HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

Tunneling TCP over RDP

rdp2tcp

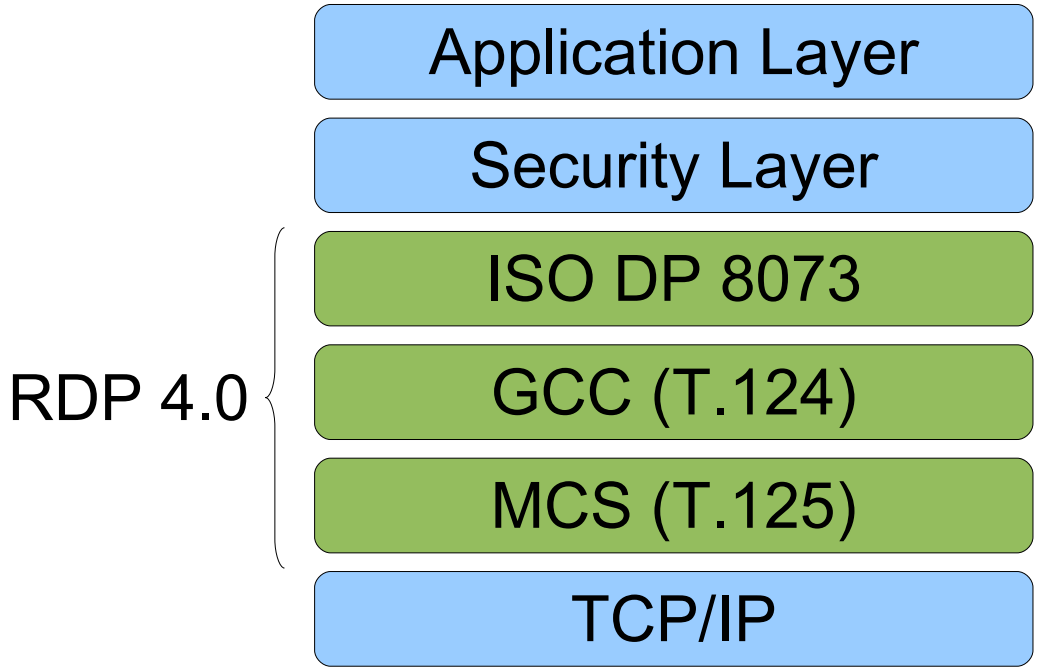
Nicolas Collignon
<Nicolas.Collignon@hsc.fr>

Why ?

- Pentesting Windows environment from Linux laptops
- 3389/TCP is the single open port
- DMZ network only accessible from the Terminal Server
- Attacks must be launched from the Terminal Server

