Android Iodine Anwenderdokumentation

Inhaltsverzeichnis

Zusammenfassung

Die Dokumentation ist zweigeteilt. Dieser Teil enthält eine Beschreibung des Programs und einen Überblick über die Funktionsweise von DNS-Tunnel. Zur technischen Beschreibung des Programs siehe *Entwicklerdokumentation*.

Ein DNS Tunnel ermöglicht regulären IP Verkehr durch den Internet Namensauflösungsdienst DNS zu tunneln. Damit ist es möglich, in Netzen die keine normales Internet Routing unterstützen, Daten auszutauschen. Voraussetzung ist, dass das Netz gewöhnliche DNS-Auflösung unterstützt. Die Datenpakete werden in DNS-Anfragen kodiert, die durch die hierarchische Struktur an einen speziellen (i.d.R. third-level) Nameserver weitergeleitet werden.

Die Software [iodine] ist eine Implementierung eines DNS Tunnel für Linux, Mac OS X, FreeBSD, NetBSD, OpenBSD and Windows. Diese Dokumentation beschreibt die Portierung auf Android mit einer angepassten Benutzeroberfläche.

1 Android Systemanforderungen

Durch die Verwendung des Android VPN Framework ist mindestens Android 4.0 (API Level 14) erforderlich.

Für Android vor 4.0 besteht bei vorhandenem Root Zugriff die Möglichkeit das tun.ko Kernelmodul zu laden und ein cross-kompiliertes iodine auszuführen.

2 Funktionsweise eines DNS-Tunnel

Das Domain-Name-System (DNS) wird eingesetzt um Namen (wie "example.com") in IP-Adressen (wie "194.71.107.50" oder "2001:db8:85a3:8d3:1319:8a2e:370:7347") zu übersetzen. DNS wurde in den 1980er Jahren ursprünglich mit dem Ziel entwickelt lokale `hosts` Datei im Internet abzulösen. Inzwischen werden auch andere Informationen als die reine Adressauflösung über DNS ausgetauscht.

Als DNS Tunnel bezeichnet man eine Verbindung die in der Lage ist über das DNS Protokoll als Transportmedium generischen IP-Verkehr zu übertragen.

2.1 Einbetten von beliebigen Daten

Im folgenden ist der Datenverkehr zur Auflösung des Namens "bla.de" dekodiert dargestellt. Das erste Paket ist die Anfrage des A-Record zu "bla.de". Das zweite Paket die Antwort des DNS Relay.

Das DNS-Relay antwortet "bla.de A IN 217.160.95.28", diese Angabe soll "5 hours, 39 minutes, 47 seconds" gültig sein. `217.160.95.28` wurde direkt binär übertragen als `d9 a0 5f 1c`.

Nichts hält einen DNS Server davon ab andere Daten als IP-Adressen in der Antwort zu verschicken und nichts kann einen Client davon abhalten beliebige Daten in subdomains (hallowelt.bla.de) zu kodieren.

Aufgrund der hierarchischen Architektur von DNS kann der Inhaber einer Domains die Auflösung von Subdomains übernehmen. Nach RFC1035 ist die maximale Länge eines auflösbaren Namens 255 Zeichen.

```
Time         Source      Destination  Protocol Info
2.425301000  10.1.1.145  10.1.0.1     DNS      Standard query 0x5e9e A bla.de

Internet Protocol Version 4, Src: 10.1.1.145 (10.1.1.145), Dst: 10.1.0.1 (10.1.0.1)
User Datagram Protocol, Src Port: 52963 (52963), Dst Port: domain (53)
Domain Name System (query)
    [Response In: 16]
    Transaction ID: 0x5e9e
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        bla.de: type A, class IN
            Name: bla.de
            Type: A (Host address)
            Class: IN (0x0001)

0030  00 00 00 00 00 00 03 62 6c 61 02 64 65 00 00 01   .......bla.de...
0040  00 01                                             ..

Time         Source    Destination  Protocol Info
2.493068000  10.1.0.1  10.1.1.145   DNS      Standard query response 0x5e9e A 217.160.95.28

Internet Protocol Version 4, Src: 10.1.0.1 (10.1.0.1), Dst: 10.1.1.145 (10.1.1.145)
User Datagram Protocol, Src Port: domain (53), Dst Port: 52963 (52963)
Domain Name System (response)
```

```
    [Request In: 15]
    [Time: 0.067767000 seconds]
    Transaction ID: 0x5e9e
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    Queries
        bla.de: type A, class IN
            Name: bla.de
            Type: A (Host address)
            Class: IN (0x0001)
    Answers
        bla.de: type A, class IN, addr 217.160.95.28
            Name: bla.de
            Type: A (Host address)
            Class: IN (0x0001)
            Time to live: 5 hours, 39 minutes, 47 seconds
            Data length: 4
            Addr: 217.160.95.28 (217.160.95.28)

0030  00 01 00 00 00 00 03 62 6c 61 02 64 65 00 00 01   .......bla.de...
0040  00 01 c0 0c 00 01 00 01 00 00 4f a3 00 04 d9 a0   ..........O.....
0050  5f 1c                                            _.
```

