

RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: SBX3-R05

RSAC Cryptoparty: An Introduction to Secure, Usable Encryption Tools for All



Connect **to**
Protect

Jessy Irwin

Security Evangelist
AgileBits/1Password
@jessysaurusrex



#RSAC

What is this session?



#RSAC

- Introduction to basic security concepts and privacy tools that you can begin to use immediately
- Hands-on experience with easy-to-use encryption apps
- Opportunity to break down complicated lingo
- Actionable information for evaluating security and privacy tools in the future





“Security is hard, and I want to learn more but I have no idea where to start.”

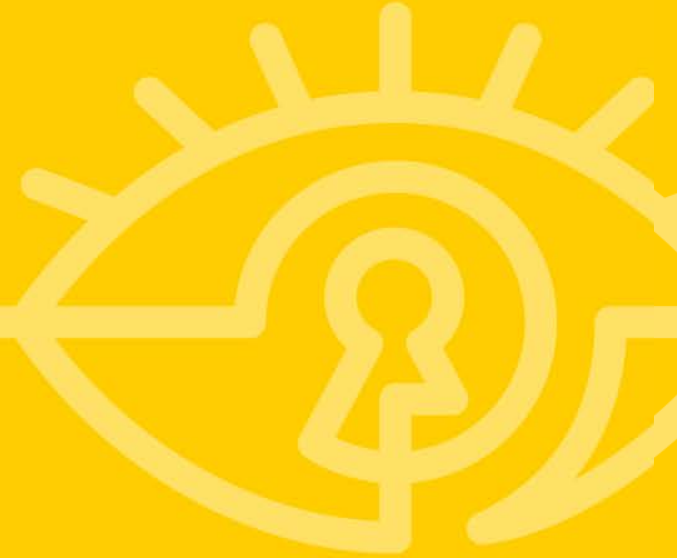
–Practically everyone who uses technology



- There is no way to have true privacy without strong security.
- Once a secret has been shared, it can't be “unshared.”
- Update your software regularly!!!!!!!!!!!!!!



Encrypting Yourself



Password Management



Full Disk Encryption



#RSAC



- Default on iOS and Android devices
- Mac: FileVault (it's in your Preferences)
- PC: Bitlocker
- Open source: TrueCrypt (<http://istruencryptauditedyet.com/>)

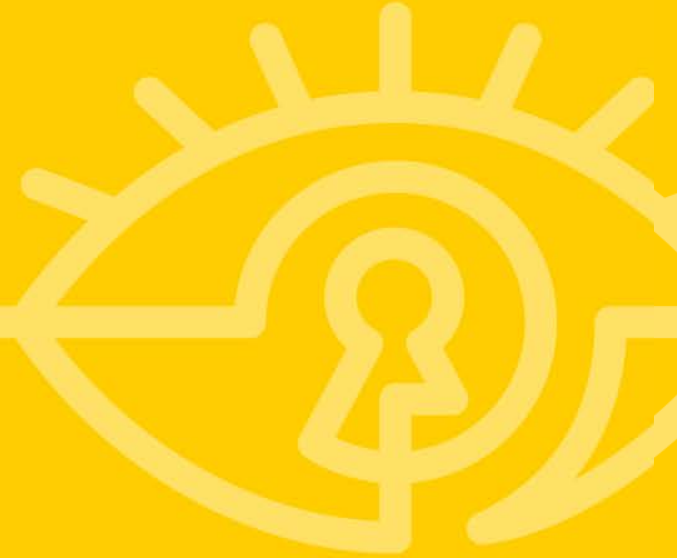




- VPN: Virtual Private Networks
- HTTPS Everywhere
- Tor, the world's most important anonymity tool
- SpiderOak, zero-knowledge storage