RDP protocol history

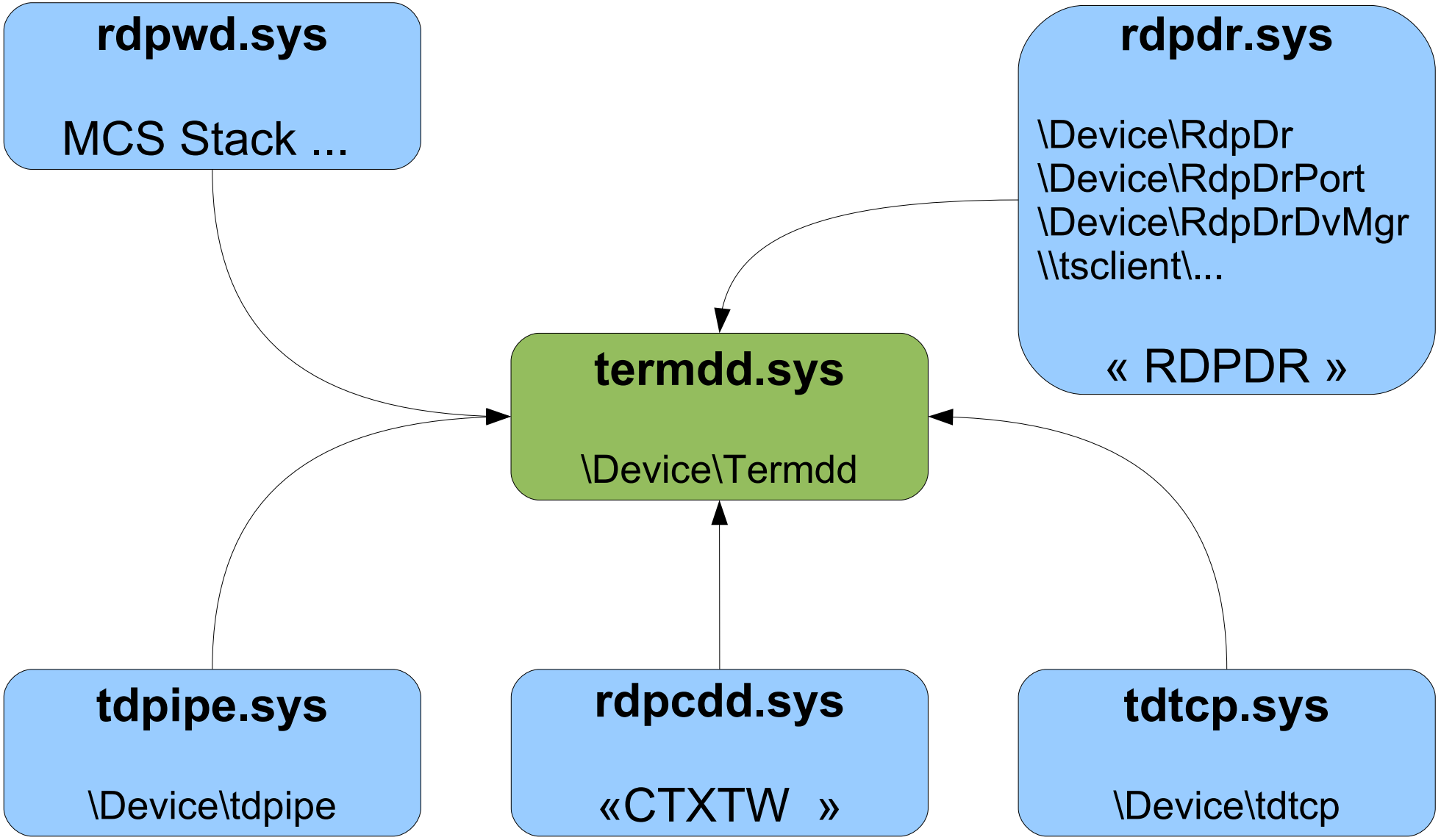
- RDP 4.0 Windows NT 4.0
- RDP 5.0 Windows 2000
- RDP 5.1 Windows XP
- RDP 5.2 Windows 2003
- RDP 6.0 Windows Vista
- RDP 6.1 Windows 2008
- RDP 7.0 Windows 2008R2
- RDP 7.1 Soon ...



