Modelos de Confiança para Segurança em Informática

Pedro A. D. Rezende

Ciência da Computação – UnB

Apresentação produzida para um Curso de Especialização em Gestão de Segurança da Informação e Comunicações

Texto de referência: Relatório de pesquisa publicado em

http://cic.unb.br/~rezende/trabs/modelos_de_confianca.pdf

Modelos de Confiança para Segurança em Informática

Investigam-se:

Elementos psicossociais que atuam no processo de segurança *e* no teatro da segurança;

Modelos de Confiança para Segurança em Informática

Investigam-se:

Elementos psicossociais que atuam no processo de segurança *e* no teatro da segurança;

Como esses elementos se constituem e se aplicam em Modelos de Confiança para segurança em informática;

Modelos de Confiança para Segurança em Informática

Investigam-se:

Elementos psicossociais que atuam no processo de segurança *e* no teatro da segurança;

Como esses elementos se constituem e se aplicam em Modelos de Confiança para segurança em informática;

Como esses modelos exploram fronteiras de confiança, as quais podem ser rastreadas em análise de riscos;

Modelos de Confiança para Segurança em Informática

Investigam-se:

- Elementos psicossociais que atuam no processo de segurança *e* no teatro da segurança;
- Como esses elementos se constituem e se aplicam em Modelos de Confiança para segurança em informática;
- Como esses modelos exploram fronteiras de confiança, as quais podem ser rastreadas em análise de riscos;
- Como esses rastros nos permitem abordar conflitos de interesse, estendendo e integrando outras modelagens

Modelos de Confiança para Segurança em Informática

Investigam-se:

Elementos psicossociais que atuam no processo de segurança *e* no teatro da segurança;

Como esses elementos se constituem e se aplicam em Modelos de Confiança para segurança em informática;

Como esses modelos exploram fronteiras de confiança, as quais podem ser rastreadas em análise de riscos;

Como esses rastros nos permitem abordar conflitos de interesse, estendendo e integrando outras modelagens

Por meio de uma abordagem semiológica, seguindo a definição de Confiança proposta por Gerck (1997).

Modelos de Confiança para Segurança em Informática

Conteúdo

I– Introdução;

II – Criptografia e a Arte da Guerra;

III– O que é Confiança?

IV– Modelando Confiança;

V– Encadeando Modelos de Confiança;

VI– Conclusão

I - Introdução

I.1– Práticas Sociais

Laços (elos), Engajamentos, Métodos

I.2– O Teatro da Segurança

Dualidade, Externalidade, Calibres

I.3– Cenários e Papéis

Mercado, Fornecedor, Consumidor, Estado

I.1– Práticas Sociais

O que significa isso?

I.1– Práticas Sociais

Possibilidades de conflito de interesses entre

- os que desenvolvem e fornecem Tecnologias de Informação e Comunicação (TIC),
- os que precisam de proteção contra seu uso indevido,
- os que competem entre si por um desses objetivos,
- os que fazem isso por meios ou para fins escusos,

I.1– Práticas Sociais

Possibilidades de conflito de interesses entre

- os que desenvolvem e fornecem Tecnologias de Informação e Comunicação (TIC),
- os que precisam de proteção contra seu uso indevido,
- os que competem entre si por um desses objetivos,
- os que fazem isso por meios ou para fins escusos,

Conflitos que se tornam elementos cada vez mais cruciais e decisivos no *processo da segurança*.

I.1– Práticas Sociais

O que significa isso?

Exercício 1 ao final do Texto de Referência

I.2– O Teatro da Segurança

o que significa isso?

I.2– O Teatro da Segurança

Pela falta de calibres aferíveis entre processo (plano externo) e sentimento (plano interno), vivemos aquilo que o criptógrafo Bruce Schneier chama de *teatro da segurança*, onde:

- encenam-se relações entre os planos externo e interno da segurança;
- no enredo: riscos, mecanismos de proteção, percepção destes;
- no cenário: “neutralidade” das TIC ou de aplicações, outros memes;
- sentimento ingênuo contribui para interação e propagação de riscos.

I.2– O Teatro da Segurança

Pela falta de calibres aferíveis entre processo (plano externo) e sentimento (plano interno), vivemos aquilo que o criptógrafo Bruce Schneier chama de *teatro da segurança*, onde:

- encenam-se relações entre os planos externo e interno da segurança;
- no enredo: riscos, mecanismos de proteção, percepção destes;
- no cenário: "neutralidade" das TIC ou de aplicações, outros memes;
- sentimento ingênuo contribui para interação e propagação de riscos.

Nesse contexto, observamos gastos crescentes com o processo de segurança, em paralelo a perdas crescentes com incidentes.

Ex: www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

I.3– Cenários e Papeis

“Alice e Bob”

I.3– Cenários e Papeis

Alice e Bob: Agentes principais de uma comunicação digital;
No atual contexto sociopolítico do teatro da segurança, onde se encena a tecnologia como bem em si mesmo, tende-se a crer:

1. Que o valor de uso das TIC supera, no geral, riscos embutidos, tornando inexorável a virtualização de práticas sociais;
2. Que o mercado deve regular o uso das TIC ... exceto quando algum interesse concentrador é atingido.
3. Que os efeitos indiretos ou de segunda ordem em perfis de riscos decorrentes de 1. e 2. se racionalizam.

I.3– Cenários e Papeis

Alice e Bob: Agentes principais de uma comunicação digital;
No atual contexto sociopolítico do teatro da segurança, onde se encena a tecnologia como bem em si mesmo, tende-se a crer:

1. Que o valor de uso das TIC supera, no geral, riscos embutidos, tornando inexorável a virtualização de práticas sociais;
2. Que o mercado deve regular o uso das TIC ... exceto quando algum interesse concentrador é atingido.
3. Que os efeitos indiretos ou de segunda ordem decorrentes de 1. e 2. sobre perfis de riscos se racionalizam.

Qualquer outra abordagem para segurança “da informação” é desdenhada como “ideológica”.

I.3– Cenários e Papeis

Como agentes principais desempenham seus papéis?

“Alice e Bob”: Exercício 2 ao final do T. de Referência

II – Criptografia e Arte da Guerra

II.1– Sun Tsu: “Conheça teu inimigo”

Dado, Informação, Valores, Interesses

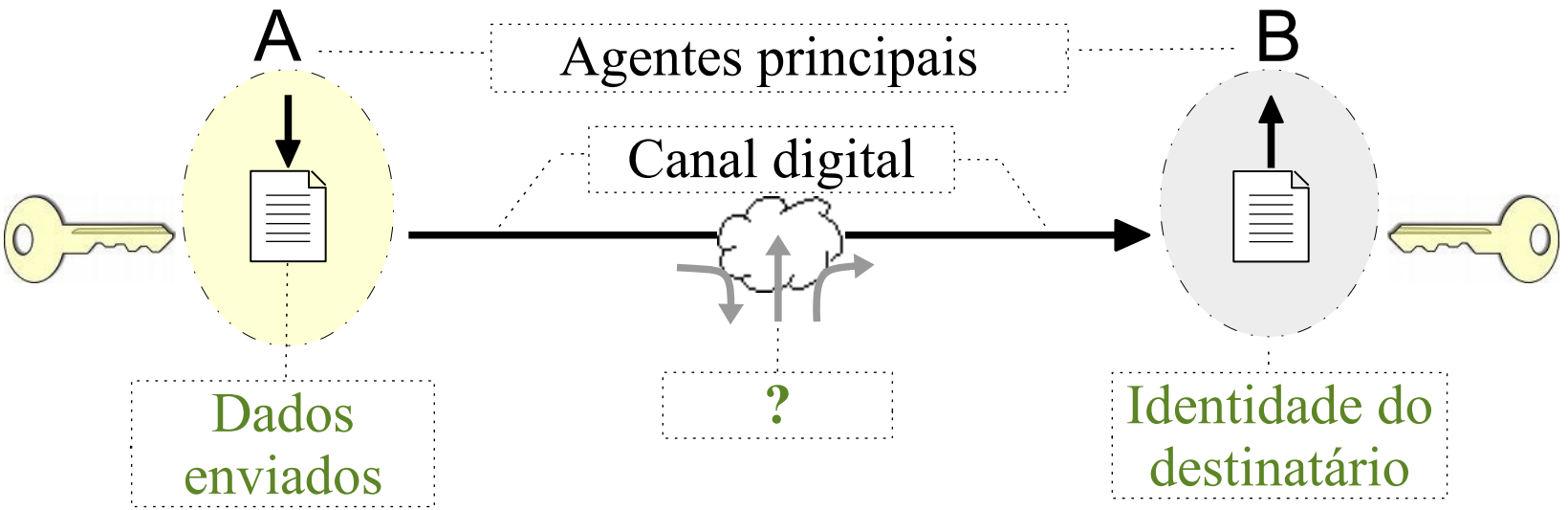
II.2– Premissas de Confiança

Canais, Disponibilidade, Eficácia

II.3– Habilitando a eficácia criptográfica

Demanda, Transporte, Estoque

II.1– “Conheça teu inimigo”



O que faz a Criptografia?

II.1– “Conheça teu inimigo”

-**Criptografia**: arte / técnica de (re)codificar, que não protege dado, informação ou comunicação *per se*.

-Dados são apenas símbolos, codificados em agregados de sinais para representar informações em alguma linguagem.

