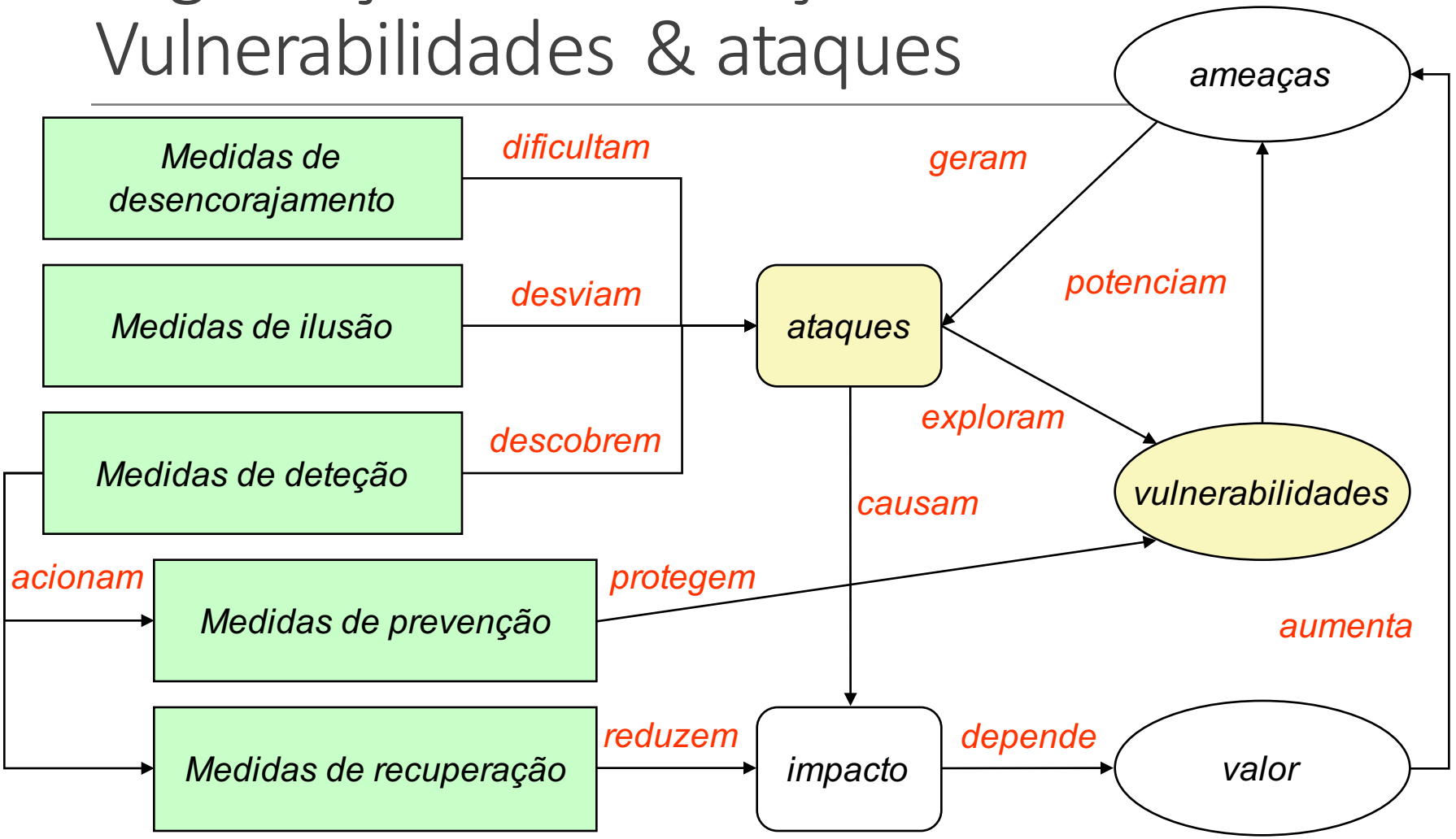
Vulnerabilidades

SEGURANÇA INFORMÁTICA E NAS ORGANIZAÇÕES

Segurança da informação: Vulnerabilidades & ataques



Medidas (e algumas ferramentas)

