Email and Cryptography

Introduction

Random Numbers

Symmetric Encryption

Hashes

Asymmetric Encryption

Certificates

Signatures

SSL/TLS

SSH

VPN

Email

Disk Encryption

Attacks

Applied Cryptography

Email Characteristics of Interest

- An email is composed of a header and a body
- The header is used by email handling programs to label, store, transmit, and route email
- The body is created by and used by the operator of an email application which does not have to be a human being
- An email header has a range of possible content formatted as name value pairs, with few names being required
- An email body can be anything at all, but is traditionally restricted to plain text
- Putting anything other than text in an email requires encoding the data as text using base64 encoding or another format, so body content is literally always plain text data under normal circumstances

MIME vs. S/MIME

- An email body may contain multiple parts, encoded to allow the entire set of parts to be a single plain text blob regardless of what each part may actually contain
- The MIME (RFC 2049) standard was invented to formalize the encodings so that multipart emails can be reliably encoded and decoded by any properly functioning email application - it is also used by other protocols such as HTTP
- S/MIME (RFC 1847) is an extension of MIME defining two specific body part types and their encodings, signed and encrypted
- Each of the new types is composed of 2 parts, the data and the control information to use the data

MIME

- Multipurpose Internet Mail Extensions

S/MIME

- Security Multiparts for MIME

PGP and Email

- Since its inception, PGP has been used with email
- It defines 3 MIME part types which can be included in a multipart email to support PGP signing, encryption, and public key transfer
- Like S/MIME, it has two parts for each defined type, a control part and a data part
- Like S/MIME, it uses ascii armor to encode the data part

Encrypting Email

- For an email to journey from its originator to its destination, the header must be readable by every program that handles the email, so it is required to be visible to more parties than the source and destination

- The email body can be encrypted without affecting its ability to be transferred correctly and all major email applications can do this encryption although they may require add-ons or plugins

- A simpler and much more common alternative is to attach only encrypted data, obviating the need to encrypt the entire email

- Some transfer programs may choose to refuse to transfer encrypted messages because they cannot examine the content

- Encrypted email is encrypted with the public key of the recipient

Handling Email

- Email headers often contain information that is useful to an attacker
- If there is a need for the email header to be protected from prying eyes while in transit, TLS can be used between email servers
- It is typically only used for encryption
- TLS protection between servers can use self-signed certificates
- No email handling program can enforce handling rules on any other email program
- Unless you are working within a network bubble, you cannot guarantee or even reasonably expect email headers to be private or secure

