Módulo 7

Segurança

Lição 1

Introdução a Segurança

Versão 1.0 - Jan/2008

Autor
Aldwin Lee
Cheryl Lorica

Equipe
Rommel Feria
John Paul Petines

Necessidades para os Exercícios

Sistemas Operacionais Suportados

NetBeans IDE 5.5 para os seguintes sistemas operacionais:

- Microsoft Windows XP Profissional SP2 ou superior
- Mac OS X 10.4.5 ou superior
- Red Hat Fedora Core 3
- Solaris™ 10 Operating System (SPARC® e x86/x64 Platform Edition)

NetBeans Enterprise Pack, poderá ser executado nas seguintes plataformas:

- Microsoft Windows 2000 Profissional SP4
- Solaris™ 8 OS (SPARC e x86/x64 Platform Edition) e Solaris 9 OS (SPARC e x86/x64 Platform Edition)
- Várias outras distribuições Linux

Configuração Mínima de Hardware

Nota: IDE NetBeans com resolução de tela em 1024x768 pixel

Sistema Operacional	Processador	Memória	HD Livre
Microsoft Windows	500 MHz Intel Pentium III workstation ou equivalente	512 MB	850 MB
Linux	500 MHz Intel Pentium III workstation ou equivalente	512 MB	450 MB
Solaris OS (SPARC)	UltraSPARC II 450 MHz	512 MB	450 MB
Solaris OS (x86/x64 Platform Edition)	AMD Opteron 100 Série 1.8 GHz	512 MB	450 MB
Mac OS X	PowerPC G4	512 MB	450 MB

Configuração Recomendada de Hardware

Sistema Operacional	Processador	Memória	HD Livre
Microsoft Windows	1.4 GHz Intel Pentium III workstation ou equivalente	1 GB	1 GB
Linux	1.4 GHz Intel Pentium III workstation ou equivalente	1 GB	850 MB
Solaris OS (SPARC)	UltraSPARC IIIi 1 GHz	1 GB	850 MB
Solaris OS (x86/x64 Platform Edition)	AMD Opteron 100 Series 1.8 GHz	1 GB	850 MB
Mac OS X	PowerPC G5	1 GB	850 MB

Requerimentos de Software

NetBeans Enterprise Pack 5.5 executando sobre Java 2 Platform Standard Edition Development Kit 5.0 ou superior (JDK 5.0, versão 1.5.0_01 ou superior), contemplando a Java Runtime Environment, ferramentas de desenvolvimento para compilar, depurar, e executar aplicações escritas em linguagem Java. Sun Java System Application Server Platform Edition 9.

- Para **Solaris**, **Windows**, e **Linux**, os arquivos da JDK podem ser obtidos para sua plataforma em http://java.sun.com/j2se/1.5.0/download.html
- Para **Mac OS X**, Java 2 Plataform Standard Edition (J2SE) 5.0 Release 4, pode ser obtida diretamente da Apple's Developer Connection, no endereço: http://developer.apple.com/java (é necessário registrar o download da JDK).

Para mais informações: http://www.netbeans.org/community/releases/55/relnotes.html

Colaboradores que auxiliaram no processo de tradução e revisão

Aécio Júnior
Alexandre Mori
Alexis da Rocha Silva
Angelo de Oliveira
Bruno da Silva Bonfim
Denis Mitsuo Nakasaki
Emanoel Tadeu da Silva Freitas
Guilherme da Silveira Elias
Leandro Souza de Jesus
Lucas Vinícius Bibiano Thomé
Luiz Fernandes de Oliveira Junior
Maria Carolina Ferreira da Silva
Massimiliano Giroldi
Paulo Oliveira Sampaio Reis
Ronie Dotzlaw

Auxiliadores especiais

Revisão Geral do texto para os seguintes Países:

- **Brasil** – Tiago Flach e Vinícius G. Ribeiro (Especialista em Segurança)
- **Guiné Bissau** – Alfredo Cá, Bunene Sisse e Buon Olossato Quebi – ONG Asas de Socorro

Coordenação do DFJUG

- **Daniel deOliveira** – JUGLeader responsável pelos acordos de parcerias
- **Luci Campos -** Idealizadora do DFJUG responsável pelo apoio social
- **Fernando Anselmo -** Coordenador responsável pelo processo de tradução e revisão, disponibilização dos materiais e inserção de novos módulos
- **Rodrigo Nunes -** Coordenador responsável pela parte multimídia
- **Sérgio Gomes Veloso -** Coordenador responsável pelo ambiente JEDI™ (Moodle)

