Riscos Associados a Vulnerabilidades de Softwares

MODELAGEM E PREVISÃO

Matheus Martins, Miguel Bicudo, Daniel Menasché (UFRJ)
Leandro P. Aguiar (SIEMENS)

Sumário

- Introdução
- Conceitos
- Dados
- Análises
- Modelos de Risco
- Conclusão
- Agradecimentos

Introdução

Introdução

Objetivo:

- Quando aplicar correções (patches) em sistemas críticos?

Por quê?

- Em sistemas críticos a ***aplicação de correções é complicada***;

Nossa proposta:

- Prever risco associado a vulnerabilidade -- ***ciclo de vida***;
- Criar e validar ***modelos*** para ***previsão***.

Introdução
Considerações na aplicação de correções

Aplicar correções pode representar problemas:

- O sistema terá de ser interrompido para aplicar a correção;
- Duração da interrupção pode ser um momento crítico;
- Como coordenar a aplicação de correções quando há sistemas interdependentes?
- A conformidade de se ter sistemas funcionais vulneráveis e um fato grave.

Não aplicar correções de vulnerabilidades trará problemas:

- O sistema ficará exposto a um ataque;
- Hackers podem ter acesso a dados sensíveis;
- Injeção de informações falsas no sistema; (DNS Poisoning)
- Podem capturar o sistema para atividades maliciosas; (DDoS)

Introdução
Crescimento do número de vulnerabilidades

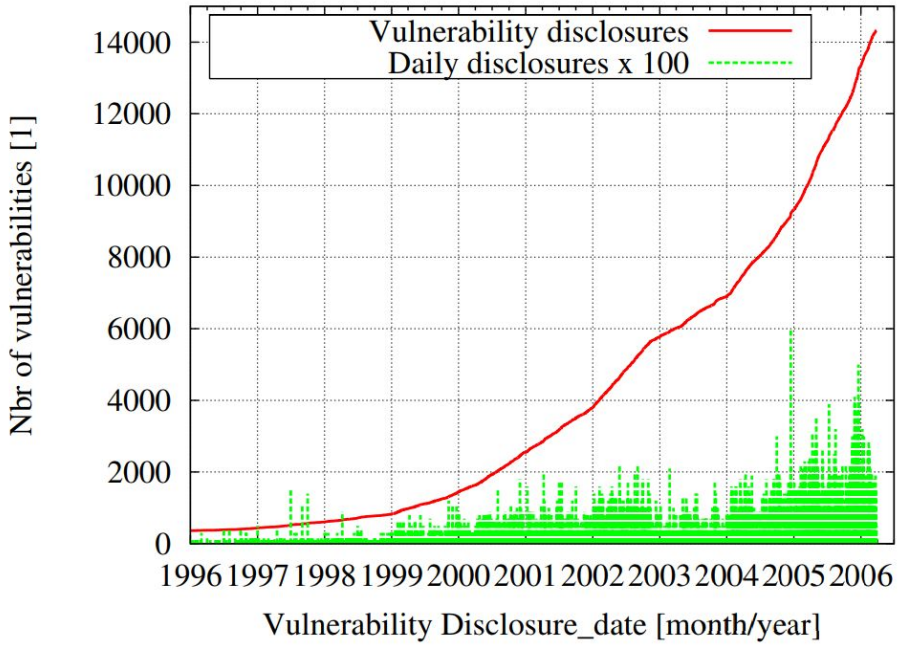


Gráfico do número de vulnerabilidades segundo o Frei

- 1996 até 2006

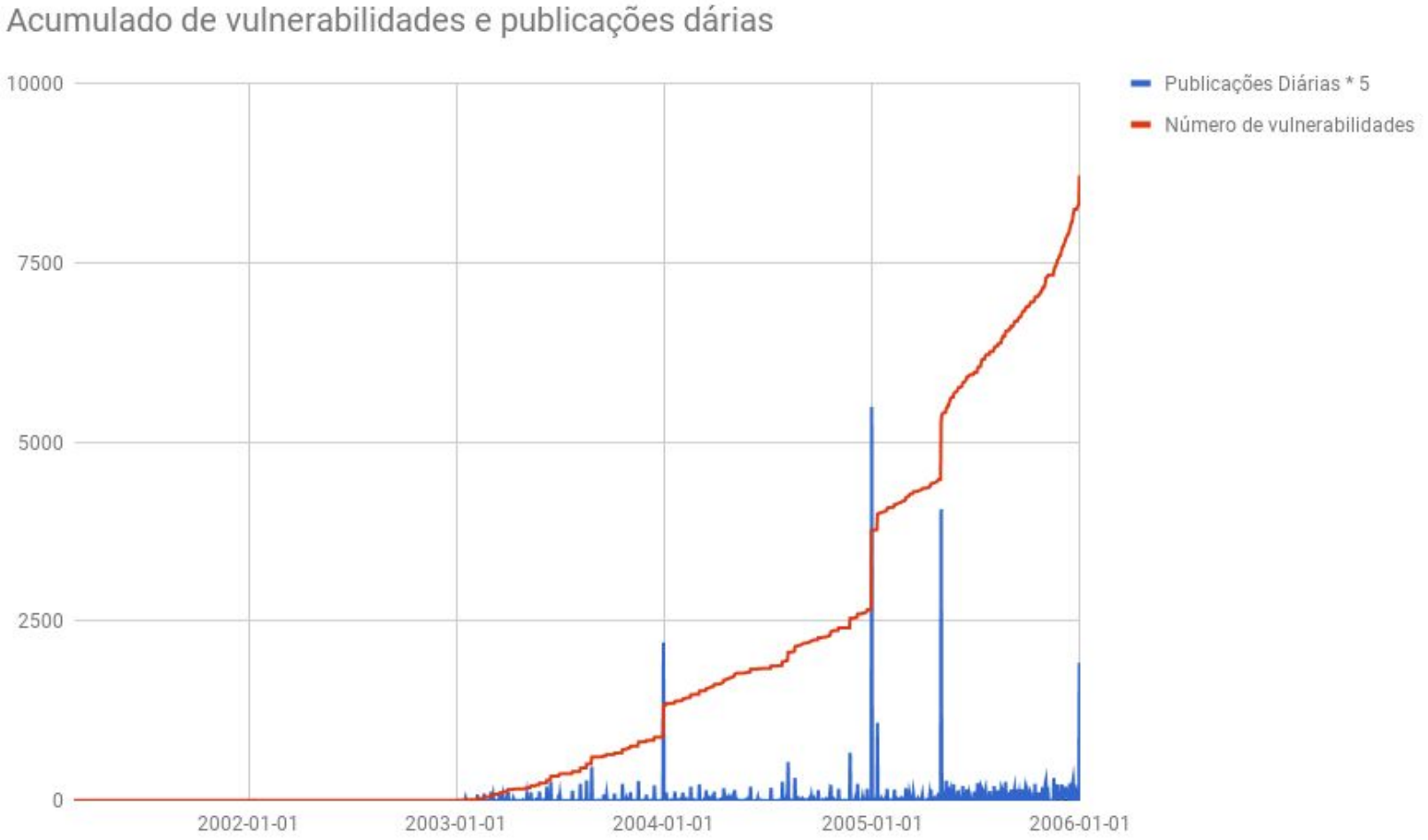


Gráfico do número de vulnerabilidades segundo nossos dados

- 2003 até 2006

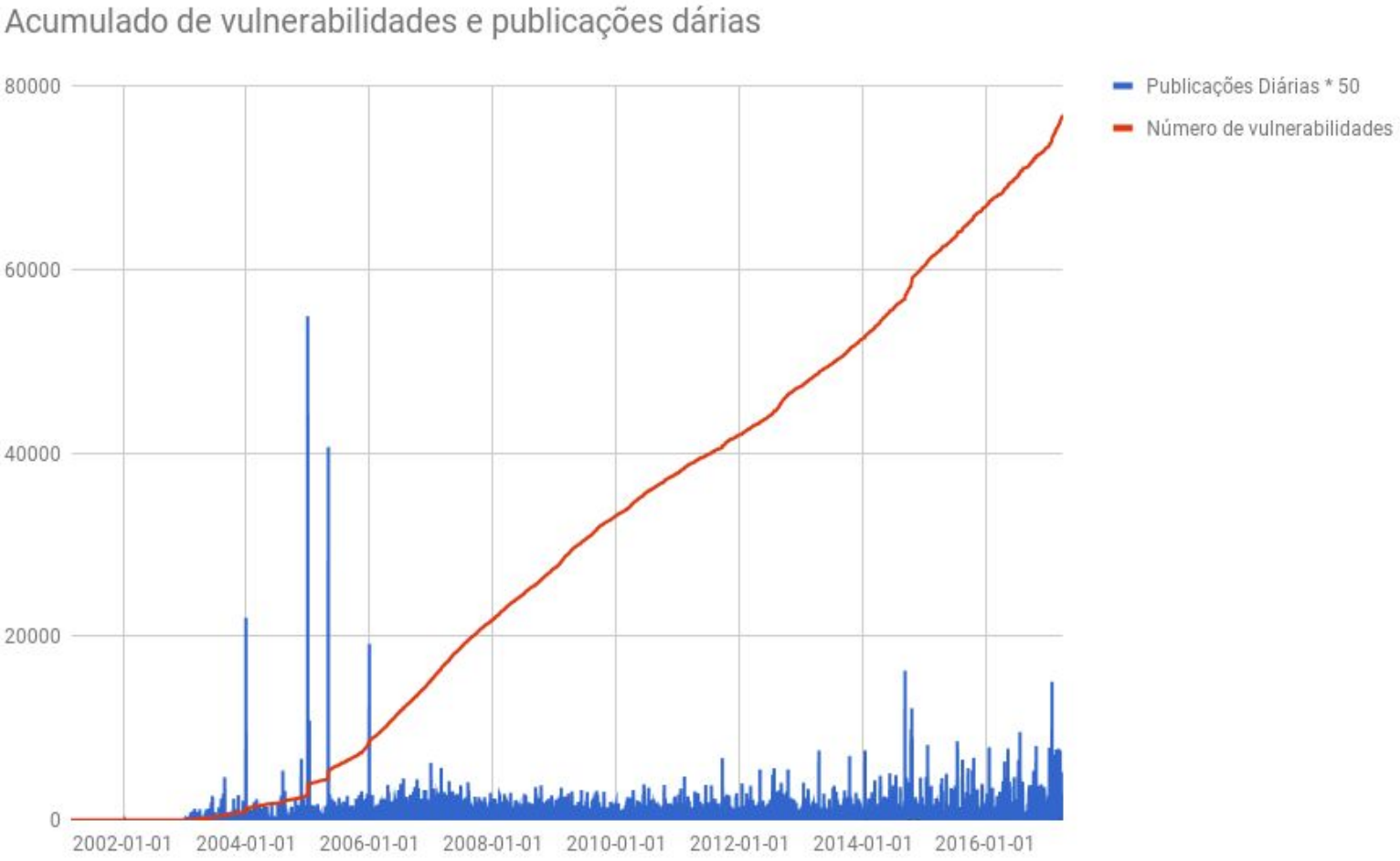


Gráfico de número de vulnerabilidades contadas no NVD

- 2003 até 2016

Conceitos

EM SEGURANÇA DA INFORMAÇÃO

Conceitos
em Segurança da Informação

Integridade

- Garantir que os dados manipulados, seja por consultas ou armazenamento, mantenham suas características originais.

