Privacy and Security: Policy and Tech

Tim Bray

tbray@textuality.com · tbray.org · @timbray · +TimBray

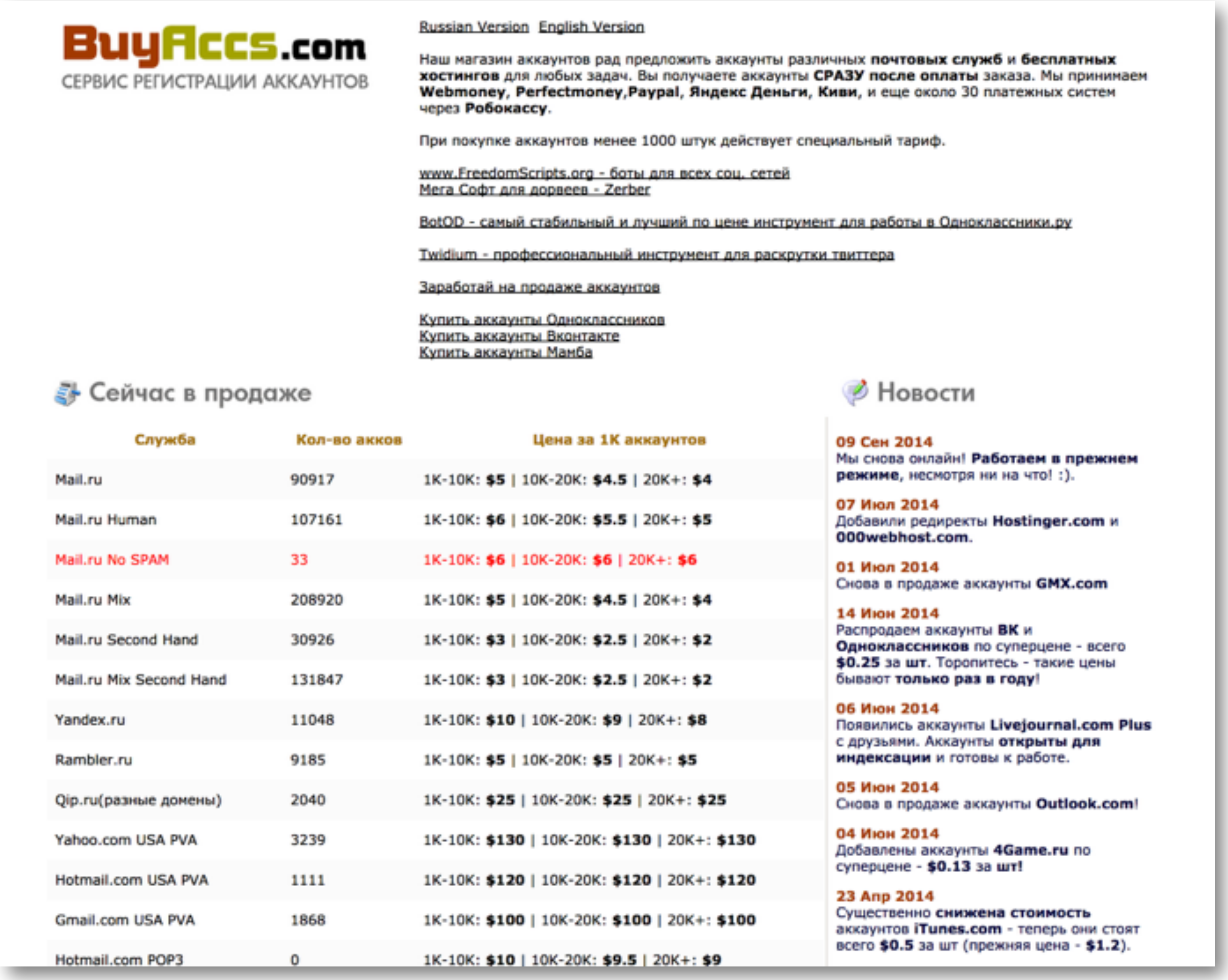
Links featured in this talk:

goo.gl/ggrSBj

Recent security blogging:

tbray.org/ongoing/What/Technology/Security

Photo: Wikimedia Commons



BuyAccs.com
СЕРВИС РЕГИСТРАЦИИ АККАУНТОВ

Russian Version English Version

Наш магазин аккаунтов рад предложить аккаунты различных **почтовых служб** и **бесплатных хостингов** для любых задач. Вы получаете аккаунты **СРАЗУ после оплаты** заказа. Мы принимаем **Webmoney**, **Perfectmoney**,**Paypal**, **Яндекс Деньги**, **Киви**, и еще около 30 платежных систем через **Робокассу**.

При покупке аккаунтов менее 1000 штук действует специальный тариф.

www.FreedomScripts.org - боты для всех соц. сетей
Мега Софт для дорвеев - Zerber

BotOD - самый стабильный и лучший по цене инструмент для работы в Одноклассники.ру

Twidium - профессиональный инструмент для раскрутки твиттера

Заработай на продаже аккаунтов

Купить аккаунты Одноклассников
Купить аккаунты Вконтакте
Купить аккаунты Мамба

Сейчас в продаже

Служба	Кол-во акков	Цена за 1К аккаунтов
Mail.ru	90917	1K-10K: **$5** | 10K-20K: **$4.5** | 20K+: **$4**
Mail.ru Human	107161	1K-10K: **$6** | 10K-20K: **$5.5** | 20K+: **$5**
Mail.ru No SPAM	33	1K-10K: **$6** | 10K-20K: **$6** | 20K+: **$6**
Mail.ru Mix	208920	1K-10K: **$5** | 10K-20K: **$4.5** | 20K+: **$4**
Mail.ru Second Hand	30926	1K-10K: **$3** | 10K-20K: **$2.5** | 20K+: **$2**
Mail.ru Mix Second Hand	131847	1K-10K: **$3** | 10K-20K: **$2.5** | 20K+: **$2**
Yandex.ru	11048	1K-10K: **$10** | 10K-20K: **$9** | 20K+: **$8**
Rambler.ru	9185	1K-10K: **$5** | 10K-20K: **$5** | 20K+: **$5**
Qip.ru(разные домены)	2040	1K-10K: **$25** | 10K-20K: **$25** | 20K+: **$25**
Yahoo.com USA PVA	3239	1K-10K: **$130** | 10K-20K: **$130** | 20K+: **$130**
Hotmail.com USA PVA	1111	1K-10K: **$120** | 10K-20K: **$120** | 20K+: **$120**
Gmail.com USA PVA	1868	1K-10K: **$100** | 10K-20K: **$100** | 20K+: **$100**
Hotmail.com POP3	0	1K-10K: **$10** | 10K-20K: **$9.5** | 20K+: **$9**

Новости

09 Сен 2014
Мы снова онлайн! **Работаем в прежнем режиме**, несмотря ни на что! :).

07 Июл 2014
Добавили редиректы **Hostinger.com** и **000webhost.com**.

01 Июл 2014
Снова в продаже аккаунты **GMX.com**

14 Июн 2014
Распродаем аккаунты **ВК** и **Одноклассников** по суперцене - всего **$0.25** за **шт**. Торопитесь - такие цены бывают **только раз в году**!

06 Июн 2014
Появились аккаунты **Livejournal.com Plus** с друзьями. Аккаунты **открыты для индексации** и готовы к работе.

05 Июн 2014
Снова в продаже аккаунты **Outlook.com**!

04 Июн 2014
Добавлены аккаунты **4Game.ru** по суперцене - **$0.13** за **шт!**

23 Апр 2014
Существенно **снижена стоимость** аккаунтов **iTunes.com** - теперь они стоят всего **$0.5** за шт (прежняя цена - **$1.2**).

buyaccs.com

National Security Agency
Central Security Service
Defending Our Nation. Securing The Future.

אצלנו תוכל לראות את הבלתי נראה
ולעשות את הבלתי אפשרי
מ' עובד מוסד

Government of Canada
Gouvernement du Canada
Communications Security Establishment

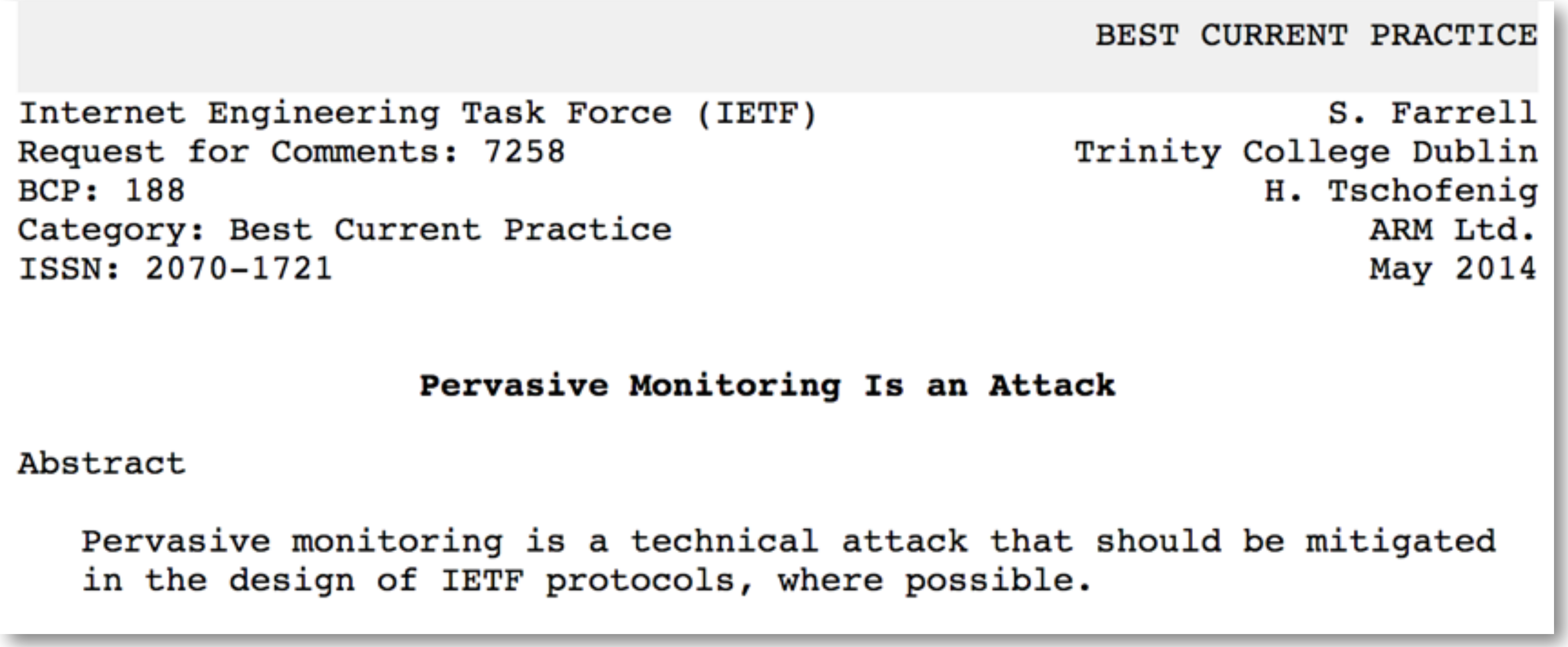
中华人民共和国国家安全部

GCHQ
WHO WE ARE
WHAT WE DO
HOW WE WORK
CAREERS
PRESS & MEDIA
Search
Go »

> “If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place...
>
> - Eric Schmidt, 2009

www.eff.org/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy

127
8
S12
76
BERKELEY POLICE



BEST CURRENT PRACTICE

Internet Engineering Task Force (IETF) S. Farrell
Request for Comments: 7258 Trinity College Dublin
BCP: 188 H. Tschofenig
Category: Best Current Practice ARM Ltd.
ISSN: 2070-1721 May 2014

Pervasive Monitoring Is an Attack

Abstract

Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible.

RFC 7258

Privacy levels

1. **Basic privacy**: Encrypted WiFi, HTTPS.
2. **Common privacy**: Ordinary crooks can’t see your data. Government employees need a warrant.
3. **Strong privacy**: Nobody can see your data without your co-operation.

tbray.org/ongoing/When/201x/2014/05/26/Privacy-Levels

Best Practice: HTTPS

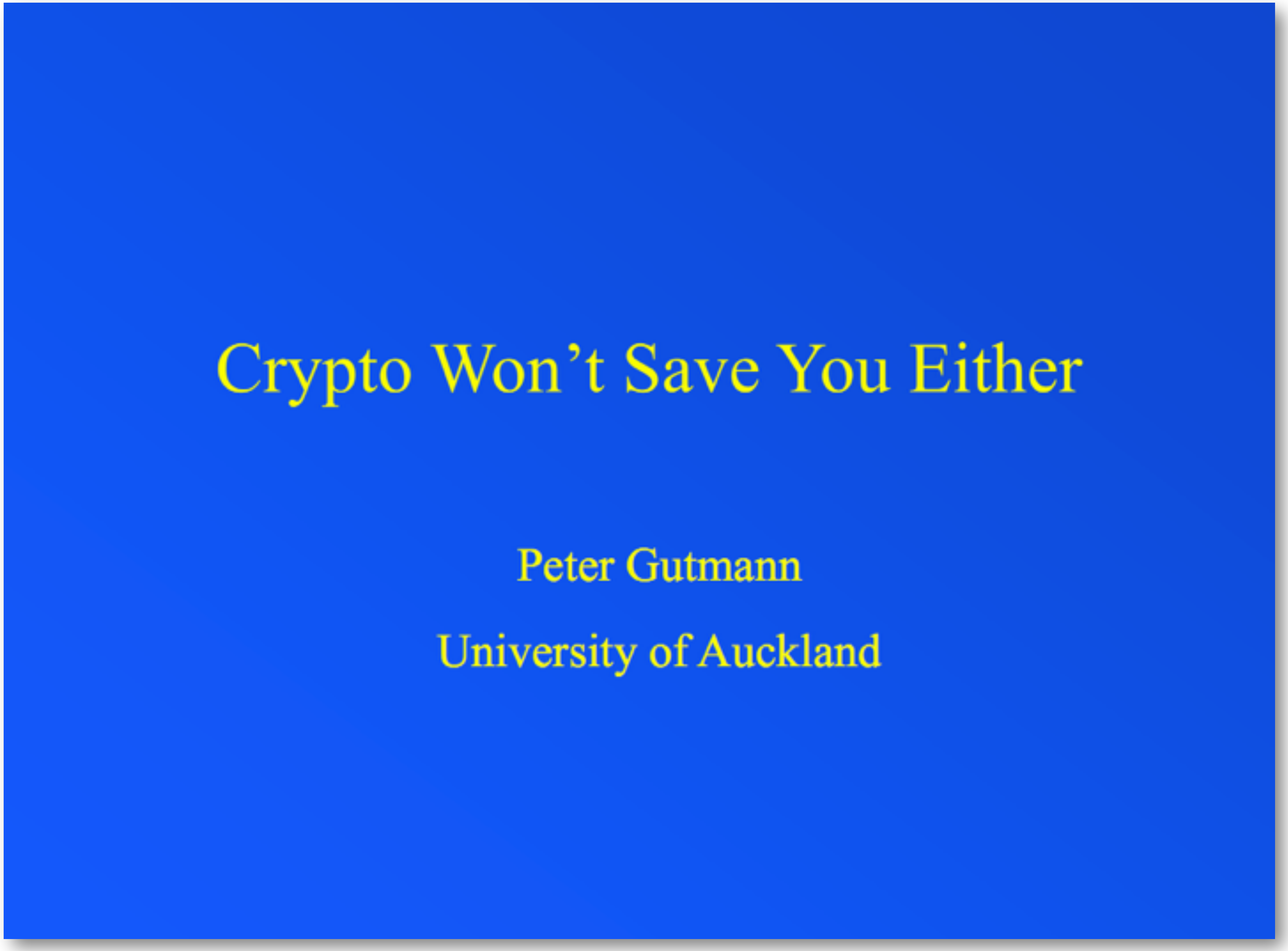
Always use HTTPS. **Never** don't use HTTPS. It doesn't matter if it's "public brochure-ware". It doesn't matter if your budget is tight. It doesn't matter if your users don't think they need privacy. Just use HTTPS.