Agradecimento Especial

John Paul Petines – Criador da Iniciativa JEDI™
Rommel Feria – Criador da Iniciativa JEDI™

1. Objetivos

Este módulo trata segurança na perspectiva da linguagem Java. Discutiremos porque Java é dito seguro, o que significa segurança e, mais importante ainda, aprenderemos as melhores formas de se utilizar os dispositivos de segurança da plataforma Java dentro de seus próprios projetos. Veremos algumas das características básicas da plataforma Java que proporcionam segurança: o *Class Loader*, o verificador de *bytecode* e o gerente de segurança. Também serão abordadas as extensões que valorizam o modelo de segurança em Java através das assinaturas digitais, provedores de segurança, e o controlador de acesso. O objetivo desta lição é fornecer uma compreensão da arquitetura de segurança do modelo Java e como esse pode ser melhor utilizado.

Pressupõe-se que o leitor tenha um bom conhecimento sobre programação Java. Em particular, como escrever projetos Java, pois avançados recursos de segurança e algoritmos de criptografia serão discutidos, é feito de tal forma que o leitor é primariamente interessado em utilizar a biblioteca para executar determinadas tarefas. Iremos analisar a um nível fundamental o que é uma assinatura digital e como ela pode ser criada e utilizada; entretanto, não abordaremos a teoria da criptografia por trás de uma assinatura digital ou provar que uma assinatura digital é realmente segura.

Para aqueles que são suficientemente versados nestas matérias, mostraremos como as bibliotecas podem ser incrementadas para suportar novos tipos de algoritmos criptográficos; porém, a matemática rigorosa e definições de criptografia não serão discutidas neste material.

Ao final desta lição, o estudante será capaz de:

- Conhecer sobre os principais aspectos de segurança
- Aprender boas práticas de segurança
- Observar as práticas de segurança aplicadas à linguagem Java

2. Introdução a Segurança

O Glossário Nacional de Segurança de Sistemas de Informação dos Estados Unidos (EUA) define a Segurança de Sistemas de Informação (**INFOSEC**) como:

> *Proteção de sistemas de informação contra o acesso não-autorizado a informação ou sua modificação, seja por meio de armazenamento, processamento ou tráfego, e contra a negação de serviços aos usuários autorizados ou o fornecimento destes para usuários não autorizados, incluindo medidas necessárias para detectar, documentar e bloquear tais ameaças.*

Um documento completo para maiores referencias pode ser encontrado em:

http://www.cnss.gov/Assets/pdf/nstissd_501.pdf

Uma forma simples para expressar esta definição é "prover informação e serviço correto para as pessoas certas no momento certo". Segurança da informação significa no fornecimento de dados corretos para pessoas de quem possuem direitos do acesso a tais dados. Além disso, está incluída o bloqueio da informação para pessoas sem permissão para sua visualização.

Há vários anos atrás, quando as redes de computadores não eram tão dominantes quanto são nos dias de hoje, era relativamente fácil guardar as informações. Naquela época, para poder causar algum dano ao sistema, era necessário ter acesso físico ao sistema. Acesso remoto, acessibilidade das redes e a *Internet* mudaram tudo isso.

"A rede é o computador", uma expressão criada pela *Sun Microsystems* em meados dos anos oitenta, representa uma das grandes verdades destes tempos. Temos mais e mais computadores conectados à rede a cada dia que passa. Aplicações passaram de um sistema único (por exemplo, época dos *mainframes*) para um modelo múltiplo de cooperação entre os diferentes módulos de sistemas.

À medida que a rede cresce, a segurança da informação torna-se mais vulnerável. Sistemas estão mais propensos a ataques e outras concessões de acesso e revelam uma janela aberta para grupos ou indivíduos com motivações hostis.

Especialistas em segurança costumam dizer que a melhor maneira de manter seus dados seguros é retirar o computador da rede e bloquear todas as portas para o acesso, isso inclui, portas USB, unidades de CD-ROM, DVD-ROM ou mesmo disquetes.

Infelizmente, nesse estado, o poder do sistema não é explorado de forma eficaz. Em vez de tornar o sistema indisponível para a rede, medidas de segurança devem ser definidas para proteger as informações e os serviços.

