditions is not constrained by this example;
- Hidden functionalities may exist in multiple locations of a device, and can be designed to interact each other;

# Przykład z szyfrem

0 → 1  
1 → 2  
2 → 3  
3 → 4  
4 → 5  
5 → 6  
6 → 7  
7 → 8  
8 → 9  
9 → 0

# Przykład z szyfrem



# Przykład urządzeń telekomunikacyjnych



# 2008 SUBMARINE CABLE MAP

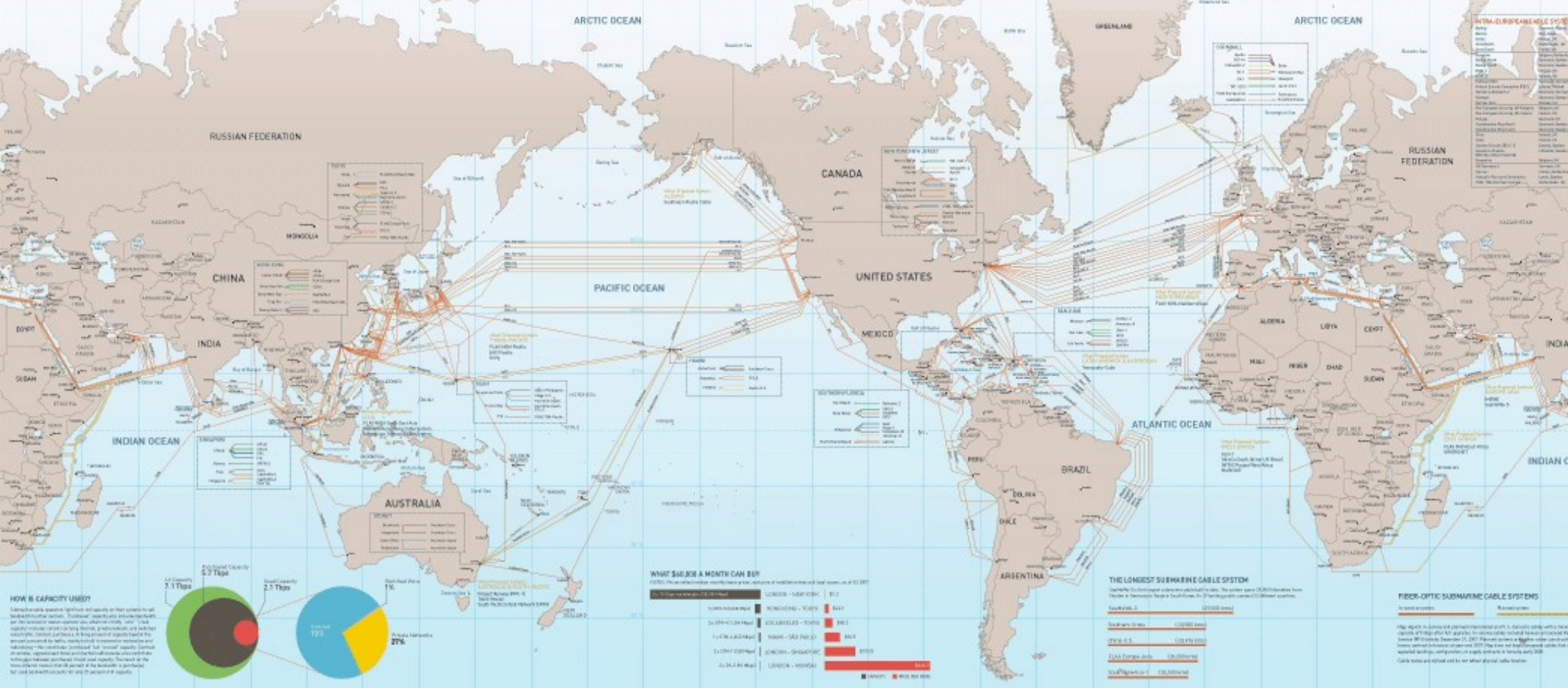
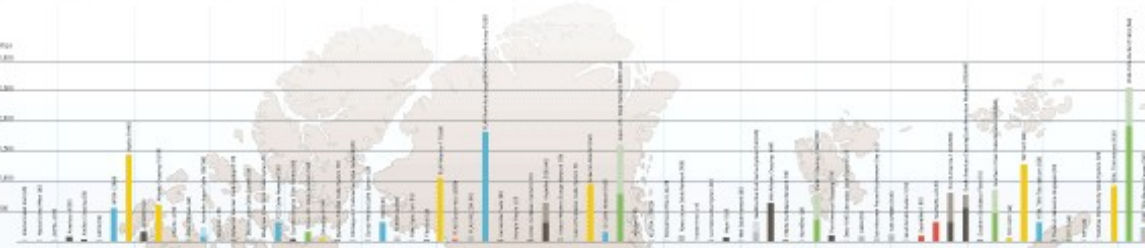
PRODUCTION & DESIGN  
**TeleGeography** **Southern Cross Cable Network**  
 The independent market leader providing fully professional services to the global industry.

**TeleGeography**  
 7801 N. 7th, 14th Floor, Seattle, Washington, DC 98109 USA  
 Tel: +1 206 732 0220 Fax: +1 206 732 0101  
 www.tele-geo.com

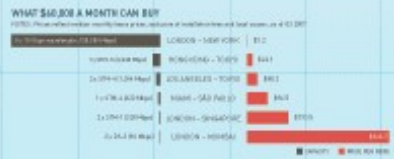
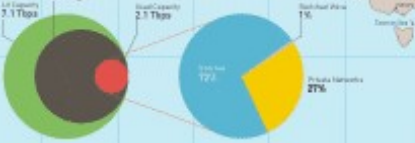
**Southern Cross Cable Network**  
 Suite 500, 701, 800 Pacific Way, West Vancouver, BC V8V 2K6 Canada  
 Tel: +1 416 296 2376 Fax: +1 416 296 2377  
 www.southern-cross.com

**SUBMARINE CABLE CAPACITY, 2007**  
 World's total capacity (independent and shared) is 42.1 Tbps, with 23 Tbps in independent capacity and 19 Tbps in shared capacity. Capacity is expected to reach 50 Tbps by 2010.

Legend:  
 • Shared Capacity  
 • Independent Capacity  
 • Shared Capacity  
 • Independent Capacity



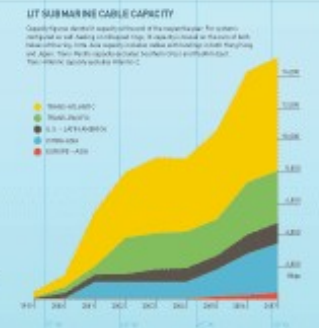
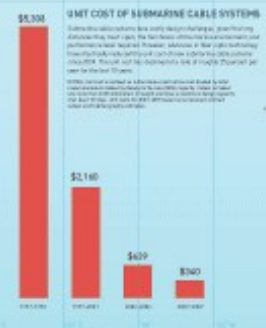
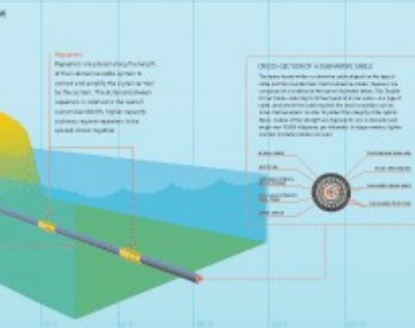
**HOW IS CAPACITY USED?**  
 Submarine capacity is split between independent and shared capacity. Shared capacity is used for inter-continental traffic, while independent capacity is used for intra-continental traffic.



**THE LONGEST SUBMARINE CABLE SYSTEM**  
 The longest submarine cable system is the SEA-ME-WE 3, which spans 19,000 km from Singapore to Los Angeles.

**FIBER-OPTIC SUBMARINE CABLE SYSTEMS**  
 Fiber-optic systems are used for high-speed data transmission. They consist of multiple fibers that carry light signals.