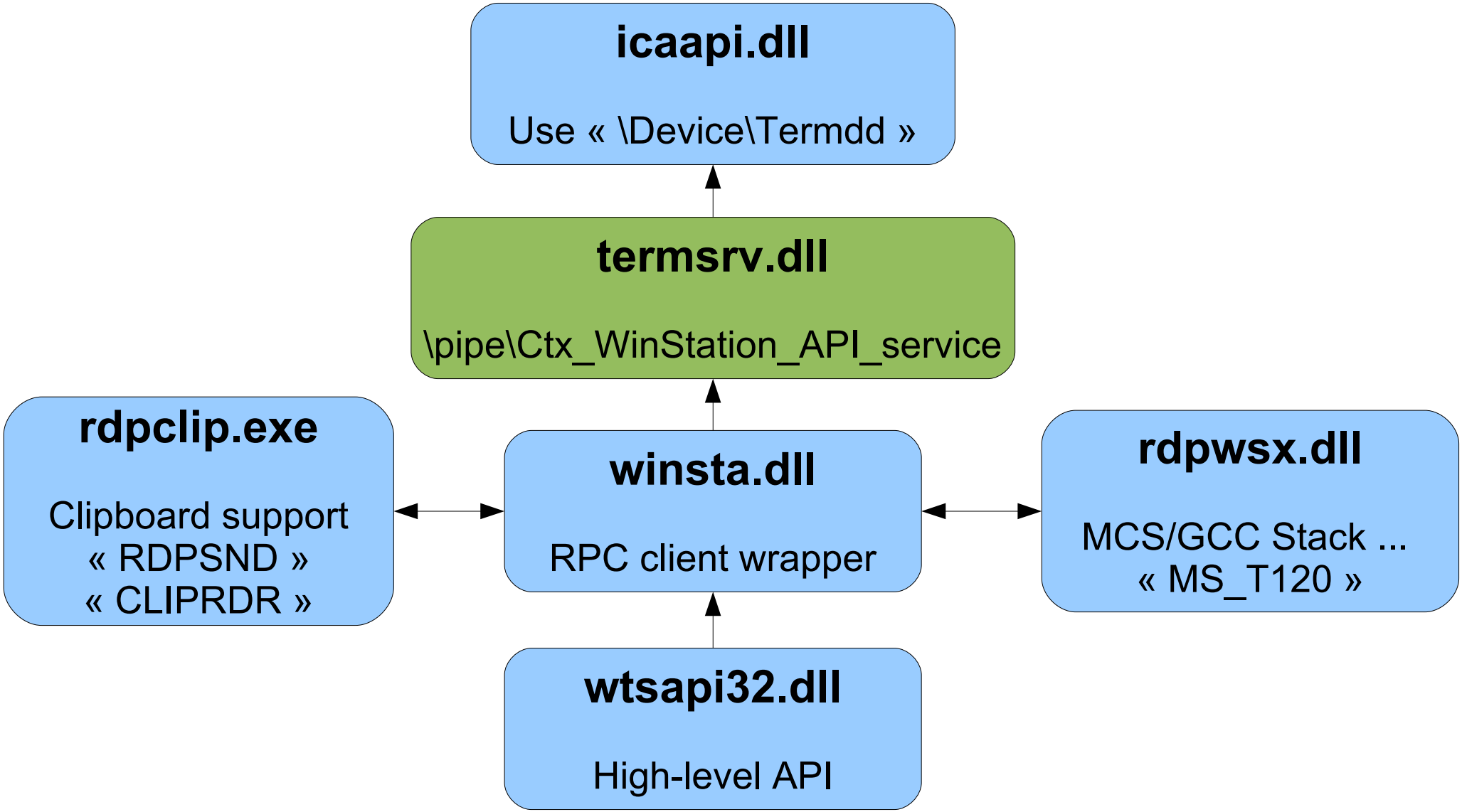
RDP protocol

- Extension of T.128 protocol
- Channels are multiplexed over a single TCP connection
  - rdpdr file sharing
  - cliprdr clipboard
  - rdpsnd sound
- Applications can dynamically register new channels
- Protocol security
  - Most information have already been said by Aurélien Bordes
  - http://www.ossir.org/paris/supports/2010/2010-07-13/CredSSP.pdf

