

Segurança e Controles

- Armas
- Automóveis
- Internet

Armas de fogo

- venda livre - compra nem tanto

Armas de fogo

- venda livre - compra nem tanto
- registro

Armas de fogo

- venda livre - compra nem tanto
- registro
- licença para porte

Armas de fogo

- venda livre - compra nem tanto
- registro
- licença para porte
- controle ocasional

Armas de fogo

- venda livre - compra nem tanto
- registro
- licença para porte
- controle ocasional
- proposta: proibição

Armas de fogo

- venda livre - compra nem tanto
- registro
- licença para porte
- controle ocasional
- proposta: proibição
 - (0 X 1 Brasil)

Armas de fogo

- venda livre - compra nem tanto
- registro
- licença para porte
- controle ocasional
- proposta: proibição
 - (0 X 1 Brasil)
- razão: segurança

Automóveis

- venda e compra livre

Automóveis

- venda e compra livre
- registro

Automóveis

- venda e compra livre
- registro
- licença "de porte"

Automóveis

- venda e compra livre
- registro
- licença "de porte"
- proposta: chips para monitoramento

Automóveis

- venda e compra livre
- registro
- licença "de porte"
- proposta: chips para monitoramento
- razão: segurança

Internet

- provimento e acesso livre (em alguns países)

Internet

- provimento e acesso livre (em alguns países)
- sem registro oficial

Internet

- provimento e acesso livre (em alguns países)
- sem registro oficial
- controle nenhum (em alguns países?)

Internet

- provimento e acesso livre (em alguns países)
- sem registro oficial
- controle nenhum (em alguns países?)
- propostas: várias formas de monitoramento

Internet

- provimento e acesso livre (em alguns países)
- sem registro oficial
- controle nenhum (em alguns países?)
- propostas: várias formas de monitoramento
- razão: segurança

Problemas levantados

Uso da rede para

- atividades caracterizadas como crimes
 - Crimes reais, envolvendo dinheiro
 - Crimes virtuais, envolvendo propriedade intelectual
- Atividades que deveriam ser crimes

Problemas levantados

Uso da rede para

- atividades caracterizadas como crimes
 - Crimes reais, envolvendo dinheiro
 - Crimes virtuais, envolvendo propriedade intelectual
- Atividades que deveriam ser crimes

Possível uso:

- computadores para atividades ilegais
- rede para atividades ilegais

Ataque legal

- EUA: proibido possuir alguns tipos de softwares

Ataque legal

- EUA: proibido possuir alguns tipos de softwares
 - Antes: proibido exportar criptografia



WIKIPEDIA
The Free Encyclopedia

Wikipedia is sustained by people like you. Please **donate** today.


Sign in / create account

article discussion edit this page history

Ten things you may not know about Wikipedia

Export of cryptography

From Wikipedia, the free encyclopedia

 The examples and perspective in this article or section may not represent a **worldwide view** of the subject.
Please [improve this article](#) or discuss the issue on the [talk page](#).

navigation

- [Main page](#)
- [Contents](#)
- [Featured content](#)
- [Current events](#)
- [Random article](#)

interaction

- [About Wikipedia](#)
- [Community portal](#)
- [Recent changes](#)
- [Contact Wikipedia](#)
- [Donate to Wikipedia](#)
- [Help](#)

search

toolbox

- [What links here](#)
- [Related changes](#)
- [Upload file](#)
- [Special pages](#)
- [Printable version](#)
- [Permanent link](#)

The **export of cryptography** refers to the transfer from one country to another of devices and technology related to [cryptography](#). Since [World War II](#), Western governments, including the [U.S.](#) and its [NATO](#) allies, have regulated the export of cryptography for national security considerations, and, for a time, defined cryptography to be a [munition](#).

