

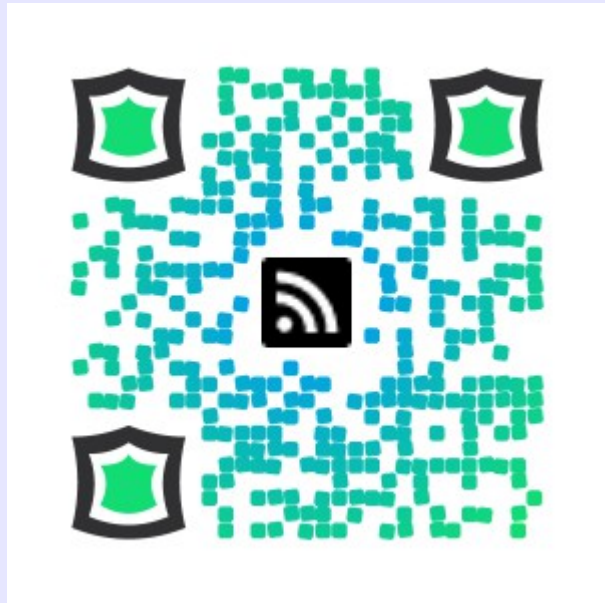
MAKING

SECURITY

SHINY

Tom Webster


"SamuraiLink3"



 SamuraiLink3.com

 SamuraiLink3@gmail.com

 Gplus.to/samurailink3

 @SamuraiLink3



DISCLAIMER

This isn't about the security of the following products, just how the interface and user experience is implemented. Certain providers in the list have had major demonstrated downfalls, attacks, and general laziness when it comes to implementing good crypto, they are here to serve as an example of how to provide a user interface, nothing more. Don't hurt me.

Most security
programs look like
this:


```

09.2012 C:\Windows\system32\DriverStore\FileRepository\ssndar9.inf_amd64_neutral_9090002af3859502
09.2012 C:\Windows\system32\DriverStore\FileRepository\ssndar9.inf_amd64_neutral_9090002af3859502
11.2012 23:28 <DIR> 11 895 sscendm.cat
11.2012 C:\Windows\system32\DriverStore\FileRepository\ssudbus.inf_amd64_neutral_929a4fd844c62452\amd64
09.2012 23:28 <DIR> em33D543es0e6mdnFileRepository\ssudbhexidffand64neutral1281B5273972828363
09.2012 23:28 <DIR> 180 360 ssdddnetsys
09.2012 23:28 <DIR> 1 499 858 5dd6adnetapi01007.dll
09.2012 23:28 fil(er) 1 499 858 5dd6adnetapi01007.dll
09.2012 C:\Windows\system32\DriverStore\FileRepository\ssudbhexidffand64neutral1281B5273972828363
09.2012 C:\Windows\system32\DriverStore\FileRepository\ssudrmnetmp.inf_amd64_neutral_4013e05387653236\amd64
09.2012 C:\Windows\system32\DriverStore\FileRepository\ssudmgr.inf_amd64_neutral_72d76636ff3ae722\amd64
09.2012 C:\Windows\system32\DriverStore\FileRepository\ssudmgr.inf_amd64_neutral_72d76636ff3ae722\amd64
11.2012 23:28 <DIR> 118 944 amd64df.sys
11.2012 23:28 fil(er) 1 499 858 5dd6adnetapi01007.dll
09.2012 23:28 fil(er) 1 499 858 5dd6adnetapi01007.dll
09.2012 C:\Windows\system32\DriverStore\FileRepository\ssudbhexidffand64neutral1281B5273972828363
09.2012 C:\Windows\system32\DriverStore\FileRepository\ssudbhexidffand64neutral1281B5273972828363
09.2012 C:\Windows\system32\DriverStore\FileRepository\ssudbhexidffand64neutral1281B5273972828363
11.2012 C:\Windows\system32\DriverStore\FileRepository\ssudmgr.inf_amd64_neutral_72d76636ff3ae722\amd64
11.2012 C:\Windows\system32\DriverStore\FileRepository\ssudmgr.inf_amd64_neutral_72d76636ff3ae722\amd64
11.2012 23:28 <DIR> 20 302 ssdddnetsys
11.2012 23:28 <DIR> 122 804 ssdddnetsys
09.2012 23:28 fil(er) 1 499 858 5dd6adnetapi01007.dll
09.2012 C:\Windows\system32\DriverStore\FileRepository\ssudbhexidffand64neutral1281B5273972828363
09.2012 C:\Windows\system32\DriverStore\FileRepository\ssudbhexidffand64neutral1281B5273972828363
11.2012 23:28 <DIR> ..
11.2012 C:\Windows\system32\DriverStore\FileRepository\ssudbhexidffand64neutral1281B5273972828363
11.2012 23:28 <DIR> 12 360 ssdddnetsys
09.2012 23:28 <DIR> 122 804 ssdddnetsys
09.2012 23:28 fil(er) 1 499 858 5dd6adnetapi01007.dll
09.2012 23:28 fil(er) 1 499 858 5dd6adnetapi01007.dll
09.2012 C:\Windows\system32\DriverStore\FileRepository\ssudbhexidffand64neutral1281B5273972828363
09.2012 C:\Windows\system32\DriverStore\FileRepository\ssudbhexidffand64neutral1281B5273972828363
11.2012 23:28 <DIR> ..
11.2012 23:28 <DIR> 69 223 ssdddnetsys
09.2012 23:28 <DIR> 1 499 858 5dd6adnetapi01007.dll
09.2012 23:28 fil(er) 1 499 858 5dd6adnetapi01007.dll
09.2012 23:28 fil(er) 1 499 858 5dd6adnetapi01007.dll
09.2012 C:\Windows\system32\DriverStore\FileRepository\ssudbhexidffand64neutral1281B5273972828363
09.2012 C:\Windows\system32\DriverStore\FileRepository\ssudbhexidffand64neutral1281B5273972828363
11.2012 23:28 <DIR> ..

