Projects on the Move

Crabgrass sets out to do battle with Facebook and company with a simple approach to founding subversive social networks, and Clipperz manages the passwords you need for them. *By Mela Eckenfels*

The whole Internet has been conquered by Facebook. The whole Internet? No, a small village populated by hardy programmers is still holding out against controlled, "social" networks and fighting to regain privacy. Their secret weapon goes by the name of Crabgrass [1].

Crabgrass is a hard and tough type of grass that constantly gives gardeners headaches. It invades tidy lawns and ousts cultivated plants. The only way to get rid of it is to use pesticides, so it's not a bad choice of name for the project, which was founded in 2009.

Just as crabgrass invades lawns, initiatives that use Crabgrass as a management tool seek to penetrate the Web 2.0 gardens of those social networks that play a leading role in the way people relax and work together. Students communicate through Facebook [2], flash mobs organize via Twitter [3], and invitations to the office party are sent via Xing [4].

All of these activities blissfully ignore the fact that today's social networks are insecure. Providers not only rework – and possibly worsen – their privacy settings every couple of weeks, but also nobody really knows whether the data still belong to the users or whether the service will still be online in a couple of months.

Anything Facebook Can Do …

… we can do better, is probably what the Crabgrass developers were thinking when they began the project. And, although that sounds very ambitious, the project isn't too far from achieving it in real life. The system, built with Ruby on Rails, has everything the Web 2.0 heart could desire, providing tools for networking, organization, and collaboration.

Crabgrass reveals its strengths when you look at the add-on features. Under the hood are numerous groupware tools – for example, an integrated wiki (see Figure 1); discussion forums; task management for individuals, groups, and subgroups; a voting platform; and a lean but very useful document management tool. The list goes on and on and includes task lists, blogging, image galleries, private chats, and much more.

In a future version, the developers are planning to add calendar management – a function that the program urgently needs. In contrast to most groupware suites, Crabgrass manages to provide intuitive controls. In fact, Crabgrass is neither a classic groupware tool nor just a social network. I would probably call it "Social Groupware."

Pesky Management

What Crabgrass gains on the user control swings it loses on the administrative roundabout. Administration takes some getting used to in Crabgrass, and documentation for the installation procedure is anything but complete. If you decide to run the software on anything other than Debian, you will need to plan enough time to fix the problems you are likely to encounter. If you are interested in contributing to the Crabgrass how-to, the *Documentation* section on the project website tells you how.

Although Crabgrass is highly unlikely to replace Facebook and company, it does give small to medium-sized organizations the ability to keep control of internal communications and protect their own members' privacy and data.

Login Credentials in the Cloud

Talking of social networks, I regularly find invitations to join up in my mailbox – a colleague entices me to join LinkedIn [5], my best friends are on Facebook, and nearly all of my family uses the "Wer-kennt-wen" (Who knows whom?) platform [6]. Typically, common sense wins, and I avoid getting involved in yet another time killer.

However, I have my weak moments too, and before you can count to 10, I have yet another account, with my tried-and-trusted, easily memorized password that I probably use to "protect" other accounts and web applications. Although multiple passwords would be ideal, even the best geek memory gives in at some stage, when faced with a flood of PINs, PUKs, and TANs. Instead of choosing between the frying pan (a handful of simple passwords for multiple logins) and the fire (jotting down your passwords on sticky notes) or the geek version of hell (regular, unencrypted mail with forgotten passwords), a password safe gives you an infinitely preferable alternative.