3. Os principais aspectos de segurança

Listados abaixo, estão os cinco elementos de segurança da informação aceitos.

- **Confidencialidade** – Garantia de que as informações não serão divulgadas a pessoas não autorizadas, processos ou dispositivos
- **Integridade de Dados** – Condição existente que os dados não serão interceptados no caminho de sua origem e não foram acidentalmente ou maliciosamente, modificados ou destruídos até seu destino.
- **Disponibilidade** – Acesso confiável a dados e informações de serviços para os usuários autorizados
- **Controle de Acesso –** Diz respeito ao acesso físico ou lógico do sistema
- **Não-repúdio** – Busca evitar que as partes envolvidas em um acordo ou protocolo neguem atos realizados. Diz respeito diretamente à votação digital e tratamento com dinheiro.

Confidencialidade, integridade e disponibilidade, também conhecidos como o Infosec da CIA Triad, são os principais aspectos de segurança. Cada elemento é discutido em detalhe a seguir.

3.1. Confidencialidade

De forma simples, confidencialidade restringe as informações apenas às pessoas que tenham o acesso autorizado. Isto significa que a informação só estará disponível para aqueles que têm permissão para acessar os dados. Os indivíduos que não têm acesso por direito à informação e não devem ser capazes de visualizar os dados e devem ter o acesso negado. A informação não deve ser fornecida ou difundida além do que é necessário ou autorizado.

Pode ocorrer violação de sigilo quando os dados são acessados, seja, por um indivíduo ou organização que não estão autorizados a visualizá-los.

Suponha ir a um terminal em uma agência bancária para verificar seu extrato. Coloca-se o cartão do banco, digita-se a senha e seleciona-se a opção "Emitir Extrato". É possível olhar para o lado ou para trás, para perceber se existe um "olheiro" observando essa transação. Estes "olheiros" podem não ser capazes de roubar o seu dinheiro; entretanto, irão saber quanto dinheiro sua conta contém. Não se deseja permitir que outras pessoas venham a conhecer o conteúdo de sua conta, quer seja para um fim malicioso ou não. Seu segredo é descoberto no momento em que alguém vê sua senha, a transação, ou o saldo de sua conta.

Outro exemplo que pode ser pouco claro é o de navegar na *Internet* em um *cybercafé*. Algumas dessas lojas podem ter pacotes de sensores olfativos instalados em seus servidores (*sniffers*). Pacotes de sensores olfativos são programas que interceptam e roubam informações que podem ser usadas para analisar cada registro passado através da rede ou parte da rede. Alguns destes sensores olfactivos são legitimamente utilizados para monitorar e solucionar problemas de rede. No entanto, a mesma utilidade pode também causar violações de sigilo. Estes pacotes podem ser utilizados por indivíduos mal intencionados para obter diversas informações, como o site navegado, o login do usuário e detalhes mais sigilosos, tais como, a senha de sua conta bancária, ou seu número de cartão de crédito.

Confidencialidade assegura que as informações estejam seguras, de uma forma que só as pessoas autorizadas têm a permissão para conhecer os dados.

3.2. Integridade

Garante que as informações passadas não sejam corrompidas ou alteradas de alguma forma. Esta propriedade não só assegura que sejam autênticas e completas como também, garante que possam ser confiáveis e invocadas.

Integridade assegura:

- Modificações não são feitas por pessoal não autorizado aos dados ou processos

- Alterações só podem ser realizadas por pessoal autorizado aos dados ou processos
- Os dados são internamente e externamente consistentes

No entanto, convém notar que a integridade dos dados não é lidar com a exatidão dos dados. Essa propriedade garante que somente as informações disponíveis no sistema seja a mesma informação que o usuário acessou em tempos trás. A integridade dos dados pode ser comprometida quando a informação seja corrompida, voluntariamente ou involuntariamente, antes que seja lida pelo seu destinatário. Assume-se que, se a informação foi gerada corretamente, será preservada nesse estado.

A fonte da integridade deve ser de confiança em que o remetente da informação seja alguem que realmente supomos que seja. A fonte de integridade pode ser comprometida quando um agente burla ou forja a sua identidade através de informações incorretas enviadas para um destinatário. *Spoofing* é uma situação em que os dados de identidade são falsificados por mascaramento numa situação de verdade.