-Símbolos não pegam fogo nem vão para a cadeia, não se quebram nem morrem;

II.1– “Conheça teu inimigo”

-**Criptografia**: arte / técnica de (re)codificar, que não protege dado, informação ou comunicação *per se*.

-Dados são apenas símbolos, codificados em agregados de sinais para representar informações em alguma linguagem.

-Símbolos não pegam fogo nem vão para a cadeia, não se quebram nem morrem; o que eles significam ou indicam, talvez.

-O que a Criptografia pode proteger são certos *valores* que esses dados significam, para algum *interesse*, em algum *contexto*.

II.1– “Conheça teu inimigo”

-**Criptografia**: arte / técnica de (re)codificar, que não protege dado, informação ou comunicação *per se*.

-Dados são apenas símbolos, codificados em agregados de sinais para representar informações em alguma linguagem.

-Símbolos não pegam fogo nem vão para a cadeia, não se quebram nem morrem; o que eles significam ou indicam, talvez.

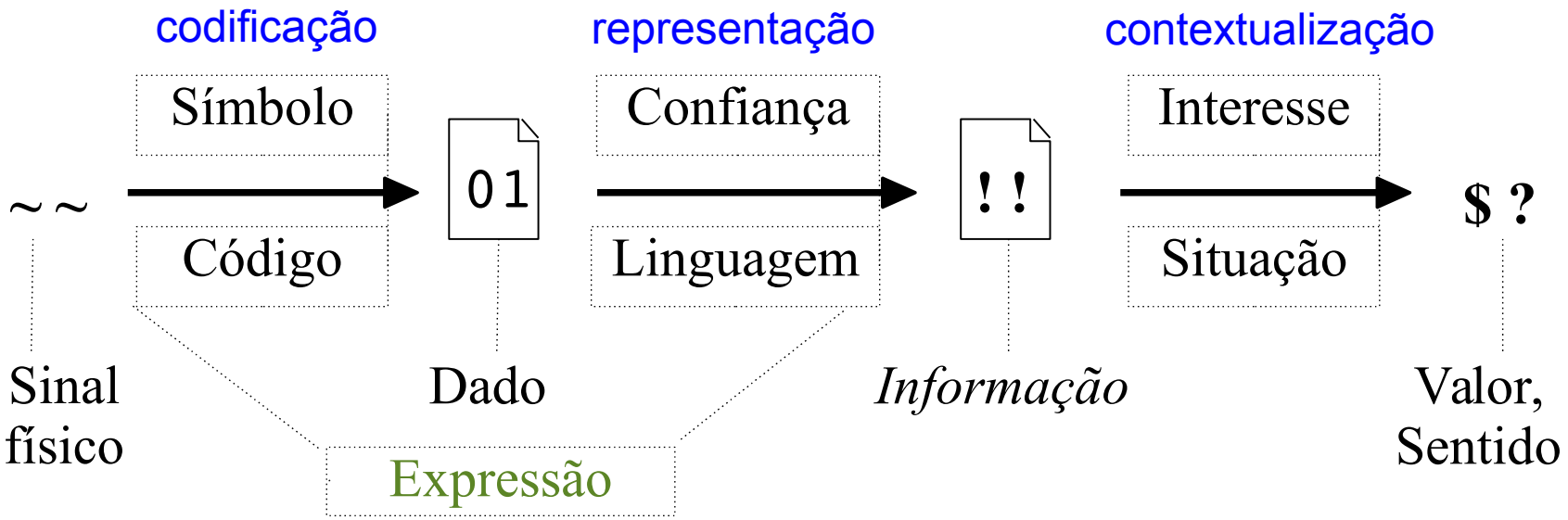
-O que a Criptografia pode proteger são certos valores que esses dados significam, para algum interesse, em algum contexto.

-Esses valores são os que podem ser protegidos por garantias relativas de sigilo, de integridade e/ou de acesso controlado.

-Garantias relativas, pois mecanismos criptográficos funcionam com base em 2 fundamentos, dos quais ao menos um é relativo: *Controle de custos* de decodificação; e *Premissas de confiança*.

II.1– "Conheça teu inimigo"

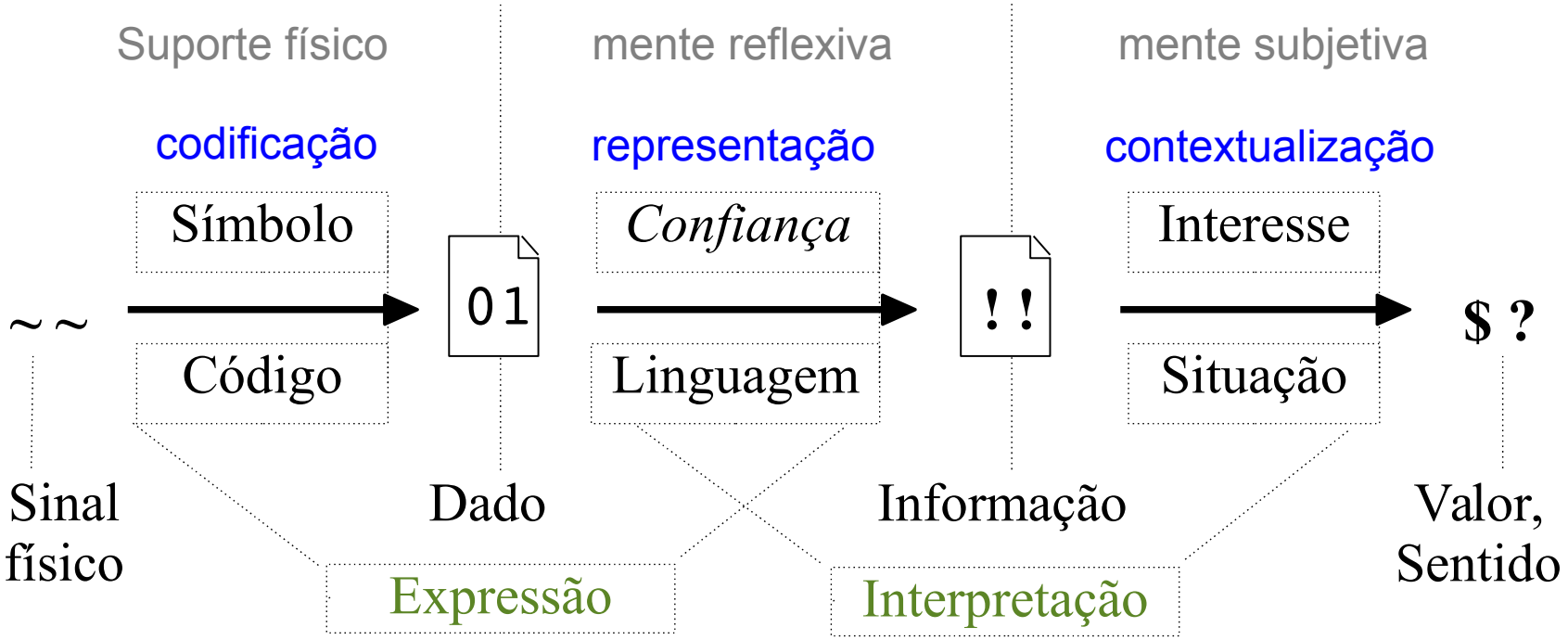
Como se produzem significados (semiose):



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

II.1– "Conheça teu inimigo"

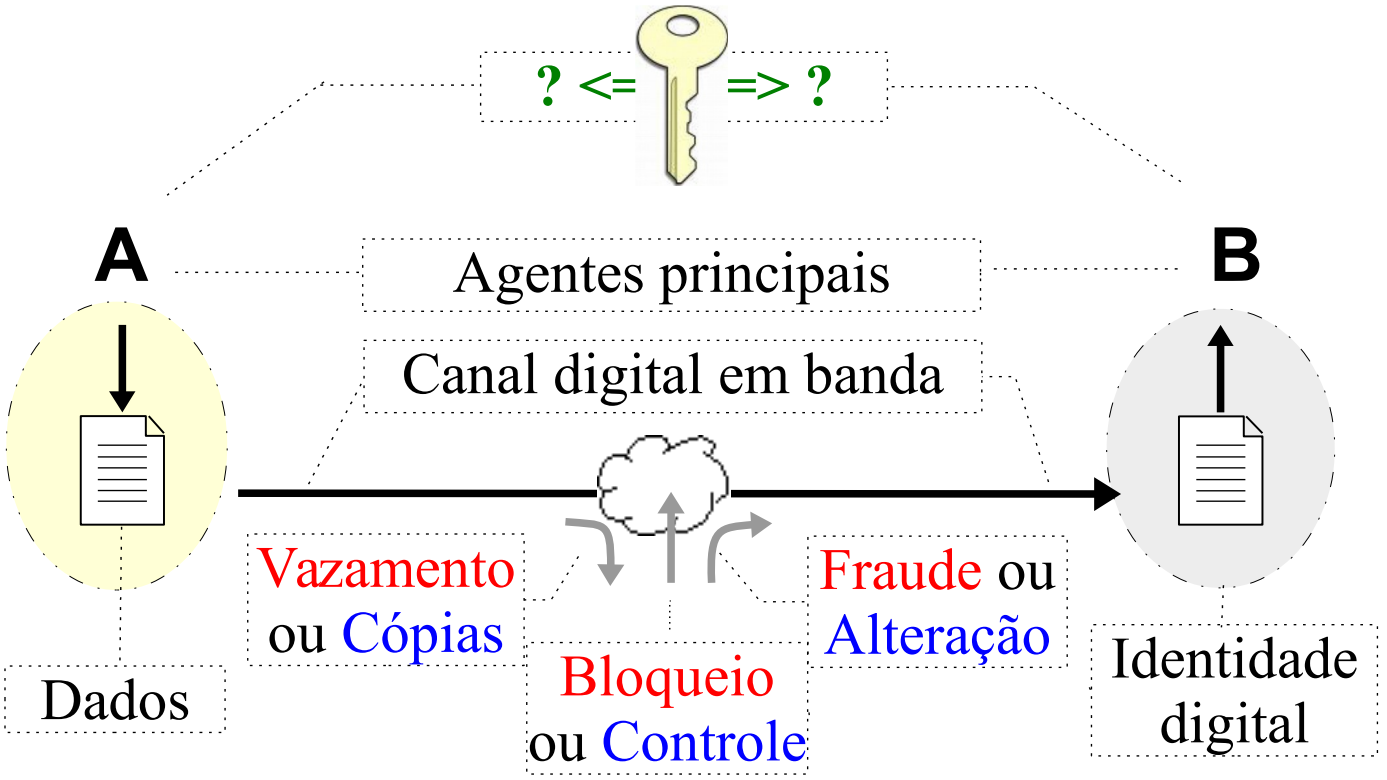
Como se produzem significados (semiose):



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 transferida *fazer sentido, i.e.,* produzir significado).

