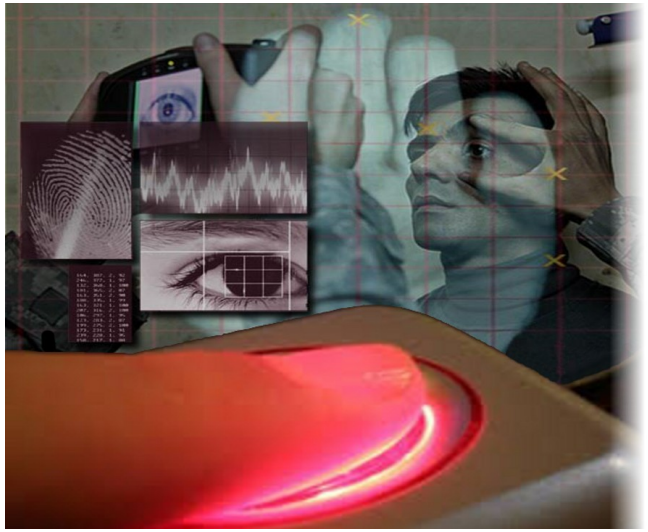


Seminário sobre Proteção à Privacidade

CGI.BR – São Paulo, setembro 2015

Criptografia, Segurança e Identidade Digital

Questões e Tendências – semiológicas, geopolíticas

Pedro A. D. Rezende

Ciência da Computação - Universidade de Brasília

pedro.jmrezende.com.br/sd.php

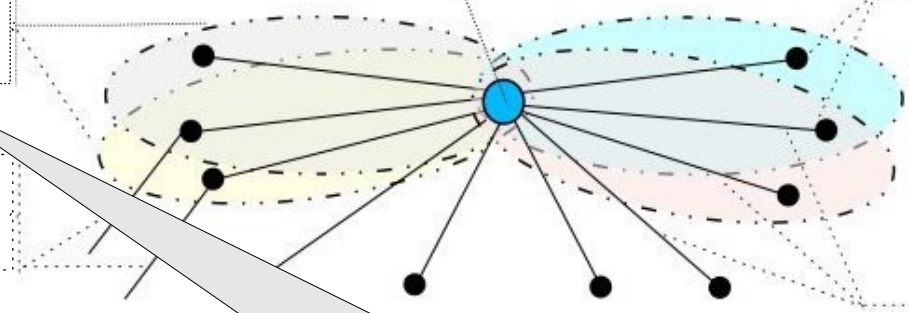
Identidade e Privacidade
Uma abordagem semiológica

Mundo da vida

Entidade Alguém, algum Ente

Identidades
i.e., **Papéis Sociais**

Comunicação
Elos semiológicos



Representações internas de outros entes

Atributos, relações ou competências

Identidade é mera projeção, que fixa carcaterísticas que são fluidas e mutáveis de um indivíduo

Inspirado em Muniz Sodré Cabral

"Claros e Escuros – identidade, povo e mídia no Brasil" (Ed. Vozes, 1999)

O que é Privacidade?
Uma definição semiológica

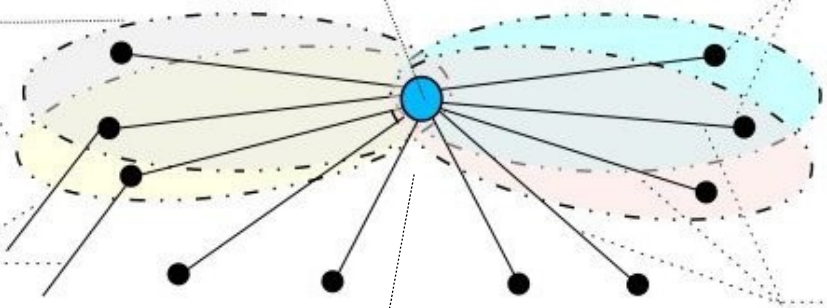
Mundo da vida

Entidade Alguém, algum Ente

Identidades
i.e., Papéis Sociais

Comunicação
Elos semiológicos

Privacidade
Separabilidade de papéis sociais:
Capacidade de exercer os seus
de forma autonôma ou livre



