**UNIVERSIDADE FEDERAL DE OURO PRETO – UFOP**

**CIÊNCIA DA COMPUTAÇÃO**



# SISTEMAS OPERACIONAIS

## PROVA 03

Marcus Vinícius Souza Fernandes

19.1.4046

**Ouro Preto**

**2021**

## Aspectos de segurança

Se tratando dos aspectos de segurança, é de suma importância atentar em alguns pontos do sistema operacional a ser desenvolvido, em nosso contexto o XSO. Antes de tudo, a segurança física é essencial, mantendo o software em máquinas cujo acesso é exclusivo para os operadores e que esse hardware esteja conectado apenas com outros hardwares essenciais e protegidos.

Já relacionando tecnicamente com o software, tratar a segurança da BIOS é fundamental, fazendo com que ela realize boot apenas pelo disco rígido e que qualquer acesso para edições na mesma seja coberto por senha.

Acessos a terminais e dispositivos acoplados ou externos devem ser devidamente tratados, permitindo acesso apenas a funcionalidades e informações indispensáveis para o uso e funcionamento. No que se refere aos arquivos, cuidados para garantir a sua segurança, integridade e permissões são imprescindíveis.

Na grande parte dos itens listados, uma forma de sanar e contornar estas situações é através de criptografia e ou autenticação, atualmente é bastante comum a presença da autenticação de dois fatores.

## SSL

SSL é a sigla para o termo *Secure Socket Layer*. Ela é usada para descrever o mecanismo de criptografia criado para aumentar a segurança dos dados compartilhados com a web. Com a instalação do Certificado SSL, a URL de um determinado site passa para o formato HTTP**S** (O **S** se refere ao termo *Security*) e exibe o ícone de um cadeado verde ou apenas um cadeado fechado para sinalizar que o site é “seguro”. Esta abordagem para segurança é bem discutida, uma vez que este processo significa apenas que os dados são criptografados durante a comunicação, não significa diretamente que está totalmente protegido de algum ato malicioso.

## TSL

TLS é a sigla para o termo *Transport Layer Security*, ela é a sucessora do SSL, em suma é um protocolo de segurança projetado para oferecer segurança nas comunicações das respectivas redes de computadores. Inúmeras páginas localizadas na web e programas deskto podem usar o TLS para proteger todas as comunicações entre seus servidores e navegadores.

## OpenSSL

OpenSSL é uma implementação de código aberto dos protocolos SSL e TLS feita em cima da linguagem e programação C. Ela implementa as funções básicas de criptografia e disponibiliza inúmeras funções utilitárias. Também estão disponíveis *wrappers* que permitem o uso desta biblioteca em várias outras linguagens de programação, tornando-a ainda mais acessível.

## Aplicação

Como já abordamos anteriormente os conceitos de SSL, TSL e OpenSSL, podemos unir estes itens ao nosso contexto de projeto, o desenvolvimento de um sistema operacional denominado XSO. Este SO deve assegurar uma série de diretrizes de segurança, para que seja considerado seguro o suficiente para contemplar sua missão. Para isso, seria interessante acoplar algumas funcionalidades/pacotes presentes no OpenSSL, uma vez que, elas criptografam todo o tráfego para que seja evitado sequestro de conexão, roubo de dados e demais ataques.

A adoção de alguns pacotes tais como o openssh, que trabalha toda a segurança entre o compartilhamento de arquivos entre máquinas, o openssh-askpass que sempre nos solicita senhas durante o uso do Agent OpenSSH, também o openssh-clients que contém os programas cliente, necessários para efetuar conexões criptografadas a servidores.

Toda essa arquitetura bem trabalhada com o uso destes pacotes, tornariam o XSO um sistema operacional seguro e justo para as necessidades que o mesmo deve suprir.

## Referências


https://web.mit.edu/rhel-doc/3/rhel-sag-pt_br-3/s1-secureserver-optionalpackages.html

https://lasca.ic.unicamp.br/paulo/papers/1999-SSI-paulo.perez-linuxsec.pdf

Curso Professor Sunny - Cybersecurity at the University of Saint Mary, Kansas