II.2– Premissas de Confiança

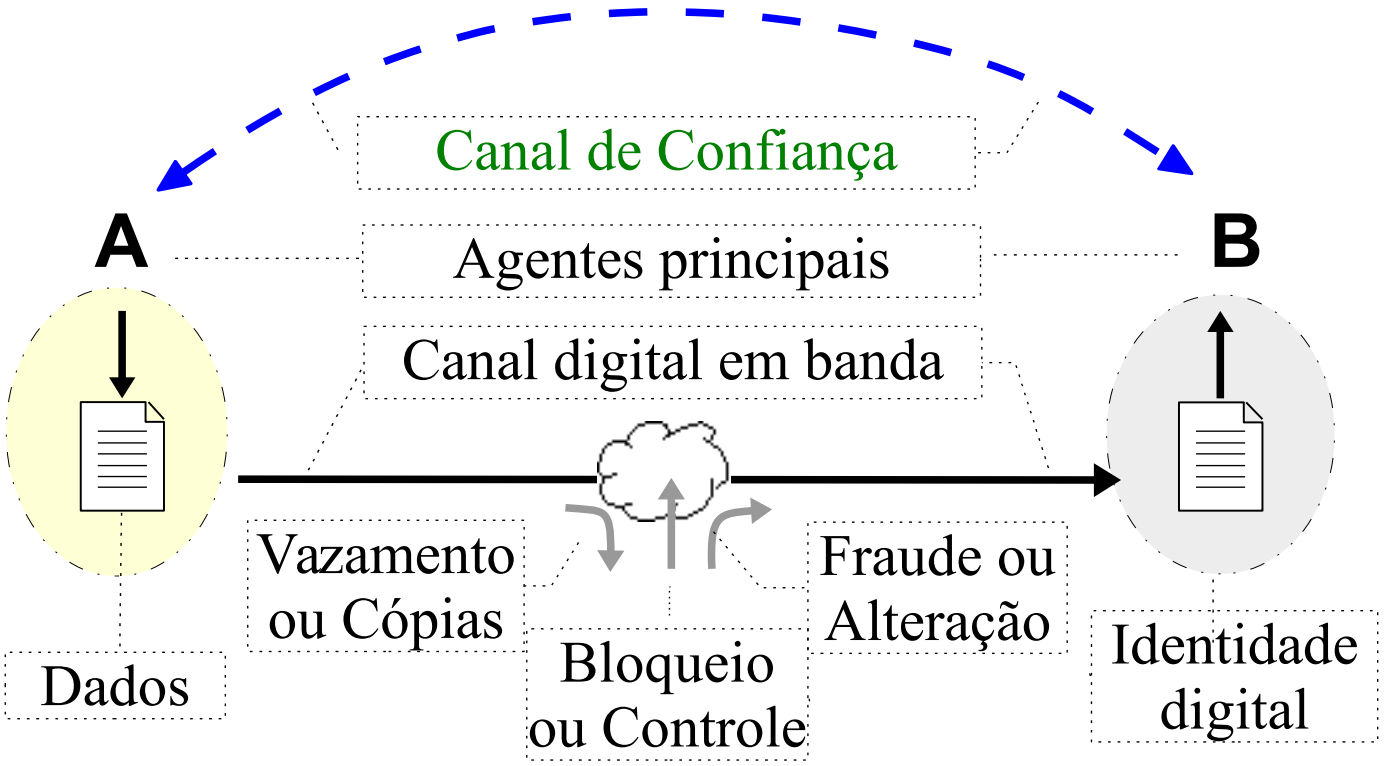
Como se protegem valores na comunicação digital?



Evitando ou permitindo certas ações (talvez de terceiros) no canal de comunicação, *conforme* a situação comunicativa e os interesses em foco

II.2– Premissas de Confiança

Como a proteção se conforma à situação comunicativa e aos interesses em foco?



Com a prévia produção, transporte e armazenagem *confiáveis* de material que habilita ao uso eficaz dos mecanismos adequados à proteção que se almeja operar num canal de comunicação inseguro (*canal em banda*)

II.2– Premissas de Confiança

-O uso *adequado* da Criptografia requer certas condições de confiança para produção, armazenagem e transporte de **material necessário** à operação do mecanismo escolhido.

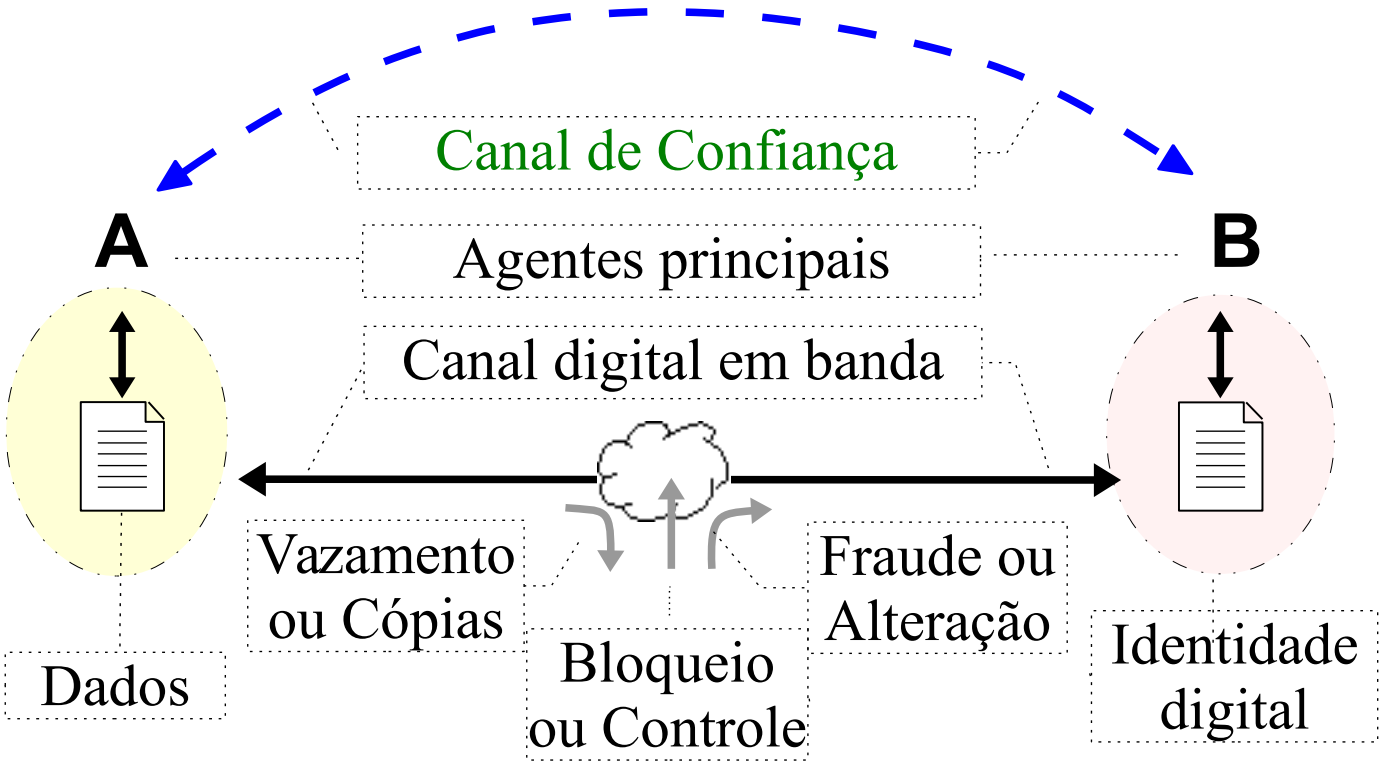
- Na informática, esse material necessário é formado, via de regra, por seqüências binárias em dispositivos e/ou codificações próprias (senhas, *nounces*, chaves, algoritmos, *tokens*, etc.)

- O uso *eficaz,* requer escolhas adequadas à proteção almejada. Chamamos ***premissas de confiança*** (dos mecanismos escolhidos) as ditas condições de uso requeridas por essas escolhas.