Representações internas de outros entes

Atributos, relações ou competências

Inspirado em Roger Clarke (Australian National University)
http://www.rogerclarke.com/DV/IdAuthFundas.html

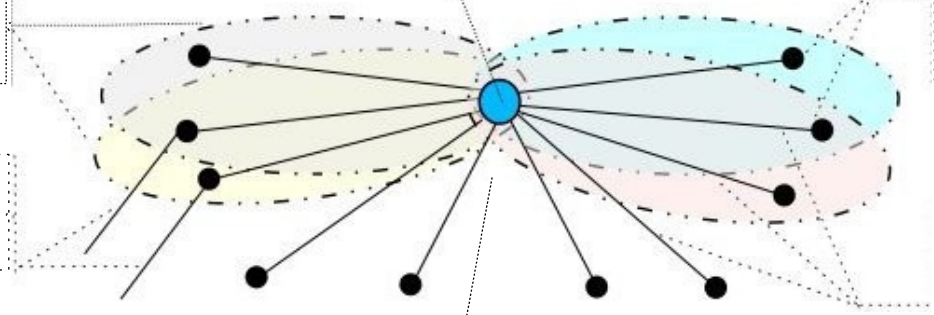
O que é Privacidade?
Uma definição semiológica

Mundo da vida

Entidade Alguém, algum Ente

Identidades
i.e., Papéis Sociais

Comunicação
Elos semiológicos



Representações internas de outros entes

Atributos, relações ou competências

Privacidade
Separabilidade de papéis sociais:
Capacidade de exercer os seus de forma autonôma ou livre

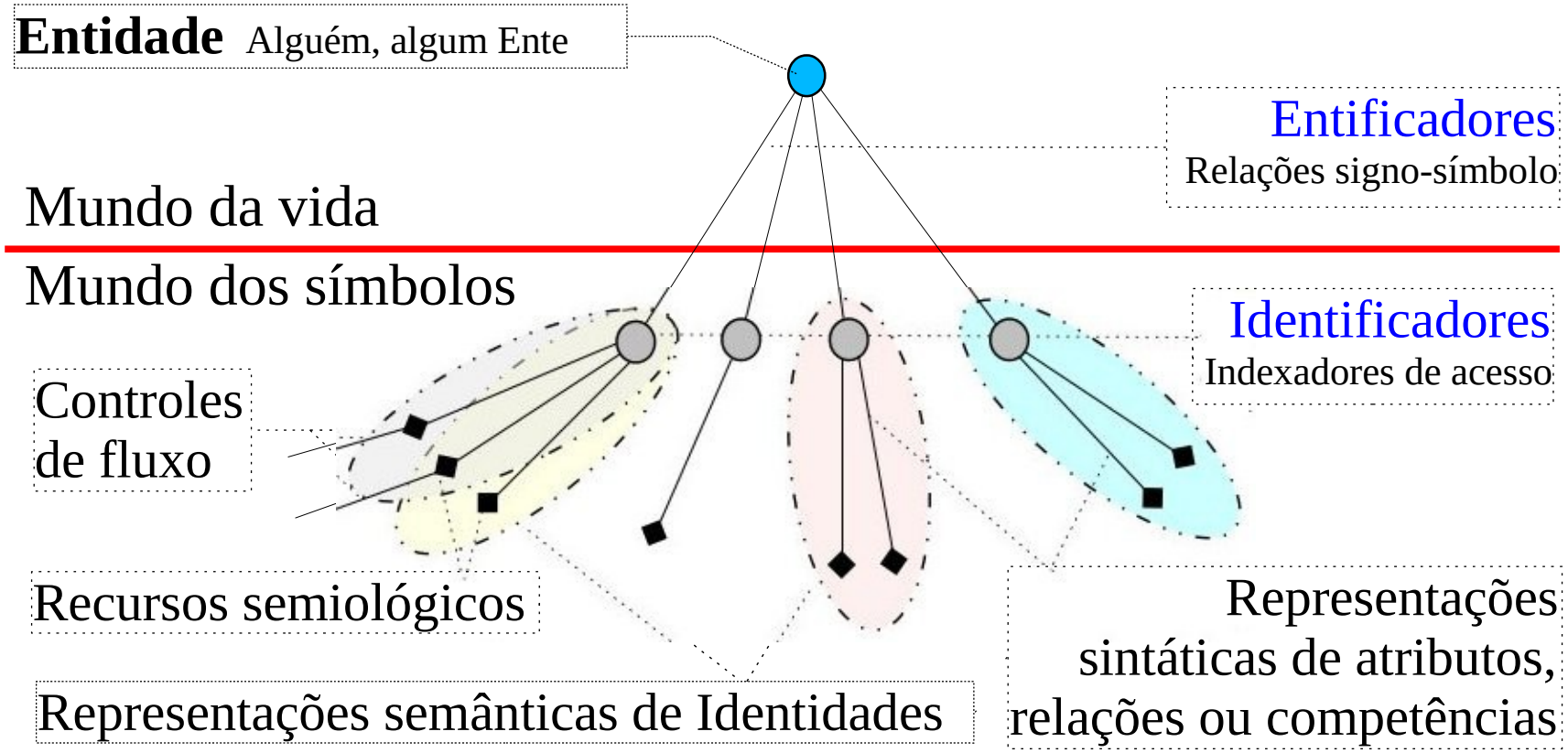
Manifestação semiológica do instinto de auto-preservação