Confidencialidade

- Visa garantir que não haja nenhum tipo de acesso não autorizado aos dados por terceiros.

Disponibilidade

- É o conceito que permite que os dados possam ser obtidos e utilizados sempre que necessários.

Conceitos
em Segurança da Informação

Vulnerabilidade

- Erro de implementação no sistema que pode ser usado para realização de um ataque;
- Está associado a um ou mais produtos e versões específicas.

Exploit

- Qualquer conceito, código ou método capaz de explorar uma vulnerabilidade afim de atingir objetivos nunca antes esperados pelos desenvolvedores.

Patch

- Rotina de correção de uma vulnerabilidade;

Conceitos
em Segurança da Informação

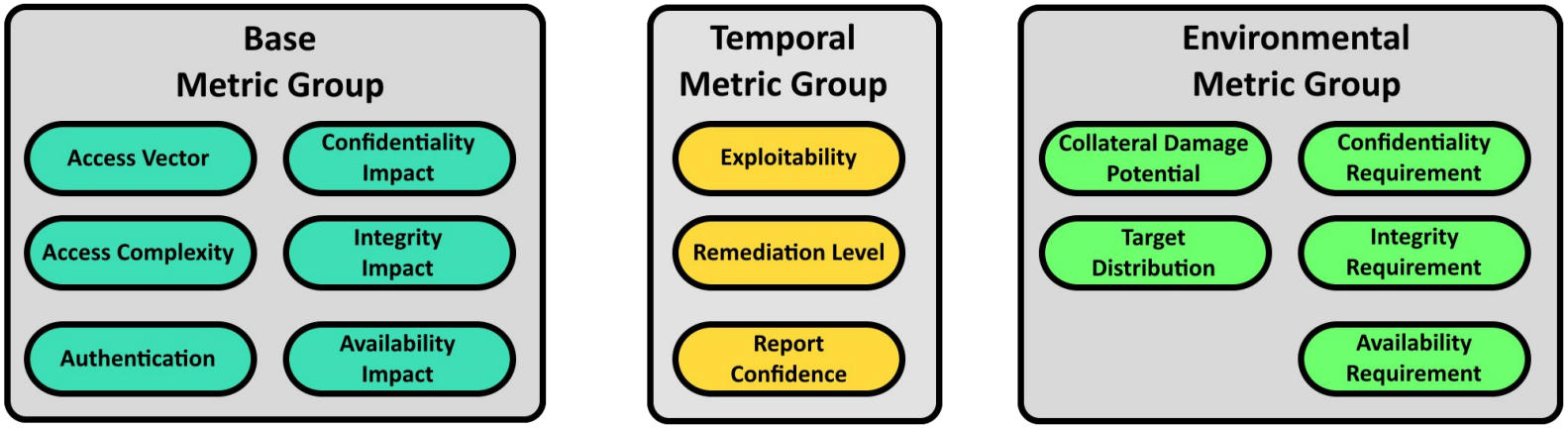
CVE

- Associa uma vulnerabilidade com um identificador único;
- Por exemplo: CVE-2015-0001 é o ID da primeira vulnerabilidade publicada em 2015;
- Atribui características fundamentais à vulnerabilidade, como o CVSS;

CVSS

- Métrica de severidade de uma vulnerabilidade;
- Trata-se de um valor entre 0 e 10 onde 10 é o valor máximo de severidade.

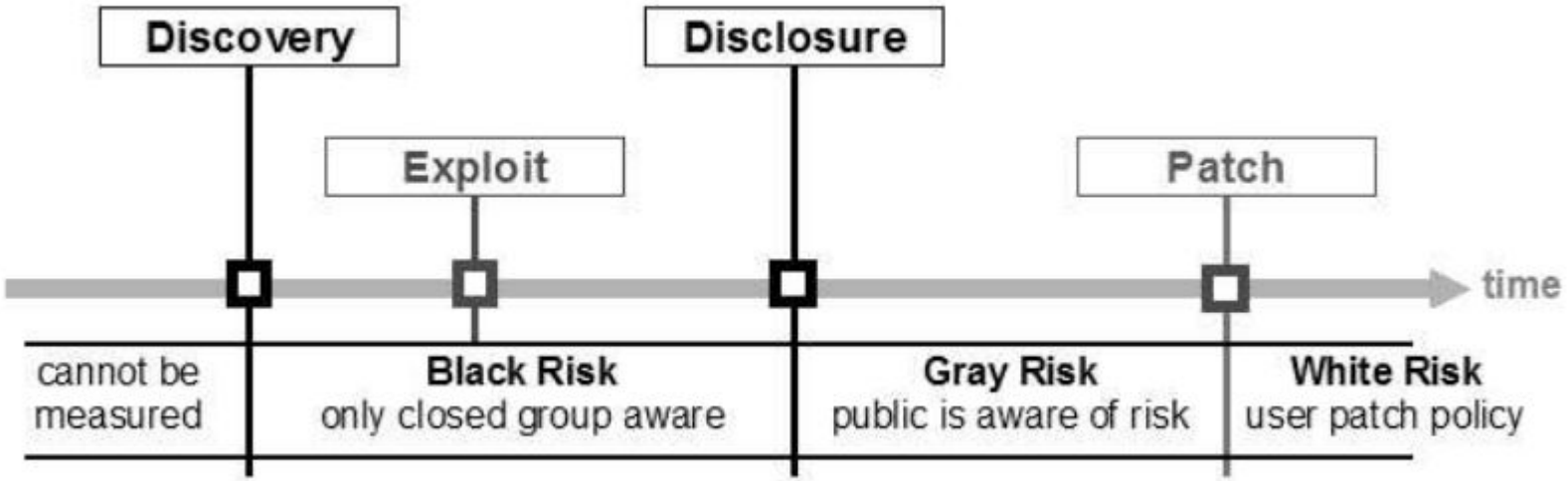
Conceitos
CVSS



Foco nas métricas temporais

- Permitem variar entre 66% e 100% do escore de base
- Para servir como métrica de risco, vamos:
  - Ignorar microparâmetros, variando continuamente na faixa de 66% até 100%
  - Extrapolar domínio do CVSS, que só existe a partir da publicação da CVE

Conceitos
Ciclo de vida de uma vulnerabilidade



Conceitos
Ciclo de vida de uma vulnerabilidade

Descoberta

- Em muitos casos a data é desconhecida;
- ***Black-risk:*** apenas um grupo pequeno sabe sobre a vulnerabilidade.

Divulgação

- Data divulgada pelo NVD;
- ***Gray-risk:*** público ciente da vulnerabilidade mas ainda sem correção.

Exploração

- Quando um *exploit* malicioso é lançado em determinada data.

Correção

- Quando um *patch* é lançado;
- ***White-risk:*** público ciente e já existe uma correção.

Desafios

Escassez de dados

- Dados sobre *exploits* são difíceis de se obter;
  - Normalmente esses dados estão em formato de texto;
  - Muitas vezes ficam ocultos na *deep-web.*
- Pouquíssimos dados sobre ataques bem sucedidos;
  - São informações sensíveis e pouco divulgadas.

Ausência de dados históricos sobre riscos

- CVSS só existe a partir da divulgação da CVE;
- Ausência de dados no grupo temporal.

Validação

- Não há um *ground-truth* sobre evolução temporal de riscos;
- O melhor que se pode fazer é ater-se a existência de *exploits* conhecidos.

Dados

FONTES E FLUXOS

Dados
Fontes

NVD

- Banco de vulnerabilidades operada pelo NIST;
- CVE – dados sobre vulnerabilidades;
- CPE – dados sobre produtos;
- Dados no site são mais amplos que no banco para download.

Exploit DB

- Banco de *exploits* operado pela *Offensive Security;*
- Dados muitas vezes não normalizados e códigos em forma de texto livre
  - Ligação com CVE e CPE se torna complicada por causa disso.
- Dados no site são mais amplas que no banco para download

Dados
Match entre as fontes

Ligação entre *exploit* e CVE

- *Ground-truth Exploit-CVE matches*
- Registro do *exploit* faz referência a uma CVE

