Beschreibung sicherheitsrelevanten Verhaltens in der Open Source Softwareentwicklung

Konzeptvorstellung Masterarbeit

Tobias Opel
Institut für Informatik
FU Berlin
28.02.2008

Agenda

Freie Universität Berlin

- Allgemeines
- Motivation
- Ziele der Arbeit
- Begriffe (IT-Security, Open Source Software)
- Kernaufgaben
- Bisherige Erkenntnisse
- Diskussion

Allgemeines

Freie Universität Berlin

- Thema: *Beschreibung sicherheitsrelevanten Verhaltens in der Open Source Softwareentwicklung*
- Bearbeiter: B.Sc. Tobias Opel
- Betreuer:
  - Dipl.-Medieninf. Martin Gruhn, Prof. Lutz Prechelt
- Anmeldung: 18.02.2008
- Abgabe: 18.08.2008

Motivation

Freie Universität Berlin

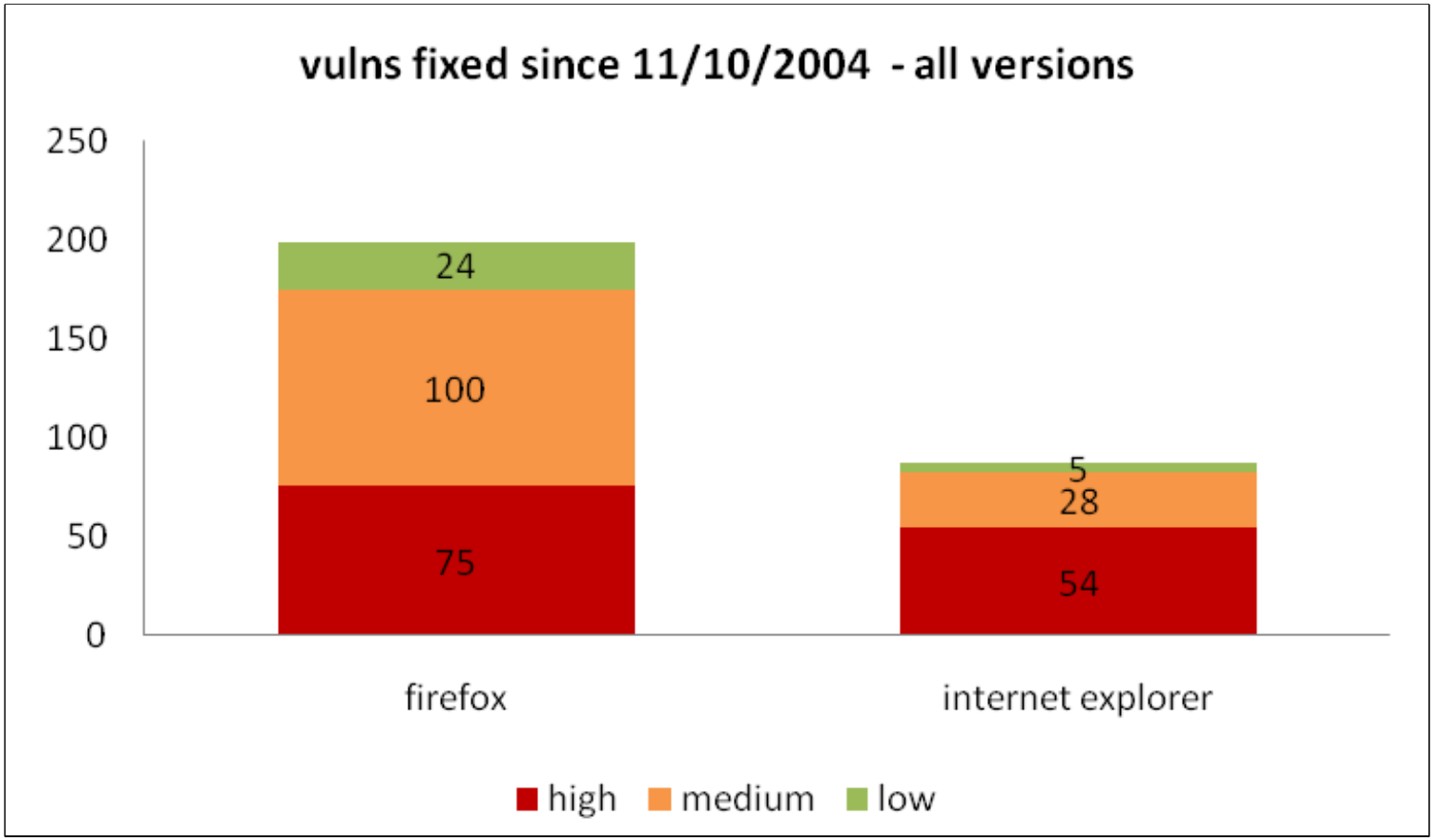
- Sicherheit von Internet Explorer (IE) und Firefox