- ***Canal de Confiança*** designa um canal de comunicação – no tempo ou no espaço – que seja fora-de-banda e confiável em relação às premissas dos mecanismos de proteção em banda

II.3– Habilitando a eficácia criptográfica

Para proteção almejada, escolhas adequadas...
mas, adequadas *para quem*?



Há situações onde *dos mesmos dados e ao mesmo tempo* um interesse interlocutor demanda sigilo enquanto outro, integridade apenas (transparência), e desses dados, nenhum deles é mais "dono"

II.3– Habilitando a eficácia criptográfica

- **KDP** (*Key Distribution Problem*): Conforme o interesse em foco (de **A** e/ou **B**) contempla proteger o quê (e do quê, e como), presume-se haver alguma garantia prévia, para o remetente *do material habilitante,* sobre a identidade do destinatário, e/ou vice-versa; E sobre a origem, a integridade e talvez o sigilo no transporte desse material.
- OBS: Se o par de chaves criptográficas é assimétrico, as premissas de confiança não requerem sigilo no Canal de Confiança (para transporte da chave pública), requerendo apenas integridade.
- **Questões programáticas desta pesquisa:**
  - Pode a Criptografia ser eficaz sem Canais de Confiança?
  - Pode a segurança em informática?
  - Se não, como o seu uso é presumido nas situações em foco?

III – O que é Confiança?

III.1– Definição semiológica

Inerente à comunicação humana

III.2– Hipótese de Trabalho

Respondendo às questões programáticas

III.3– Interesses e Riscos

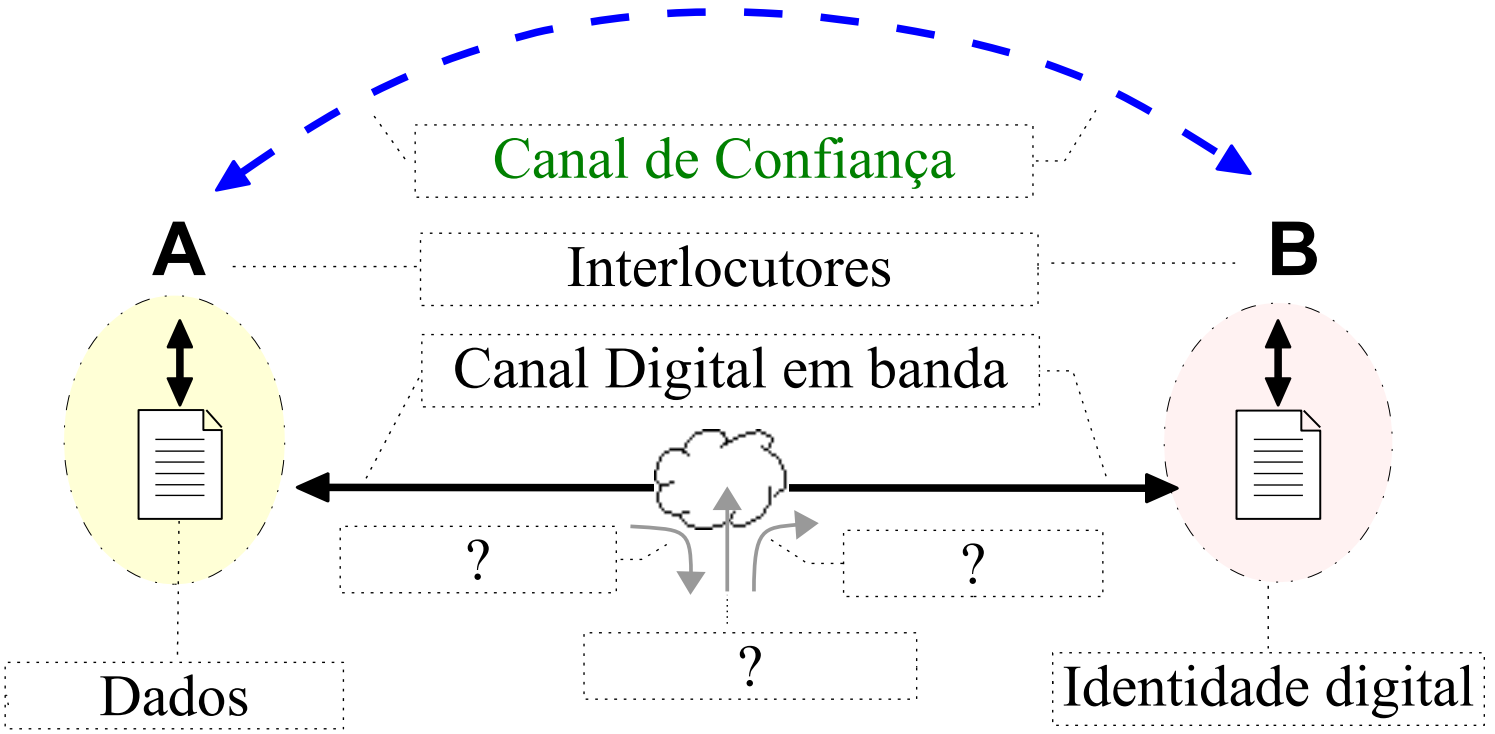
Mediações, Mediadores, Interferências

III.1– Definição Semiológica

- **Confiança**: Em 1997, Ed Gerk propõe uma definição geral e abstrata para o conceito (http://mcwg.org/mcg-mirror/trustdef.htm, citada no slide 26), derivada da teoria que se tornou basilar para a Criptografia: a teoria da informação de Shannon.
- Gerk observa que, apesar do conceito sempre ter sido avesso a definições precisas e a tratamento científico (www.misrc.umn.edu/wpaper/wp96-04.htm), com o advento da Internet ele ganha importância. E nos parece revelar sua natureza semiológica.
- Para definir "Informação", Shannon a concebeu que fosse, ao mesmo tempo, precisa para a engenharia das telecomunicações e significativa para o mundo da vida. Abstraindo, ele evitou se basear na estrutura interna, na função cognitiva ou no aspecto semântico da informação. Nisso Gerk o segue, para definir "confiança"

III.2– Hipótese de Trabalho

Pode a segurança em informática ser eficaz sem canais de confiança?



Respondendo às questões programáticas (2008): Qualquer procedimento ou mecanismo que almeje alguma forma de segurança em informática demanda algum Canal de Confiança para habilitar seu uso eficaz.

III.2– Hipótese de Trabalho

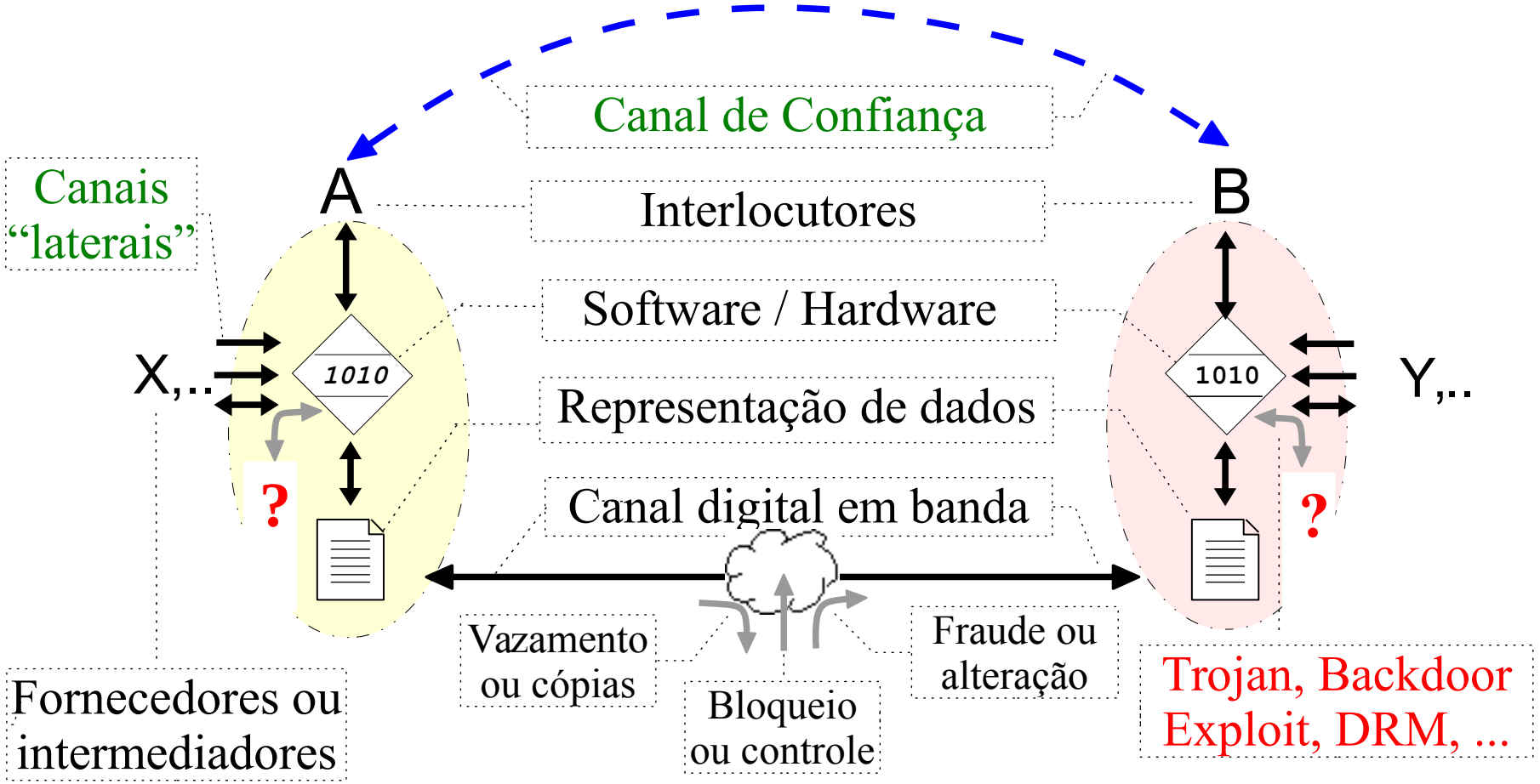
Como um mecanismo de segurança informacional demanda canais de confiança?