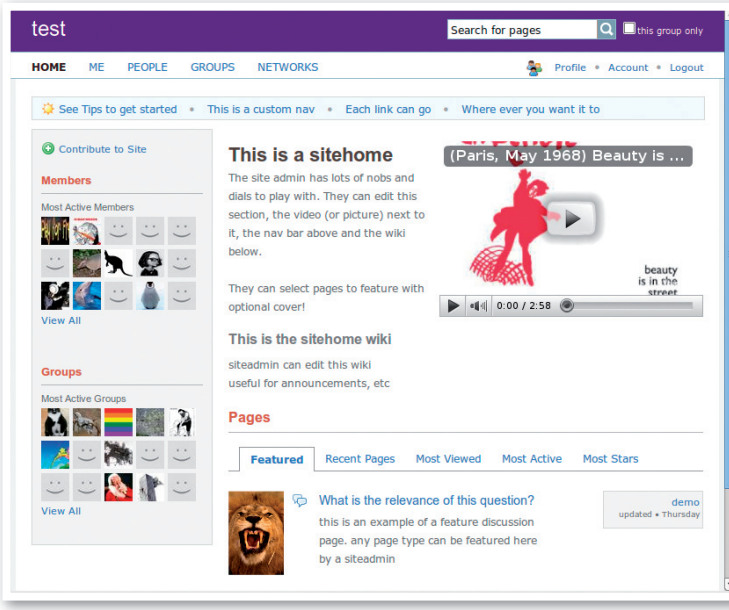

Figure 1: Not a weed – the Crabgrass dashboard gives you rapid access to the integrated wiki, users, and groups.

The idea of a central repository for credentials does sound enticing, and I do have an account with Flickr [7] and Dropbox [8], but who in their right mind would want to entrust their passwords to a third-party server?

Luckily, you don't have to, thanks to Clipperz Community Edition [9]. This online password manager is the open source version of Marco Barulli and Giulio Cesare Solaroli's Clipperz-hosted password safe service.

Encryption in the Browser

The software, licensed under the AGPL, is based on the JavaScript Crypto Library, which the two Italians also developed. The library relies on trusted algorithms such as SRP, AES-256, SHA-256, and Fortuna. Data encryption is handled client side without any server involvement, so only fully encrypted information crosses the wire.

Server side, Clipperz only requires MySQL and PHP, plus the BCMath, JSON, and PDO modules. Although it can make you feel safer, you do not need to run SSL on the server. The client is a standard, JavaScript-capable web browser. Firefox, Opera, Chrome, Konqueror, and Safari all work reliably. It comes as little surprise that the complex JavaScript doesn't always work as the developers intended in Internet Explorer. A script blocker is also an obstacle, so it's a good idea to disable this before you start using Clipperz.

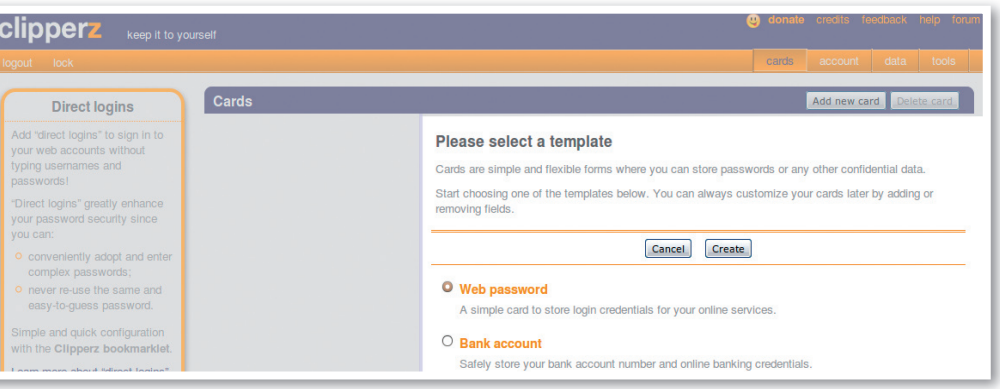

Figure 2: Clipperz offers various templates for special scenarios, including storage for bank and credit card data.

One known error is also caused by the popular "It's All Text!" [10] add-on for Firefox, which blocks the Clipperz login if the *Edit* button is enabled.

On an Android smartphone, at least the Dolphin browser will cooperate with Clipperz. In contrast, however, you will need to jailbreak the iPhone to convince Safari to give JavaScript the required resources.

Security and Convenience

Clipperz not only manages simple passwords, it also gives users a template option for encrypted storage of account and credit card data (see Figure 2). The password manager also provides users who want to access their data offline with a read-only copy of the data, which is available under the *data* button in the Clipperz menubar.

