Modelo de Segurança

- Que ameaças existem sobre o sistema?
- Que ataques são possíveis?

- Assumiremos que **muitas** existem ameaças sobre o sistema

Programa

1. Redes de dados e programação da comunicação distribuída (revisão)
2. RPC (Remote Procedure Call),
   RMI (Remote Method Invocation),
   Web Services
3. Gestão de Nomes
4. **Segurança**
   Canais seguros
   Autenticação
   Autorização
5. Tolerância a Faltas
   Replicação
   Transacções

Segurança em Sistemas Informáticos

Políticas de Segurança

- Quando é que se torna necessário uma política de segurança?
  - Quando existe um **Bem** num espaço partilhado

- Uma política de segurança procura garantir a proteção do **Bem** contra os ataques esperados dentro de determinadas condicionantes

Ameaça típica

- A **partilha** está na base da maioria das ameaças
  - Espaços públicos
  - Espaços físicos partilhados
  - Utilização de infraestruturas comuns
  - Partilha de recursos

A Informação como um Bem

- Confidencialidade/Privacidade da informação
  - Ex.: Pessoal, Médica, relação com o Governo
- Integridade da Informação
- Disponibilidade dos serviços que permitem aceder a informação

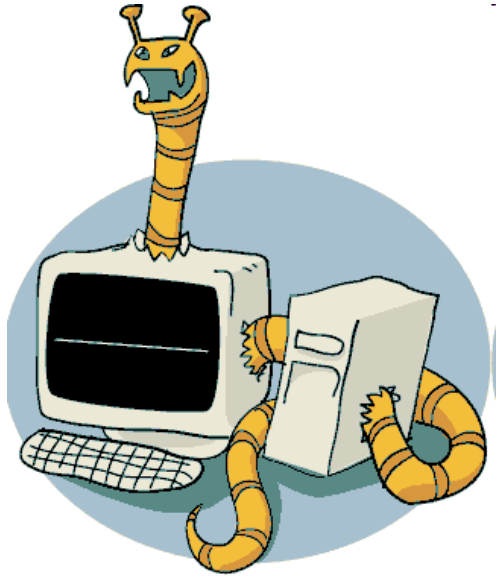
- Identidade – não efetuar ações em nome de outro
- Anonimato – realizar ações que são autenticadas mas em que não se deve conhecer a identidade (ex.: votações)

Ameaças em sistemas informáticos

- Fuga de informação (*leakage*)
  - Aquisição de informação por agentes não autorizados
- Corrupção de informação (*tampering*)
  - Alteração não autorizada de informação
- Vandalismo
  - Interferência no funcionamento correto do sistema sem que tal traga benefícios ao atacante

Características dos sistemas informáticos que facilitam os ataques

- Automação
  - Facilidade de reproduzir uma ação milhões de vezes rapidamente.
- Ação à distância
  - Com a Internet, a distância entre o atacante e o Bem não é um limitador ao ataque
- Propagação rápida das técnicas



Partilha nos Sistemas Informáticos

- Os sistemas informáticos são feitos para partilhar informação…
  - O que complica seriamente a segurança!

- Partilha nos Sistemas Multiprogramados
  - Ficheiros
  - Memória
  - Programas
  - Periféricos
- Partilha nas Redes
  - Meios físicos de comunicação
  - Mecanismos de comutação

Isolamento

- Como a partilha cria a maioria das oportunidades de ataque o isolamento foi desde sempre uma das formas de garantir segurança
  - Isolamento físico: cofres; paredes
  - Isolamento de pessoas: só um determinado grupo é informado
  - Isolamento lógico: cifrar um documento torna ininteligível a informação

Política vs Mecanismo de Segurança

Políticas de segurança são suportadas/asseguradas por uma utilização adequada de mecanismos de segurança

Política de Segurança

- Uma política de segurança define-se respondendo às seguintes questões:
  - O que queremos proteger?
  - Quais são as ameaças potenciais?
  - Quem as pode executar? Ou seja, quem são os atacantes?
  - Quais os ataques? Como se materializam as ameaças
  - Quais os procedimentos e mecanismos de proteção que podem impedir os ataques considerados?
  - Qual o custo de implementação da política de segurança?
- O custo da segurança deve ser inferior ao valor do Bem

Quem pode ser o atacante?