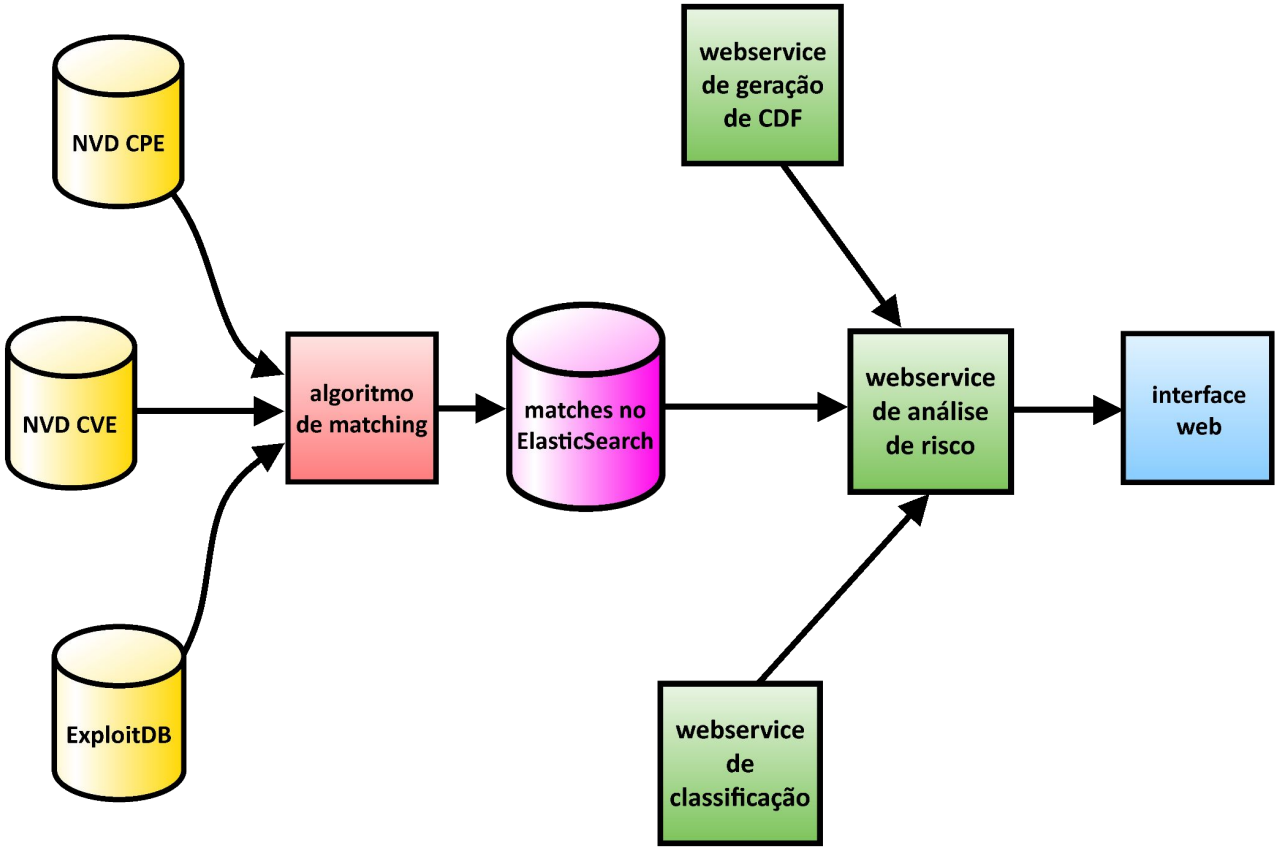
Ligação entre exploit e CPE

- *Ground-truth Exploit-CPE matches*
- Registro do *exploit* indica uma CPE diretamente
- Transitivo a partir da referência a uma CVE, que possui uma lista de CPE

Dados
Estrutura de tabelas

cve	cpe	exploit
cve_id	cpe_id	exploit_id
publish_datetime	deprecation_date	file
last_modified_datetime	title	date
cvss_access_vector	lang	author
cvss_access_complexity	vendor	platform
cvss_authentication	id	type
cvss_confidentiality_impact	is_deprecated	port
cvss_integrity_impact	product	id
cvss_availability_impact	version	
cvss_source		
cvss_generated_on_datetime		
cvss_score		

Dados
Fluxo


NVD CPE
NVD CVE
ExploitDB
algoritmo de matching
matches no ElasticSearch
webservice de geração de CDF
webservice de análise de risco
webservice de classificação
interface web

Análises

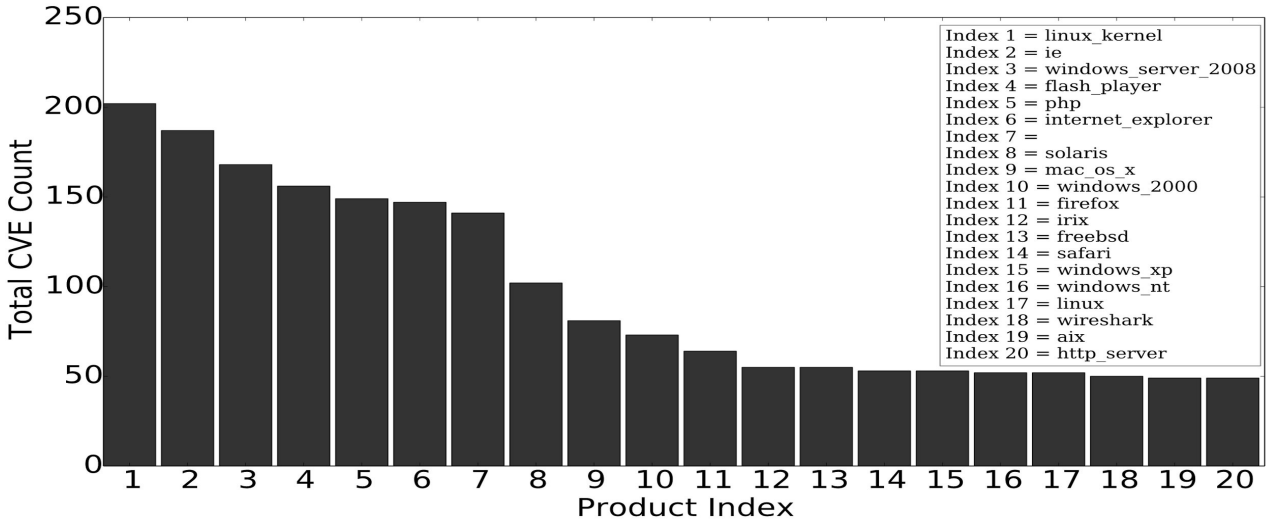
MATCHES CVE-EXPLOIT E CPE-EXPLOIT

Análises
Propósito

Vamos apresentar a partir deste ponto

- Questões sobre o que é esperado das visualizações de nossas análises;
- Construir visualizações gráficas que podem ou não ser condizentes com a realidade;
- Justificativas sobre as visualizações.

Análise
CVEs por Produto



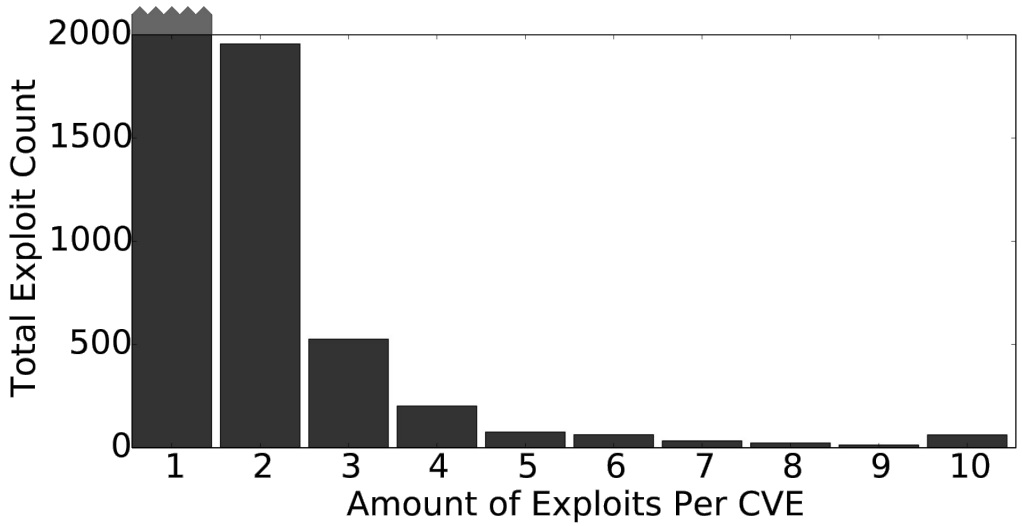
O *kernel* do Linux possui o maior número de vulnerabilidades totalizando 200 CVEs;

O Internet Explorer aparece nas colunas 2 e 6: ie e internet_explorer; com 330 CVEs;

O Windows aparece nas colunas 3, 10, 15 e 16, totalizando 350 CVEs;

O produto de índice 7 representa produtos não identificados.

Análise
Exploits por CVE



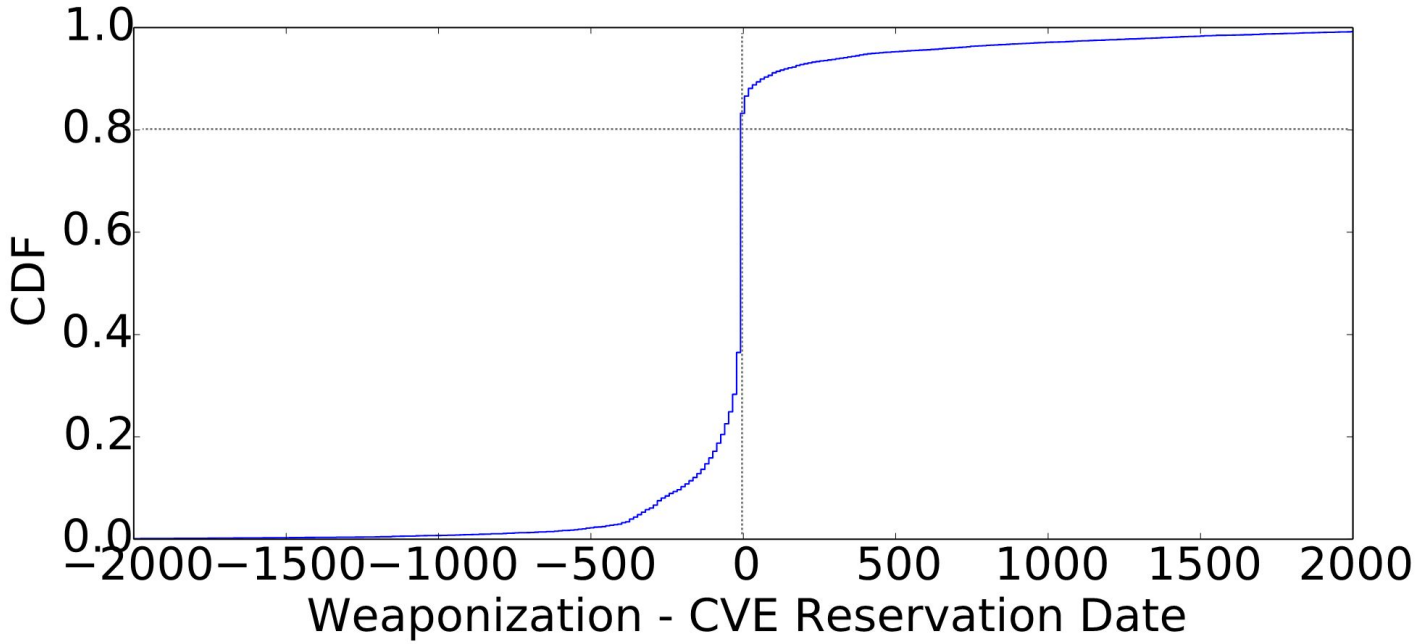
O gráfico está cortado na linha de 2.000 *exploits* para visualização;

Na primeira coluna, aproximadamente 18.000 CVEs possuem apenas 1 *exploit;*

Quase 2.000 CVEs possuem 2 *exploits*

A razão máxima é de 10 *exploits* explorando uma única CVE;

Análise
Impacto Geral



Aproximadamente 80% dos *exploits* são *zero-day*

- Ou seja, no dia de divulgação da CVE já existe um ou mais *exploits;*
- Estudos do Frei mostraram quem em 2006 70% das vulnerabilidades eram z*ero-day*.

