オープンソースカンファレンス 2018 Tokyo/Fall

xrdpの最新開発動向 ～2段階認証どうする？～

日本 xrdp ユーザ会 / xrdp project

xrdp v0.9.8 リリース

xrdp v0.9.8 のトピック

- 3ヶ月に1回 時期が来たらリリース
  - ないといえばない
  - リリース月 (3/6/9/12) なのでリリースした
- リリースを年に3回に変更することを検討中
  - 一時期ほど変更が活発でない
  - 4/8/12月
  - 最近ちょっと忙しい

xrdp v0.9.8 のトピック

- TLSv1.3 サポート
  - TLSv1, TLSv1.1 デフォルト無効化
- ドライブ転送のアンマウントバグ修正
- PulseAudioモジュールの分離
- 細かな修正

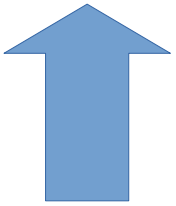
TLSv1.3 サポート

- OpenSSL 1.1.1 のリリースによる
- xrdp が TLSv1.3 をサポートする OpenSSL とコンパイルされていれば使用可能

```
xrdp 0.9.8
  A Remote Desktop Protocol Server.
  Copyright (C) 2004-2018 Jay Sorg, Neutrino Labs, and all contributors.
  See https://github.com/neutrinolabs/xrdp for more information.

  (snip)

  Compiled with OpenSSL 1.1.0i  14 Aug 2018
```



TLSv1.3 サポート

- 実は何も手を加えなくても OpenSSL 1.1.1 とコンパイルされていれば TLSv1.3 は使用可能
- そのままでは無効化ができない

  tls_ciphers=TLSv1,2 TLSv1.3 と書けば有効

  tls_ciphers=TLSv1.2 と書けば無効
- この部分を今回のリリースで実装した

xrdp の TLS ライブラリ対応

- OpenSSL / LibreSSL の両方をサポート
- 両者は基本的には互換性があるため互換性頼み
- LibreSSL が TLSv1.3 をサポートすれば
  xrdp 側では特に何もしなくてもよい

TLSv1.3 サポート (クライアント)

- OSSの場合はTLS部分をOpenSSLなどの外部ライブラリにまかせていることが多い
- FreeRDPの場合は OpenSSL 1.1.1 とコンパイルすればTLSv1.3が使用可能
  - xrdp – FreeRDP の組み合わせでテスト
  - TLSv1.3 with cipher TLS_AES_256_GCM_SHA384
- Windowsは2018年9月末時点のInsider PreviewではTLSv1.2が最高

TLSv1, TLSv1.1 の無効化

- 最近のHTTPSの傾向を見て決定
- デフォルト設定が変わっただけで設定ファイルの編集でいつでも再度有効化できる
- tls_ciphers=TLSv1, TLSv1.1
- お好みで設定してください

PulseAudioのモジュール分離

- オーディオ転送で使用
- PulseAudioとxrdpの橋渡しをするための
  モジュール
- 原理的にxrdpの一部ではない
- 別パッケージで提供するのが自然
- 分離して管理＆コンパイルしやすくした
- 詳しくはリポジトリで
  https://github.com/neutrinolabs/pulseaudio-module-xrdp

ビルド方法

- 手でビルドする手順はREADMEに書いてある
- CIでDockerを使用してテストビルド
  - .travis.yml を参照
  - Ubuntu 18.04 / CentOS 7 ではDockerでビルド可

ここから2段階認証の話

おことわり

- 定義については勘弁してください

  (2|Multi)-(Step|Factor)

  (Authentication|Verification)
- 認証なのか検証なのか
- 段階なのか要素なのか
- ここでは(H|T)OTPのことを指すことにします

SSHでの2段階認証

- Google の提供するPAMモジュールで実現可
  - google-authenticator-libpam
- 設定方法など情報は多数あり
- PAMモジュールなので