- Para responder à esta terceira questão programática, aborda-mos situações nas quais algum interesse de quem confia, em algo ou alguém sobre algum assunto, esteja em potencial conflito com algum outro interesse pertinente à análise de riscos subjacente, sejam tais interesses representados no processo de segurança por pessoa, por software ou por máquina.
- Seguindo o clássico tratado de Garfinkel & Spafford*, devemos contemplar os interesses de fornecedores das tecnologias intermediadoras, e os que podem se fazer representar na sua operacionalização, como pertinentes à análise de riscos.

*- Garfinkel & Spafford: "*Practical Unix and Internet Security*" (1996), Chapter. 27

III.3– Interesses e Riscos

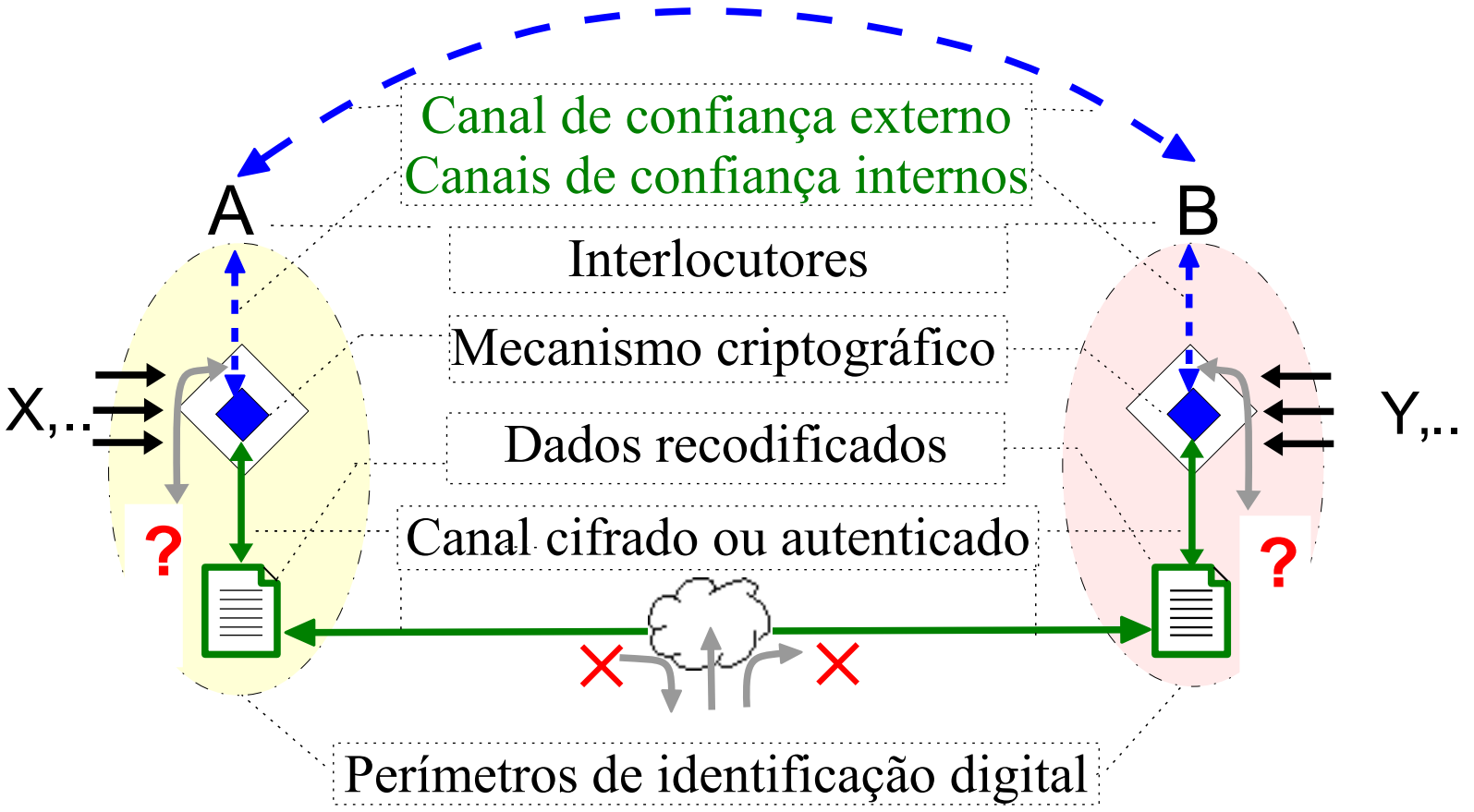
Mediações



Situações comunicativas intermediadas por tecnologias digitais também envolvem "canais laterais" (*side channels*), por onde atuam fornecedores e intermediadores segundo seus próprios interesses.

III.3– Interesses e Riscos

Interferências



Interferências via canais laterais sobre um dos perímetros internos de um Canal de Confiança (*side channel attacks*) anulam a eficácia de qualquer mecanismo criptográfico operando em banda.

IV – Modelando Confiança

IV.1– Política de Segurança em Informática (PSI)

O que é, Quem faz, Para quem e para quê?

IV.2– Modelando Confiança para PSIs

Por que, Como e Para quê?

IV.3– Usando Modelos de Confiança

Estratégias para análise de riscos

IV.1– Política de Segurança

O que é

- Política de Segurança em Informática (PSI) é, basicamente, definição de restrições.
- Sentidos: *policy, politics; safety, security*,
- *Policy*: Prioriza interesses afetos a TICs (baseada em missão, competitividade, *politics*, etc.)

IV.1– PSI

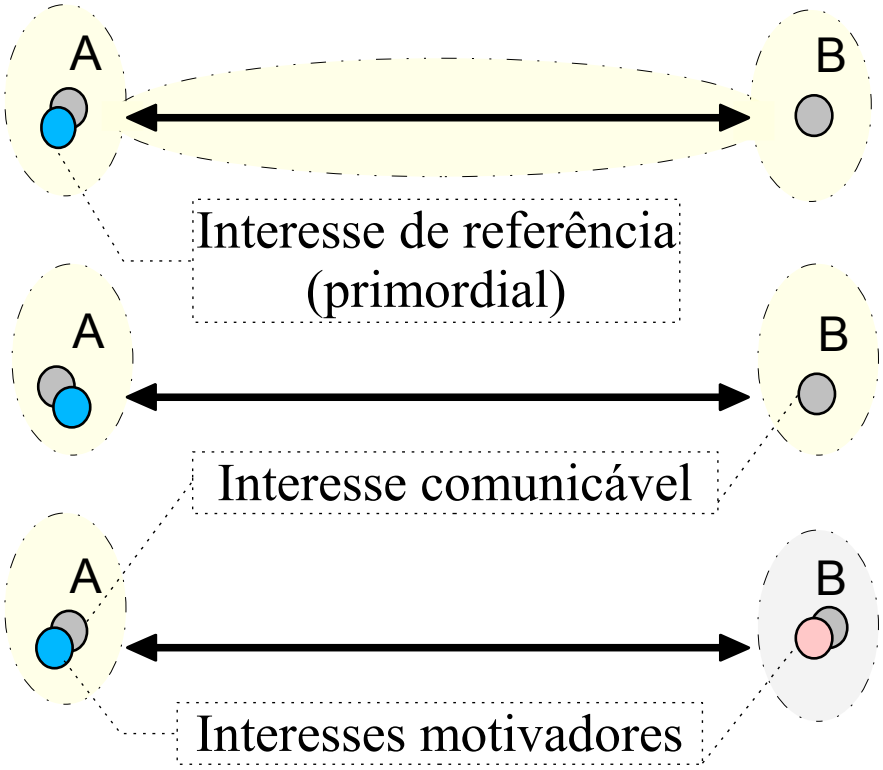
Que faz, para quem e para quê

- Formaliza, em linhas gerais, crenças, princípios, metas, objetivos gerenciais e procedimentos aceitáveis ou mandató-rios para agentes de uma ou numa entidade (que a adota), incluindo modos de ação visando a sancionar desvios, enfrentar contingências e reformular-se com aferições.
- Reflete a nautreza da entidade: PSI informal ou terceirizada. Identifica interesses (entidade simples), e/ou política (*poli-tics*) de atribuição de competências (entidade complexa)
-Mapeia interesses pertinentes: Conforme o sentido de segurança (*safety* ou *security*), i.e., segundo as leis de Murphey ou segundo a 1ª hipótese metafísica de Descartes

IV.2– Modelando confiança para PSIs

Modelagem sintática, sobre condições de intermediação

MC_1:
Sistema
Fechado



A confia:
1. Na plataforma (A, B);
2. No interesse c. de B.
3. No controle do canal.