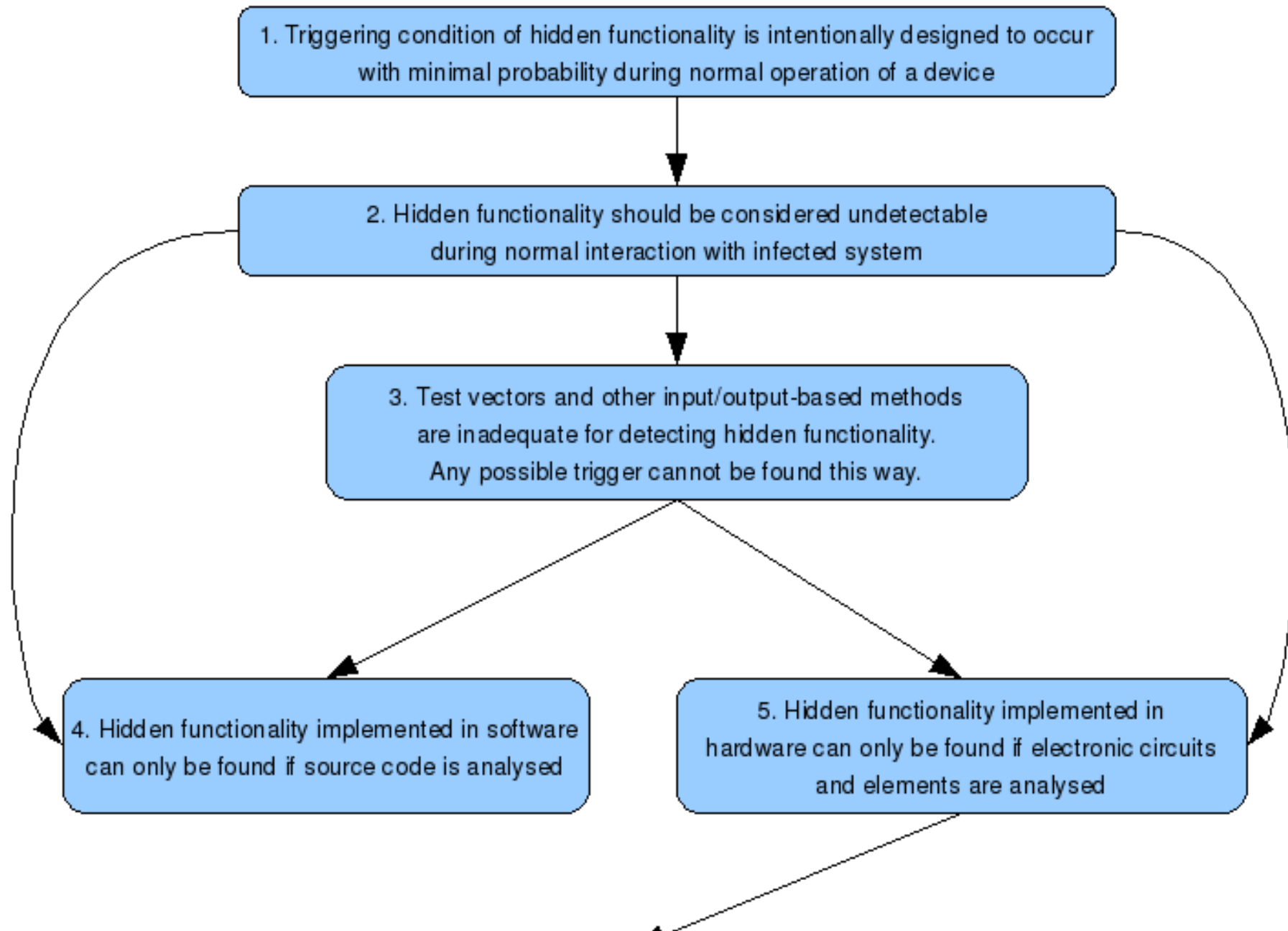
**COMPONENTS OF A SUBMARINE CABLE SYSTEM**  
 A submarine cable system consists of several key components: the cable itself, repeaters, and shore-based equipment.



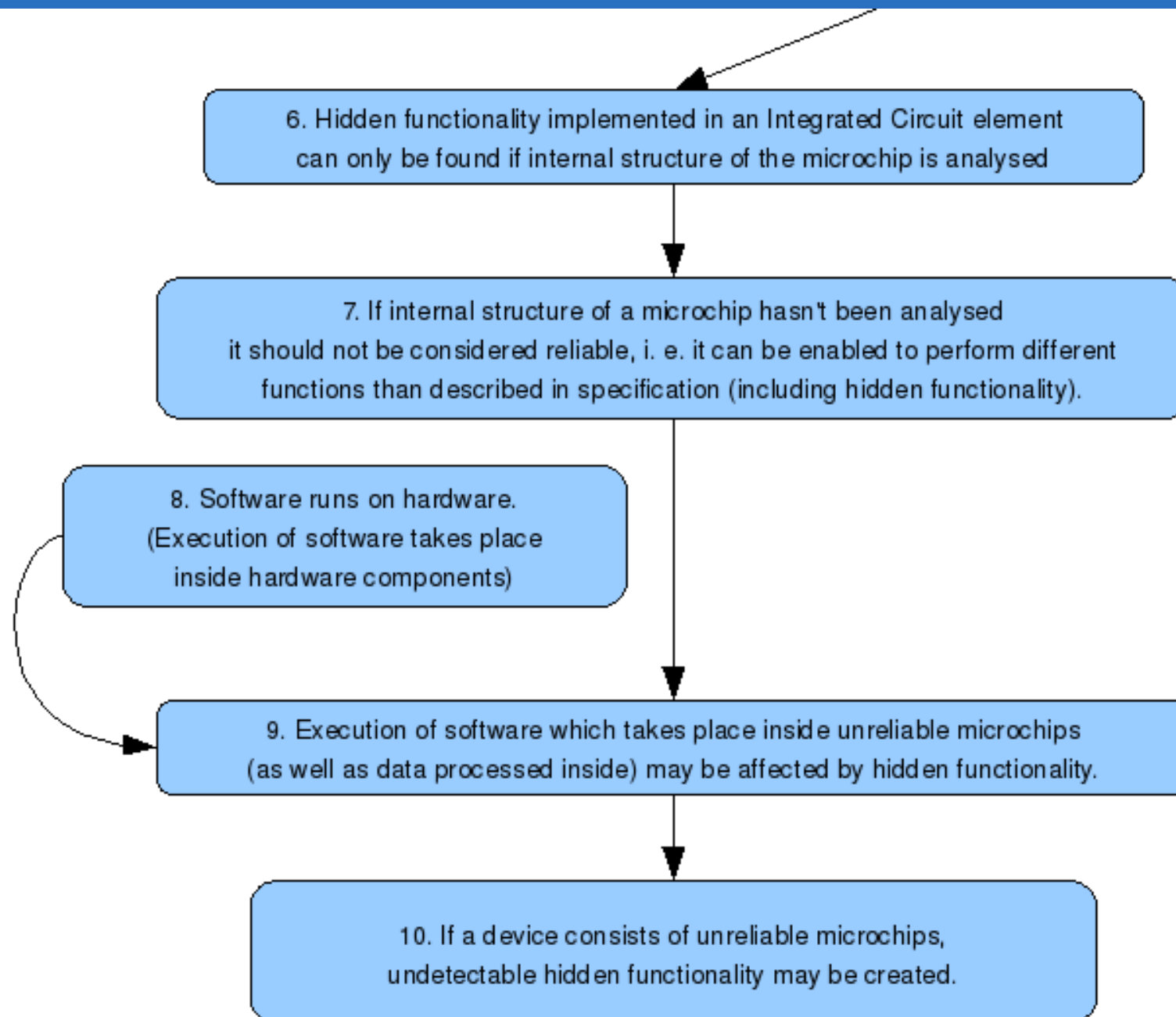


# Analiza podatności

# Analiza podatności części hardware



# Analiza podatności części hardware



# Ekonomia zagrożenia

1. Jaki rodzaj ukrytej funkcjonalności atakujący może chcieć zaimplementować?
2. Ile nakładu potrzeba (pieniądze lub inne zasoby) by zrealizować pożądaný cel?
3. Ile przyniesie mu to zysku lub innego rodzaju korzyści ?

# Gazociąg w Urengoi

Rok 1982

Szpieg KGB w kanadyjskiej firmie

Ukryta funkcjonalność w oprogramowaniu  
turbiny

# Gazociąg w Urengoi



# Gazociąg w Urengoi

Thomas C. Reed : “The result was the most monumental non-nuclear explosion and fire ever seen from space. At the White House, we received warning from our infrared satellites of some bizarre event out in the middle of Soviet nowhere. NORAD (North American Aerospace Defense Command) feared a missile liftoff from a place where no rockets were known to be based. Or perhaps it was the detonation of a small nuclear device...They (the satellites) had detected no electromagnetic pulse, characteristic of nuclear detonations. Before these conflicting indicators could turn into an international crisis, Gus Weiss came down the hall to tell his fellow NSC staffers not to worry”

# Ekonomia zagrożenia

1. Jaki rodzaj ukrytej funkcjonalności atakujący może chcieć zaimplementować?
2. Ile nakładu potrzeba (pieniądze lub inne zasoby) by zrealizować pożądaný cel?
3. Ile przyniesie mu to zysku lub innego rodzaju korzyści ?