2.2 Gegenmaßnahmen

Die von einem idealen DNS Tunnel gestellten Anfragen sind gültig und unterscheiden sich in erster Linie nicht von denen einer gewöhnlichen Anwendung von DNS. Um Tunnel aufzuspüren wären daher statistische Verfahren nötig die Kriterien wie Anzahl, Größe und Inhalt der Pakete betrachten. Aufgrund der Fehleranfälligkeit ist es damit aber auch möglich legitime Anwendungen zu blockieren.

Möchte man lediglich iodine als konkrete Implementierung blockieren ist dies sehr einfach möglich. Der vom iodine Client Verwendete "ping" Aufruf kann sehr einfach erkannt werden, es könnte jeder Client der regelmäßíg eine Subdomain mit dem Anfangsbuchstaben "p" der gleichen Restdomain erfragt geblockt werden.

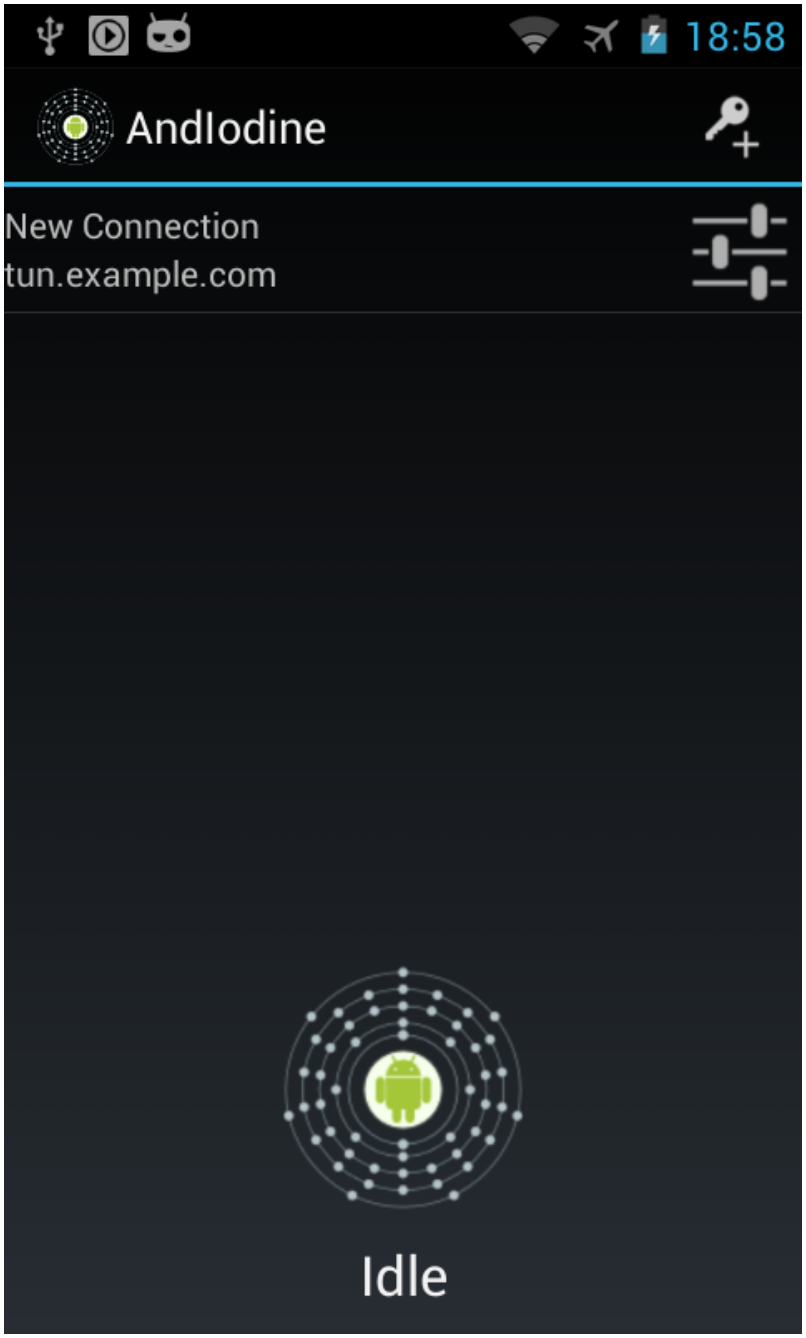
In einem durch Proxy Server sowieso schon stark eingeschränkten Netzwerk ist es denkbar, dass auf die Auflösung von Namen ausserhalb der lokalen Domain durch den DNS Server allgemein verzichtet wird. Sowohl ein HTTP-Proxyserver als auch ein SOCKS Server kann dies für den Client übernehmen.