Justification

- Positive failure: They got privacy but didn’t need it. Negative failure: They needed privacy but didn’t get it. These are **not symmetrical**.
- It’s **hard** for both you and users to make the correct privacy choices. So, don’t make them; opt for privacy.
- The cost of HTTPS (financial and technical) falls **every year**. Check it out; it’s actually amazingly cheap.

But…

> “HTTPS is flawed, and the certificate authorities are corrupt and stupid, and the NSA has broken HTTPS anyhow, and they might just put a key logger on the PC. You shouldn’t promise privacy because it doesn’t really work, and you’re creating a false sense of security.”

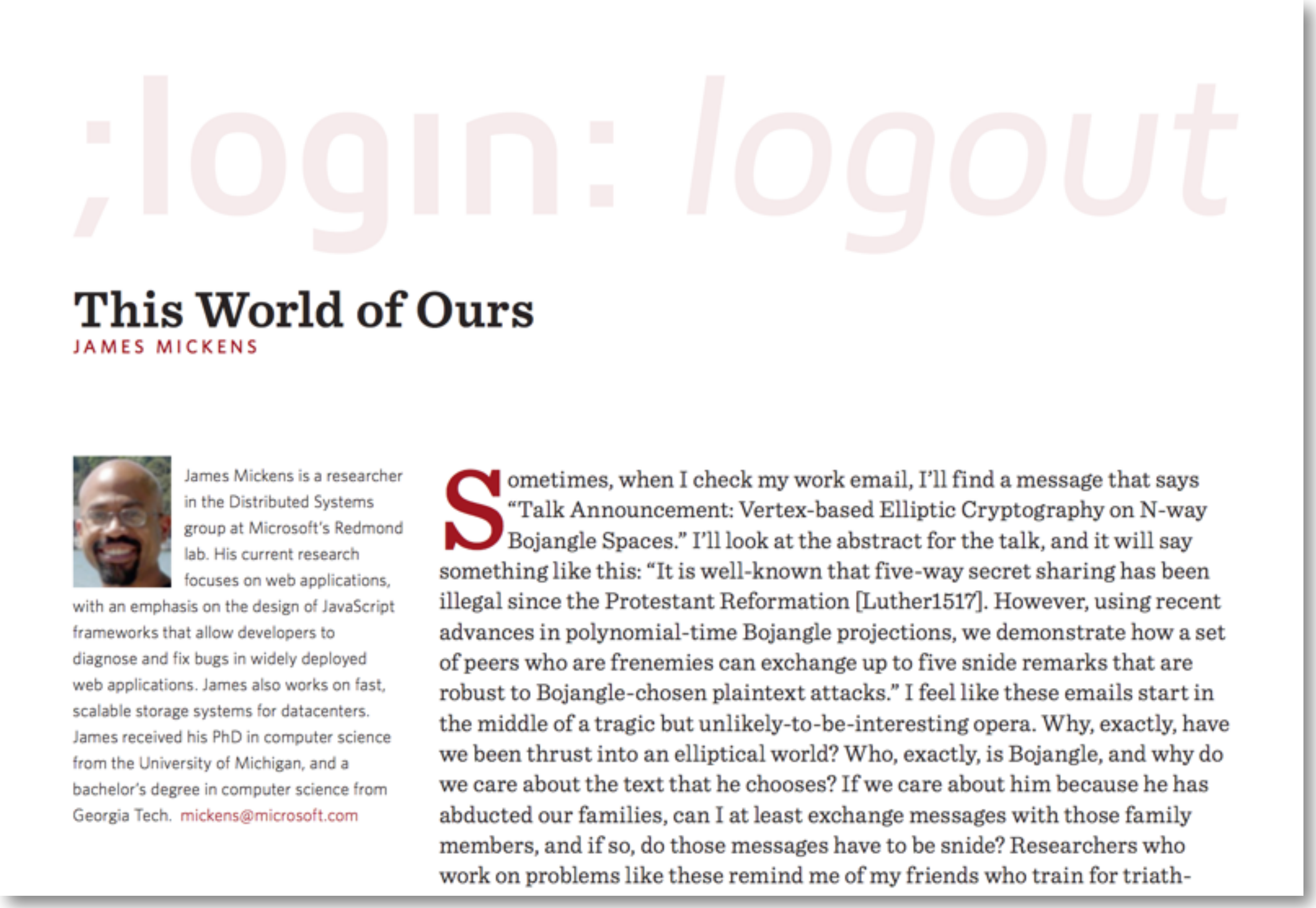


Crypto Won’t Save You Either

Peter Gutmann

University of Auckland

regmedia.co.uk/2014/05/16/0955_peter_gutmann.pdf



;login: *logout*

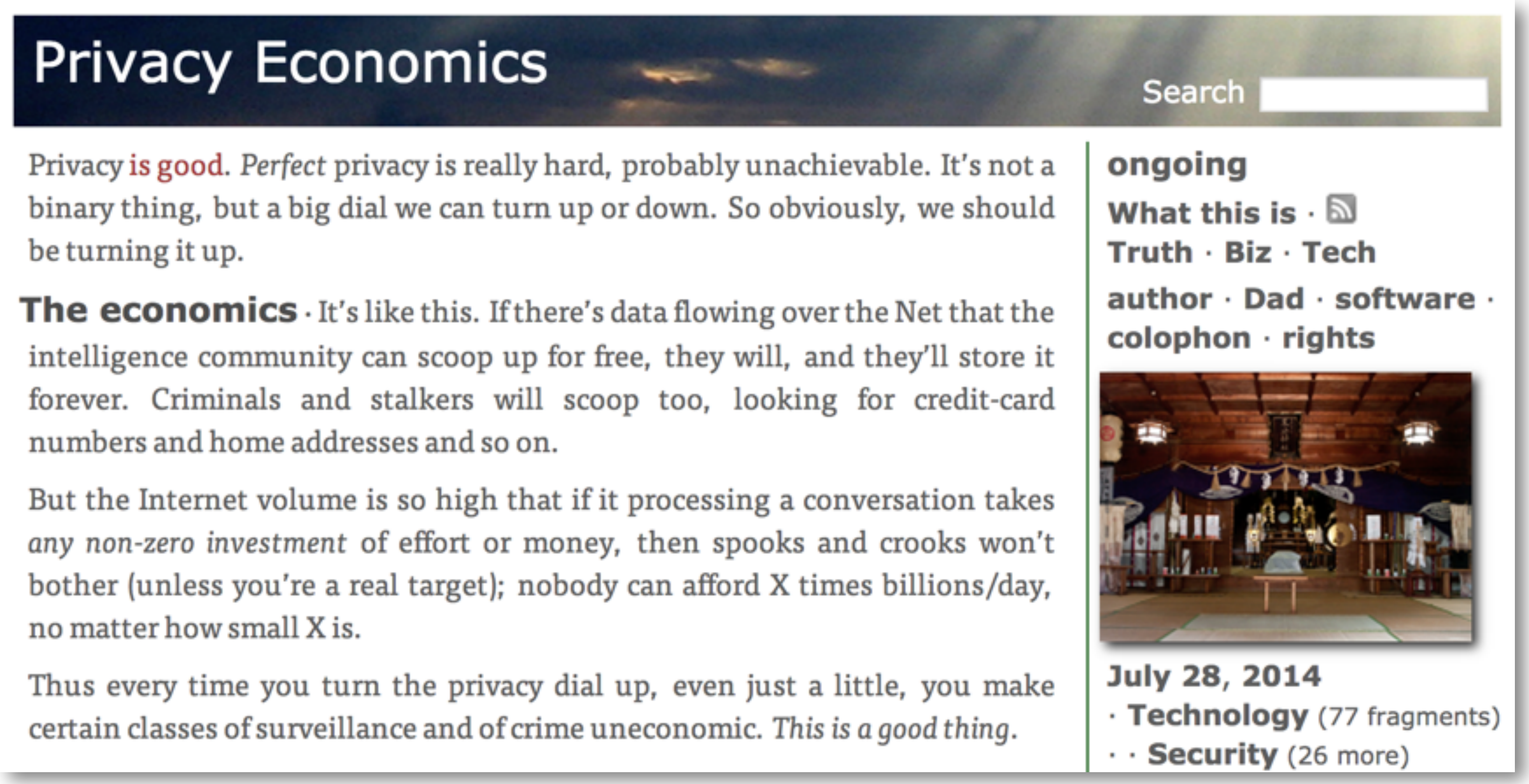
This World of Ours

JAMES MICKENS

James Mickens is a researcher in the Distributed Systems group at Microsoft's Redmond lab. His current research focuses on web applications, with an emphasis on the design of JavaScript frameworks that allow developers to diagnose and fix bugs in widely deployed web applications. James also works on fast, scalable storage systems for datacenters. James received his PhD in computer science from the University of Michigan, and a bachelor's degree in computer science from Georgia Tech. mickens@microsoft.com

Sometimes, when I check my work email, I'll find a message that says "Talk Announcement: Vertex-based Elliptic Cryptography on N-way Bojangle Spaces." I'll look at the abstract for the talk, and it will say something like this: "It is well-known that five-way secret sharing has been illegal since the Protestant Reformation [Luther1517]. However, using recent advances in polynomial-time Bojangle projections, we demonstrate how a set of peers who are frenemies can exchange up to five snide remarks that are robust to Bojangle-chosen plaintext attacks." I feel like these emails start in the middle of a tragic but unlikely-to-be-interesting opera. Why, exactly, have we been thrust into an elliptical world? Who, exactly, is Bojangle, and why do we care about the text that he chooses? If we care about him because he has abducted our families, can I at least exchange messages with those family members, and if so, do those messages have to be snide? Researchers who work on problems like these remind me of my friends who train for triath-

research.microsoft.com/en-us/people/mickens/thisworldofours.pdf



Privacy Economics

Search

Privacy is good. *Perfect* privacy is really hard, probably unachievable. It's not a binary thing, but a big dial we can turn up or down. So obviously, we should be turning it up.

The economics · It's like this. If there's data flowing over the Net that the intelligence community can scoop up for free, they will, and they'll store it forever. Criminals and stalkers will scoop too, looking for credit-card numbers and home addresses and so on.

But the Internet volume is so high that if it processing a conversation takes *any non-zero investment* of effort or money, then spooks and crooks won't bother (unless you're a real target); nobody can afford X times billions/day, no matter how small X is.

Thus every time you turn the privacy dial up, even just a little, you make certain classes of surveillance and of crime uneconomic. *This is a good thing.*

ongoing

What this is ·

Truth · **Biz** · **Tech**

author · **Dad** · **software** · **colophon** · **rights**

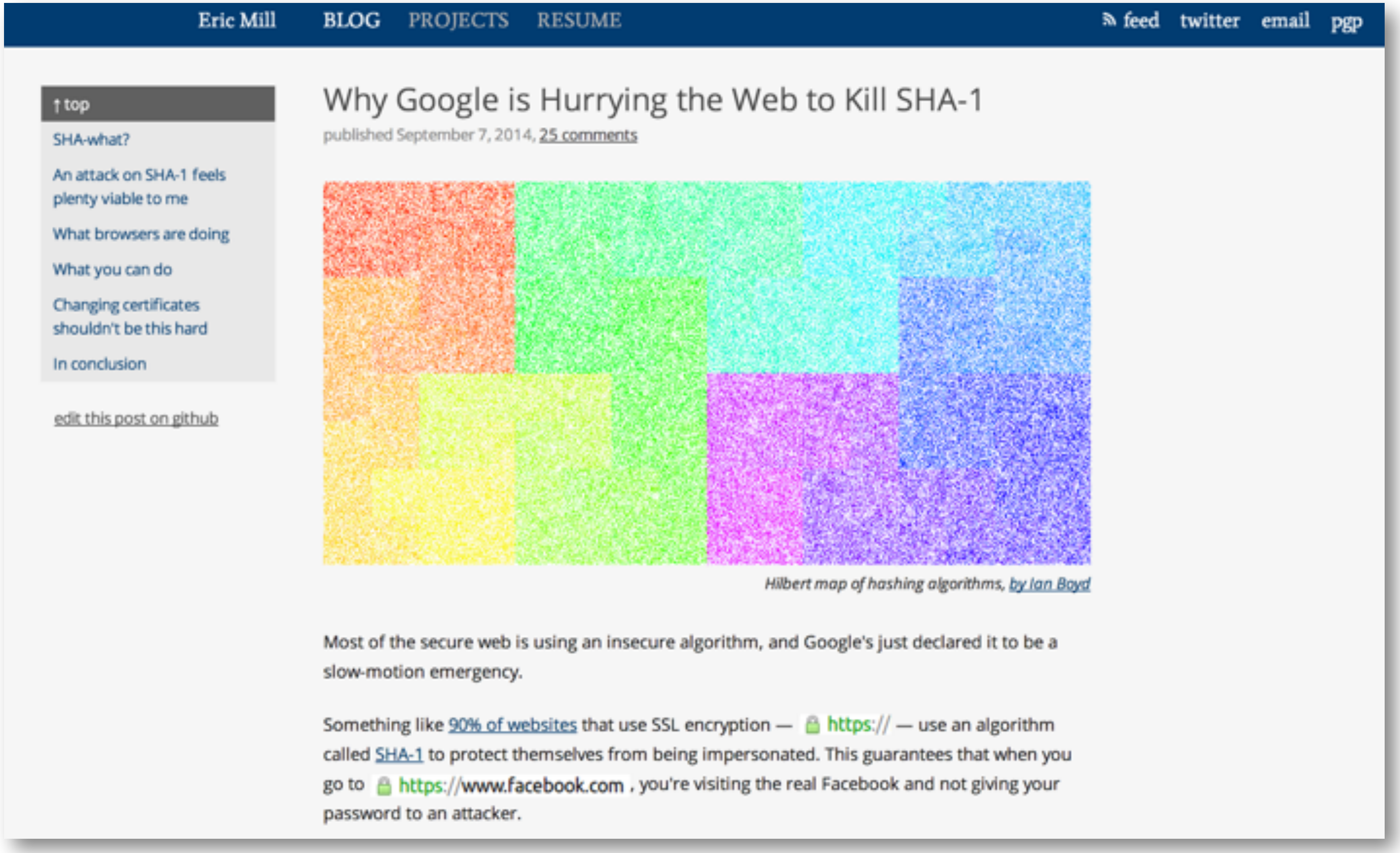
July 28, 2014

· **Technology** (77 fragments)

· · **Security** (26 more)

tbray.org/ongoing/When/201x/2014/07/28/Privacy-Economics

Best Practice: No SHA-1



Why Google is Hurrying the Web to Kill SHA-1

published September 7, 2014, 25 comments

Hilbert map of hashing algorithms, by Ian Boyd

Most of the secure web is using an insecure algorithm, and Google's just declared it to be a slow-motion emergency.