MC_2:
Rede
Fechada

A confia:
1. Na sua plataforma;
2. No interesse c. e na plataforma de B.

MC_3:
Rede
Aberta

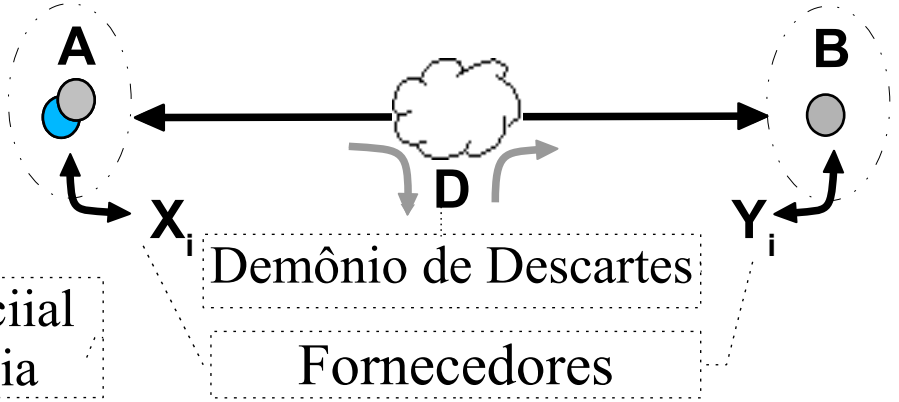
A confia:
1. [Quando muito,]
Em sua plataforma.

Modelos de Confiança para Sistemas de Comunicação

IV.2– Modelando confiança para PSIs

Modelagem semântica, sobre polarização de interesses

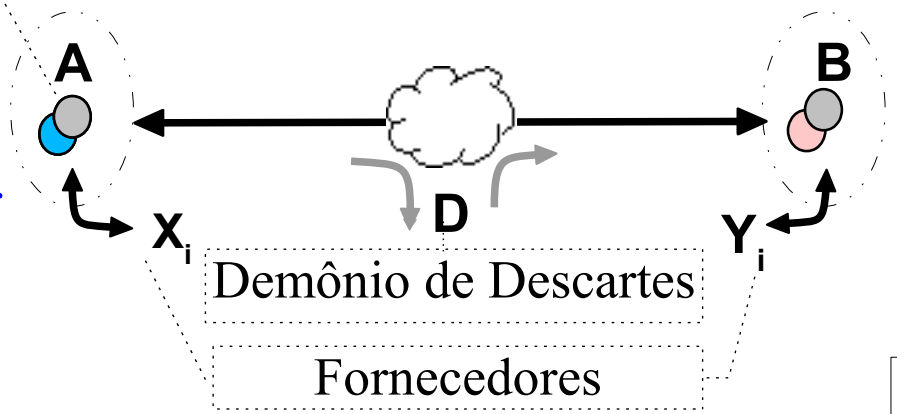
MS_2:
Sistema
Bipolar



Interesse iniciial
de referência

Premissas mínimas:
A ~ B, A ⊥ D, ...
ou
A ~ Y, B ~ X, ...
etc.

MS_3:
Sistema
Multipolar



Premissas mínimas:

A ⊥ B, A ⊥ D, ...
ou
A ⊥ Y, B ⊥ X, ... etc.

⊥ : interesses confiltantes
~ : interesses alinhados

Modelos de Confiança para Sistemas de Significação

IV.3– Usando modelos de confiança

Mapeamento e Acoplagem

- **Idéia**: Situar interesses mapeáveis pela PSI em modelos adequados, para delinear as fronteiras do processo de segurança.

  Essas fronteiras "de confiabilidade" são os canais de confiança presumidos (como disponíveis) pela situação em foco.

- "Demônio de Descartes" modela vazamento e fraude, mas nem sempre o bloqueio (ação e agente podem ser identificáveis)

- Um modelo de Confiança em Comunicão (sintático) se acopla a um modelo de Confiança em Significação (semântico), através do referencial fixado em um interesse primordial (motivador);

  E vice-versa, através do referencial fixado em um interesse inicial (comunicável).

IV.3– Usando modelos de confiança

Sobre escolha do modelo semântico

- MS1 (que consideraria apenas um pólo de interesses) é desconsiderado por representar uma situação de riscos paradisíaca'.
- MS3 colapsa semânticas com mais de dois pólos de interesses potencialmente conflitantes porque o refinamento de MS2 para MS3 introduz um novo tipo de risco – de conluios – que ofuscam conflitos e até mesmo a análise da polarização.
- Doutra feita, uma PSI que mapeia interesses segundo uma lógica binária de riscos ('nós' contra 'eles') – isto é, para MS2 – pode ser excessivamente reducionista para a situação em foco. Exemplos abundam em sistemas sensíveis em rede aberta, ou em rede fechada que atendem interesses conflitantes e oponíveis ao interesse superveniente (do dono do sistema).

V – Encadeando Modelos

V.0 – Encadeamento sintático

A comunicação digital é transitiva

V.1– MC_1: Sistema Fechado

Apresentação, Identificação, Autorização, Rastreamento

V.2 – MC_2: Rede Fechada

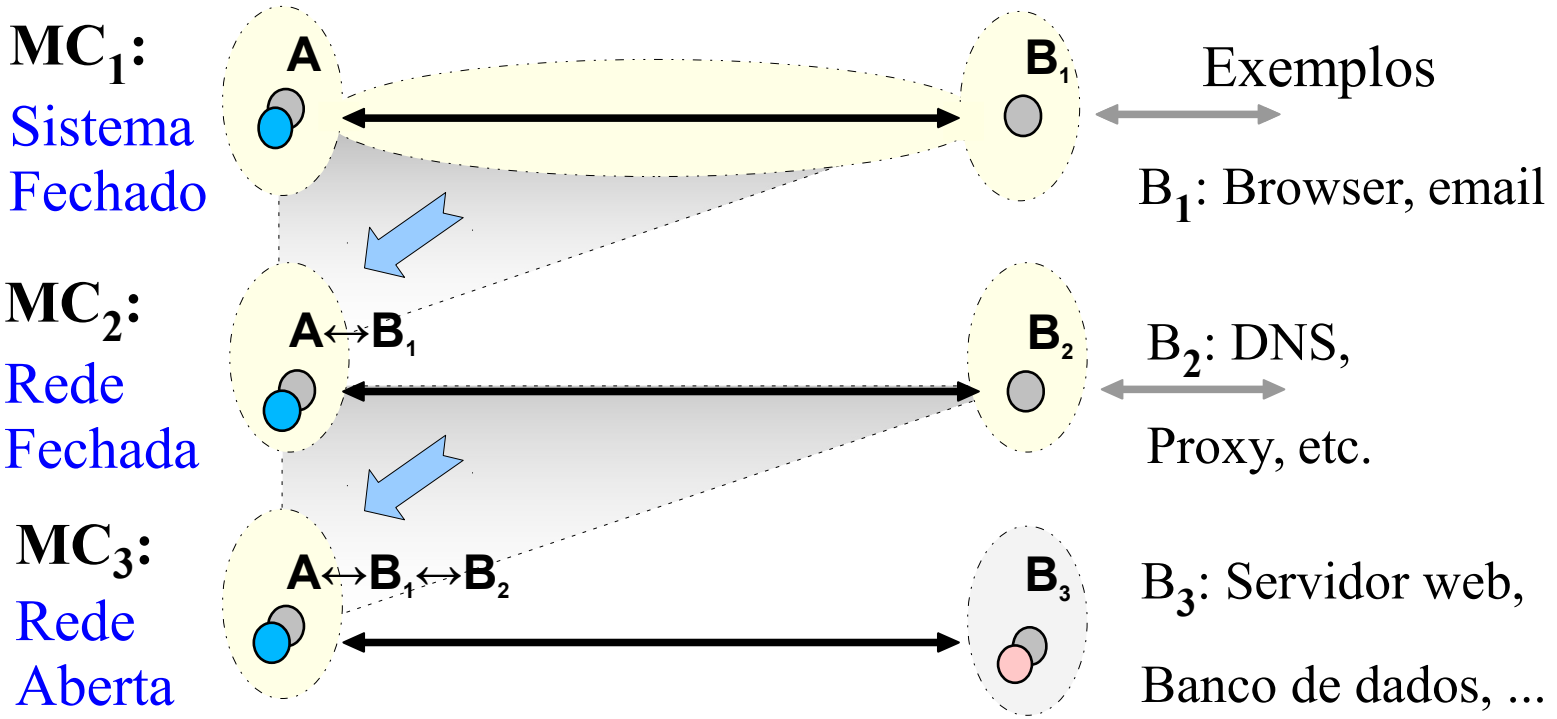
Autenticação intersubjetiva, Cifragem, Habilitação