# Maszyny do zliczania głosów

Clinton Curtis



# Maszyny do zliczania głosów

eWyborczy skandal w USA - Aktualności IDG.pl - Konqueror

Location Edit View Bookmarks Tools Settings Help

http://www.idg.pl/news/73269.html

al wyborczy w usa

eWyborczy skandal w USA - A...

IDG.pl: Aktualności - IDG TV - Podcasty - Fider - RSS - Programy - Testy - Porady - Artykuły - Newslettery  
Forum - Czat - Blogi - Galeria - Drony - Qui - Wirtualny Dom - Program TV - Słowniki - Usługi - E-Wydania - Kiosk  
Aukcje - Księgarnia - Placa - Fotolab - Karty PrePaid - Centrum Finansowe - Domeny i Serwery

IDG.pl jako strona startowa

WYSZUKIWANIE: [ ] W [ ] mapa [ ] serwis

2008 KWIECIEŃ

PN WT ŚR CZ PT SO ND  
7 8 9 10 11 12 13

Aparaty Biznes Bezpieczeństwo DVD Gry GPS HDTV Mobile

**MOJE KONTO**

- Zaloguj się
- Zarejestruj się
- Dlaczego warto?

**QUIZ**

Co to jest?



- Temperówka
- Odtwarzacz CD
- Stacja dokująca do iPoda
- Stylowy mikrofon

**AKTUALNOŚCI: OPROGRAMOWANIE** << Pokaż panel

## eWyborczy skandal w USA

Autor: **Paweł Krawczyk** Zmień rozmiar liter: **A A A**

8 grudnia 2004 11:44

**Amerykański programista Clinton Curtis złożył doniesienie w sprawie... napisanego przez niego programu do modyfikacji tablic danych za pomocą ekranu dotykowego. Nie byłoby w tym niczego dziwnego, gdyby nie fakt że program ten miał działać w amerykańskich maszynach wyborczych i jego zadaniem było fałszowanie wyników kandydatów, wskazanych specjalnymi kombinacjami klawiszy.**

Według oświadczenia Curtisa, sprawa zaczęła się w 2000 roku kiedy był on zatrudniony przez firmę Yang Enterprises, będącą podwykonawcą NASA w zakresie oprogramowania maszyn zliczających głosy w trakcie wyborów. Został on wówczas zaproszony jako ekspert do udziału w spotkaniach odbywanych przez zarząd firmy z

# Maszyny do zliczania głosów

Stanowisko Stowarzyszenia Internet Society Poland w sprawie głosowania elektronicznego, styczeń 2007



## Stanowisko Stowarzyszenia Internet Society Poland w sprawie głosowania elektronicznego w wyborach powszechnych

styczeń 2007

### **streszczenie:**

*W mediach pojawiają się ostatnio informacje o inicjatywach wprowadzenia powszechnych elektronicznych form głosowania (w tym "przez internet"). Stowarzyszenie Internet Society Poland<sup>1</sup> analizuje je w świetle wymogów przejrzystości procedury wyborczej oraz nadziei na poprawę frekwencji wyborczej. Przedstawiono wybrane doniesienia o przypadkach manipulowania wynikami wyborczymi oraz kompromitacji elektronicznych maszyn wyborczych. Wskazano też na przykłady nasilającego się lobbingu producentów rozwiązań wspierających elektroniczne głosowania. Na ich tle zdaniem ISOC postulaty modyfikacji procedury wyborczej w kierunku dopuszczenia głosowania przez internet niosą ryzyko zagrożenia dla demokracji oraz wyeliminowania wyborców z procesu wyborczego.*

# Analiza podatności części software

# Analiza podatności części software

The screenshot shows a web browser window displaying the Microsoft Security Bulletin MS06-013. The browser's address bar shows the URL <http://www.microsoft.com/technet/security/bulletin/ms06-013>. The page header includes the Microsoft TechNet logo and a search bar. The main content area displays the following information:

[TechNet Home](#) > [TechNet Security](#) > [Bulletins](#)

## Microsoft Security Bulletin MS06-013

### Cumulative Security Update for Internet Explorer (912812)

Published: April 11, 2006

**Version:** 1.0

**Summary**

**Who should read this document:** Customers who use Microsoft Windows

**Impact of Vulnerability:** Remote Code Execution

**Maximum Severity Rating:** Critical

**Recommendation:** Customers should apply the update immediately.

**Security Update Replacement:** This bulletin replaces several prior security updates. See the frequently asked questions (FAQ) section of this bulletin for the complete list.

**Caveats:** [Microsoft Knowledge Base Article 912812](#) documents the currently known issues that customers may experience when they install this security update. The article also documents recommended solutions for these issues. For more information, see [Microsoft Knowledge Base Article 912812](#).

This security update also replaces the cumulative update for Internet Explorer that was released for Windows XP Service Pack 2, Windows Server 2003 Service Pack 1, Windows XP Professional x64 Edition, Windows Server 2003 x64 Edition family, and Windows Server 2003 with Service Pack 1 for Itanium-based

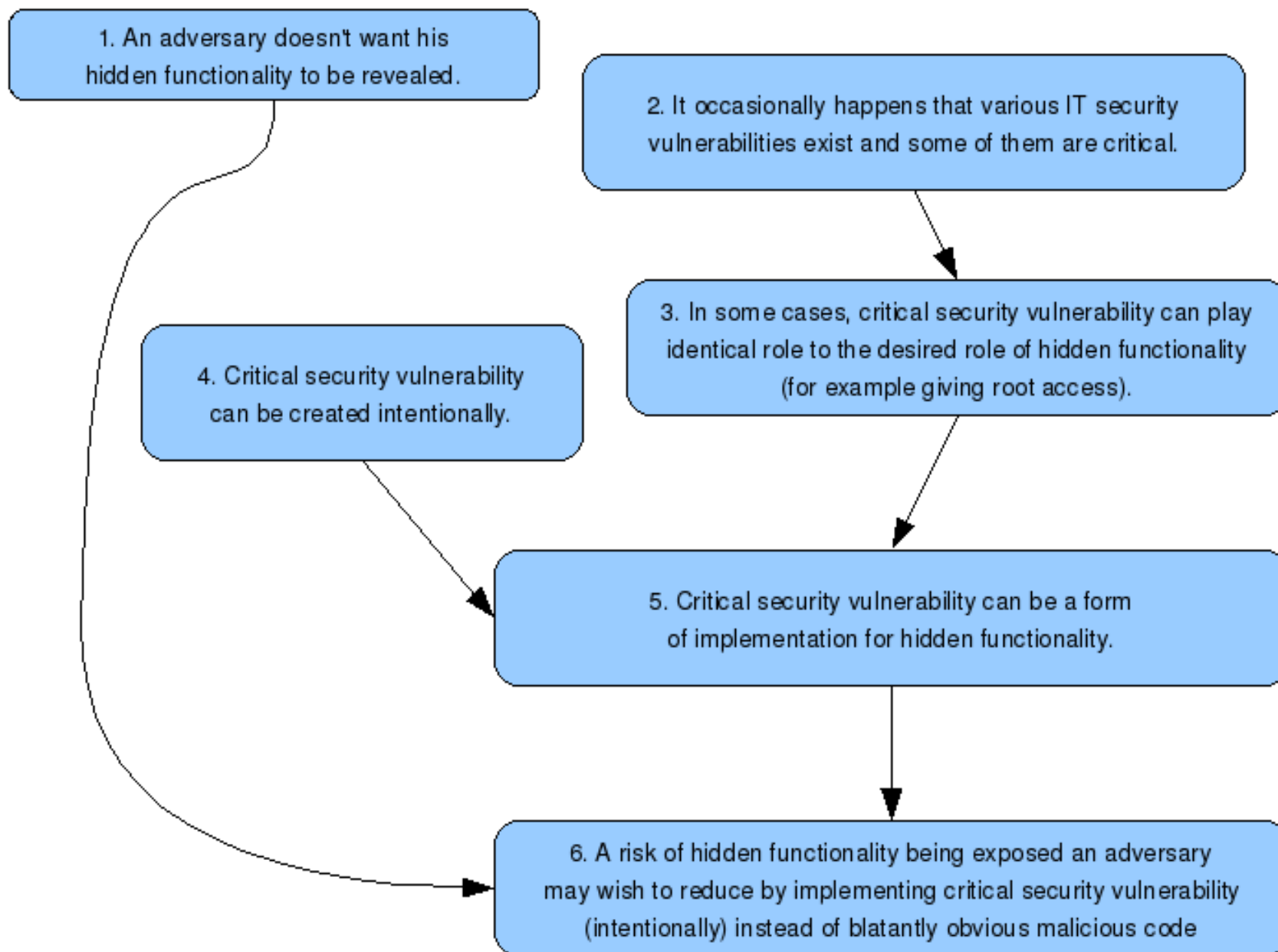
The left sidebar contains a search bar and a navigation menu with the following items:

- TechNet Security
- Security Bulletin Search
- Products
- Guidance
- Tools
- Understanding Security
- Partners
- Downloads
- Community
- Events & Webcasts
- Virtual Labs
- Scripting for Security
- Small Business Security
- Midsize Business Security

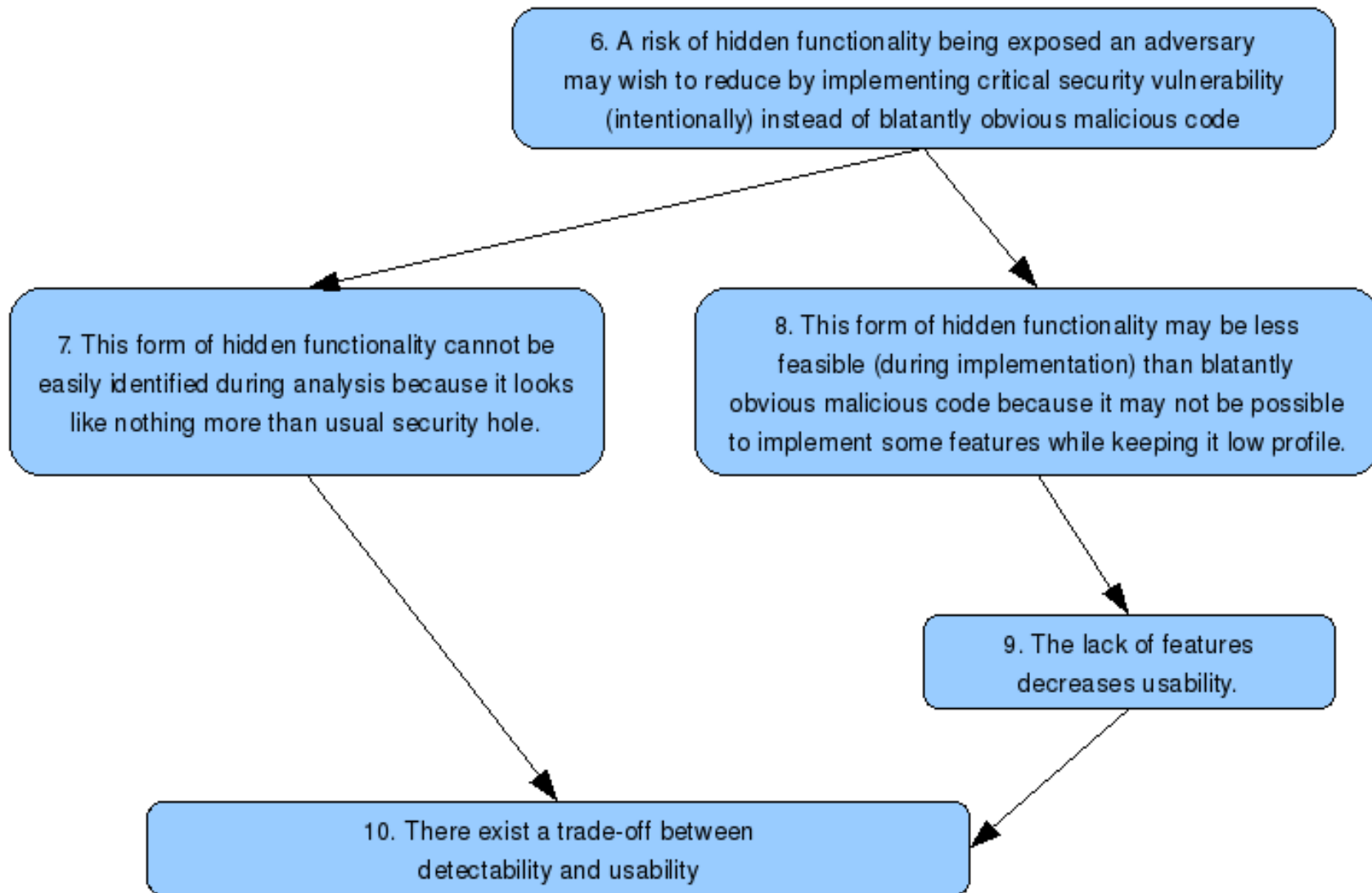
Additional Resources

- Events & Errors

# Analiza podatności części software



# Analiza podatności części software



# Krytyczne luki w roli ukrytej funkcjonalności



# Krytyczne luki w roli ukrytej funkcjonalności

Computerworld > French Embassy site for Libya said to be serving malware - Konqueror

Location Edit View Bookmarks Tools Settings Help

http://computerworld.co.nz/news.nsf/scr/7ABECA9FFB08

Computerworld > French Emba...

Fairfax Business Media  
FairfaxBM | Computerworld | PC World | Reseller News | CIO | JobUniverse  
Advertise with us - Contact us - Newsletters - Subscribe - Privacy

**COMPUTERWORLD**  
The Voice of the ICT Community

RSS

Sunday, 06 April 2008

**Don't click and drag.  
Click and move.**

New Zealand's ICT jobsite

HOME NEWS TECHNOLOGY SECURITY DEVELOPMENT NETWORK & TELCO SPECIAL MANAGEMENT CAREERS E-TALES FRYUP EVENTS

## French Embassy site for Libya said to be serving malware

The French Embassy website for Libya has been compromised and is serving up malware to visitors, according to McAfee.

By Ellen Messmer Framingham | Monday, 17 December, 2007

Email Print

McAfee researcher Francois Paget discovered this on Thursday and the company says it has reported its findings to the French government. The site has been attacked using an [iFrame exploit](#) that inserts an invisible frame in the page in order to re-direct some web browser connections to another location, which serves up a "downloader," code that attempts to reside on the victim machine. If the downloader is successful, the attacker can then remotely attempt to download other malware, "typically a bot or a password-stealing Trojan," says Dave Marcus, McAfee security researcher and communications manager.

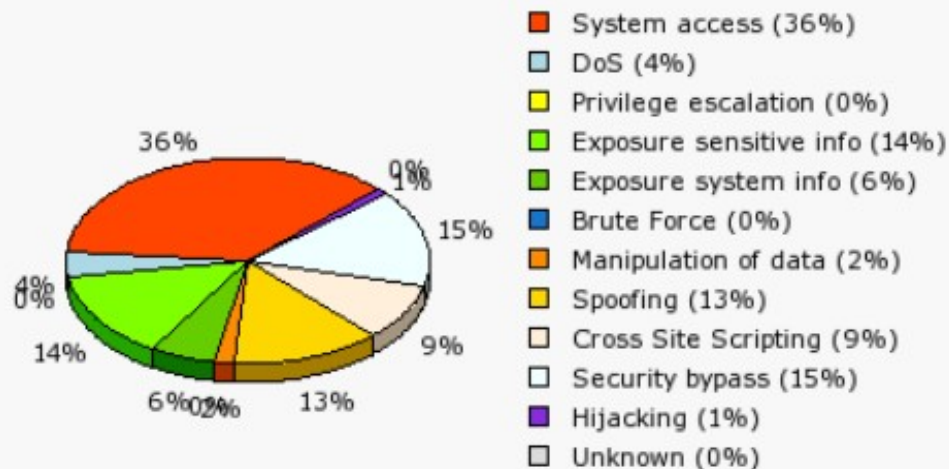
**Most Read**

- Apple's BlackBerry offensive contains some untruths
- Microsoft's ISO win may worsen antitrust woes
- Forum: Bubble bursts for Telecom's business customers
- Last-mile fibre monopoly proposed for broadband

http://inl.adbureau.net/accipiter/adclick/CID=000037d...eid=5526108083/site=CW/area=F.CW.scr (In new window)

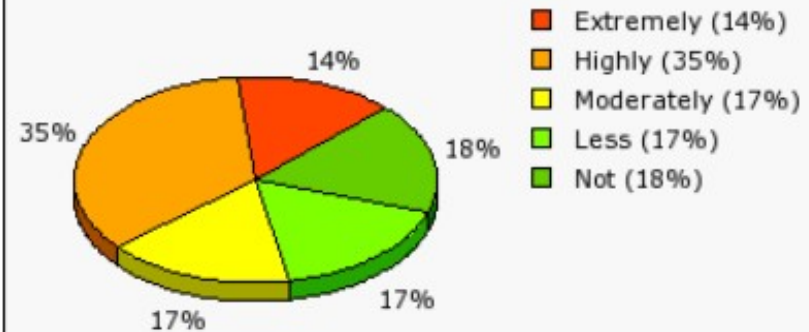
# Krytyczne luki w roli ukrytej funkcjonalności

**Microsoft Internet Explorer 6.x  
Impact (Based on 107 advisories from 2003-2008)**



This graph was generated by Secunia.  
Based on vulnerability information available at <http://secunia.com/>

**Microsoft Internet Explorer 6.x  
Criticality (Based on 107 advisories from 2003-2007)**



This graph was generated by Secunia.  
Based on vulnerability information available at <http://secunia.com/>

źródło: Secunia statistics 31.01.2008r.

