Risks, Encryption, and Key Escrow

Eric Norman
University of Wisconsin
Overview

- Risk
- Encryption/decryption basics
- It's more about data handling
  - Protection of confidential data
  - Preservation of University data
- Relationship with public key cryptography
  - Short answer: not much
- About possibilities and processes
- Not about products
PKI Entanglements

- Key escrow
- Non-repudiation
- Dual certificates
- Smart cards, USB hardware tokens
- Multi-party encryption
- Certificate revocation
- Certificate repositories
Risk: Fun with Metaphors

Encryption is not a magic bullet

but it is a bullet,

and bullets can be dangerous.
Carrie's Admonition

(Compliments of Carrie Regenstein).

In your zeal to keep the bad guys out,

don't forget to let the good guys in!
Risk Assessment

- It's all about asking if things don't work
- What's the worst that can happen?
- What would normally happen?
- How many people would be affected?
- How easily would the breach be detected?
- How much response would be required?
  - Corrective action?
  - Notification?
- Would there be sanctions?
Biggest Risks to Confidential Data

Storing it on a computer that's connected to the Internet. Who really benefits from this practice?

Storing it on a laptop. Who really benefits from this practice?
Decryption Fundamentals

Decryption Key
(Secret)

Decrypted
(Gibberish)

Plaintext
(Data)
Decryption Fact

To access plaintext (data), you must have both

access to decryption key,

and

access to ciphertext.
Basic Encryption Risks

Loss of ciphertext: nothing new here.

Loss of decryption key: new risk.

Inverse hologram effect: with some encryption systems, if you lose just a little bit of the ciphertext, you've lost it all.
Key Escrow

Key escrow means that a third party can obtain access to the decryption key *without consent* of the keyholder, and perhaps without their knowledge.

This (the consent part) should not be an issue for purposes of records preservation.

Loss of the decryption keys is a risk for the good guys, hence the phrase “key backup” will be used.
Key Escrow – Not!

Some folks will go ballistic at the idea of a third party holding the keys.

For instance, attorney – client privilege.

For instance, physician – patient privilege.

For instance, ...
Key Accountability

The most important things to know about decryption keys (during their entire lifecycle):

How many copies are there?

Where is each copy?

Who has access to each copy?
Key Lifecycle Risks

- All copies become extinct
  - This is why you do backups
- Some copy escapes into the wild
  - Mitigate with access control
  - Hardware might help
- “The wild” infiltrates key usage processes
  - More access control
  - Check audit trails
Password Based Encryption

- Encryption/decryption keys are derived from a password (i.e. a secret)

- This is symmetric, not public key encryption
  
  - The same password must be available for both encryption and decryption operations

- Risk: you need to remember this password
  
  - You won't be able to call the help desk and have them reset it!
Encrypted File Systems

This is **always** done with symmetric encryption, usually password based.

Using public key operations wouldn't make sense since ciphertext isn't destined for someone else.

Risk: you need to remember the password or decryption key.
Public Key Encryption

Public key operations are **never** used for bulk encryption.

Symmetric keys are used for bulk encryption.

If such keys are needed elsewhere, then public key operations might be used to encrypt them for transport.
Data Transport

This is where public key encryption is useful because data is destined for someone else.

That still doesn't mean it's necessary, though.

There's not much risk of data loss since if the data is lost in transit, just resend it. You've been doing this for decades.
Storing Data After Transport

It's real easy to just store encrypted data as the same ciphertext after it was transported. This is what email clients usually do.

Risk: recovering of such data if that's the only way to recover it. This is considered a “worst practice”.

This is a problem with electronic mail. Key escrow or backup may add protection of confidentiality but also makes the recovery problem worse.
Confidential Data on Desktops

Is there a reason to store confidential data on desktops or laptops?

It depends on the data and who you ask (the data custodian).

University administration will say no.

But ask a researcher about their research data.
Desktops and Laptops

- Usually don't listen for connections
- Attended; secrets can be unlocked for use, locked when not in use
- Risk: but will users do that?
- Risk: generally more accessible in a university environment
- Risk: laptops can be easily stolen
  - But what is the motive?
- Risk: if at home, they're usually shared
Cryptographic Hardware

- Remember strong keys (and passwords)
- Protect knowledge of those keys
- Can be locked and unlocked (e.g. by a PIN)
- Tamper evident
- Secure messaging
- Maintain audit trail
- Tamper resistance
Hardware Decryption (operational)
Confidential Data on Servers

Servers run unattended. Ergo, any secrets that they need like decryption keys are always available (somewhere nearby).

How do you supply or unlock those keys when the server reboots?

Cryptographic hardware can protect knowledge of keys, but it doesn't protect access to the process.
Secret Obfuscation

- Yes, I know it's security by obscurity, but in the digital world, that's what all security is
- Decryption key in separate, obscure file or buried in code
- It's better to derive key when needed (like by a hash) so that the bad guys have to disassemble code
- Sometimes, you can arrange that ciphertext is stored on a separate host with only transient appearance on host with key
Simple Encrypted Backup

Write data (or decryption key) in a file.

Encrypt file with password based encryption.

Write ciphertext on a CD-ROM.

Write down password and store it in a safe place.

And you get 2-factor access control for free!
Outsourced Backup

You can always just send the ciphertext to the backup service and backup the decryption key by other means.

Risk: you can't lose the decryption key.

If a service provides you with a public key that you can use to “encrypt” data that you send to them, then they'll have access to the plaintext.

But you could still send them ciphertext!
Summary

- Do an honest risk assessment
- It's more about managing access to computers and processes than anything else
- It's the data that you'll need to recover
- If data is encrypted, you need to recover both the ciphertext and the decryption key
- Public key encryption is at most useful for transport
- And don't forget to let the good guys in!
PKI Pop Quiz

You have a keypair and the public key has been included in a certificate that is used for encryption only.

The private key has been compromised.

What are your next steps?