Sichere Dienste im Unternehmen mit Tor Hidden Services

Tor goes Business

René 'Lynx' Pfeiffer

Crowes Agency OG
https://www.crowes.eu/, rene@crowes.eu

Linuxwochen Wien
FH Technikum Wien, Wien, Österreich.

Table of Contents I

Table of Contents II

TOR? Tor!

Tor - Übersicht

- Kernprinzipien *onion routing* Mitte 1990er (US Naval Research Laboratory)
- Zweck: Anonymisierung
- α Version The Onion Routing (TOR) Projekt (20. September 2002)
- Tor: The Second-Generation Onion Router - vorgestellt 13. August 2004
- Tor ist Freie Software, daher wichtig für Nationale Sicherheit (siehe US Department of Homeland Security)
- Tor Clients für alle gängigen Plattformen

Tor Mythen und Fallstricke

- Tor schützt nicht automatisch vor allem - RTFM!
- Tor muß mit Verschlüsselung verwendet werden
- Tor schützt vor Traffic-Analyse, nicht vor Traffic-Korrelation
- Tor kann Client Fingerprinting nicht verhindern
  - **immer** den Tor Browser verwenden!
  - JavaScript, HTML5, Plugins sind Gefahren
- manche Protokolle verraten Client Adressen
- hiesige CryptoParty warnt gerne vor Risiken und Nebenwirkungen

Unwort der Dekade: Dark Web

- ☣Achtung! Cyber-/Bullshitwarnung! ☢
- *The dark web is the World Wide Web content that exists on darknets, overlay networks which use the public Internet but which require specific software, configurations or authorization to access.*
- Definition gilt für
  - Anonymisierungsnetzwerke
  - Behördennetzwerke
  - lokale Netzwerke, die per VPN verbunden sind
  - Unternehmensnetzwerke
  - . . .
- *Going dark* gilt nur für Stromausfälle

Wer verwendet Tor?