Inspirada em Roger Clarke (ANU) e Piotr Pisarewicz (UnB)

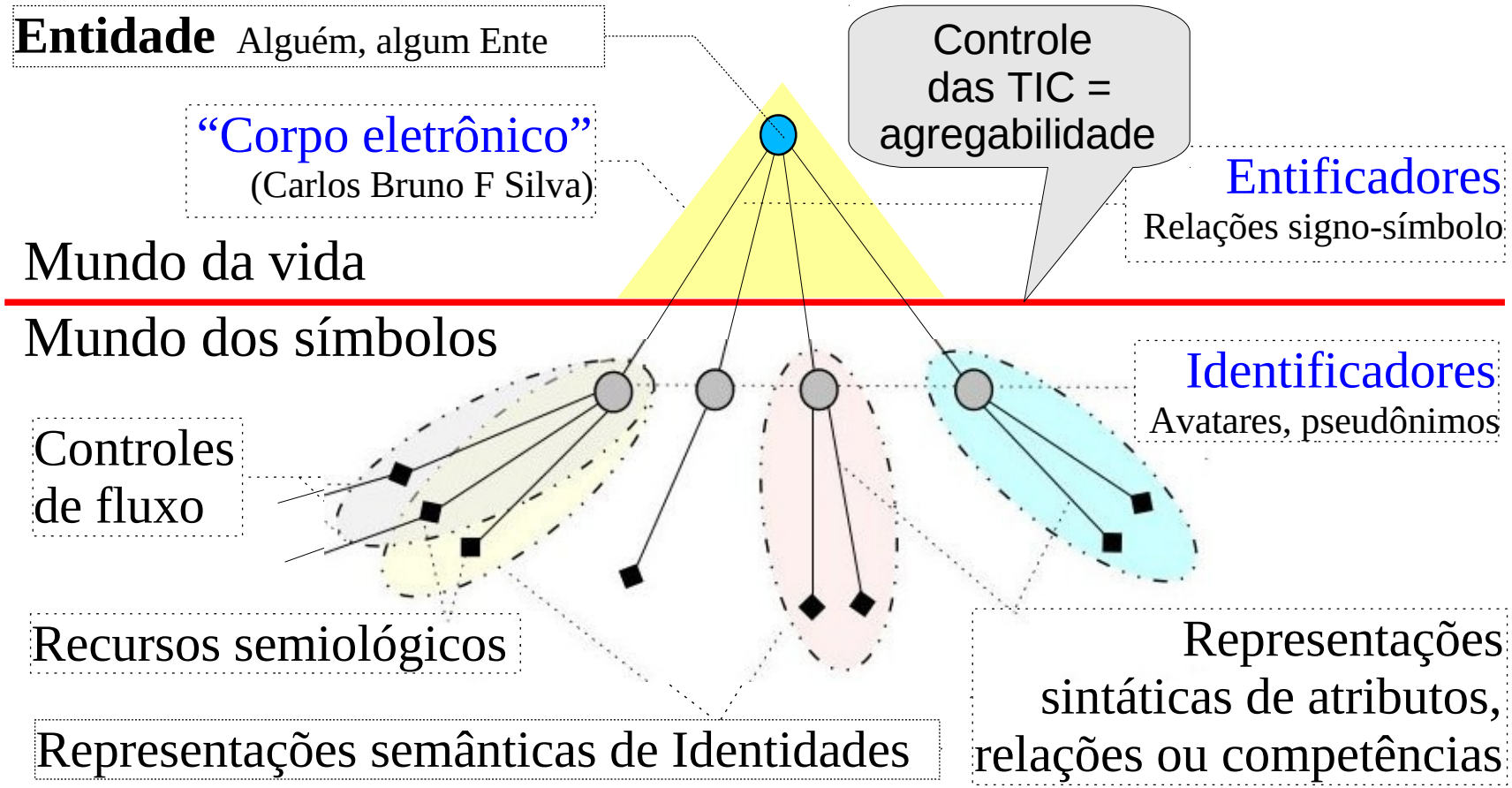
http://www.rogerclarke.com/DV/IdAuthFundas.html