- Os mesmos do mundo físico...
- Podemos classificá-los de acordo com os seguintes características:
  - Objetivos
  - Acesso ao sistemas
  - Recursos
  - Capacidade técnica
  - Riscos que estão dispostos a correr

Possível Lista de Atacantes

- Jornalistas
- *Hackers*
- Criminosos isolados
- Crime Organizado
- Pessoal interno
- Terroristas
- Polícia
- Organizações Militares
- Espiões industriais
- Organizações de Segurança Nacionais

PRISM/US-984XN Overview

OR

*The SIGAD Used **Most** in NSA Reporting*

Overview

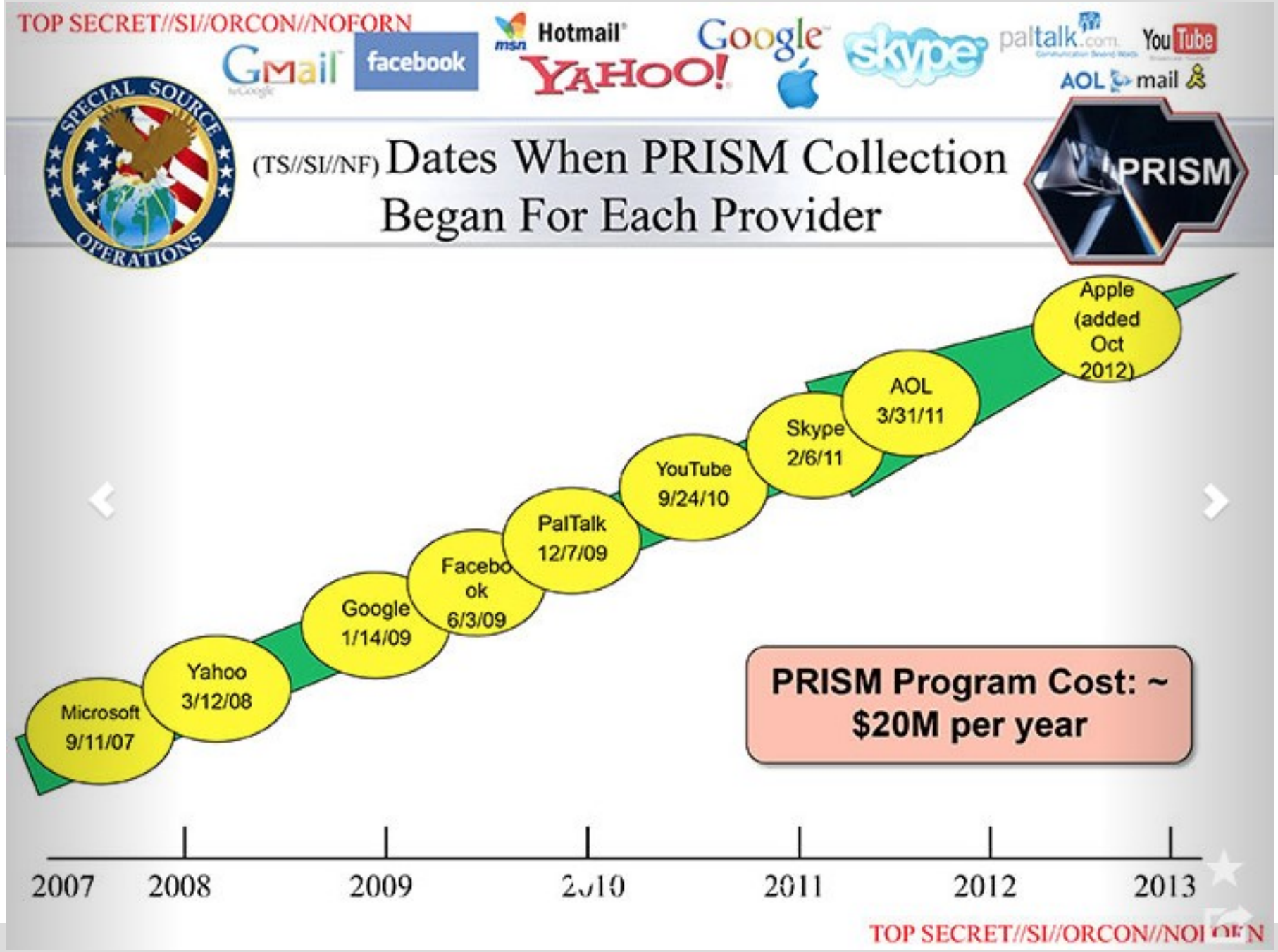
[redacted]

