



Security in een Linux Distributie

Wat een distributie kan doen voor de beveiliging van computers

Linux World, Utrecht, November 2005

Arjan van de Ven



Computer security: hype of noodzaak

- Es is veel media aandacht voor beveiligingsproblemen:
 - ‘Computerkrakers hackten 1,5 miljoen computers’
 - ‘Nieuwe Zotob-achtige exploit duikt op’
 - ‘Scans naar lek in Microsoft SQL Server vertragen internet’
 - ‘Spam kost bedrijven 22 miljard per jaar’
 - ‘Sober-worm achter uitbraak Duitstalige spam’
 - ‘Experts bang voor grote uitbraak Sasser-worm’
 - ‘Explosieve groei uitgaven computerbeveiliging’
 - ‘Yahoo! dicht veiligheidsgat in email dienst’
- Wat als anderen via uw computer kinderporno aanbieden?
- Wat als anderen informatie over uw klanten in handen krijgen?

Wat is computer security ?

- “security” heeft veel aspecten, die vaak door elkaar gebruikt worden
- Vergelijk het met de beveiliging van een kantoor gebouw:
 - een bewaker aan de deur - LDAP directory server
 - een open raam - Buffer overflow
 - metaal detector bij de deur - Firewall
 - bagage X-ray - Virus scanner
 - alarm systeem - Intrusion Detection System
 - tralies voor de ramen - Exec-Shield
 - brandwerende deuren - SELinux
- Beveiliging moet in proportie zijn met de bedreiging...
- ... maar zelfs de beste kantoor beveiliging houdt de special forces niet tegen

De rol van een distributie

- Linux distributies (maar ook Microsoft en Sun) brengen regelmatig security updates uit
- Security Response Team staat klaar voor het ergste
- Priorisatie van beveiligings problemen
 - Critical - Automatisch en op afstand te misbruiken
 - Important - Lokaal of door bekende gebruikers
 - Moderate - Moeilijk te misbruiken / Niet default
 - Low - Onwaarschijnlijk en met weinig impact
- Mitre: het CVE systeem
- “Days at Risk” concept geïntroduceerd door Microsoft

- Maar.. is dit wel genoeg??

