More Architecture — Email Security

- We want to secure email
- Generally, that requires crypto, which in turn requires protecting keys
- How shall we do that?
Standard Techniques

- Encrypt the private key with a user-typed passphrase
- Use special-purpose crypto hardware
- The latter is rarely available; we need to use the former, at least in some cases
Where are Decryption and Signing Done?

- Gateway machine?
- End-user’s machine?
Signing at the Gateway

- Tempting target
- Hard for user to supply the key or the passphrase
- How does the gateway \textit{know} who sent the mail?
- Best for \textit{organizational} signatures
Decrypting at the Gateway

- Again, how are keys supplied?
- When is decryption done?
- Is the mail stored internally in the clear?
Signing Every Message

- Suppose we want to sign every message
- Do we prompt users for a passphrase on each email sent?
- Rather annoying — can we cache passphrases?
(Why Sign Everything?)

- Principle?
- Prevent false attribution?
- Anti-spam?
Caching Keys

- If we cache keys, they’re exposed to bugs in the mailer
- How risky are mailers?
- (How big are they?)
Some Mailer Sizes

<table>
<thead>
<tr>
<th>Mailer</th>
<th>KLOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thunderbird</td>
<td>6000</td>
</tr>
<tr>
<td>Evolution</td>
<td>2500</td>
</tr>
<tr>
<td>(extras)</td>
<td>2200</td>
</tr>
<tr>
<td>Claws-Mail</td>
<td>840</td>
</tr>
<tr>
<td>Pine</td>
<td>530</td>
</tr>
<tr>
<td>Mutt</td>
<td>288</td>
</tr>
</tbody>
</table>

Numbers are very imprecise. All of these mailers require many libraries, especially the GUI mailers.
(Why are Mailers So Big?)

- Mail formats are complex
  - MIME
  - Multilingual
  - GUIs
- HTML rendering
- Other stuff bundled in (calendar, vCard, etc)
- Frequently include an editor
Why are Mailers Insecure?

- Size
- Accept untrusted input
- Plenty of room for user error
Entrust our Keys to Mailers?

- They’re big and complicated
- They interact with lots of other programs
- They have long histories of security problems
- Handing them keys doesn’t sound like a great idea...
Outboard Key Manager

- Should we have a separate application to handle keys?
- How big are such applications?
- Can we trust them?
# Key Managers

<table>
<thead>
<tr>
<th>Component</th>
<th>KLOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>GNOME Keyring</td>
<td>150</td>
</tr>
<tr>
<td>GNOME Keyring Manager</td>
<td>97</td>
</tr>
<tr>
<td>GPG</td>
<td>520</td>
</tr>
<tr>
<td>GPG2</td>
<td>737</td>
</tr>
<tr>
<td>pinentry</td>
<td>55</td>
</tr>
</tbody>
</table>

These aren’t exactly tiny, either...
Bug Rates

• How many bugs per 1,000 lines of code?
• Hard to measure
• Different types of software have different rates
• We can’t count bugs that aren’t found!

<table>
<thead>
<tr>
<th>Component</th>
<th>Bugs/KLOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux 2.6 Kernel</td>
<td>.17</td>
</tr>
<tr>
<td>Commercial code</td>
<td>20–30</td>
</tr>
</tbody>
</table>

That said...
Managing the Key Manager

• The mailer still tells the key manager what to decrypt or sign
• If the mailer is buggy, it can fool the key manager
• You don’t know what’s really being signed or decrypted
• (This all applies to crypto hardware solutions, too)
Pure Outboard Solution?

- Save inbound mail; manually decrypt it
- Edit outbound mail separately; manually sign, then paste that into mailer buffer
- Does this work?
It’s Too Inconvenient

• Most users won’t put up with this
• Result: very few signed messages
• Result: reluctance to receive inbound encrypted messages
• Does this give us worse security?
What Do We Do?

• There are no perfect solutions
• How disciplined are the users?
• How important is secure email?
• Can you have separate grades of keys?
• Who is your enemy?
Outboard Keys

- Despite the risks, outboard keys are still better
- Still simpler than the mailer
- Less risk of key theft
- Easier to add (secure) audit trail
Windows Vista and IE 7

• Web browsers have also been problematic
• Internet Explorer has been worse…
• IE 7 on Vista is a lot better
• Why?
Protected Mode

- Run web browser with fewer privileges (exception: trusted sites can have full privileges)
- Compromise of the browser does not result in compromise of (most) user files
Components

• User Account Control (UAC)
• Mandatory Integrity Control (MIC)
• User Interface Privilege Isolation (UIPI)
User Account Control

- Eliminate need to log in as Administrator
- Even Administrator can run most applications without privilege — they changed the privilege requirements for some operations
- Privilege can be raised as needed, with password entry. (Will users make that decision correctly?)
The message is rather mysterious…
Mandatory Integrity Control

- Low-privilege processes cannot write to protected files
- Available levels: low, medium, high
- Similar to MAC
Bell-Lapdula and MIC

- Recall how Bell-Lapadula confidentiality mechanisms could be used for integrity protection, by reversing labels
- MIC uses half of it: it’s really “no write down”
- MIC does not provide confidentiality protection
Privilege is Inherited

- The privilege level of a process is inherited by its children
- Children spawned by protected mode IE also run at Low privilege
- This blocks attacks by ActiveX, VBScript, etc.
Virtualization

- A lot of existing code wants to write files (cache, temporary files, cookies, history, registry, etc.)
- A shim layer virtualizes these functions
- Files to be modified in Low mode are copied to the Low area; the changes are made only to the copies
Gaining Privilege

- Sometimes, Low processes need to do things requiring privilege
- Special *broker* processes will perform such operations on request
- Brokers ask user consent before proceeding
- Is that reliable?
Trusting the User?

- Users can be tricked
- Many of today’s dialog boxes are useless
- From a W3C glossary Wiki:

  *Dialog box: A window in which resides a button labeled “OK” and a variety of text and other content that users ignore.*
Users Don’t Like It

- Some older applications break
- These were probably insecure to begin with
- But people are used to them
Lack of Confidentiality Protection

- Low mode malware can still read your files
- It appears possible for Low mode applications to export data
- But — full Bell-Lapadula confidentiality control is impractical
- Cookies are a special case — prevent (some) cross-site scripting attacks
User Interface Privilege Isolation

- Prevents Low mode processes for sending certain messages to higher-mode processes
- Blocks “shatter attack” (inject code into another process via Windows messages)
- In essence, ACL for message-passing
What Has Microsoft Done?

- Separated Internet Explorer from Windows Explorer (i.e., restored the distinction between net and desktop)
- Used OS access controls to isolate browser
- Added more access controls
- *Structural separation*
Does it Work?

• IE7 on Vista is immune to the .ani file (animated cursor) attack (see http://www.microsoft.com/technet/security/bulletin/MS07-017.mspx)

• More precisely, the attack code couldn’t escape the Low mode jail

• Human interface attacks may still be an issue

• Other delivery mechanisms for .ani still work
Summary

- Structural separation helps
- It’s not a panacea
- There are still challenging user interface issues
- Backwards compatibility is a problem