April 2013

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360901

TOP SECRET//SI//ORCON//NOFORN

https://archive.org/details/NSA-PRISM-Slides


TOP SECRET//SI//ORCON//NOFORN
Gmail
facebook
msn Hotmail
YAHOO!
Google
skype
paltalk.com
YouTube
AOL mail
SPECIAL SOURCE OPERATIONS
(TS//SI//NF) Dates When PRISM Collection Began For Each Provider
PRISM
Microsoft 9/11/07
Yahoo 3/12/08
Google 1/14/09
Facebook 6/3/09
PalTalk 12/7/09
YouTube 9/24/10
Skype 2/6/11
AOL 3/31/11
Apple (added Oct 2012)
PRISM Program Cost: ~ $20M per year
2007
2008
2009
2010
2011
2012
2013
TOP SECRET//SI//ORCON//NOFORN

Segurança no Sistema Operativo

Máquinas sem ligação em rede

Base Computacional de Confiança

- Normalmente o sistema operativo é uma plataforma que oferece uma: **Base Computacional de Confiança**
  - TCB *(Trusted Computing Base)*
- Faz parte da TCB tudo o que no sistema operativo é necessário para garantir a política de segurança

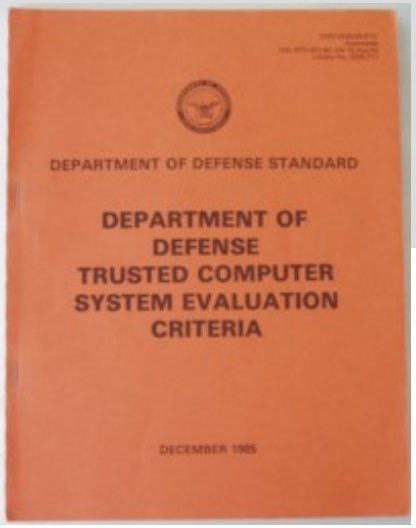
Ataques em sistemas centralizados

- Em sistemas informáticos centralizados:
  - Assumir a identidade de outro utilizador
  - Executar operações que, indiretamente, ultrapassam os mecanismos de proteção
  - Infiltrar código em programas que sub-repticiamente executam outras funções
  - Canais encobertos de comunicação

Base Computacional de Confiança (TCB)

- Nos Sistemas Multiprogramados a TCB inclui:
  - **Isolamento dos espaços de endereçamento** garantido pelo hardware da gestão de memória
  - **Restrição à execução em modo utilizador de instruções privilegiadas** que possam ultrapassar o isolamento dos espaços de endereçamento, (ex.: interrupções, operações de E/S)
  - **Utilização do núcleo exclusivamente através de funções do sistema** que validam a correta utilização dos mecanismos do sistema a que dão acesso
  - **Autenticação** sob controlo do sistemas
  - **Controlo de acessos** validado por um ou vários monitores de controlo de referência
  - **Algoritmos de criptografia** que permitem manter a confidencialidade de informação sensível que esteja acessível aos utilizadores