**De meeste gebruikers installeren de
beschikbare updates niet op tijd!**

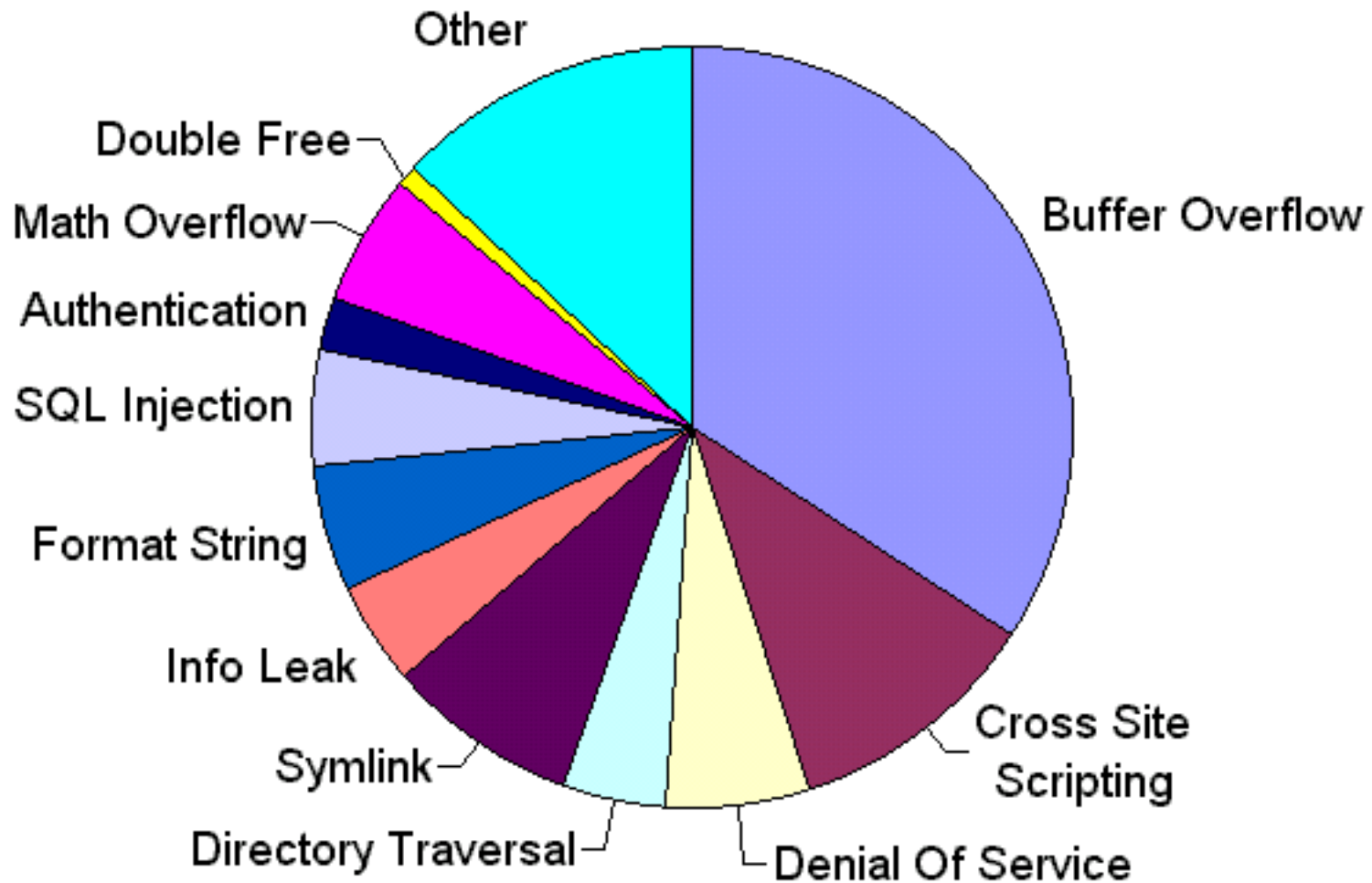
Dus... distributies moeten verder gaan

- Preventie van lekken
 - Kritisch zijn bij de keuze van open source pakketten (wu-ftpd vs vsftpd)
 - Code audits
 - Standaard firewall
 - Standaard weinig open netwerk poorten
- Gebruikers aanmoedigen om updates te installeren
 - Gevoelig item; automatische update gewenst maar niet haalbaar vanwege privacy bezwaren
- Schade van lekken beperken
 - Exec Shield: Inbraak en gebruik van een lek moeilijker maken
 - SELinux: Isolatie van de inbreker

Het Exec Shield project

- Multi-disciplinair, meerjarig project in Red Hat
- Doel
 - beperken van de gevolgen van veiligheids lekken in de distributie
 - geef sysadmins meer tijd om updates te installeren voordat een exploit live gaat
 - blokkeer hele categorieën van veiligheids lekken
- Randvoorwaarde
 - 100% compatibiliteit
 - Geen compromis aan de bruikbaarheid van het OS: gebruikers zetten beveiligingen uit die in de weg zitten
- Methode
 - Analyse van bestaande exploits naar de mechanismen en de randvoorwaarden die nodig zijn om een exploit succesvol te laten zijn
 - Analyse van bestaande preventie technologieën
 - Focus is op het voorkomen van de inbraak

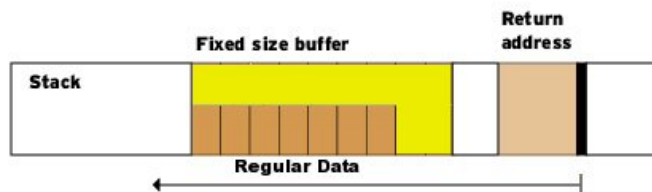
Verschillende soorten veiligheids lekken



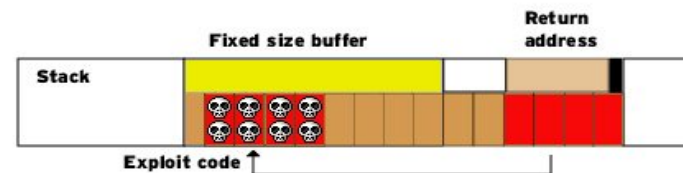
Based on 2004, Information collected by Steven M Christey from Mitre