Uma espécie de falsificação é chamada de *phising*. Alguns bem conhecidos endereços WEB são reproduzidos de forma a ter um visual parecido com o do endereço oficial. Este tipo de ataque é freqüentemente realizado com um endereço falso, onde as vulnerabilidades dos navegadores WEB são exploradas para encobrir a falha. Estes endereços procuram enganar os usuários solicitando informações sobre seus dados pessoais, tais como, nome completo, nome de usuário, senha e informações do cartão de crédito. Sem suspeitas, as vítimas são encaminhados para endereço e no final uma mensagem de erro é exibida indicando que a senha está incorreta. Neste momento, a informação já foi recolhida pelos atacantes para o seu próprio benefício.

Integridade de dados é ter confiança de que a informação não foi alterada entre a sua transmissão e sua recepção. Note que, em um modo formal de segurança, a integridade é mais interpretada restritivamente no sentido de proteção contra a destruição ou alteração não autorizada de informações.

3.3. Disponibilidade

No momento em que a informação é necessária, será exibida e pronta para ser utilizada pelo pessoal autorizado. Todos os recursos autorizados – dados, funcionalidades e serviços - devem estar disponíveis quando necessários.

É possível que a confidencialidade e a integridade da informação estejam protegidas porém, para um invasor, estes dados não devem ser acessíveis. Isso faz com que a informação seja inútil e, portanto, sem garantia.

Um bom exemplo da violação de disponibilidade é o da "negação de serviço" ou "ataque DoS". Um "ataque DoS" é um tipo de ataque contra uma determinada rede que se destina a colocar as redes em situação de submissão de dados, através da inundação de ataques, isto torna o tráfego inútil. Talvez um dos mais populares foi o ataque "**Code Red**" realizado em 2001.

Code Red explorava a vulnerabilidade de um determinado servidor WEB para perturbar o serviço. ***Code Red*** era um **verme** (um programa que conecta-se a outras máquinas e se auto-replica) que começou a infectar as máquinas rodando suas várias versões no servidor. O vírus enviava seu código através de uma solicitação HTTP e explorava uma determinada porta – descobrindo a vulnerabilidade. O vírus era executado no computador do cliente. Em vez de voltar a corrigir uma página da WEB, o vírus retornava seu próprio código HTML e exibia a seguinte mensagem:

Bem vindo ao http:// www.worm.com!

Atacado por chineses!

Outra versão do mesmo vírus tentou atacar um determinado endereço IP, enviando grandes quantidades de dados inúteis. O referido endereço IP pertencia ao endereço www.whitehouse.gov. Em vez de exibir o site oficial da Casa Branca, o texto apresentado acima era exibido. O tráfego do site da Casa Branca foi redirecionado para um outro endereço IP e atacou o endereço IP numa URL que não era mais válida.

Disponibilidade é a garantia de que os sistemas sejam responsáveis pela entrega,

armazenamento e processamento de informações e sejam disponíveis quando necessário, por aqueles que necessitam.

4. Boas Práticas de Segurança

Boas práticas de segurança dizem respeito aos seguintes atributos:

- Identificação e autenticação
- Autorização
- Controle de acesso
- Não repudiação
- Auditoria

4.1. Identificação e Autenticação

É um processo de dois passos que determina quem é autorizado a acessar a informação em um sistema. **Identificação** valida a identidade do usuário provendo um identificador único como o nome de usuário ou o número do usuário. **Autenticação** é o processo de verificar a identidade mostrada pelo usuário. Usada para estabelecer a validade da transmissão, do emissor ou da mensagem.

Autenticação é baseada em, pelo menos, um dos três fatores a seguir:

- *O usuário sabe* – autenticação pode ser verificada provendo algo que somente o usuário sabe, como a sua senha ou seu número de identificação pessoal (NIP)
- *O usuário possui* – autenticação pode ser verificada provendo detalhes através de um dispositivo como um cartão inteligente ou um *token*
- *O usuário é* – autenticação pode ser verificada usando a biometria, tal como, impressão digital, voz, DNA, retina ou características da íris

Identificação e autenticação são geralmente implementadas para serviços pessoais de aplicações WEB como programas de envio de e-mail, bancos on-line e leilões on-line para determinar a identidade do usuário. Sem a identificação e a autenticação, esses serviços não poderiam ser implementados porque a identidade de outros usuários seria comprometida. Imagine se fosse possível conhecer a conta bancária de outras pessoas sem nenhuma autenticação. A confidencialidade dos usuários seria comprometida.