In light of the enormous impact of [cryptanalysis in WWII](#), it was abundantly clear to these governments that denying current and potential enemies access to cryptographic systems looked to be militarily valuable. They also wished to monitor the diplomatic communications of other nations, including the many new nations that were emerging in the [post-colonial period](#) and whose position on [Cold War](#) issues was regarded as vital. (Kahn, [The Codebreakers](#), Ch. 19) Since the U.S. and U.K. had, they believed, developed more advanced cryptographic capabilities than others, there arose a notion that controlling *all* dissemination of the more effective crypto techniques might be beneficial.^[*citation needed*] The [First Amendment](#) made controlling all use of cryptography inside the U.S. difficult, but controlling access to U.S. developments by others was thought to be more practical — there were at least no constitutional impediments. Accordingly, regulations were introduced as part of [munitions](#) controls which required licenses to export cryptographic methods (and even their description); the regulations established that cryptography beyond a certain strength (defined by algorithm and length of [key](#)) would not be licensed for export except on a case-by-case basis. The expectation seems to have been that this would further national interests in reading 'their' communications and prevent others from reading 'ours'. This policy was also adopted elsewhere for various reasons.

The development, and public release, of [DES](#) and [asymmetric key](#) techniques in the [1970s](#), the rise of the [Internet](#), and the willingness of some to risk and resist prosecution, eventually made this policy impossible to enforce, and by the late 1990s it was being relaxed in the US, and to some extent (e.g. France) elsewhere. Nevertheless, some officials in the [U.S.](#) believe that widespread availability of strong [cryptography](#) world-wide has hampered the ability of the [NSA](#) to read intercepted communications that might reveal important information about intentions hostile to the United States.^[1] Others feel that the export controls in place in the last half of the 20th century discouraged incorporation of widely known cryptographic tools into commercial products, particularly [personal computer operating systems](#), and are a root cause of the present crisis in [information security](#), aside from interfering with U.S. trade in such products. They observe that many of the

Ataque legal

- EUA: proibido possuir alguns tipos de softwares
 - Antes: proibido [exportar criptografia](#)
 - Hoje: proibido decodificar ([DMCA](#))

Your *continued donations* keep Wikipedia running!

Sign in / create account

- article
- discussion
- edit this page
- history

Find out more about navigating Wikipedia and finding information



WIKIPEDIA
The Free Encyclopedia

navigation

- Main page
- Contents
- Featured content
- Current events
- Random article

interaction

- About Wikipedia
- Community portal
- Recent changes
- Contact Wikipedia
- Donate to Wikipedia
- Help

search

Search input field with Go and Search buttons

toolbox

- What links here
- Related changes
- Upload file
- Special pages
- Printable version
- Permanent link

Digital Millennium Copyright Act

From Wikipedia, the free encyclopedia
(Redirected from [DMCA](#))

The **Digital Millennium Copyright Act (DMCA)** is a [United States copyright law](#) which implements two 1996 [WIPO](#) treaties. It criminalizes production and dissemination of technology, devices, or services that are used to [circumvent](#) measures that control access to copyrighted works (commonly known as [DRM](#)) and criminalizes the act of circumventing an access control, even when there is no infringement of copyright itself. It also heightens the penalties for copyright infringement on the [Internet](#). Passed on [October 8, 1998](#) by a unanimous vote in the United States Senate and signed into law by President [Bill Clinton](#) on [October 28, 1998](#), the DMCA amended title 17 of the [U.S. Code](#) to extend the reach of copyright, while limiting the liability of Online Providers from [copyright infringement](#) by their users.

On [May 22, 2001](#), the [European Union](#) passed the [EU Copyright Directive](#) or EUCD, similar in many ways to the DMCA.

Contents [hide]

- 1 Provisions
 - 1.1 DMCA Title I: WIPO Copyright and Performances and Phonograms Treaties Implementation Act
 - 1.2 DMCA Title II: Online Copyright Infringement Liability Limitation Act
 - 1.3 DMCA Title III: Computer Maintenance Competition Assurance Act
 - 1.4 DMCA Title IV: Miscellaneous Provisions
 - 1.5 DMCA Title V: Vessel Hull Design Protection Act
- 2 Exemptions
- 3 Reform and opposition
- 4 Criticisms
 - 4.1 Example of DMCA Takedown Provision



