Linux a Vzdálená plocha

Ondřej Caletka
o.caletka@sh.cvut.cz
http://shell.sh.cvut.cz/~oskar

SUT SH

Vzdálená plocha

- Protokol X11
  - Nativní UNIXový
- Protokol VNC (RFB)
  - Nezávislý multiplatformní
- *Protokol RDP*
  - Nativní pro MS Windows
- Protokol NX
  - Optimalizovaný protokol X11

Proč vzdálenou plochu?

- Spousta administrativních činností v UNIXových OS nevyžaduje GUI
  - Musíme to ale umět :-)
- Střih videa na příkazovém řádku je utopií
- Tenký klient + tlustý server
  - Při dnešní ceně tenkých PC poněkud překonané
- Aplikační servery
  - Přesun kritických aplikací (např. e-mail klient) pryč z uživatelského (zavirovaného) PC
- Sdílení software, licencovaného na počítač
  - Pokud na takové jednání v EULA zapomněli :)

Rootless vs. Rootfull

- Rootfull
  - Připojujeme se k vzdálené ploše
  - Cílem je „akvárium“ s plochou vzdáleného PC
  - Jediná možnost pro protokol VNC, RDP (?)
- Rootless
  - Připojujeme se pouze k oknu dané aplikace
  - Okno získá dekoraci lokálního správce oken
  - Na první pohled nerozlišitelné od místní aplikace

Protokol X11

- První UNIXy – sériové textové terminály
- Později – telnet – převedení sériové linky na síťový soket
- X Window(!) System – grafická nastavba, síťově transparentní
- Model server – klient
  - Server na straně uživatele, poskytuje abstrakci displeje, klávesnice, myši pro další programy
  - Klient na straně počítače, prezentuje uživateli prostřednictvím X serveru výsledky své činnosti, obvykle uvnitř okna
- => Tenký klient = X Server

Protokol X11

- X klienti komunikují se servery:
  - UNIX socketem /tmp/.X11-unix/X<č. displeje>
  - TCP/IP socketem na portu 6000 + č. displeje
    - Bývá obvykle zakázáno v konfiguraci serveru
- Pro usnadnění rootfull režimu existuje XDMCP (X Display Manager Control Protocol)
  - X server při spuštění požádá DM (xdm, gdm, kdm), aby se k němu připojil a zobrazil na něm přihlašovací obrazovku
  - Používá se u tenkých klientů, kde server obvykle neví, kde všude tencí klienti jsou
- Pád spojení s X serverem téměř vždy vyvolá ukončení klienta

Protokol X11 – autorizace

- Spojení X11 protokolem je nešifrované.
- Je však zabezpečeno, aby se kterýkoli klient nemohl připojit kamkoli:
  - xhost – omezení na IP adresy (nebezpečné, použitelné jen pro debug)
  - xauth – autorizace pomocí cookie:
    - přenášeného v otevřené podobě – neochrání před sniffingem
    - vytvořeného programem startx, nebo ?dm
  - Autorizace pomocí DES, Kerberos,...
    - Na linuxu se obvykle nepoužívá
  - Autorizační cookies jsou uloženy v souboru ~/.Xauthority, spravují se příkazem xauth

Tunelování pomocí SSH

- Nejjednodušší vzdálené spuštění X11 aplikací na X11 klientovi
- Rootless:
  - ssh -X host
  - ssh -Y host
- Rootfull:
  - Xnest :1
  - DISPLAY=“:1“ ssh -X host
- Ruční tunelování
  - ssh -L <locport>:<remotehost>:<remoteport>
  - ssh -R <remoteport>:<localhost>:<localport>

Shrnutí protokolu X11

- Výhody:
  - Nativní propojení, jednoduché a rychlé
  - Přenášeny jsou grafické objekty
- Nevýhody:
  - Nutné velmi rychlé připojení s nízkou latencí
  - Při přerušení spojení se klienti ukončí
  - Obtížné (ne však nemožné) připojení z Windows
  - Slabé (žádné) zabezpečení před odposlechem
- Poznámky na okraj:
  - Aktuální verze Xorg mají vypnutou podporu Security Extensions, takže ssh -X nefunguje
  - Jak používat xauth se dočteme např. ve skriptu startx