In einer Konfiguration für einen Internet Hotspot mit Autorisation der Benutzer (z.B. nach Bezahlvorgang) ist es unbedingt sinnvoll die Autoriserungsregeln auch auf den DNS Server anzuwenden, sodass für den nicht autorisierten Benutzer nur das Loginformular aufrufbar ist. Dies in vielen öffentlichen Hotspots momentan nicht umgesetzt. Für weitere Informationen zum Blockieren von DNS Tunneln siehe [schillinger11].

3 Bedienung

Im folgenden wird die Bedienung der Android Oberfläche beschrieben. Die Anwendungen teilt sich für den Benutzer in zwei Bereiche: Die Steuerung der Tunnel und die Verbindungskonfiguration.

3.1 Hauptbildschirm

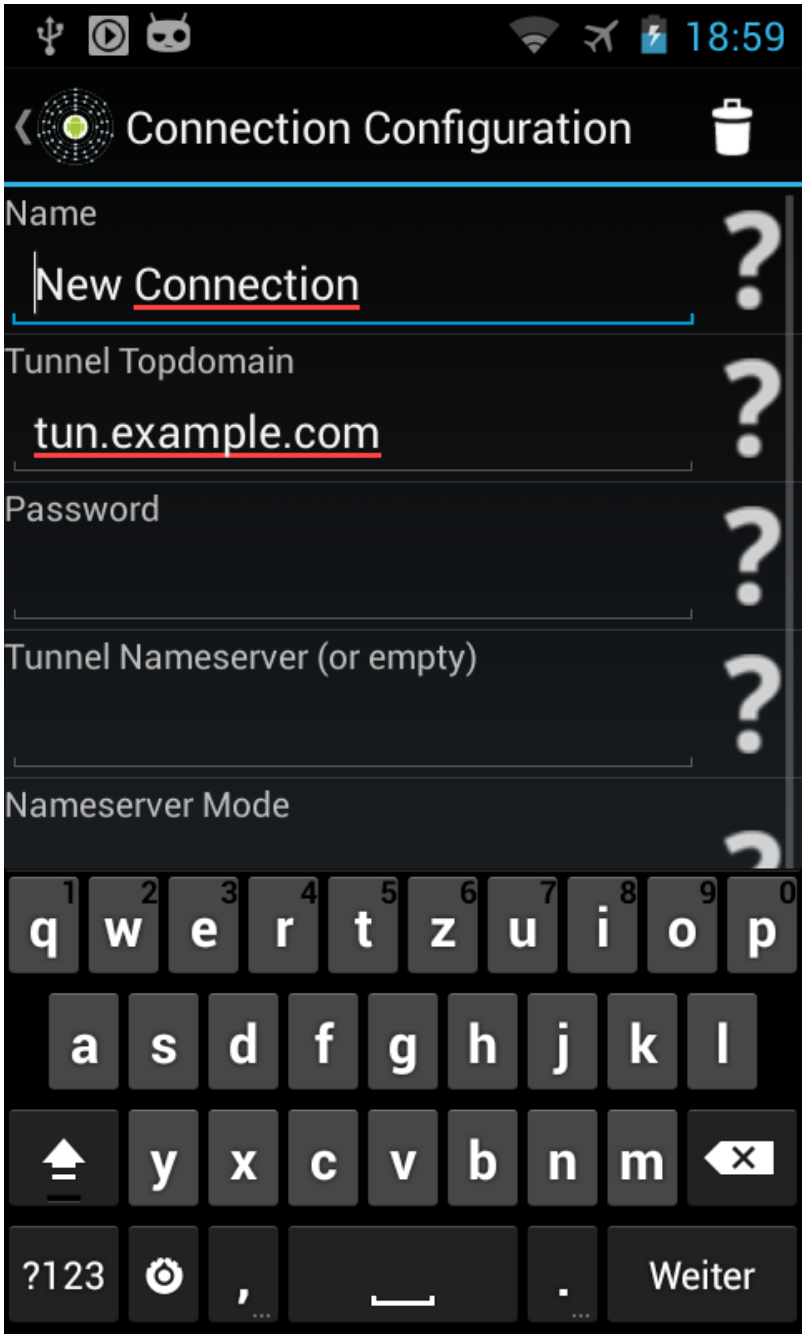


Der Hauptbildschirm zeigt die konfigurierten Verbindungsprofile. Eine Verbindung wird mit Auswahl des Eintrags gestartet.

