



# Theoretische und praktische Risiken der Verwendung von URL-Verkürzungsdiensten

Alexander Neumann  
alexander.neumann@redteam-pentesting.de  
RedTeam Pentesting GmbH  
<http://www.redteam-pentesting.de>

19. DFN Workshop „Sicherheit in vernetzten Systemen“  
21./22. Februar 2012, Hamburg



## Über mich

- ★ Alexander Neumann
- ★ Vortrag und Ergebnisse basieren auf meiner Diplomarbeit
- ★ Seit 2009 Penetrationstester bei RedTeam Pentesting





# RedTeam Pentesting - Daten und Fakten

- ★ Gegründet 2004
- ★ Spezialisierung ausschließlich auf Penetrationstests
- ★ Firmensitz in Aachen, weltweite Durchführung von Penetrationstests
- ★ Forschung im IT-Sicherheitsbereich





# Lange URLs und ihre Probleme

Warum URL-Verkürzungsdienste?

- ★ Lange URLs brechen ungünstig um
- ★ Twitter beschränkt Nachrichten auf 140 Zeichen
- ★ Foren filtern URL-Ziele (z.B. keine ebay-URLs)
- ★ URLs Abtippen ist fehleranfällig
- ★ Lange URLs können verschleiert werden
- ★ Zugriffsstatistiken (ohne Zugriff auf die Zielseite)

→ URL-Verkürzungsdienste

Beispiel: `http://bit.ly/B1E9j`



# Motivation

Warum lohnt eine Untersuchung?

- ★ Benutzer verwenden URL-Verkürzungsdienste (Twitter)
- ★ Manchmal sogar unbeabsichtigt (z.B. Twitter-Clients)
- ★ Seit Mitte 2011 verkürzt Twitter alle URLs zwangsweise
- ★ Risiken von Verkürzungsdiensten sind wenig untersucht
- ★ Und: Benutzer sind sich der Risiken nicht bewusst

Also:

- ★ Welche Risiken bergen Verkürzungsdienste?
- ★ Sind diese praxisrelevant?



# Geschäftsmodelle

Welches Geschäftsmodell haben URL-Verkürzungsdienste?

Üblich:

- ★ „Freemium“, kostenlose Basis- und kostenpflichtige Premiumfunktionen
- ★ Werbung



# Malware

Fiktives Geschäftsmodell eines arglistigen Dienstes:

- ★ Bei jeder Anfrage wird neu entscheiden
- ★ Bei verwundbarem Browser: Umleitung auf Malware
- ★ Ansonsten: Normale Umleitung auf lange URL
- ★ Poweruser haben aktuelle Software und merken nichts
- ★ Anbieten von Zugriffen verwundbarer Benutzer

Gibt es einen solchen Verkürzungsdienst?



# Überwachung

URL-Verkürzungsdiensten können Benutzer überwachen:

- ★ Verkürzungsdienst muss immer kontaktiert werden
- ★ Liefert Statistiken für Ersteller der URL  
Beispiel: `http://bit.ly/B1E9j+`
- ★ Kann Cookie mit langer Laufzeit hinterlegen
- ★ Anschließend Profile von Benutzern erstellen
- ★ Verkürzungsdienst ist für Benutzer transparent
- ★ Bei populären Diensten höhere Genauigkeit des Profils

Welche Cookies und Laufzeiten verwenden populäre Dienste?





## Geheime URLs

Zugriff auf (vertrauliche) Dokumente anhand einer geheimen URL:

- ★ Beispiele: Google Documents, Scribd, Flickr, ...
- ★ Durch Verkürzung:
  - ★ Kurze URLs sind enumerierbar  
→ URL kann gefunden werden
  - ★ Verkürzungsdienst kennt geheime URL  
→ Missbrauch?

Offene Fragen:

- ★ Verkürzen Benutzer geheime URLs?
- ★ Sind Administratoren von Diensten vertrauenswürdig?



## Verfügbarkeit & Latenz

Welche Auswirkung hat die Nutzung von Verkürzungsdiensten?

- ★ Einschränkungen beim Verkürzungsdienst betrifft alle Aufrufe
- ★ Beispiele: Erreichbarkeit, Latenz, Reaktionszeit, ...
- ★ Wird der Dienst eingestellt, sind **alle** kurzen URLs defekt
- ★ Gehackter Dienst → Umleitung auf Spam/Malware
- ★ Kein Backup → URLs permanent verloren

Untersuchung: Wie lange wird der Aufruf einer URL verzögert?