TCSEC (Orange Book)



- No *Orange Book* são definidas quatro classes de segurança que por sua vez se subdividem em vários níveis:
  - D - proteção mínima
  - C - política baseada no controlo de acessos, vulgar nos sistema operativos comerciais
  - B - políticas baseadas em controlo mandatório (obrigatório) do nível de segurança da informação. Nos subníveis mais elevados implica critérios de segurança na estrutura interna do sistema operativo;
  - A - classificação mais elevada que implica não só a existência dos mecanismos, mas a sua verificação formal

Criterion	D	C1	C2	B1	B2	B3	A1
Security policy							
Discretionary access control		X	X	→	→	X	→
Object reuse			X	→	→	→	→
Labels				X	X	→	→
Label integrity				X	→	→	→
Exportation of labeled information				X	→	→	→
Labeling human readable output				X	→	→	→
Mandatory access control				X	X	→	→
Subject sensitivity labels					X	→	→
Device labels					X	→	→
Accountability							
Identification and authentication		X	X	X	→	→	→
Audit			X	X	X	X	→
Trusted path					X	X	→
Assurance							
System architecture		X	X	X	X	X	→
System integrity		X	→	→	→	→	→
Security testing		X	X	X	X	X	X
Design specification and verification				X	X	X	X
Covert channel analysis					X	X	X
Trusted facility management					X	X	→
Configuration management					X	→	X
Trusted recovery						X	→
Trusted distribution							X
Documentation							
Security features user's guide		X	→	→	→	→	→
Trusted facility manual		X	X	X	X	X	→
Test documentation		X	→	→	X	→	X
Design documentation		X	→	X	X	X	X

Segurança nos Sistemas Distribuídos

Ataques em sistemas distribuídos

Todos os anteriores mais…

- Escuta de mensagens (*eavesdropping*)
- Falsificação de identidades (*masquerading*)
- Interferência com o fluxo de mensagens
  - Modificação de mensagens (*tampering*)
  - Inserção de mensagens
  - Remoção de mensagens
  - Troca da ordem de mensagens
- Repetição de diálogos passados (*replaying*)

Base Computacional de Confiança (TCB) nos Sistemas Distribuídos

- Existem 3 combinações possíveis:
  - Rede e sistemas operativos seguros
    - Limitativo
    - Difícil de garantir uma administração globalmente segura
    - Custo muito elevado da rede
  - Rede insegura, sistemas operativos seguros
    - Importa garantir a segurança das comunicações e a correção das interações remotas
    - A gestão dos sistemas é complexa e normalmente onerosa
  - Rede e sistemas operativos inseguros
    - Muito vulnerável
    - É difícil assegurar um nível aceitável de segurança

Base Computacional de Confiança Sistemas Distribuídos

- As duas primeiras soluções tem custos ou complexidades de gestão que são na maioria dos casos incomportáveis, mesmo para grandes organizações
- Na Internet ou redes abertas é manifestamente impossível confiar nos sistemas ou na rede

A politica mais adequada é considerar que
a segurança não se baseia na segurança da rede ou dos sistemas e admitir um **princípio de suspeição mútua** em relação a todas as entidades

“Trust no one”

Política de Segurança

- Antes de definirmos uma política de segurança, devemos responder às seguintes questões:
  - O que queremos proteger?
  - Quais as ameaças potenciais?
  - Quem as pode executar? Ou seja, quem são os atacantes?
  - Quais os ataques? Como se materializam as ameaças?

