INE5429-07208 Segurança em Computação Noções Básicas de Segurança

Prof. Jean Everson Martina

O que é segurança em Computação?

Math?

Engineering?

Philosophy?

Natural Sciences?

Qual a diferença?

Conhecendo o adversário

- Segurança em Computação estuda como os sistemas computacionais se comportam na presença de um adversário.
- Nós consideramos este adversário inteligente.
  - Ele tenta achar formas de comportamento não esperado que levam o sistema falhar
  - Essas falahas podem ser exploradas subvertendo a segurança.

Para Ganhar devemos Conhecer o Adversário

- Quais os motivos para sermos atacados?
- Quais são as capacidades do atacante?
- O que ele sabe de antemão?
- Quais os pontos fracos da minha estrutura?
- Quem pode ser o atacante?
- Qual o nível de acesso dele?
- Que contra-medidas eu posso tomar?
- Deu Ruim! O que eu faço pra continuar?
- Como eu descubro exatamente o que aconteceu?

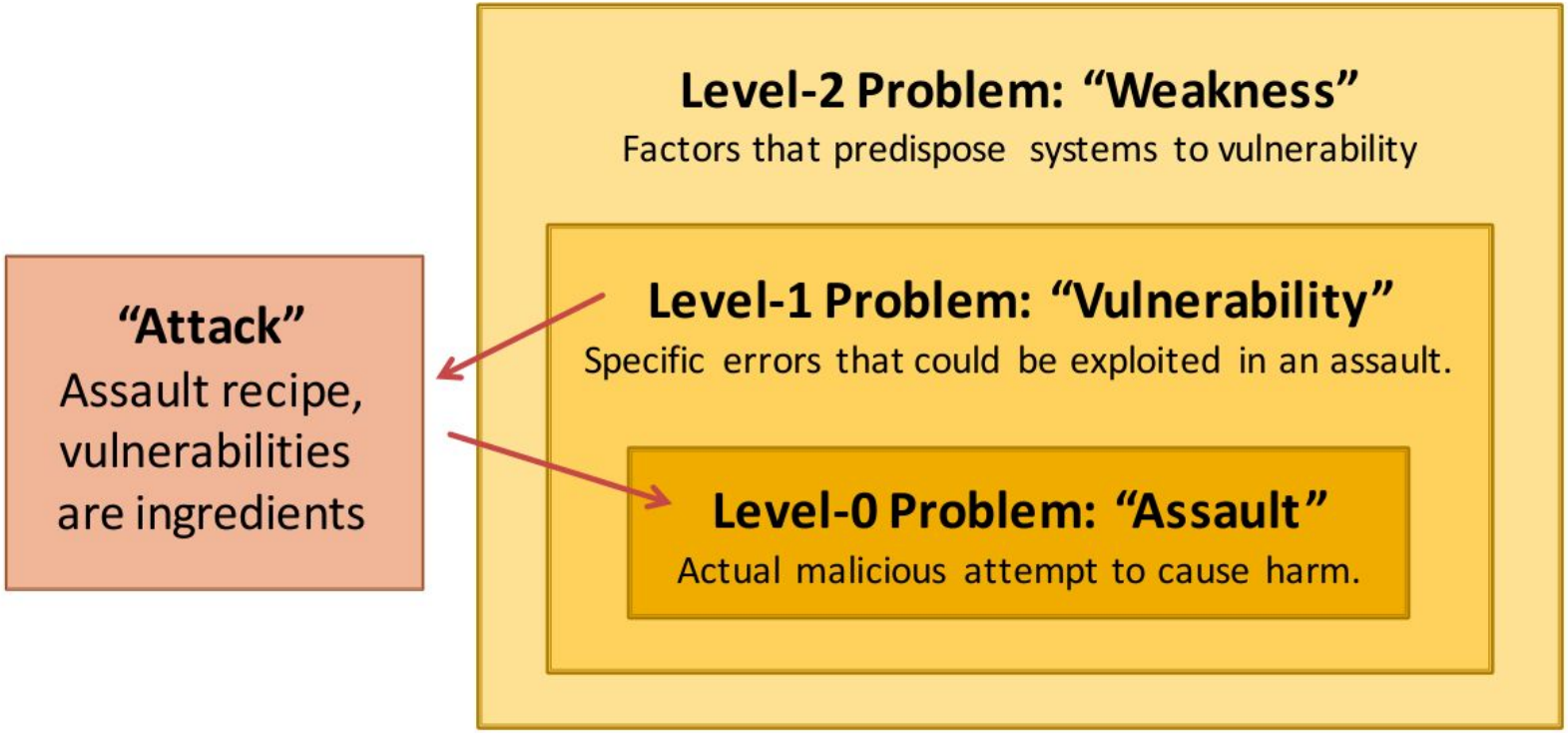
A Forma de Pensar em Segurança

- Pensando como um atacante:
  - Entender as técnicas para contornar a segurança.
  - Procurar formas como o mecanismo de segurança podem quebrar
- Pensando como um defensor
  - Entenda o que você está defendendo e contra quem
  - Leve em conta o custo x benefício
  - Nenhum sistema é seguro pra sempre
  - Tenha um certo grau de paranóia.

Porque Estudar Ataques?

- Ajudar a identificar vulnerabilidades pra corrigir e estabelecer novas defesas.
- Criar incentivos para todos serem mais cuidadosos no futuro
- Aprender sobre diferentes classes de ameaças
- Nos ajuda a projetar sistemas mais robustos em termos de segurança
- Nos ajuda a avaliar mai precisamente o risco que estamos sujeitos.

Hierarquia de Insegurança



Pensando como um Atacante:

- Procure pelo elo mais fraco