Encrypt with Friends



Encrypted Email



-----BEGIN PGP PUBLIC KEY BLOCK-----

```
mQENBFN00EBCADA3DjUQSSp0sq6bsbWjld+zLrME255pfEwa5EnVLVHLt/SDLdH
VKhJku0Y4vv82SDx/kJDvUJI1XRfHh91hw+YcqRCz80ohp6JIxEx22pmQClaw8
r/bfwjN6Iu7Pujld+iu95jkkwe78ePluzWb6c0c6A50kKnkXiuP4zFBTc0MbtelL
8Lub9G6T5Hh0/DgPC7i3rYcGyQqWDrTgxi0d+D4oTck+WFFmQnpgP69zVB7cy41
PQd6AqtSacFY/M0Myk+uJQpPpRlWw1BejjIDHfykoxb5P5qX1KBbwZ7S/fXw+5w
7FDXZpwBRLsYF7vCPUisrwpzj1dxMd3B8sDLABEBAAQ0IEpLc3N5IElyd2LuIDxw
ZXNzeS5pcn0pbk8tcZ5jB20+IQFABMBGcGAgAhsDBQkxhh+A8Q5JCAcDBRUKCQgI
BRVCwEAhA4BhbaE80JVKgpwAhkBAANoJEF/ci6E99MKc00ZALH9snm+xbvFap0
hbaqZ6po0DnvJcm1XBd6B56n3Zc0N+Uz6hfV9nJps8bbj53TugVg/dLW4yioZw
8l0TMy0eT0EjflW04dhPgBZE+ZDPs87Ji.k3j.cM/yIPfJZ5F/aGzxWgRWg7hd8r
3oDuXScowZnibhyex/YmtBX7Mgu0ofL10eYQNSrHdjJm83ho1053njuTIUqzZbr
xmw8y3ot0EXNRfo3lxi/VhmZnSYB0SiIP0PDgHV4nhTQ0NV8Ca3F3qJ6a1KF3Q
07FQMZuf/J2okpRaLWZdvrLWnISdx0vFgK0ccCApsUuGk060WfUSeUXit/SGuX
lc9ak1KJAT0EEwEKaccFALN00WEC6wMFCQeGH4AFcwkIBwMFF0oJcAsFFgIDAQc
HgECF4AACgkOX9zXoS/30yTBxwf/URBFATiJcQg+oGQWVrUpfkoLg+tGRND1uvN5
/qojjHU0dh5+sbIq8Bou7uXEPsngFh4VrddQq2XVpuRHAw4jJ6h4eL0htjNGjX9
VYjESZhu1VpJNBesPgCh57aIuq4lhGrYwrxmv3LevalwX2J06zZHJjvZ2eJ7T6a
tJXj+oPR5UxZZtwvUSXA/hpEBURGLiVKAzvhdzg/9n9L1L7LcTdaDpInd2nFRk+b
tzD8c0PmkdMkwK01SL4xgoP4Y6y2JWABksDnG999etsz7UwQt05NftUCybtMkU4
bWxcfz5MkuIXtn0erQilvVhk0Iy6qGNZsLxt0vWUeiM405u2okCHAQQAQIABgUC
V5oGVQAKCRDLYejBUNU8XxiLEACr7YwXHCjQnNAqymxmLqC0A0DLFRbVoERbzHw
m0jIoEqzo0wN152sArTB04J3C9UPK1Wl7bCbUNUJD0sgGPPAe+nKNB9axX7a7H81
7et0gHUsG8Ls/TfQ2iGx7HG0JGQrtw2XeT140hY6Px1ang6xomv6V6TNNxJvH0I
DLFF9DsAT+pY8fEz2c+DvngfxUvaBd0P2QA0xwXft0HsJ2cFhPkJRI4VwLSBiB4
xsjBshZgvJLdkaQ7qazlhfwZ9VtyokHSTdLvrQJpnk15KJgVKGzq+w4x+AiL8nWu
kSgrbr3LuAhT9leNDxz+6kg/0BV5Nn3NhKcWbCassLwxz0s7fpZJKR07MvWHDy3s
uwugFDVphe9lcKZQ2b003353ZgubUo7a/fU9FoFnn5k6VgsMVVYbzHj8VZt4cEM0
06yecD6aQkYX02KicdKhUhwP9xgVU7i67jtX0C28x5NFpcWoonAKwyrWp61t88qj
```

Key ID: ZH+/D324

Length: 2,048

Algorithm: RSA

Fingerprint: 104C 99F1 AC82 758A 6102 B002 5FDC D7A1 2FF7 D324

Validity: Ultimate

Capabilities: Esc

Card:

- PGP, Keybase, GPG Tools
- ProtonMail, as seen in Mr. Robot
- Advanced email encryption: S/MIME + STARTTLS





- "Off the Record" encrypted chat protocol
- Works with numerous chat clients like Pidgin, Adium (Mac)



End-to-End Encrypted Messaging Apps



All Tools	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?	Is the code open to independent review?	Is security design properly documented?	Has there been any recent code audit?
AIM	✓	✗	✗	✗	✗	✗	✗
BlackBerry Messenger	✓	✗	✗	✗	✗	✗	✗
BlackBerry Protected	✓	✓	✓	✗	✗	✓	✓
ChatSecure + Orbot	✓	✓	✓	✓	✓	✓	✓

Secure Messaging Scorecard, Electronic Frontier Foundation





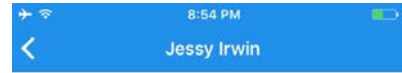
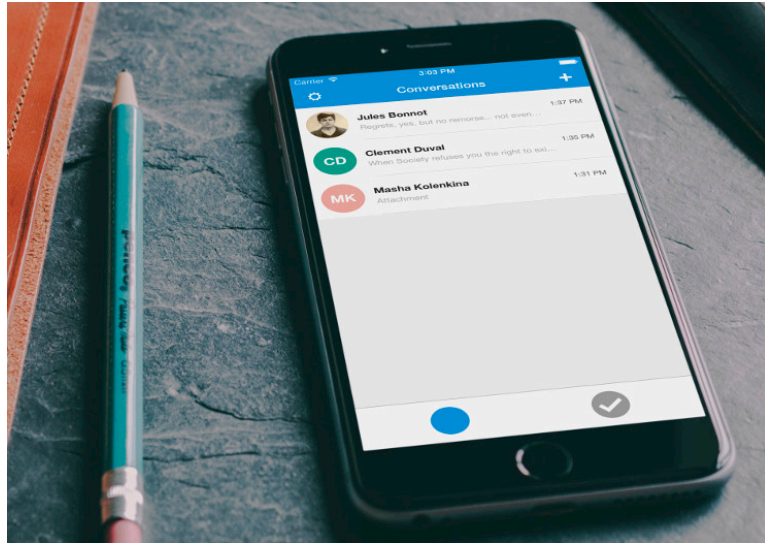
- Encrypted calling + text
- Hands on: Fingerprints
- Coming soon: Desktop chat




Signal



#RSAC



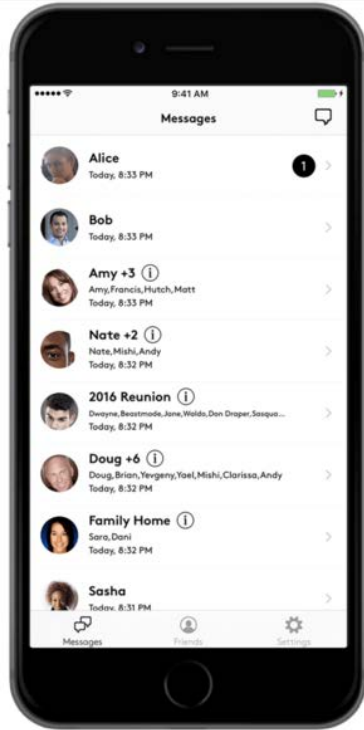
Your Fingerprint



```
05 3e 9c 5d 6e 37 23 00 ae
5e c5 8b f1 bf f0 96 d2 05
6a 8b 99 72 19 61 33 86 89
ad 49 a0 90 d2 40
```

Tap to display your fingerprint for another user





- Free, closed-source encrypted messaging for iOS and Android
- Self-destructing images that actually go away (unlike Snapchat!)
- Desktop Chat



Encrypt /ALL/ the things



- Next week you should:
 - Improve your password security habits
 - Get into the habit of updating your software
- In the next month, you should:
 - Setup Full Disk Encryption on your devices
 - Using an end-to-end encrypted app with a colleague or partner that you share private or sensitive information with
 - Use a VPN when you're connected to unsecured WiFi
- Within three months, you should:
 - Encourage others around you to encrypt private or sensitive information
 - Try sending an encrypted email– just once!



Encrypt /ALL/ the things!