- Assim definimos um **Modelo de Ameaças**

Do Modelo de Ameaças à Política de Segurança

- A partir do modelo de ameaças, devemos decidir:
  - Quais os procedimentos e mecanismos de proteção que podem impedir os ataques considerados?
  - Qual o custo de implementação da política?
- Uma política de segurança apropriada:
  - Tem um custo inferior ao do Bem
  - Não restringe em demasia as ações dos agentes legítimos do sistema

Do Modelo de Ameaças à Política de Segurança

- Nenhum modelo de ameaças é garantidamente completo
- É necessário monitorizar sistemas para detetar ataques não previstos
  - Registar ações efetuadas por cada utilizador do sistema
  - Quando há suspeita de violação/intruso, registos devem permitir perceber ameaça imprevista
  - Política de segurança deve então ser atualizada

Que pressupostos devemos assumir?

- Normalmente, o pior caso *worst-case scenario* (salvo raras exceções)

Pressupostos no pior caso

1. As interfaces são públicas
   - As interfaces dos processos do sistema distribuído são conhecidas de todos
   - Qualquer atacante pode enviar mensagens para qualquer interface
2. As redes são inseguras
   - Mensagens podem ser escutadas, modificadas, repetidas, eliminadas, injetadas, etc.
   - Endereço do nó de origem pode ser falsificado

Pressupostos no pior caso

3. Os segredos são quebrados ao fim de algum tempo

- Chaves secretas, partilhadas entre dois interlocutores, podem ser comprometidas e descobertas por terceiros ao fim de algum tempo
- Probabilidade de chave comprometida aumenta com:
  - Tempo desde que foi gerada
  - Número de vezes que foi usada para cifrar informação trocada na rede

Pressupostos no pior caso

4. Os algoritmos e o código do programa são conhecidos pelo atacante
   - Normalmente é irrealista manter algoritmo/código secreto
   - Tornar público o algoritmo e o código permite que terceiros o validem e melhorem
5. Atacantes podem ter acesso a muitos/grandes recursos
   - Poder computacional cada vez mais barato
   - Redes permitem agregar muitos recursos a trabalhar para o ataque

Pressupostos no pior caso

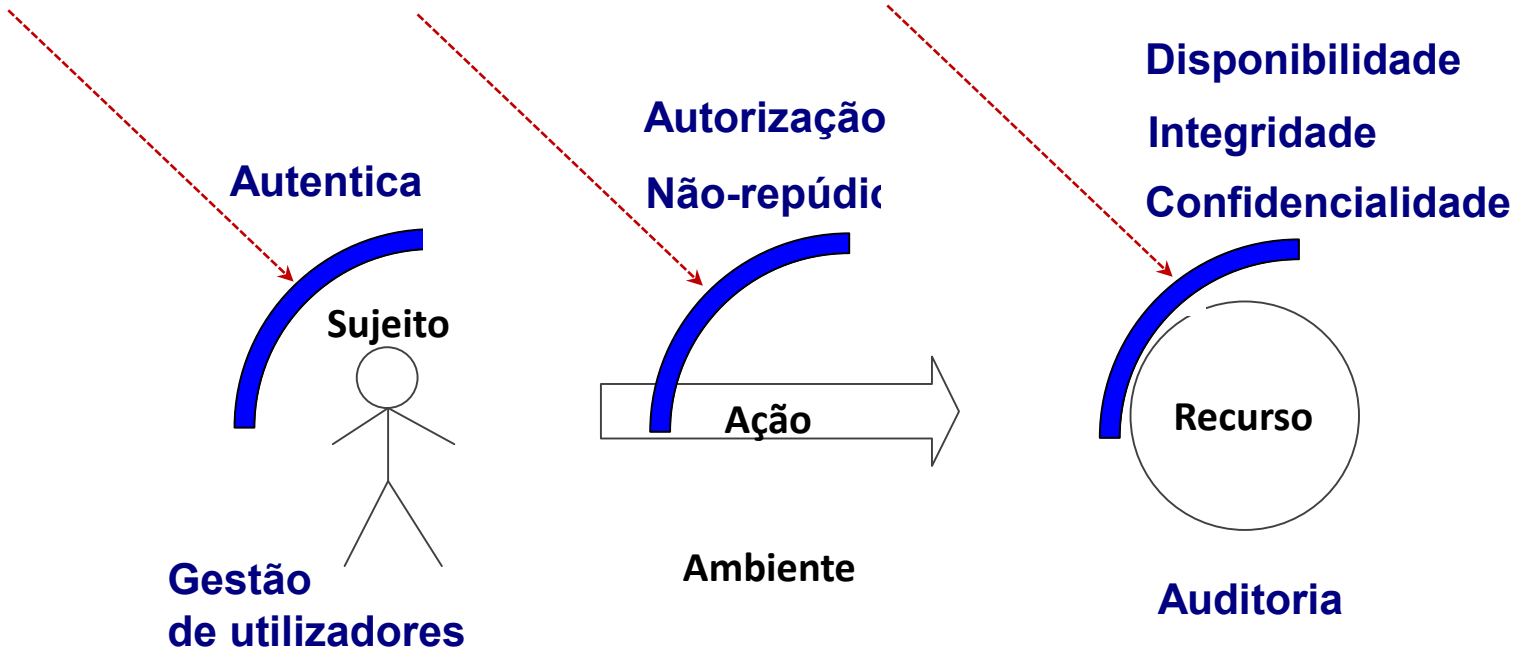
6. A base computacional de confiança (TCB) pode ter defeitos (*bugs*)