  - Ele é mais fácil de atacar
- Identifique as suposições que o mecanismo de segurança depende
  - Da para tornar essas suposições falsas?
- Pense fora da caixinha:
  - Não se atenha a forma de pensar de quem projetou o sistema.
- Pratique pensar como um atacante:
  - Para cada sistema que você for usar pense o que significa ele ser seguro e como você poderia fazer para ele não ser.

E se eu não pensar como um atacante?

Exercício:

Pensando como um Defensor:

- Politica de Segurança
  - O que estamos protegendo?
  - Que propriedades estamos esperando?
- Modelo de Ameaça
  - Quem são os atacantes?
  - Quais as capacidades deles? Quais a motivações?
  - Que tipos de ataques queremos previnir?
- Gerenciamento de Risco
  - Quais as fraquezas do sistema?
  - Quanto vai custar um ataque pra gente?
  - Qual a probabilidade de um ataque com sucesso?
- Contramedidas
  - Custo x Benefício?
  - Solução técnica x Nâo Técnica?

Politicas de Segurança

- O que estamos tentando defender?
- Quais propriedades nós queremos?
  - Confidencialidade
  - Integridade
  - Temporalidade
  - Disponibilidade
  - Privacidade
  - Autenticidade
  - etc...

Modelos de Ameaça

- Quem são os nossos adversários?
  - Quais seus motivos?
  - Quais suas capacidades?
- Que tipo de ataques nós precisamos previnir?
  - Pense como um atacante!
- Limites das ameaças:
  - Que tipos de ataques podemos ignorar?
  - Isso é importante para manter o custo baixo.

Avaliando o Risco

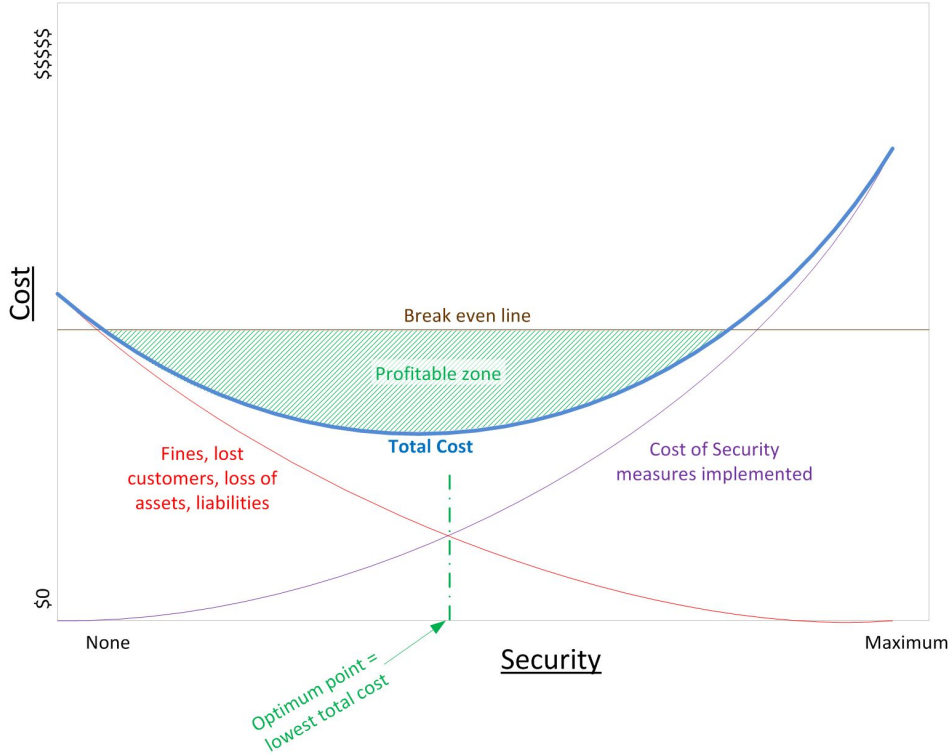
- O que uma invasão vai nos custar?
  - Custo direto:
    - Dinheiro
    - Propriedade
    - Proteção
  - Custo Indireto:
    - Reputação
    - Negócios futuros
    - Bem Estar
- Qual a probabilidade destes custos?
  - Qual a probabilidade de um ataque?
  - Qual a probabilidade de sucesso?

