Instituto Federal de Educação, Ciência e Tecnologia da Bahia - IFBA
Departamento de Ciência da Computação
Tecnólogo em Análise e Desenvolvimento de Sistemas

Confiabilidade e proteção

André L. R. Madureira <andre.madureira@ifba.edu.br>
Doutorando em Ciência da Computação (UFBA)
Mestre em Ciência da Computação (UFBA)
Engenheiro da Computação (UFBA)

Confiabilidade de sistemas

- Sistemas de software são muito importantes para os governos, empresas e indivíduos
  - Sem software, muitas atividades não seriam viáveis
  - **Ex**: lançamento de foguetes, controle de tração e estabilidade das rodas, freio ABS
- É essencial que o software usado seja confiável
  - O software deve estar disponível quando necessário
  - O software deve funcionar corretamente, sem efeitos colaterais indesejáveis

Confiabilidade de sistemas

- A confiança de um sistema é mais importante do que sua funcionalidade
  - Falhas no sistema afetam um grande número de pessoas
    - Já a ausência de uma função afeta um pequeno número de pessoas
  - Usuários rejeitam sistemas não confiáveis ou inseguros
  - Custos de falha de sistema podem ser enormes
  - Sistemas não confiáveis podem causar perda de informações

Confiabilidade de sistemas

- Ao projetar um sistema confiável, precisamos considerar:
  - **Falha de hardware**
  - **Falha de software**
  - **Falha operacional**
- Essas falhas podem ser inter-relacionadas
  - Falha de hardware => Estresse nos usuarios
  - Estresse nos usuários => Falhas operacionais e de software

Confiança

- **Confiança** de um sistema de computador é uma propriedade do sistema que reflete sua **fidedignidade**
  - **Fidedignidade:** grau de confiança de um usuário no funcionamento esperado pelo sistema
    - *“o sistema não falhará em condições normais de uso”*
  - **Métrica qualitativa**
    - **Ex**: não confiável, muito confiável, ultraconfiável

Confiança x Utilidade

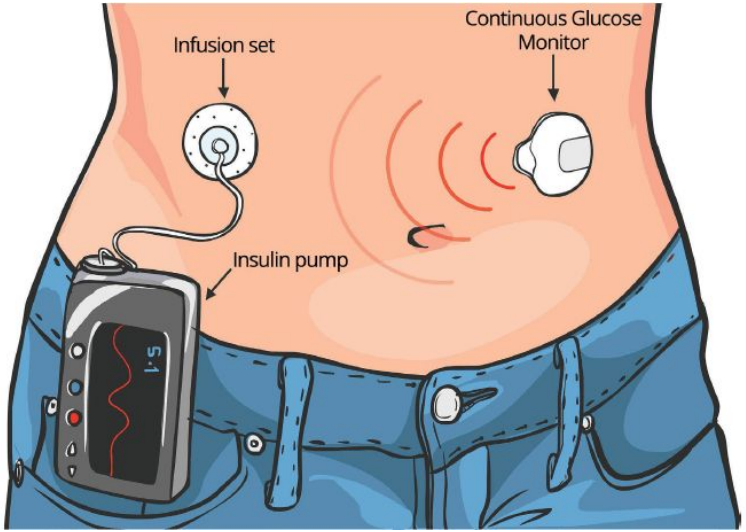
- **Confiança e utilidade não são sinônimos**
  - **Ex:** Word
    - É útil, pois facilita a escrita de documentos
    - Não é confiável, pois ele tem bugs e trava com frequência
      - **Solução**: salvar várias cópias de um documento, como um mecanismo controle de danos e falhas

Dimensões da confiança (propriedades)

- **Disponibilidade:** A probabilidade do sistema de entregar serviços quando requisitado (sistema estar ativo e funcionando)
- **Confiabilidade:** A probabilidade do sistema de entregar serviços conforme especificados
- **Segurança:** A probabilidade do sistema de operar sem **falhas catastróficas**
- **Proteção:** A probabilidade do sistema de se **proteger de intrusão** acidental ou não

Dimensões da confiança (propriedades)

- **Nem todo sistema precisa de todas as propriedades da confiança**
  - **Ex:** sistema de bombeamento de insulina