- Vergleich beider Browser in der Studie "Browser Vulnerability Analysis"[1] von Jeffrey R. Jones
  - Jones ist Security Strategy Director in Microsoft's Trustworthy Computing group
- Betrachtung von geschlossenen und offenen sicherheitsrelevanten Schwachstellen in beiden Browsern
  - Schwachstellen unterliegen Common Vulnerabilities and Exposures (CVE) Namenskonvention
- Betrachtungszeitraum November 2004 – Oktober 2007
- Firefox 199 sicherheitsrelevante Schwachstellen behoben
- IE 87 sicherheitsrelevante Schwachstellen behoben

[1] http://blogs.technet.com/security/attachment/2594822.ashx, 27.11.2007

Motivation

- Geschlossene Schwachstellen nach Schweregrad

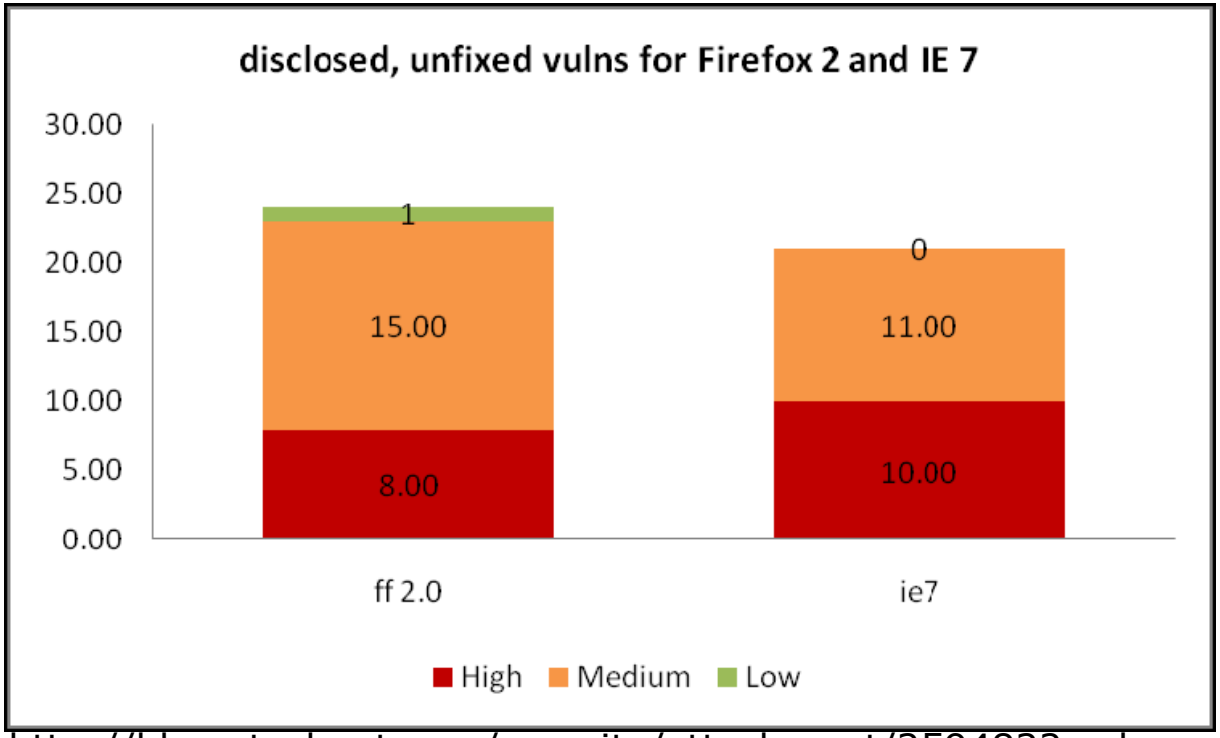


http://blogs.technet.com/security/attachment/2594822.ashx

Motivation

Freie Universität Berlin

- Bekannte offene Schwachstellen zum Zeitpunkt der Studie



http://blogs.technet.com/security/attachment/2594822.ashx

- Ergebnis der Studie: IE sicherer als Firefox
  - da weniger sicherheitsrelevante Schwachstellen im IE entdeckt worden sind als im Firefox