Análise
Impacto da Criticidade (escore CVSS)

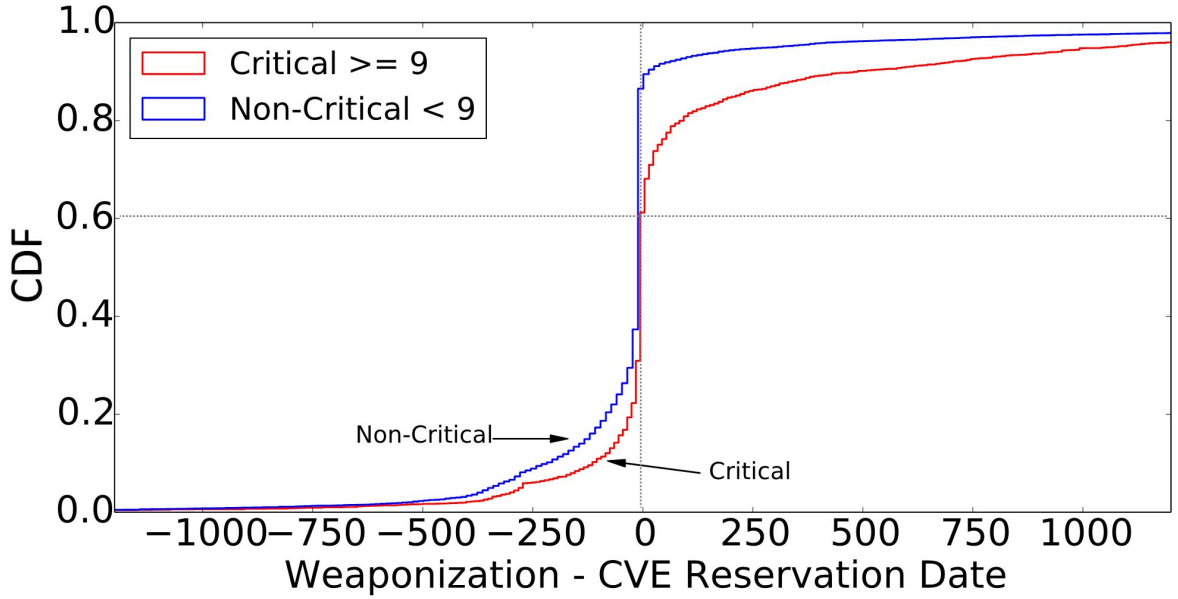
Dividimos todos as vulnerabilidades em duas faixas de acordo com o escore CVSS final.

- ≥ 9 são vulnerabilidades críticas
- < 9 são vulnerabilidades que não são críticas

Mostramos a CDF da data de lançamentos de *exploits* menos a data de reserva da CVEs.

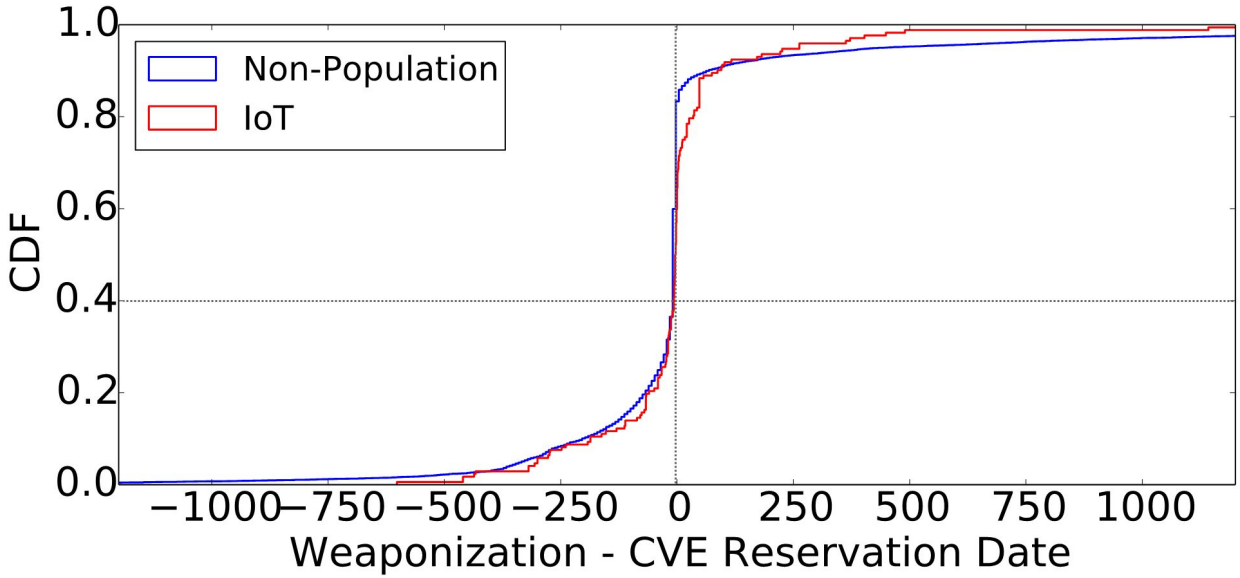
Esperamos que para os casos críticos os fabricantes tenham uma reação mais rápida olhando para das datas.

Análise
Impacto da Criticidade (escore CVSS)



- Fabricantes reagem mais rapidamente após aparecimento de *exploits* críticos
- 40% dos *exploits* críticos aparecem depois da CVE
- Esse fatos talvez tenham relação com o valor dos exploits no mercado negro (estudos futuros)

Análise
Impacto sobre Produtos IoT



- Fabricantes de produtos IoT respondem mais rapidamente a *exploits*
- Criação de *exploits* é mais rápida após divulgação da CVE
- Aproximadamente 40% dos *exploits* são *zero-day* para produtos IoT

Análise
Impacto sobre Produtos IoT

O que sabemos sobre os produtos IoT?

- A maioria destas CPEs estão associadas a CVEs mais críticas do que a população em geral
- Isso justifica de certa forma os 40% de *zero-day*

Análise
Impactos segregados por microparâmetros

Há três microparâmetros do grupo de base que são interessantes aqui:

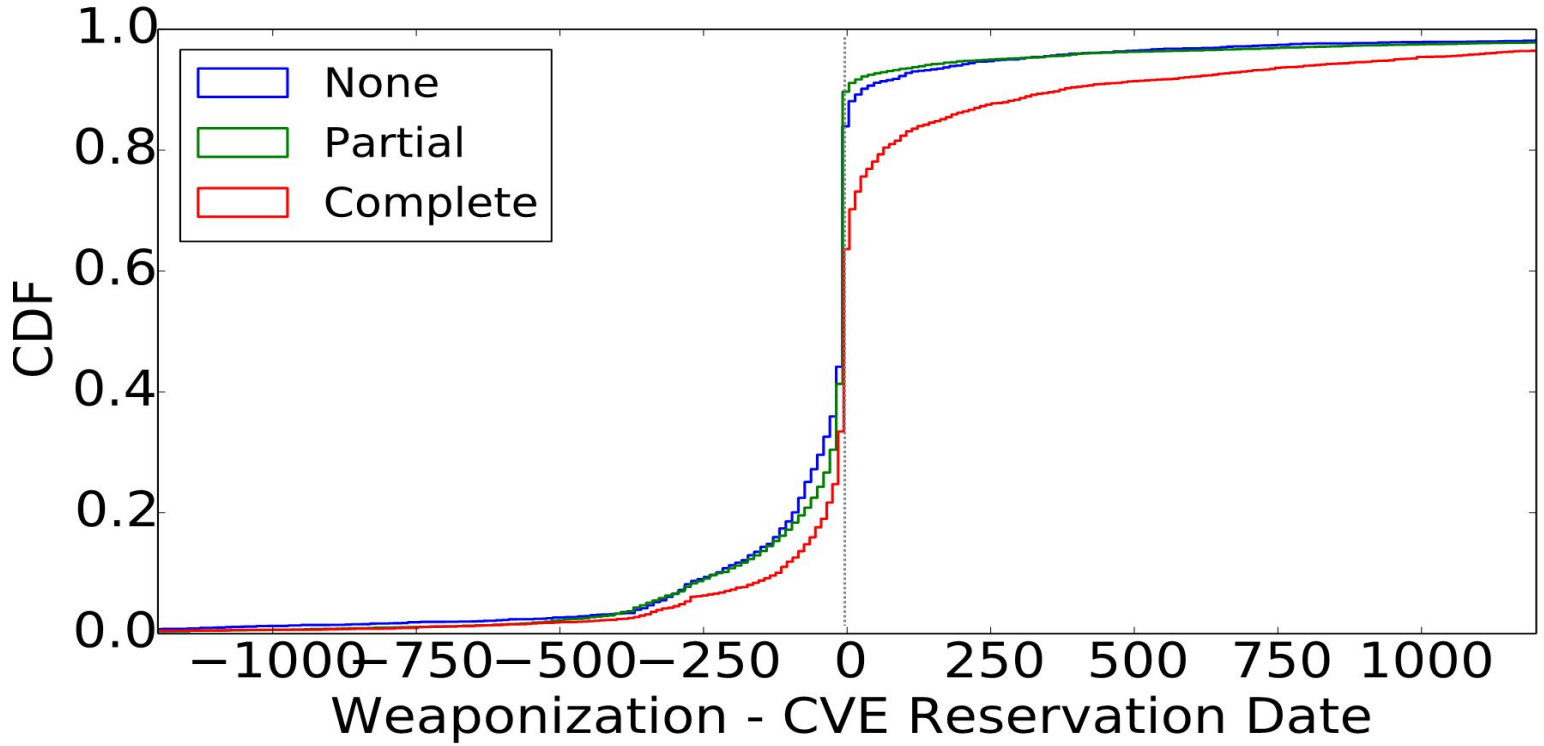
- Integrity – impacto sobre a integridade do sistema.
- Confidentiality – impacto sobre a confidencialidade do sistema.
- Availability – impacto sobre a disponibilidade do sistema