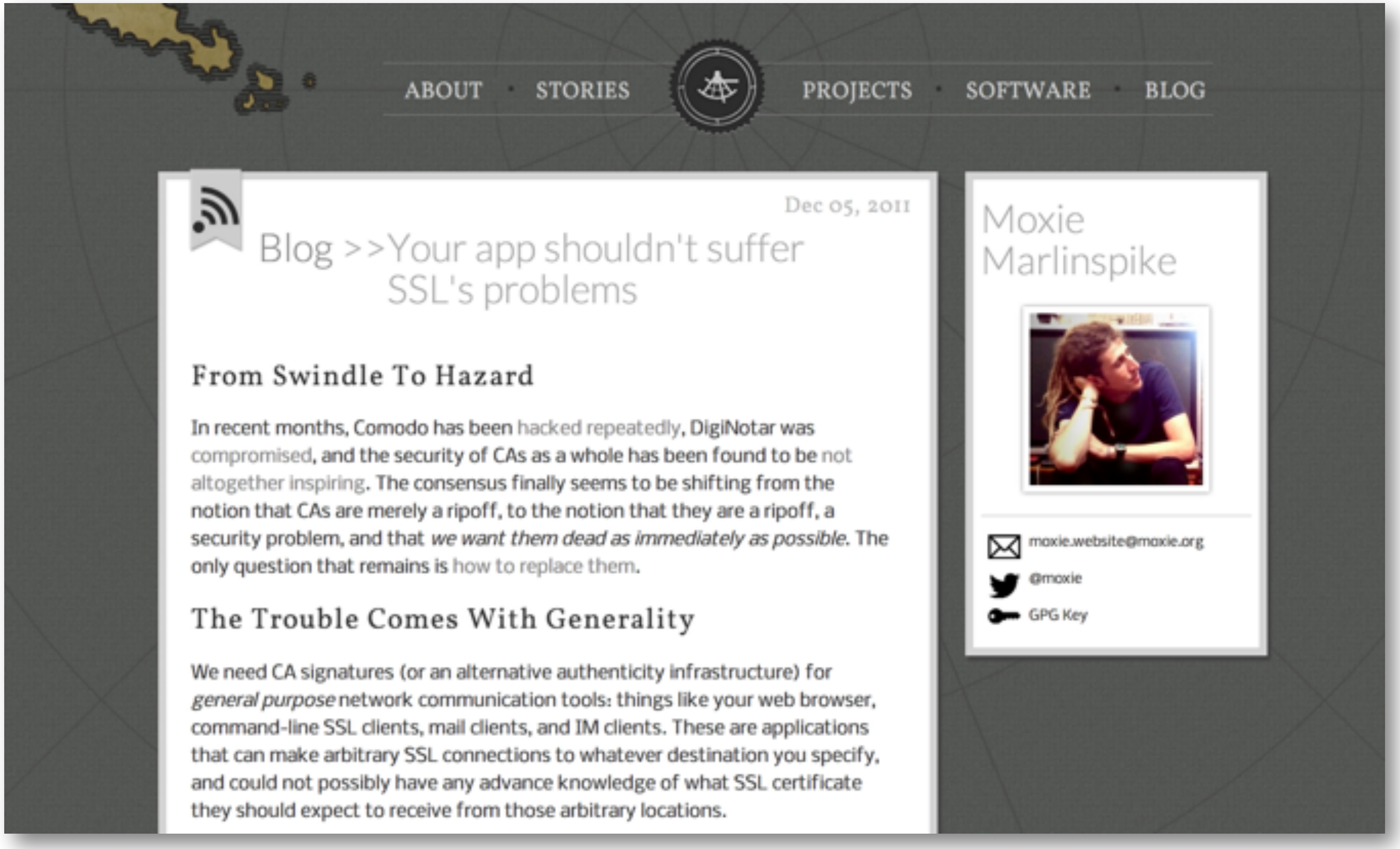
Something like 90% of websites that use SSL encryption — https:// — use an algorithm called SHA-1 to protect themselves from being impersonated. This guarantees that when you go to https://www.facebook.com , you're visiting the real Facebook and not giving your password to an attacker.

konklone.com/post/why-google-is-hurrying-the-web-to-kill-sha-1

Best Practice: Pin certs

```
JSONObject getFromKeybase(String path, String query) {
  String u = ”https://keybase.io/” + path +
    URLEncoder.encode(query, ”utf8”);
  URL url = new URL(u);
  HttpURLConnection conn = (HttpURLConnection)
    url.openConnection();
```

Best Practice: Pin certs



Dec 05, 2011

Blog >>Your app shouldn't suffer SSL's problems

From Swindle To Hazard

In recent months, Comodo has been hacked repeatedly, DigiNotar was compromised, and the security of CAs as a whole has been found to be not altogether inspiring. The consensus finally seems to be shifting from the notion that CAs are merely a ripoff, to the notion that they are a ripoff, a security problem, and that *we want them dead as immediately as possible*. The only question that remains is how to replace them.

The Trouble Comes With Generality

We need CA signatures (or an alternative authenticity infrastructure) for *general purpose* network communication tools: things like your web browser, command-line SSL clients, mail clients, and IM clients. These are applications that can make arbitrary SSL connections to whatever destination you specify, and could not possibly have any advance knowledge of what SSL certificate they should expect to receive from those arbitrary locations.

Moxie Marlinspike

moxie.website@moxie.org

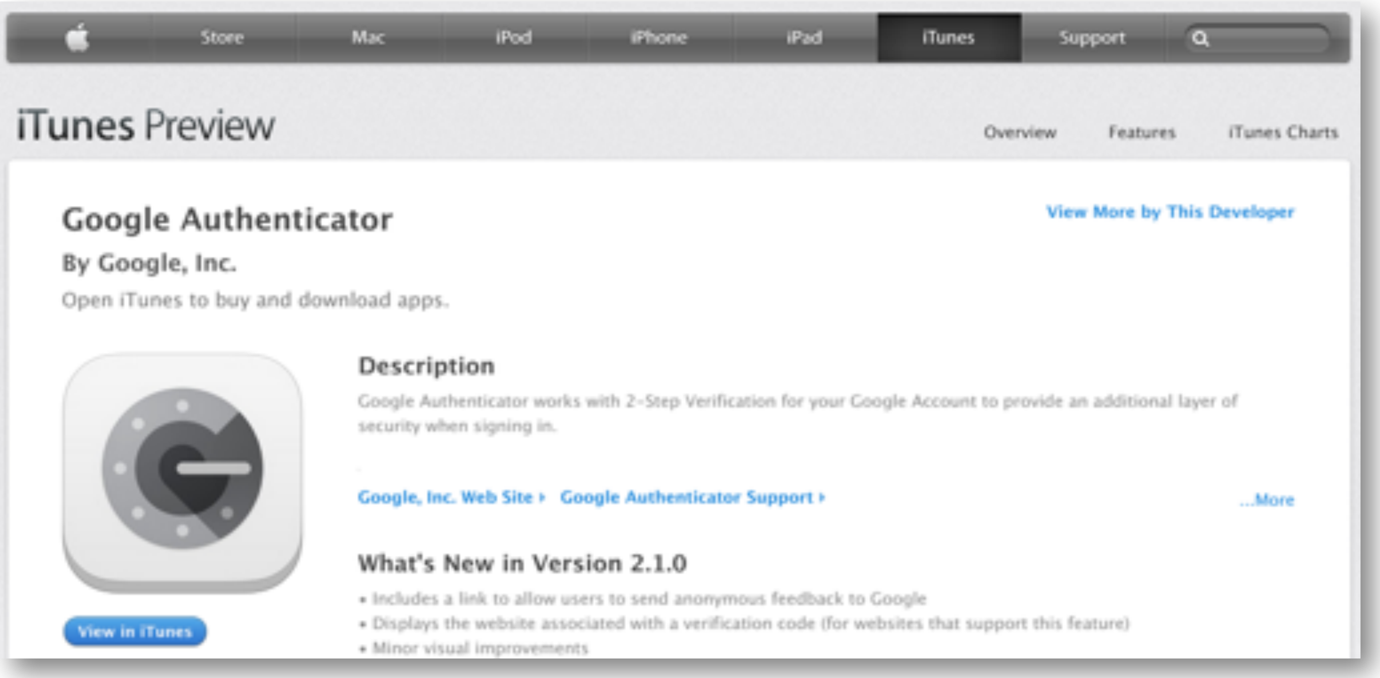
@moxie

GPG Key

thoughtcrime.org/blog/authenticity-is-broken-in-ssl-but-your-app-ha/

Best Practice: 2-factor

1. Always use 2-factor yourself on your Google/ Microsoft/Steam/whatever accounts.
2. Consider offering 2-factor authentication to your app's users.



Google Authenticator

By Google, Inc.

Open iTunes to buy and download apps.

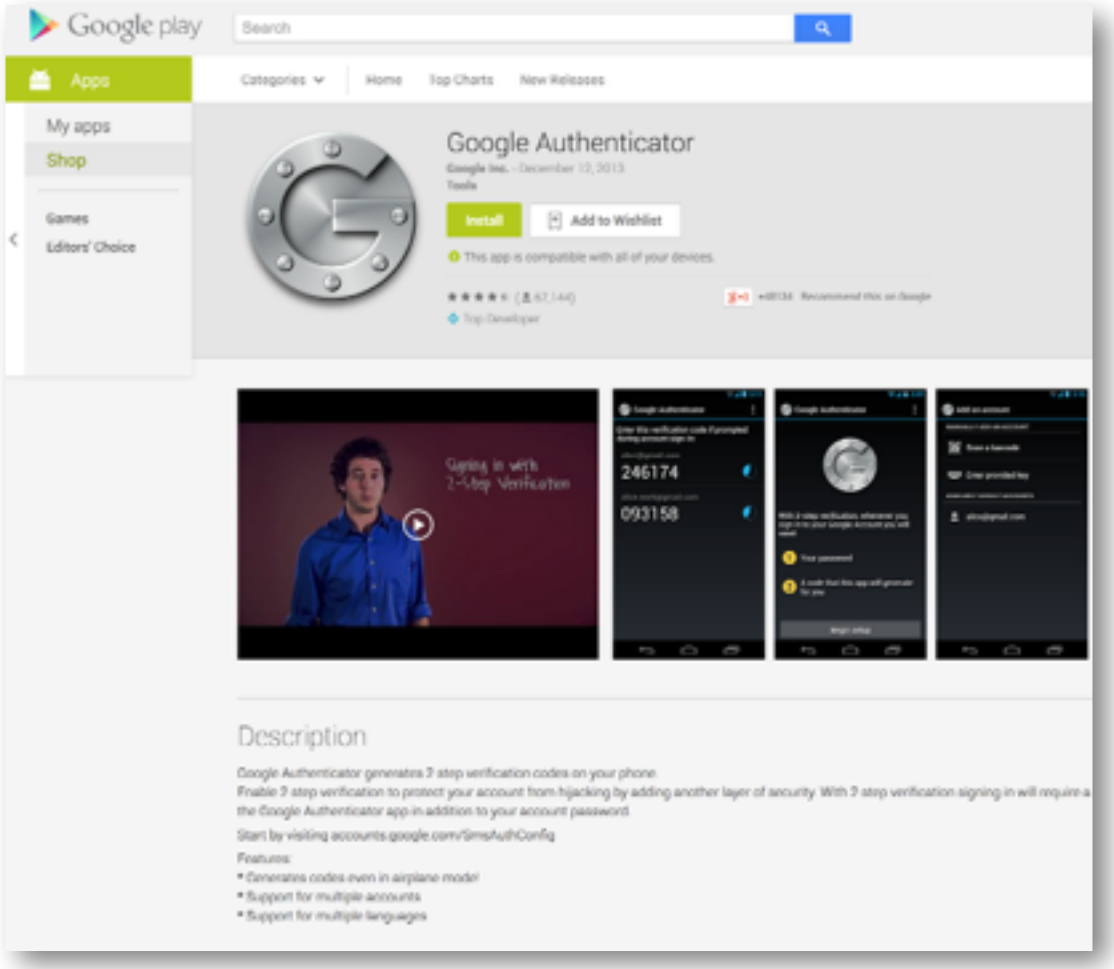
Description

Google Authenticator works with 2-Step Verification for your Google Account to provide an additional layer of security when signing in.

Google, Inc. Web Site ▸ Google Authenticator Support ▸ ...More

What's New in Version 2.1.0

- Includes a link to allow users to send anonymous feedback to Google
- Displays the website associated with a verification code (for websites that support this feature)
- Minor visual improvements



Google Authenticator

Google Inc. - December 12, 2013
Tools

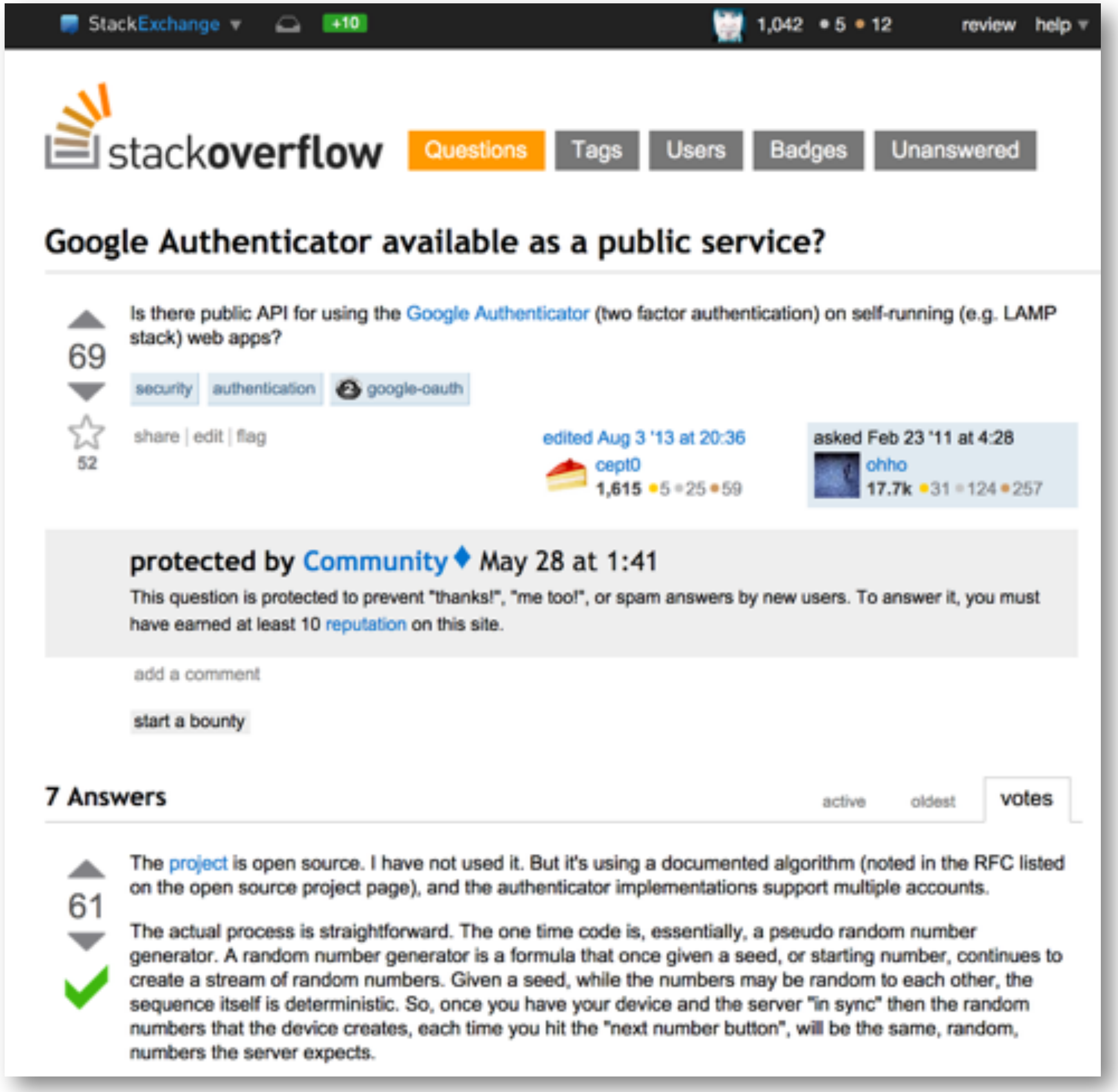
This app is compatible with all of your devices.