Disponibilidade: sistema ativo para quando for necessário aplicar insulina

Confiabilidade: sistema aplica a dose correta de insulina

Segurança: sistema nunca aplica uma dose perigosa de insulina

Proteção: não é necessária

Disponibilidade e confiabilidade

- **Sistema com alta disponibilidade:** é aquele no qual os usuários esperam que um serviço esteja sempre disponível
  - **Ex:** 

- Nem todo sistema que requer alta disponibilidade precisa também de alta confiabilidade
  - **Ex**: 

Disponibilidade e confiabilidade

- Formalmente:
  - **Disponibilidade**: *"É a probabilidade de um sistema, em determinado momento, ser operacional e capaz de entregar os serviços solicitados." (SOMMERVILLE, 2003)*
  - **Confiabilidade**: *"É a probabilidade de uma operação livre de falhas durante um tempo especificado, em determinado ambiente, para uma finalidade específica." (SOMMERVILLE, 2003)*

Disponibilidade

- Disponibilidade não depende apenas do número de falhas no sistema, mas também do **tempo necessário para reparar os defeitos que causaram a falha**
  - **Ex**: o sistema A falha 1 vez por ano |
    o sistema B falha 1 vez por mês
    - Quando A falha, demora 3 dias para reiniciar
    - Quando B falha, demora 10 min para reiniciar
    - Qual é mais confiável em termos de disponibilidade?

Exemplo de Calculo de Disponibilidade

- **Ex**: sistema A falha 1 vez por ano (e reinicia em 3 dias), enquanto que sistema B falha 1 vez por mês (e reinicia em 10 min)

Tempo Offline (A) = 3 dias x 24 horas x 60 min x 1 vez ao ano = 4320 min / ano

Tempo Offline (B) = 10 min x 1 vez ao mes x 12 meses = 120 min / ano

Apesar de B falhar mais vezes, ele é mais confiável.
Qual a disponibilidade em percentual?

Exemplo de Calculo de Disponibilidade

- **Ex**: sistema A falha 1 vez por ano (e reinicia em 3 dias), enquanto que sistema B falha 1 vez por mês (e reinicia em 10 min)

Tempo Offline (A) = 3 dias x 24 horas x 60 min x 1 vez ao ano = 4320 min / ano

Tempo Offline (B) = 10 min x 1 vez ao mes x 12 meses = 120 min / ano

Total de minutos em um ano = 12 meses x 30 dias x 24 h x 60 min = 518400 min / ano

Disponibilidade = 100 - 100 x Tempo Offline / Total de Tempo

Disponibilidade (A) = 100 - 100 x 4320 / 518400 = **99,1666%**
Disponibilidade (B) = 100 - 100 x 120 / 518400 = **99,9768%**

Exercício

Marque a alternativa que contém **somente** as assertivas VERDADEIRAS.

I - Falhas de um sistema não estão inter-relacionadas. F

II - Um sistema confiável deve avaliar possíveis falhas de hardware, software e operacionais, somente. V

III - A confiança de um sistema é uma propriedade que reflete a sua fidedignidade, podendo ser avaliada por uma métrica qualitativa. V

IV - A confiança e utilidade são sinônimos, pois um sistema não confiável não é útil para seu usuário. F

- ( ) Somente II, III e IV.
- ( ) Somente II.
- ( ) Somente I, II e III.
- ( ) Somente III.
- ( ) Somente II e III.

Seguem as assertivas com os ajustes necessários para torná-las VERDADEIRAS:

I - Falhas de um sistema ESTÃO inter-relacionadas, pois a presença de uma falha pode implicar na ocorrência de outra (ex: falha de hardware => falha de software).

IV - A confiança e utilidade NÃO são sinônimos, pois um sistema PODE SER ÚTIL, porém NÃO CONFIÁVEL devido a presença de falhas ou bugs.

Impacto da Interrupção na Disponibilidade

- É difícil avaliar o impacto na interrupção de um serviço fornecido por um sistema usando uma métrica simples
  - O momento em que a interrupção ocorre é importante
  - **Ex**: Suponha dois sistemas A e B, que são usados pelas Casas Bahia. Ambos ficam indisponíveis por 1h por dia.
    - Sistema A fica indisponível entre as 03 e 04h da manhã, e B fica indisponível entre as 13 e 14h da tarde
    - Qual deles irá afetar mais usuários?