Cada um dos parâmetros pode assumir 3 valores:

- None – não há risco no quesito
- Partial – pode haver risco no quesito
- Complete – o quesito está com certeza em risco

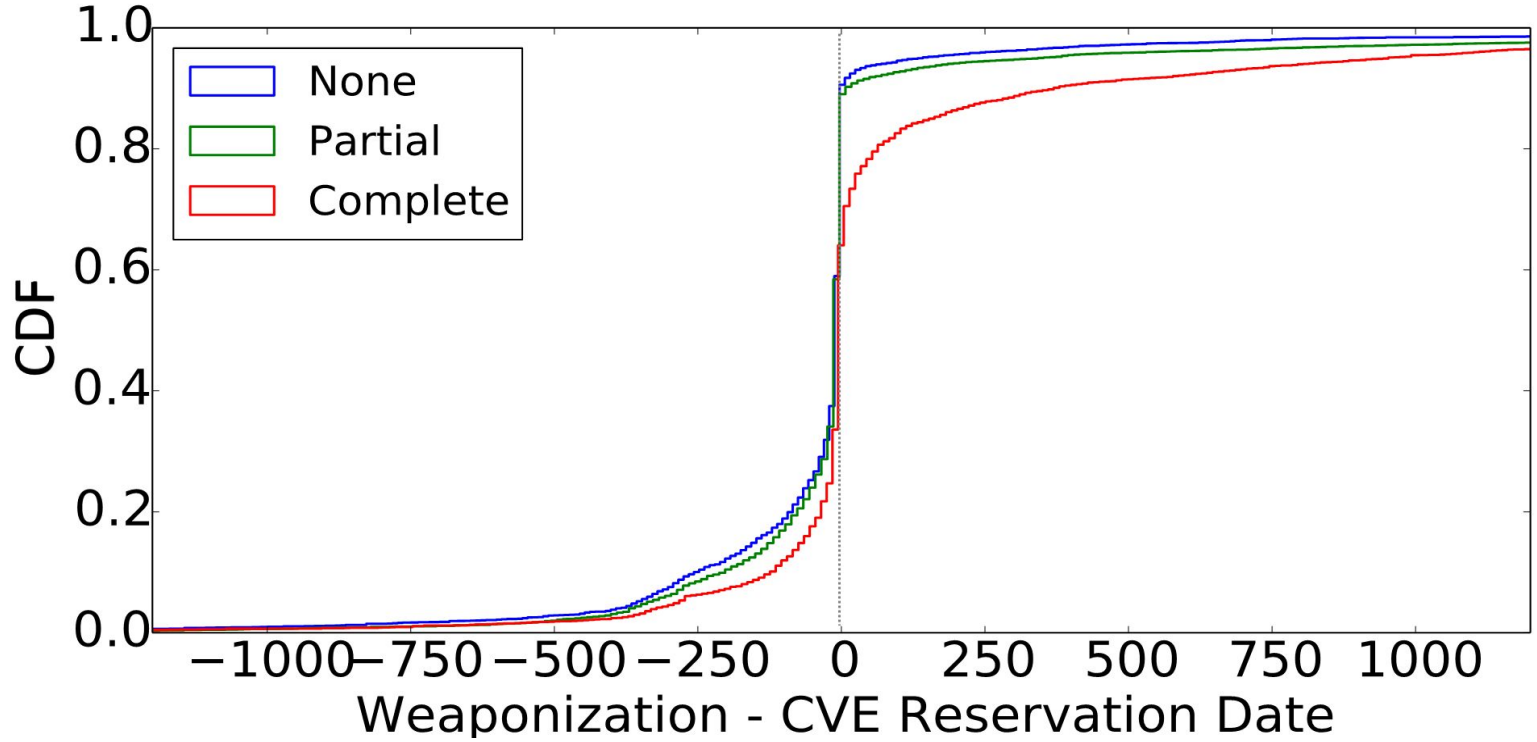
Esperamos que a relação entre o menor risco e o maior risco seja parecido com o gráfico de criticidade apresentado anteriormente

Análise
Impacto quanto à Integridade



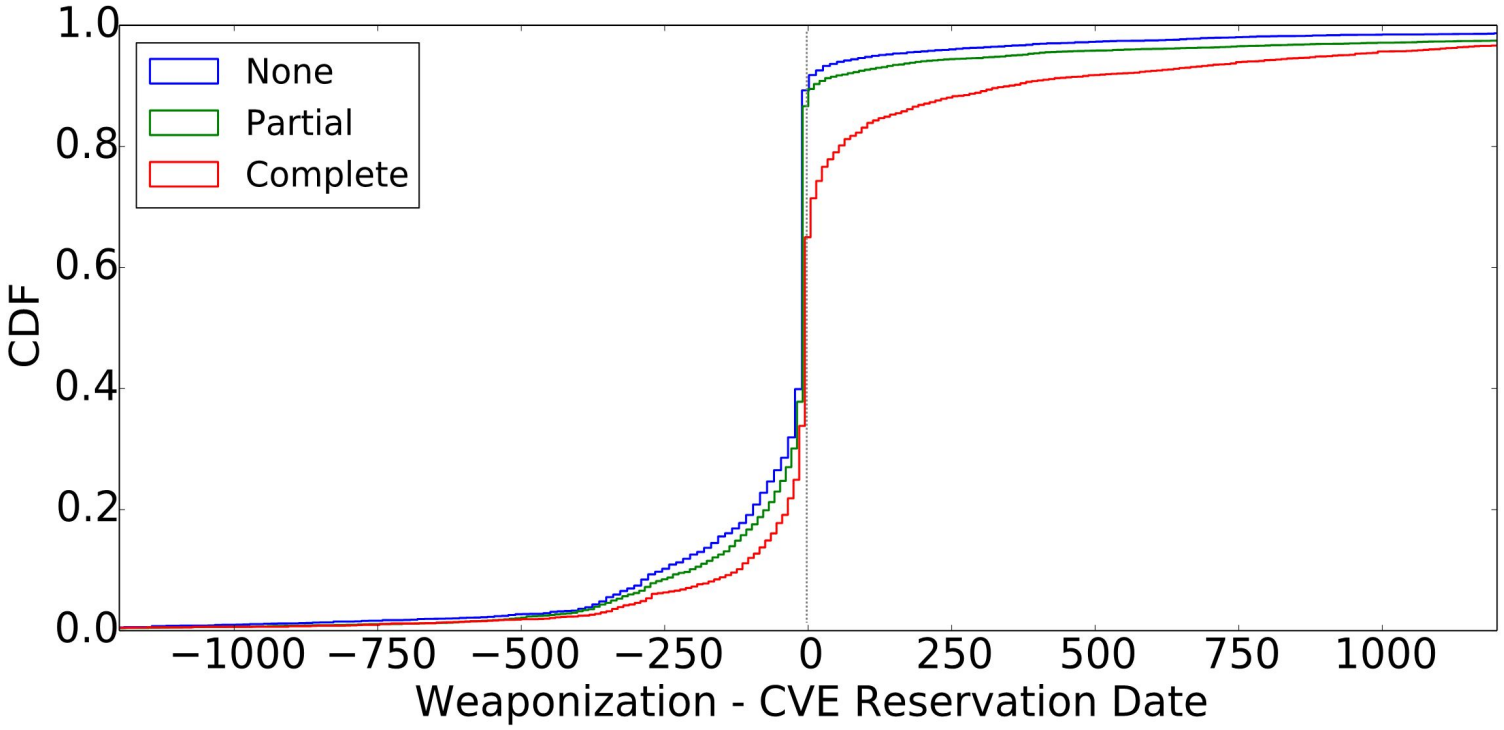
CDFs condicionadas ao microparâmetro *Integrity* do CVSS

Análise
Impacto quanto à Confidencialidade



CDFs condicionadas ao microparâmetro *Confidentiality* do CVSS

Análise
Impacto quanto à Disponibilidade



CDFs condicionadas ao microparâmetro *Availability* do CVSS

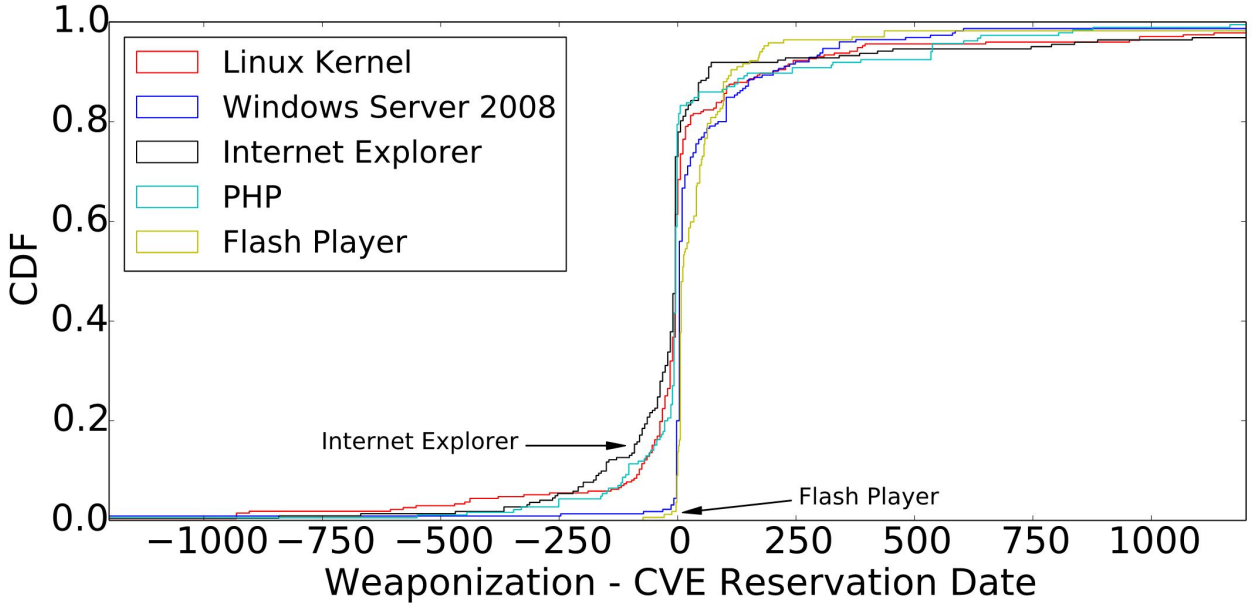
Análise
Impacto nos 5 Produtos principais

Já vimos anteriormente quais são os produtos mais afetados

- Windows Server 2008;
- Internet Explorer;
- Linux Kernel;
- Flah Player;
- PHP.