http://pedro.jmrezende.com.br/trabs/PrivacidadePiotr.pdf

Pivacidade na esfera digital
sob erosão cultural



Privacidade é protegível?
sob imersão digital?

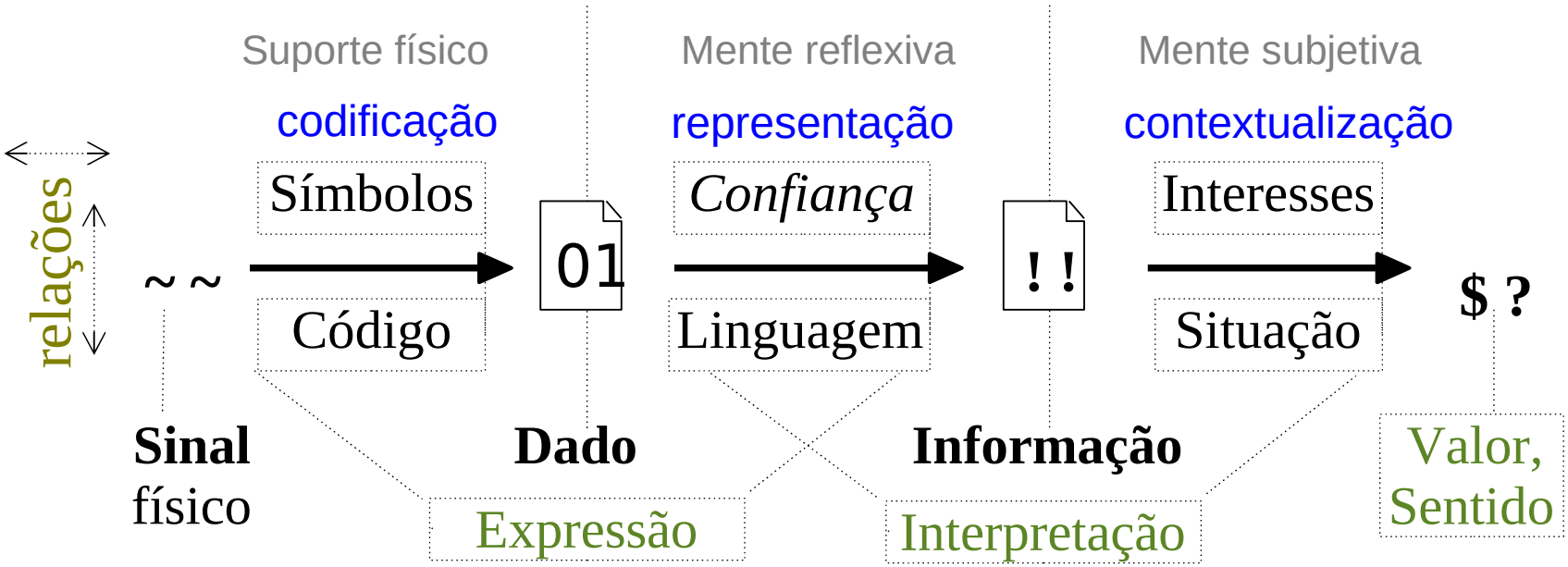


Rezende, P. A. D.: "Modelos de Confiança para Segurança em Informática"