Terminologia da Confiabilidade

- Quando se trata de confiança de sistemas, precisamos saber usar os termos corretos para descrever os problemas:

Termo	Descrição
Erro humano ou engano (1)	O comportamento humano, que resulta na introdução de defeitos em um sistema. Por exemplo, no sistema meteorológico no deserto, um programador pode decidir que a forma de calcular o tempo para a próxima transmissão é acrescentar uma hora à hora atual. Isso funciona, exceto quando o tempo de transmissão é entre as 23:00 hs e a meia-noite (meia-noite é 00:00 no horário de 24 horas).
Defeito de sistema (2)	Uma característica de um sistema de software que pode levar a um erro de sistema. O defeito é a inclusão do código para adicionar uma hora à hora da última transmissão, sem verificar se já passou das 23:00 hs.
Erro de sistema (3)	Um estado errôneo de sistema que pode levar a um comportamento do sistema inesperado por seus usuários. O valor do tempo de transmissão é definido incorretamente (a 24.XX em vez de 00.XX) quando o código com defeito é executado.
Falha de sistema (4)	Um evento que ocorre em algum momento em que o sistema não fornece um serviço como esperado por seus usuários. Nenhum dado meteorológico é transmitido porque a hora é inválida.

Confiabilidade

- A confiabilidade de um programa depende do **número de entradas que causam saídas errôneas** (falhas) durante o uso normal do sistema pela maioria dos usuários
  - Os defeitos de software que só ocorrem em situações excepcionais têm pouco efeito prático sobre a confiabilidade do sistema
    - **Porque?**

Confiabilidade

Devemos investir nosso tempo para corrigir defeitos que sejam relevantes!

- Os defeitos de software que só ocorrem em situações excepcionais têm pouco efeito prático sobre a confiabilidade do sistema
  - **Ex**: Mills et al. (1987) descobriu que a remoção de 60% dos erros conhecidos em seu software resultou em melhora na confiabilidade do sistema de apenas 3%
  - **Ex**: Adams (1984) observou que muitos defeitos nos produtos da IBM só causariam falhas após centenas ou milhares de meses de uso do produto

Confiabilidade

- Defeitos de sistema nem sempre resultam em erros de sistema, e erros de sistema não resultam necessariamente em falhas de sistema
  - Nem todos os códigos de um programa são executados
  - Os erros são transitórios
  - O sistema pode incluir a detecção de defeitos e mecanismos de proteção
  - Os usuários evitam entradas que eles sabem que causam falhas no sistema

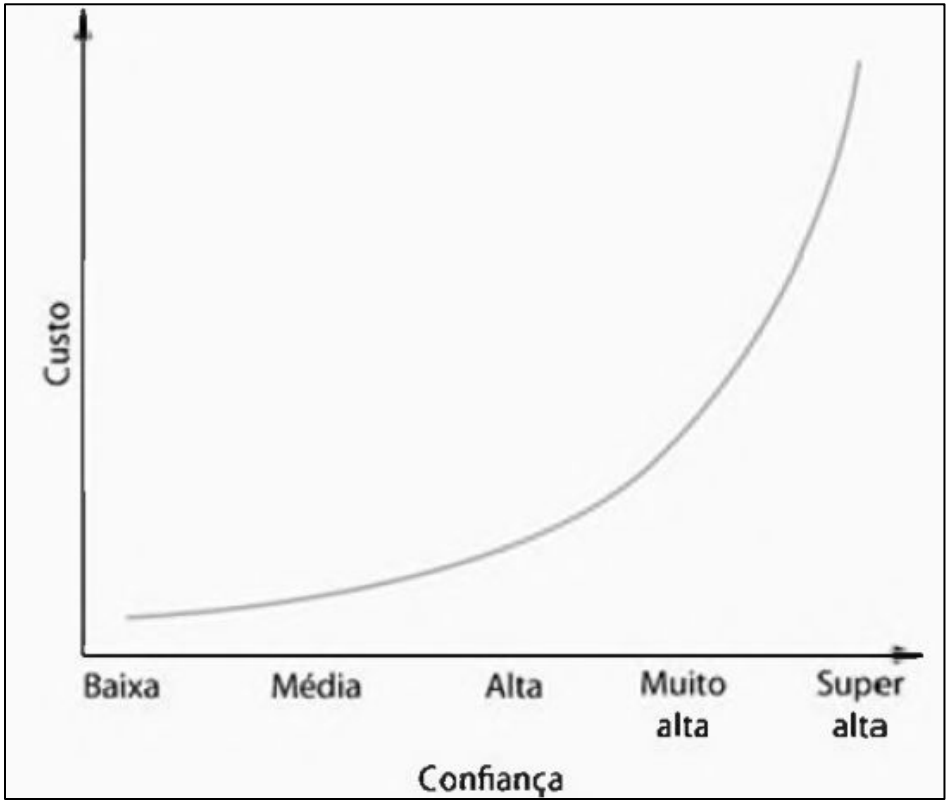
Como garantir a confiança de um sistema?