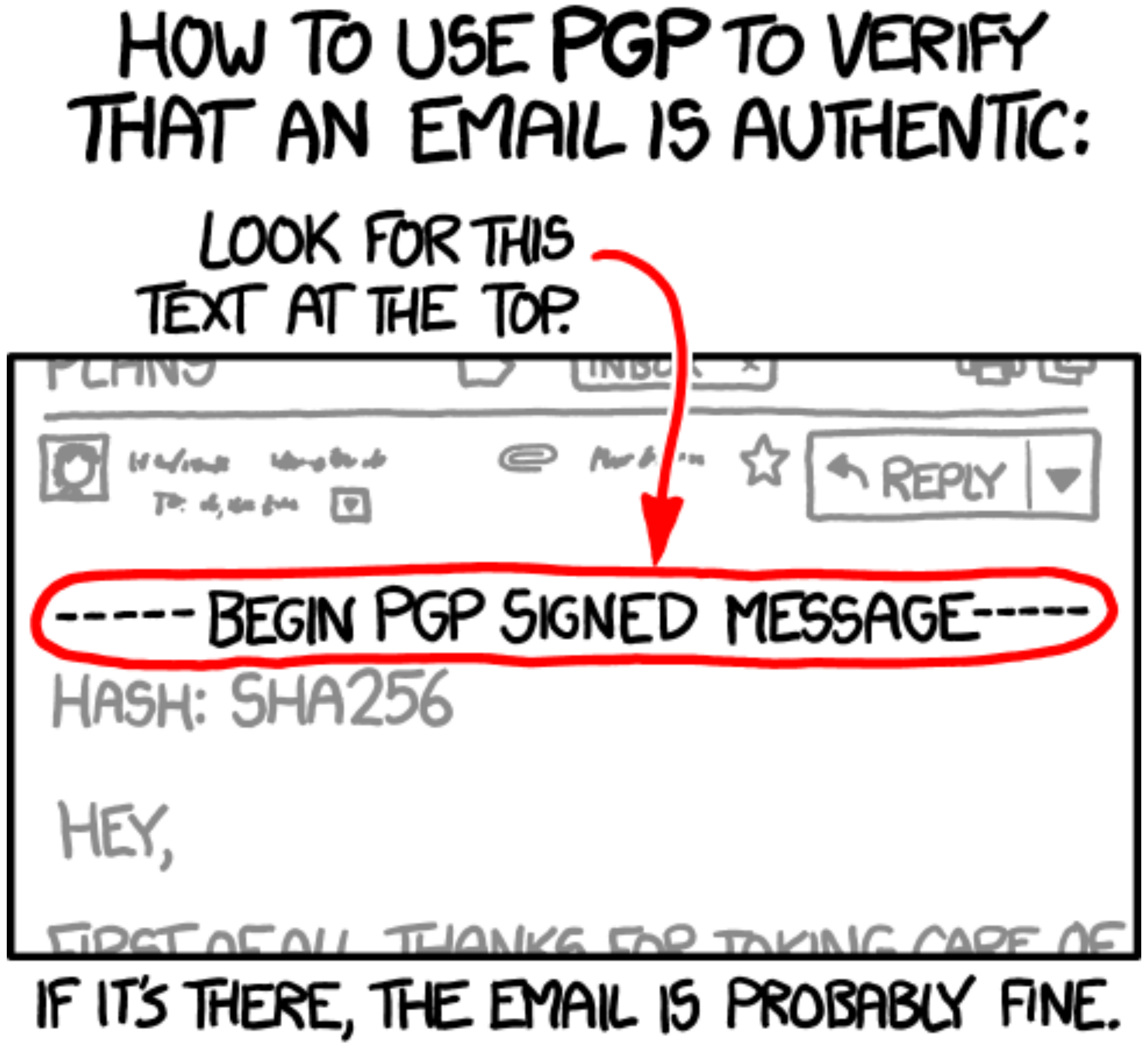
Signing Email

- Signing an email is supported by many email applications, see link on course website
- A user will compose an email and choose to send it from an identity they have configured into their email application
- If they have configured their email application to sign emails, they will have assigned a key pair and algorithm to their sending address in that application
- The application will generate a keyed hash and add it to the email prior to sending using the sender's private key
- The sender's public key must be available to the recipient for the signature to be validated by the receiver

Signed Email

- An application that displays that email can display a tag or icon to indicate the email had the necessary signing parts, and whether the signature is valid
- An email can be signed without being encrypted and vice-versa
- The creation of keys and certificates and distribution of those follows the same processes already covered for both web of trust (PGP keys) and PKI (OV/IV CA-signed certs) public key distribution
- Various email user agents provide differing levels of support for signing, e.g. as shipped by Apple, Apple Mail only supports PKI signing and encryption but PGP can be added using an extension such as GPG Mail whereas Thunderbird supports both fully out of the box

Signing Email


HOW TO USE PGP TO VERIFY THAT AN EMAIL IS AUTHENTIC:
LOOK FOR THIS TEXT AT THE TOP.
REPLY
-----BEGIN PGP SIGNED MESSAGE-----
HASH: SHA256
HEY,
IF IT'S THERE, THE EMAIL IS PROBABLY FINE.

https://xkcd.com/1181/