Description

Google Authenticator generates 2-step verification codes on your phone.
Enable 2-step verification to protect your account from hijacking by adding another layer of security. With 2-step verification signing in will require a
the Google Authenticator app in addition to your account password.

Start by visiting accounts.google.com/SmsAuthConfig

Features:
- Generates codes even in airplane mode!
- Support for multiple accounts
- Support for multiple languages



Google Authenticator available as a public service?

69

Is there public API for using the Google Authenticator (two factor authentication) on self-running (e.g. LAMP stack) web apps?

security authentication google-oauth

52

share | edit | flag

edited Aug 3 '13 at 20:36
cept0
1,615 •5 •25 •59

asked Feb 23 '11 at 4:28
ohho
17.7k •31 •124 •257

protected by Community♦ May 28 at 1:41

This question is protected to prevent "thanks!", "me too!", or spam answers by new users. To answer it, you must have earned at least 10 reputation on this site.

add a comment

start a bounty

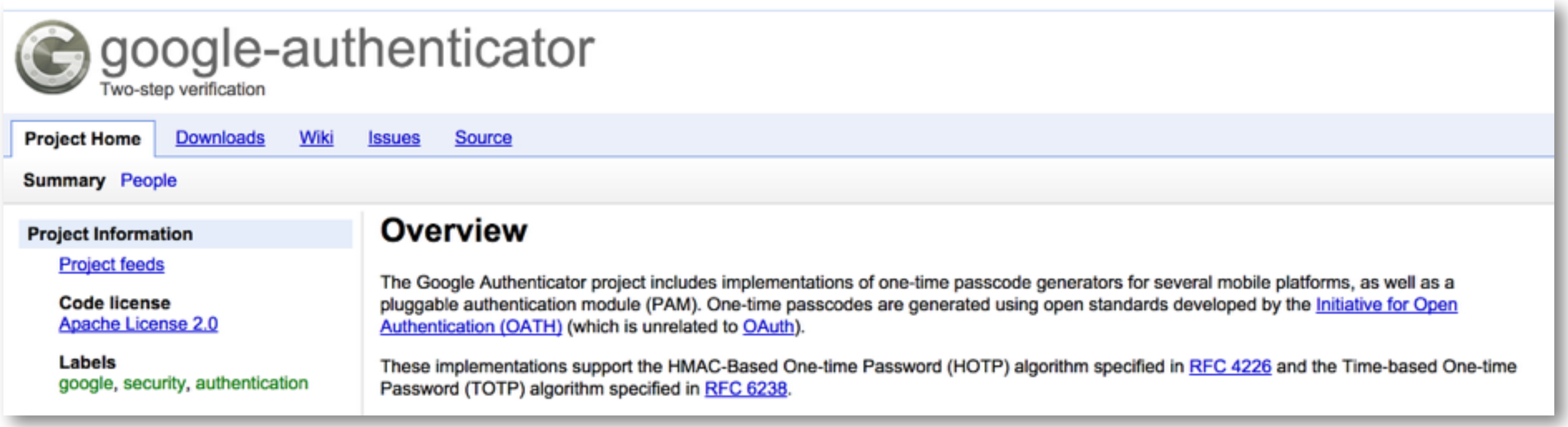
7 Answers

61 ✓

The project is open source. I have not used it. But it's using a documented algorithm (noted in the RFC listed on the open source project page), and the authenticator implementations support multiple accounts.

The actual process is straightforward. The one time code is, essentially, a pseudo random number generator. A random number generator is a formula that once given a seed, or starting number, continues to create a stream of random numbers. Given a seed, while the numbers may be random to each other, the sequence itself is deterministic. So, once you have your device and the server "in sync" then the random numbers that the device creates, each time you hit the "next number button", will be the same, random, numbers the server expects.

stackoverflow.com/questions/5087005/google-authenticator-available-as-a-public-service



google-authenticator

Two-step verification

Project Information

Project feeds

Code license

Apache License 2.0

Labels

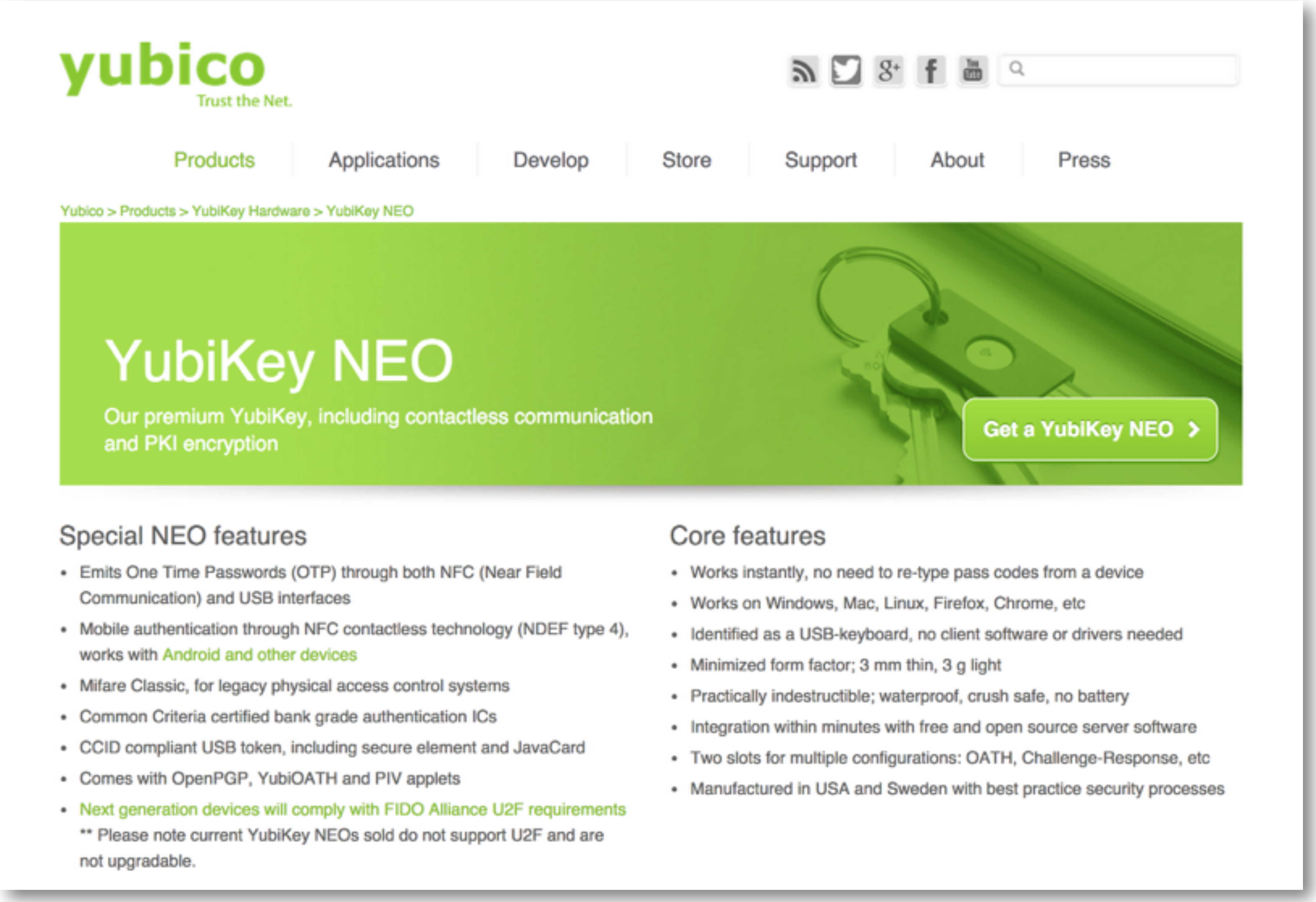
google, security, authentication

Overview

The Google Authenticator project includes implementations of one-time passcode generators for several mobile platforms, as well as a pluggable authentication module (PAM). One-time passcodes are generated using open standards developed by the Initiative for Open Authentication (OATH) (which is unrelated to OAuth).

These implementations support the HMAC-Based One-time Password (HOTP) algorithm specified in RFC 4226 and the Time-based One-time Password (TOTP) algorithm specified in RFC 6238.

code.google.com/p/google-authenticator



YubiKey NEO

Our premium YubiKey, including contactless communication and PKI encryption

Special NEO features

- Emits One Time Passwords (OTP) through both NFC (Near Field Communication) and USB interfaces
- Mobile authentication through NFC contactless technology (NDEF type 4), works with Android and other devices
- Mifare Classic, for legacy physical access control systems
- Common Criteria certified bank grade authentication ICs
- CCID compliant USB token, including secure element and JavaCard
- Comes with OpenPGP, YubiOATH and PIV applets
- Next generation devices will comply with FIDO Alliance U2F requirements
  ** Please note current YubiKey NEOs sold do not support U2F and are not upgradable.

Core features

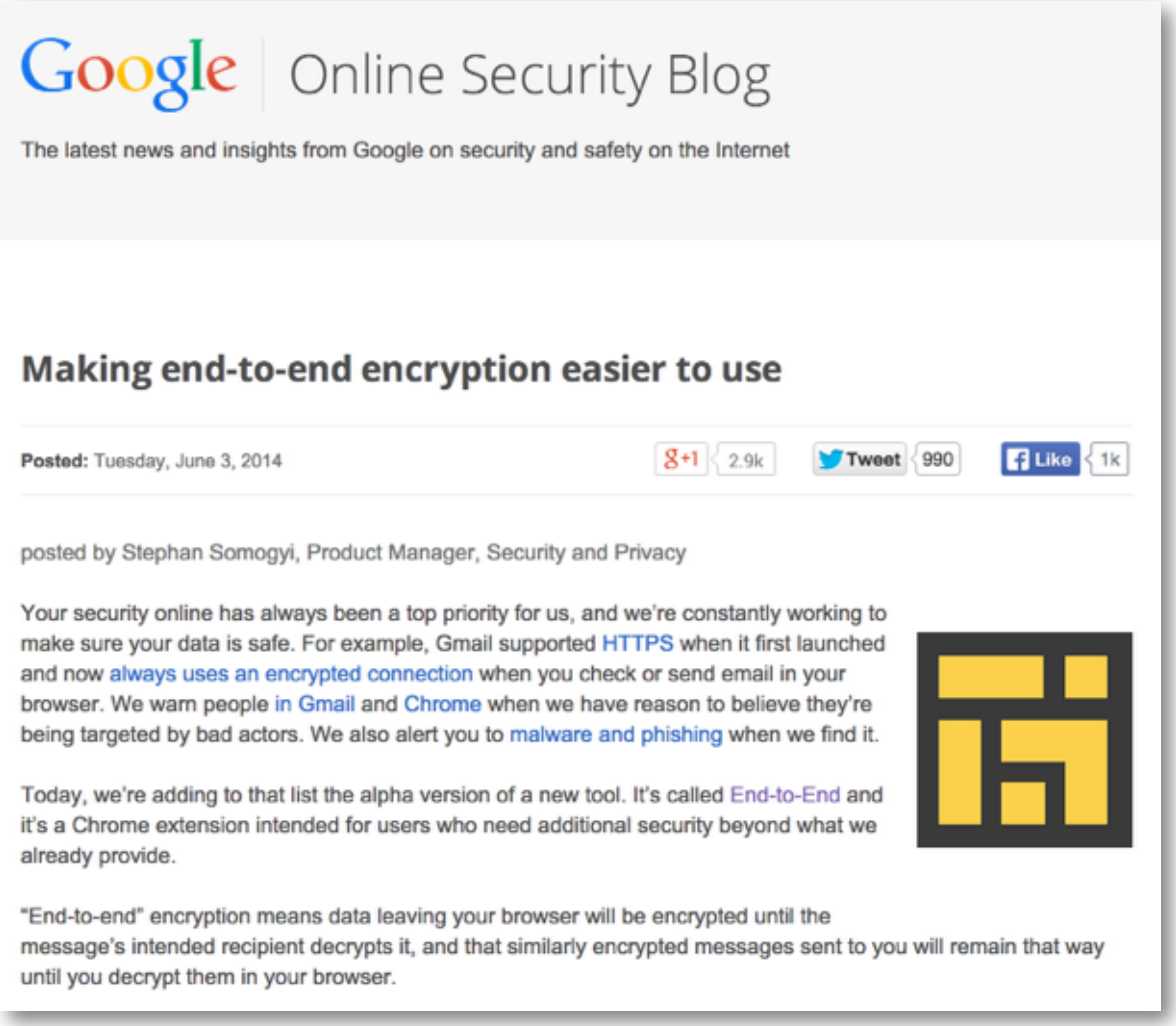
- Works instantly, no need to re-type pass codes from a device
- Works on Windows, Mac, Linux, Firefox, Chrome, etc
- Identified as a USB-keyboard, no client software or drivers needed
- Minimized form factor; 3 mm thin, 3 g light
- Practically indestructible; waterproof, crush safe, no battery
- Integration within minutes with free and open source server software
- Two slots for multiple configurations: OATH, Challenge-Response, etc
- Manufactured in USA and Sweden with best practice security processes

www.yubico.com/products/yubikey-hardware/yubikey-neo/

Privacy levels

1. **Basic privacy**: Encrypted WiFi, HTTPS.
2. **Common privacy**: Ordinary crooks can't see your data. Government employees need a warrant.
3. **Strong privacy**: Nobody can see your data without your co-operation.