Contramedidas

- Contramedidas tecnicas
  - Software
  - Hardware
- Contramedidas não técnicas
  - Legais
  - Procedimentos
  - Treinamento
  - Auditoria
  - Incentivos

Custo das Medidas de Segurança

- Nada que vai te deixar mais seguro é de graça
  - Custos Diretos:
    - Projeto
    - Implementação
    - Execução
    - Falsos Positivos
  - Custos Indiretos:
    - Perda de produtividade
    - Adição de complexidade
- Um grande desafio é balancear custo versus risco:
  - A NAtureza humana torna dificil avaliar eventos de alto custo e baixa probabilidade.



Exercício:

- Você deve trancar a porta ao sair de casa?
- É seguro passar o seu cartão de cŕedito em qualquer lugar?
- Você andaria num carro autônomo?

- Ativos?
- Adversários?
- Gerenciamento de Risco?
- Contramedidas?
- Custo/Beneficio?

Projeto de Sistemas Seguros

- Erro principal:
  - Tentar se convencer que o sistema que voce está projetando é seguro
- Melhor abordagem:
  - Sempre identificar as fraquezas do seu design e se focar em corrigi-las.
- Projeto de sistemas seguros é um processo e não um produto
- Tem que ser constante durante todo ciclo de vida.
- Não dá pra pegar algo pronto e transformar em algo seguro.
- Uma boa estratégia é trabalhar com segurança em profundidade.

Onde focar as nossas defesas?

- Componentes seguros
  - Partes do sistema que tem que funcionar corretamente para que o sistema seja seguro
  - Ex.: Hardware de proteção de chaves, TPM, etc
- Superficie de ataque
  - Que partes do sistema ficam expostos ao atacante?
  - Ele consegue acesso direto a componente seguros?
- Complexidade versus Segurança
  - Ser seguro normalmente é sinônimo de ser simples.
  - Muitas camadas abrem espaço para erros conceituais.