Pesquisa em andamento pedro.jmrezende.com.br/trabs/modelos_de_confianca.pdf

Dado, informação e conhecimento

Como se produzem significados na comunicação

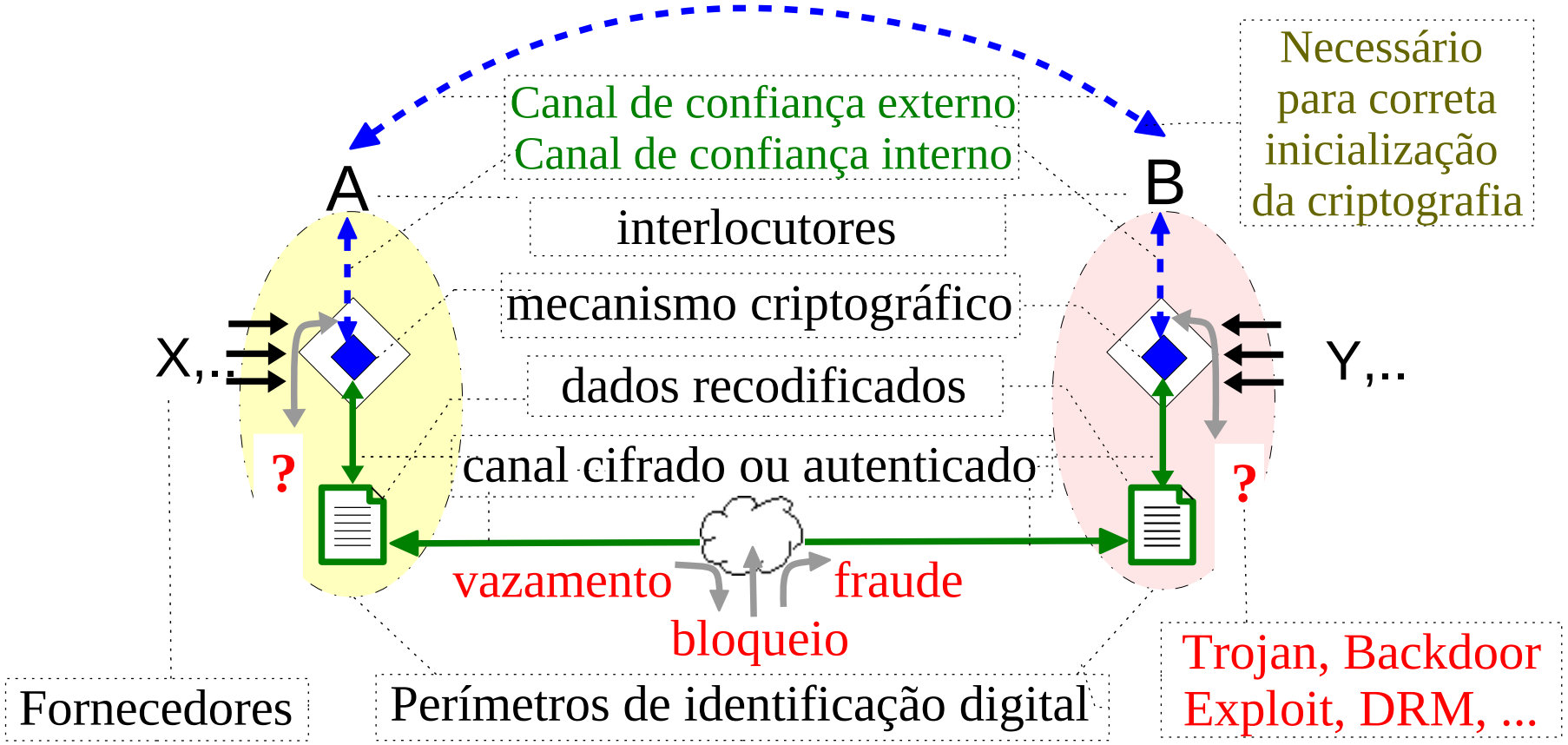


Informação (Shannon, 1948): Aquilo que é *transferido* de uma fonte a um destino através de um *canal de comunicação*, medido em termos de probabilidade do que *não é antecipável*, em relação ao que *pode ser esperado e entendido* do contexto pelo receptor (mudança no *estado de conhecimento*).

