**Universidade do Minho**
**Departamento de Informática**

Mestrado Integrado em Engenharia Informática

# Network Security

---

# TP1 Report – Simplified Risk Analysis /Análise de Risco Simplificada

---

Grupo 5
A86617 Gonçalo Nogueira
A74806 João Amorim
A75876 Jorge Cardoso
A78566 Marcos Silva
A82529 Carlos Afonso

Braga
Outubro, 2020

# Conteúdo

# 1 Introdução

Este primeiro trabalho prático surge no âmbito da temática de Análise de Risco Simplificada de uma determinada infraestrutura de processos e comunicações, no caso com a integração da tecnologia X-Tee/X-Road, com o principal objetivo de definir e identificar possíveis vulnerabilidades, ataques e ameaças de forma a estimar o risco e sugerir controlos de segurança que possam gerir o mesmo.

O termo "segurança"é usado de diversas formas no nosso dia a dia, mas quando se trata de *computer security*, esta assenta em três pilares fundamentais em qualquer sistema: confidencialidade, integridade e disponibilidade. O primeiro assegura que todos os recursos relacionados com o sistema de informação são apenas acedidos por partes autorizados, o segundo significa que os recursos são acessíveis em momentos oportunos, ou seja, se um indivíduo tem acesso a um determinado conjunto de objetos, o mesmo não deve ser impedido de os conseguir, e por fim, integridade indica que a modificação de dados é apenas permitida a partes autorizadas.

# 2 Contextualização

É importante agora definir conceitos fundamentais em torno desta temática de forma a facilitar a análise posterior à rede fornecida no enunciado.

Começando pela distinção entre ameaça, vulnerabilidade e ataque:

- **Ameaça** - No contexto de segurança de computadores, uma ameaça é um conjunto de circunstâncias com potencial para causar perda ou dano da infraestrutura;
- **Ataque** - Um ataque é uma ameaça de segurança que envolve tentativas por parte de terceiros de obtenção, destruição, alteração, remoção ou revelação publica de dados privados de entidades quer individuais quer organizações.
- **Vulnerabilidade** - Também conhecida como falha ou fraqueza de um sistema informático que pode ser explorada e que eventualmente possibilita um ataque.

É também fulcral o esclarecimento em relação a **controlos de segurança**, que são protocolos, procedimentos ou dispositivos de *hardware/software* que visam atenuar o risco, tais como políticas de gestão de *password*, políticas de uso inapropriado, práticas de gestão de risco, entre outros.

# 3 Tarefas

Antes de passar à enumeração de possíveis ameaças, vulnerabilidades e ataques, elaborámos uma pequena análise à tecnologia *X-Tee*.

*X-Tee* é um ecossistema interoperável, pois este possui a capacidade de troca de dados entre os diversos membros. Qualquer membro do sistema se encontra capaz de aceder a um qualquer conjunto de dados que provém desta mesma tecnologia, sendo que essa troca de dados entre membros respeita os três princípios da segurança(integridade, disponibilidade e confidencialidade), uma vez que nenhumas *third parties* devem ser autorizadas a modificar esses dados durante o processo de transferência(integridade), os dados devem ser protegidos de partes não autorizadas (confidencialidade) e acessíveis por todas as partes autorizadas pelo sistema(disponibilidade).

## 3.1 Ameaças, Vulnerabilidades e Ataques

| **Ameaças** | **Ataques** | **Vulnerabilidades** |
|---|---|---|
| Acesso indevido por entidades externas (Pessoa, programa ou sistema computacional) | Cópia/Modificação/Destruição não autorizada de um programa ou ficheiro de dados / Introdução de malwares ou escutas no sistema dos utilizadores | Avaria ou falha no sistema de autenticação (Passwords fracas) / Software de fraca qualidade |
| Acesso indevido por parte de indivíduos com autorização e de baixa suspeita | Logic Bombs / Cópia/Modificação/Destruição de programas ou ficheiro de dados / Obtenção de dados privados para proveito próprio, divulgação pública ou venda | Falta de inspeção na contratação de pessoal habilitado / Baixa segurança e controlo de todo os indivíduos com acesso ao Sistema / Ex colaborador com acessos privilegiados ou conhecimento do sistema de segurança |
| Destruição de Hardware/Registos | Causas Naturais (Cheias, Incêndios) e destruição maliciosa por parte de entidades externas/internas (Medical Registries, Electronic Health Records) | Falta de segurança do Hardware (Falta Seguranças, Câmaras de Segurança e Alarmes, Localização de Hardware em zonas de risco em caso de Catástrofes Naturais). |
| 1 | 2 | 3 |

## 3.2 Recurso Crítico

Após a explicação do ponto anterior relativamente ás diversas ameaças, vulnerabilidades e ataques que a tecnologia fica exposta, abordamos agora os recursos de maior risco. O valor do recurso pode variar dependendo de vários factores, perspectiva do utilizador, o valor da reposição do recurso e o factor tempo.