```


Or this:

AC N°1

OFF AUTO SERVICE SERVICE OUT OF SERVICE WASHING WASH FAILED WAITING LOSS OF HEAD

FILTER No.1

INLET VALVE OUTLET VALVE AIRSCOUR VALVE WASH OUTLET VALVE
OPEN - OFF - CLOSE OPEN - OFF - CLOSE OPEN - OFF - CLOSE OPEN - OFF - CLOSE

FILTER No.1

INLET VALVE OUTLET VALVE AIRSCOUR VALVE BACKWASHING VALVE WASH OUTLET VALVE
OPEN - OFF - CLOSE OPEN - OFF - CLOSE OPEN - OFF - CLOSE OPEN - OFF - CLOSE OPEN - OFF - CLOSE

OUT OF SERVICE WASHING WASH FAILED WAITING LOSS OF HEAD TURBIDITY TIME ELAPSED

AIRSCOUR VALVE BACKWASHING VALVE
OPEN - OFF - CLOSE OPEN - OFF - CLOSE

PLC OFF AUTO SERVICE SERVICE OUT OF SERVICE WASHING WASH FAILED WAITING LOSS OF HEAD TURBIDITY TIME ELAPSED

AC N°2

OFF AUTO SERVICE SERVICE OUT OF SERVICE WASHING WASH FAILED WAITING LOSS OF HEAD

FILTER No.2

INLET VALVE OUTLET VALVE AIRSCOUR VALVE WASH OUTLET VALVE
OPEN - OFF - CLOSE OPEN - OFF - CLOSE OPEN - OFF - CLOSE OPEN - OFF - CLOSE

FILTER No.2

INLET VALVE OUTLET VALVE AIRSCOUR VALVE BACKWASHING VALVE WASH OUTLET VALVE
OPEN - OFF - CLOSE OPEN - OFF - CLOSE OPEN - OFF - CLOSE OPEN - OFF - CLOSE OPEN - OFF - CLOSE

PLC OFF AUTO SERVICE SERVICE OUT OF SERVICE WASHING WASH FAILED WAITING LOSS OF HEAD TURBIDITY TIME ELAPSED

AIRSCOUR VALVE BACKWASHING VALVE
OPEN - OFF - CLOSE OPEN - OFF - CLOSE

PLC OFF AUTO SERVICE SERVICE OUT OF SERVICE WASHING WASH FAILED WAITING LOSS OF HEAD TURBIDITY TIME ELAPSED

AC N°3

OFF AUTO SERVICE SERVICE OUT OF SERVICE WASHING WASH FAILED WAITING LOSS OF HEAD

FILTER No.3

INLET VALVE OUTLET VALVE AIRSCOUR VALVE WASH OUTLET VALVE
OPEN - OFF - CLOSE OPEN - OFF - CLOSE OPEN - OFF - CLOSE OPEN - OFF - CLOSE

FILTER No.3

INLET VALVE OUTLET VALVE AIRSCOUR VALVE BACKWASHING VALVE WASH OUTLET VALVE
OPEN - OFF - CLOSE OPEN - OFF - CLOSE OPEN - OFF - CLOSE OPEN - OFF - CLOSE OPEN - OFF - CLOSE

AIRSCOUR VALVE BACKWASHING VALVE
OPEN - OFF - CLOSE OPEN - OFF - CLOSE

BORNEHOLZ V00011 POWERMILL RES. V00012 BORWELL RES. V00013 FLOW TO CLEAR WATER TANK V00014 PLC MANUAL

BACKWASH MANUAL INITIATION

CHEMICAL STORAGE TANKS ISOLATORS
FERRIC TANK N°1 - TANK N°2 SODIUM HYPOSULFITE TANK N°1 - TANK N°3 SULPHURIC ACID TANK N°1 - TANK N°2 SUPPLY HEALTHY LAMP TEST

THIS

IS

A

PROBLEM

WHY DO WE CARE?



With the advent of the Snowden leaks, people are finally starting to take security seriously.

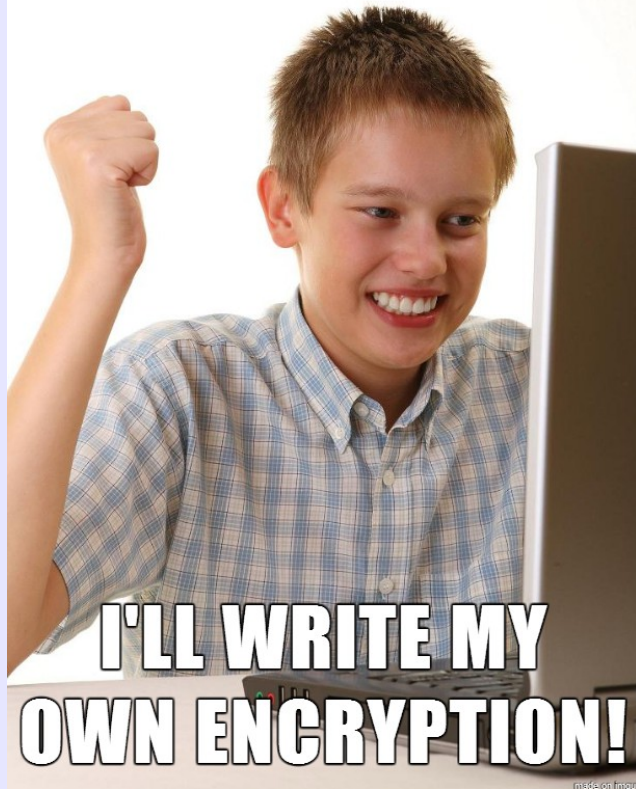
We're about to see a major influx of 'security' apps/programs/sites/oils that a pretty to look at, easy to use, and, best of all, utterly ineffective or **malicious**.

People are going to create 'security' applications and market them to the general public like we've never seen before.

WHY DO WE CARE?

Including these guys:

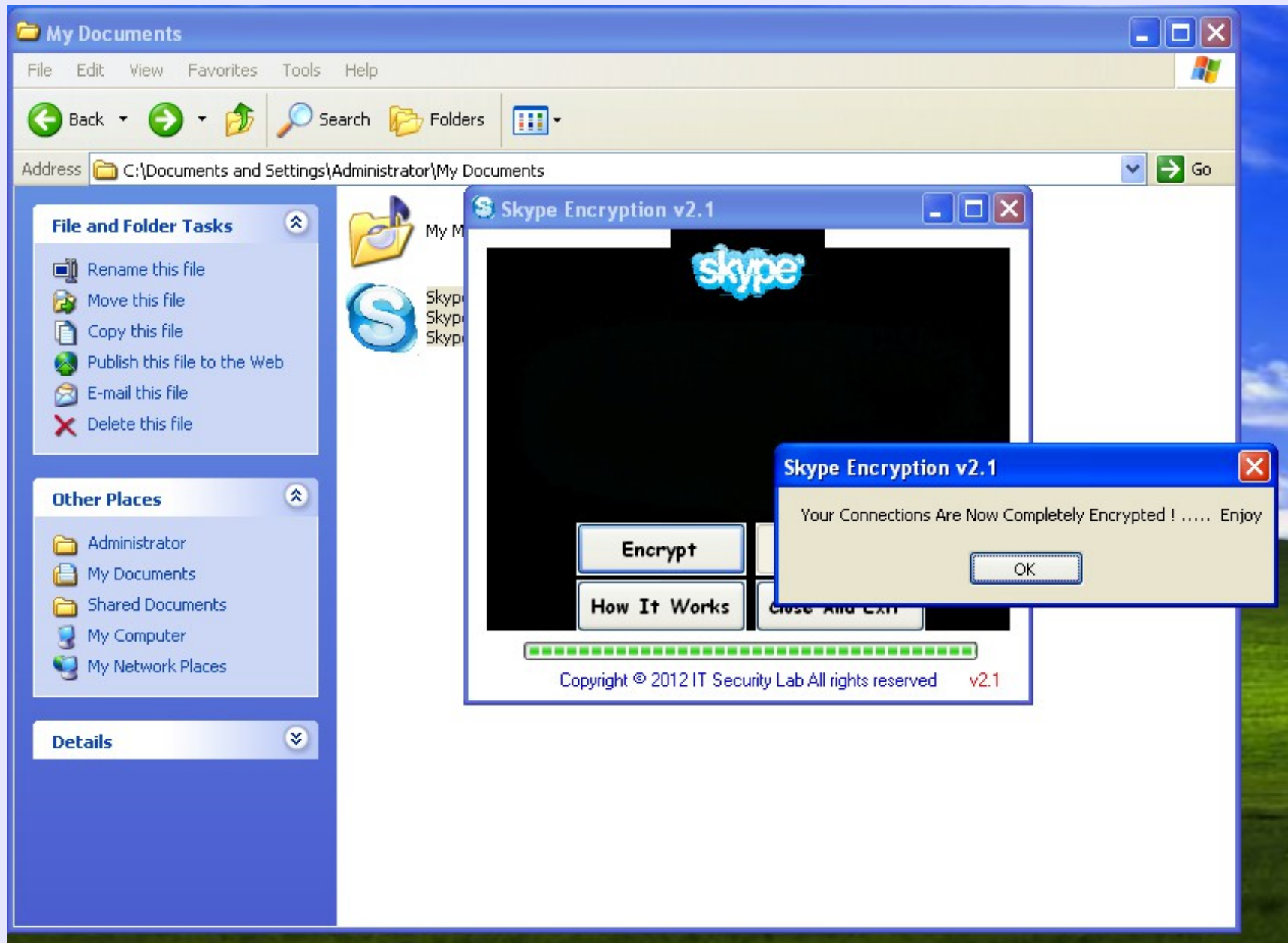
NSA SPYING?



Reality: These guys will sell and give away a lot of software to our mothers and co-workers.

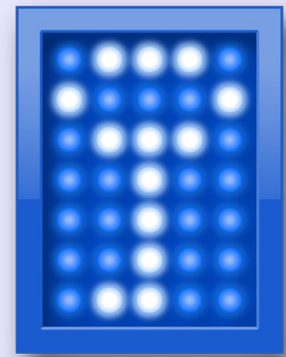
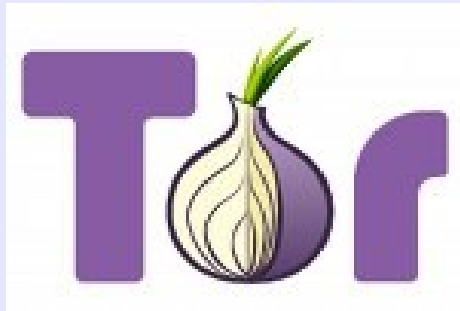
WHY DO WE CARE?

This is already happening:



WHY DO WE CARE?

Let's make sure the real champions stay on top:



WHAT CAN

WE DO?



MAKE



MAKE

SECURITY



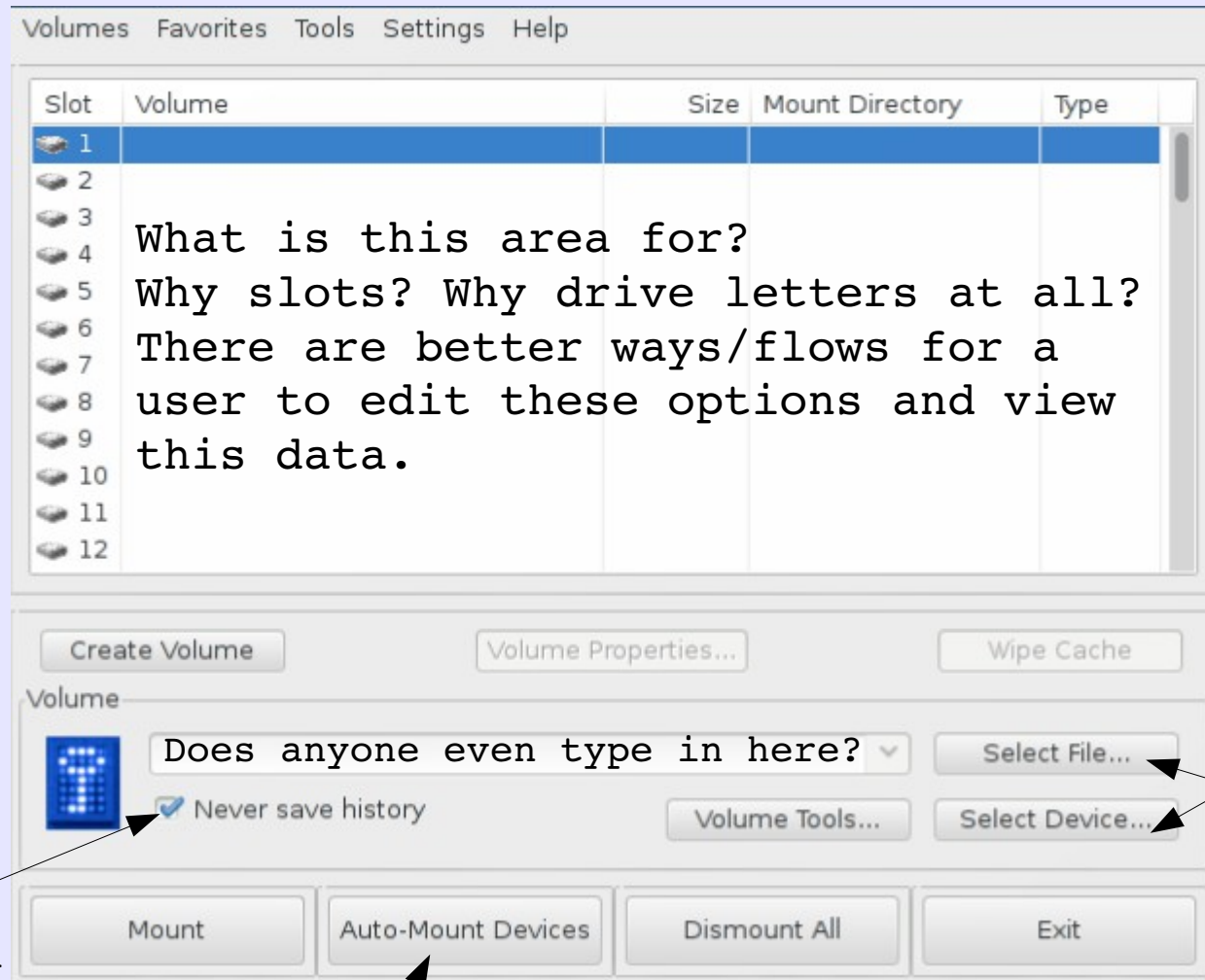
MAKE

SECURITY

SHINY

EXAMPLES

TrueCrypt



Why is this even an option?