- Nos Sistemas Multiprogramados a TCB inclui:
  - **Isolamento dos espaços de endereçamento**
  - **Restrição à execução em modo utilizador de instruções privilegiadas** (ex.: interrupções, operações de E/S);
  - Utilização do núcleo exclusivamente através de **funções do sistema**
  - **Algoritmos de criptografia**
  - **Autenticação** sob controlo dos sistemas
  - **Controlo de acessos**

Sistemas Distribuídos: Políticas de Segurança

- Técnicas fundamentais para garantir a segurança num ambiente distribuído:
  - **Canais** de comunicação **seguros**
  - **Autenticação** fidedigna dos **agentes**
  - **Autorização** (controlo de acessos) no acesso aos objetos com base na identidade do agente remoto e nos direitos de acesso
  - **Autenticação** de **informação** transmitida
  - Garantia de **integridade** da **informação** transmitida

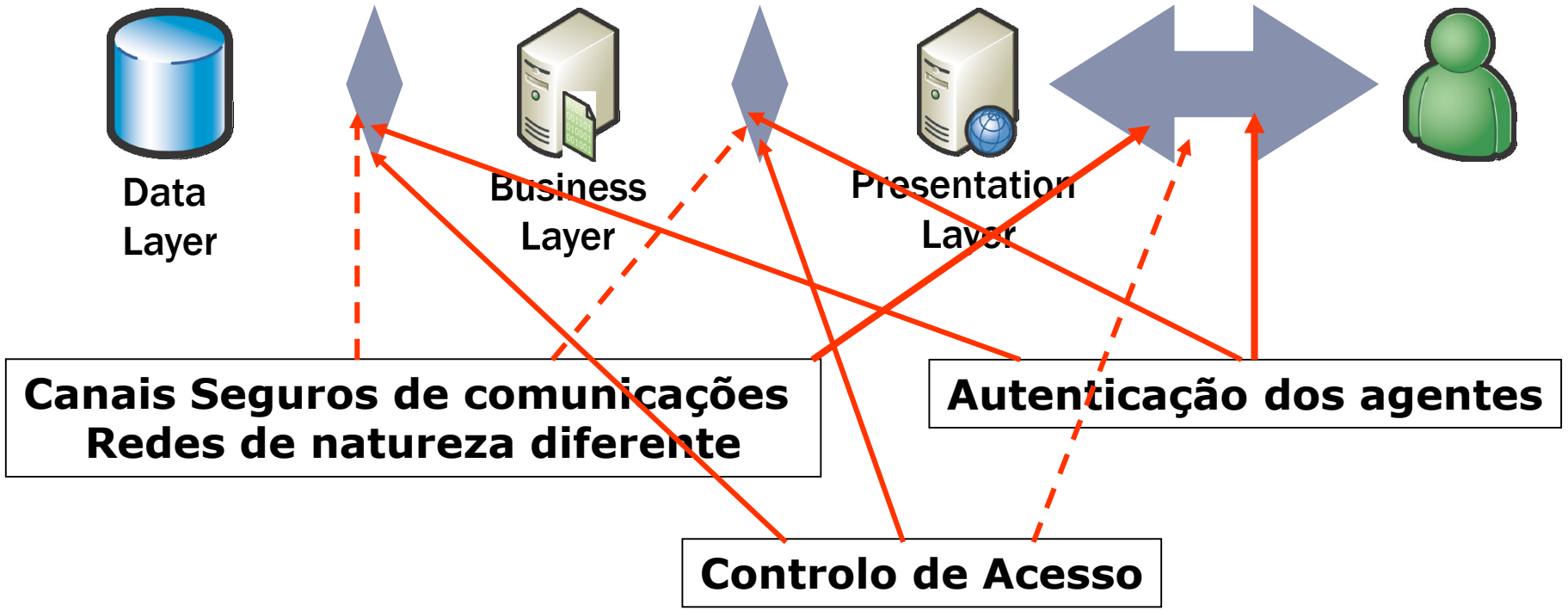
Sistemas Distribuídos:
Políticas e Mecanismos de Segurança