Motivation

- Kritiken und Ergänzungen zu der Studie[2]
  - intern gefundene Defekte des IE nicht in der Statistik, sondern nur extern gemeldete sicherheitsrelevante Schwachstellen
  - unklar, inwiefern sicherheitsrelevante Schwachstellen im Betriebssystem mit Auswirkungen auf den Browser in die Statistik eingegangen sind
  - unklar, ob einzelne Vulnerability Einträge mit mehreren Komponenten in der Studie als ein Eintrag gezählt oder auseinander dividiert wurden
  - lange Wartezeit bis Bugfix bei IE vorhanden
  - IE Nutzer seien regelmäßig bedroht, Firefox Nutzer nur zweimal bisher kurzzeitig hoher Gefahr ausgesetzt

[2] http://blog.mozilla.com/security/2007/11/30/critical-vulnerability-in-microsoft-metrics/
http://weblogs.mozillazine.org/schrep/archives/2007/11/use_the_metric_which_suits_you.html

Motivation

- Fazit: Vergleich Internet Explorer und Firefox
  - ein einheitliches Messverfahren fehlt
  - alle Daten (offene und interne) müssen im korrekten Kontext herangezogen werden
  - somit kein Vergleich zwischen „Closed" Source und Open Source Software aufgrund dieser Studie möglich

- der Qualitätsaspekt Sicherheit wird in der Studie auf Produktebene betrachtet
- Behebung von sicherheitsrelevanten Schwachstellen liegt ein Prozess zu Grunde
- **mehr** über diesen Prozess herausfinden

Motivation

- Fragen, die sich mir dazu stellen:
  - Welche Verhaltensweisen und Rollen treten bei der Behebung von sicherheitsrelevanten Schwachstellen auf?
  - Was hätte zur Vermeidung unternommen werden können?
  - Ist die Aussage '*Closed Source ist sicherer als Open Source Software oder umgekehrt*' generell möglich? Oder muss man differenzieren?
  - Ist OSS in allen Fällen gleich sicher?

- die ersten beiden Fragen führen zu den Zielen meiner Arbeit
- Antworten zu den letzten Beiden können möglicherweise aus den Erkenntnissen meiner Arbeit gewonnen werden

Ziele der Arbeit

- Beschreibung der **Behebung** von sicherheitsrelevanten Schwachstellen innerhalb der Open Source Softwareentwicklung
  - Verhaltensweisen und Rollen identifizieren und beschreiben

- Beschreibung der **Vermeidung** des Auftretens von sicherheitsrelevanten Schwachstellen bei der Open Source Softwareentwicklung
  - leicht erkennbare Verhaltensweisen und Mechanismen beschreiben

Begriffe - Sicherheit

- Was ist IT-Sicherheit?

Schutz von IT-Systemen vor unautorisiertem Informationsgewinn und Veränderung von gespeicherten oder verarbeiteten Informationen.[3]

- Was ist eine sicherheitsrelevante Schwachstelle?

Eine sicherheitsrelevante Schwachstelle oder auch Sicherheitslücke ist ein Defekt in einer Software die oben genannten Schutz verletzt.

[3] C. Eckert (2004): IT-Sicherheit.

Begriffe – Open Source Software

- Was ist Open Source Software?
  - Quelltext der Software muss offen für Bearbeitung und Weiterverbreitung sein
  - unterliegt wenigstens einer Open Source Software Lizenz (z.B. Open Source Initiative zertifiziert)

- Was sind typische Eigenschaften der Open Source Softwareentwicklung?[4]
  - Entwicklung ist iterativ und inkrementell
  - Asynchrone Kommunikation
  - Modularer Architekturentwurf
  - Allgegenwärtige Werkzeugunterstützung
  - geteilter Informationsraum