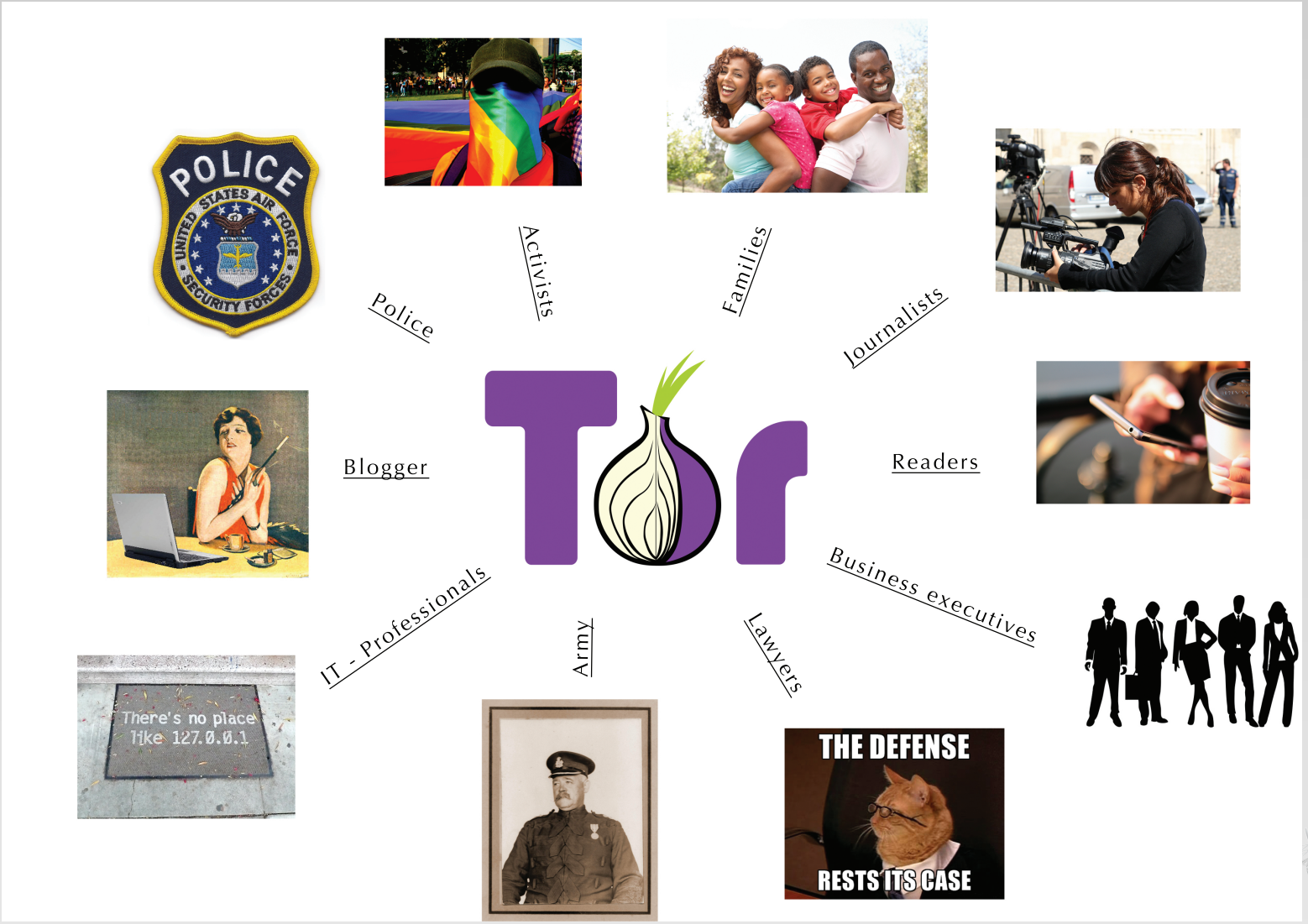


Table of Contents I

Table of Contents II

Tor im Unternehmen

Schutzbedarf

- Virtual Private Networks (VPN) / Verschlüsselung verbreitet
- Metadaten sehr verräterisch
  - Geolocation
  - Kommunikationspartner
  - „gesprächige“ Protokolle
  - Zeiten und Zeitzonen
  - DNS / URLs
- Tor Client(s) leicht zu verbreiten („deployen“)
- Wie ist es mit angebotenen Diensten?