O que esperar?

Análise
Impacto nos 5 Produtos principais



Impacto nos produtos mais afetados por *exploits*

- Internet Explorer é o mais lento em reagir à *exploits*
- Windows Server 2008 e o Flash Player são os mais rápidos na reação

Análise
Impacto nos 5 Produtos principais

Windows Server 2008
- Produto voltado para empresas e negócios
- Faz sentido a reação rápida?

Internet Explorer
- Produto voltado para o consumidor final
- Faz sentido a reação lenta?

Flash Player
- Produto voltado para o consumidor final?
- Talvez não... YouTube já foi totalmente baseado no Flash Player

Análise
Impacto nos 5 Produtos principais

PHP
- Desenvolvido abertamente

Linux Kernel
- Desenvolvido abertamente
- Talvez seja mais complicado alocar recursos para reagir mais rapidamente quando o código é aberto? Aplicações open source não costumam ser centralizadas.

Análise
Impacto nos 5 Fabricantes principais

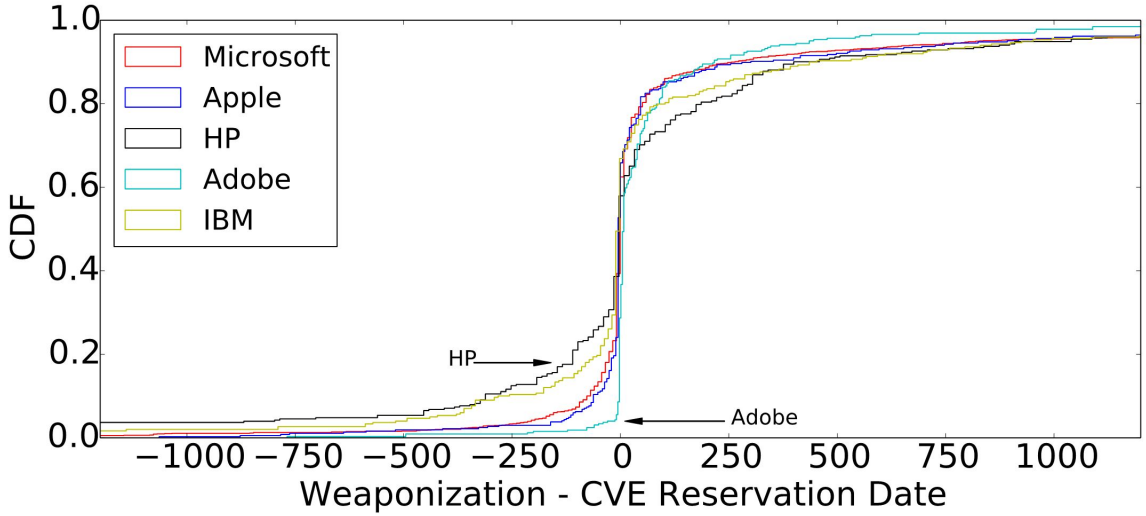
A ligação entre CVE/CPE é dada, não é necessário criar expectativas (as maiores empresas do mundo devem estar na lista)

- Microsoft
- Apple
- HP
- Adobe
- IBM

O que esperar?

- Já temos dados sobre os produtos de maior peso da Adobe e Microsoft
  - Expectativas internas, pois esses dados também vieram das visualizações

Análise
Impacto nos 5 Fabricantes principais



Impacto nos fabricantes com maior número de CVEs

- Adobe reage rapidamente a *exploits;*
- HP possui capacidade baixa de reação;
- Adobe possui menos exploits surgindo após divulgação da CVE;
- HP possui mais exploits após o CVE, talvez valham mais no mercado negro

Modelos de Risco

MODELOS PARA ANÁLISE E PREVISÃO DE RISCOS

Modelos de Risco
Aprendizado por Máquina

Pensado como problema de classificação

Tempo de lançamento do primeiro *exploit* menos divulgação da CVE dividido em 4 classes

- Mais ou menos o mesmo número de CVEs em cada classe
- São elas:
  - *Exploit* lançado anteriormente a 2 meses antes da divulgação da CVE
  - *Exploit* lançado nos 2 meses anteriores à divulgação da CVE
  - *Exploit* lançado no dia ou até 2 meses após divulgação da CVE
  - *Exploit* lançado após 2 meses depois da divulgação da CVE

Features: 18.776

- Dados da CVE
- Dados de CPE: fabricantes e produtos impactados
- Valores do escore e subescores do CVSS
- Binárias de todas as palavras achadas nas descrições e títulos

Modelos de Risco
Aprendizado por Máquina

Vários classificadores foram testados

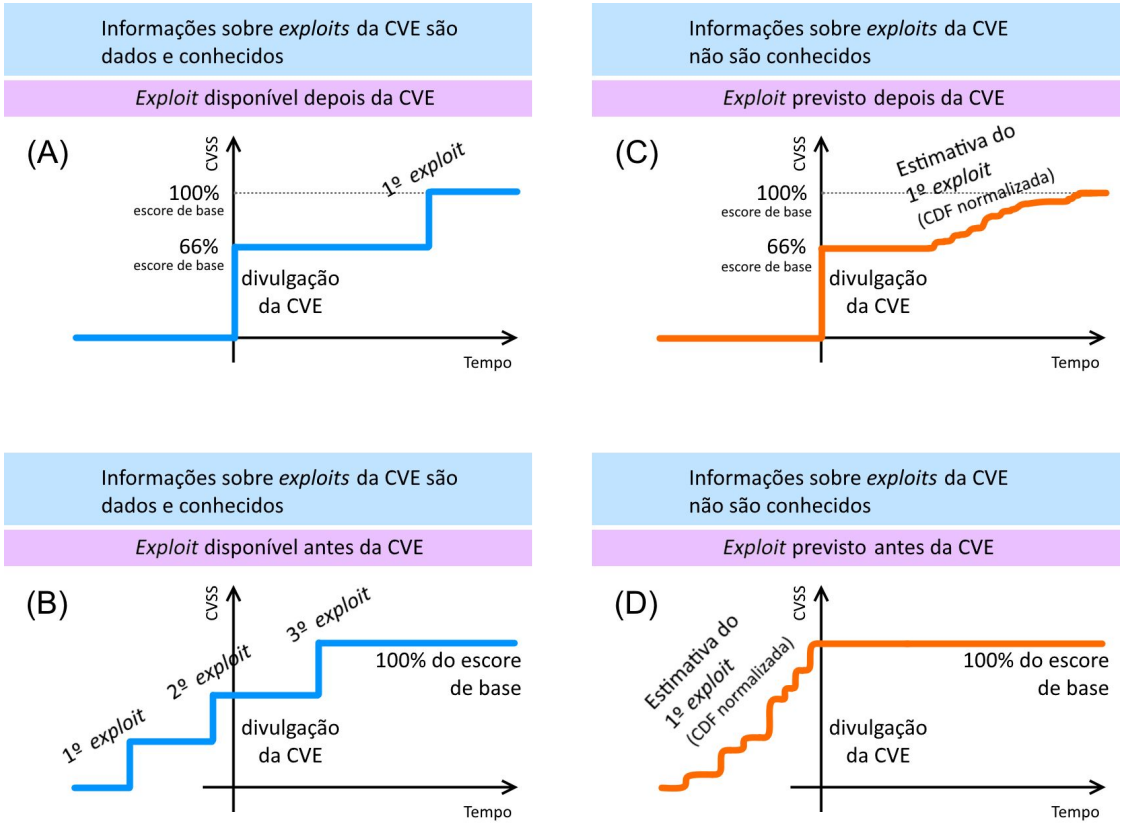
- A rede neural obteve os melhores resultados

Classificador	Acurácia	Desvio padrão
Naive Bayes	24%	1%
SVM linear	56%	2%
SVM com núcleo RBF	57%	1%
Gradient Boosting Tree	62%	13%
Rede Neural	67%	3%

Modelos de Risco
Aprendizado por Máquina

Dados	Fração	Utilidade
Treinamento	60%	Dados que alimentam o algoritmo de aprendizado
Validação	20%	Dados que servem para validar os hiperparâmetros
Teste	20%	Dados que testam como o algoritmo com os hiperparâmetros se comporta frente a dados novos

Modelos de Risco
Normalização de CDFs na escala do CVSS



Modelos de Risco
CDF baseada em fabricantes

Usado em conjunto com o modelo preditivo
- Útil quando o modelo preditivo apresenta erro