Protokol VNC

- Open-source multiplatformní
- Přenáší bitmapy
  - Existují i KVM2VNC konvertory
- Pouze rootfull režim
- Jako jediný umožňuje sdílení plochy
- Mnoho různých mutací, obvykle ne zcela kompatibilních
  - RealVNC
  - TightVNC
  - UltraVNC (Windows)

VNC servery pro Linux

- Xvnc
  - X server, který má místo reálného displeje VNC klienta
  - Může pracovat ve spolupráci s (x)inetd jako multiplatformní náhrada XDMCP připojení
  - Uživatelsky spustitelný rodinou skriptů vncserver, vncpasswd,...
- x11vnc, VNC modul do Xorg
  - Zpřístupnění tradiční pracovní plochy VNC protokolem (stejně jako na Windows)
  - x11vnc je běžný X11 klient, který cyklicky vyčítá obsah X displeje a zároveň VNC server, kterým tento obsah zpřístupňuje
    - Funguje díky neexistující meziokenní ochraně v X

VNC – protokol RFB

- VNC používá, obdobně jako X11 číslované plochy. Komunikuje přes TCP/IP s číslem portu 5900 + <číslo displeje>
- Některé implementace mají navíc na portu 5800 + <číslo displeje> malý HTTPd server, který obsahuje VNC Viewer jako Java applet.
- Přenos není šifrován.
  - Nicméně se velice snadno tuneluje přes SSH – dokonce i z Windows
- Uživatel je autorizován osm znaků dlouhým heslem

VNC – shrnutí

- Výhody:
  - Jednoduchá instalace a použití i pro ne-roota
  - Funguje i na pomalejších linkách
  - Pracuje mezi různými platformami
  - Umožňuje sdílení jedné plochy více uživateli
  - Java klient
  - Přerušení spojení neukončí programy
    (grafická náhrada programu screen)
- Nevýhody:
  - Bitmapový přenos
  - Nelze Rootless
  - Nelze dynamicky měnit velikost plochy
  - Nešifrováno

