Email and Message Privacy and Security

About this outline:
The outline is an attempt to summarize the info in the referenced links.
An adequate understanding of Email and Message Privacy and Security will require that you read the info on the linked web pages.
- - Jim Macak

I. Why encrypt your email?

A. Understand the Privacy Risks of Email - *Take Control of Your Online Privacy* (ebook, $14.99)
1. on your end
2. in transit
3. on email servers
4. on the recipient's end
5. in backups

B. ECPA - Wiki article about the Electronic_Communications_Privacy_Act
- allows release of emails without judicial review

C. Recent news: Edison Mail "bug"
1. see https://9to5mac.com/2020/05/16/edison-mail-unauthorized-access
2. this update glitch revealed email accounts to other users!

II. Intro-to-Crypto.pdf

A. Two main types of encryption
1. secret key (symmetric key)
   a. uses just one secret key
   b. problematic because of difficulty of secure key distribution
2. public key (asymmetric)
   a. uses 2 paired keys - a public key and a corresponding secret key
   b. solves the problem of secure key distribution

B. Digital certificates (certs)
1. simplifies establishing whether a public key truly belongs to the purported owner
2. two certificate formats
   a. X.509 certificate - from a certificate authority (CA)
      - used for S/MIME (**S**ecure/MIME)
      - mainly employed by corporations/employees
      - usually not free
   b. PGP certificate
      - used for PGP/MIME (MIME = **M**ultipurpose **I**nternet **M**ail **E**xtensions)
      - commonly used by the general public
      - free

III. How Do Public Key Encryption Systems Work?

A. Contrast symmetric key encryption with public key (**PK**) encryption
1. PK encryption solves the problem of sharing a single secret encrypt/decrypt key
2. you need to use the public key of a recipient to encrypt email to them
3. use your own private key to decrypt incoming email to you

B. Sign data with a private key to verify origin and non-tampering

C. Warning: metadata (email header info) is not encrypted
1. sender and recipient name and email address is not encrypted
2. date of email is not encrypted
3. subject of email is not encrypted
4. all other header data is not encrypted

IV. What is PGP encryption and how does it work?

A. About PGP (**P**retty **G**ood **P**rivacy)

1. history of (PGP - OpenGPG)
    a. created in 1991 by Paul Zimmerman; released for free
    b. PGP™ is now owned by Symantec Corporation
    c. development of the OpenPGP standard began in 1997
2. OpenPGP is now an accepted Internet Standard message format
    a. implementations of OpenPGP are freely available
    b. GNU Privacy Guard (GPG or GnuPG) is the program that implements the OpenPGP standard

B. Keys used in OpenPGP

1. public key/private key pair
    a. generated for each individual upon first using OpenPGP
    b. saved and reused
    c. public key can be freely distributed
    d. *private key must be kept secret*
2. session key
    a. a key that is generated uniquely for each and every message that is encrypted
    b. session key is used only once and is never reused to encrypt another message

C. How OpenPGP works

1. the sender creates a message.
2. the sending OpenPGP generates a random number to be used as a session key
    - session key is used for this message only.
3. the session key is encrypted using each recipient's public key
    - these "encrypted session keys" start the message.
4. the sending OpenPGP encrypts the message using the session key
    a. this forms the remainder of the message
    b. the message is also usually compressed
5. the receiving OpenPGP decrypts the session key using the recipient's private key.
6. the receiving OpenPGP decrypts the message using the session key.
    - if the message was compressed, it will be decompressed

D. Digital signatures

1. used to verify the identity of the sender and verify that message wasn't tampered with
2. can be used alongside PGP's message encryption or separately
3. the sender's private key is used in generating the digital signature
4. the recipient uses the sender's public key to check the digital signature

E. Web of trust

- used to vouch for each the digital signatures of others

F. How secure is OpenPGP?

- essentially "airtight" as long as it is used correctly

V. How to- Use PGP for macOS | Surveillance Self-Defense

A. Includes step-by-step guide on "rolling your own" email GnuPG (GPG) capability

1. install GnuPG for OS X (free)
2. install and setup the Mozilla **Thunderbird** email client (free)
3. install the **EnigMail** add-on for Thunderbird (free)
    - EnigMail does not work with Apple's Mail application