## Untersuchung - Vorbereitungen

Analyse von zweimal 24h etwa 10% aller Twitter-Nachrichten  
(2010: 7,5 und 2011: 8,6 Millionen Nachrichten)

Die populärsten Dienste in diesen Nachrichten sind:

- |                      |            |
|----------------------|------------|
| 1 bit.ly (auch j.mp) | 6 dlvr.it  |
| 2 t.co               | 7 is.gd    |
| 3 tinyurl.com        | 8 migre.me |
| 4 goo.gl             | 9 dld.bz   |
| 5 ow.ly              | 10 lnk.ms  |



# Malware und arglistige Verkürzungsdienste

Entscheiden Verkürzungsdienste anhand des Browsers, welche Ziel-URL ausgeliefert wird?

Vorgehen:

- ★ Anfragen von 319 URLs von 187 Verkürzungsdiensten
- ★ Jeweils mit 83 unterschiedlichen Browserversionen
- ★ Auswerten von Location- und Set-Cookie-Header

Ergebnis: Kein arglistiger Dienst gefunden.

Aber: Hinweise auf unterschiedliche Behandlung



# Überwachung

Cookies aus dem vorherigen Experiment, berechne „Eindeutigkeit“:

$$Q := \frac{\text{Anzahl eindeutiger Werte}}{\text{Anzahl Cookies}}$$

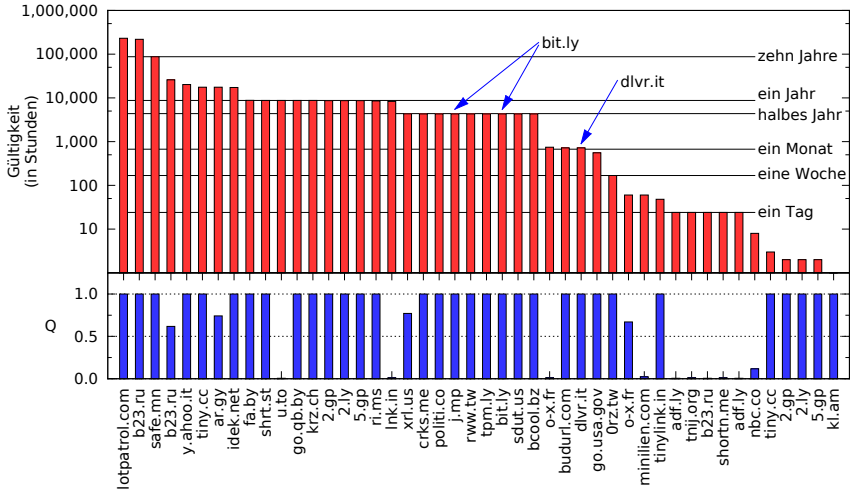
Dann gilt:

- ★  $Q \approx 0 \Rightarrow$  Cookie vermutlich nicht anfrage-/benutzerspezifisch
- ★  $Q \approx 1 \Rightarrow$  Cookie ist anfrage-/benutzerspezifisch  
 $\Rightarrow$  Benutzertracking bei weiteren Anfragen möglich

Weiterhin: Analyse der Gültigkeitsdauer persistenter Cookies



# Ergebnis





# Geheime URLs #1

Gelangen geheime URLs über Verkürzungsdienste an Dritte?

Experiment:

- ★ Aufsetzen eines Honeypot-Webserver
- ★ Generieren und Verkürzen von eindeutigen URLs (255 Dienste)
- ★ Jeweils verdächtige und harmlose URLs, Beispiele:
  - ★ <http://fd0.me/secret/a0df29ac/bb42ce8b>
  - ★ <http://www.fd0.me/blog/archive/2011/01/14/index.php?article=69e325eb#a5a6c61c>

Nach zwei Wochen: Logdatei analysieren



## Geheime URLs #1 - Ergebnisse

Honeypot-Webseiten wurden angefragt von:

- ★ Google: 15 URLs
- ★ Yahoo: 13 URLs
- ★ Baidu: 2 URLs
- ★ 13 URLs wurden vom Verkürzungsdienst-Admin angeklickt  
(Bei 9 Anfragen war im Referer die Admin-URL enthalten)

⇒ Niemals geheime URLs verkürzen!