This should be a hidden option.

Redundant:
This choice should present itself after 'Mount' is clicked.

Errata:

Bad:

- Very text heavy
- Language, language, language.
- In your applications:
Talk to people, not security auditors
- In your documentation:
Talk to security auditors, user's don't read anything anyway...
- 'Easy buttons' don't exist.

Good:

- Wizard for volume creation is good.

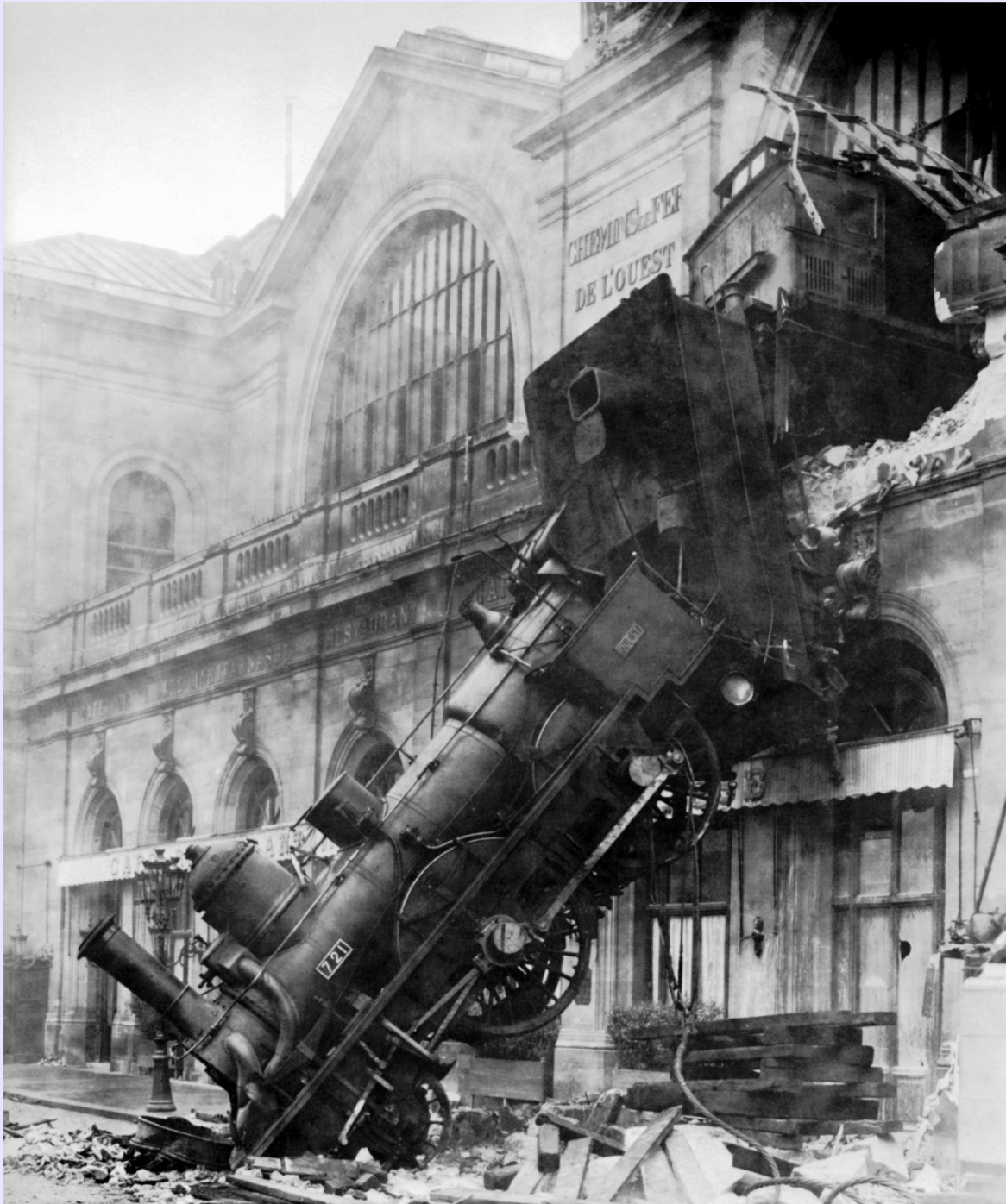
LESSONS LEARNED

1. BE UP FRONT

2. USE PLAIN LANGUAGE

EXAMPLES

GPG



EXAMPLES

GPG

```
C:\Windows\system32\cmd.exe
C:\Users\Admin>gpg --help
gpg (GnuPG) 2.0.22 <Gpg4win 2.2.1>
libgcrypt 1.5.3
Copyright (C) 2013 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Home: C:\Users\Admin\AppData\Roaming\gnupg
Supported algorithms:
Pubkey: RSA, ELG, DSA, ?, ?
Cipher: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH,
        CAMELLIA128, CAMELLIA192, CAMELLIA256
Hash: MD5, SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
Compression: Uncompressed, ZIP, ZLIB, BZIP2

Syntax: gpg [options] [files]
Sign, check, encrypt or decrypt
Default operation depends on the input data

Commands:

-s, --sign                make a signature
--clearsign              make a clear text signature
-b, --detach-sign         make a detached signature
-e, --encrypt             encrypt data
-c, --symmetric           encryption only with symmetric cipher
-d, --decrypt             decrypt data (default)
--verify                verify a signature
-k, --list-keys           list keys
--list-sigs              list keys and signatures
--check-sigs             list and check key signatures
--fingerprint            list keys and fingerprints
-K, --list-secret-keys   list secret keys
--gen-key               generate a new key pair
--gen-revoke            generate a revocation certificate
--delete-keys           remove keys from the public keyring
--delete-secret-keys    remove keys from the secret keyring
--sign-key              sign a key
--lsign-key             sign a key locally
--edit-key              sign or edit a key
--passwd               change a passphrase
--export               export keys
--send-keys            export keys to a key server
--recv-keys            import keys from a key server
--search-keys          search for keys on a key server
--refresh-keys         update all keys from a keyserver
--import               import/merge keys
--card-status          print the card status
--card-edit            change data on a card
--change-pin           change a card's PIN
--update-trustdb       update the trust database
--print-md             print message digests
--server              run in server mode

Options:

-a, --armor              create ascii armored output
-r, --recipient USER-ID encrypt for USER-ID
-u, --local-user USER-ID use USER-ID to sign or decrypt
-z N                    set compress level to N (<0 disables)
--textmode             use canonical text mode
-o, --output FILE       write output to FILE
-v, --verbose           verbose
-n, --dry-run          do not make any changes
-i, --interactive       prompt before overwriting
--openpgp              use strict OpenPGP behavior

(See the man page for a complete listing of all commands and options)
```