B. Includes step-by-step guide for creating your PGP public/private key pair

C. Includes instructions and tips for managing your own keys and public keys of others

VI. Email Self-Defense - a guide to fighting surveillance with GnuPG encryption

A. Includes a similar guide to the above, also oriented towards macOS

1. install and setup the Mozilla **Thunderbird** email client (free)

2. install GPG Suite - also known as GPGTools (free)
3. install the **EnigMail** add-on for Thunderbird (free)

B. Includes a guide for key creation and management
1. make a keypair
2. upload your public key to a keyserver

C. Includes instructions for trying out your new OpenGPG functionality
- send and receive encrypted/signed emails with a test "bot"

D. Includes info about the "web of trust"
1. info about signing and identifying keys
2. important considerations when signing keys

VII. Use Apple Mail with GPG Mail plug-in (the latter is part of GPG Suite)

A. *Provides the only way to use OpenGPG directly in Apple Mail*
1. GPGSuite/GPG Tools provides a polished Mac-like interface
2. after free trial, GPG Mail cost is $23.90 for full plug-in functionality in Apple Mail

B. GPG Suite/GPGTools installation and use videos
1. watch videos on the GPGTools Support webpage
2. short screencast: install/use **GPGTools** in **Apple Mail** and in macOS **Services** menu
3. long screencast shows a much more inclusive demo
   a. installation
   b. key pair generation
   c. sending and encrypted/signed email with Apple Mail
   d. searching for the public keys of others
   e. GPG Suite preferences
   f. adding email addresses to a key
   g. using OpenPGP services

VIII. The Mailvelope browser extension/add-on provides webmail encryption (free and paid options)

A. uses the OpenPGP standard
- ensures compatibility with any OpenPGP generated email

B. the Mailvelope extension/add-on works in Firefox, Chrome, Edge and Brave browsers
- *Mailvelope does not work in Safari*

C. works with webmail sites of Gmail, Yahoo, Outlook.com

D. *may* be able to be configured to use your ISP's webmail site

IX. Private Email Service Providers

A. Provide encrypted/signed email functionality without requiring extensive configuration
- minimal technical expertise is needed to use these services

B. Important considerations
1. end-to-end encryption (E2EE) is preferred
   a. data is never unencrypted from when it leaves your device until it reaches recipient
   b. What is end-to-end encryption and how does it work? - ProtonMail Blog
2. zero-access encryption
   a. protects data at rest (e.g., once it is stored on a remote email server)
   b. What is zero access encryption? - ProtonMail Blog
3. comprehensive list of private email provider criteria
   a. this list is from a reliable and respected non-biased not-for-profit source
   b. available at https://www.privacytools.io/providers/email/#criteria

C. Recommended Email Services
1. these services meet the above-noted criteria of the privacytool.io website
2. available at https://www.privacytools.io/providers/email/#email
3. detailed comparison table of recommended (and other) providers

D. Two popular providers from the recommended list
1. **ProtonMail** (free and paid options)
a. uses OpenPGP
b. is compatible with externally sourced OpenPGP generated email
c. uses webmail browser interface on computers
- an app is available for iPhone and iPad
d. offers some compatibility with Apple Mail with paid option
2. **Tutanota** (free and paid options)
a. does not use OpenPGP but rather its own protocols
b. is **not** compatible with externally sourced OpenPGP generated email
c. uses native application client and/or webmail browser interface on computers
- an app is available for iPhone and iPad

X. iOS, iPad OS options

A. mobile app versions of desktop solutions
1. **ProtonMail** (free download)
2. **Tutonota** (free download)

B. iOS/iPadOS only, these essentially provide add-on OpenPGP functionality
1. **iPGMail** ($1.99)
2. **PGP Everywhere** ($4.99)

XI. Private instant messaging

A. Apple **Messages**
1. Messages in iCloud provides encryption in transit and when stored on the server
- uses end-to-end encryption
2. however, backing up to iCloud opens up a security issue
a. your backup includes a copy of the key protecting your Messages
b. a government agency could access the key and thereby decrypt your messages

B. **Signal** (well-respected, very secure, free and open-source)
1. provides private instant messaging, as well as voice and video calling
2. all of the above are end-to-end encrypted
3. cross-platform - iOS or Android phones, macOS, Windows, Linux
4. installation
a. must download and install the app first on phone
b. register your account under your phone number
- no other info is requested
c. then download the desktop app and link it to your Signal account