Buffer overflows

- Een snel gemaakte fout, met grote gevolgen



Regular use: data fits in the buffer

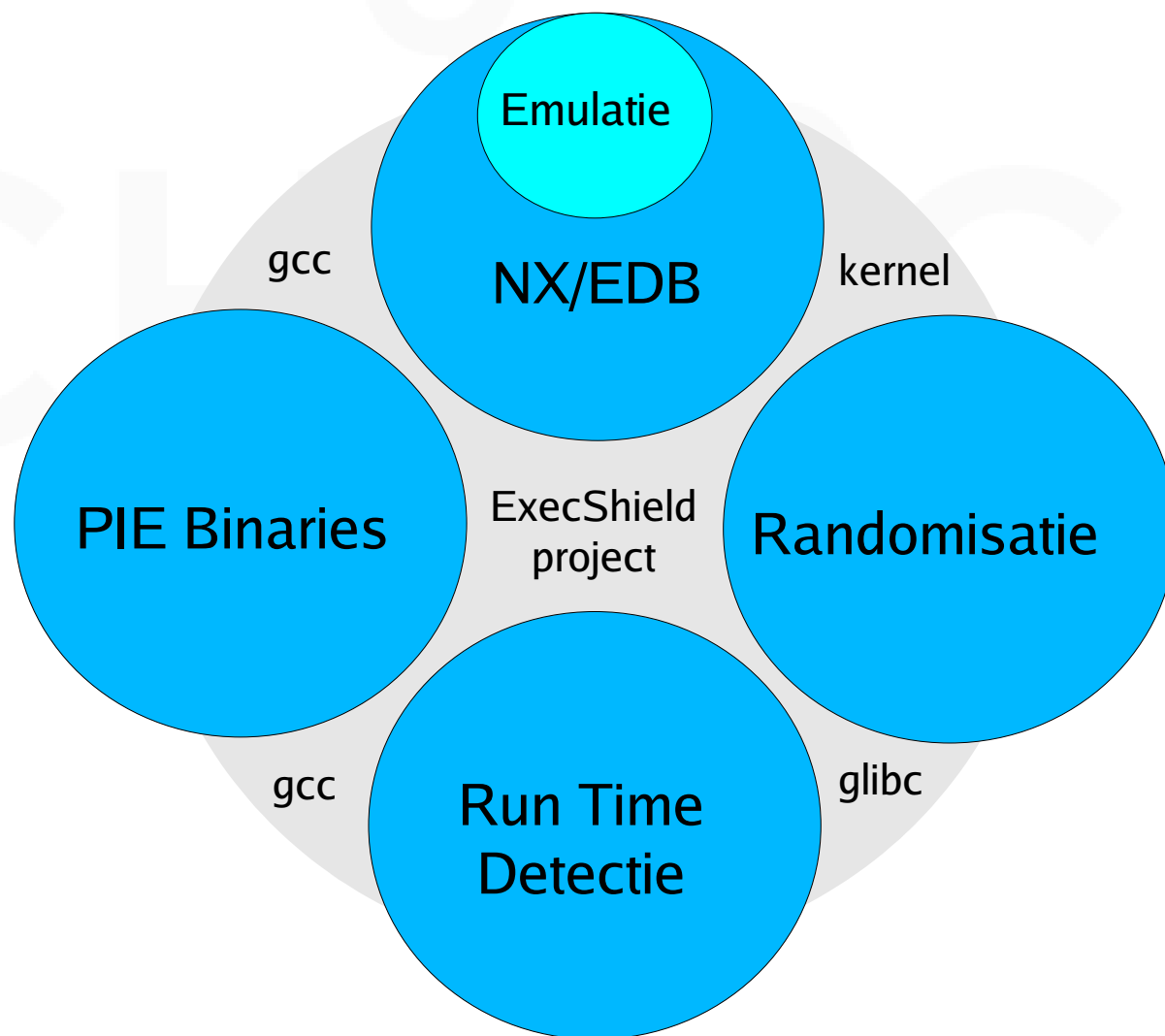


More data than fits in the buffer:
overflow overwrites critical data

- Vanwege het exploit gemak is dit de meest gevaarlijkste soort
- De “Code Red” en “Slammer” wormen waren de eerste buffer overflows die op het NOS 8 uur journaal te zien waren
- Er is veel literatuur over dit soort exploits, inclusief eenvoudige tutorials
 - Hacking: The art of exploitation (ISBN 1593270070)
 - The Shellcoder's Handbook : Discovering and Exploiting Security Holes (ISBN 0764544683)
 - Exploiting Software : How to Break Code (ISBN 0201786958)
 - Buffer Overflow Attacks : Detect, Exploit, Prevent (ISBN 1932266674)
 -