Mit dem Einstellungsbutton  können die Verbindungsparameter geändert werden.

Mit dem Button  in der ActionBar wird ein neues Verbindungsprofil angelegt.

3.2 Verbindungskonfiguration



In der Verbindungskonfiguration werden Parameter festgelegt die beim Starten des Tunnels gesetzt werden. Die Änderungen werden sofort übernommen.

Zu jeder Einstellung kann mit Drücken des Hilfebuttons die Hilfe aus der Nachfolgenden Tabelle aufgerufen werden.

Mit mit der Auswahl von  wird die aktuell geöffnete Konfiguration gelöscht.

Tabelle 1: Parameter

Parameter	**Beschreibung**
Name	Name für diese Verbindungskonfiguration<

Tabelle 1: (continued)

Parameter	Beschreibung
Lazy-Mode	Lazy mode erhöht den Durchsatz und senkt die Reaktionszeit. Eine kleine Minderheit an DNS Relays scheint damit nicht klarzukommen was darin resultiert dass keine oder fast keine Daten übertragen werden. Der Client wird dies aber in der Regel feststellen und den Lazy mode ausschalten. Falls nicht, kann lazy-mode mit dieser Option ausgeschaltet werden.
Tunnel Nameserver	Der Nameserver/DNS Relay, der verwendet wird um mit iodined zu kommunizieren. Dieses Feld ist optional und wenn es nicht gesetzt ist wird der im System hinterlegte DNS Server verwendet
Nameserver-Mode	Legt fest wie der Nameserver gesetzt werden soll nachdem der Tunnel aufgebaut wurde
Nameserver	IP-Adresse eine speziellen Nameserver der gesetzt werden soll wenn Nameserver Modus = Custom ist.
Password	Dieses Feld ist optional. Es werden nur die ersten 32 Zeichen verwendet. pwasswo cont
Raw-Mode	Falls gesetzt wird iodine versuchen die öffentliche IP-Adresse des iodined Server aufzulösen und testen ob er direkt erreichbar ist. Falls ja, wird er den Traffic direkt an den Server senden anstatt an ein DNS relay
Request-Type	Typ der DNS Abfragen. Standardmäßig wird die beste Request type automatisch ausgewählt.
Top-Domain	Der DNS Traffic wird als Anfragen für subdomains unterhalb dieser Topdomain gesendert. Dies ist gewöhnlich eine Domain die Dir gehört. Verwende eine kurze Domain um mehr Durchsatz zu erzielen. Diese Einstellung muss am Server und am Client gleich sein
Default Route	Legt fest ob die Default Route gesetzt wird nachdem die Verbindung aufgebaut wurde

4 Einrichtung eines iodine Server

Vorraussetzung für den Betrieb eines Iodine Server ist eine öffentlich erreichbare IP-Adresse und ein freier Port 53/dns.

Es muss ein NS-Record für diese IP-Adresse eingerichtet werden. Angenommen die Tunnel Toplevel Domain soll "t.example.com" sein und der Server hat die IP-Adresse 192.0.43.10, dann lautet der Eintrag:

```
t.example.com.        8192    IN  NS    192.0.43.10
```

Die Konfiguration der IP-Adressen erfolgt nicht über DHCP oder statisch, sondern diese werden den Clients vom iodine Server, aus einem IP Subnetz das beim Start festgelegt wird, zugewiesen.

```
iodined -c -P PASSWORD 192.168.0.1/24 t.example.com
```

Die Option `-c` ist nicht immer erforderlich. Sie bewirkt, dass iodine die Quelladressen der Anfragen nicht überprüft. Die Überprüfung ist nicht möglich wenn die DNS Anfragen über ein Cluster verarbeitet werden, sodass die beim Server einkommenden Pakete von verschiedenen Quelladressen stammen.

Der Server legt ein TUN-Device an (typischerweise "dns0"), je nach Zweck ist noch das IP Routing/Masquerade zu konfigurieren.

4.1 Testen

Die Funktionstüchtigkeit eines iodine Server kann mit einfachen DNS Anfragen getestet werden:

```
$ dig -t A zabc.t.example.com
....
;; QUESTION SECTION:
;zabc.t.example.com.      IN  A

;; ANSWER SECTION:
zabc.t.example.com.   0 IN  CNAME hpjqweyzo.dh.

$ ./base32 d pjqweyz
Decoded 4 bytes:
0x7a (z) 0x61 (a) 0x62 (b) 0x63 (c)
```

Unter http://code.kryo.se/iodine/check-it/ wird ein Online Service zum Testen der Konfiguration angeboten.

5 Anhang

5.1 Literatur

[1] [schillinger11] Fabian Schillinger, DNS-Tunnel, Universität Freiburg 2011

[2] [iodine] http://code.kryo.se/iodine/