You're making this
too easy...

```
C:\Windows\system32\cmd.exe
C:\Users\Admin>gpg -a --clearsig

You need a passphrase to unlock the secret key for
user: "Tom Webster <samurailink3@gmail.com>"
2048-bit RSA key, ID 7B74B0AB, created 2013-10-09

Verify this message!
^Z
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Verify this message!
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2.0.22 (MingW32)

iQEcBAEBAgAGBQJSUe1ZAaoJEBLxikx7dLCr7cwH/izAY9x5RYQaRUZTLR7fpYCh
kJobjffITKpGqKfZQPAuJu2AUozm7e9BGIathA6IXcs4/m1ZA+L9TCo7AcEgoCuQU
/rphvAKtYU29S08d9rSm1keG8Ya0oKyQ8KaIX0XOYPLy+gaDp1+BULt8TH2nxZ37
DS0rUF7gWJGKUafneM/rKFe9sID2HJbDMBSUIkLIIP8pkqCrDmVY8Chuh2zzmKy
+x91H8LUA99RE1gt9ZMJoo3L7qvAdLgqrcASbOweLueELbY75msy7dGd7cXJw9c0
C32n/3vBpH+5N8ifUSp4EaC1+AYyR6zjFTDFN55TTS6ZD6K0SBaaLhsOMi/K3o=
=hmEv
-----END PGP SIGNATURE-----

C:\Users\Admin>
```


Errata:

Bad:

- Command Line
- Command Line
- Command Line

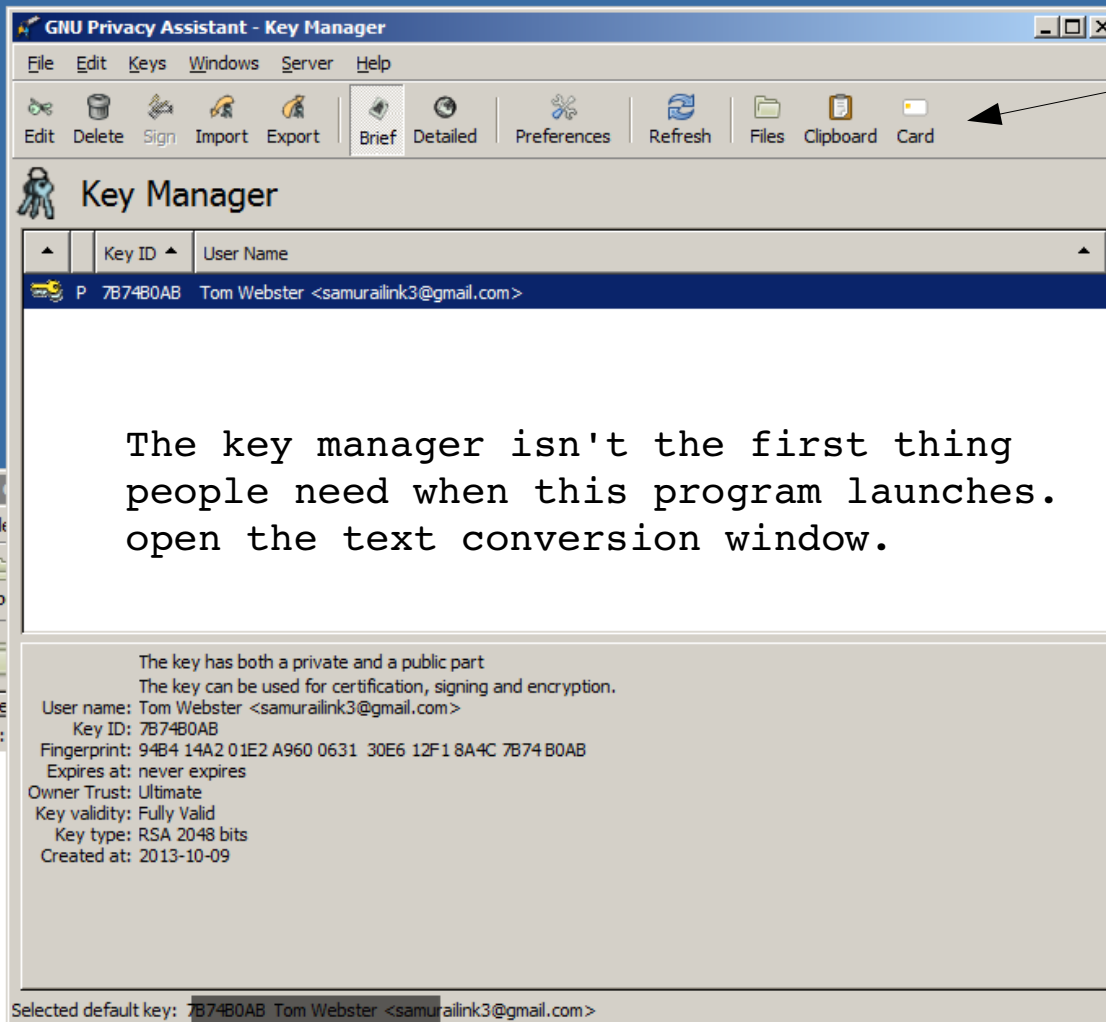
Good:

- Nothing. At all. Ever. Stop it.