- **Evitar a introdução de erros** no sistema durante a sua especificação e desenvolvimento
- Projetar **processos de verificação e validação** eficazes na descoberta de erros que afetam a confiança do sistema
- Projetar **mecanismos de proteção contra ataques** externos que comprometam a disponibilidade ou a proteção do sistema
- O sistema implantado e seu software de suporte sejam **configurados corretamente** para seu ambiente operacional

Limitações no projeto de sistemas confiáveis

- Projetar sistemas confiáveis envolve maior custo durante as etapas de implementação e validação
  - Sistemas ultra confiáveis possuem custos ainda maiores
    - **Ex**: sistemas de controle de segurança em aeroportos
- Há perda de desempenho conforme monitoramos o sistema por erros (ex: erros de entrada de usuário, erros outros)
  - Verificações adicionais são necessárias a cada vez que o sistema executa

Limitações no projeto de sistemas confiáveis



É fácil (e barato) obter melhorias significativas em softwares com baixa confiança

Conforme o software se torna mais confiável, aumentar ainda mais essa confiança requer custos (e esforço) exponencialmente maiores

Precisamos de mais testes para garantir níveis de confiança maiores

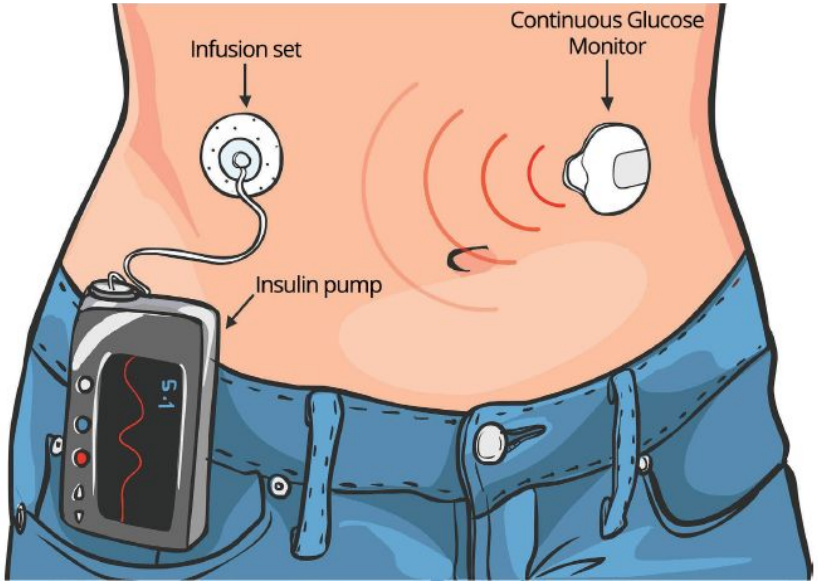
Construir testes envolve custo e esforço significativos!