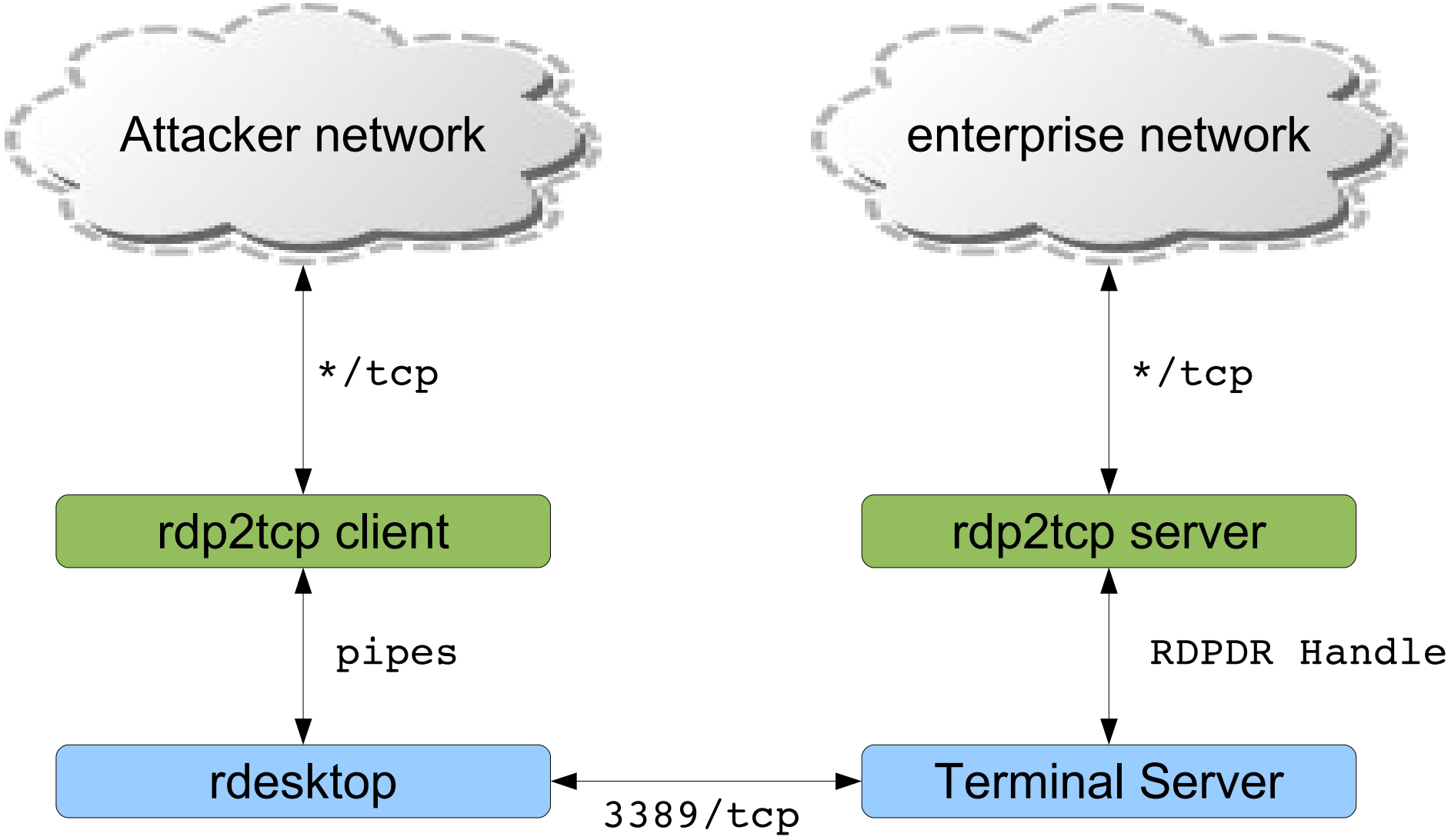
TS overview / Kernel-land



TS overview / User-land



Architecture



Client implementation

- Virtual channel implementation to be used with rdesktop client
- Need OOP rdesktop patch
- rdesktop -r addin:rdp2tcp:/usr/bin/rdp2tcp 192.168.0.2
- ~256 tunnels / rdp2tcp instance

Rdp2tcp server

- Executable must be uploaded on the TS host
  - SMB, file sharing, ...
- Run on more instances of rdp2tcp.exe within the RDP session
- WTSVirtualChannelOpen(“rdp2tcp”)

Tunnels management

- the rdp2tcp client has a controller listening locally
- basic telnet/netcat friendly ASCII protocol
  - “t 127.0.0.1 1234 192.168.0.56 445”
  - “r 127.0.0.1 9999 cmd.exe”
- Tunnels management tool provided