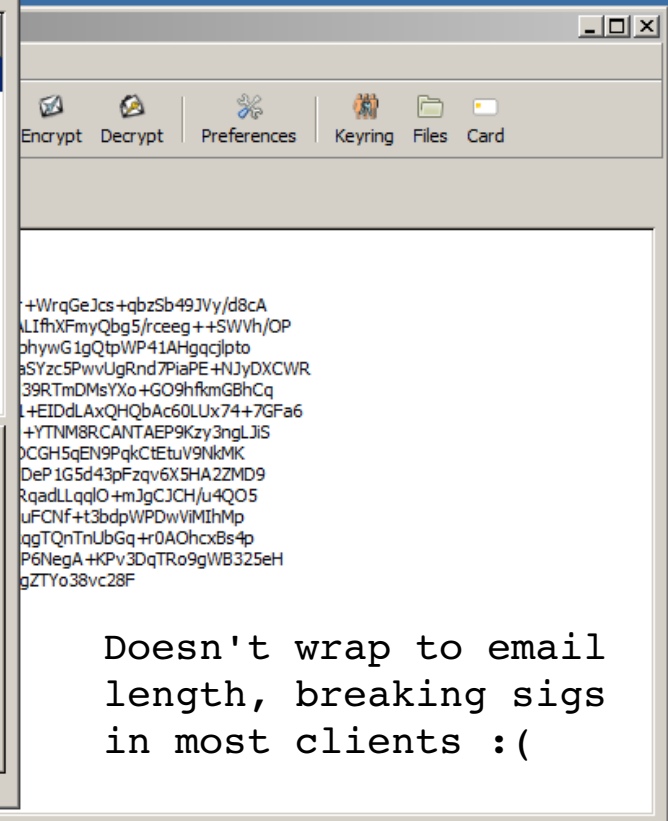
EXAMPLES

GPA

A 'little' better...



Not bad! Nicely labeled, not overly complex. Not bad at all.



There are better ways to do per-file encryption. Stop this madness.

Errata:

Bad:

- Looks like it's from 1996
- File encryption area confuses users and offers no explanations at all
- Key-manager-as-default puts off users who just want to send a secure message
- If you think this will copy/paste into an email client nicely, you're gonna have a bad time.

Good:

- The buttons up top are nice

LESSONS LEARNED

3. PEOPLE USE SOFTWARE.
DEVELOPERS USE LIBRARIES

EXAMPLES

SpiderOak

The screenshot displays the SpiderOak web interface. At the top, the username is 'samurailink3', the device is 'Manacotti', and the version is 'V. 5.0.2'. Navigation links for 'PREFERENCES', 'ACCOUNT', and 'HELP' are present. The main interface has tabs for 'STATUS', 'BACK UP', 'VIEW', 'SYNC', and 'SHARE'. Below these are sub-tabs: 'Overview', 'Queue', 'Actions', 'Log', and 'Stats'. A 'Pause All Uploads' button is also visible.

Devices

- Manacotti: 2.633 GB
- BWI LAPPY: 798.99 MB
- Debian Virtual (BWI): 9.08 MB
- Lasagna: 0 bytes

Network Health

Visual indicator showing 10 bars, with the first 8 being yellow and the last 2 being grey. Labels 'bad' and 'good' are at the ends.

Control Center

Connected

Last Scan:

BACK UP

Activity: Upload complete as of Wed Oct 9 20:07:34 2013
Currently Uploading: 0 items
Items Remaining: 0 items (0 bytes)
Backup Schedule: Frequency - Automatic

SYNC

Activity: Syncs Complete
of Syncs: 5
Sync Schedule: Frequency - On Backup Schedule

SHARE

Activity: No Shares Setup
of Shares: 0
Share Schedule: Frequency - On Backup Schedule

Storage Bar

Visual progress bar showing 3.441 GB used out of 7 GB total. A 'BUY MORE SPACE' button is on the right.

Legend: Desktop (red), Documents (orange), Movies (green), Pictures (purple), Unknown (grey)

Tip #4 - Secure - No one will ever know what data you are storing on your SpiderOak Network.

This one needs some conversation.

Errata:

Good:

- It looks pretty good
- It looks easy to use

Bad:

- It's a damn liar
- Uses confusing wording when setting up syncs or shares
- Offers little to no explanation of features in application
- You actually have to read the documentation on their site.

Like some sort of savage.

LESSONS LEARNED

4. NEVER BETRAY
EXPECTATIONS

5. DON'T TEACH UNLESS IT
OFFERS A CLEAR BENEFIT

EXAMPLES

LastPass



LastPass ****

URL:

Name: Group:

Username: Password:

[\[History\]](#) [\[History\]](#)

Notes:

This isn't my real password, guys... :P

I wish I could say something bad about this.. that eye icon isn't great... But honestly, now. Everything here is useful, uncomplicated, easy-to-understand, and friendly.

☒ Favorite ☐ Never AutoFill [Edit Form Fields](#)

☐ Require Password Reprompt ☒ AutoLogin

But...

EXAMPLES

LastPass

Edit Settings

General | Security | Equivalent Domains | Never URLs | Multifactor Options | Mobile Devices | Trusted Computers | URL Rules

Email: samurailink3@gmail.com [Test Email](#)

New Master Password: [Change Master Password](#) [Revert password change](#)

Password Reminder: No hints here, bub...

Password Iterations (PBKDF2): 10000 [Increase Iterations](#) 5000 recommended. [More](#)

Time Zone: (-05:00) Eastern Time (US & Canada)

Language: English

Website auto-logout timeout: 1 Hour website ONLY, extension auto-logout in [extension preferences](#)

Bookmarklet auto-logout timeout: 1 Day based on last login or last bookmarklet usage

☐ Only allow login from selected countries:

- ☒ United States
- ☐ Afghanistan
- ☐ Aland Islands
- ☐ Albania
- ☐ Algeria

☒ Disallow logins from [Tor network](#)

☒ Keep track of login and form fill history

☐ Kill other sessions on login. Must have 'polling' enabled in the plugins to be effective. [More](#)

☒ Send anonymous error reporting data to help improve LastPass

[Remove duplicate sites from your account](#)

[Cancel](#) [Update](#)

NO

Errata:

Good:

- Great password entry screen
- Simple, easy, to the point
- No overburdened with security jargon
- Technical details that crypto nerds care about is in the documentation.

Bad:

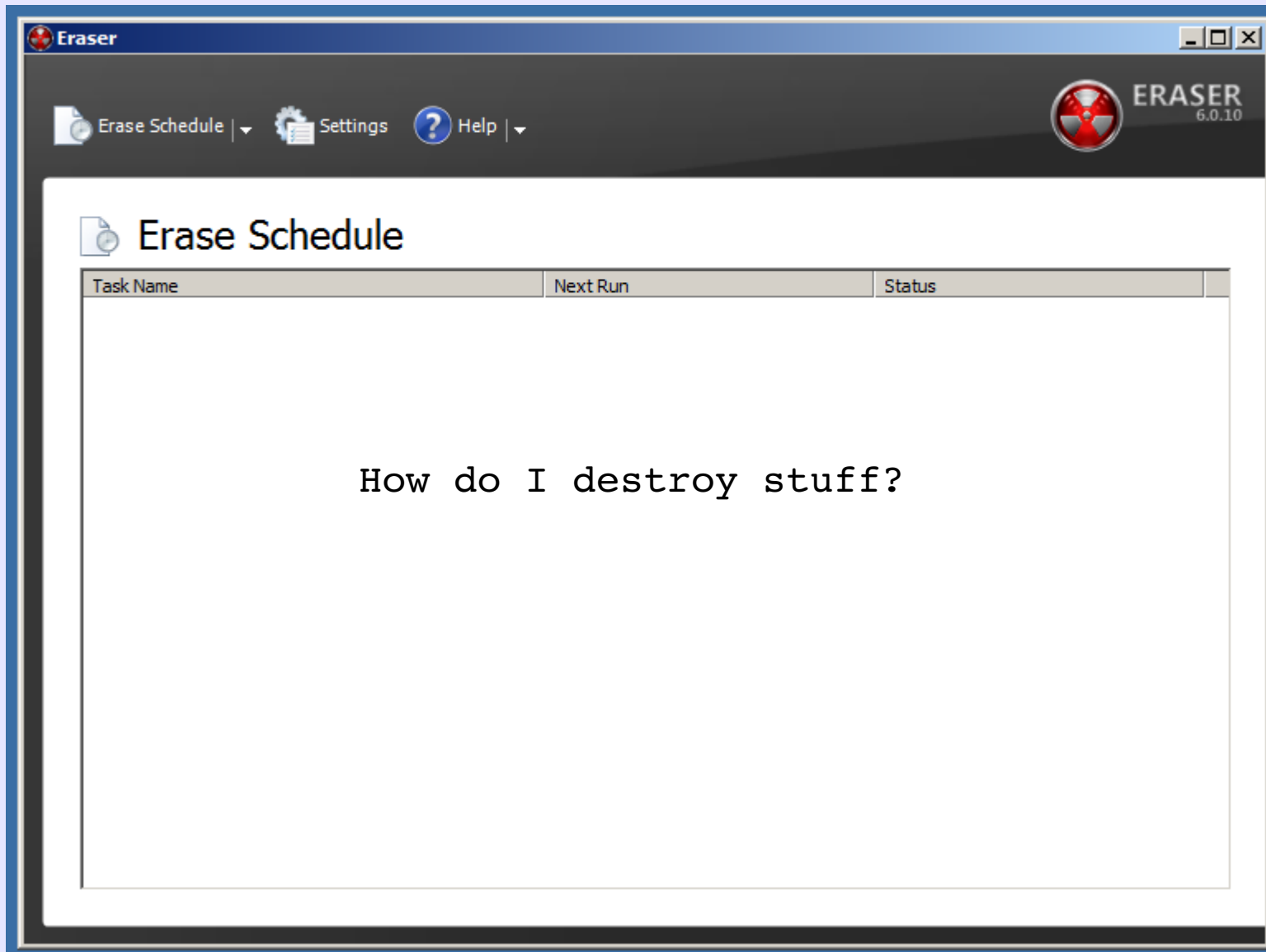
- Don't ever let the user hurt themselves. Ever. No matter what.
- Setting a low PBKDF2 value will make brute force attacks easier.
- If the recommendation is changed to a higher value than the user has set, no prompt or notification is issued.
- Be opinionated. Pick a value, use it.

LESSONS LEARNED

6. NEVER LET USERS HURT
THEMSELVES. EVER.

EXAMPLES

Eraser



Errata:

Good:

- Simplified Interface

Bad:

- Simplified in the exact wrong way
- 95% of your users want to do a simple thing quickly and easily. Enable that.
- Why put the scheduler first? Most people are looking to shred a single file.

LESSONS LEARNED

7. BUILD FOR THE 99%


EXAMPLES

Carbonite

Select your current computer or register a new one.

If you have registered this computer before, select it from the list. Otherwise select an empty tab and register a new computer.

New computer

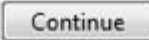



Name your computer:
BackupTest



Enter a key to use encryption:
Encryption key

Warning! Remember the key.
It cannot be restored.

Keep it simple. You could have pages upon pages of options and buttons here, but you don't need them. Most of your users don't want them. Be opinionated. Make the right choice for your user. Tuck your advanced options away.