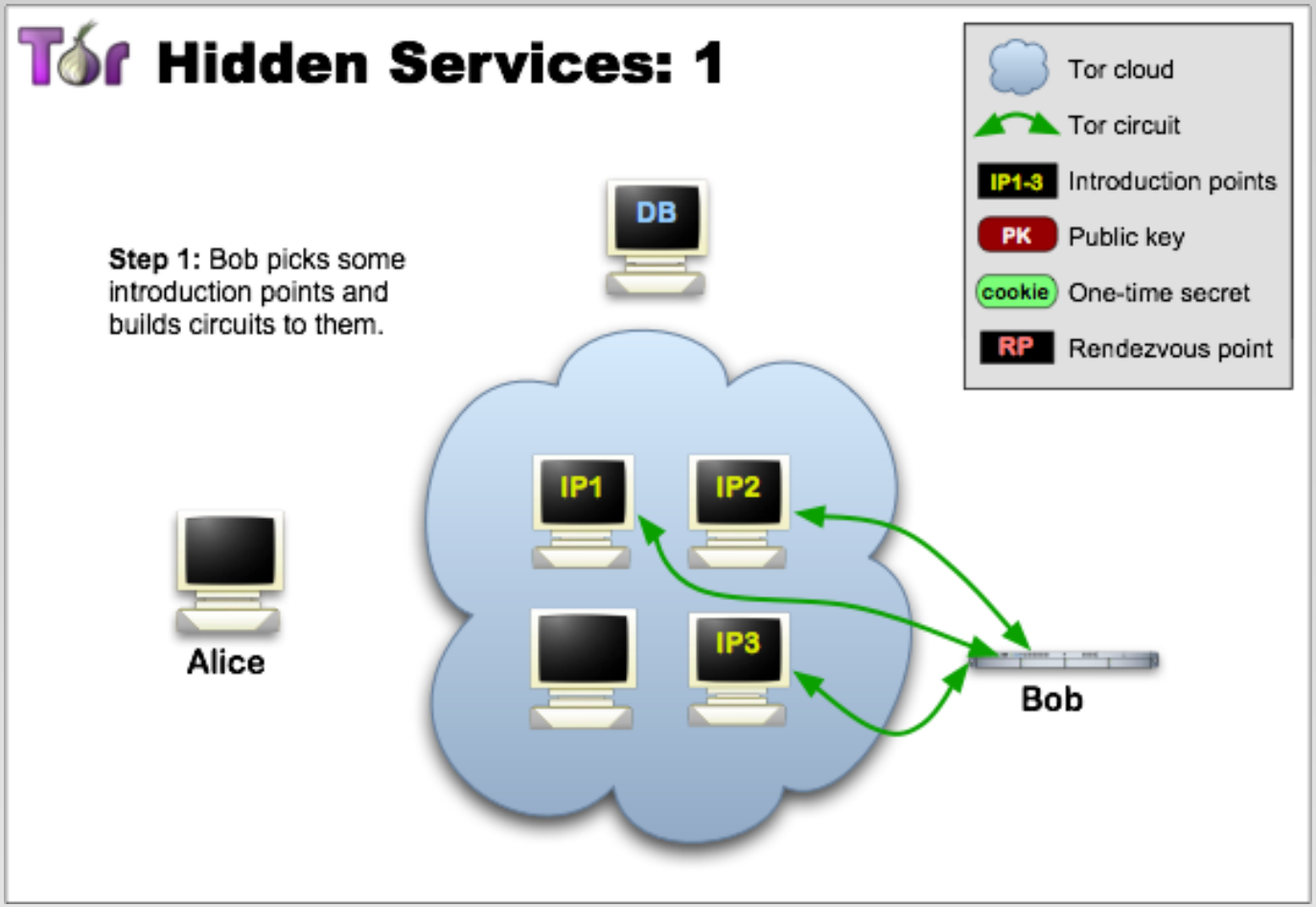
Tor Hidden Services

- Hidden Service - Server ist nur über Tor erreichbar
- Anonymisierung der Adresse (TCP/IP und Domain) - eigene *.onion* TLD
  z.B.: `http://auutwvpt2zktxwng.onion/`
- kein zentrales Verzeichnis der *.onion* Adressen
- Ressource ausschließlich über Tor erreichbar
  - *.onion* nicht im DNS
  - Aber: Server kann mehrere „Erreichbarkeiten“ haben
- Hidden Service hat eigenen Public Key
  - automatische Verschlüsselung bis zum Ende
  - zusätzliche Verschlüsselung möglich