tbray.org/ongoing/When/201x/2011/12/27/Type-Systems



Online Security Blog

The latest news and insights from Google on security and safety on the Internet

Making end-to-end encryption easier to use

Posted: Tuesday, June 3, 2014

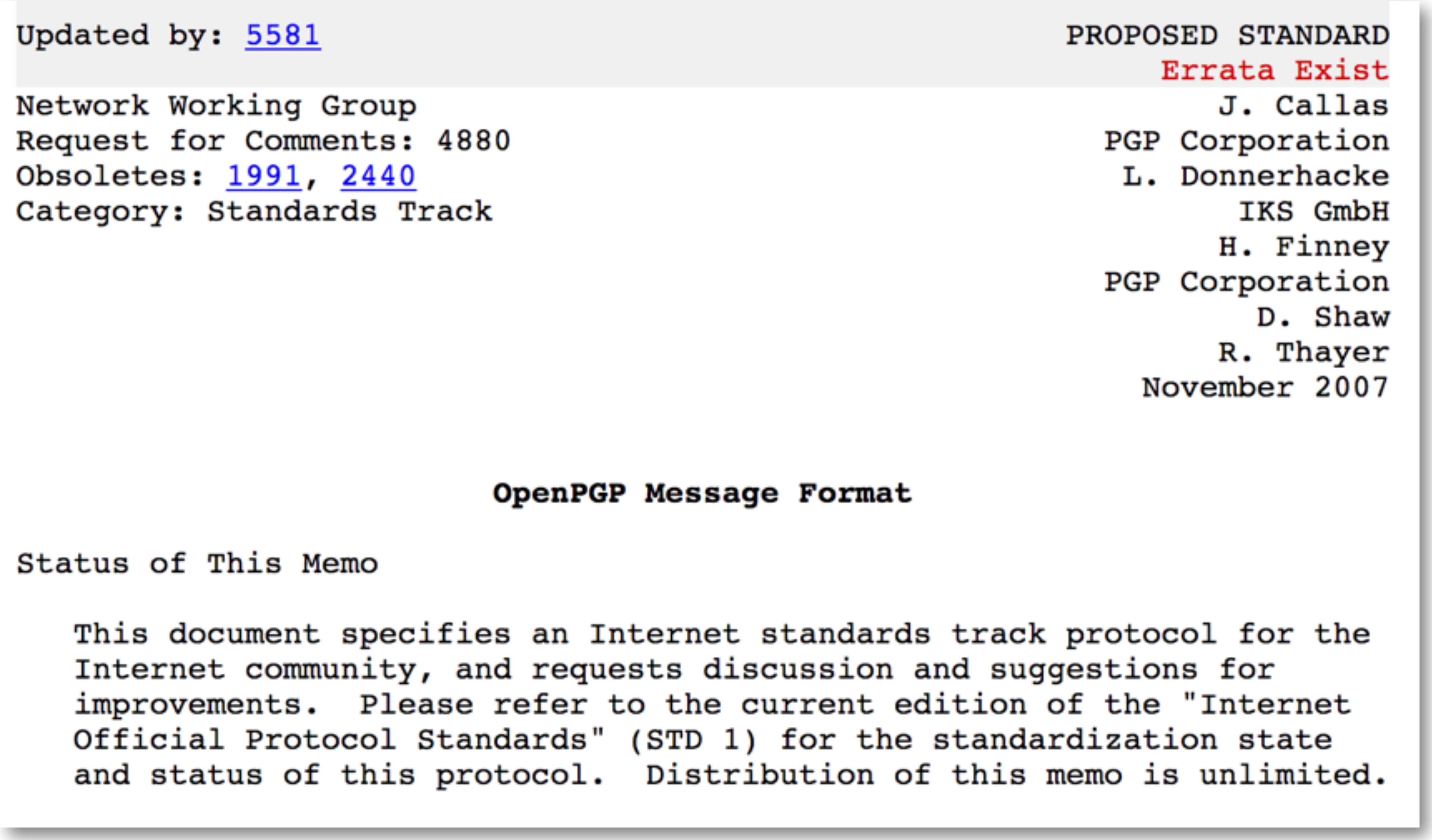
posted by Stephan Somogyi, Product Manager, Security and Privacy

Your security online has always been a top priority for us, and we're constantly working to make sure your data is safe. For example, Gmail supported HTTPS when it first launched and now always uses an encrypted connection when you check or send email in your browser. We warn people in Gmail and Chrome when we have reason to believe they're being targeted by bad actors. We also alert you to malware and phishing when we find it.

Today, we're adding to that list the alpha version of a new tool. It's called End-to-End and it's a Chrome extension intended for users who need additional security beyond what we already provide.

"End-to-end" encryption means data leaving your browser will be encrypted until the message's intended recipient decrypts it, and that similarly encrypted messages sent to you will remain that way until you decrypt them in your browser.

googleonlinesecurity.blogspot.com/2014/06/making-end-to-end-encryption-easier-to.html



```
Updated by: 5581                                   PROPOSED STANDARD
                                                        Errata Exist
Network Working Group                                      J. Callas
Request for Comments: 4880                           PGP Corporation
Obsoletes: 1991, 2440                                 L. Donnerhacke
Category: Standards Track                                   IKS GmbH
                                                           H. Finney
                                                     PGP Corporation
                                                             D. Shaw
                                                           R. Thayer
                                                       November 2007
```

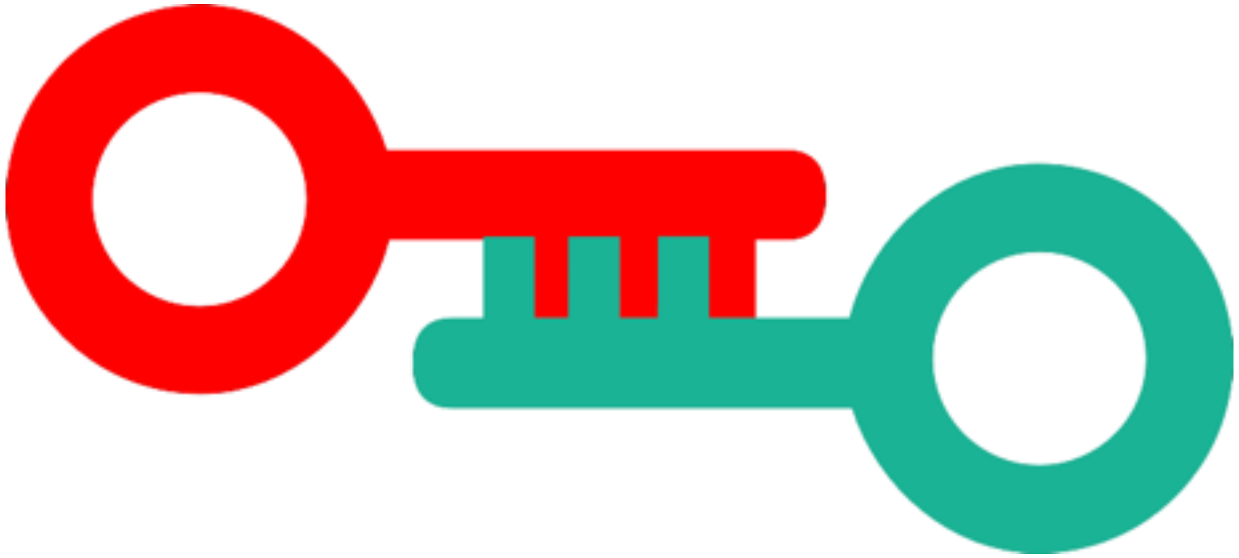
OpenPGP Message Format

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

RFC 4880

Public/Private key pair



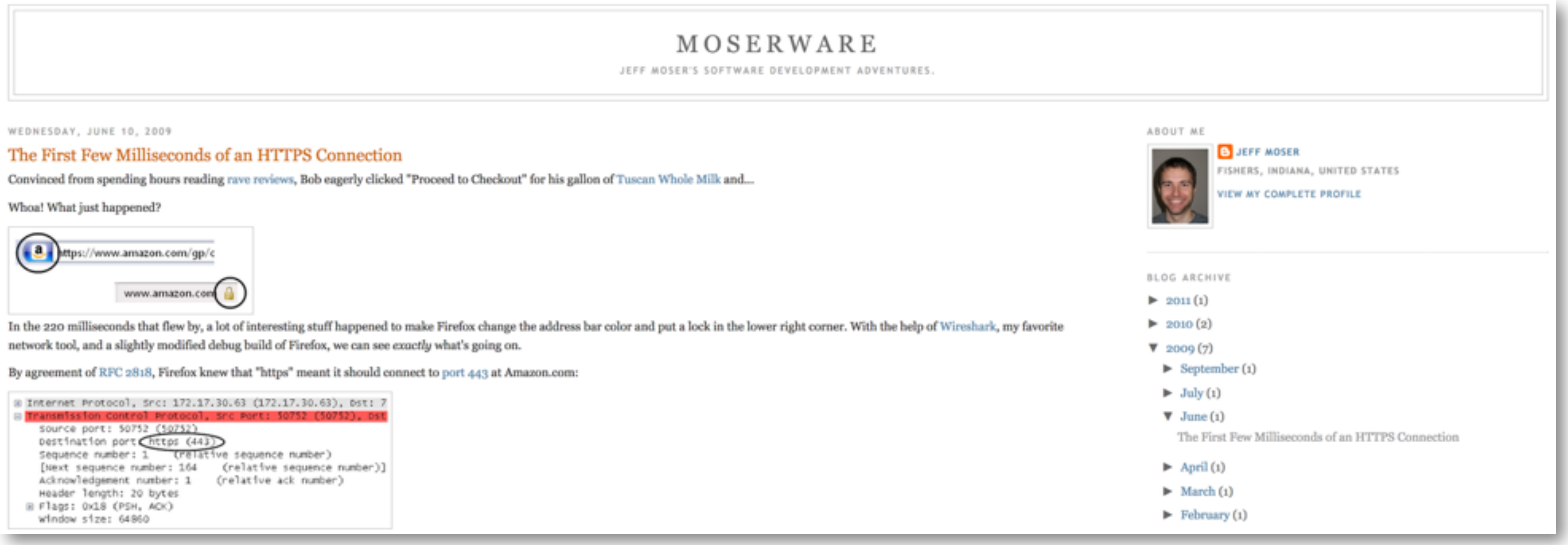
Two binary objects, created as a pair, called the **private key** (red) and **public key** (green). This can be done cheaply on any computer, and there are an infinite number available.

The private key:

- Is kept secret, and is always passphrase-protected.
- Can’t be discovered by knowing the public key.
- Anything encrypted with it can be decrypted with the public key.
- Can decrypt anything encrypted with the public key.

The public key:

- Is published on the Net.
- Anything encrypted with it can be decrypted with the private key.
- Can decrypt anything encrypted with the private key.



MOSERWARE

JEFF MOSER'S SOFTWARE DEVELOPMENT ADVENTURES.

WEDNESDAY, JUNE 10, 2009

The First Few Milliseconds of an HTTPS Connection

Convinced from spending hours reading rave reviews, Bob eagerly clicked "Proceed to Checkout" for his gallon of Tuscan Whole Milk and...

Whoa! What just happened?

In the 220 milliseconds that flew by, a lot of interesting stuff happened to make Firefox change the address bar color and put a lock in the lower right corner. With the help of Wireshark, my favorite network tool, and a slightly modified debug build of Firefox, we can see *exactly* what's going on.

By agreement of RFC 2818, Firefox knew that "https" meant it should connect to port 443 at Amazon.com:

```
⊞ Internet Protocol, Src: 172.17.30.63 (172.17.30.63), Dst: 7
⊟ Transmission Control Protocol, Src Port: 50752 (50752), Dst
    Source port: 50752 (50752)
    Destination port: https (443)
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 164    (relative sequence number)]
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x18 (PSH, ACK)
    Window size: 64860
```

ABOUT ME

JEFF MOSER

FISHERS, INDIANA, UNITED STATES

VIEW MY COMPLETE PROFILE

BLOG ARCHIVE

- ► 2011 (1)
- ► 2010 (2)
- ▼ 2009 (7)
  - ► September (1)
  - ► July (1)
  - ▼ June (1)
    - The First Few Milliseconds of an HTTPS Connection
  - ► April (1)
  - ► March (1)
  - ► February (1)

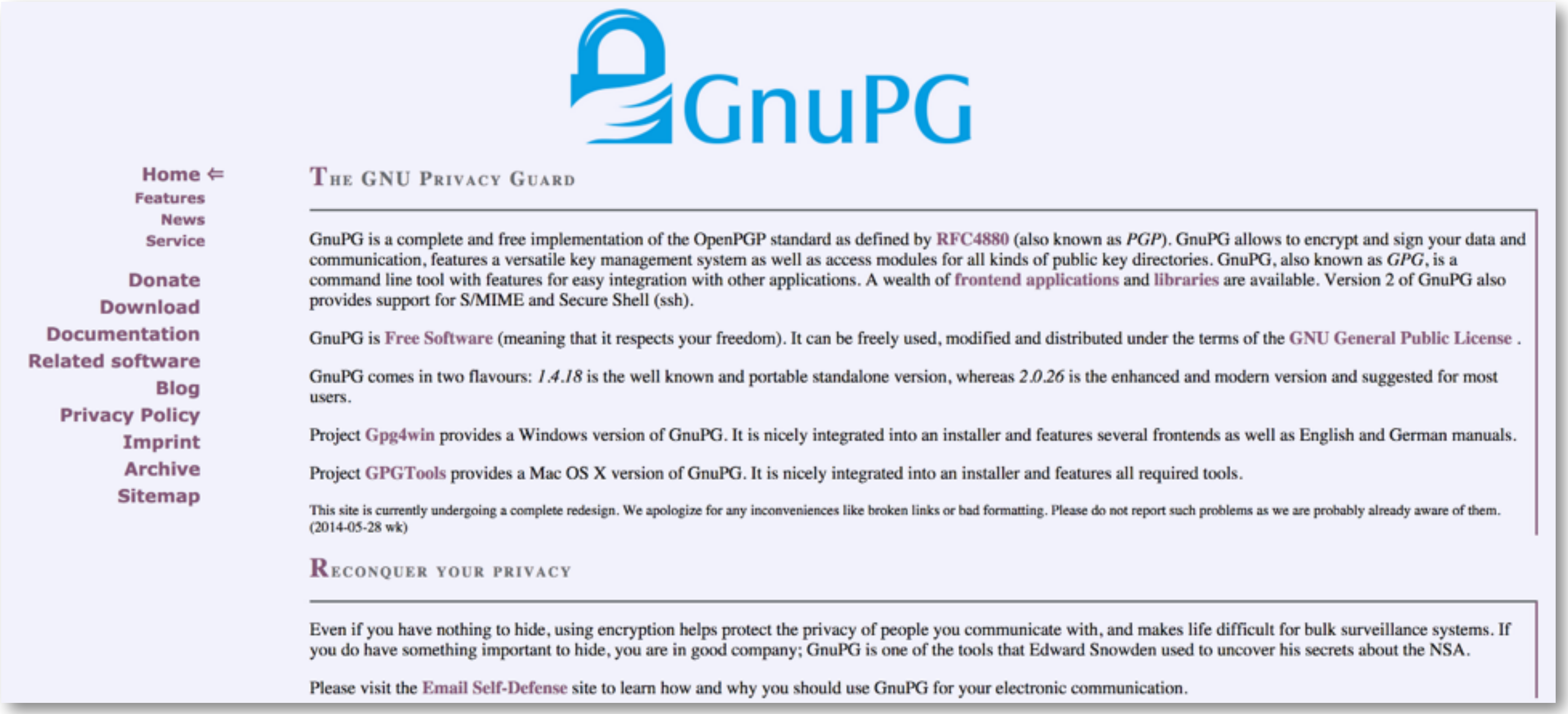
www.moserware.com/2009/06/first-few-milliseconds-of-https.html