V.3 – MC_2: Rede Aberta

Autenticação objetiva, Certificação, Registro

V.0– Encadeando modelos

Comunicação transitiva, modelos sintáticos se encaixam



Cadeia de Modelos de Confiança em Comunicação

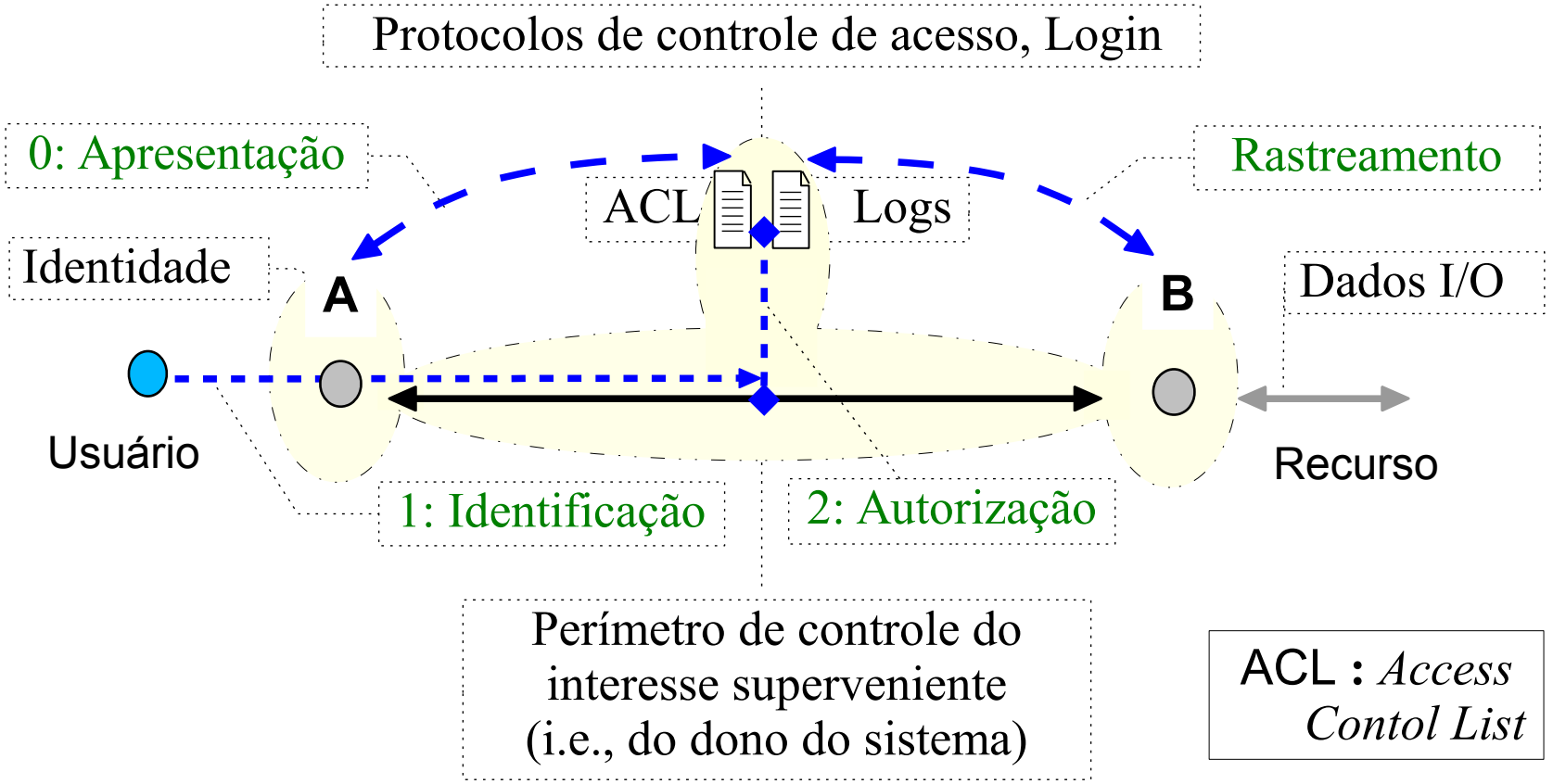
V.0– Encadeando modelos

Sobre os modelos sintáticos encaixantes

- **MC1** : A situação típica a ser modelada é a de uma plataforma formada por computador, sistema operacional multiusuário e recursos (aplicativos, etc.). Cobre também dispositivos móveis e de *firmware* (roteadores, etc.) que disponham de mecanismo de controle de acesso baseado em segredo compartilhado (senha) ou em identificador único (dispositivo biométrico, *token* de chave privada, etc.).
- **MC2** : Modela redes fechadas, i.e., redes que tenham dono. A situação típica a ser modelada é uma rede de sistemas fechados na qual o controle físico sobre seus canais de comunicação digital seja inviável para o dono (ex., LAN ou VPN), que controla os sistemas conectados.
- **MC3** : Para redes abertas, i.e., redes digitais formadas por acordo tácito. A situação típica a ser modelada é uma rede de redes fechadas que funciona por adesão voluntária a protocolos e formatos digitais de comunicação abertos (por ex., a Internet, ou qualquer rede de serviço oferecido nela e prestado através dela).

V.1 – MC1: Sistema fechado

Fronteiras de confiabilidade (em verde)



Modelo de Confiança em Comunicação para sistemas fechados

V.1– MC1: Sistema fechado

O processo de segurança em foco é delineado por protocolo(s) de controle de acesso que se classificam em discricionários, mandatórios ou baseados em papéis (RBAC). Os canais de confiança externos presumidos por tais protocolos são os de Apresentação e de Rastreamento (onde tais sub-processos ocorrem), os quais habilitam o controle de acesso ao sistema.

Identificação e Autorização : Os canais de confiança presumidos pelo acesso autorizado, internos à plataforma modelada, são os elementos de protocolo aqui nomeados Identificação e Autorização. Identificar é reconhecer (conhecer outra vez). A situação mais simples reconhece por nome-de-usuário e senha, através da componente de protocolo denominada *login*, que presume a senha como segredo compartilhado entre apenas o usuário e o sistema (por este, até o ponto do fluxo de dados onde o *hash* da senha é calculado), para fins de identificação mútua. Mas conhecer pela primeira vez, não pode ser por este (sub)processo. Quando uma conta de usuário é criada, presume-se que um (novo) usuário está sendo apresentado à plataforma, que assim o conhece pela primeira vez.

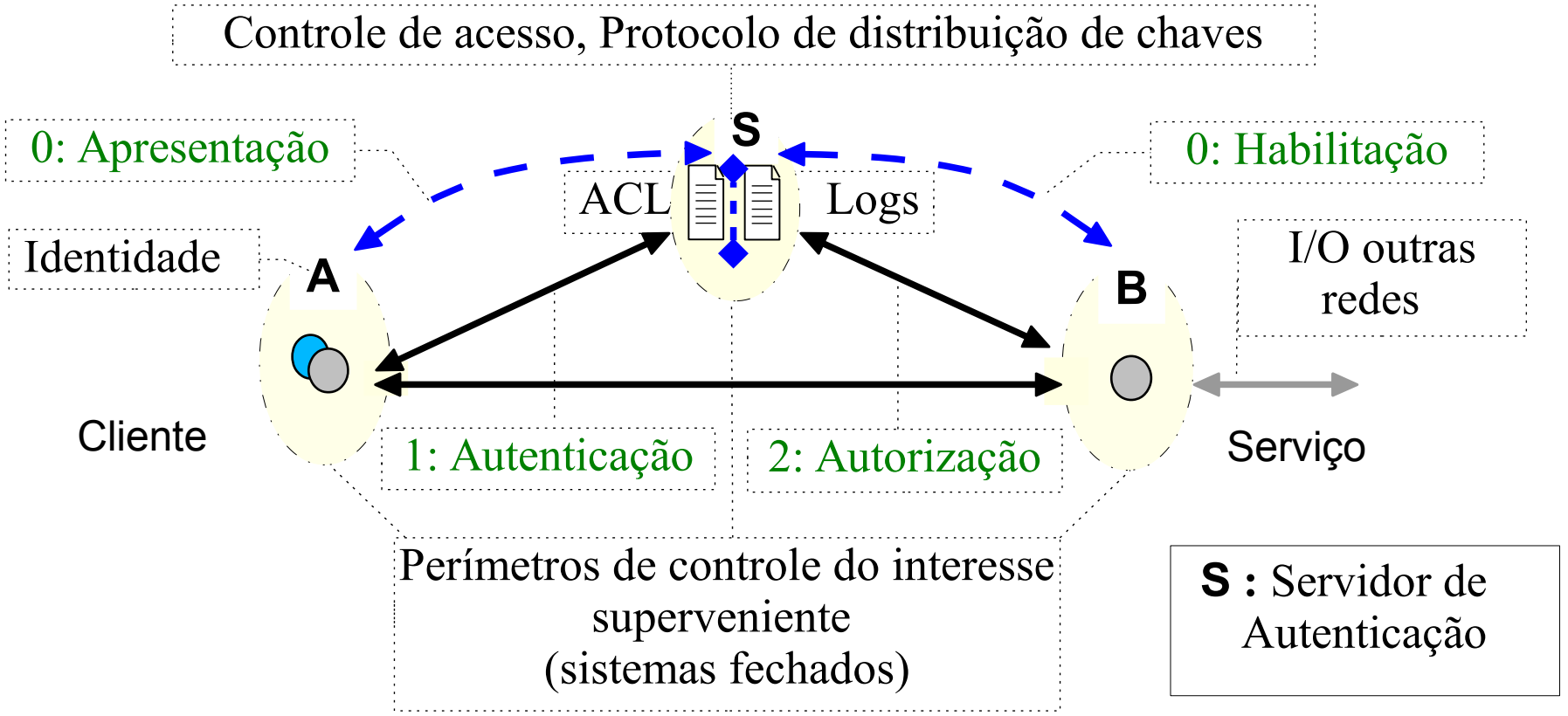
V.1– MC1: Sistema fechado

- **Apresentação** : Processo administrativo que tem um lado executado na plataforma, outro lado fora dela. Na plataforma se habilita um usuário ao *login*, fora do *login.* Fora da plataforma se justifica o uso que tal agente deve ou pode fazer da plataforma, a quem responde por ela. Este lado da Apresentação conecta o processo de segurança na plataforma a outros processos pertinentes. Quem responde pela plataforma deve presumir que registros deste uso podem ser rastreados através dela (por ex., em logs).