4.2. Autorização

É o privilégio de acesso aos dados de um usuário, sistema ou processo. Autorização define as permissões e os direitos de um usuário em um sistema. Geralmente, depois de um usuário (ou processo) ser autenticado, a autorização determina o conjunto de ações que aquele usuário pode efetuar no sistema.

Os sistemas operacionais mais modernos definem conjuntos de permissões que são variações ou extensões de três tipos básicos de acesso:

- Leitura: O usuário pode ler o conteúdo dos arquivos e listar o conteúdo dos diretórios
- Escrita: O usuário pode mudar o conteúdo de um arquivo ou diretório adicionando, criando, apagando ou renomeando
- Execução: Se o arquivo for um programa, o usuário pode executar o programa. Os usuários podem entrar no diretório

Estas permissões e direitos são implementadas de maneira diferentes nos sistemas baseados em *Controle de Acesso Discrecionária* e *Controle de Acesso Mandatório*.

4.3. Controle de Acesso

Limita o acesso a recursos do sistema a usuários, processos, programas ou outros sistemas autorizados. Este é um termo genérico para o processo pelo qual um sistema controla a interação entre os usuários e os recursos do sistema.

O Controle de Acesso provê proteção contra o uso não autorizado de recursos, incluindo:

- Uso de recurso de comunicação
- Leitura, escrita ou deleção em um recurso de informação
- Execução de um recurso de processamento

Um esquema popular de controle de acesso é manter uma *Access Control List* (lista de controle de acesso) ou ACL. ACL especifica quais operações o conjunto de usuários ou grupos podem realizar nos vários recursos.

Existem dois tipos de Técnicas de Controle de Acesso:

Controle de Acesso Discrecionária (CAD) é um meio de restringir acesso a objetos baseado na identidade e na necessidade de conhecer dos usuários e/ou grupos dos quais o objeto pertence. Os controles são Discrecionária na medida em que um objeto com uma certa permissão de acesso é capaz de passar aquela permissão (direta ou indiretamente) para qualquer outro objeto.

Geralmente, elas são feito na discrição do dono do objeto, como permissões de arquivo/diretório e posse de usuário/grupo. Sistemas CAD permitem ao usuário determinar inteiramente o acesso dado aos seus recursos, o que significa que eles podem, por acidente ou malícia, conceder acesso a usuários não autorizados.

Controle de Acesso Mandatório (CAM) é um meio de restringir acesso a objetos baseado na sensitividade da informação contida nos objetos e na autorização formal dos assuntos para acessar informações de tal sensitividade.

A característica mais importante do CAM diz respeito a proibição do controle total de objetos para os usuários que os criaram. A política de segurança do sistema (como criada pelo administrador) determina inteiramente os direitos de acesso concedidos, e o usuário não pode conceder acesso mais restrito ao seus recursos do que aquele que o administrador especifica.

Por exemplo, em CAD, a usuária **Alice** pode ter a permissão tanto para ler como para alterar um arquivo, enquanto que o usuário **Bob** só pode ler o arquivo. Em contraste, um controle de acesso não discrecionário implica em que todos os usuários acessando um determinado recurso recebem os mesmos direitos, quaisquer que sejam os níveis de compartilhamento destes.

4.4. Não Repudiação

É o conceito de garantir que um contrato ou um acordo, que tenha sido feito, não possa ser negado por nenhuma das partes envolvidas em momento futuro.

- Não repudiação de origem protege contra o emissor que nega que a mensagem foi enviada. Prova que o dado foi enviado
- Não repudiação de entrega protege contra o receptor que nega que os dados foram recebidos. Prova que o dado foi recebido

Isto significa que a não repudiação garante que o emissor e o receptor foram as partes que realmente enviaram e receberam as mensagens. Em outras palavras, isto assegura que o emissor dos dados recebe uma prova da entrega da mensagem e que o receptor recebe uma prova da identidade do emissor, ou seja, nenhum dos dois poderá negar o fato.

Muitas organizações querem tornar seguras as mensagens de email de seus colaboradores. MIME Seguro é uma solução de segurança de email comumente suportada pelos servidores nos dias de hoje pois, não provê somente confidencialidade, autenticação de dados e proteção de integridade como também a não repudiação para mensagens de email usando assinaturas digitais.