[4] L. Prechelt (2007): Spezielle Themen der Softwaretechnik

Kernaufgaben – Überblick

Freie Universität Berlin

1. Datenbestände auswählen und Geschichten zur Behebung sicherheitsrelevanter Schwachstellen finden
2. Verhaltenskategorien, Rollen und ihre Beziehungen untereinander aus den Geschichten ableiten
3. Vergleich von Literatur zur Qualitätssicherung mit den eigenen Erkenntnissen
4. Entwicklung von Erfolgsmaßen und Bewertung unterschiedlicher Formen sicherheitsrelevanten Verhaltens
5. Beschreibung von Verhaltensweisen und Mechanismen zur Vermeidung sicherheitsrelevanter Schwachstellen

Aufgabe 1: Geschichten

Freie Universität Berlin

- Aufgabe:

  Auswahl existierender Datenbestände und Auffinden geeigneter Geschichten, die Verhalten und Rollen bei der Behebung sicherheitsrelevanter Schwachstellen beschreiben.

- Geplantes Vorgehen:
  - Fokus liegt auf Open Source Webanwendungen und Bibliotheken
  - Datenbestände zu diesen Projekten in Form von Mailinglisten, Bugtrackern und Webseiten identifizieren
  - Vulnerability Datenbanken als weitere Hilfe/Einstiegspunkte heranziehen
  - Geschichten aus der gefunden Datenbasis extrahieren

Aufgabe 1: Geschichten

Freie Universität Berlin

- bereits vorgenommene Arbeiten:
  - einige Datenbestände und Vulnerability Datenbanken identifiziert
  - erste Geschichten gefunden und rudimentär dokumentiert
  - Mitarbeit an einer Umfrage zur FOSDEM 08, um weitere Informationen bezüglich der Datensammlung zu erlangen

- Herausforderungen:
  - geschlossene Datenbestände (interne Security Mailinglisten)
  - relevante Geschichten identifizieren

Geschichten: Beispielgeschichte

Freie Universität Berlin

Verwirrung durch Schwachstellenmeldung bei OpenSSL

- CVE-Name: CVE-2007-3108
- Schwachstellenbeschreibung

  verschiedene Implementierungen von RSA besitzen eine sicherheitsrelevante Schwachstelle, die einem Angreifer Zugriff auf den Kodierungsschlüssel ermöglichen

- Beteiligte in dieser Geschichte:
  - Developer aus dem Development Team (Andy Polyakov - appro)
  - Externer Beteiligter (Kurt Roeckx)

Verwirrung durch Schwachstellenmeldung bei OpenSSL

- Inhalt der Geschichte:
  - externer Beteiligter findet Schwachstellenmeldung und Sicherheitspatch
  - dazu gibt es aber kein Mailinglisten - Announcement
  - durch entstandene Verwirrung erfolgt Mailinglistenpost mit Angabe der Schwachstellenmeldungen und Codeänderungen im Repository, welche eine Behebung der Schwachstelle darstellen
  - Schwachstellenmeldung und Codeänderungen werden durch den Verantwortlichen der Codeänderungen bestätigt

Aufgabe 2: Abstraktion

- Aufgabe:

  Ableitung von Verhaltenskategorien, Rollen und ihrer Beziehungen untereinander zur Beschreibung sicherheitsrelevanten Verhaltens in der Open Source Softwareentwicklung.

- Geplantes Vorgehen:
  - Geschichten codieren und kategorisieren
  - Verhaltenskategorien und Rollen und deren Beziehungen aus den Geschichten ableiten

Aufgabe 2: Abstraktion

Freie Universität Berlin

- bereits vorgenommene Arbeiten:
  - Tags bzw. Schlüssel für bisher gesammelte Geschichten gesucht und sie damit gekennzeichnet
  - Rollen identifiziert und in Kategorien eingeordnet

- Herausforderungen:
  - Finden von Vielzahl an unnötigen und überflüssigen Schlüsselwörtern und Kategorien, gerade am Anfang
  - Gesamte Bandbreite der Kategorien erst im späteren Verlauf der Geschichtensammlung sichtbar

Abstraktion: Beispielgeschichte

Verwirrung durch Schwachstellenmeldung bei OpenSSL

- vergebene Tags:
  - Behebung der sicherheitsrelevanten Schwachstelle
  - Patch/Lösung vorhanden
  - keine vorangegangene/zugehörige Diskussion ersichtlich
  - keine externe Anteilnahme
- Rollen:
  - Entwickler aus dem Development Team

Aufgabe 3: Related Work

Freie Universität Berlin

- Aufgabe:

  Vergleich von in der Literatur zu Qualitätssicherung in der Softwaretechnik beschriebenen Modelle, Prozesse und Rollen mit den eigenen Erkenntnissen.