CDF de *exploits* do produto principal da CVE

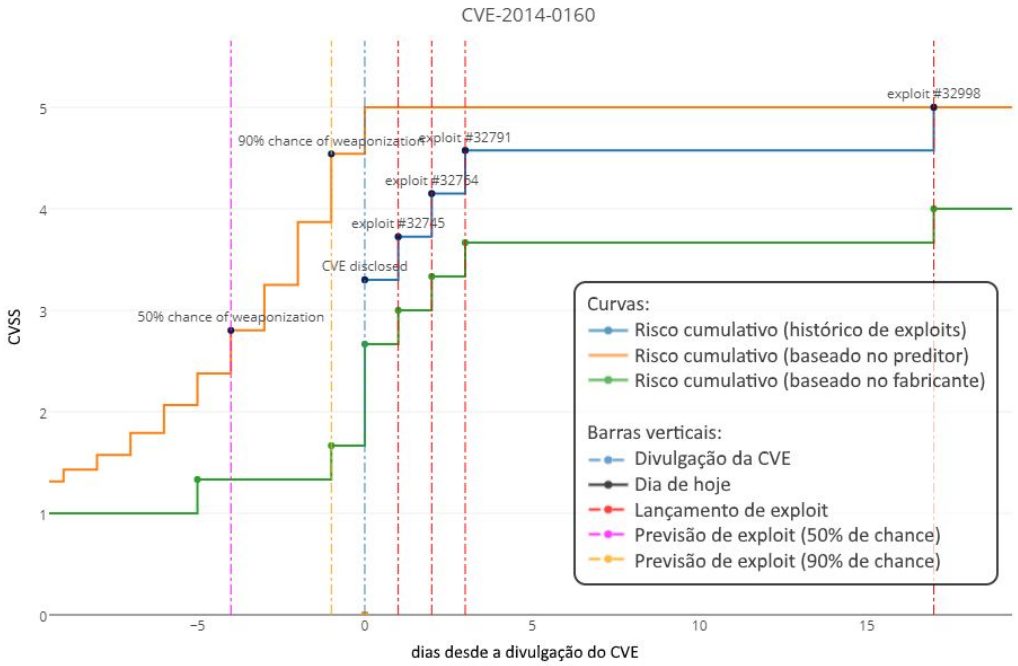
Modelos de Risco
Casos

Curva azul
- Lançamentos de *exploits*

Curva laranja
- CDF normalizada do modelo preditivo

Curva verde
- CDF normalizada do modelo por fabricante

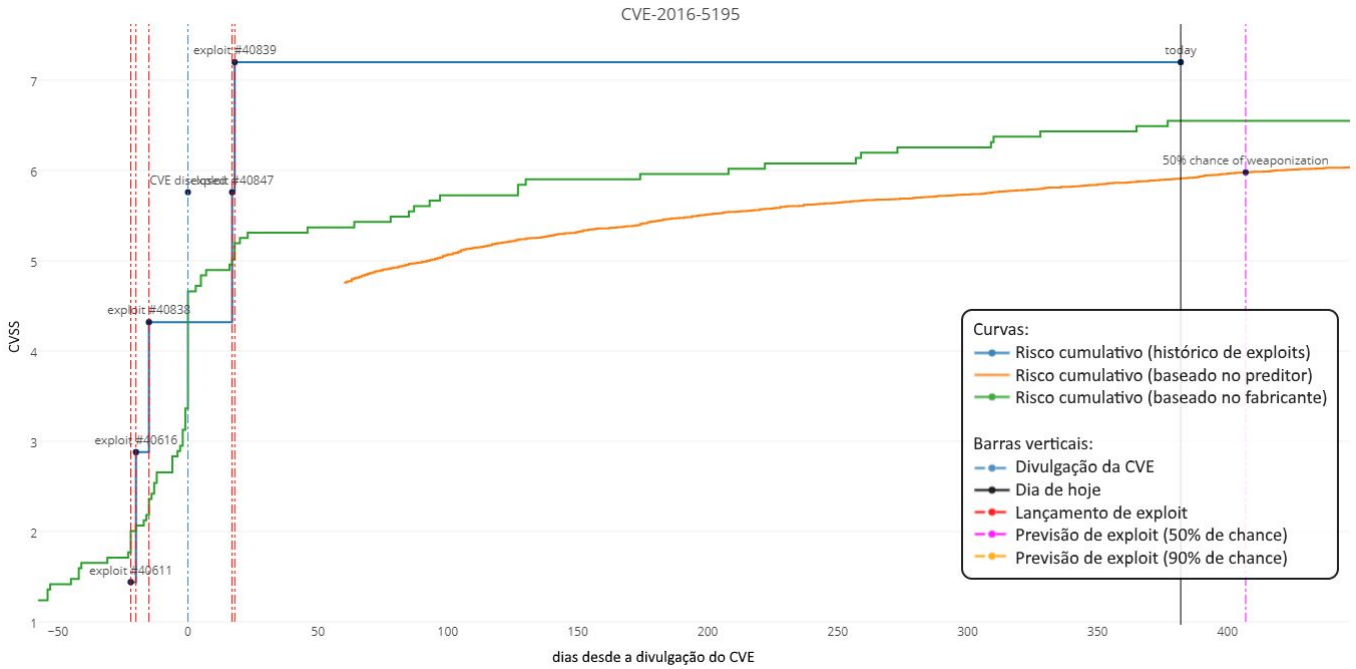
Modelos de Risco
Casos



CVE-2014-0160 – Heartbleed – Openssl

- Classificador foi conservador, curva do fabricante ficou atrasada

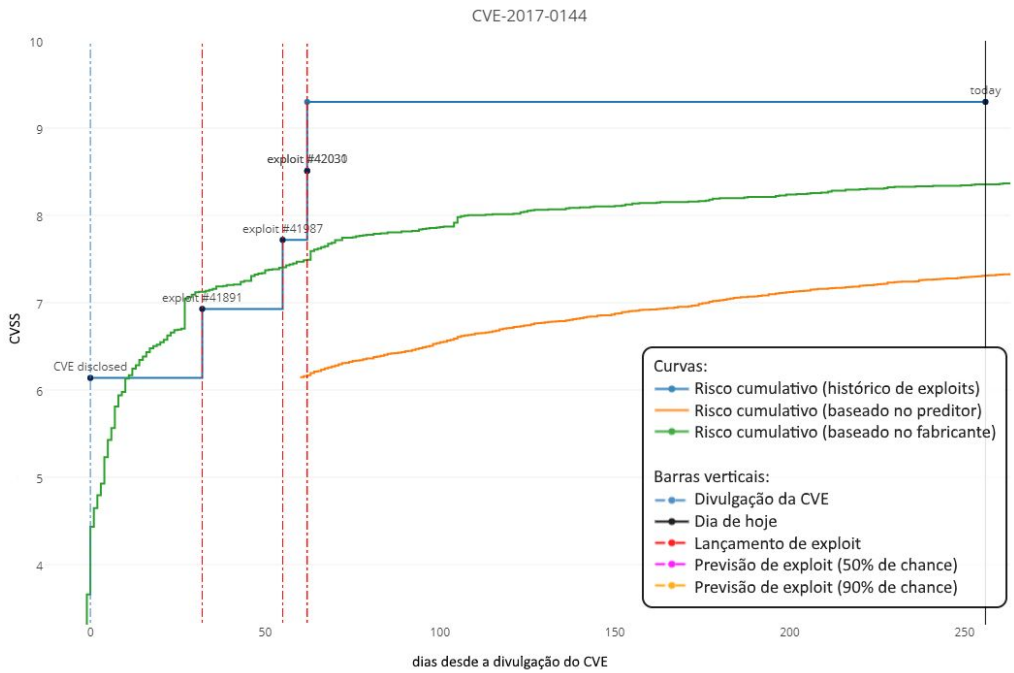
Modelos de Risco
Casos



CVE-2016-5195 – DirtyCow – Google

- Classificador errou; curva do fabricante compensa o erro nesse caso

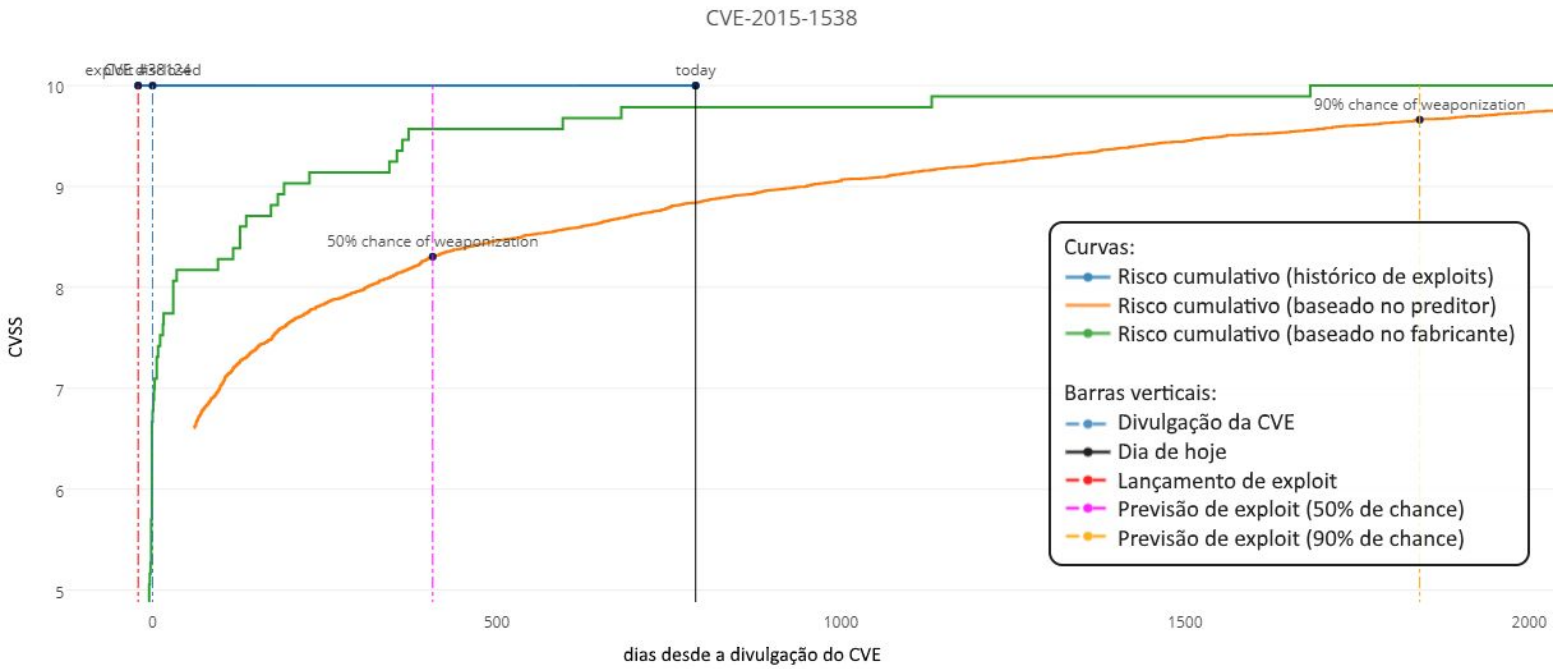
Modelos de Risco
Casos



CVE-2017-0144 – WannaCry – Microsoft

- Classificador errou; curva do fabricante compensa o erro nesse caso

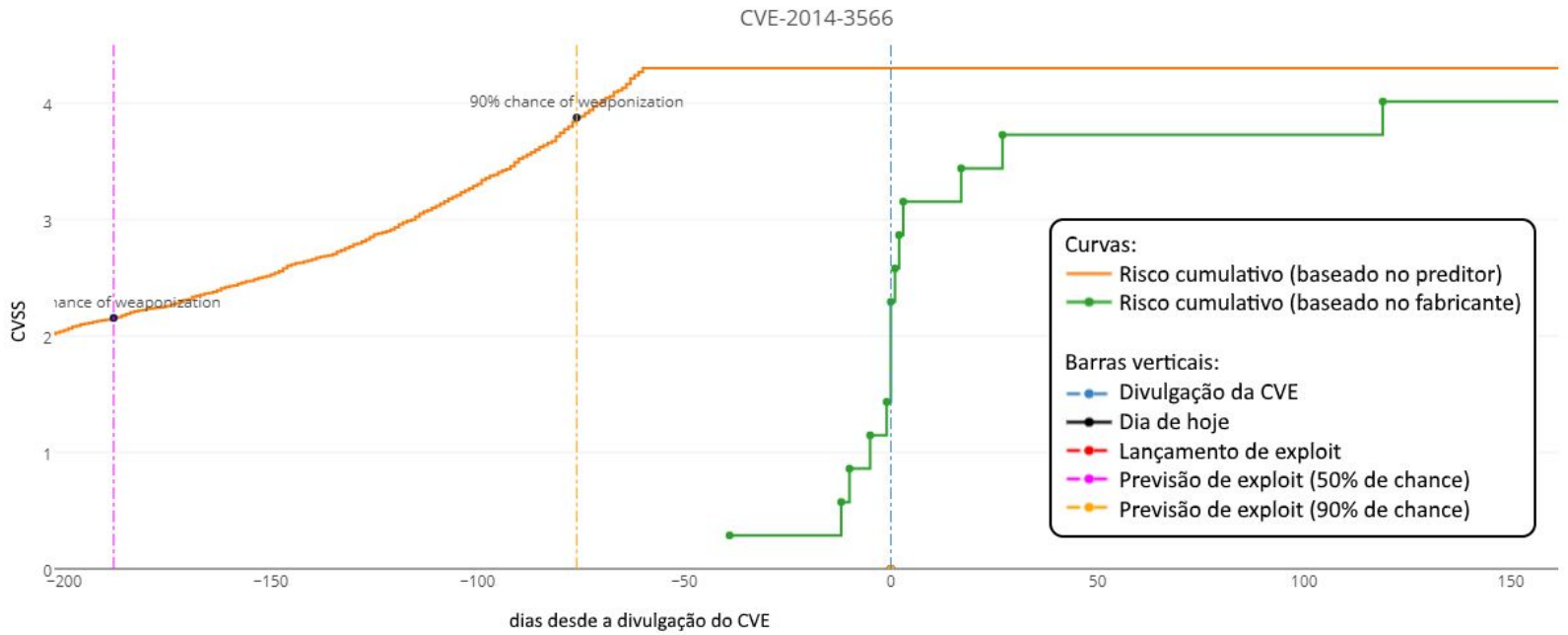
Modelos de Risco
Casos



CVE-2015-1538 – Stagefright – Google

- Classificador errou; curva do fabricante compensa o erro nesse caso

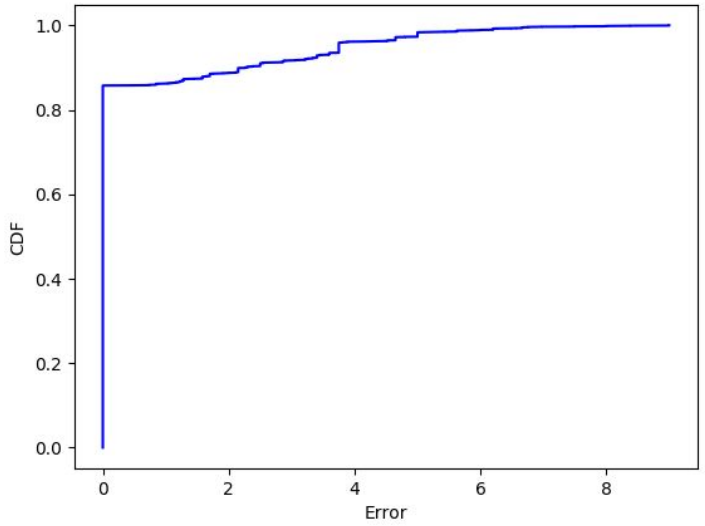
Modelos de Risco
Casos



CVE-2014-3566 – POODLE Attack – Openssl

- Não há *ground-truth* nesse caso... analista terá de decidir

Modelos de Risco
Validação

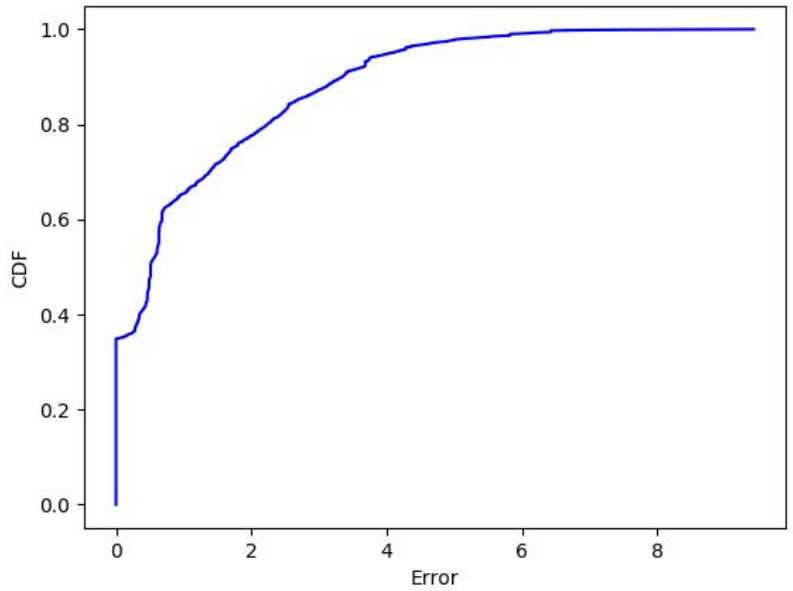


Erro condicionado a CVEs com 1 *exploit*

CDF do erro entre o risco no dia do único *exploit* menos risco estimado

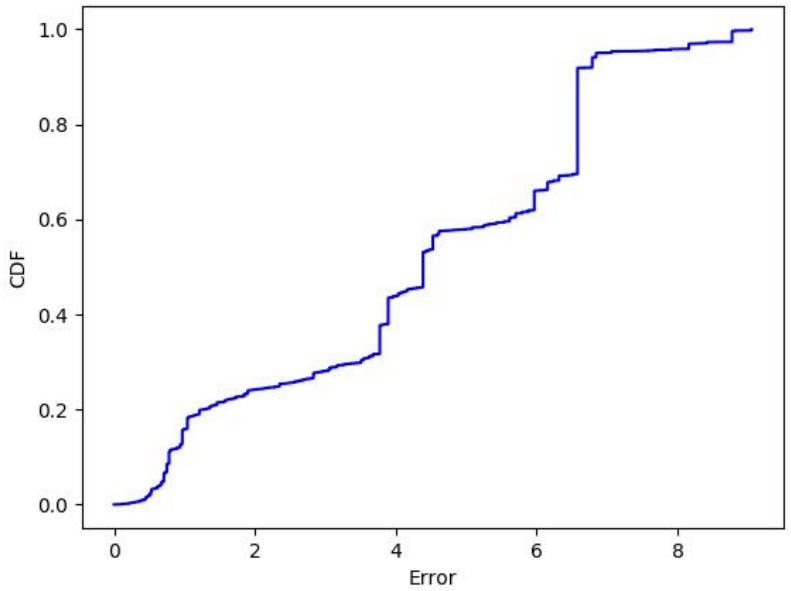
- 80% classificados sem nenhum erro

Modelos de Risco
Validação



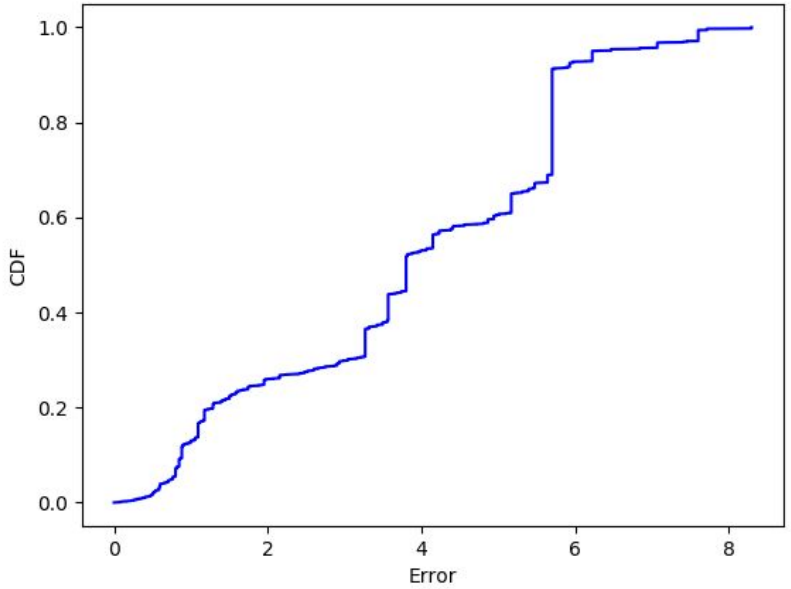
CDF do erro somado em todo o intervalo, dia a dia, em que existem as curvas de risco de *exploits* e do classificador