This single HTML file lets you access your passwords without any additional software and without needing an Internet connection.

The Achilles heel of any password safe is the passphrase ultimately chosen by the user. If you regularly work on computers that don't belong to you, or you use computers in Internet cafés, you can protect your main password against keyloggers by telling Clipperz to generate one-time passwords.

Bookmarklets let security-aware users create quick logins for websites that contain login forms. With one click, Clipperz will pass in your access credentials directly to the form and log you in. The password safe also protects you against shoulder surfing of cleartext passwords and against copy-and-paste incidents with its quick login function.

Any password safe worth its salt will include a password generator. Clipperz locates its password-generating function directly next to the password field when you create a new card, and it creates passwords that any normal user would find impossible to remember (see Figure 3).

Clipperz development is currently fairly slow. The next innovation scheduled on the project staff's roadmap involves the use of sharing, which will allow Clipperz users to share passwords selectively.

The Gamma test version [11] will give you some idea of the imminent changes to the Community Edition. ■■■

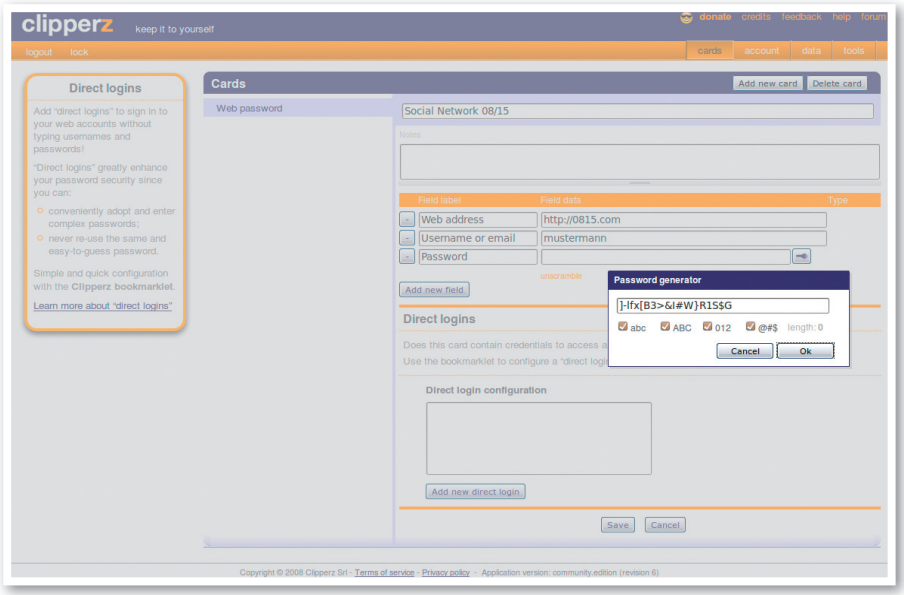

Figure 3: If a user decides not to use nonstandard characters in the Clipperz password generator, the generator automatically chooses a longer password and, in this way, maintains security levels.

INFO

[1] Crabgrass: *http://crabgrass.riseup.net*
[2] Facebook: *http://www.facebook.com/*
[3] Twitter: *http://twitter.com/*
[4] Xing: *http://www.xing.com*
[5] LinkedIn: *http://www.linkedin.com*
[6] Wer-kennt-wen: *http://www.wer-kennt-wen.de*
[7] Flickr: *http://www.flickr.com*
[8] Dropbox: *https://www.dropbox.com*
[9] Clipperz Community Edition: *http://www.clipperz.com/open_source/clipperz_community_edition*
[10] "It's All Text!" for Firefox: *http://addons.mozilla.org/de/firefox/addon/4125* (in German)
[11] Clipperz gamma test version: *http://www.clipperz.com*

THE AUTHOR

Mela Eckenfels is a freelance author and trainer who previously worked as a Unix system administrator. She co-authored *Das Kochbuch für Geeks* (Geek Cookbook) with Petra Hildebrandt; the book, which was published by O'Reilly Germany, just goes to show that cooking has much in common with programming.