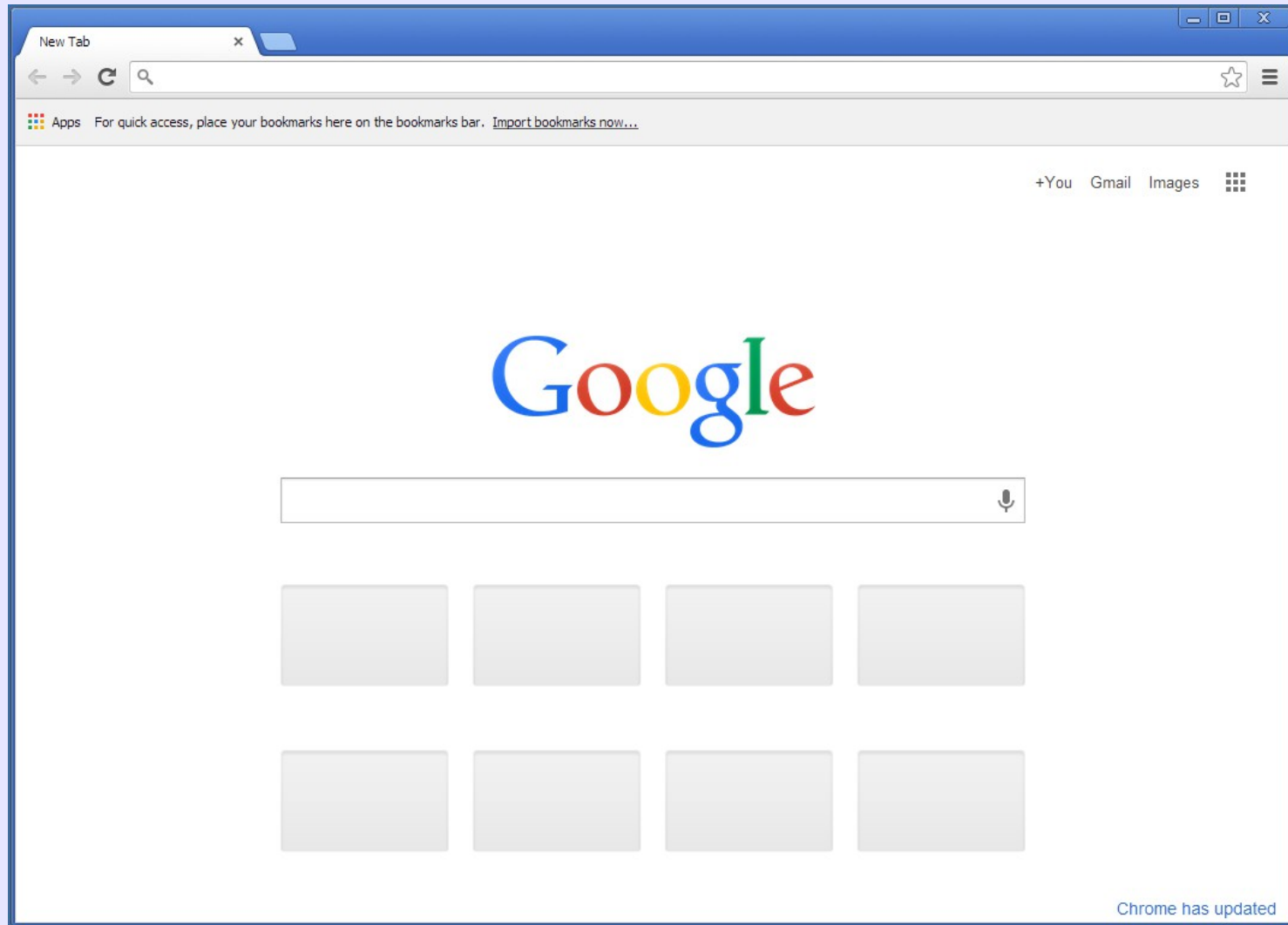
LESSONS LEARNED

8. MAKE OPINIONATED
SOFTWARE

EXAMPLES

Google Chrome

Possibly the best blend of prowess and usability out there.

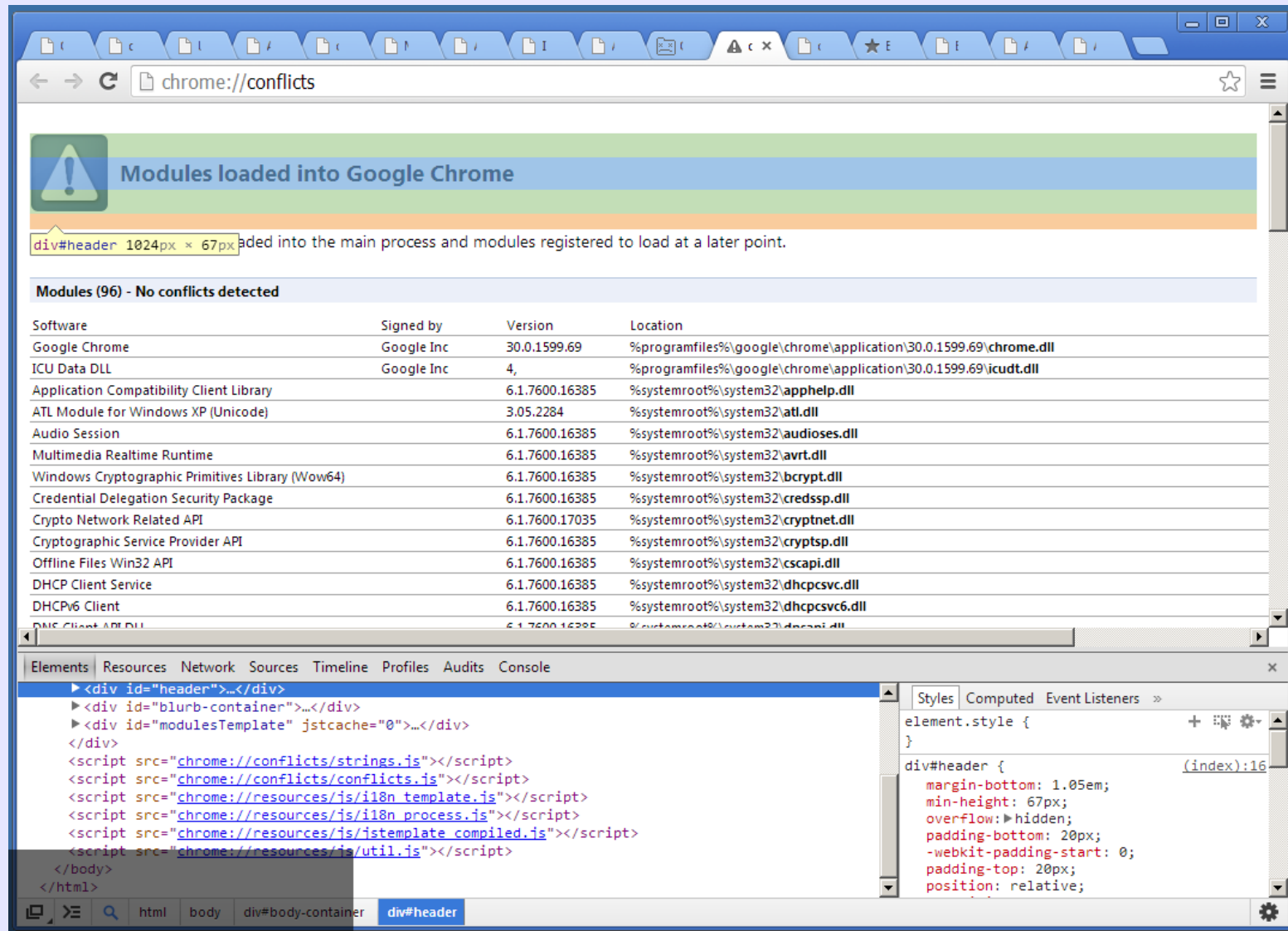


Simple. Clean. Chrome gives you only what you need up front and not a bit more. But! Dig just a little deeper, and Chrome becomes one of the best web-dev/debugging/perf testing suites ever created. Ever.

EXAMPLES

Google Chrome

Possibly the best blend of prowess and usability out there.



Everything from OpenGL testing to live CSS edits, Chrome's developer tools give you an incredible amount of control over how your browser operates.

LESSONS LEARNED

9. IF YOU NEED TO
INCLUDE ADVANCED
OPTIONS, HIDE THEM.

EXAMPLES

Mega.co.nz

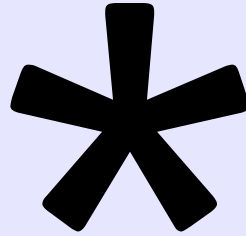


LESSONS LEARNED

10. KEEP IT SIMPLE

EXAMPLES

SSL/TLS



- * SSL/TLS actually doesn't have a defined interface. It is the most pervasive form of encryption used today, but it doesn't have an official GUI, logo, or desktop application.

If your software can protect people without them knowing it, you've won.

LESSONS LEARNED

11. IF YOU CAN,
HAVE NO INTERFACE AT ALL

THE ULTIMATE LESSON

0. MAKE IT WORK

This should go without saying, if you're building a crypto app that you want people to use, actually make it secure, make it work. People who do 5 minutes of Googling avoid Hushmail like the plague because they find out they aren't really secure at all. If you build an application, make it right, make it in public (open source), and report any and every breach you have. This is our industry, don't screw it up.

THANKS!

Slides, Fonts, Colors, Software, and Image credits to
appear on samurailink3.com/talks.