4.5. Auditoria

Auditoria de segurança é a prática de coletar e avaliar as evidências de um sistema das práticas e operações de uma organização. Auditoria pode envolver avaliar e monitorar sistemas, verificar computadores em busca de fraquezas de segurança e executar sistemas de detecção de intrusos que possam sinalizar possíveis falhas. A avaliação das evidências garante se os sistemas de informação da organização estão seguros, mantem a integridade dos dados e se os mesmos estão operando efetivamente e eficientemente para atingir os objetivos da organização.

O objetivo de uma auditoria de TI é revisar e avaliar a disponibilidade, confidencialidade e integridade dos sistemas de informação das organizações respondendo as seguintes perguntas:

- Os sistemas da organização estarão disponíveis para o negócio sempre que requeridos? (Disponibilidade)
- A informação presente nos sistemas será mostrada apenas para usuários autorizados? (Confidencialidade)
- A informação provida pelo sistema é sempre confiável, precisa, e entregue no prazo? (Integridade)

Vale a pena notar que auditoria de maneira nenhuma prevê ataques. Apenas grava eventos, maliciosos ou não, para que se tenha registro de possíveis brechas que possam ser consultados para ajudar a reparar os defeitos.

Trilhas de Auditoria podem ser implementadas em qualquer sistema para gravar todas as ações dos usuários. Auditoria pode ser usada para monitorar as atividades dos usuários garantindo que nenhuma atividade maldosa seja executada. Eventos, ações e data e hora que podem ser usados para auditar uma atividade do usuário em um determinado sistema.

5. Práticas de Segurança e a linguagem Java

A plataforma Java foi projetada com uma forte ênfase em segurança. A linguagem Java é segura em tipagem. O código só pode acessar locais de memória que é autorizado a acessar, e somente, numa maneira bem definida. No mais, na linguagem Java, carregamento seguro de classe e mecanismo de verificação garantem que apenas código Java legítimo seja executado.

A arquitetura inclui um grande conjunto de interfaces de programação de aplicações, ferramentas, e implementações de protocolos de segurança, mecanismos e algoritmos comumente usados,

Interfaces de infra-estrutura de criptografia e chave pública provêm as bases para se desenvolver aplicações seguras. Interfaces para atribuir autenticação e controle de acesso habilitam aplicações a se resguardarem contra acessos não autorizados de recursos protegidos.

Isto dá ao usuário um *framework* de segurança consistente para se escrever aplicações, e também provê ao usuário ou administrador um conjunto de ferramentas para gerenciar as aplicações de maneira segura.

A plataforma Java implementa boas práticas de seguranças como mostradas na tabela abaixo. Cada característica será discutida em maior detalhe ao longo deste módulo.

	Confidencialidade	*Integridade*	*Disponibilidade*	*Identificação e Autenticação*	*Autorização*	*Não-Repudiação*	*Auditoria*	*Conteúdo*
JVM		**X**	**X**					**X**
Carregadores de Classe		**X**						**X**
Gerenciadores de Segurança		**X**			**X**		**X**	**X**
Domínios de Segurança					**X**			**X**
Criptografar, Encriptar, SSL	**X**							
Sumário de Mensagens				**X**		**X**		
Assinaturas e Certificados Digitais				**X**		**X**		
Lista de Controle de Acesso					**X**			
JAAS				**X**	**X**			

Tabela 1: Boas Práticas de Segurança e a linguagem Java

Parceiros que tornaram JEDI™ possível

Instituto CTS
Patrocinador do DFJUG.

Sun Microsystems
Fornecimento de servidor de dados para o armazenamento dos vídeo-aulas.

Java Research and Development Center da Universidade das Filipinas
Criador da Iniciativa JEDI™.

DFJUG
Detentor dos direitos do JEDI™ nos países de língua portuguesa.

Banco do Brasil
Disponibilização de seus *telecentros* para abrigar e difundir a Iniciativa JEDI™.

Politec
Suporte e apoio financeiro e logístico a todo o processo.

Borland
Apoio internacional para que possamos alcançar os outros países de língua portuguesa.

Instituto Gaudium/CNBB
Fornecimento da sua infra-estrutura de hardware de seus servidores para que os milhares de alunos possam acessar o material do curso simultaneamente.