# Krytyczne luki w roli ukrytej funkcjonalności

Microsoft Internet Explorer window showing the URL: <http://www.microsoft.com/presspass/features/2003/>

United States | Change | All Microsoft Sites

Search Microsoft.com for:  Go

## PressPass - Information for Journalists

PressPass Home | PR Contacts | Fast Facts About Microsoft | Site Map | Advanced Search | RSS Feeds

### Microsoft News

- Product News
- Consumer News
- International Contacts
- Legal News
- Security & Privacy News
- Events
- News Archive

### Corporate Information

- Microsoft Executives
- Fast Facts About Microsoft
- Image Gallery
- Broadcast Room

### Related Sites

- Analyst Relations
- Community Affairs
- Essays on Technology
- Executive E-Mail
- Global Citizenship

## A Matter of National Security: Microsoft Government Security Program Provides National Governments with Access to Windows Source Code

Q&A: A new Microsoft initiative provides government agencies with the technical information they need to be confident in the security features of the Microsoft Windows platform.

**REDMOND, Wash., Jan. 14, 2003** – As information technology has become increasingly central to our daily lives, computer security and privacy have taken on a growing importance. For national governments, the questions surrounding computing security are especially critical. From protecting personal data about their citizens to safeguarding secret information related to national defense issues, public agencies face a wide range of security issues that have profound social and political implications. That has made the task of implementing secure information technology systems one of the most pressing concerns for national governments.



**Craig Mundie, senior vice president and chief technical officer of advanced**

### Related Links

#### Feature Stories:

- [Trustworthy Computing Continues to Build Momentum](#) - Jan. 13, 2005
- [Microsoft Shared Source Initiative Encourages Academic Innovation](#) - March 27, 2002
- [Nothing Common in "Common Criteria": How Microsoft Customers Can Utilize the Unprecedented Security Recognition Awarded to Windows 2000](#) - Oct. 29, 2002



- Menu
- Home
- News Briefs
- News
- Opinion & Analysis
- Audio
- Video
- Documents
- Featured Articles
- Newsletter Issues
- Letters
- Blog Entries

- Static
- About
- Constitution
- Basic Facts
- Bibliography
- Books
- Links
- Economic Indicators
- What's new?

- Interactive
- Contact Us
- Letter to the Editor
- Sign up for Newsletter
- RSS & Podcasts
- Search

# 50% of Venezuela Government Software will be Open Source by 2007

March 5th 2005, by ABN / Venezuelanalysis.com

Caracas, Venezuela, March 5, 2005– Venezuela’s president of the National Technology and Information Center (CNTI), Jorge Berrizbeitia, says that the migration from private software to free software in Venezuela’s public administration will present a great challenge for the government and the country’s data processing companies.



According to a presidential decree passed in December 2004, Venezuela’s public administration must present a plan within three months for how it will raise its usage of free software. The best known example of free software is the Linux operating system, which is steadily gaining in market share worldwide, relative to the private operating system Microsoft Windows. Following the president’s approval of the plans, the departments of the public administration will have two years to implement it.

Berrizbeitia explained that the Venezuelan government is aware that such a transition will cost money and that it also means transition expenses for the companies that currently supply the government with software. Berrizbeitia said that the government would be willing to take over the costs of translating software, so that it can be used in Venezuela.

One of the main reasons the government is interested in switching to free software is that it wants to consolidate its technological independence and lower its vulnerability for not controlling the software it uses.

- News
- ECONOMY
  - Venezuela To Nationalize Cement Industry in Order to Boost Construction April 5th 2008
- INTERNATIONAL
  - "Perverse Intention" Behind Colombian Rebel Documents Says Venezuelan Foreign Minister April 2nd 2008
- LABOR
  - Venezuelan Steel Workers to Vote on New Contract, Possibly Ending Year-Long Conflict April 1st 2008
- MASS MEDIA
  - Venezuelan Media Terrorism Conference Denounces Negative Role of Private Media April 1st 2008
- ECONOMY
  - Chavez Announces \$3 Billion for Venezuela's "Energy" Revolution March 31st 2008

# Krytyczne luki w roli ukrytej funkcjonalności

Niemiecki szpieg w postaci trojana - Nowe Technologie w INTERIA.PL - Swiftweasel

File Edit View History Bookmarks Tools Help

http://nt.interia.pl/news/niemiecki-szpieg-w-p i trojana site:inte

Getting Started Latest BBC Headli...

**INTERIA.PL** NOWE TECHNOLOGIE

Szukaj w Internecie  szukaj enhanced by Google

» NA KOMÓRKĘ · AGD RTV · FORUM · HALO · WIRUSY · BAZZAR · FOTO · CENTRUM TANICH ROZMÓW · TELEKOM · NA KOMÓRKĘ

Start Komputery Telekomunikacja Internet Foto Audio-Wideo Testy Gadżety Galerie Relacje wideo Tylko u nas

Wiadomości | Mapa serwisu | Newsroom **Specjalne:** HP Pavilion podbija Polskę

## Niemiecki szpieg w postaci trojana

Czwartek, 22 listopada 2007 (10:30)

**Niemiecki rząd rozpoczął rekrutację programistów, których celem będzie stworzenie programu typu malware.**

Celem trojana będzie inwigilowanie komputerów osób podejrzanych o terroryzm. Z propozycją zwiększenia uprawnień przedstawicieli prawa w kwestii dostępu do informacji i możliwości zarażania podejrzanych komputerów wyszedł w tym roku Sąd Federalny.

Geoff Sweeney z Tier-3 obawia się, że konie trojańskie stworzone dla potrzeb rządu czy choćby policji będą mogły w trywialny sposób wpaść w ręce hakerów, którzy rozpowszechniliby je i użyli do "kradzieży" danych osobowych

**zrobie**  Znajdź cel i opisz go. Zrób to co postanowiłeś. Więcej

REKLAMA

smerfne radiowozy!  
i nie tylko

ORMO

zobacz! >>

ubuntu

# Krytyczne luki w roli ukrytej funkcjonalności

The screenshot shows a web browser window with the title "heise online - Austria plans to start conducting secret online searches in 2008 - Konqueror". The address bar contains the URL "http://www.heise.de/english/newsticker/news/97595". The page content includes a navigation menu, a logo for "heise online", a banner for "HEIDELBERGER innovations FORUM", and a news article titled "Austria plans to start conducting secret online searches in 2008". The article text discusses the planned use of online searches by the Austrian police from autumn 2008 onwards, mentioning the Minister of Justice, Maria Berger, and the Minister for Internal Affairs, Günther Platter. A sidebar on the right lists "Latest News" with several headlines.

heise online - Austria plans to start conducting secret online searches in 2008 - Konqueror

Location Edit View Bookmarks Tools Settings Help

http://www.heise.de/english/newsticker/news/97595

heise online - Austria plan...

heise online · ct · iX · Technology Review · Telepolis · mobil · Security · Netze · Open Source · Resale · Foto · Autos · ct-TV · Jobs · Kios

heise online

HEIDELBERGER innovations FORUM

news 18.10.2007 13:56 << Previous | Next >>

## Austria plans to start conducting secret online searches in 2008

It is planned that the police will use online searches in Austria from autumn 2008 onwards. According to a report of the radio station [Ö1](#), the Minister of Justice, Maria Berger (SPÖ) [Social Democratic Party of Austria] and her colleague, the Minister for Internal Affairs, Günther Platter (ÖVP) [Austrian People's Party] have agreed to this. In the station's morning news show called "Morgenjournal" Platter maintained that online searches would only be used in the case of serious crime or suspicion of supporting a terrorist organisation. The law drafted by Platter and Berger is to be discussed today in a cabinet meeting. After that a group of experts will settle the legal and technical details arising from the use of a Trojan program.