Desencorajamento
- Punição
  - Restrições legais
  - Evidências forenses
- Barreiras de segurança
  - *Firewalls*
  - Autenticação
  - Comunicação segura
  - *Sandboxing*

Prevenção
- Políticas restritivas
  - e.g. princípio do privilégio mínimo
- Pesquisa de vulnerabilidades
  - e.g. OpenVAS
- Eliminação de vulnerabilidades
  - e.g. atualização regulares

Ilusão
- *Honeypots / honeynets*
- Acompanhamento forense

Deteção
- Sistemas de deteção de intrusões
  - e.g. Snort
- Auditorias
- Análise forense de penetrações

Recuperação
- *Backups*
- Sistemas redundantes
- Recuperação forense

Prontidão (*security readiness*) (1/3)

O desencorajamento, a ilusão e a deteção servem sobretudo para lidar com problemas conhecidos

- Tentativas de reconhecimento (e.g. *port scanning*)
- Ataques genéricos (e.g. escuta da rede)
- Ataques específicos (e.g. *buffer overflows*)

As medidas de prevenção protegem de vulnerabilidades conhecidas ou desconhecidas

- Vulnerabilidades genéricas
  - e.g. reação a mensagens mal formadas (*protocol scrubbers*)
  - e.g. ataques furtivos (normalização para formatos canónicos)
- Vulnerabilidades específicas
  - e.g. um erro de software em particular

Prontidão (*security readiness*) (2/3)

A aplicação das medidas requer conhecimento sobre:

- Vulnerabilidades conhecidas
  - Problema, forma de exploração, impacto, etc.
- Padrões dos ataques que exploram essas vulnerabilidades
  - *Modus operandi*
  - Assinaturas de ataques
- Padrões anormais de atividade
  - Mas será fácil estabelecer um padrão de normalidade?
  - Os ambientes heterogéneos são um problema

Prontidão (*security readiness*) (3/3)

As ameaças em redes de computadores são diferentes de outros tipos de ameaças

- Os ataques podem ser lançados em qual hora, de qualquer local e por intermediários inocentes
- Podem ser facilmente coordenados
  - e.g. Distributed Denial of Service attacks (DDoS)
- São baratos
- Podem ser automatizados
- São rápidos

Requerem uma capacidade permanente (24x7) de reação a ataques

- Equipas de especialistas em segurança
- Alertas de ataque na hora
- Teste e avaliação dos níveis de segurança existentes
- Procedimentos de reação expeditos

Deteção de Vulnerabilidades

Ferramentas específicas podem detetar vulnerabilidades em sistemas

- Implementam ataques usando vulnerabilidades conhecidas
- Implementam ataques usando padrões de vulnerabilidades
  - Buffer Overflow, SQL Injection, XSS, etc…

Vitais para a robustez das aplicações e sistemas implementados

- Serviço frequentemente contratado

Podem ser aplicadas a:

- Código desenvolvido (Análise Estática): OWASP LAPSE+, RIPS, Veracode, ….
- Aplicação a executar (Análise Dinâmica): Valgrind, Rational AppScan, …
- Externamente como um sistema remoto: Metasploit, …

Não devem ser aplicadas de forma cega a sistemas em produção!

- Potencial perda/corrupção de dados
- Potencial negação de serviço

Ataques ou ameaças do dia zero

Ataque que ocorre no dia zero do conhecimento das vulnerabilidades que o permitem

- Para as quais não existem soluções conhecidas
- Pode explorar mesmo um padrão desconhecido

Ataque que explora vulnerabilidades que:

- São desconhecidas das vítimas
- São desconhecidas dos fabricantes implicados
- São desconhecidas dos organismos e empresas que apoiam a defesa contra ataques

Podem existir como "dia zero" durante muito tempo

- Dias... Meses... Anos

Sobrevivência

Como se sobrevive a uma ataque do dia zero?

Como se reage a uma ataque do dia zero massivo?