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG/MacGPG2 v2.0.22 (Darwin)
Comment: GPGTools - https://gpgtools.org

mQINBFMnXY4BEACt8c+S5UfOo3t1YdLy5yEdgTebwDH+lwzsILsyBc1i28gWh12S
gc6yJRr65jumPVh7A8RxdOtvn2g7cwuuYpIlFKNhL3KSCzfGQfrbX0QlYbr9J+hz
DpS0crQoTHgOZpy/HAbb1VduGGuWP7Jox0ijvbU+crbSLNZmB4Ixj/lB5cvv8aMX
CyEosDRPGNXW1Coj3QqhSOrOqgQUxXNjarodVwmTaDQnAAzKAno7qVfRfoXxjkDd
nzMw+BKeU1E+CEJ4Yg1pFPHG8P2CmQjQtPKbGc8px5hPPOdEebodSyLffHbguPyF
jFW2YbN8U6uRbiaYVbmpTxGgi07fQ+CWX6L8HBuFiwMsAMiEdQLDe6siSJ9gw3SF

... (45 lines omitted) ...

gZI88DByix/qRUTdETCKex2sZXuu+UxWG/HTGgAfDHO60Z59ZOt9zaG8gbpgJ0+9
0c/Xfsr9GgcfhYXikcJR3DD21z/EqftVed9HIzFZudCg7RbZHYXhfAGWsIcRWHh0
tDagPY38rSs1g4MpwT4iNjzhhahN04Sd3mrQoz4vUA9J7H++vrvxSDCsipC4+zHB
+pi8rmIDaeKQHPxH0wY1vcFTC6EzNJ8HU9mj1Sj7s4gcgL8APHaH5K1BB5srQEN4
B37dYbON/5HBL962g+ZUBjKs87UPNoyqe3jn5AA9AlKMOyz5ZusNbUlcw4DVRue7
fRBhWSIZ7DkpTYEBejvyepWf6UAgI26xiG5ZhDQcPzg=
=eaPK
-----END PGP PUBLIC KEY BLOCK-----
```

An OpenPGP public key ("ASCII-armored" form)

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG/MacGPG2 v2.0.22 (Darwin)
Comment: GPGTools - https://gpgtools.org

hQIMAwkuBalYH40qAQ/+J5NzcRNBdhcfipIzDal4cFEgvtfjFLvrEHMaWZn51h5m
EceX+ittkZNwOsDcTacyp2dnIzduqjShFN9Um7eLdkc1G1zENyyvasreB5G2IIMn
IRBCBxPC0nfnFpk+M/KrUCU3yl3oiBebtSwbIKhXsO9ujcWWp5x8uOfM4NcROKVa
HibbtE6YI+t0oZc9+BvidkiCQIZnwbG7Vojg8cNgXQXaFHLYsIS5dXQwVcfG5g4P
fI8qTcFtWNe6x4C3gE25Ztt5xim9JGOrYDpP1jy3FOKfVv7kp9qSz3+69cEFZLG3
1J7hznY4HxHiv0J+TtNtZvPNPs1zq4KDwtZxPA7/qCsayFYBGF2ivw6d6kPOuZZV
E0kMHfSVSygSIkd2FAeLfVWCdPQaWvJr/diahu0+B1Bg6xmt7uqPccaiZ043Kmf3
q/KLADE5e9FDLVs6rOSfwnR7szDUxCUWQBxCzLTH6aZKQSzf3LG/nJkSUOrWUXiO
eHRcujIgjsXDRS8KyVCLMdpcd4za3ndcGxcHbH8eIEik1GjmyoxMYRxIAOw7Cqj0
STLFqHmB0pXKhx23iUrKC0+ivAOVpMEtbjWxeEE1HkV8u5sNkA9d4OHyjuoMLpaW
aa0rsD6LTRF2lsEMtSM5WBHbeplMYinv7fPnFGjM19flc5loFX6SuhnfUxOJ5D3S
SQFdX9omfQWrmGnI/8zv9/z4zkRswv0pD6qGepFaTrcFTieHnnieYogH7E3/n0eW
UIFZkbw/3thlwZ4b6uwDro/26y5ovCayB80=
=9CtG
-----END PGP MESSAGE-----
```

An OpenPGP message



The GNU Privacy Guard

GnuPG is a complete and free implementation of the OpenPGP standard as defined by RFC4880 (also known as *PGP*). GnuPG allows to encrypt and sign your data and communication, features a versatile key management system as well as access modules for all kinds of public key directories. GnuPG, also known as *GPG*, is a command line tool with features for easy integration with other applications. A wealth of frontend applications and libraries are available. Version 2 of GnuPG also provides support for S/MIME and Secure Shell (ssh).

GnuPG is Free Software (meaning that it respects your freedom). It can be freely used, modified and distributed under the terms of the GNU General Public License .

GnuPG comes in two flavours: *1.4.18* is the well known and portable standalone version, whereas *2.0.26* is the enhanced and modern version and suggested for most users.

Project Gpg4win provides a Windows version of GnuPG. It is nicely integrated into an installer and features several frontends as well as English and German manuals.

Project GPGTools provides a Mac OS X version of GnuPG. It is nicely integrated into an installer and features all required tools.

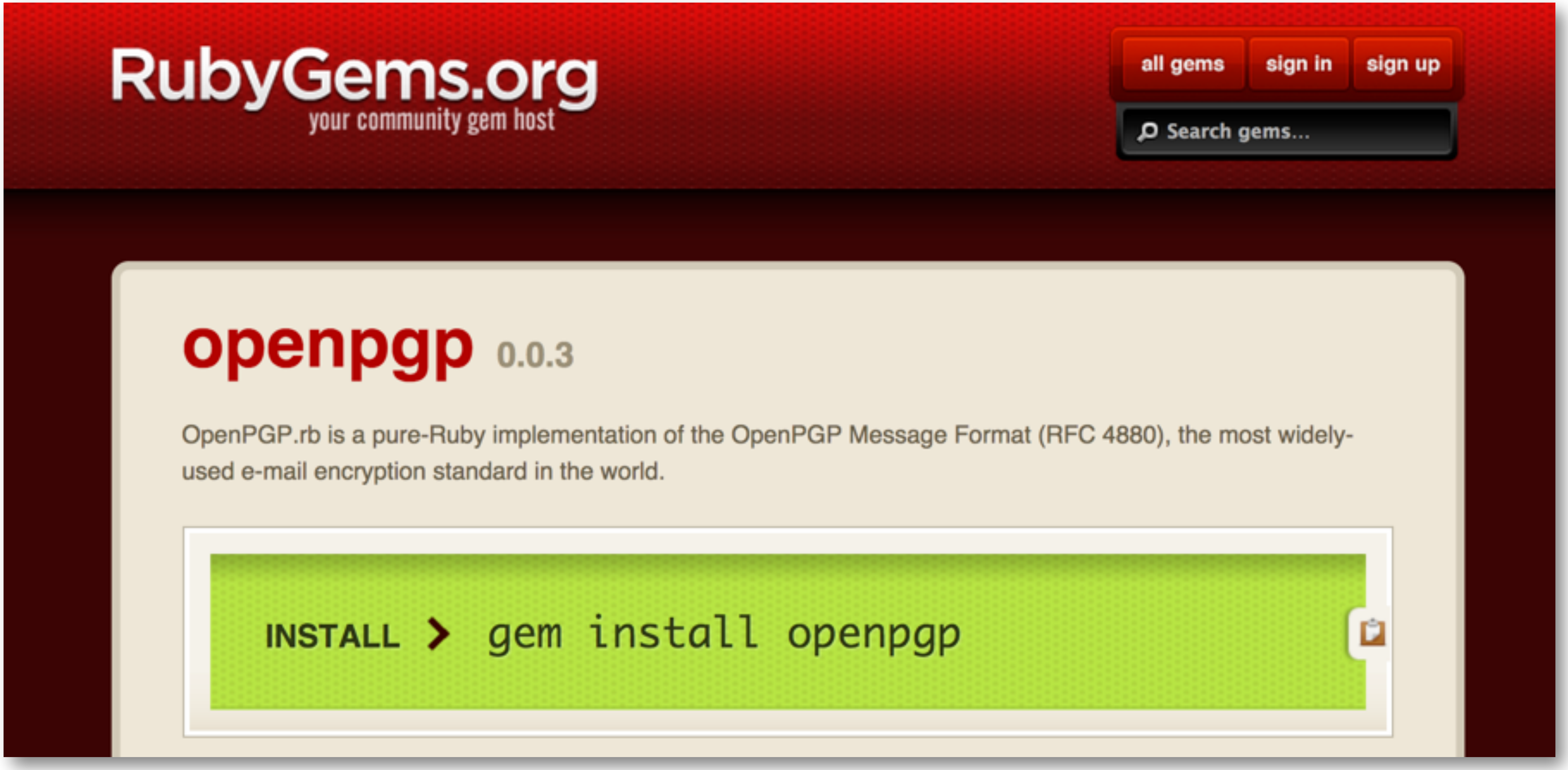
This site is currently undergoing a complete redesign. We apologize for any inconveniences like broken links or bad formatting. Please do not report such problems as we are probably already aware of them. (2014-05-28 wk)

Reconquer your privacy

Even if you have nothing to hide, using encryption helps protect the privacy of people you communicate with, and makes life difficult for bulk surveillance systems. If you do have something important to hide, you are in good company; GnuPG is one of the tools that Edward Snowden used to uncover his secrets about the NSA.

Please visit the Email Self-Defense site to learn how and why you should use GnuPG for your electronic communication.

www.gnupg.org

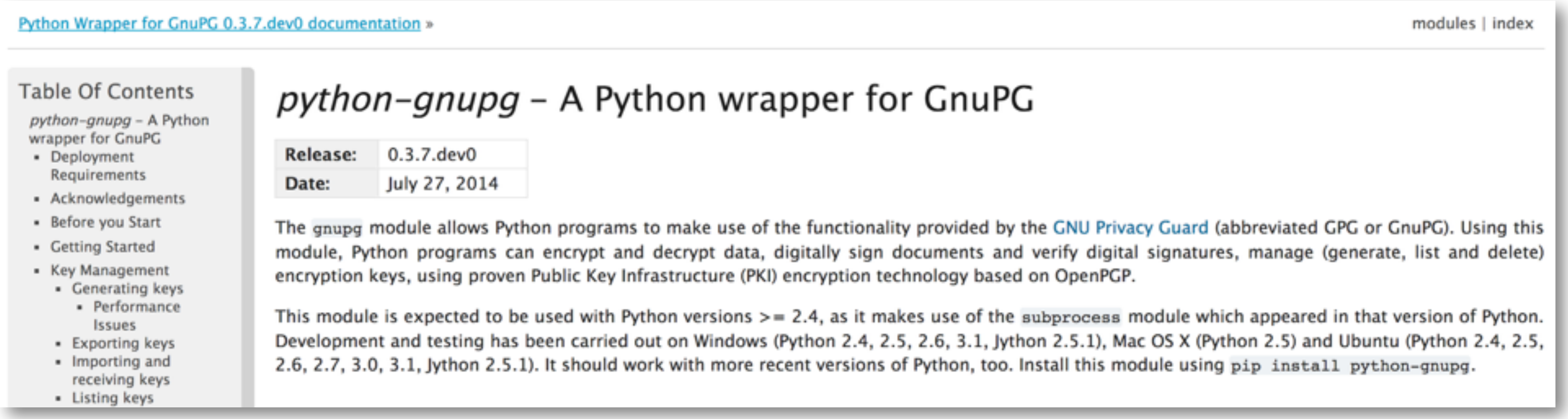


openpgp 0.0.3

OpenPGP.rb is a pure-Ruby implementation of the OpenPGP Message Format (RFC 4880), the most widely-used e-mail encryption standard in the world.

```
INSTALL > gem install openpgp
```

rubygems.org/gems/openpgp



Python Wrapper for GnuPG 0.3.7.dev0 documentation »

modules | index

Table Of Contents

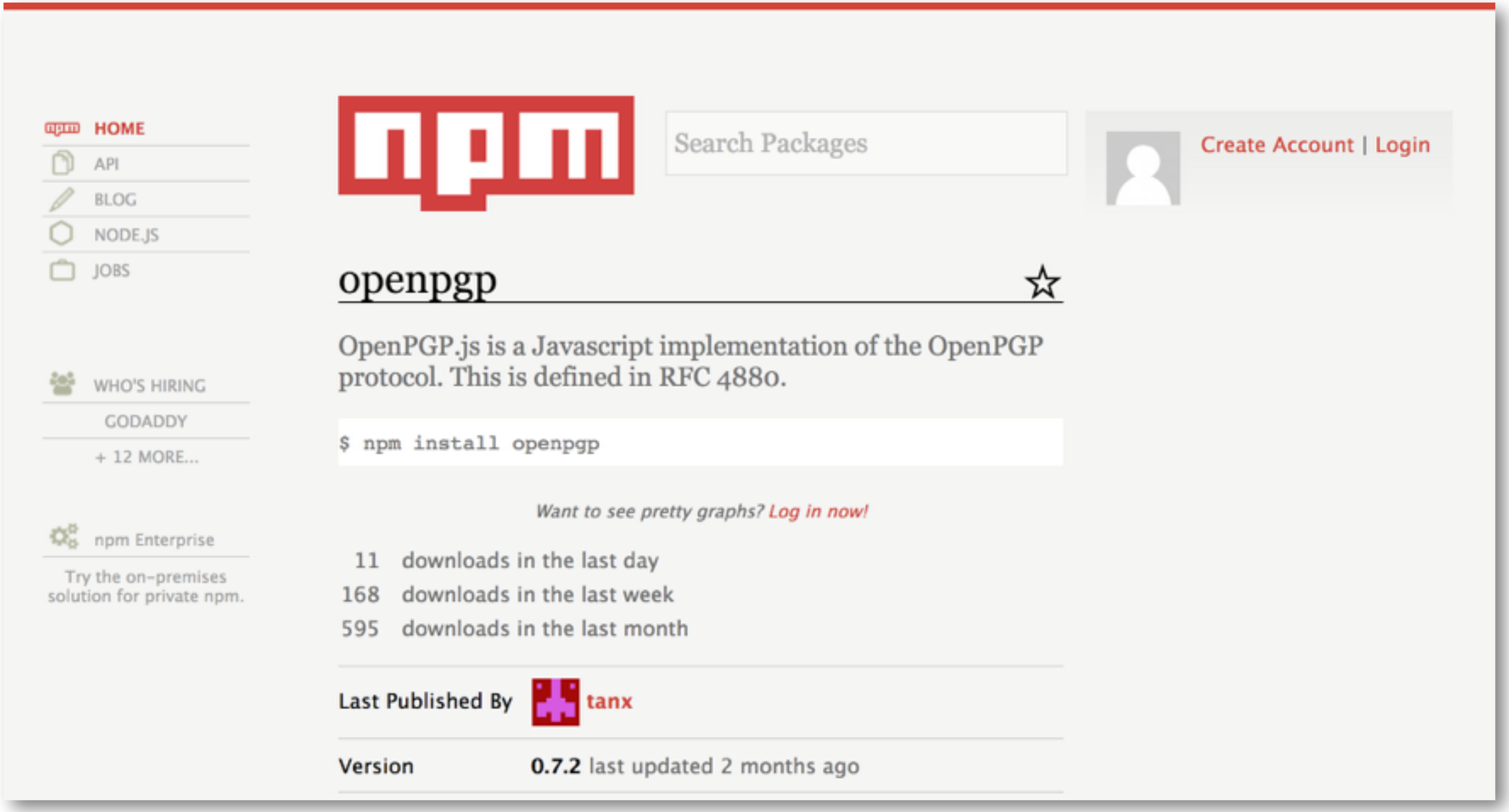
python-gnupg – A Python wrapper for GnuPG

Release:	0.3.7.dev0
Date:	July 27, 2014

The `gnupg` module allows Python programs to make use of the functionality provided by the GNU Privacy Guard (abbreviated GPG or GnuPG). Using this module, Python programs can encrypt and decrypt data, digitally sign documents and verify digital signatures, manage (generate, list and delete) encryption keys, using proven Public Key Infrastructure (PKI) encryption technology based on OpenPGP.