- **Rastreamento** : Também administrativo, também tem um lado executado na plataforma e outra lado fora dela. Na plataforma gerencia-se o acesso (administração de contas, de logs, de gravação de *back-ups*, etc.), conforme o interesse superveniente (do dono da plataforma). Fora da plataforma se conecta esta gerência a outros processos pertinentes (auditoria, forênsica, etc.), inclusive a processos regidos por normas civis e criminais, que visam a proteger o valor probante desses registros se dela extraídos.
Se o *login* não é usado, é usado sem eficácia, ou se o interesse superveniente é alvo de suspeição, tal proteção pode requerer o flagrante, a busca e apreensão desta plataforma quando indícios externos apontarem para ela.

V.2 – MC2: Rede fechada

Fronteiras de confiabilidade (em verde)



Modelo de Confiança em Comunicação para redes fechadas

V.2– MC2: Rede fechada

O processo de segurança em foco é delineado por protocolo(s) de distribuição de chaves (Kerberos, LDAP+SSL, etc.). Os canais de confiança externos (à rede fechada) presumidos por tais protocolos são os de Apresentação e de Habilitação (onde tais subprocessos ocorrem), os quais habilitam controle de acesso aos recursos disponíveis na rede (conforme autorizações configuradas na ACL).

Autenticação e Autorização : Os canais de confiança presumidos pelo acesso autorizado, internos à rede modelada, são serviços de integridade e de sigilo que visam a oferecer, através de canais inseguros: a) Para o dono da rede: confiabilidade na identificação de usuários, de serviços e de acessos autorizados e/ou executados por estes; b) Para um usuário ou serviço: confiabilidade na identificação do outro interlocutor e da integridade das transmissões.

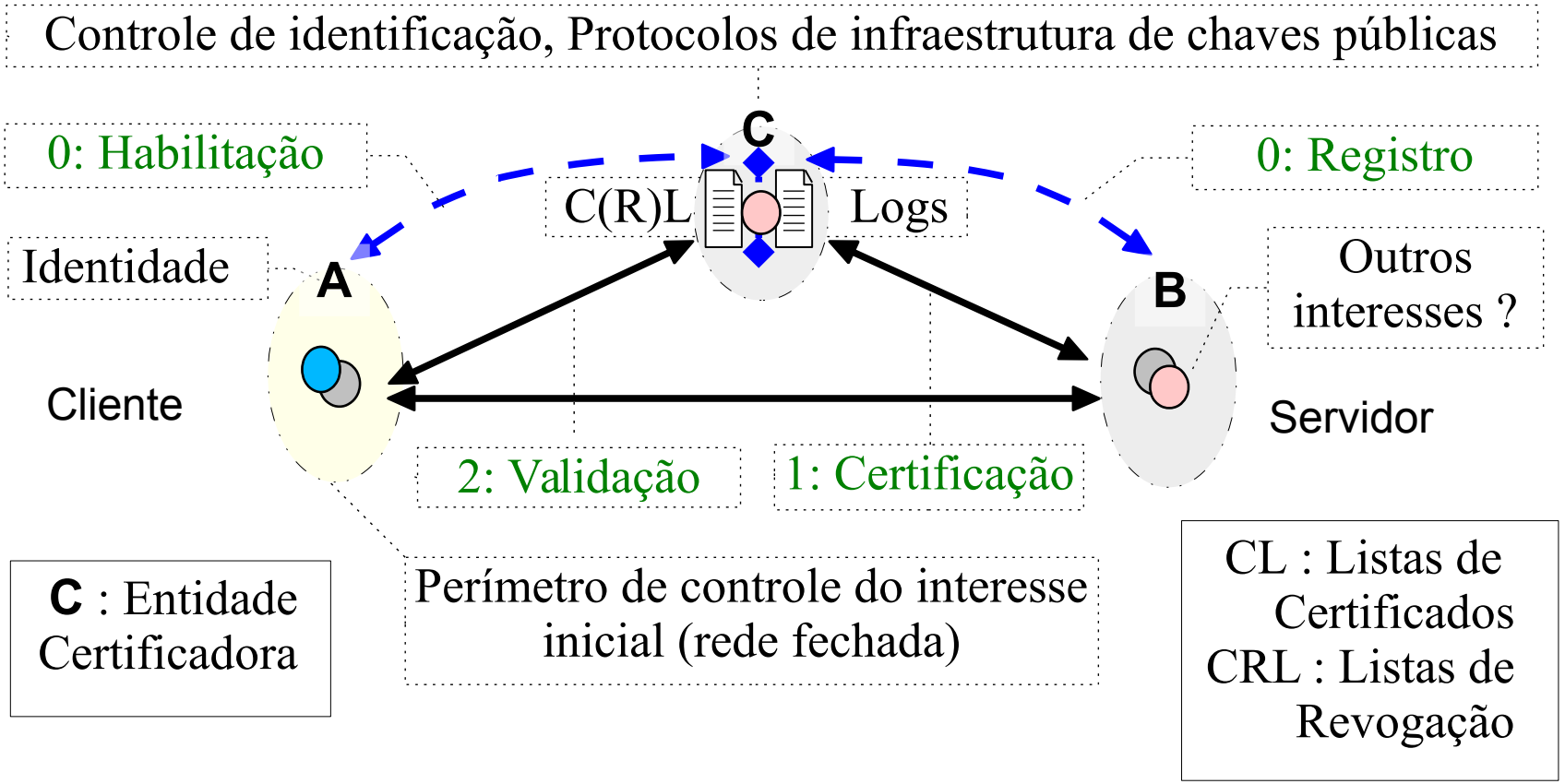
V.2– MC2: Rede fechada

Numa rede fechada, o interesse superveniente (do dono da rede) pode, em princípio, modular potenciais conflitos de interesse entre principais. Neste caso a autenticação para autorização e rastreamento pode ser subjetiva (lastreada em compartilhamento de segredo).

Apresentação e Habilitação: Os canais de confiança externos, através dos quais o interesse superveniente instala e habilita suas escolhas (de normas internas e serviços), servem também a que pares de agentes que se reconhecem nessas normas (o servidor de autenticação e um usuário ou serviço) estabeleçam entre ambos uma chave mestra, na apresentação (ou na instalação) do último pelo primeiro. As chaves mestras habilitam os serviços internos de integridade e de sigilo para sessões autorizadas, necessários aos objetivos do protocolo, via mecanismo escolhido e chave de sessão distribuída (sob a chave mestra) pelo servidor.

V.3 – MC3: Rede aberta

Fronteiras de confiabilidade (em verde)



Modelo de Confiança em Comunicação para redes abertas

V.3– MC3: Rede aberta

O processo de segurança em foco é delineado por agregado(s) de protocolos conhecidos por Infraestrutura de Chaves Públicas. (PKIX, SPKI, etc.), ou por uma sigla genérica (ICP, PKI). Estes agregados são por vezes implementados sob a jurisdição de uma norma civil superveniente (por exemplo, ICP-Brasil, sob a MP 2.200). Os canais de confiança externos presumidos por tais protocolos são os de Habilitação e Registro, que habilitam a identificação certificada de principais.

Validação e Certificação: Os canais de confiança presumidos pela identificação certificada, internos à rede modelada, são serviços de integridade que visam a oferecer: a) para o titular de um certificado: confiabilidade na apresentação desta titularidade, visando a utilização adequada da chave pública transportada neste certificado, para fins ou de transmissões sigilosas de terceiros a si, ou de verificação da autenticidade de emissões suas a terceiros, na rede aberta; b) para um usuário de um certificado: confiabilidade na apresentação do titular deste certificado, visando a utilização adequada da chave pública que ali é transportada.

V.1– MC1: Sistema fechado

Numa rede aberta, o modelo presume apenas um acordo tácito (sobre como se comunicar nela). Não haverá escolha possível para norma administrativa, além dos protocolos e serviços de comunicação tecnicamente acordados e nela operáveis (como num idioma). Nada nela impede ou modula potenciais conflitos entre interesses que motivam interlocuções (a começar pelos interesses envolvidos em apresentações). Por isso, a confiabilidade de um interlocutor na identificação de outro deve ser objetiva (*não* pode ser lastreada em prévio segredo compartilhado).

Habilitação e Registro: Numa ICP, os certificados-raiz funcionam como âncoras de confiabilidade para identificação: de signatários em esquemas de autenticação, e de destinatários em esquemas de cifragem (a habilitação de um certificado-raiz falso permite ao falsário se passar por qualquer usuário da ICP durante a Validação). Da mesma forma, acesso à chave privada funciona como âncora para a confiabilidade na identificação do titular. A manipulação de *sua* chave privada por interesse escuso permite ao falsário se passar por *você* ante qualquer usuário da ICP.

VI – Conclusão

Confiança

Se merecida
não carece ser pedida
ou conferida.

Desmerecida,
não parece ter medida;
será perdida.

Desmedida,
perece ao se ver imposta
ou transposta. Decida.