Diversidade de aplicações poderia ser uma solução …

- mas a produção, distribuição e atualização de software vai no sentido contrário
  - E o mesmo acontece com as arquiteturas de hardware
- Porque é que o MS Windows é um alvo primordial?
  - E o MAC OS X nem por isso?
- Está a usar um telemóvel Android?
  - Qual é a probabilidade de estar na linha da frente das vítimas?
  - Talvez um telemóvel com Windows Phone seja mais seguro ☺

CVE
Common Vulnerabilities and Exposures

Dicionário público de vulnerabilidades e exposições de segurança

- Para gestão de vulnerabilidades
- Para gestão de correções (*patches*)
- Para alarmística de vulnerabilidades
- Para deteção de intrusões

Identificadores comuns do CVE

- Permite a troca de informações entre produtos de segurança
- Fornece uma base de indexação para avaliar a abrangência de ferramentas e serviços

Detalhes de uma vulnerabilidade podem ser restritos

CVE: Vulnerabilidade

Erro no software

- Que pode ser usado diretamente por um atacante para ganhar acesso ao sistema ou à rede

Um erro só é uma vulnerabilidade se permitir que o atacante viole uma política de segurança

- Exclui políticas de segurança "abertas" onde todos os utentes são de confiança ou onde não se considera a existência de riscos para o sistema

Um vulnerabilidade é um estado de um sistema computacional (ou conjunto de sistemas) que, alternativamente:

- Permite que um atacante execute comandos em nome de terceiros
- Permite que um atacante aceda a dados ao arrepio do especificado nas restrições de acesso para esses dados
- Permite que o atacante se apresente como outrem
- Permite que o atacante negue a prestação de serviços

CVE: Exposição

Problema de configuração de um sistema ou um erro no software

- que permitem aceder a informação ou capacidades que podem auxiliar um atacante

O CVE considera um problema de configuração ou um erro como uma exposição se não permitir comprometer diretamente um sistema ou rede

- Mas for uma componente importante para o sucesso de um ataque e uma violação de uma política de segurança expectável

Uma exposição é um estado de um sistema computacional (ou conjunto de sistemas) que, alternativamente:

- Permite que um atacante realize recolhas de informação
- Permite a um atacante esconder as suas atividades
- Inclui uma funcionalidade que se comporta como esperado mas que pode ser facilmente comprometida
- É um ponto de entrada frequente para atacantes que tentam obter acesso ao sistema ou a dados
- É considerado problemático por uma política de segurança razoável

CVE: Benefícios

Fornece uma linguagem comum para referir problemas

Facilita a partilha de dados entre

- Sistemas de deteção de intrusões
- Ferramentas de aferição
- Bases de dados de vulnerabilidades
- Investigadores
- Equipas de resposta a incidentes

Permite melhorar as ferramentas de segurança

- Maior abrangência, facilidade de comparação, interoperabilidade
- Sistemas de alarme e reporte

Fomenta a inovação

- Local primordial para discutir conteúdos críticos das BDs

CVE: Limitações

Não ajuda à defesa contra ataques do dia zero!

CVE: Identificadores

Aka CVE *names*, CVE *numbers*, CVE-IDs, or CVEs

Identificadores únicos para vulnerabilidades conhecidas e públicas da CVE List

- Estados possíveis: "candidate" ou "entry"
- **Candidate**: sob revisão para inclusão na CVE List
- **Entry**: aceite na CVE List

Formato

- Identificador numérico CVE (CVE-Ano-Índice)
- Estado (*candidate* ou *entry*)
- Descrição sumária da vulnerabilidade ou exposição
- Referências para informação adicional

CVE e Ataques

Ataques podem ser compostos/possibilitados por várias vulnerabilidades

- Um CVE para cada vulnerabilidade
- Pode necessitar de uma sequência de vulnerabilidades
- Pode necessitar de uma das vulnerabilidades

Exemplo: Stagefright (Android, videos em mensagens MMS)