Isolamento da Informação

- Tornar ininteligível a informação para quem não conheça um segredo
  - **Criptografia**
- A informação cifrada encontra-se isolada porque quem não conhece o segredo que a permite decifrar não a consegue distinguir de ruído
- A informação
  - Pode ser enviada nas redes de comunicação
  - Armazenada nos sistemas de informação

Canais de segurança



Canal de Comunicação Seguro

Exemplo de invocação remota com Web Services

Cifra no Canal de Comunicação

- A base dos canais de comunicação seguros é a **cifra** da informação
- A informação é cifrada antes de ser transmitida pelo emissor
  - E é decifrada quando é recebida pelo recetor
- Se as mensagens forem cifradas
  - Evita a escuta de mensagens
  - Evita a falsificação da informação contida nas mensagens
  - Mas não evita a reutilização das mensagens

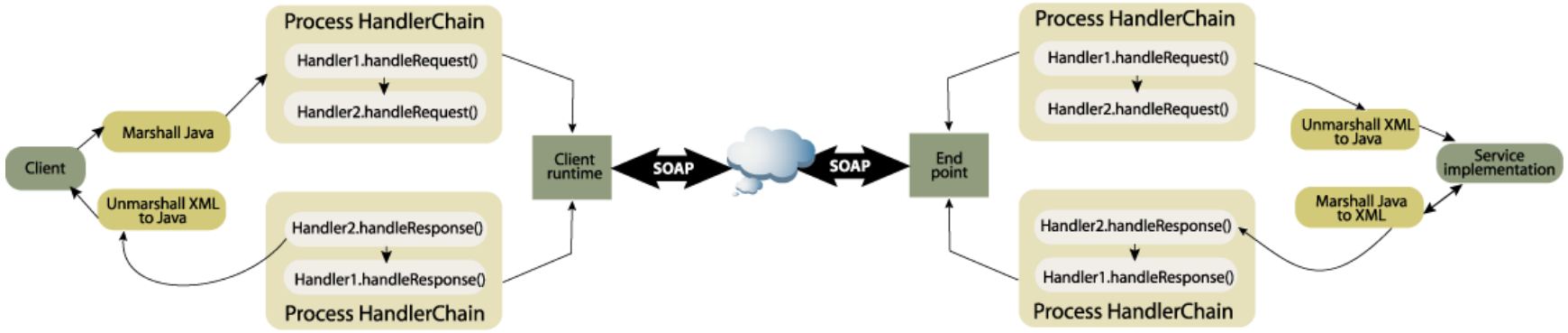
Exemplo: Canal seguro e os RPC

- Se a cifra para garantir o canal seguro for efetuada antes dos *stubs* perde-se a sua capacidade de tratar a heterogeneidade
  - Que é uma grande vantagem dos sistemas de RPC:
    tratar a heterogeneidade automaticamente
    nas funções de adaptação - *stub*
- A cifra tem de ser feita depois
  - Mas convém que seja dentro do mecanismo de RPC
    para garantir segurança de extremo-a-extremo (*end-to-end*)