Segurança

- Alguns sistemas são críticos em termos de segurança
  - **Ex**: usina nuclear, plantas químicas, aeronaves
- Esses sistemas nunca devem causar danos às pessoas ou ao ambiente, mesmo que ocorra uma falha
- Podem ser classificados como:
  - **Software crítico de segurança primária**
  - **Software crítico de segurança secundária**

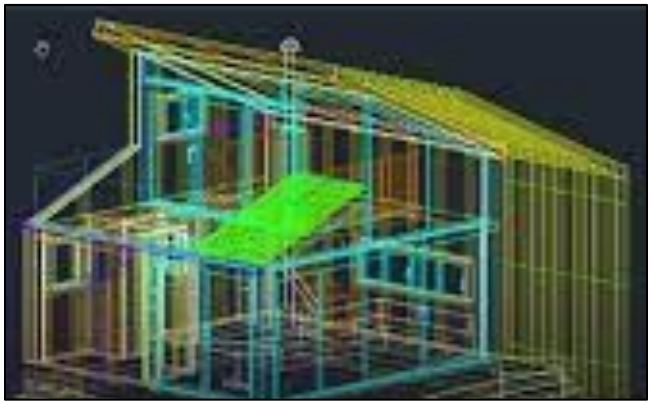
Software crítico de segurança **primária**

- É um software que está embutido (**ex**: *firmware* de hardware, controlador de um sistema)
- O mau funcionamento do software pode causar mau funcionamento do hardware
  - Causando danos às pessoas ou ao ambiente
  - **Ex**: bomba de insulina



Software crítico de segurança **secundária**

- É um software que pode resultar indiretamente em um dano
  - **Ex**: Autocad, Revit
    - Uma falha no projeto estrutural de uma casa pode causar uma execução incorreta da construção, culminando com o desabamento da casa!



Segurança x Confiabilidade

- Os sistemas de software que são confiáveis não são neces sariamente 100% seguros
  - **Não há como ter certeza que um software é tolerante a defeitos, ou está completamente livre de defeitos**
    - Defeitos podem ficar adormecidos por muitos anos
  - **A especificação do sistema pode estar incompleta** (requisitos mal descritos, ausencia de requisitos importantes)
  - **Sistema suscetível ao mau funcionamento de hardware** (que causam instabilidades no sistema)

Segurança x Confiabilidade

- Os sistemas de software que são confiáveis não são neces sariamente 100% seguros
  - **Os operadores de sistema podem gerar entradas que causem mau funcionamento do sistema**
    - Não necessariamente as entradas estão erradas
    - **Ex**: (CASO REAL) Um piloto de aeronave solicitou o levantamento do trem de pouso do avião, sendo que este ainda estava em solo (não tinha levantado voo ainda)

Exercício

Marque a alternativa que contém **somente** as assertivas VERDADEIRAS.

I - Podemos calcular a disponibilidade de um sistema e utilizar essa métrica isoladamente para avaliar o impacto da interrupção na disponibilidade de um sistema. F

II - Os defeitos de software que ocorrem somente em situações excepcionais têm pouco efeito sobre a confiabilidade do sistema. V

III - Uma falha no sistema pode ocorrer em consequência de um defeito, resultante de um erro de sistema ocasionado por um erro humano. F

IV - Defeitos nem sempre ocasionam erros de sistema. E erros de sistema não geram, necessariamente, falhas de sistema. V

- ( ) Somente I, II e IV.
- ( ) Somente II, III e IV.
- ( ) Somente II.
- ( ) Somente III e IV.
- (→) Somente II e IV.

Seguem as assertivas com os ajustes necessários para torná-las VERDADEIRAS:

I - Podemos calcular a disponibilidade de um sistema e utilizar essa métrica para avaliar o impacto da interrupção na disponibilidade de um sistema, PORÉM esta não deve ser utilizada isoladamente. Isto porque o momento em que a falha acontece pode impactar mais ou menos usuários de um sistema (Ex: estar indisponível entre as 03 e 04h não tem o mesmo impacto sobre a disponibilidade do que a indisponibilidade entre as 13 e 14h da tarde).

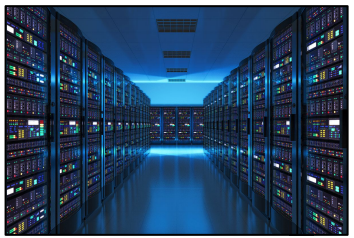
III - Uma falha no sistema pode ocorrer em consequência de um ERRO DE SISTEMA, resultante de um DEFEITO ocasionado por um erro humano.