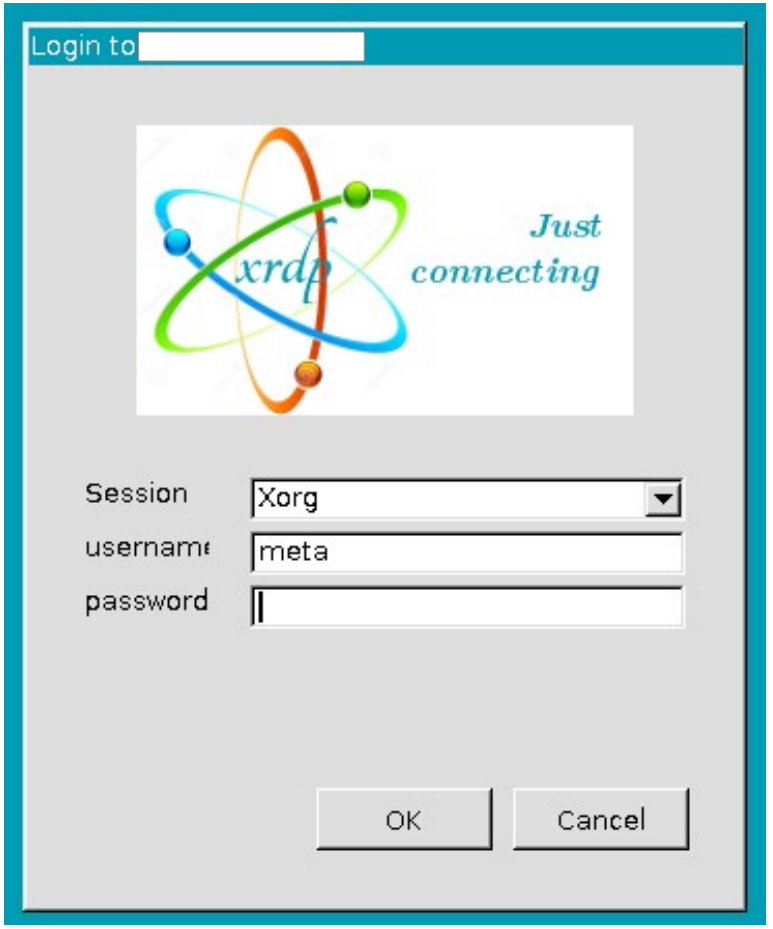
xrdpでの2段階認証

- 通常はユーザ名とパスワードで認証
- xrdp と xrdp-sesman という要素に分かれる
  - xrdp が通信担当
  - xrdp-sesman が認証担当
- xrdp 固有の事情
  - あくまでも RDP のオープンソース実装
  - Microsoft のプロトコルに縛られるので勝手に拡張できない

xrdpでの2段階認証

- OTPをどこで入力するか
- パスワードとOTPは同時に検証しないと
  セキュリティが低下する
  - ブルートフォース攻撃を可能にしてしまう
- ユーザ名とパスワードを入力した後に別画面でOTP
  を入力するような実装はNG
  - パスワードが間違っていてもOTPを要求すべき
  - AWSコンソールのログインページはこれ