RDP

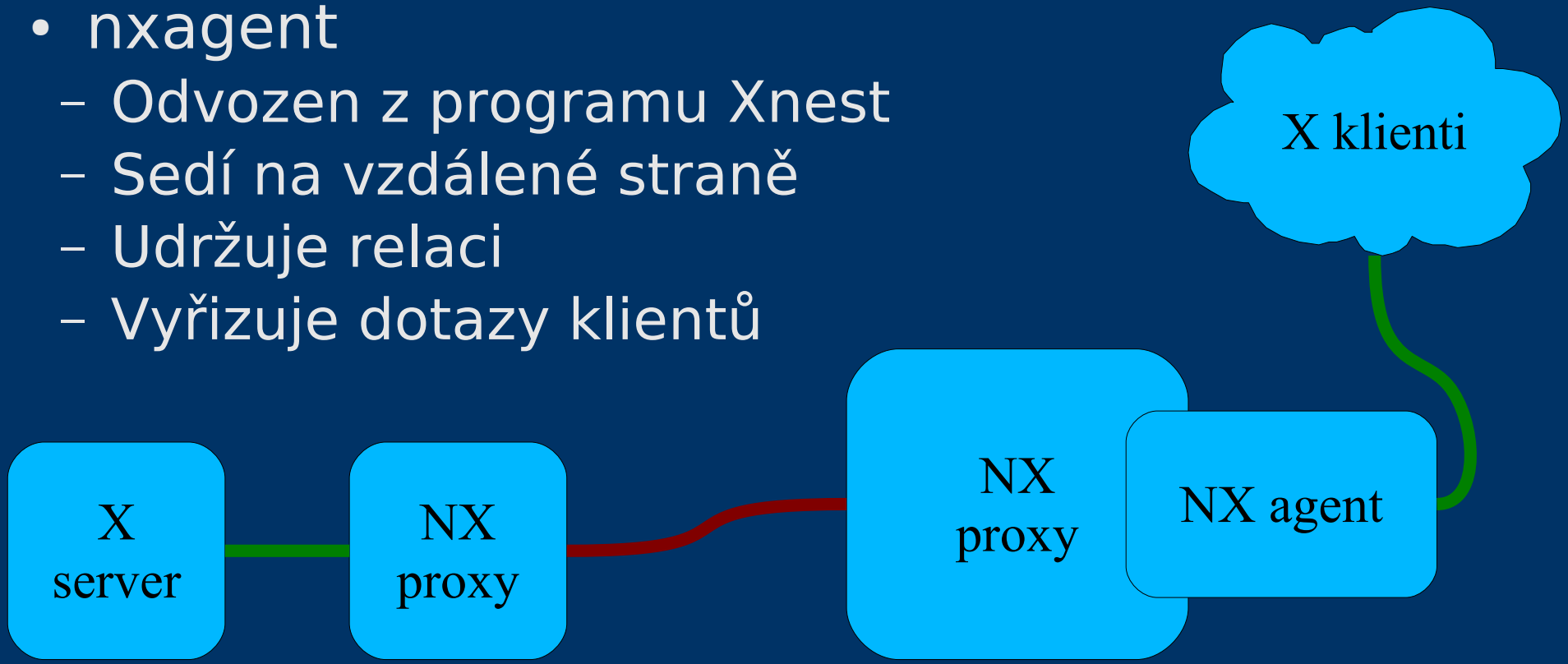
- Nativní protokol MS Windows
- Objektový přenos
- Přenos zvuku, disků, tiskáren
- Funguje i po pomalých linkách
- Klient pro linux: rdesktop
- Server pro linux: xrdp

NX (Nomachine's X)

- Vylepšený X11 systém od firmy Nomachine
- Cíle:
  - Zlepšit přenos X11 protokolu na pomalých linkách
  - Neztratit spuštěné programy přerušením spojení
  - Přidat podporu zvuku, sdílení, šifrování
- Klíčové komponenty jsou open-source (odvozeny od X11)
- Komerční nadstavba pro snadné nastavení a spuštění (existuje i freeware verze)

Klíčové komponenty NX

- nxproxy
  - Provádí inteligentní kompresi X11 protokolu
  - Cacheuje objekty
  - Sedí na straně klienta i serveru
- nxagent
  - Odvozen z programu Xnest
  - Sedí na vzdálené straně
  - Udržuje relaci
  - Vyřizuje dotazy klientů



Architektura NX server – klient

- Veškerá uživatelská nastavení se provádí v NX klientovi
- NX klient nejprve naváže SSH spojení na vzdálený stroj a uživatele nx. Tím spustí NX server.
- NX server je speciální „shell“
- NX server provede na příkaz klienta lokální SSH na požadovaného uživatele.
- Veškerá komunikace mezi klientem a serverem je by default slabě šifrovaná SSH tunelem
  - Slabě proto, že jsou použité klíče jsou známy

Shrnutí systému NX

- Výhody
  - Kombinace objektového a bitmapového přenosu
  - Vysoká účinnost komprese a cacheování
  - Rootfull i Rootless režim
  - Výpadek spojení nezavře programy
  - Šifrováno SSH tunelem (při použití vlastních klíčů velmi bezpečné)
  - Přenos zvuku, souborů
- Nevýhody
  - Closed-source

Vychytávka na závěr

- Programy X2X, X2VNC, WIN2VNC
  - Tzv. dual-screen hack
  - Ovládání dvou různých počítačů, jako by to byl jeden s více monitory
    - Přejetím přes okraj obrazovky se události klávesnice a myši začnou posílat druhému PC
  - Spouštění přes SSH tunel – například:

```
ssh -fY <druhyPC> x2x -to :0 -north
```

Závěr

- Děkuji za pozornost
- RTFM
- UTFG
- Přístí týden coreBoot
- EOF ❑