Terminologia de Segurança

	Termo	Definição
(2)	Acidente (ou desgraça)	Um evento não planejado ou uma sequência de eventos que resulta em morte ou dano pessoal, danos à propriedade ou ao meio ambiente. Uma *overdose* de insulina é um exemplo de acidente.
(1)	Perigo	Uma condição com o potencial de causar ou contribuir para um acidente. Uma falha do sensor que mede a glicose no sangue é um exemplo de um perigo.
(3)	Dano	Uma medida do prejuízo resultante de um acidente. Os danos podem variar desde muitas pessoas sendo mortas como resultado de um acidente a ferimentos leves ou danos materiais. Danos resultantes de uma overdose de insulina podem ser lesões graves ou a morte do usuário da bomba de insulina.
	Severidade do perigo	Uma avaliação dos piores danos possíveis que poderiam resultar de um perigo. Severidade de perigo pode variar de catastrófico, em que muitas pessoas são mortas, a menor, em que os resultados são pequenos danos. Quando a morte de um indivíduo é uma possibilidade, uma avaliação razoável da severidade do perigo é 'muito elevado'.
	Probabilidade de perigo	A probabilidade dos eventos que estão ocorrendo e são capazes de criar um perigo. Os valores de probabilidade tendem a ser arbitrários, mas variam de 'provável' (digamos 1/100 chance de ocorrência de perigo) a 'implausível' (sem situações concebíveis ou prováveis de ocorrência de perigo). A probabilidade de uma falha de sensor da bomba de insulina resultar em uma *overdose* provavelmente é baixa.
	Risco	Essa é a medida da probabilidade de o sistema causar um acidente. O risco é avaliado considerando-se a probabilidade de perigo, a severidade do perigo e a probabilidade de o perigo causar um acidente. O risco de uma *overdose* de insulina é, provavelmente, médio a baixo.

Acidentes

- Acidentes normalmente acontecem em consequência de uma **combinação de falhas** em partes diferentes de um sistema
  - Combinações inesperadas de falhas de subsistemas, que levam a interações que resultam em falha global do sistema
  - **Ex**:



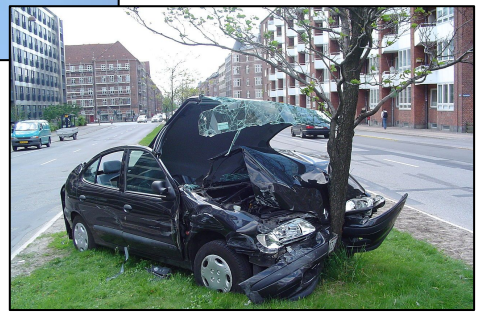
falha no ar-condicionado => superaquecimento do datacenter

superaquecimento => sinais incorretos no hardware

sinais incorretos no hardware => falha do sistema

Acidentes

- **Não é possível prever todas as combinações possíveis de falhas**
  - Acidentes são inevitáveis, em qualquer sistema



Proteção

- É um atributo do sistema que reflete sua capacidade de se proteger de ataques externos (acidentais ou deliberados)
  - **Ex**: virus, cavalos de troia, backdoors

Proteção

- Há sistemas em que a proteção é a dimensão mais importante da confiança do sistema
    - **Ex**: sistemas militares, sistemas que armazenam informações sigilosas (Serviço Único de Saúde - SUS)

SUS
Sistema Único de Saúde

ALCOÓLICOS ANÔNIMOS
UNIDADE SERVIÇO RECUPERAÇÃO

Terminologia de Proteção

Termo	Definição
Ativo (0)	Algo de valor que deve ser protegido. O ativo pode ser o próprio sistema de software ou dados usados por esse sistema.
Exposição (4)	Possíveis perdas ou danos a um sistema de computação. Pode ser perda ou dano aos dados, ou uma perda de tempo e esforço, caso seja necessária a recuperação após uma brecha de proteção.
Vulnerabilidade (1)	A fraqueza em um sistema computacional, que pode ser explorada para causar perdas ou danos.
Ataque (2)	Uma exploração da vulnerabilidade de um sistema. Geralmente, vem de fora do sistema e é uma tentativa deliberada de causar algum dano.
Ameaças (3)	Circunstâncias que têm potencial para causar perdas ou danos. Você pode pensar nisso como uma vulnerabilidade de um sistema submetido a um ataque.
Controle	Uma medida de proteção que reduz a vulnerabilidade do sistema. A criptografia é um exemplo de controle que reduz a vulnerabilidade de um sistema de controle de acesso fraco.