Confiança (Gerk, 1997): Aquilo que é *essencial* para um canal de comunicação e que *não pode ser transferido* da fonte para o destino *através deste canal*. (essencial para a informação *fazer sentido*).

Segurança Computacional

Contextualização para uso eficaz de criptografia



Canais laterais (de confiança internos) vulneráveis podem tornar o mecanismo criptográfico ineficaz

Identificação digital
A criptografia e/ou a certificação são panacéias?

Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices

Nadia Heninger[†*] Zakir Durumeric[‡*] Eric Wustrow[‡] J. Alex Halderman[‡]

[†] *University of California, San Diego*
nadiah@cs.ucsd.edu

[‡] *The University of Michigan*
{zakir, ewust, jhalderm}@umich.edu

Abstract

RSA and DSA can fail catastrophically when used with malfunctioning random number generators, but the extent to which these problems arise in practice has never been comprehensively studied at Internet scale. We perform the largest ever network survey of TLS and SSH servers and present
widespread.
keys due to
and we susp
faulty imple
promise. Even more alarmingly, we are able to obtain RSA private keys for 0.50% of TLS hosts and 0.03% of SSH hosts,
common fa
vate keys fo

expect that today's widely used operating systems and server software generate random numbers securely. In this paper, we test that proposition empirically by examining the public keys in use on the Internet.

The first component of our study is the most comprehensive Internet-wide survey to date of two of the most
and SSH (Sec-
address space,
rtificates from
SSH host keys
ore TLS hosts
than the latest released EFF SSL Observatory dataset [20]. Our techniques take less than 24 hours to scan the entire
than 96 hours
ive us a macro-

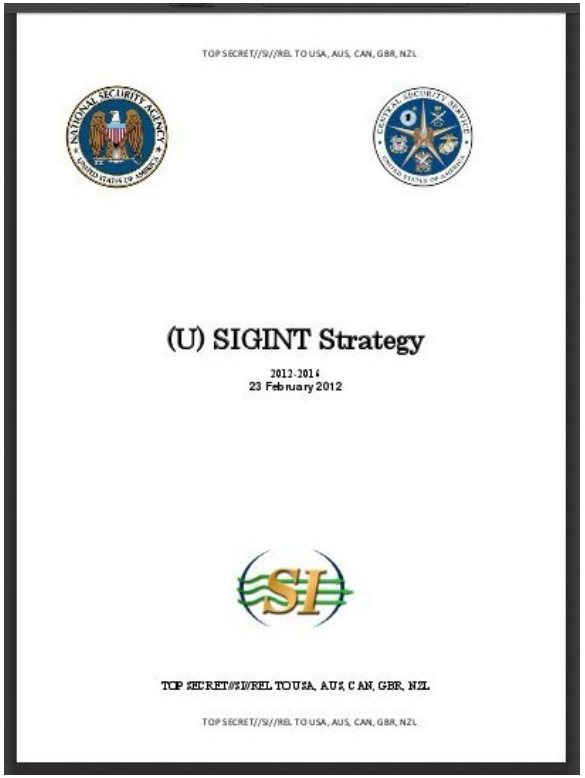
we present evidence that vulnerable keys are surprisingly widespread. We find that 0.75% of TLS certificates share keys due to insufficient entropy during key generation,

Even more alarmingly, we are able to obtain RSA private keys for 0.50% of TLS hosts

https://factorable.net/

Cerco tecnológico – agências de 3 letras

SIGINT (Signals Intelligence) - Planejamento 2012-2016 (5 Olhos):



https://s3.amazonaws.com/s3.documentcloud.org/documents/838324/2012-2016-sigint-strategy-23-feb-12.pdf

Vazado para o Wikileaks - Destaque para:

"2.1.3. (TS//SI//REL) *Enfrentar softwares de criptografia domésticos ou alheios atingindo suas bases industriais com nossas capacidades em inteligência de sinais (SIGINT) e humanas*"

"2.1.4. (TS//SI//REL) *Influenciar o mercado global de criptografia comercial por meio de relações comerciais e pessoais de inteligência, e por meio de parceiros diretos e indiretos."*

"2.2. (TS//SI//REL) *Derrotar as práticas de segurança cibernética adversárias para obtermos os dados que precisamos, de qualquer um, a qualquer momento, em qualquer lugar.*"

Cerco tecnológico – agências de 3 letras

www.kaspersky.com/about/news/virus/2015/equation-group-the-crown-creator-of-cyber-espionage

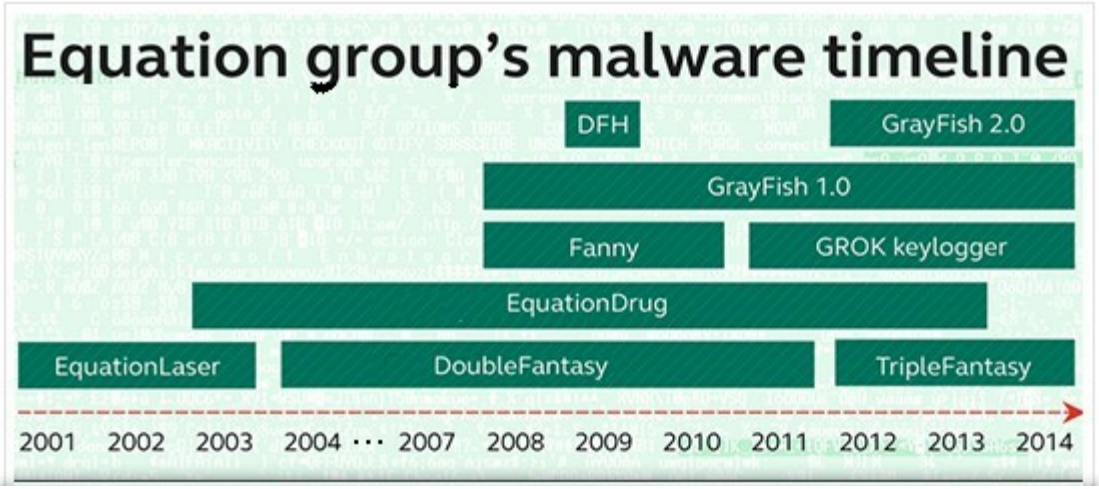
Home → About Us → Corporate News → Malware → 2015 → Equation Group: The Crown Creator of Cyber-Espionage

KASPERSKY lab

16 Feb 2015
Virus News

Equation Group: The Crown Creator of Cyber-Espionage

For several years, Kaspersky Lab's Global Research and Analysis Team (GReAT) has been closely monitoring more than 60 advanced threat actors responsible for cyber-attacks worldwide. The team has seen nearly everything, with attacks becoming increasingly complex as more nation-states got involved and tried to arm themselves with the most advanced tools. However, only now Kaspersky Lab's experts can confirm they have discovered a threat actor that surpasses anything known in terms of complexity and sophistication of techniques, and that has been active for almost two decades – The Equation Group.



Feb 2015: Grupo único em quase todos aspectos: complexidade dos *malwares*, técnicas de infecção, *stealth*, extração sobre *air gap*, etc.

Kaspersky lab recuperou módulos que permitem re-programar o *firmware* de HDs e *pendrives* dos doze maiores fabricantes, talvez a mais poderosa arma para vigilantismo global no arsenal desse grupo (talvez o mesmo grupo que desenvolveu o Stuxnet e seus derivados)

ww.kaspersky.com/about/news/virus/2015/equation-group-the-crown-creator-of-cyber-espionage

Estamos em Ciberguerra?