Digital Millennium Copyright Act

Full title	To amend title 17, United States Code, to implement the World Intellectual Property Organization Copyright Treaty and Performances and Phonograms Treaty, and for other purposes.
Acronym / colloquial name	DMCA
Enacted by the	105th United States Congress
Effective	October 28, 1998
Citations	
Public Law	Pub. L. 105-304
U.S. Statutes at	112 Stat. 2860 (1998)

Ataque legal

- EUA: proibido possuir alguns tipos de softwares
 - Antes: proibido [exportar criptografia](#)
 - Hoje: proibido decodificar ([DMCA](#))
- **Proposta no Brasil: registro detalhado de tudo por 5 anos, [quase tudo é crime](#)**



Realização e Apoio:

English

+ HOME +

Realização FGV DIREITO RIO

- + WeBlog
- + O Projeto
- + A2K e a Sociedade
- + A2K e o Governo
- + A2K internacional
- + Estudos e Artigos
- + Eventos
- + Fale Conosco
- + Pesquisadores / Colaboradores

Arquivos Weblog

- outubro de 2007
- setembro de 2007
- agosto de 2007
- julho de 2007
- junho de 2007
- maio de 2007
- abril de 2007
- março de 2007
- fevereiro de 2007
- janeiro de 2007
- dezembro de 2006
- novembro de 2006
- outubro de 2006
- setembro de 2006
- agosto de 2006
- julho de 2006
- junho de 2006
- maio de 2006

WEBLOG



- VOLTAR PARA O WEBLOG -

+O PROJETO DE LEI DO SENADOR EDUARDO AZEREDO E SEUS CUSTOS PARA O BRASIL

Internet brasileira precisa de marco regulatório civil
terça-feira 22 de maio de 2007

www.diretorio.fgv.br/cts

O projeto de lei de crimes virtuais do senador Eduardo Azeredo (PSDB-MG) propõe que o primeiro marco regulatório da Internet brasileira seja criminal. Enquanto isso, o caminho natural de regulamentação da rede, seguido por todos os países desenvolvidos, é primeiramente estabelecer um marco regulatório civil, que defina claramente as regras e responsabilidades com relação a usuários, empresas e demais instituições acessando a rede, para a partir daí definir uma regras criminais.

A razão para isso é a questão da inovação. Para inovar, um país precisa ter regras civis claras, que permitam segurança e previsibilidade nas iniciativas feitas na rede (como investimentos, empresas, arquivos, bancos de dados, serviços etc.). As regras penais devem ser criadas a partir da experiência das regras civis. Isso de cara eleva o custo de investimento no setor e desestimula a criação de iniciativas privadas, públicas e empresariais na área.

Isso acontece especialmente pela abrangência e incertezas geradas pelo projeto, que usa conceitos vagos e amplos ("dados", "sistemas de comunicação" e outros) para regular um assunto que demanda discussão técnica prévia, que ainda não foi feita no país.

Prova disso é que a Convenção de Cibercrimes, que é citada como "inspiração" para o projeto de lei, não foi assinada por nenhum país latino-americano e nem pela maioria absoluta dos países em desenvolvimento (contam-se nos dedos os países pobres que assinaram a convenção). Os países ricos, sigantários da convenção, já fizeram seu dever de casa de regulamentar a Internet do ponto de vista civil e, somente depois disso, estabeleceram os parâmetros criminais para a rede. O Brasil está seguindo a via inversa: está criando primeiro punições criminais, sem antes regulamentar técnica e civilmente a Internet.

Ataque legal

- EUA: proibido possuir alguns tipos de softwares
 - Antes: proibido [exportar criptografia](#)
 - Hoje: proibido decodificar ([DMCA](#))
- Proposta no Brasil: registro detalhado de tudo por 5 anos, [quase tudo é crime](#)

Privilegia a ação policial, contra o uso normal

Segurança de software

- [Aberto X fechado](#)



WIKIPEDIA
The Free Encyclopedia

Help us provide free content to the world by **donating today!**

- [article](#)
- [discussion](#)
- [edit this page](#)
- [history](#)

Ten things you may not know about images on Wikipedia

Security through obscurity

From Wikipedia, the free encyclopedia

In [cryptography](#) and [computer security](#), **security through obscurity** (sometimes **security by obscurity**) is a controversial principle in [security engineering](#), which attempts to use [secrecy](#) (of design, implementation, etc.) to provide [security](#). A system relying on security through obscurity may have theoretical or actual security vulnerabilities, but its owners or designers believe that the flaws are not known, and that attackers are unlikely to find them. The technique stands in contrast with [security by design](#), although many real-world projects include elements of both strategies.