This module is expected to be used with Python versions >= 2.4, as it makes use of the `subprocess` module which appeared in that version of Python. Development and testing has been carried out on Windows (Python 2.4, 2.5, 2.6, 3.1, Jython 2.5.1), Mac OS X (Python 2.5) and Ubuntu (Python 2.4, 2.5, 2.6, 2.7, 3.0, 3.1, Jython 2.5.1). It should work with more recent versions of Python, too. Install this module using `pip install python-gnupg`.

pythonhosted.org/python-gnupg



openpgp ☆

OpenPGP.js is a Javascript implementation of the OpenPGP protocol. This is defined in RFC 4880.

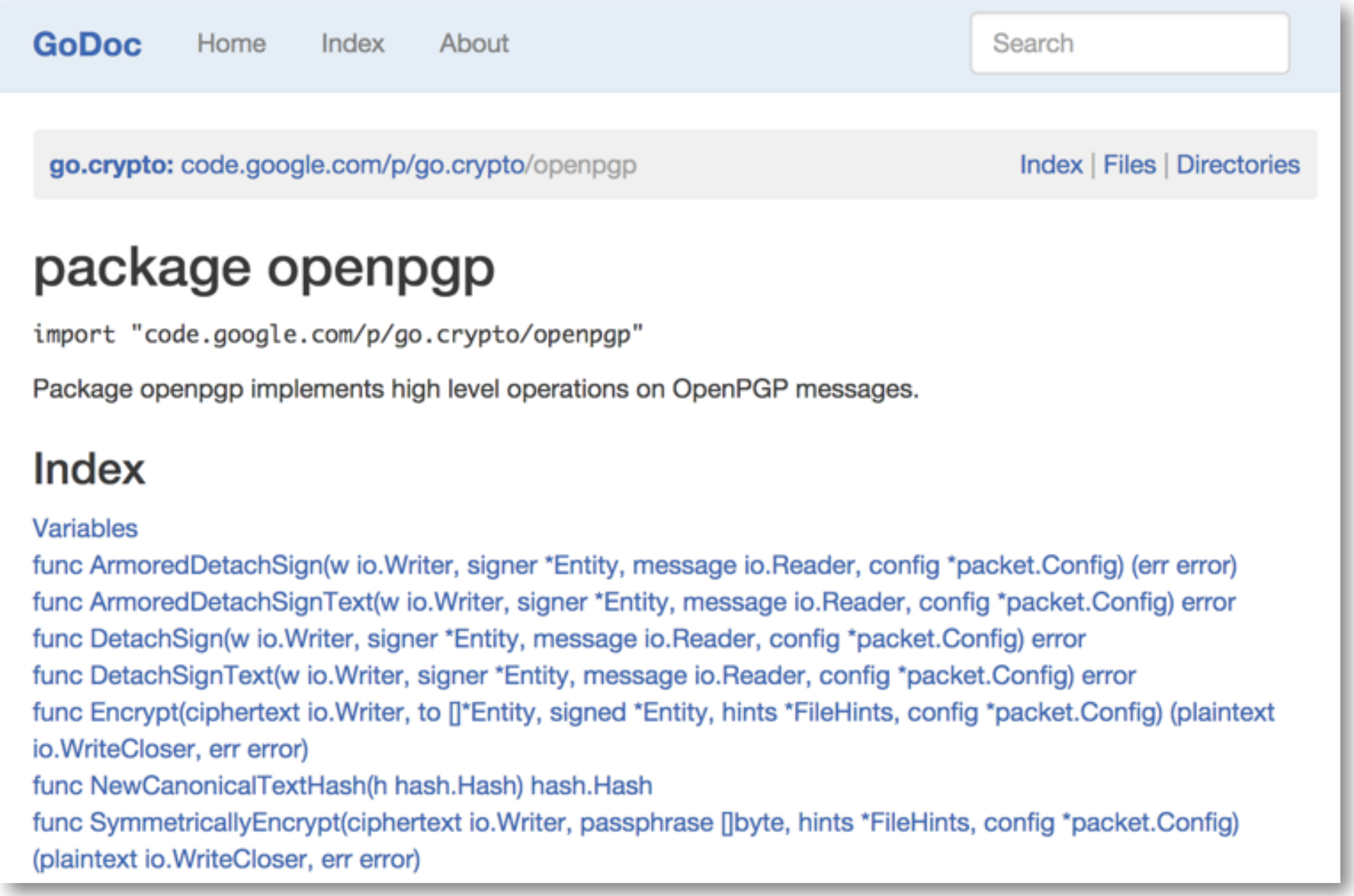
```
$ npm install openpgp
```

Want to see pretty graphs? Log in now!

```
 11  downloads in the last day
168  downloads in the last week
595  downloads in the last month
```

Last Published By	tanx
Version	**0.7.2** last updated 2 months ago

www.npmjs.org/package/openpgp



go.crypto: code.google.com/p/go.crypto/openpgp

package openpgp

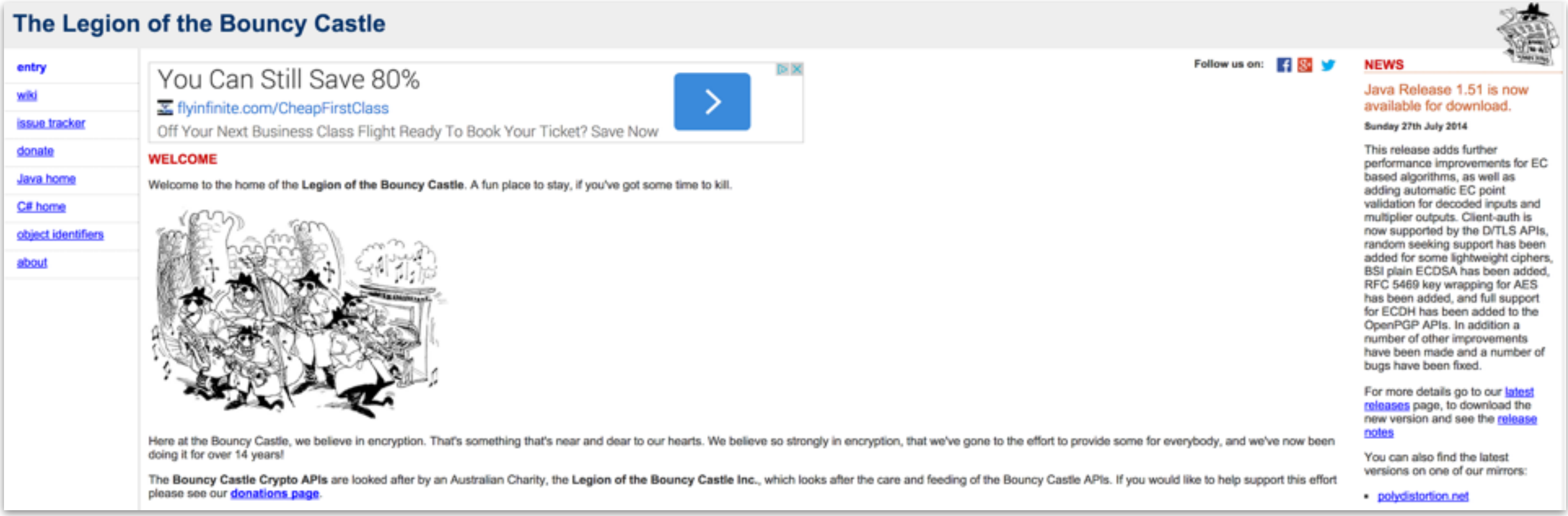
```
import "code.google.com/p/go.crypto/openpgp"
```

Package openpgp implements high level operations on OpenPGP messages.

Index

Variables
func ArmoredDetachSign(w io.Writer, signer *Entity, message io.Reader, config *packet.Config) (err error)
func ArmoredDetachSignText(w io.Writer, signer *Entity, message io.Reader, config *packet.Config) error
func DetachSign(w io.Writer, signer *Entity, message io.Reader, config *packet.Config) error
func DetachSignText(w io.Writer, signer *Entity, message io.Reader, config *packet.Config) error
func Encrypt(ciphertext io.Writer, to []*Entity, signed *Entity, hints *FileHints, config *packet.Config) (plaintext io.WriteCloser, err error)
func NewCanonicalTextHash(h hash.Hash) hash.Hash
func SymmetricallyEncrypt(ciphertext io.Writer, passphrase []byte, hints *FileHints, config *packet.Config) (plaintext io.WriteCloser, err error)

godoc.org/code.google.com/p/go.crypto/openpgp



The Legion of the Bouncy Castle

WELCOME

Welcome to the home of the **Legion of the Bouncy Castle**. A fun place to stay, if you've got some time to kill.

Here at the Bouncy Castle, we believe in encryption. That's something that's near and dear to our hearts. We believe so strongly in encryption, that we've gone to the effort to provide some for everybody, and we've now been doing it for over 14 years!

The **Bouncy Castle Crypto APIs** are looked after by an Australian Charity, the **Legion of the Bouncy Castle Inc.**, which looks after the care and feeding of the Bouncy Castle APIs. If you would like to help support this effort please see our donations page.

NEWS

Java Release 1.51 is now available for download.

Sunday 27th July 2014

This release adds further performance improvements for EC based algorithms, as well as adding automatic EC point validation for decoded inputs and multiplier outputs. Client-auth is now supported by the D/TLS APIs, random seeking support has been added for some lightweight ciphers, BSI plain ECDSA has been added, RFC 5469 key wrapping for AES has been added, and full support for ECDH has been added to the OpenPGP APIs. In addition a number of other improvements have been made and a number of bugs have been fixed.

For more details go to our latest releases page, to download the new version and see the release notes

You can also find the latest versions on one of our mirrors:

- polydistortion.net

www.bouncycastle.org

Making Crypto Useful

You need to be able to:

1. Get your own keys, and store them.
2. Move them around, desktop to mobile.
3. Find other people's public keys.
4. Have good tools to encrypt/sign messages…
5. … and decrypt/verify them.

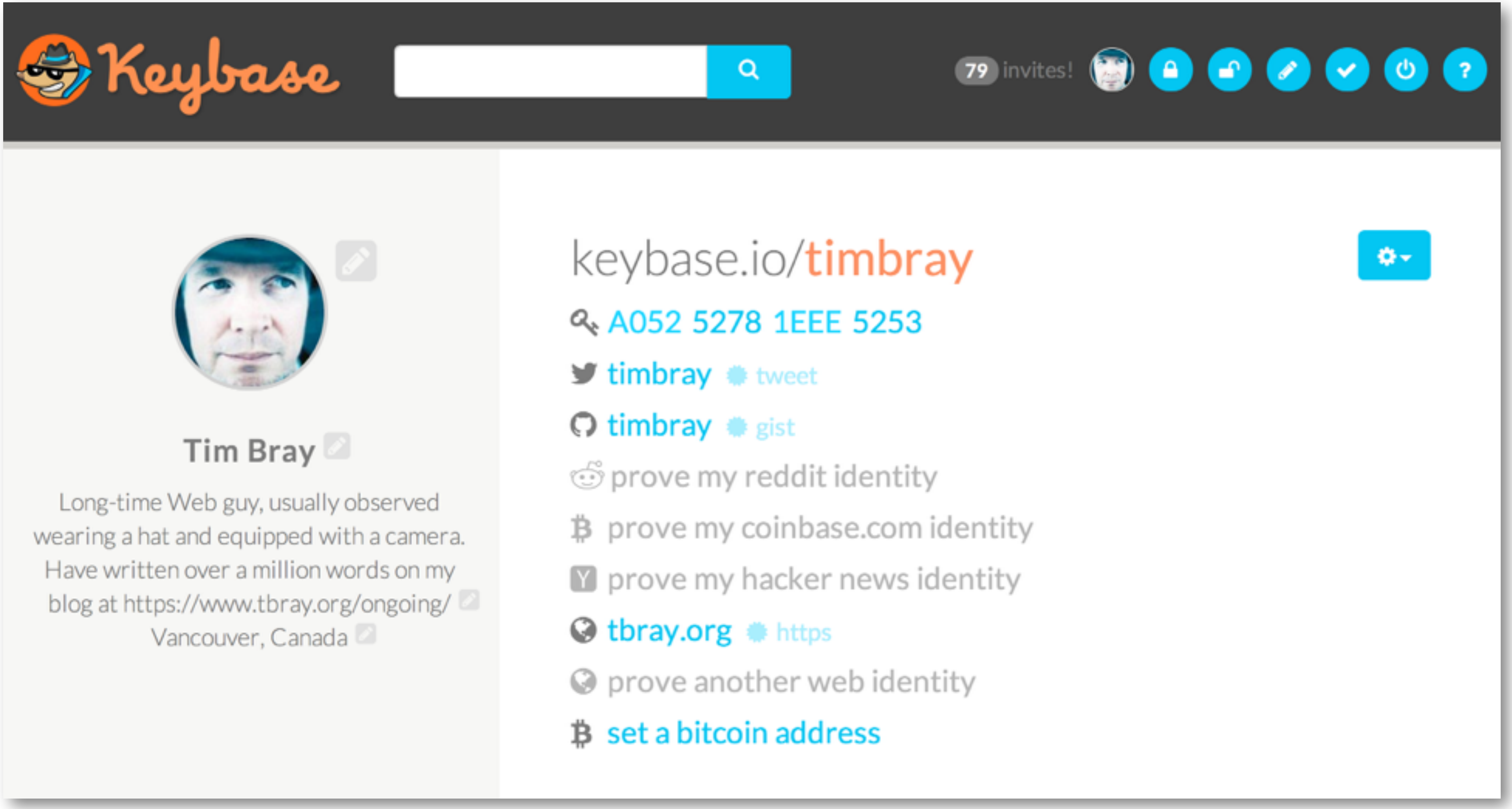
Without ever seeing a hex digit or needing to understand how keys work.