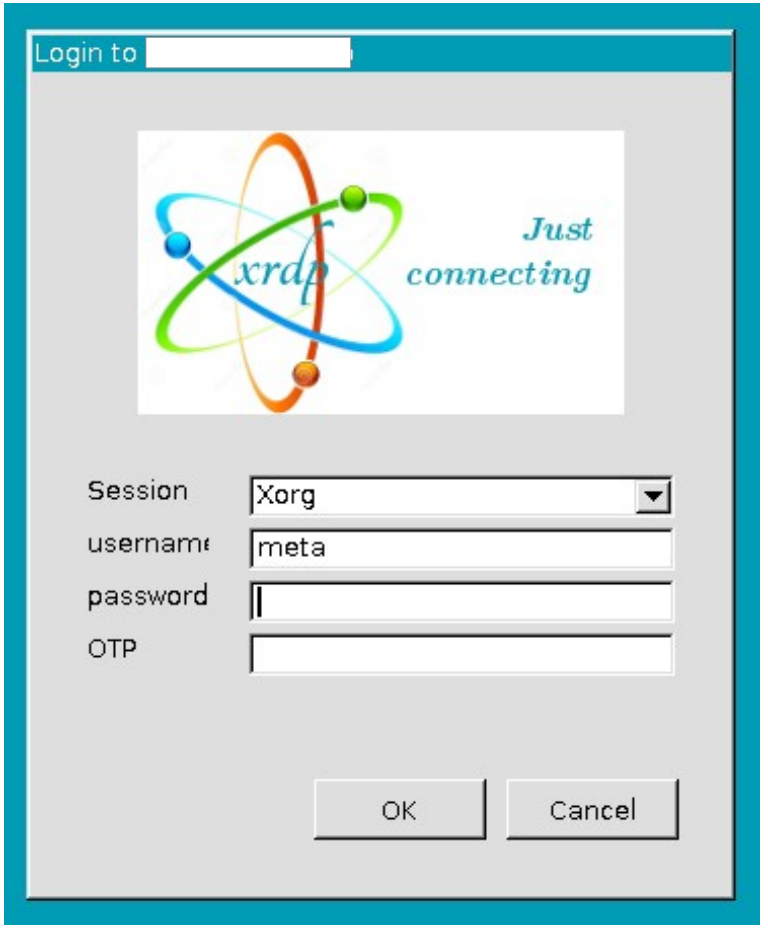
xrdp のログイン画面



↑こっちは弄れない

xrdp のログイン画面

- こっち側はフィールドを増やせる
- クライアント側はRDPに縛られる
- プロトコル上OTPを渡すためのフィールドがない



Google Authenticator PAM

- SSHのように入力フォームを柔軟に変えられるものばかりではない
- 当然それを想定した機能がある
  - パスワード入力フォームにパスワードに続けて認証コードを入力することで、認証コード入力欄がなくてもOK
- これを利用してxrdpで二段階認証できる

xrdpで二段階認証をするには

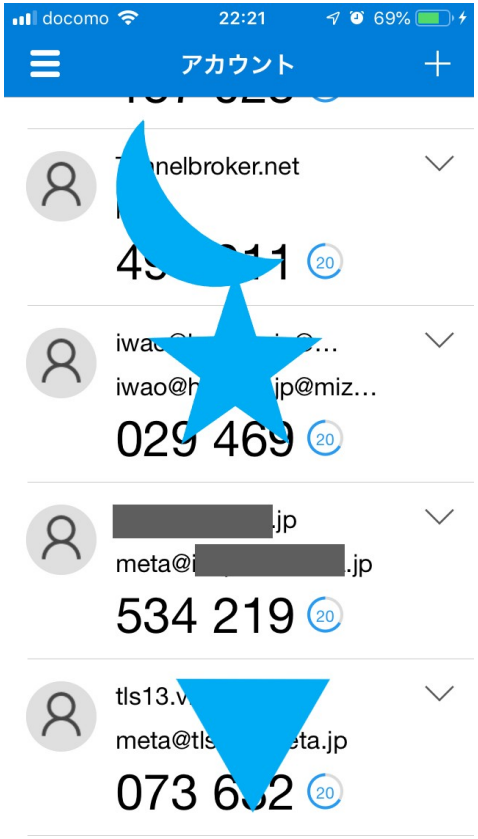
G/Authenticator インストール

- google-authenticator-pam をインストール
  - インストール方法は省略します
  - パッケージでもOK (古いかもしれない)
  - 今回は 1.05 を使用
- デバイス側にも認証アプリをインストール
  - ブラウザのアドオンでも
  - スマートフォンアプリでも
  - なんでもOK お好みで

G/Authenticator 初期設定

$ google-authenticator

(質問に答えてQRコードを読み取る)



アプリ上に6桁の認証コードが表示されたら成功

このコードを認証時に入力する

PAMの設定 (pam.d/xrdp-sesman)

UNIXのローカルユーザで認証する場合は以下のように修正
(auth セクションのみ抜粋)

auth required pam_google_authenticator.so
nullok forward_pass ⏎

auth requried pam_unix.so no_warn use_first_pass ⏎

session, account セクションはそのまま

PAMの設定

- nullok
  - 空パスワードを許可する
  - 二段階認証が未設定のユーザでも認証するため
- forward_pass
  - 次のモジュールにパスワードを渡す
  - 認証コードを取り除いた文字列でUNIX認証する

二段階認証でログイン

- パスワードに続けて6桁の認証コードを入力
  - パスワード: pAsswORd
  - 認証コード: 930444
- 認証時のパスワードに以下を入力
  - pAsswORd93044
- ひとつ弱点がある
  - 認証情報を記憶できない
  - フィールドが別々でないため

ユーザ名とパスワードを記憶させて
認証コードだけ手入力することはできない

デモします
(環境が許せば)