As in Germany, the Austrian politicians emphasise the fact that this measure will only be used in exceptional circumstances. According to Minister of Justice Berger, online searches will only be carried out once or twice a year, more or less at the same frequency as phone

Latest News

- [IDF: Intel reveals Nehalem architecture](#)
- [IDF: Intel closer to graphics card production](#)
- [European Patent Office revokes web-to-print patent](#)
- [IDF: Intel says Moore's Law holds until 2029](#)
- [Microsoft extends availability of Windows XP](#)
- [Return of the web bugs](#)
- [IDF: Intel's atomic era](#)
- [Four per cent of](#)

heise  
Security  
Konferen  
2008

# Krytyczne luki w roli ukrytej funkcjonalności

The screenshot shows a web browser window with the title "PC Pro: News: Swiss look to Trojan code for VoIP tapping - Swiftweasel". The address bar shows the URL "http://www.pcpro.co.uk/news/95394/swiss-look-to-troja". The browser's search bar contains "i trojana site:interi". The page content includes a navigation menu with "File", "Edit", "View", "History", "Bookmarks", "Tools", and "Help". Below the browser window, there is a large banner for "PC PRO COMPUTING IN THE REAL WORLD" and "The Ultimate Guide to Windows Vista". The main content area features a search bar, a navigation menu with "NEWS", "PRODUCT REVIEWS", "ANALYSIS", and "INTERACTIVE", and a main article titled "Swiss look to Trojan code for VoIP tapping" dated "Tuesday 10th October 2006". The article text discusses Swiss authorities investigating VoIP tapping and the challenges of decryption. A sidebar on the right contains a "Compare Broadband" section and "Latest News" items.

PC PRO  
COMPUTING IN THE REAL WORLD

The Ultimate Guide to Windows Vista

SEARCH FOR: IN: All IT Sites Search Advanced Search Guest Level 00

NEWS  
Home > News

News [PSUs]  
Tuesday 10th October 2006

Swiss look to Trojan code for VoIP tapping  
1:08PM, Tuesday 10th October 2006

CREDIT CARD AUTHORIZATION  
Date: Member:  
Percent in Full:  
Please visit us as it appears on pp

Swiss authorities are investigating the possibility of tapping VoIP calls, which could involve commandeering ISPs to install Trojan code on target computers.

VoIP calls through software services such as Skype are encrypted as they are passed over the public Internet, in order to safeguard the privacy of the callers.

This presents a problem for anyone wanting to listen in, as they are faced with trying to decrypt the packets by brute force - not easy during a three-minute phone call. What's more, many VoIP services are not based in Switzerland, so the authorities don't have the jurisdiction to force them to hand over the decryption keys or offer access to calls made through these services.

The only alternative is to find a means of listening in at a point before the data is encrypted.

According to the Swiss paper *SonntagsZeitung*, the Swiss Department of the Environment, Transport, Energy and Communications (UVEK) has hired software company ERA IT solutions to design an application to do just this.

Compare Broadband  
Broadband?  
Compare 50+ packages  
Enter your postcode below:  
GO  
Powered by: **TOP 10 broadband**

Latest News  
The week in your words: ISP anger, Phorm fury and BBC  
US Army goes into spam business  
Patch Tuesday promises eight critical updates  
Freeview brings HD at cost of upgrade

# Krytyczne luki w roli ukrytej funkcjonalności

Czarny rynek  
krytycznych luk systemowych



# Krytyczne luki w roli ukrytej funkcjonalności

The screenshot shows a web browser window titled "Mpack attack infects PCs on massive scale - Swiftweasel". The address bar contains the URL "http://www.securityfocus.com/brief/529". The page content includes the SecurityFocus logo, navigation links for "About" and "Advertising", and a "Free Tech Info" section with two articles: "Manage Servers with Group Policy" and "Your credit card methods secure?". Below this is a navigation menu with links for "Home", "Bugtraq", "Vulnerabilities", "Mailing Lists", "Jobs", "Tools", and "Vista". The main content area features a "News" section with a sub-section "Infocus" containing a list of categories like "Foundations", "Microsoft", "Unix", "IDS", "Incidents", "Virus", "Pen-Test", and "Firewalls". The main article is titled "Mpack attack infects PCs on massive scale" and is dated "Published: 2007-06-19". The article text describes a malware distribution and attack kit sold commercially through underground channels, which has compromised hundreds of thousands of systems. It mentions that the software was first mentioned in an analysis by Panda Software in mid-May, which had compromised at least 160,000 computers. A quote from Luis Corrons, technical director of PandaLabs, is included: "Mpack offers the type of features you would expect from a legal application," Luis Corrons, technical director of PandaLabs, said in a previous statement. "For example, client updates. These updates, effectively different versions of the application, are actually the exploits needed to take advantage of the latest vulnerabilities discovered."

# Analiza podatności części software

”We sometimes pay for exploits. An average price for a 0-day Internet Explorer flaw is US\$10,000 in case of good exploitation.”

Źródło:

<http://www.securityfocus.com/news/11476>

Robert Lemos, SecurityFocus 2007-07-20

# Analiza podatności części software

TippingPoint Zero Day Initiative



The Zero Day Initiative (ZDI), founded by TippingPoint, is a program for rewarding security researchers for responsibly disclosing vulnerabilities. Depending on who you are, here are a few links to get you started:

- **Researchers:** Learn [how we pay](#) for your vulnerability discoveries, [register](#) for the ZDI or [login](#).
- **Vendors:** Read our [disclosure policy](#) or join our [security partner program](#)
- **Press, Curiosity Seeker:** [Learn more](#) about ZDI or read answers to some [frequently asked questions](#)

Please contact us at [zdi \[at\] tippingpoint \[dot\] com](mailto:zdi@tippingpoint.com) with any questions or queries. For sensitive e-mail communications, please use our [PGP key](#).

[About](#) | [Upcoming Advisories](#) | [Published Advisories](#) | [Researcher Login](#)

# Analiza podatności części software

**ZDI Rewards Program**

As a member of the ZDI program, you earn points each time a vulnerability submission is purchased. Points are treated in a manner similar to airline frequent flyer miles - points accrue each year on a dollar-for-dollar basis based on the total dollar amount paid for vulnerability submissions by the researcher during that calendar year. For instance, if the Zero Day Initiative buys your vulnerability for \$5,000, then you receive 5,000 points for that submission. For all of calendar year 2008, if you received 37,000 points, then for calendar year 2009 you will be considered to have ZDI Gold status. The following are the various levels of ZDI Reward membership:

ZDI Reward Points	Status
10,000	ZDI Bronze
20,000	ZDI Silver
35,000	ZDI Gold
50,000	ZDI Platinum

Each level offers exclusive awards and benefits, each of which last for the one calendar year period following the year in which the points were earned:

# Jak temu zaradzić

# Jak temu zaradzić

- Random supplier strategy
- Diversification strategy
- Redundancy strategy
- Domestic products

# Jak temu zaradzić

## Random supplier strategy



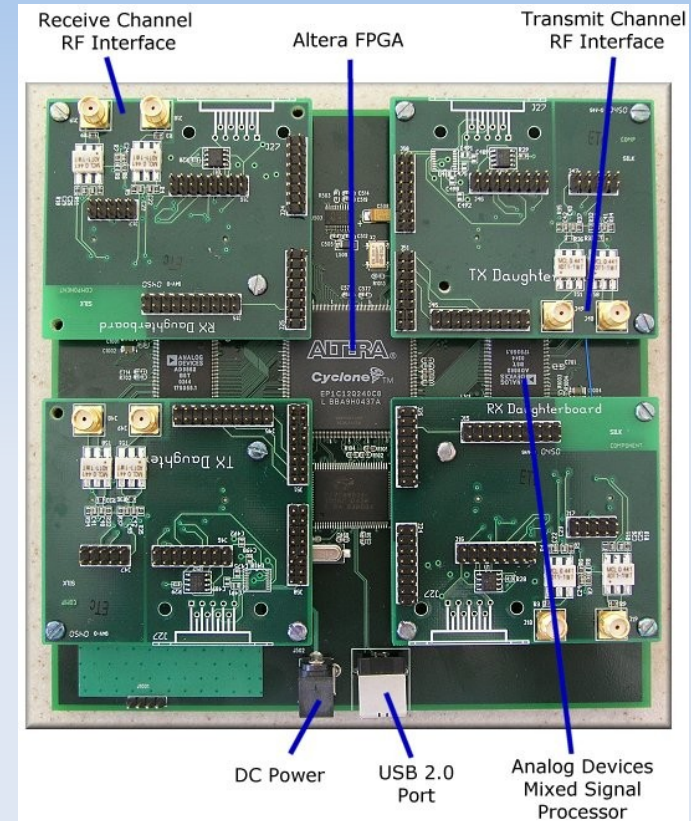
- produkt komercyjny sprzedawany wiadomym odbiorcom