- A ciberguerra é (pode ser entendida como) uma forma de **Contrarrevolução Digital**.

cujo paradigma é:

"Como pode ser a virtualização destrutível"

Pela ideologia neoliberal, como em J. Schumpeter, vivemos uma era – histórica – de “destruição criativa” (em “*Capitalismo, Socialismo e Democracia*”, 1942)

Como surge a Ciberguerra?
da (r)evolução cibernética

Evolução da Cibernética

Ciclo Década	Inovação principal	Paradigma: Como pode ser...
1940	Arquiteturas	a máquina programável?
1950	Transistores	a programação viável?
1960	Linguagens	a viabilidade útil?
1970	Algoritmos	a utilidade eficiente?
1980	Redes	a eficiência produtiva?
1990	Internet	a produtividade confiável?
2000	Cibercultura	a confiança virtualizável?
2010	Ciberguerra	a virtualização destrutível?

Dados pessoais ou sensíveis?

Alvos de *drones* selecionados sem identificação pessoal,
apenas pelo padrão de comportamento minerado do vigilantismo global

rt.com/usa/cia-drone-strikes-unknown-targets-293

Classified documents reveal CIA drone strikes often killed unknown people

Published time: June 06, 2013 03:36
Edited time: June 07, 2013 05:47

A review of classified US intelligence records has revealed that the CIA could not confirm the identity of about a quarter of the people killed by drone strikes in Pakistan from 2010 to 2011.

One key term in analyzing drone strike records are what are known as *"signature"* strikes, when drones kill suspects based on behavior patterns but without positive identification, versus *"personality"* strike, One former senior intelligence official said that at the height of the drone program in Pakistan in 2009 and 2010, as many as half of the strikes were classified as signature strikes.

Northrop Grumman / Chad Slattery / Handout via Reuters

Colapso econômico, *Reset* e Lei marcial

Vários eventos financeiros atuais – QEs, ZIRP, AIIB, Grexit, SDR, etc – indicam importante redefinição nos rumos do nosso futuro.

Agentes do poder vão fazer tudo a seu alcance para adiar um colapso, e nisso estão sendo pró-ativos (por enquanto, nos bastidores).

O mundo está sufocado em dívida intransponível; se nada for feito, o cenário se desdobra em hiperinflação global. O resultado desse novo rumo inclui desagregação e caos; Quando o desabastecimento e a desobediência civil dispararem e o caos social se espallhar, governos se tornarão ditatoriais na tentativa de salvarem a si mesmos. Alguns acreditam que operaçõ-es como *Jade Helm 15* servem de **preparo para um *reset* financeiro**

modernsurvivalblog.com/current-events-economics-politics/the-crash-the-reset-martial-law-by-this-time-next-year

Megacibercrime e *reset* financeiro

International New York Times

The Opinion Pages | EDITORIAL

Banks as Felons, or Criminality Lite

By THE EDITORIAL BOARD MAY 22, 2015

As of this week, Citicorp, JPMorgan Chase, Barclays and Royal Bank of Scotland are felons, having pleaded guilty on Wednesday to criminal charges of conspiring to rig the value of the world's currencies. According to the Justice Department, the lengthy and lucrative conspiracy enabled the banks to pad their profits without regard to fairness, the law or the public good.

Besides the criminal label, however, nothing much has changed for the banks. And that means nothing much has changed for the public.

http://www.nytimes.com/2015/05/23/opinion/banks-as-felons-or-criminality-lite.html
http://investmentwatchblog.com/market-manipulation-can-and-does-happen-for-very-long-times

Para adiar hiperinflação do dólar, 'estímulos' seletivos de crédito-como-moeda geram bolhas e fraudes que tornam a crise e colapso inevitáveis. Evitadas por enquanto com chantagem, ameaça militar e *regime change*.

Tendências

Um conselho de guerra cibernética formado pela Casa Branca e os maiores bancos do mundo – como quer ex-diretor da NSA – consolidaria o fascismo (conforme definido por Mussolini) como regime de um protogoverno global

Arquitetura de Opressão

- “Um Estado totalitário realmente eficiente seria um no qual os todo-poderosos mandantes da política e seus exércitos de executivos controlam uma população de escravizados que não precisam ser coagidos, porque eles adoram a sua servidão."

- “*A really efficient totalitarian state would be one in which the all-powerful executive of political bosses and their army of managers control a population of slaves who do not have to be coerced, because they love their servitude*.”

— Aldous Huxley, em “Admirável Mundo Novo”,