Making Crypto Useful

You need to be able to:

1. Get your own keys, and store them.
2. Move them around, desktop to mobile.
3. Find other people’s public keys.
4. Have good tools to encrypt/sign messages…
5. … and decrypt/verify them.

Without ever seeing a hex digit or needing to understand how keys work.



Tim Bray

Long-time Web guy, usually observed wearing a hat and equipped with a camera. Have written over a million words on my blog at https://www.tbray.org/ongoing/

Vancouver, Canada

keybase.io/timbray

A052 5278 1EEE 5253

timbray tweet

timbray gist

prove my reddit identity

prove my coinbase.com identity

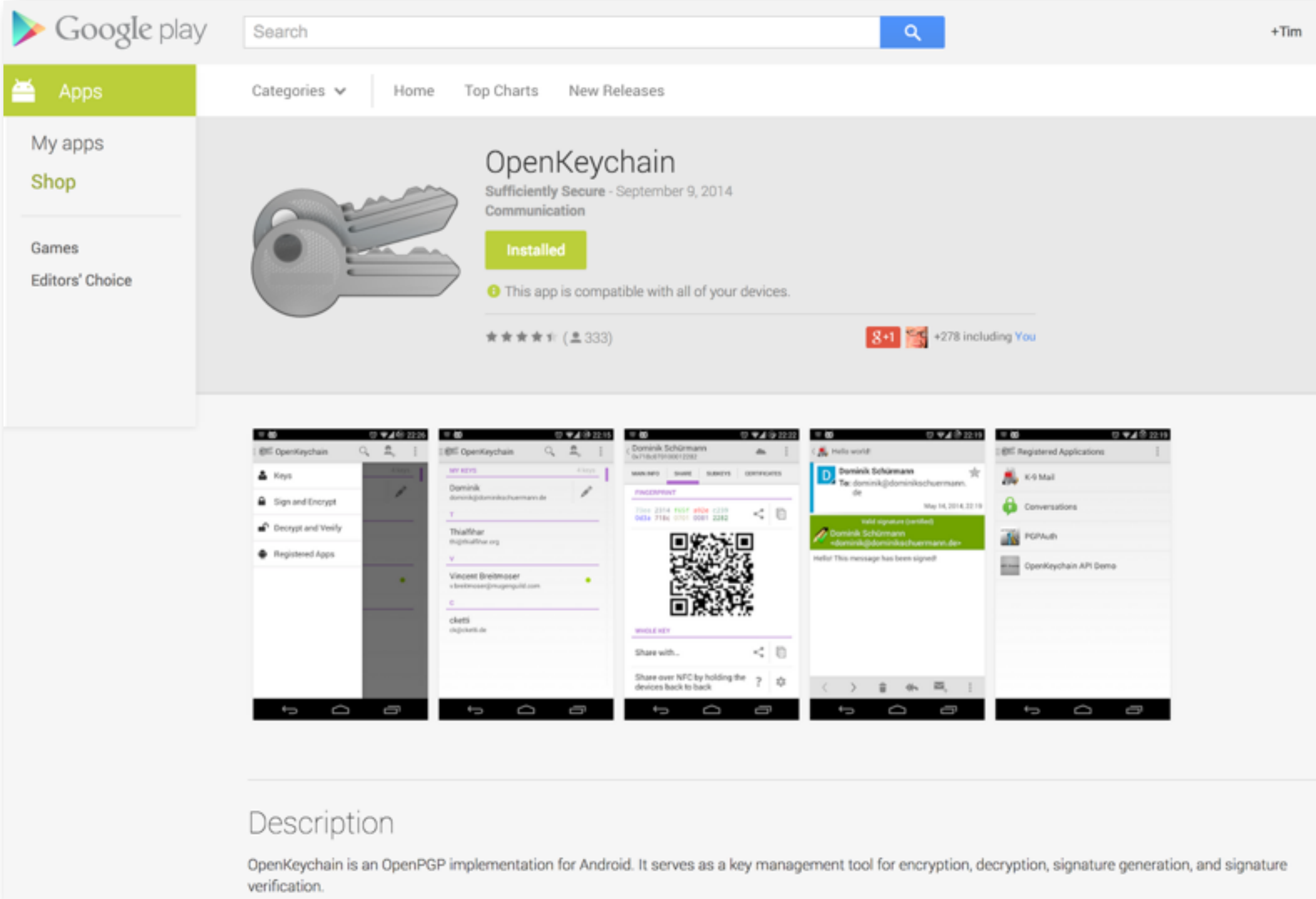
prove my hacker news identity

tbray.org https

prove another web identity

set a bitcoin address

keybase.io/timbray



OpenKeychain

Sufficiently Secure - September 9, 2014

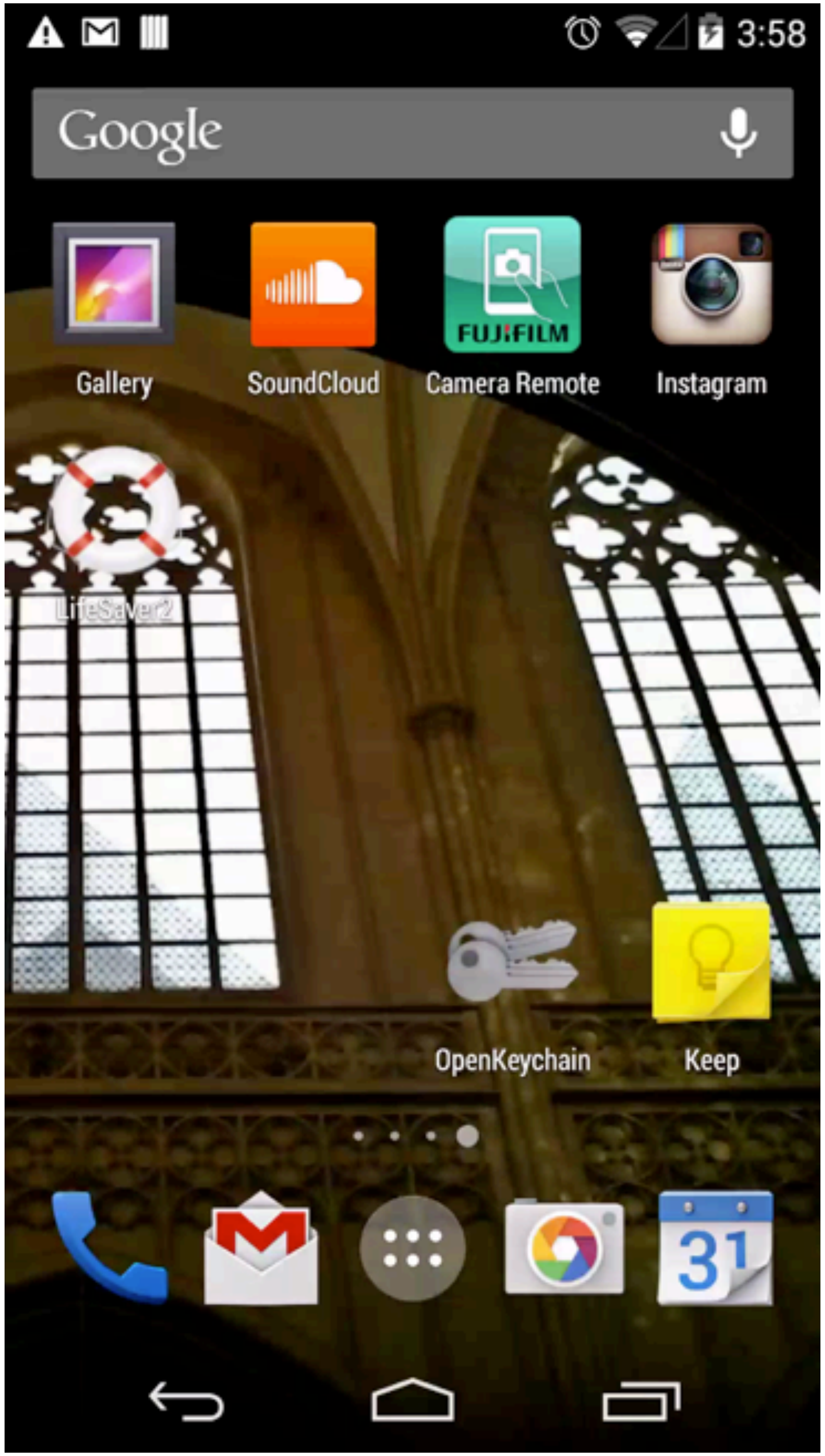
Communication

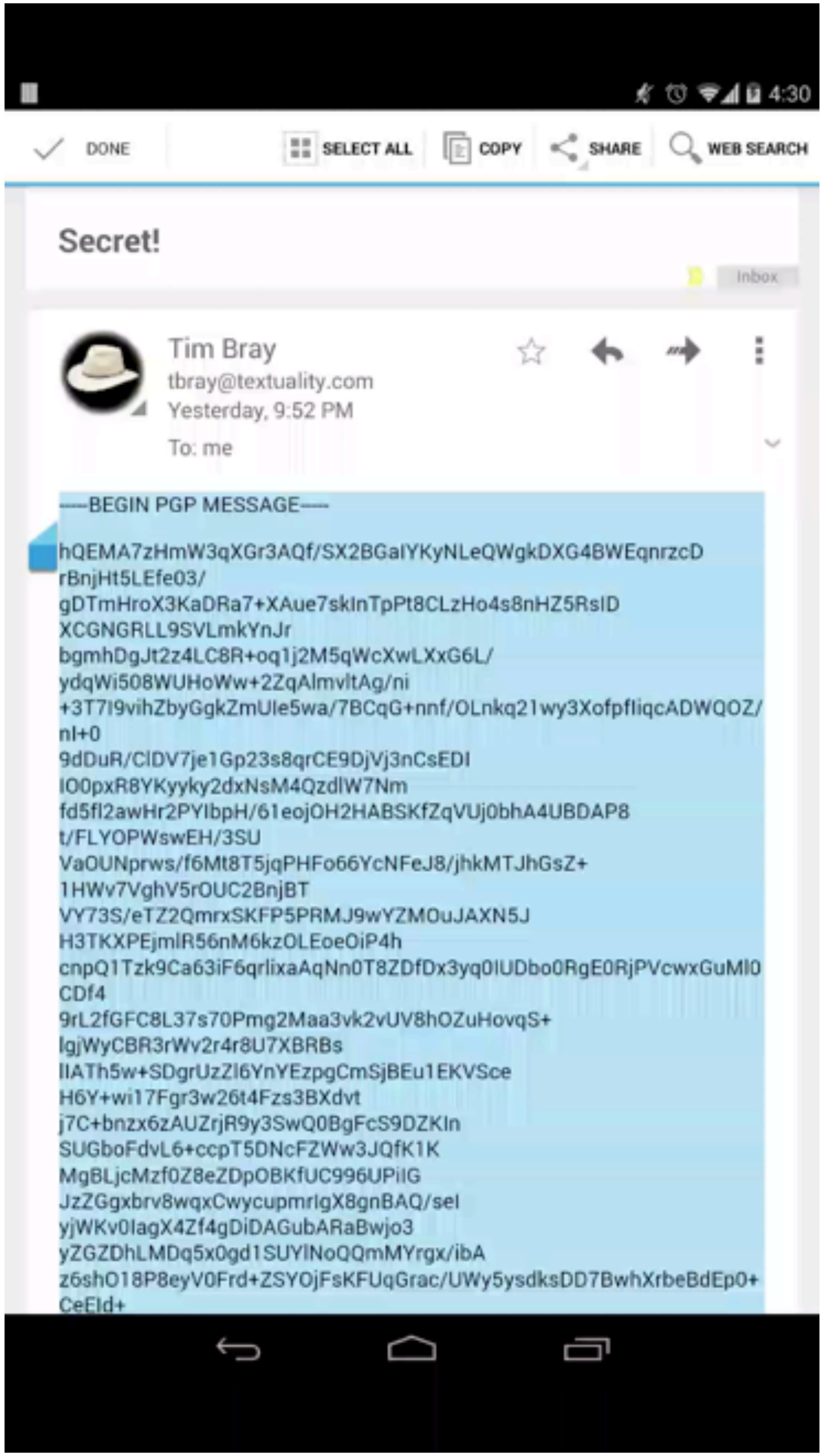
This app is compatible with all of your devices.

Description

OpenKeychain is an OpenPGP implementation for Android. It serves as a key management tool for encryption, decryption, signature generation, and signature verification.

play.google.com/store/apps/details?id=org.sufficientlysecure.keychain


3:58
Google
Gallery
SoundCloud
FUJIFILM
Camera Remote
Instagram
LifeSaver2
OpenKeychain
Keep
31



Secret!

Tim Bray
tbray@textuality.com
Yesterday, 9:52 PM
To: me

-----BEGIN PGP MESSAGE-----

hQEMA7zHmW3qXGr3AQf/SX2BGaIYKyNLeQWgkDXG4BWEqnrzcD
rBnjHt5LEfe03/
gDTmHroX3KaDRa7+XAue7skInTpPt8CLzHo4s8nHZ5RsID
XCGNGRLL9SVLmkYnJr
bgmhDgJt2z4LC8R+oq1j2M5qWcXwLXxG6L/
ydqWi508WUHoWw+2ZqAlmvltAg/ni
+3T7I9vihZbyGgkZmUle5wa/7BCqG+nnf/OLnkq21wy3XofpfliqcADWQOZ/
nl+0
9dDuR/ClDV7je1Gp23s8qrCE9DjVj3nCsEDI
IO0pxR8YKyyky2dxNsM4QzdlW7Nm
fd5fl2awHr2PYIbpH/61eojOH2HABSKfZqVUj0bhA4UBDAP8
t/FLYOPWswEH/3SU
VaOUNprws/f6Mt8T5jqPHFo66YcNFeJ8/jhkMTJhGsZ+
1HWv7VghV5rOUC2BnjBT
VY73S/eTZ2QmrxSKFP5PRMJ9wYZMOuJAXN5J
H3TKXPEjmlR56nM6kzOLEoeOiP4h
cnpQ1Tzk9Ca63iF6qrlixaAqNn0T8ZDfDx3yq0IUDbo0RgE0RjPVcwxGuMl0
CDf4
9rL2fGFC8L37s70Pmg2Maa3vk2vUV8hOZuHovqS+
lgjWyCBR3rWv2r4r8U7XBRBs
lIATh5w+SDgrUzZl6YnYEzpgCmSjBEu1EKVSce
H6Y+wi17Fgr3w26t4Fzs3BXdvt
j7C+bnzx6zAUZrjR9y3SwQ0BgFcS9DZKIn
SUGboFdvL6+ccpT5DNcFZWw3JQfK1K
MgBLjcMzf0Z8eZDpOBKfUC996UPiIG
JzZGgxbrv8wqxCwycupmrlgX8gnBAQ/seI
yjWKv0IagX4Zf4gDiDAGubARaBwjo3
yZGZDhLMDq5x0gd1SUYlNoQQmMYrgx/ibA
z6shO18P8eyV0Frd+ZSYOjFsKFUqGrac/UWy5ysdksDD7BwhXrbeBdEp0+
CeEld+