# Jak temu zaradzić

## Random supplier strategy



- produkt komercyjny sprzedawany wiadomym odbiorcom



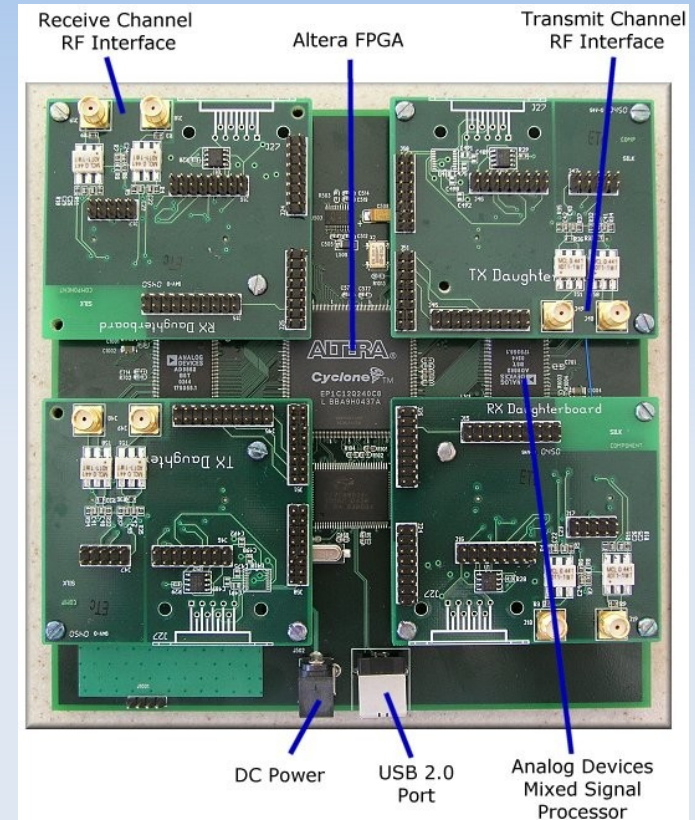
- komputer PC ogólnego przeznaczenia (kupiony w losowo wybranym lub zaufanym sklepie)
- system operacyjny linux
- uniwersalny odbiornik USRP
- oprogramowanie do podsłuchu GSM typu free software



# Jak temu zaradzić Random supplier strategy



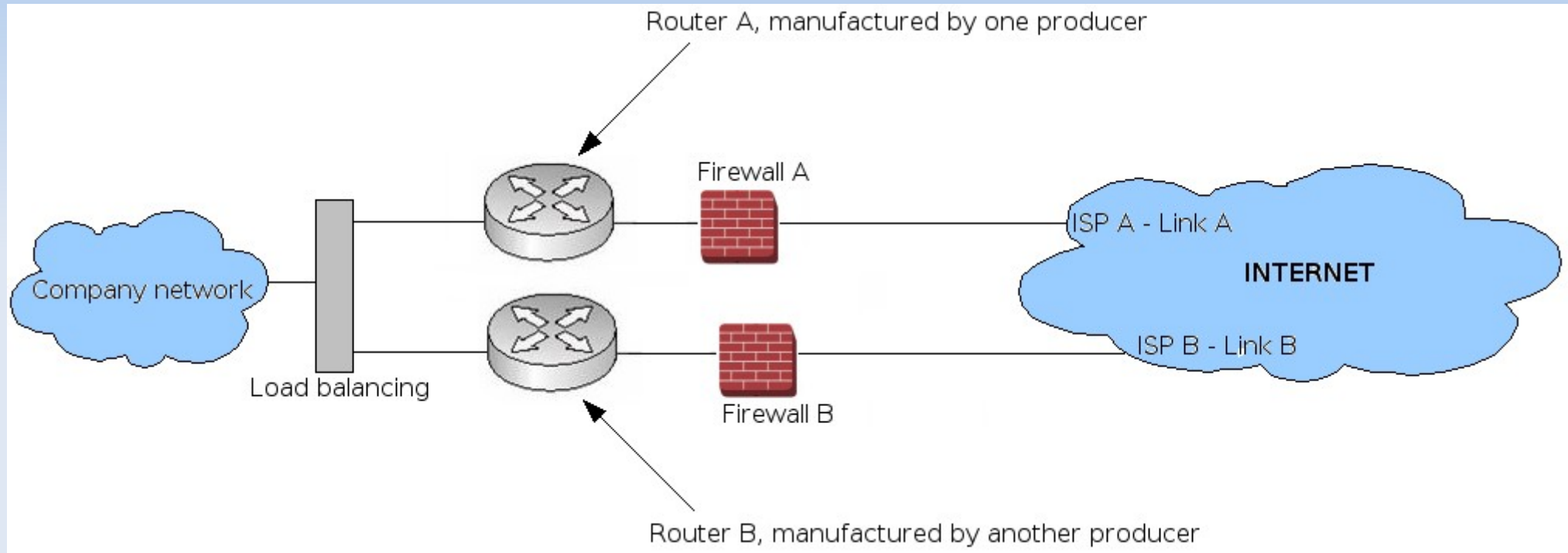
Producent dobrze zdaje sobie sprawę z tego, że sprzęt będzie użytkowany przez służby specjalne i może mieć interes w umieszczeniu tam ukrytej funkcjonalności.



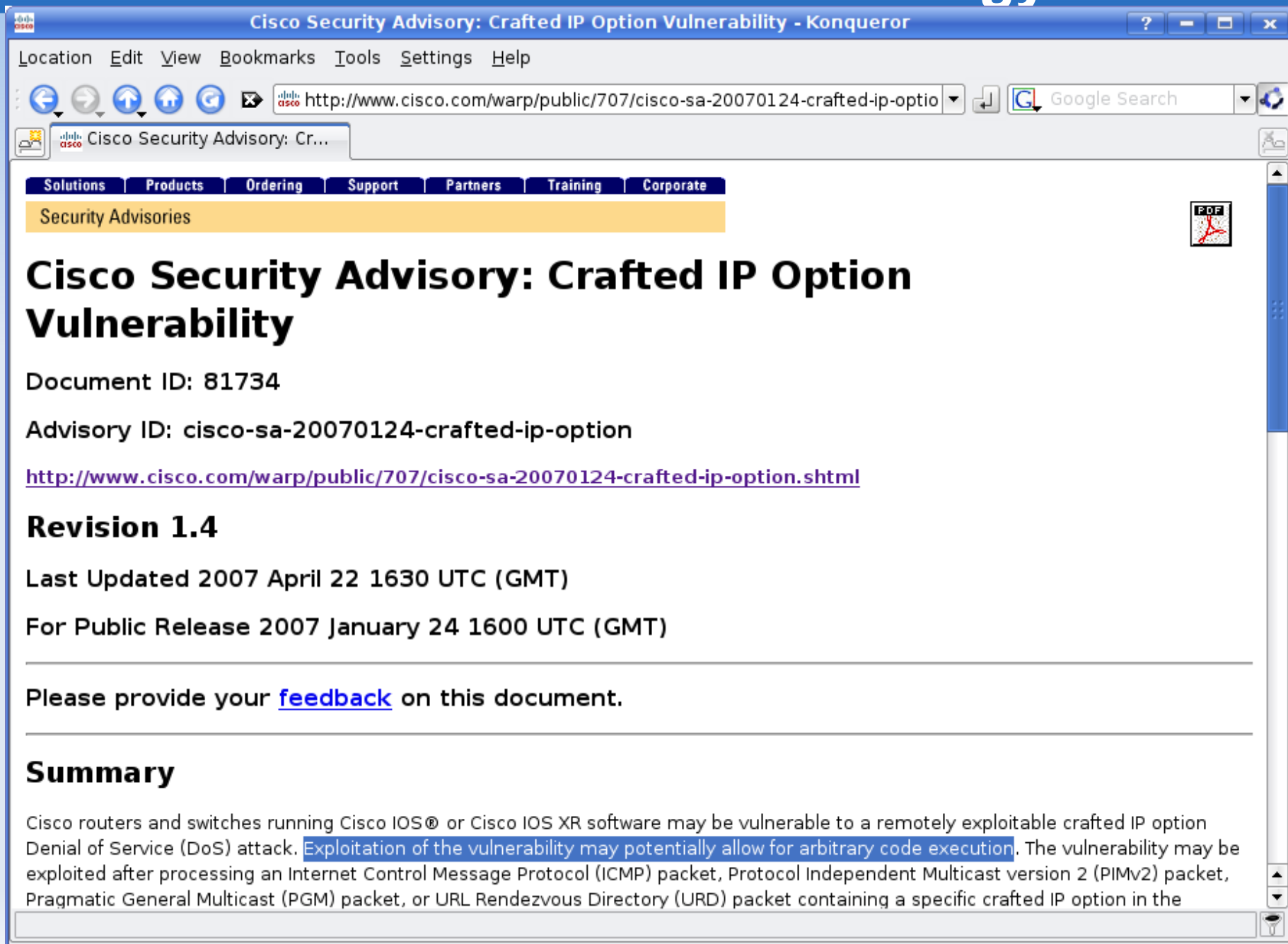
Nikt nie wie, jakim urządzeniem będzie kupowany sprzęt i kto będzie jego użytkownikiem