Exemplo: Canal seguro e os RPC sobre SSL

- O RPC pode ser baseado num canal SSL
  mas há limitações importantes
  - Se a mensagem SOAP tiver intermediários,
    estes têm de receber apenas parte da informação
    mas não necessitam de a receber toda em aberto
- Surge a necessidade de cifrar apenas partes da mensagem
  - Os *Handlers* foram pensados para permitir implementar
    as funções de segurança na sequência certa

Web Services – JAX-WS *Handlers*



- *Handler Chain*
  - Sequência de *handlers* executados sobre pedidos e respostas
- Handler
  - Estende a classe
    - `javax.xml.ws.handler.Handler`
  - Métodos relevantes
    - `handleMessage(MessageContext context)`
    - `handleFault(MessageContext context)`

Exemplo JAX-WS *handler* de segurança

```
public boolean handleRequest(MessageContext context) {
    System.out.println("handleRequest(MessageContext=" + context + ")");
    try {
        SOAPMessageContext smc = (SOAPMessageContext) context;
        SOAPMessage msg = smc.getMessage();
        SOAPPart sp = msg.getSOAPPart();
        SOAPEnvelope se = sp.getEnvelope();
        SOAPBody sb = se.getBody();
        SOAPHeader sh = se.getHeader();
        if (sh == null) { sh = se.addHeader(); }

    // cipher message with symmetric key
        ByteArrayOutputStream byteOut = new ByteArrayOutputStream();
        msg.writeTo(byteOut);
        Cipher cipher = Cipher.getInstance("DES/ECB/PKCS5Padding");
        cipher.init(Cipher.ENCRYPT_MODE, KeyManager.getSecretKey());
        byte[] cipheredMessage = cipher.doFinal(byteOut.toByteArray());
```

Exemplo JAX-WS *handler* de segurança

```
        // encode in base64
        BASE64Encoder encoder = new BASE64Encoder();
        String encodedMessage = encoder.encode(cipheredMessage);
        // remove clear text
        sb.detachNode();
        sh.detachNode();
        // reinitialize SOAP components
        sb = se.addBody();
        sh = se.addHeader();
        // store message
        SOAPBodyElement element = sb.addBodyElement(se.createName("CipherBody"));
        element.addTextNode(encodedMessage);
        } catch (Exception e) {
            System.out.println("Exception caught in handleRequest:\n" + e);
            return false;
        }
        return true;
    }
```

Representação de dados binários em texto

- Codificação de Base 64
- Usa um subconjunto de 64 caracteres do ASCII que são os caracteres mais “universais”
  - Caracteres que são iguais em praticamente todos os códigos:
  - A-Z, a-z, 0-9, +, /
- Caracter ‘=‘ usado no final para identificar quantidade de enchimento (*padding*) requerido
- Aumenta tamanho do conteúdo… Qual o sobrecusto (*overhead*)?
- Fundamental para sistemas baseados na comunicação em texto
  - Como os Web Services, Email, …

Exemplo

Text content	M	a	n
ASCII	77 (0x4d)	97 (0x61)	110 (0x6e)
Bit pattern	0 1 0 0 1 1 0 1	0 1 1 0 0 0 0 1	0 1 1 0 1 1 1 0
Index	19	22	5	46
Base64-encoded	T	W	F	u

Octetos transformados em grupos de 6 bits ($2^6 = 64$)

Overhead = 4/3 = +33%