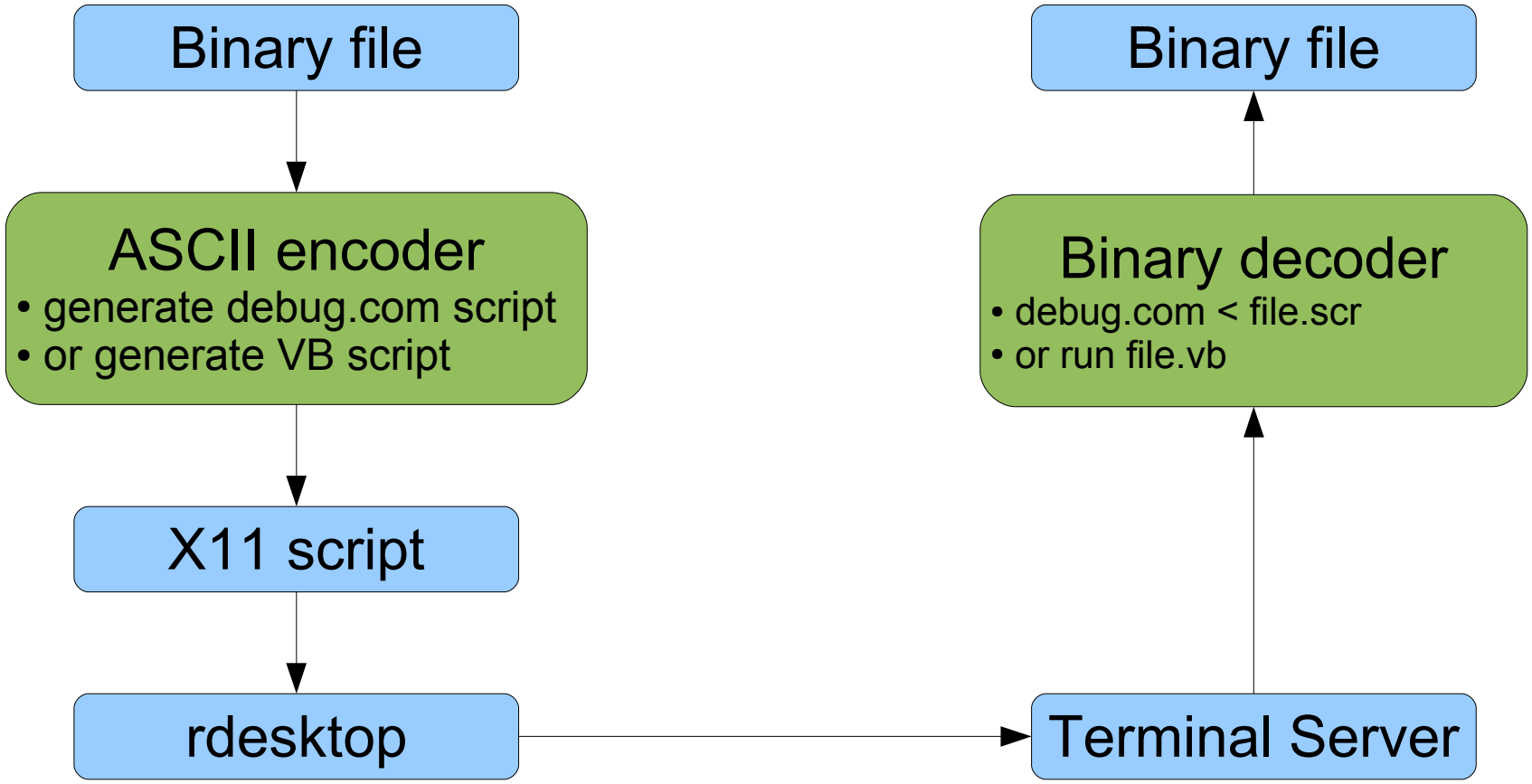
```
$ ./rdp2tcp.py info
ctrlsrv 127.0.0.1:8477
$ ./rdp2tcp.py add forward 127.0.0.1 1234 127.0.0.1 4567
tunnel [127.0.0.1]:1234 --> [127.0.0.1]:4567 registered
$ ./rdp2tcp.py info
ctrlsrv 127.0.0.1:8477
tunsrv  127.0.0.1:1234 127.0.0.1:4567
```

Fancy features

- Hacking Web app with Internet Explorer :(?
  - rdp2tcp SOCKS5 listener
  - configure your favorite browser
- Need to nmap from the Terminal Server ?
  - rdp2tcp SOCKS5 listener
  - use a SOCKS5 wrapper (proxychain, tsocks, …)
- Need a reverse shell after service exploitation
  - rdp2tcp forward tunnel to exploit the vulnerable service
  - rdp2tcp reverse connect tunnel to receive shell input/output

Bonus Track / rdpupload

- Terminal Server file sharing policy bypass
  - Need to upload a file on the server without file-sharing support



Ending

- Source code published on sourceforge
- Troubles with buggy Windows hacking tools disappeared :)

Questions ?