# Jak temu zaradzić

## Diversification strategy

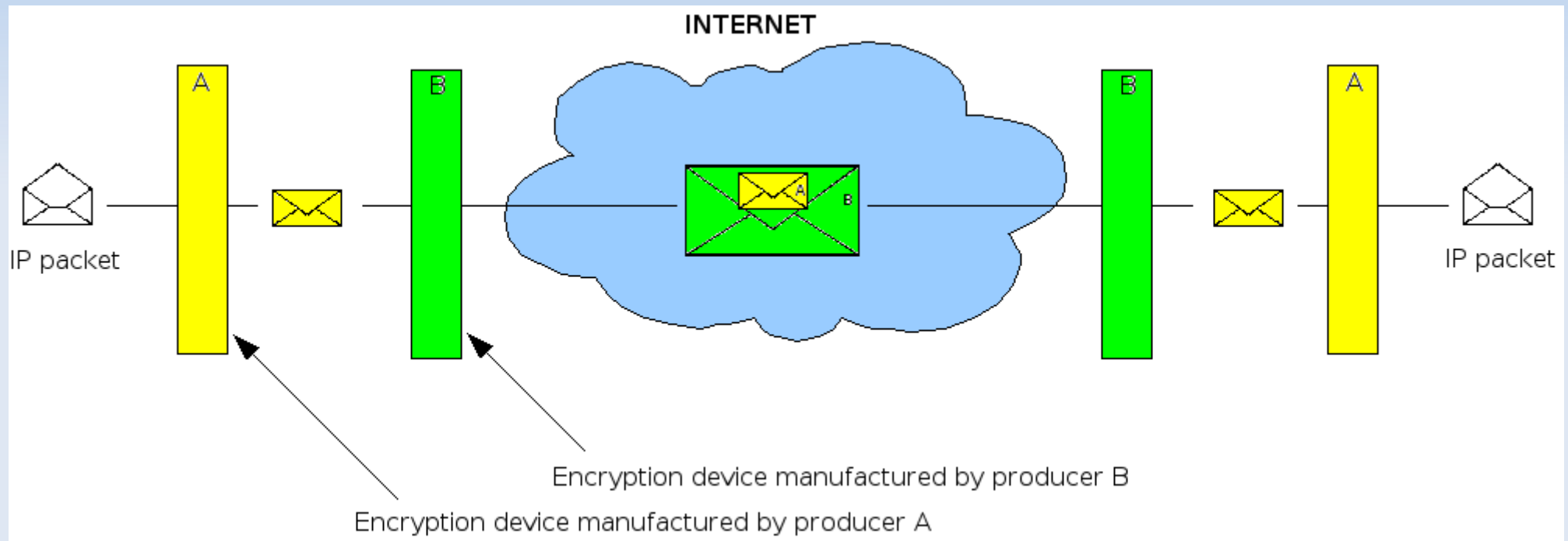


# Jak temu zaradzić Diversification strategy



The image shows a screenshot of a web browser window. The title bar reads "Cisco Security Advisory: Crafted IP Option Vulnerability - Konqueror". The address bar shows the URL "http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-optio". The page content includes a navigation menu with "Solutions", "Products", "Ordering", "Support", "Partners", "Training", and "Corporate". Below this is a "Security Advisories" section. The main heading is "Cisco Security Advisory: Crafted IP Option Vulnerability". Below the heading, it lists "Document ID: 81734" and "Advisory ID: cisco-sa-20070124-crafted-ip-option". A link is provided: "http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml". The section "Revision 1.4" is followed by "Last Updated 2007 April 22 1630 UTC (GMT)" and "For Public Release 2007 January 24 1600 UTC (GMT)". A request for feedback is included: "Please provide your [feedback](#) on this document." The "Summary" section begins with: "Cisco routers and switches running Cisco IOS® or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. [Exploitation of the vulnerability may potentially allow for arbitrary code execution](#). The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the

# Jak temu zaradzić Redundancy strategy



# Jak temu zaradzić Redundancy strategy

For years US eavesdroppers could read encrypted messages without the least difficulty - Swiftweasel

File Edit View History Bookmarks Tools Help

http://www.inteldaily.com/?c=169&a=4686

Getting Started Latest BBC Headli...

The Intelligence daily  
In service to the world

Home About Shop Writers RSS Links Email us

World Economy Geopolitics Energy Intelligence Defense / Security Sex Trade Trafficking Sci/Tech Society Analysis Commentary

Ads by Google

**CRYPTO-BOX USB Dongle**  
Software Protection, License Mgt. Remote Update for Win, Linux & Mac  
www.cryptotech.com

**WWII Crypto Museum**  
Photos, manuals, and more! Enigma, M-209, M-94  
www.ilord.com

**Museum Ludwig Hotels**  
Hotels near Museum Ludwig cologne Pay at check-in. No booking fees.  
www.priceline-europe.com

**Travel & Travel to Iran**  
Ultimate source of travel to Iran Hotels, Tours, Visa,

Home > Intelligence > Reports

Sat, 29 Dec 2007 04:02:00

Email this Print this PDF version

## For years US eavesdroppers could read encrypted messages without the least difficulty

By Ludwig De Braeckeleer

(OhMyNews) -- For decades, the US National Security Agency (NSA) has been reading effortlessly ultra sensitive messages intercepted from all parts of the world. This extraordinary feat was not the consequence of the work of some genius cyber mathematician. Nor was it the result of the agency dominance in the field of super computers, which allegedly have outpaced their most direct rivals by orders of magnitude. The truth is far simpler and quite troubling. The game was rigged.

**More News**

- US jobless figures: The specter of a new...
- Protesters attacked at Bucharest NATO summit
- Haiti: Thousands protest over growing hunger
- Sudan, Ethiopia, and the American Empire
- Has America Overcome Segregation?

See what  
Watch the  
the truth  
cruel  
the factor  
with the  
Re  
Adv  
Make  
ama buntu

# Jak temu zaradzić Domestic products

The screenshot shows a web browser window with the title "People's Daily Online -- Lenovo releases China's first security chip - Swiftweasel". The address bar shows the URL "http://english.peopledaily.com.cn/200504/12/eng:". The page content includes the "People's Daily Online" logo, a navigation menu with categories like "China", "World", and "Opinion", and a main article titled "Lenovo releases China's first security chip". The article text discusses the development of the "Hengzhi" chip and its approval by the State Encryption Administration. A sidebar on the right contains a "Recommendation" section with links to "China Forum", "PD Newsletter", and "Most Popular", as well as a "Related News" section with links to "Intel unveils new 64-bit chip" and "Chipmaker claims IPR violation".

People's Daily Online -- Lenovo releases China's first security chip - Swiftweasel

File Edit View History Bookmarks Tools Help

http://english.peopledaily.com.cn/200504/12/eng: Google

Getting Started Latest BBC Headli...

人民网 English  
People's Daily Online

» Newsletter  
» Weather  
» Community

English home Forum Photo Gallery Features Newsletter Archive About US Help Site Map languages

China  
World  
Opinion  
Business  
Sci-Edu  
Culture/Life  
Sports  
Photos

Services

- Newsletter
- Online Community
- China Biz Info
- News Archive
- Feedback
- Voices of Readers
- Weather Forecast

RSS Feeds

- China XML
- Business XML
- World XML

Home >> Sci-Edu UPDATED: 15:22, April 12, 2005

## Lenovo releases China's first security chip

Lenovo Group on Monday in Beijing released China's first security chip - "Hengzhi" which has been approved by the State Encryption Administration and independently developed by the company.

It means that China's information security-sensitive departments in the government, military and research institutions can now purchase safe PCs independently developed and controlled by Chinese.

According to relevant regulations the design, development and manufacture of China's encryption chips must rely on independent domestic ability and are forbidden from using relevant foreign products.

Safe Lenovo PCs installed with Hengzhi chips will provide security-sensitive departments in the government, military and research institutions with PC terminals completely developed and controlled by Chinese.

As learned Lenovo will officially launch safe PCs installed with Hengzhi security chips within this year.

*By People's Daily Online*

Recommendation

- China Forum
- PD Newsletter
- People's Comment
- Most Popular

Related News

- Intel unveils new 64-bit chip
- Chipmaker claims IPR violation
- China develops new AV chip

Online marketplace of  
Find Suppliers

Done

# Jak temu zaradzić

## Domestic products

According to relevant regulations the design, development and manufacture of China's encryption chips must rely on independent domestic ability and are forbidden from using relevant foreign products.