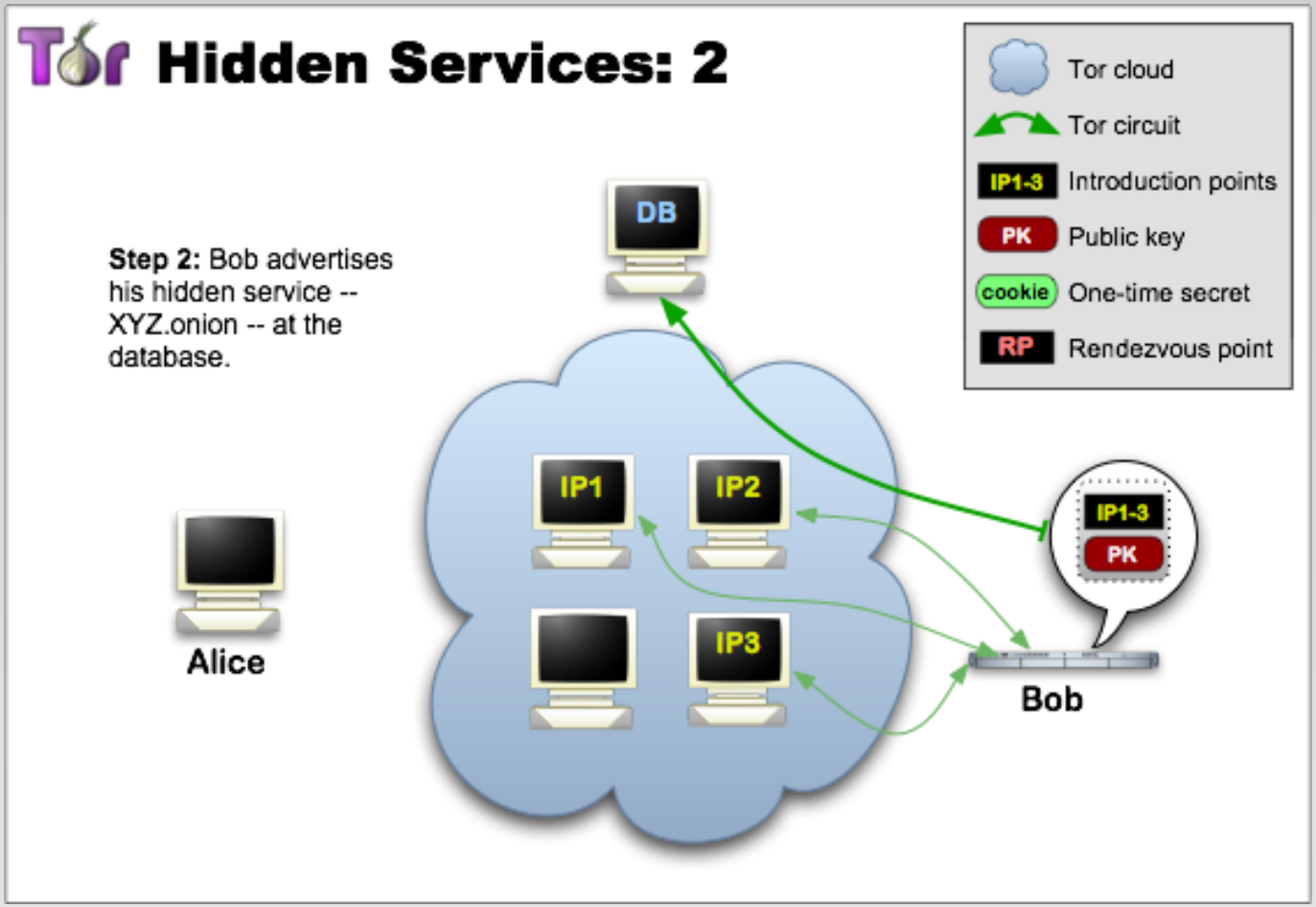
Konfiguration

- funktionierender Tor Client
- in `torrc` Konfiguration eintragen:
  ```
  HiddenServiceDir /var/lib/tor/ssh
  HiddenServicePort 22 127.0.0.1:22
  ```
- Tor Client neu starten
- im `HiddenServiceDir` finden sich Name und Public Key; beides sichern!
- *.onion* Adresse wird automatisch generiert

