About Me

I work as an independent consultant performing system and small network administration, and writing specialized technical documentation.

I have been responsible for implementing the use of KeePass at a client site.
What's The Problem?

• Too many usernames and passwords

• Passwords are weak in order to be memorable

• Passwords are written down in order to be strong
What is KeePassX

- KeePassX is a password manager that stores usernames, passwords, and related information under strong encryption and provides auto-type form fill-in support.

- Remember 1 strong password; KeePassX remembers everything else.
Features

• Username/Password pairs searchable, organized by groups

• AES (Rijndael) 256-bit encryption

• Hotkey auto-type support
How to get it

• 'Classic'
• [https://www.keepassx.org/downloads](https://www.keepassx.org/downloads) (v0.4.3)
• In your distribution?

• 2.0 Alpha 6
• [https://github.com/keepassx/keepassx](https://github.com/keepassx/keepassx) (latest)
• Daily build PPA: ppa:keepassx/daily (latest)
Configuration

• Add the groups you want
• Set the 'auto-type' shortcut
• Ask before auto-type?
• Set password generator defaults – 20 characters, exclude look-alike characters
Migration

● Use your browser's list of saved passwords

● Use your browser's list of 'never save' sites

● Still lots of work
Demo!
Advanced Issues
Other Platforms – KeePass

- Windows
- Android
- Others
Small Business Applications

- Vs. single sign-on
- Use template, pre-filled .kdbx file
- Pre-set password generator defaults
KeePassX

SLUUG – April 2019

KeePassX; 10 June 2015, SLUUG; Ken Johnson (contact-point@pobox.com)