Contents [hide]

- [Literature review](#)
- [Arguments against](#)
- [Arguments for](#)
- [Historical notes](#)
- [Notes](#)
- [See also](#)
- [External links](#)

Literature review [\[edit\]](#)

There is scant formal literature on the issue of security through obscurity. Books on [security engineering](#) will cite [Kerckhoffs' doctrine](#) from 1883, if they cite anything at all. For example, in a discussion about secrecy and openness in Nuclear Command and Control:^[1]

[T]he benefits of reducing the likelihood of an accidental war were considered to outweigh the possible benefits of secrecy. This is a modern reincarnation of Kerckhoffs' doctrine, first put forward in the nineteenth century,^[2] that the security of a system should depend on its key, not on its design remaining obscure.

In the field of legal academia, Peter Swire has written about the trade off between the notion that "security through obscurity is an illusion" and the military notion that "loose lips sink ships"^[3] as well as how competition affects the incentives to disclose.^[4]

navigation

- [Main page](#)
- [Contents](#)
- [Featured content](#)
- [Current events](#)
- [Random article](#)

interaction

- [About Wikipedia](#)
- [Community portal](#)
- [Recent changes](#)
- [Contact Wikipedia](#)
- [Donate to Wikipedia](#)
- [Help](#)

search

toolbox

- [What links here](#)
- [Related changes](#)
- [Upload file](#)
- [Special pages](#)
- [Printable version](#)
- [Permanent link](#)

Segurança de software

- [Aberto X fechado](#)
- FUD: código aberto sujeito a ataques ([IE X Mozilla](#))



Where Technology Means Business

Members login | Site Assistance | Newsletters | RSS Feeds

- HOME
- NEWS**
- BLOGS
- WHITE PAPERS
- DOWNLOADS
- REVIEWS

- Security
- Networking
- Hardware
- Software
- Web Technology
- IT Management
- OSes
- Photo Galleries
- All News

home / ZDNet news

Security

SEARCH GO

Symantec: Mozilla browsers more vulnerable than IE

By Tom Espiner, News.com
Published on ZDNet News: Sep 19, 2005 8:10:00 PM



SHARE
 PRINT
 E-MAIL
 WORTHWHILE?
 0 VOTES

Tags: [Tom Espiner](#)

Mozilla Web browsers are potentially more vulnerable to attack than Microsoft's Internet Explorer, according to a Symantec report.

But the report, released Monday, also found that hackers are still focusing their efforts on IE.

The open-source Mozilla Foundation browsers, such as the popular Firefox, have typically been seen as more secure than IE, which has suffered many security problems in the past. Mitchell Baker, president of the foundation, said earlier this year that its browsers were fundamentally more secure than IE. She also predicted that Mozilla Foundation browsers would not face as many problems as IE, even as their market share grows.

LATEST SECURITY CONTENT

- MVP awards, Messenger Plus! and adware -- a good combination?
- Malware being spammed as PDF from retail stores
- So what about user education on security?
- Is Zango stealing affiliate commissions from adult webmasters?
- Edelman on 'Deceptive Door Openers' and Ask toolbars

[Subscribe to Feed](#)

From our sponsors

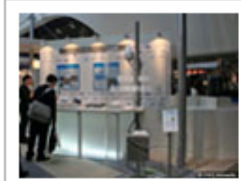
The office politics playbook



You don't need dirty tricks, but you do need to know the rules. Use these techniques to get what you

Hot Spot
What's Important

Mobile Broadband



Gallery: Scenes at Ceatec (Japan)
A WiMax antenna from carrier KDDI.
[View all images >](#)

Turn Your Wireless Modern Into a Wi-Fi Access Point
[Read the post](#)
on BNET's Business