- CVE-2015-1538, P0006, Google Stagefright 'stsc' MP4 Atom Integer Overflow Remote Code Execution
- CVE-2015-1538, P0004, Google Stagefright 'ctts' MP4 Atom Integer Overflow Remote Code Execution
- CVE-2015-1538, P0004, Google Stagefright 'stts' MP4 Atom Integer Overflow Remote Code Execution
- CVE-2015-1538, P0004, Google Stagefright 'stss' MP4 Atom Integer Overflow Remote Code Execution
- CVE-2015-1539, P0007, Google Stagefright 'esds' MP4 Atom Integer Underflow Remote Code Execution
- CVE-2015-3827, P0008, Google Stagefright 'covr' MP4 Atom Integer Underflow Remote Code Execution
- CVE-2015-3826, P0009, Google Stagefright 3GPP Metadata Buffer Overread
- CVE-2015-3828, P0010, Google Stagefright 3GPP Integer Underflow Remote Code Execution
- CVE-2015-3824, P0011, Google Stagefright 'tx3g' MP4 Atom Integer Overflow Remote Code Execution
- CVE-2015-3829, P0012, Google Stagefright 'covr' MP4 Atom Integer Overflow Remote Code Execution

CVE-ID	
CVE-2015-1538	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

Date Entry Created	
20150206	Disclaimer: The entry creation date may reflect when the CVE-ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20150206)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is an entry on the CVE list, which standardizes names for security problems.

SEARCH CVE USING KEYWORDS: Submit

You can also search by reference using the CVE Reference Maps.

For More Information: cve@mitre.org

CVE: Criação de um identificador

1. **Discovery of a potential security vulnerability or exposure**
   - The information assigned a CVE candidate number by a CVE Candidate Numbering Authority (CNA)
   - CVE identifier is posted on the CVE Web site
   - Which publishes the CVE List
   - This list contains both candidate and entry CVE identifiers
   - CVE Editor proposes the CVE identifier to the Board
   - MITRE Corporation functions as Editor and Primary CAN

2. **CVE Editorial Board discusses candidates and votes on whether or not they should become CVE entries**
   - If rejected, the reason for rejection is noted in the Editorial Board Archives posted on the CVE Web site
   - If accepted, its status is updated to "entry"

CWE
Common Weakness Enumeration

Linguagem comum para discutir, encontrar e lidar com as causas das vulnerabilidades de segurança

- De programas, do seu desenho ou da arquitetura de sistemas
- Cada CWE representa um tipo de vulnerabilidade
- Gerida pela MITRE Corporation
  - Uma CWE list é disponibilizada pela MITRE website
  - Esta lista fornece uma definição pormenorizada de cada CWE

Os CWEs são catalogados segundo uma estrutura hierárquica

- CWEs localizados nos níveis superiores fornecem uma descrição genérica sobre o tipo de vulnerabilidade
  - Podem ter vários CWEs filhos associados
- CWEs nos níveis inferiores descrevem problemas de uma forma mais focada
  - Com menos ou sem CWEs filhos

Bases de dados de vulnerabilidades

NIST NVD (National Vulnerability Database)

CERT Vulnerability Card Catalog

US-CERT Vulnerability Notes Database

CERT
Computer Emergency Readiness Team

Organização orientada para a assegurar que a tecnologia e as práticas de gestão de sistemas adequados são usados para

- Resistir a ataques em sistemas em rede
- Limitar estragos e assegurar a continuidade de operação de sistemas críticos apesar da ocorrência de ataques bem sucedidos, acidentes ou falhas

CERT/CC (*Coordination Center*) @ CMU

- Uma componente do vasto CERT Program
- Centro primordial para questões de segurança na Internet
  - Criado em Novembro de 1988, após o "Morris Worm“
  - O verme demonstrou a vulnerabilidade crescente da rede a ataques globalizados

CSIRT
Computer Security Incident Response Team

Uma organização responsável por fornecer serviços de apoio para problemas de segurança em sistemas computacionais

- Serviço 24x7 para particulares, empresas, departamentos governamentais e outras organizações
- Ponto único de contacto para reportar incidentes de segurança computacional
- Disseminação de informação relevante de incidentes

CSIRT portugueses

- CERT.PT
  - Gerido pela FCCN
- CSIRT.FEUP
  - Gerido pela FEUP
- CERT-IPN
  - Gerido pelo Lab. de Informática e Sistemas do Inst. Pedro Nunes

Alarmes de segurança

Vitais para a disseminação rápida do conhecimento sobre novas vulnerabilidades

- US-CERT Technical Cyber Security Alerts
- US-CERT (non-technical) Cyber Security Alerts
- SANS Internet Storm Center
  - Aka DShield (Defense Shield)
- Microsoft Security Response Center
- Cisco Security Center

E muitos outros …