それ以外の開発の話

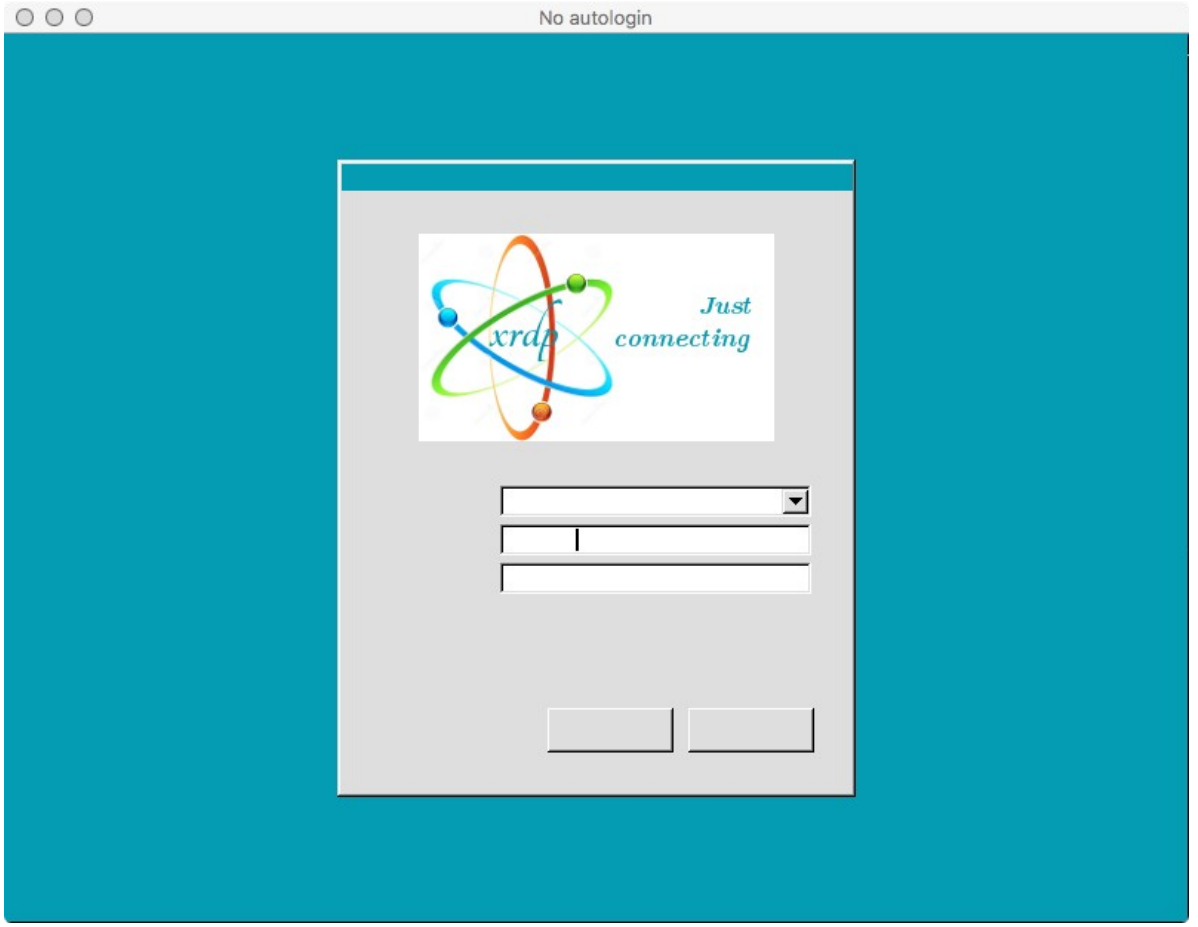
v0.9.9 に向けて開発中の機能

- 無操作の場合にセッションを切断する機能
  - スポンサーがついたので開発中
- セッション管理系の機能は2つ
  - 切断されたセッションを一定時間後に終了
  - 一定時間無操作の場合に切断する
- 大きな問題がなければ v0.9.9 に含まれる予定

v0.9.9 に向けて開発中の機能

- 動的セッションリサイズ機能
  - 現在はセッション接続のタイミングのみ
  - Windows 8.1 から登場した機能
  - FreeRDP は 2.0-rc2 で対応 #4265
  - 仕様は MS-RDPEDISP で公開されている
- 間に合えば12月のリリースに含めます

一部クライアントで文字が出ない



一部クライアントで文字が出ない

- Mac, iOS, Android のMS純正クライアント
- ログイン画面の文字が出ないという問題
- neutrinolabs/xrdp#1235 で修正
- Glyph Cache v2 に対応
- テストしたところよさそう
- マージして v0.9.9 に含める予定

ちゃんと表示されるようになった