Segurança de software

- [Aberto X fechado](#)
- FUD: código aberto sujeito a ataques ([IE X Mozilla](#))
- **real: código fechado sendo atacado**

Segurança de software

- [Aberto X fechado](#)
- FUD: código aberto sujeito a ataques ([IE X Mozilla](#))
- real: código fechado sendo atacado
- FUD: mais problemas de segurança em linux ([ou igual](#))

Aberdeen Group says Linux/UNIX is as vulnerable as Windows

by John McCormick | Jan 6, 2003

Tags: Cyberthreats, Operating systems, Viruses and worms, John McCormick, LINUX/UNIX, Aberdeen Group Inc., virus, CERT, Unix, trojan horse, Microsoft Windows



E-MAIL SAVE PRINT DIGG THIS WORTHWHILE? 5 VOTES

Takeaway: Read how an Aberdeen report claims that Linux/UNIX is not more secure than Windows, despite common assumptions.

Turning up the heat up another notch on a long-simmering debate, the Aberdeen Group has published a study comparing the security of Linux/UNIX systems with that of the Microsoft Windows family of products.

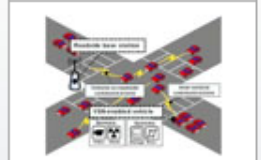
"Contrary to popular misperception, Microsoft does not have the worst track record when it comes to security vulnerabilities. Also contrary to popular wisdom, UNIX- and Linux-based systems are just as vulnerable to viruses, Trojan horses, and worms."

Ad Feedback Fast Color Laser Printers and All-In-Ones Starting around \$399 brother

TechRepublic Featured Jobs

Hot Spot What's Important

Car Tech



Turning cars into wireless network nodes Read the post >

How hydrogen cars work Could hydrogen cars become the next popular hybrid vehicle? Watch the video >

From our sponsors OnStar treatment Buick

Tiger Woods gets it. Unlock gets Tiger back into his Buick. The OnStar treatment can

Segurança de software

- Aberto X fechado
- FUD: código aberto sujeito a ataques (IE X Mozilla)
- real: código fechado sendo atacado
- FUD: mais problemas de segurança em linux (ou igual)
- **real: Critérios como gravidade, possibilidade de exploração**



Ads by Google

<p>Cheap Dedicated Server 99.99% uptime, starts @ \$99 24/7 support, order now www.Qualispace.com</p>	<p>Free Download LogMeIn is Top for IT Consultants Free Remote Access to Support PCs www.LogMeIn.com</p>	<p>Secret Satellite TV on PC Shocking discovery they don't want you to know. www.secretsatellite.com</p>	<p>USB Spartan 3 FPGA Boards With programmer's API for Windows & Linux. High speed USB 2.0 interface www.opalkelly.com</p>
--	---	---	---

[The Register](#) » [Security](#) »

Security Report: Windows vs Linux



An independent assessment

By [Nicholas Petreley](#) → [More by this author](#)

Published Friday 22nd October 2004 07:26 GMT

Jobsite - find your next IT job quickly & easily

[Executive Summary](#)

[Busting The Myths](#)

[Myth: There's Safety In Small Numbers](#)

[Myth: Open Source is Inherently Dangerous](#)

[Myths: Conclusions Based on Single Metrics](#)

[Windows vs. Linux Design](#)

[Windows Design](#)

Ads by Google

CRYPTO-BOX USB Dongle
Copy Protection, License Management Remote Update for Win, Linux & Mac
www.cryptotech.com

CompTIA Certification
CompTIA Certification Training Now Available Online. Free Info Online!
www.CertificationTrainingOnline.com

Free UML 2.1 Design Tool
Visually develop applications with Roundtrip model to code,

Search

[Reg Hardware](#)

[Reg Developer](#)

[Channel Register](#)

[Whitepapers](#)

News Tools

[Newsletters & Feeds](#)

[Reg Mobile](#)

[Reg Desktop News Alerts](#)

[US Edition](#)

Reg Shops

[Reg Merchandise](#)

[Reg Books](#)

[Mobile Gadgets](#)