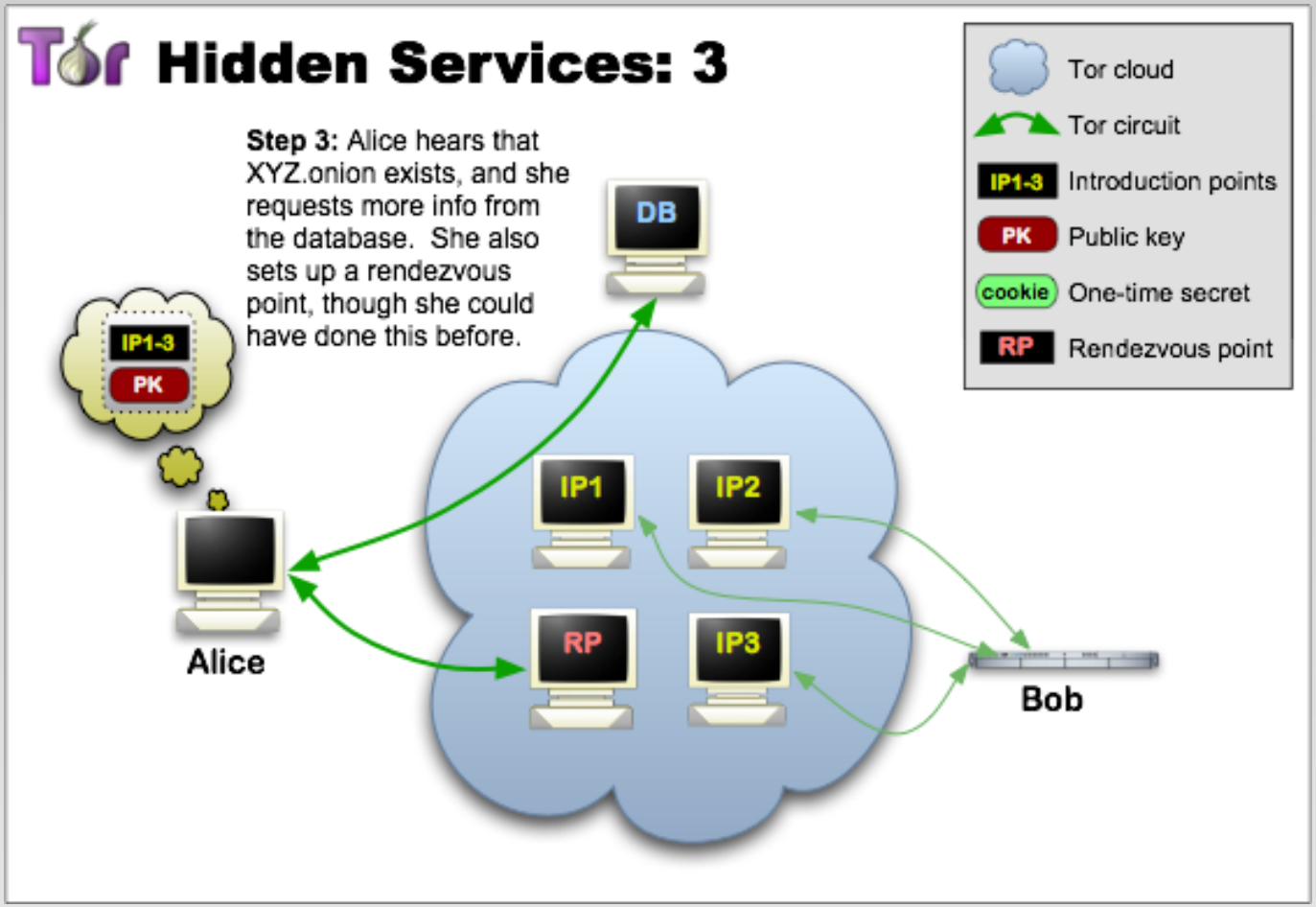
Hidden Service - Initialisierung



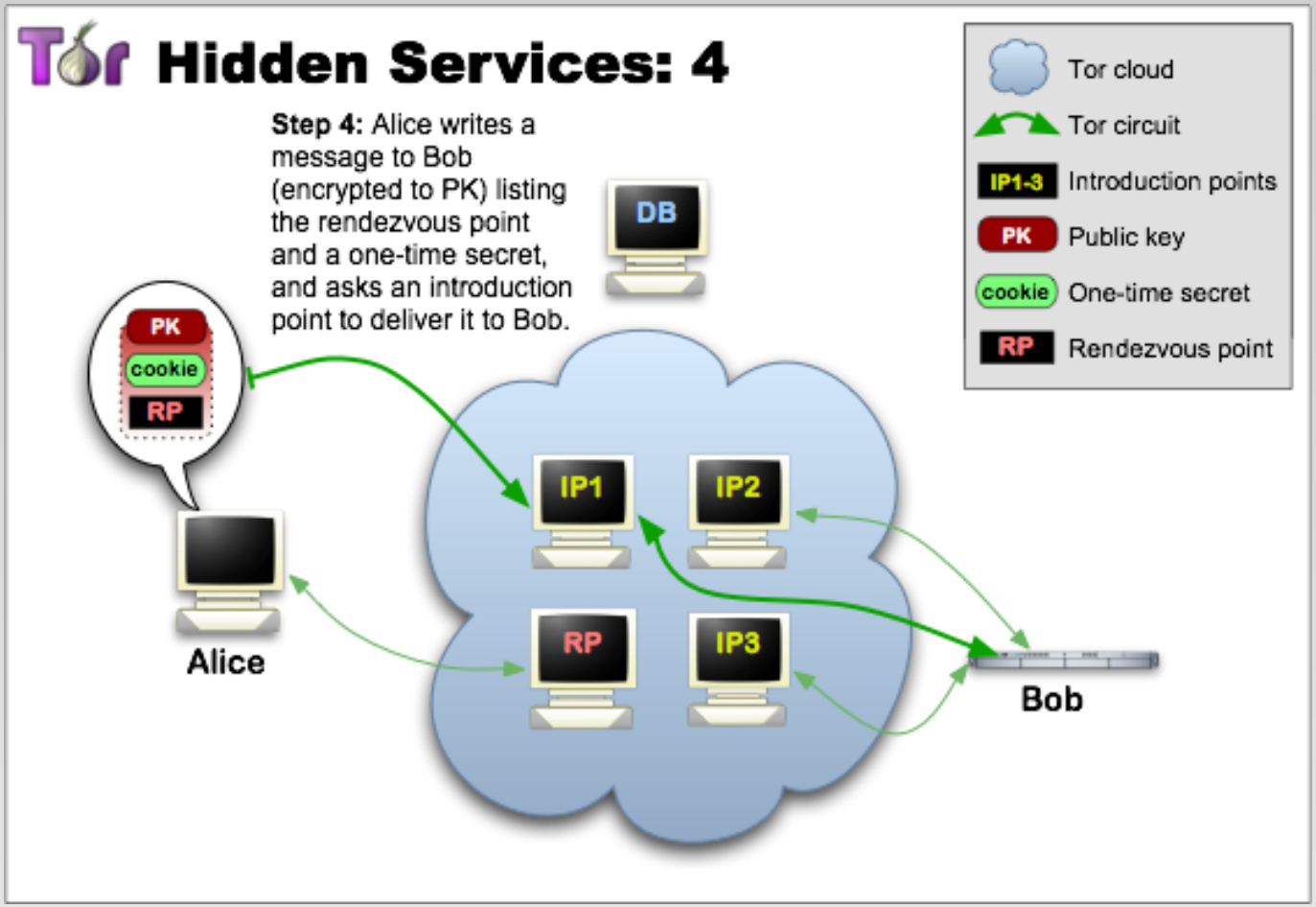
Hidden Service - Schlüsselgenerierung



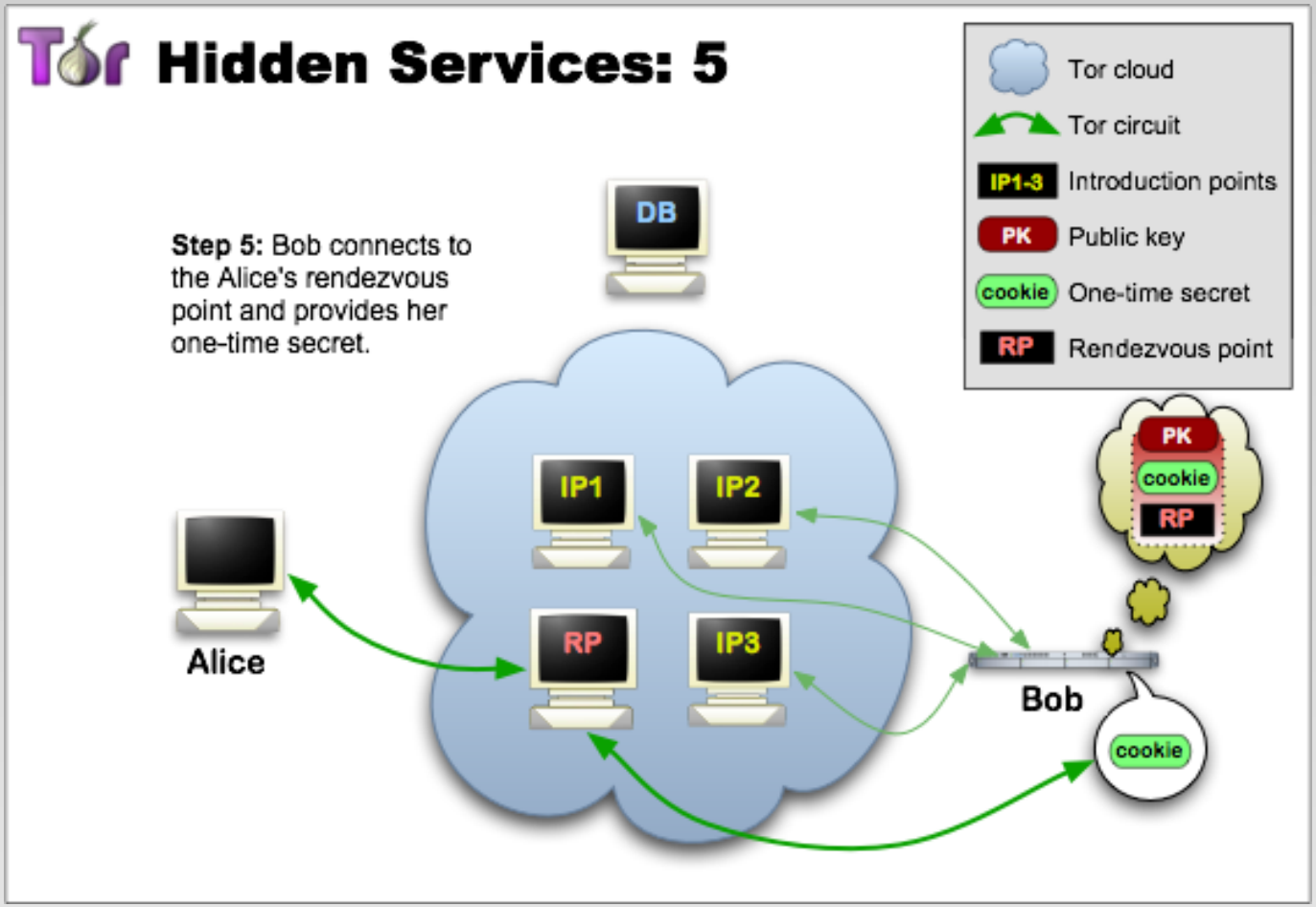
Hidden Service - Clientaufruf



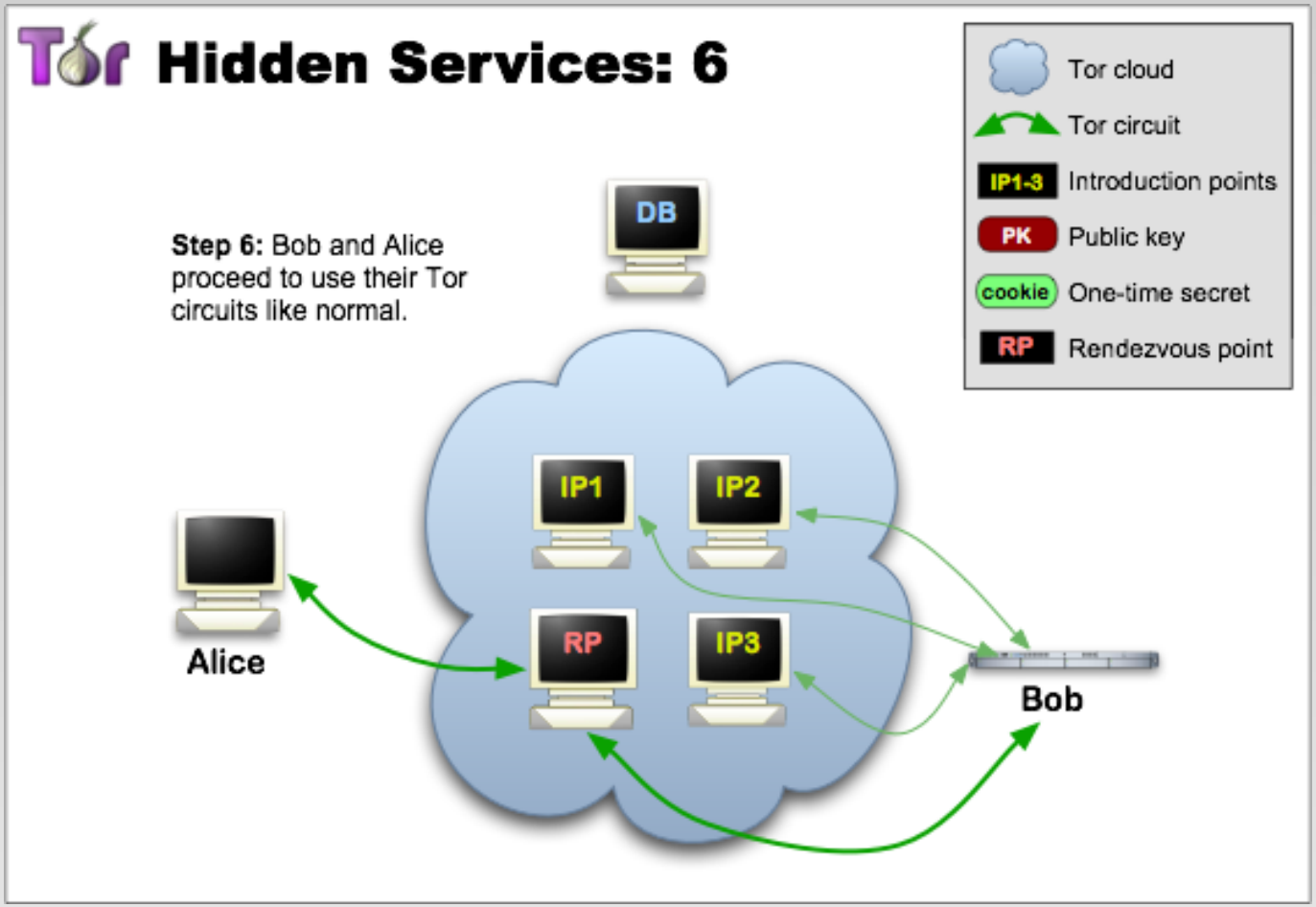
Hidden Service - OTP & Introduce



Hidden Service - OTP & Handshake



Hidden Service - RP bestätigt



Verbinden zu Hidden Services

- Browser verbunden mit Tor Client / Tor Browser
- SSH: `.ssh/config` ergänzen mit:

```
Host *.onion
Compression yes
Protocol 2
ProxyCommand connect -R remote -5 -S 127.0.0.1:9050 %h %p
```

- `connect` stammt aus `connect-proxy` Paket
- `torify` geht ebenso