Buffer overflow exploits tegen houden

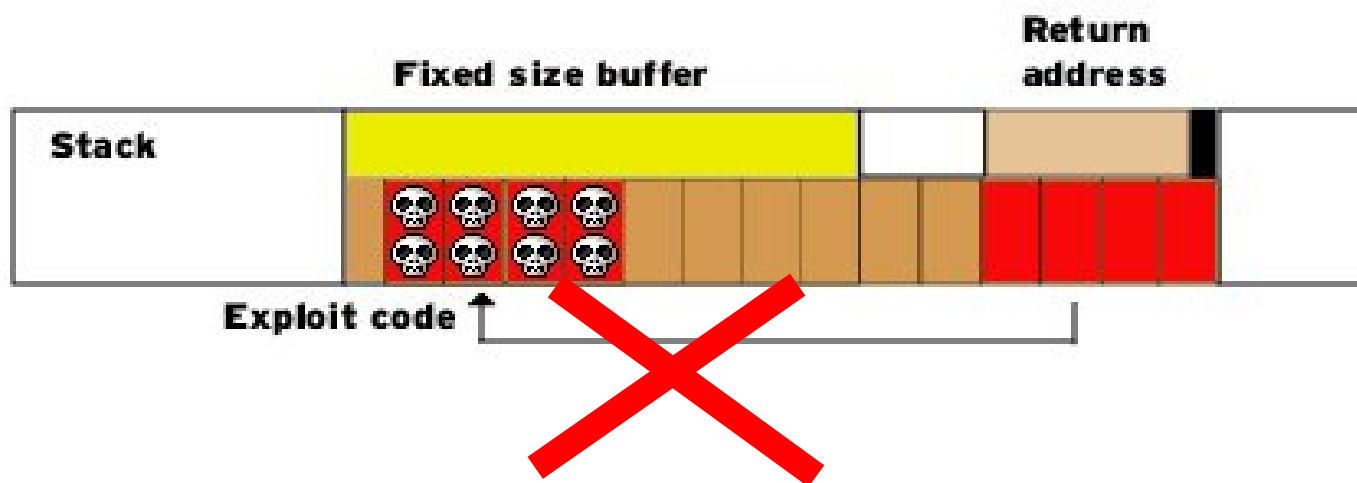
- Overzicht van de verschillende technieken



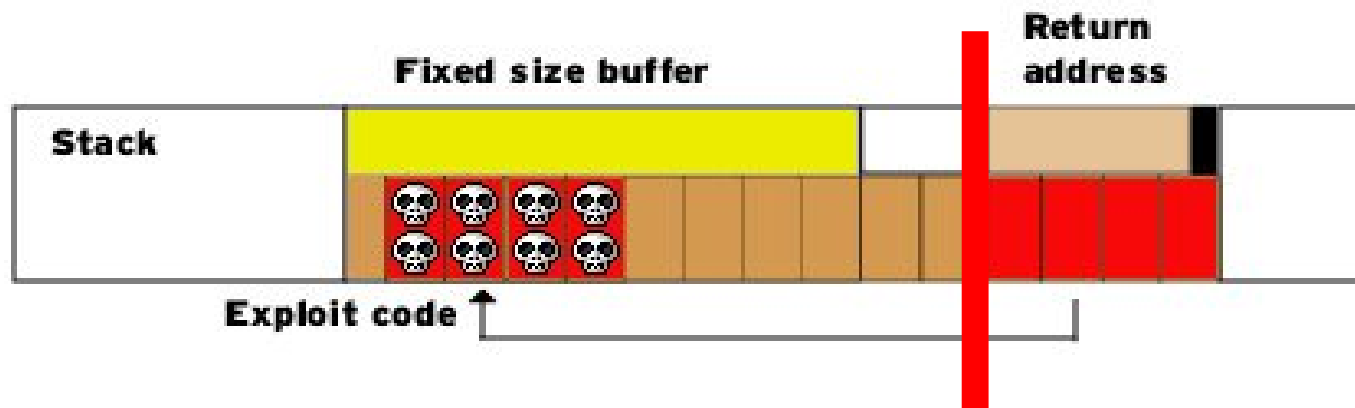
NX / EDB (of emulatie)