- Geplantes Vorgehen:
  - Literatur zu den Themen *Sicherheit in der Softwaretechnik*, *Sicherheit in der Open Source Software* und *Qualitätssicherung* im weitesten Sinne suchen und durcharbeiten
  - die dort beschriebenen Verhaltensweisen, Prozesse und Rollen identifizieren und mit denen aus meinen Geschichten vergleichen

Aufgabe 3: Related Work

Freie Universität Berlin

- bereits vorgenommene Arbeiten:
  - Literaturrecherche parallel zur Vorbereitung betrieben
  - größtenteils zum Thema Sicherheit und Open Source Software
  - aber auch zu Qualitätssicherung in OSS und Patchprozessen

- Herausforderungen:
  - Literatur zur Qualitätssicherung in der Softwaretechnik könnte unvollständig sein oder in die falsche Richtung abzielen
  - Vergleich zwischen konventioneller Softwaretechnik und eigenen Erkenntnissen könnte schwierig sein

Aufgabe 4: Erfolgsmaße

- Aufgabe:

  Entwicklung von Erfolgsmaßen für sichere Open Source Software und Bewertung unterschiedlicher Formen sicherheitsrelevanten Verhaltens.

- Geplantes Vorgehen:
  - Erfolgsmaße aufstellen
  - Erfolgsmaße anhand der Geschichten bewerten
  - vorangegangenen Vergleich zwischen eigenen Erkenntnissen und der Literatur für die Bewertung der Erfolgsmaße heranziehen

Aufgabe 4: Erfolgsmaße

Freie Universität Berlin

- Herausforderungen:
  - fehlerhaftes bzw. ungültiges Erfolgsmaß aufstellen
  - falsche Voraussetzungen für die Bewertung des Erfolgsmaßes heranziehen
  - Bewertung von sicherheitsrelevantem Verhalten falsch durchführen oder zu einem ungültigem Ergebnis gelangen

- Ich sehe in dieser Aufgabe die größte Herausforderung!

Aufgabe 5: Vermeidung

Freie Universität Berlin

- Aufgabe:

  Beschreibung von leicht erkennbaren Verhaltensweisen und Mechanismen zur Vermeidung sicherheitsrelevanter Schwachstellen in ausgewählten Projekten.

- Geplantes Vorgehen:
  - Hinweise zur Vermeidung sicherheitsrelevanter Schwachstellen, die im Rahmen der Arbeit anfallen, untersuchen und dokumentieren

- bereits vorgenommene Arbeiten:
  - im Rahmen der Datenbeschaffung und der Vorbereitung der Arbeit auf Angaben von Mechanismen zur Vermeidung von Schwachstellen gestoßen

Bisherige Erkenntnisse

Freie Universität Berlin

- Geschichten finden ist nicht einfach
- größte Hürde bisher – geschlossene Informationsbereiche, wie z.B. interne Mailinglisten/ Tracker
- Qualitative Analyse ist aufwändiger als reine quantitative Datenerhebung und -auswertung

- ABER, mit jeder neuen Geschichte wird der Prozess der Auswahl existierender Datenbestände und des Auffindens geeigneter Geschichten einfacher

Diskussion

- Sind die von mir vergebenen Tags in der Beispielgeschichte sinnvoll? (siehe nächste Folie)
  - unvollständig
  - zu speziell
  - zu allgemein

Diskussion: Beispielgeschichte

Freie Universität Berlin

- Inhalt der Geschichte:
  - externer Beteiligter findet Schwachstellenmeldung und Sicherheitspatch
  - dazu gibt es aber kein Mailinglisten - Announcement
  - durch entstandene Verwirrung erfolgt Mailinglistenpost mit Angabe der Schwachstellenmeldungen und Codeänderungen im Repository, welche eine Behebung der Schwachstelle darstellen
  - Schwachstellenmeldung und Codeänderungen werden durch den Verantwortlichen der Codeänderungen bestätigt
- vergebene Tags:
  - Behebung der sicherheitsrelevanten Schwachstelle
  - Patch/Lösung vorhanden
  - keine vorangegangene/zugehörige Diskussion ersichtlich
  - keine externe Anteilnahme

Vielen Dank!