## Geheime URLs #2

### Fragen:

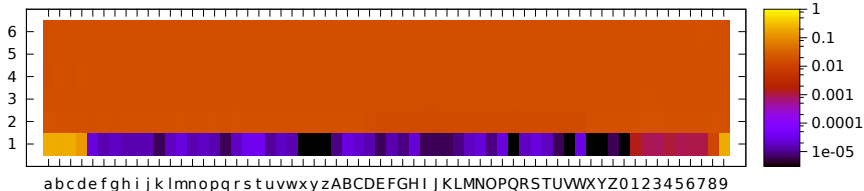
- ★ Verkürzen Benutzer geheime URLs?
- ★ Lassen sich durch Enumerieren geheime URLs finden?
- ★ Verhindern Verkürzungsdienste dies?

### Vorgehen:

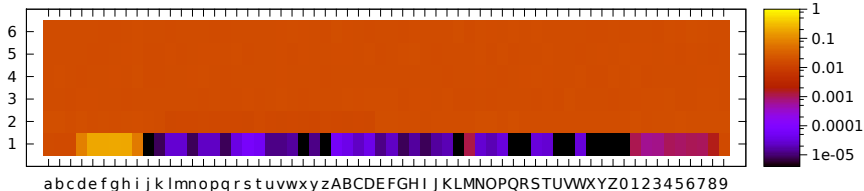
- ★ Analysiere Struktur der Top-10 Dienste aus bei Twitter gefundenen URLs
- ★ Enumeriere jeweils etwa 240.000 URLs pro Dienst
- ★ Frage lange URL sowie zugehörige robots.txt an
- ★ (Manuelle) Suche nach geheimen URLs



## Zeichenhäufigkeit in 350.000 bit.ly-URLs (2010):

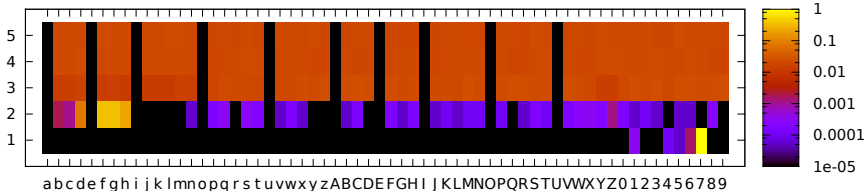


## Zeichenhäufigkeit in 260.000 bit.ly-URLs (2011):

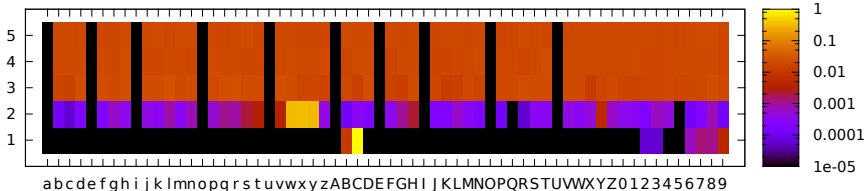




## Zeichenhäufigkeit in 18.300 dlvr.it-URLs (2010):

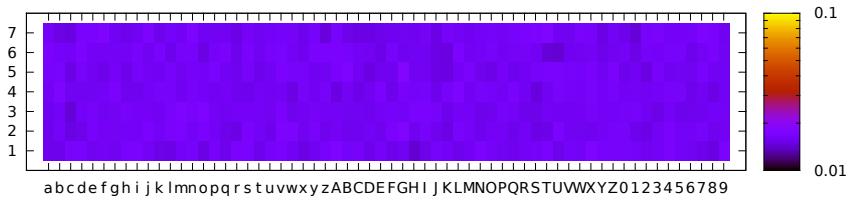


## Zeichenhäufigkeit in 16.900 dlvr.it-URLs (2011):

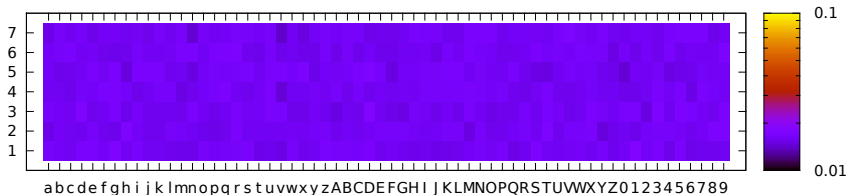




## Zeichenhäufigkeit in 40.400 t.co-URLs (2010):



## Zeichenhäufigkeit in 42.400 t.co-URLs (2011):





## Ergebnisse

Gefundene lange URLs:

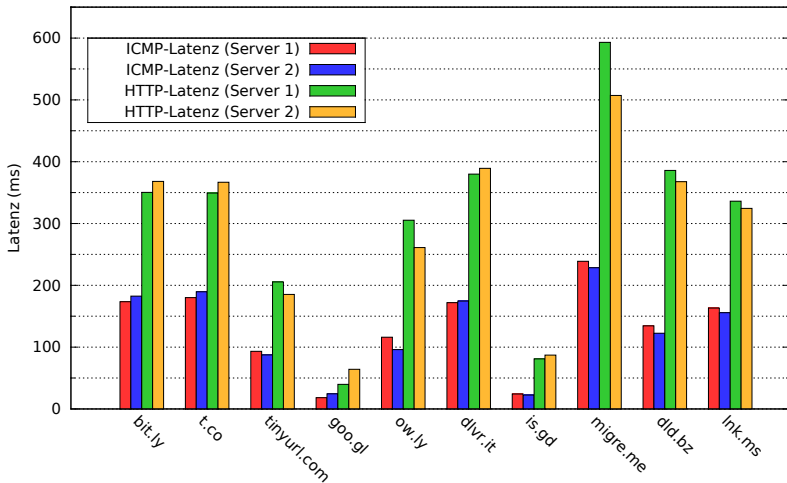
- ★ Anteil von für Suchmaschinen verbotenen URLs bis 6,2 %
- ★ Insgesamt 153 administrative Webseiten (Pfad /admin/)
- ★ 71 öffentlich zugängliche Dokumente bei Google Documents:
  - ★ Archive eindeutig privater Fotos
  - ★ Lebensläufe
  - ★ Liste der Einnahmen und Ausgaben einer Firma
  - ★ Telefonliste einer Kindergartengruppe

Weiterhin: Nur `goo.gl` ergreift Maßnahmen gegen Enumerieren

⇒ Niemals geheime URLs verkürzen!



## Latenzmessung über zwei Wochen





# Verfügbarkeit

The screenshot shows the RWTH Aachen University website. The header includes the RWTH logo and navigation links for 'Suche', 'Hilfe', 'RZ Intern', 'A-Z', 'Feedback', and 'RWTH'. The main navigation bar lists 'Studierende', 'Institute und Mitarbeiter', 'Projekte und Kooperationen', and 'MATSE-'. The left sidebar contains a menu with 'Aktuelles', 'Wir über uns', 'Unsere Dienste', 'Hochleistungsrechnen', 'Virtuelle Realität', 'Veranstaltungen', and 'RZ-ServiceDesk'. The main content area displays a notice titled 'RWTH KurzURL' with the following text:

[RZ](#) > [Unsere Dienste](#) > RWTH KurzURL

## RWTH KurzURL

Liebe Nutzer des KurzURL Dienstes,

aufgrund der geringen Nutzung wird der KurzURL Dienst zum 1.3. eingestellt.

Die Abschaltung wird schrittweise geschehen:

1. ab sofort ist es nicht mehr möglich, neue KurzURLs anzulegen.
2. ab dem 1.3.2012 werden vorhandene KurzURLs nicht mehr funktionsfähig sein.

Bitte beachten Sie, dass entsprechend auch Webseiten und Dokumente, die die KurzURLs benutzen, angepasst werden müssen.

Alternativen zu dem Dienst sind frei im Internet verfügbar.

Danke für Ihr Verständnis,

Ihr Rechen- und Kommunikationszentrum



## Fazit

- ★ Verkürzungsdienste bergen Risiken
- ★ Diese sind praxisrelevant
- ★ Niemals geheime URLs verkürzen
- ★ URL-Verkürzungsdienste sollten nicht in statischen Dokumenten (Paper, Bücher) verwendet werden
- ★ Verkürzungsdienste können Benutzer überwachen
- ★ Verkürzte URLs sind nicht zufällig
- ★ Dienste unterscheiden sich deutlich in Zuverlässigkeit, Geheimhaltung, Statistikfunktionen, Überwachungsmöglichkeiten





Fragen?

Vielen Dank für Ihre Aufmerksamkeit!