Verbinden zu Hidden Services (2)

```
ssh -N -f -C -L 2501:127.0.0.1:25 abcdefghijklmnop.onion

torify openvpn --config tcpvpn.conf

torify mutt -f imap://abcdefghijklmnox.onion/

torify lynx http://abcdefghijklmnoy.onion/

torify telnet abcdefghijklmnoz.onion

torify irssi -c abcdefghijklmnzo.onion
```

Hidden Service Authentication

- Hidden Services lassen sich auf bekannte Clients einschränken
- Direktive für Server
  - `HiddenServiceAuthorizeClient basic alice,bob`
  - `HiddenServiceAuthorizeClient stealth alice,bob`

  in `hostname` finden sich dann Auth Cookies:

```
qfn6rcogpbfadrrr.onion pMaCvZ9O96oicewJOQIpdB # client: alice
vgfremmydldzgfld.onion f3cJeHARFIbGx+TX0itZex # client: bob
```

- Direktive für Client
  - `HidServAuth qfn6rcogpbfadrrr.onion pMaCvZ9O96oicewJOQIpdB` bzw.
  - `HidServAuth vgfremmydldzgfld.onion f3cJeHARFIbGx+TX0itZex`
- `stealth` Modus skaliert schlecht, minimale Aktivität

Pflege und Härtung

- Backups - Tor Config, Hostname & RSA Schlüssel
- nicht Hidden Service auf Relay aufsetzen (wegen Korrelation/Fingerprinting)
- Sockets statt TCP/IP:

  ```
  HiddenServicePort 80 unix:/etc/lighttpd/unix.sock
  ```

- ausgelieferte Informationen säubern
  - Banner
  - Inhalte (Bilder, CSS, HTML, . . .)
  - Protokollmetadaten (X.509 Informationen, Hostnamen, . . .)
- DNS Look-Ups des Hidden Service Servers beachten!