Modelos de Risco
Validação



CDF do erro entre o risco do dia do primeiro *exploit* e a mediana da classe prevista pelo classificador

Modelos de Risco
Validação



CDF do erro entre o risco do dia do primeiro *exploit* e a média da classe prevista pelo classificador

Conclusão

Conclusão

Bases de dados públicas não possuem informações temporais

81% dos *exploits* são *zero-days,*

Contribuições

- Modelos de análise para as datas de lançamentos de *exploits*
- Modelo de classificação
- Validação dos modelos

Conclusão
Trabalhos futuros

- Extensão das análises sobre o ciclo de vida de vulnerabilidades com a adição de datas sobre *patch* e datas sobre ataques reais;
- Extensão das análises realizados neste trabalho para *exploits* encontrados no mercado negro;
- Uso de diferentes técnicas para melhorar nosso classificador e, consequentemente, a curva de previsão de *exploits*;
- Uso de técnicas de aprendizado de máquina para mapeamento dos dados temporais do modelo do CVSS padrão;

Agradecimentos

Agradecimentos

Este trabalho não seria possível sem a colaboração e o esforço contínuo de nossos pares de trabalho e de nossos orientadores:

- Daniel Sadoc – orientador e coordenador do projeto
- Fabrício Firmino – co-orientador e colaborador no projeto
- Andressa Kappaun – colaboradora no projeto
- Zubair Shafiq – Universidade de Iowa, colaborador no projeto
- Treyton Krupp – Universidade de Iowa, colaborador no projeto
- Leandro de Aguiar – Siemens, responsável pelo projeto
- David Hingos – Siemens, colaborador no projeto
- Harsha Boggaram – Siemens, colaborador no projeto