Tipos de Ameaças à Proteção de um Sistema

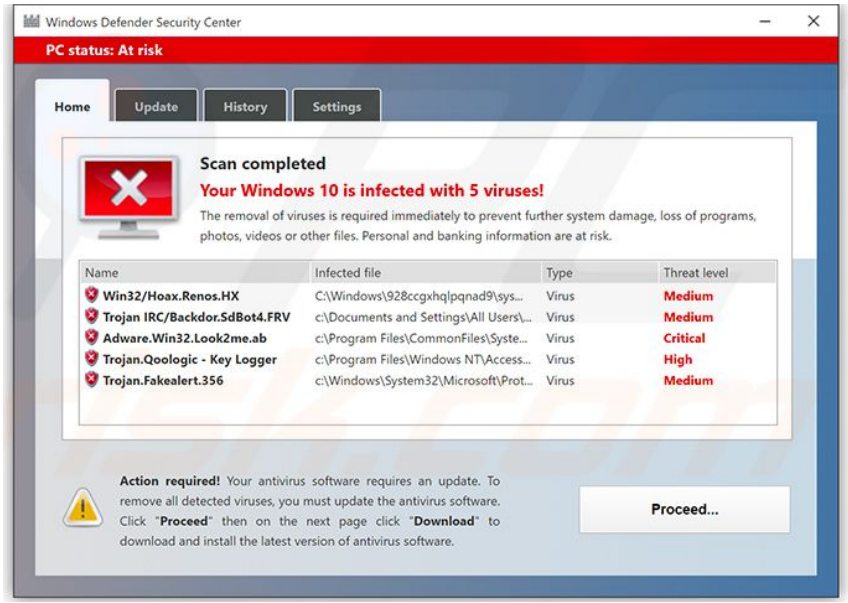
- Existem várias ameaças à proteção de um sistema, dentre elas as mais relevantes são:
  - Ameaças à **confidencialidade**
  - Ameaças à **integridade**
  - Ameaças à **disponibilidade**

Ameaças à confidencialidade

- Ameaças que podem divulgar informações para pessoas ou programas não autorizados

Ameaças à integridade

- Ameaças que podem danificar o software ou corromper seus dados
  - **Ex**: virus, cavalo de troia



Ameaças à disponibilidade

- Ameaças que podem restringir o acesso ao software ou a seus dados para os usuários do sistema
  - **Ex:** *ransomware*

Proteção

- A maioria das vulnerabilidades em sistemas sociotécnicos resulta de falhas humanas e não de problemas técnicos
  - **Ex:** senhas fáceis de adivinhar, anotar a senha em um pedaço de papel, erros na configuração de controle de acesso
- Como melhorar a proteção de sistemas:
  - **Prevenção de vulnerabilidade**
  - **Detecção e neutralização de ataques**
  - **Limitação de exposição e recuperação**

Exercício

Considerando a segurança de sistemas, marque a alternativa que contém **somente** as assertivas VERDADEIRAS.

I - A severidade do perigo é a avaliação dos piores danos possíveis que poderiam resultar em um perigo. V

II - Probabilidade de perigo é uma avaliação da possibilidade de um perigo causar um acidente. F

III - Risco é a probabilidade de um perigo causar um dano. F

IV - Seguindo a terminologia de segurança de sistemas, a ordem correta de ocorrencia de um dano é: (1) Perigo, (2) Acidente (ou desgraça), e (3) Dano. V

- Todas as assertivas são verdadeiras.
- Somente I, II e III.
- Somente II, III e IV.
- Somente II e III.
- Nenhuma das alternativas anteriores.

Seguem as assertivas com os ajustes necessários para torná-las VERDADEIRAS:

II - Probabilidade de perigo é uma avaliação da possibilidade dos eventos que estão ocorrendo serem capazes de criar um perigo.

III -Risco é a probabilidade do sistema causar um acidente.

Referencial Bibliográfico

- SOMMERVILLE, Ian. **Engenharia de Software**. 6. ed. São Paulo: Addison-Wesley, 2003.

- PRESSMAN, Roger S. **Engenharia de Software**. São Paulo: Makron Books, 1995.

- JUNIOR, H. E. **Engenharia de Software na Prática**. Novatec, 2010.

Obrigado!

- **Perguntas?**