Randomisatie en PIE binaries



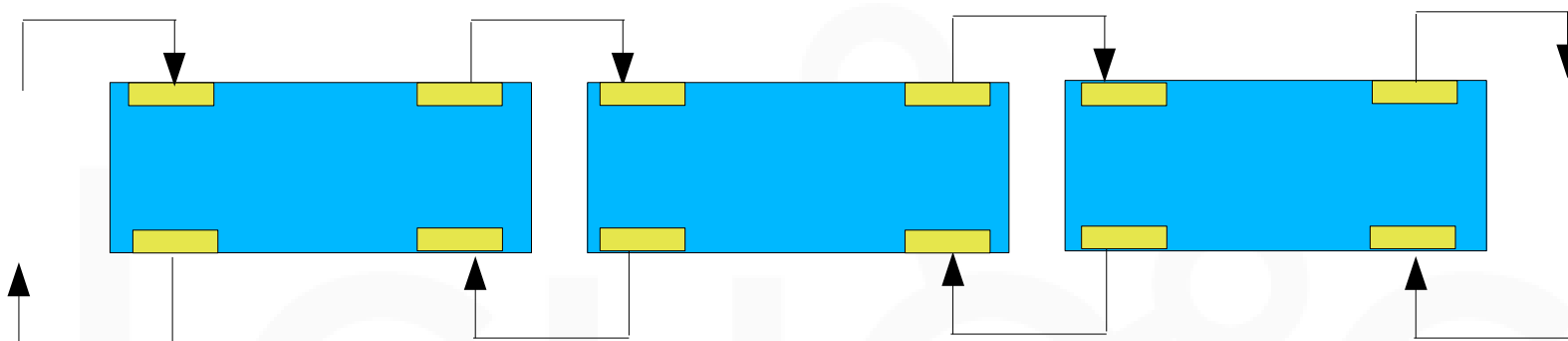
Runtime detectie



Heap / Double free exploits

- Deze exploits misbruiken de glibc memory allocator via een programma bug
- Veel literatuur te vinden, maar het misbruiken is veel moeilijker dan een buffer overflow
- ... maar bij misbruik zijn ze even gevaarlijk als buffer overflows
- Voorbeeld: de Linux Adore worm in 2001
- Recenter in het nieuws: De presentatie die Cisco op de BlackHat conferentie heeft voorkomen was van dit type.
- Hoewel het aandeel van dit type niet zo groot is, zijn deze wel belangrijk:
 - Van de 11 “critical” problemen in Red Hat Enterprise Linux 3, vanaf de start tot midden 2005 waren 3 van dit type

Double free: wat is het



Resultaten van Exec-Shield

- Misbruik van Buffer Overflows is nu (vrijwel) onmogelijk
 - bij 43% van de security issues die binnen komen wordt misbruik voorkomen op hardware met ondersteuning voor NX/EDB.
 - bij emulatie is dit 33%
- Double Free bugs zijn niet meer te misbruiken
 - 3 van de 11 “critical” bugs in RHEL3

SELinux

- Omgekeerd rechten model
 - traditioneel linux (DAC): “wie kan deze file openen”
 - SELinux model (MAC): “welke files kan deze applicatie openen”
- Alle OS objecten (files en dergelijke) hebben een label
- Elk process is in een “role”
- SELinux regels beschrijven permissies op labels per role, en voor role-overgangen
- Valse start in Fedora Core 2 betas:
 - het system policy probeerde alles te doen, maar was niet goed genoeg
 - bijna iedereen zette SELinux gewoon uit
- Nu: “targeted policy”
 - Bescherm alleen netwerk daemons
 - de rest van het systeem is onbeperkt

SELinux en beveiliging

- SELinux probeert de schade van een inbraak te beperken
- SELinux beperkt zich niet tot buffer overflows of andere bekende exploit technieken, maar is algemeen
- SELinux geeft applicaties need-to-know rechten; een inbreker kan de applicatie dus geen rare “andere” dingen laten doen
- “root” is niet meer almachtig; het is “root in een role”, een role met strenge beperkingen
- Dit beschermt dus ook tegen rotte PHP scripts (de nummer 1 oorzaak van linux inbraken)
- ... mits apache (en dus PHP) in een beperkte role werken.

SELinux is niet altijd makkelijk

- Gebruik van het volledige potentieel van SELinux zal nog jaren duren
- Uitdagingen
 - “Legacy” bestandssystemen (inclusief NFS en VFAT) die geen labels kunnen gebruiken
 - Applicaties met zeer veel configuratie mogelijkheden (apache)
 - Desktop applicaties zoals Evolution en Firefox
 - Plugins
 - Externe applicaties

SELinux in de toekomst

- Meer hulp om policy te schrijven of te genereren
- Automatische policy validatie
- Integratie met desktop infrastructuur (X, d-bus etc)
- Integratie met cryptographie
- SELinux met en over het netwerk

Meer informatie

- Whitepaper about ExecShield technology in Red Hat Enterprise Linux 3
 - http://www.redhat.com/f/pdf/rhel/WHP0006US_Execshield.pdf
- Red Hat Magazine Article about ExecShield
 - <http://www.redhat.com/magazine/009jul05/features/execshield/>
- Defensive programming paper by Ulrich Drepper
 - <http://people.redhat.com/drepper/defprogramming.pdf>
- How to write shared libraries
 - <http://people.redhat.com/drepper/dsohowto.pdf>
- Technical details about the security features
 - <http://people.redhat.com/drepper/nonselsec.pdf>