De acordo com a observação do nosso grupo sobre toda a Arquitetura apresentada, encontramonos com duas situações. Se o Recurso Crítico corresponder ao Sistema que apresentará mais problemas em caso de ataque/falha, este corresponderá ao Nó Central X-Road. Este corresponde a uma arquitetura centralizada em que toda a informação e controlo passa pelo mesmo. Tal como vemos na imagem, todas as entidades fazem/recebem pedidos ao/do nó central X-Road, quer sejam Interfaces com Bases de Dados externas, sistemas informáticos dos Hospitais, Portais Online, etc.

## 3.3 Controlo de Segurança

Para uma completa análise de segurança relativamente à arquitetura apresentada, é necessário definir certos métodos de defesa que preservem a confidencialidade, integridade e disponibilidade, nomeadamente os Controlos de Segurança. Nesta arquitetura, tal como em muitas outras, será possível dividir estes controlos em partes diferentes.

Em primeiro lugar temos a Encriptação. Apesar do facto de que a Encriptação corresponde a um Controlo de Software que será mencionado mais em baixo, achamos que esta merecia uma explicação mais detalhada. Esta permite assegurar a confidencialidade, assim como a integridade dos dados, ao transformar os mesmos de maneira a que estes fiquem ilegiveis na eventualidade de um ataque. Para esta arquitetura em especifico, uma implementação de protocolos de encriptação do lado das entidades que possuem bases de dados com informações sensíveis, aliado à encriptação já existente no nó central da tecnologia X-Road, seria na opinião do grupo algo necessário para a segurança global do sistema. De notar que nem todas as entidades presentes na imagem possuem bases de dados, com um caso em que a mesma parece ser construída com base em registos fisicos, tal como se vê nos "Medical Registries".

De seguida, os Controlos de Software. Uma vez que cada entidade no sistema terá acesso a determinadas informações, baseadas nos protocolos previamente definidos, é necessário que cada uma tenha programas de controlo internos que funcionarão com base nos já mencionados protocolos, controlos a nível de sistema operativo e de rede que protejam cada utilizador de entidades externas, programas de controlo independentes como o caso de anti-virus e detetores de invasões, verificadores de passwords, entre outros. Por mim e não menos importante, garantir a qualidade de código produzido nos programas que são desenvolvidos de maneira a prevenir ao máximo quaisquer vulnerabilidades. Uma vez que nesta arquitetura, qualquer componente é constituída por hardware que por sua vez funciona à base de software, com a exceção dos Medical Registries, todos estes Controlos de Software deveriam ser aplicados em cada um.

Por fim e não menos importante, é imprescindível a implementação de Controlos de Hardware, Controlos Físicos e certas Políticas de Segurança. Os controlos de Hardware passarão pela Encriptação de peças de hardware utilizadas nos diferentes sistemas, sistemas de deteção de invasões, verificação das identidades de cada utilizador, firewalls, entre outros. No caso dos controlos físicos, é extremamente necessário a criação de controlos físicos para cada sistema, sejam estes para a prevenção de desastres naturais, como cheias ou incêndios, ou o uso de fechaduras avançadas, seguranças, câmaras de segurança e backup de dados e software relevantes. Por fim, o uso de políticas de segurança, baseadas na definição de regras para utilizadores assim como o treino especializado para os mesmos, tal como a constante troca de passwords e o cuidado no acesso a websites indevidos, diminuirá sem dúvida o risco para este e qualquer outro sistema.

# 4 Conclusão

Com este trabalho introdutório à Segurança de Informação, o nosso grupo adquiriu conhecimentos que serão certamente necessários para futuros trabalhos, nomeadamente a noção de algumas propriedades fundamentais como a confidencialidade, a integridade e a disponibilidade, assim como a percepção daquilo que são ameaças, ataques e vulnerabilidades, e a capacidade de as distinguir.

# 5 Bibliografia

Pfleeger, Charles P., Pfleeger, Shari L., *Security in Computing*, Fourth Edition, Prentice Hall PTR, 2007

`https://www.ria.ee/en/state-information-system/x-tee.html`