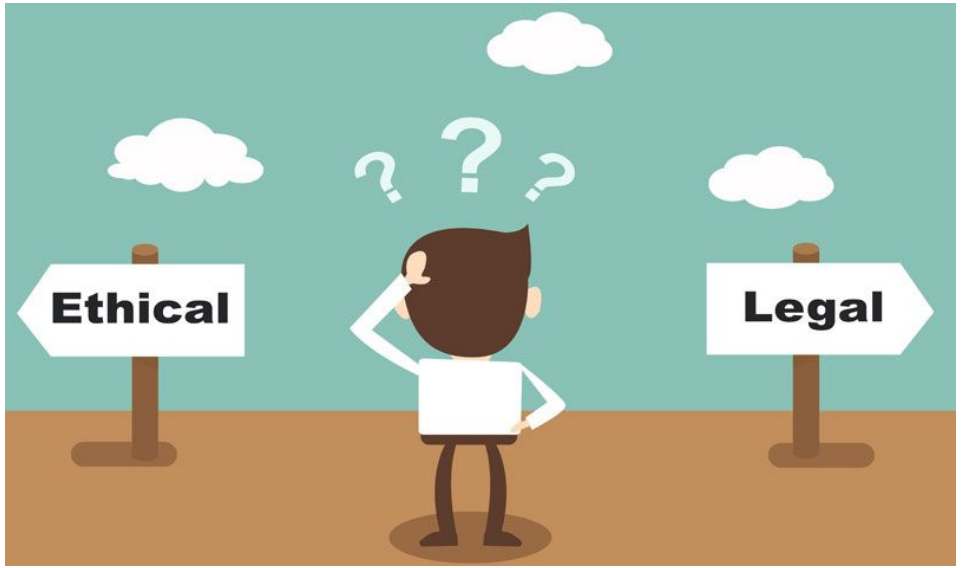
Testes de Segurança

- Especifique requisitos para que voce possa testar contra eles.
  - Quais são os requisitos corretos?
- Apliques testes como se fosse um atacante
  - Black box testing
  - Gray box testing
  - White box testing

Como se tornar um 1337 hax0r

- Pensamento Crítico
  - Como pensar como um atacante
  - Como raciocinar sobre ameaça e risco
  - Como balancear custo e benefício
- Capacidade Técnica
  - Como se proteger
  - Como gerenciar e defender sistemas
  - Como projetar e programar sistemas seguros
- Aprenda a ser consciente da sua segurança sempre
- Seja ético!

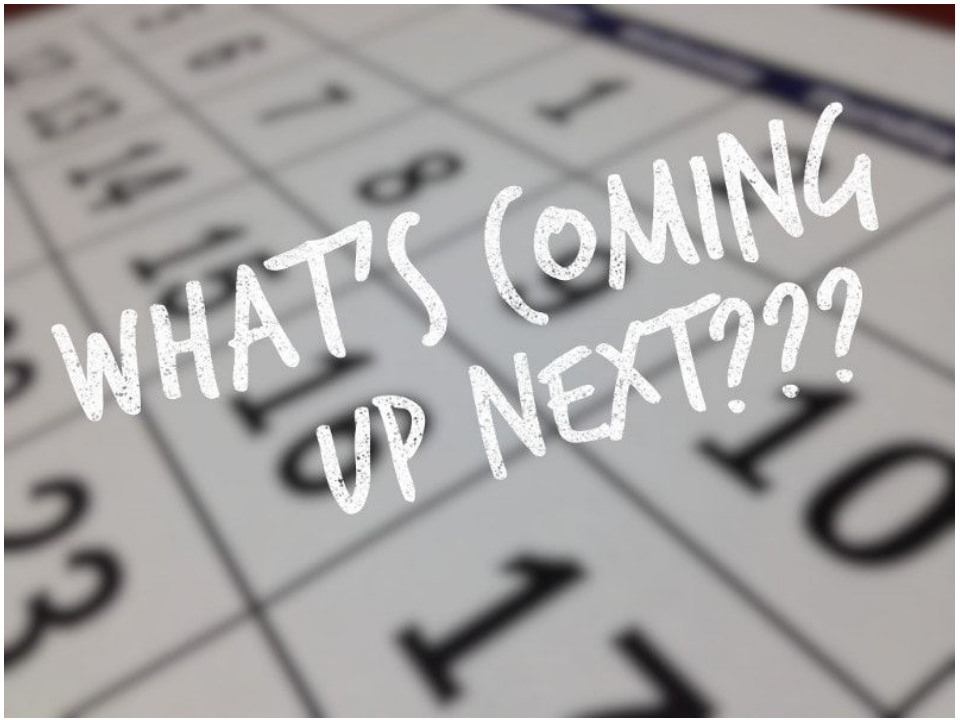
Preceitos Éticos da Disciplina



- Don't be EVIL
  - Preceitos éticos requerem que menos sabendo como você de abstenha de praticar o mal
  - Sempre respeite a privacidade e a propriedade alheia
  - Uma falta ética é motivo de reprovação sumária nesta disciplina.,
- Existem leis federais e estaduais sobre crimes cibernéticos
  - Se você fizer algo de errado o professor vai te denunciar
- Regras da UFSC proíbem você de atacar quaisquer sistemas no CAMPUS
  - As penas iniciam em suspensão e vão até a expulsão da Universidade.

Próximas Aulas

- Prática:
  - Trabalho Individual I
    - Envolve todo este conteúdo que vimos na aula de hoje
- Teórica:
  - Introdução a criptografia e criptosistemas classicos
    - Parte mais difícil da disciplina



Perguntas?

jean.martina@ufsc.br