Onionscan

- `onionscan` untersucht (Web) Hidden Service auf Lecks
- Webscanner (Prototyp) sucht nach
  - Verzeichnislistings
  - Webserversignatur(en)
  - EXIF Daten in Bilddateien
- Tests auch mit „normalen“ Webscannern möglich
- Fokus auf Datenlecks zur Deanonymisierung

Table of Contents I

Table of Contents II

Zusammenfassung

- Tor gibt es für Clients und Server
- Hidden Services bieten
  - hohen Grad an Anonymisierung
  - verschlüsselte Kommunikation
  - Erreichbarkeit (auch in restriktiven Netzwerken)
- geeignet für alle TCP-basierten Protokolle (single stream)
- leicht zu implementieren, leicht zu migrieren
- Vorsicht vor Informationslecks!

Table of Contents I

Table of Contents II

Fragen?


466.100239] PAX: terminating task:
466.100243] PAX: bytes at PC: c3 00 00 00 00 00 00 00000000000400c90 0000000100000000
466.100245] PAX: bytes at SP-8: 0000000000400c90 0000000100000000
466.100256] PAX: bytes at SP-8: 000003da23831c38 0000000100000000
grsec: bruteforce prevention initiated for the next 30 minutes or until service
466.100265] grsec: bruteforce prevention initiated for the next 30 minutes or until service
crash report for /usr/lib/paxtest/execheap[execheap:4190] uid/euid:0/0 gid/egid:0/0, parent /usr/lib/paxtest
466.100276] grsec: more alerts, logging disabled for 10 seconds
466.100914] PAX: execution attempt in: <stack>, 39f1b2b8000-39f1b2da000 3fffffdd000
466.100916] PAX: terminating task: /usr/lib/paxtest/execstack(execstack):4193, uid/euid: 0/0, PC:
466.100918] PAX: bytes at PC: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
466.100927] PAX: bytes at SP-8: 0000000000000000 0000000000400b79 0000000000000000
466.101767] PAX: execution attempt in: /usr/lib/paxtest/shlibtest2.so, 3810d9a5000-3810d9a7000
466.101770] PAX: terminating task: /usr/lib/paxtest/shlibbss(shlibbss):4196, uid/euid: 0/0, PC:
466.101771] PAX: bytes at PC: c3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
466.101780] PAX: bytes at SP-8: 000003810ddc7538 0000000000400eef 0000000000400c9a
466.102654] PAX: execution attempt in: /usr/lib/paxtest/shlibtest2.so, 31f4606e000-31f46070000
466.102658] PAX: terminating task: /usr/lib/paxtest/shlibdata(shlibdata):4199, uid/euid: 0/0, PC:
466.102660] PAX: bytes at PC: c3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
466.102669] PAX: bytes at SP-8: 0000031f46490538 0000000000400eef 0000000000400c9a
466.103783] PAX: execution attempt in: <anonymous mapping>, 3a7da6f0000-3a7da6f1000 3a7da6f0000
466.103787] PAX: terminating task: /usr/lib/paxtest/mprotanon(mprotanon):4202, uid/euid: 0/0, PC:
466.103790] PAX: bytes at PC: c3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PAX: bytes at SP-8: 00000000000400a6a 0000000000400c70 0000000000000000
/usr/lib/paxtest/mprotbss, 00601000-00602000 00001000
/usr/lib/paxtest/mprotbss(mprotbss):4205, uid/euid: 0/0, PC:

Table of Contents I

Table of Contents II

Über die Crowes Agency OG

Die Crowes Agency OG ist eine Gruppe von Experten aus verschiedenen Feldern. Wir bieten unsere Erfahrungen im Rahmen von großen und kleinen Projekten an. Der Fokus liegt auf den Gebieten Grafikdesign, Software-Entwicklung, öffentlichen Erscheinungen (wie beispielsweise Webseiten und Kommunikation mit der „Außenwelt“), Systemadministration, IT Sicherheit und Unternehmensberatung. Die Crowes Agency stellt aus ihrem Pool von Mitarbeitern Teams für die Lösung von Kundenproblemen zusammen.

Kontakt Crowes Agency OG

- http://www.crowes.eu/
- Kontaktinformation des Autors
  - rene@crowes.eu
  - PGP/GPG 0x28CAC51F8C413583
  - +43.676.5626390 (Signal verfügbar)
  - +43.677.61356623 (unverschlüsselte Sprache & TextSecure verfügbar)
  - Threema ID 4WFYBWCJ
- E-Mail allgemeine Anfragen enquiry@crowes.eu