Real Licensing for Virtualized COTS

Presentation for GSAW 2012

Jeremy Jacobsohn
GMV USA
Justification

Why licensing?

• Supports a business model where vendors build and enhance products
• Ensures vendor is paid
• Confirms legal agreements (T&Cs)
Dawn Age of Computing

- Mainframe era 1960s
  - Very expensive hardware in small numbers
  - Most software was licensed with hardware purchase
  - Small number of customers were individually identifiable
Virtualization

- VM/370 introduced in 1972
  - ‘hypervisor’ OS based on CP-40 research prototype from IBM’s Cambridge Scientific Center
    - Virtual machines with console, private disk
    - Preferred guest OS ‘CMS’ single-user environment
    - Open Source until about 1980
PC Arrives

Why run a VM when you can have your own computer?
- Exit virtualization, for now
An Open Letter to Hobbyists

To me the most evil
Is the lack of good
Software and
Hardware.

Almost a yearly
Market to expand, hired to

And the initial work
Spent most of the lost ye-

The value of the computer

The feedback we have
Say they are using BASIC has all been positive. Two surprising
Things are apparent, however, and they are true. First, that
Many of these "users" have bought
BASIC (less than 10% of all Altair owners have bought BASIC), and
And the amount of royalties we have received from sales to hobbyists
Makes the time spent of Altair BASIC worth less than $2 an hour.

Why is this? As the majority of hobbyists must be aware, most
Of you steal your software. Hardware must be paid for, but soft-
Ware is something to share. Who cares if the people who worked
On it get paid?

In this case? One thing you don’t do by stealing software is
Get back at MITS for some problem you may have had. MITS
Doesn’t make money selling software. The royalty paid to us, the manual,
The tape and the overhead make it a local-area operation. One thing
You do do is prevent good software from being written. Who can affor-
Ded to do professional work for nothing? What hobbyist can put
5000 man-hours into programming, finding all bugs, documenting his prod-
Duct and distribute for free? The fact is, no one besides us has
Invented a lot of money in hobby software. We have written 6500
BASICs, and are writing 6800 BASICs, but there is very lit-
Le incentive to make this software available to hobbyists. Most
Directly, the thing you do is theft.

What about the guys who resell Altair BASIC, aren’t they makin-
Ging money on hobby software? Yes, but those who have been reported
To us by us is the end. They are the ones who give hobbyists a
Bad name, and should be kicked out of any club meeting they show up at.

I would appreciate letters from any one who wants to pay up, or
Has a suggestion or comment. Just write me at 120C Alvarado St. 614,
Albuquerque, New Mexico 87104. Nothing would please me more than
Being able to hire a few programmers and deluxe the hobby market with
Good software.

Bill Gates
General Partner, Micro-Soft
Responses

- Microsoft: sell direct to manufacturers
- Apple: bundle software & devices
- Free Software Foundation: Gnu “copyleft”
Responses - Node Locking

- NIC card (IP address or MAC)

- Trusted hardware
  - Dongle
  - ‘copy protected’ CD in drive
  - EPROM on system board
Responses - Signatures

- Software-calculated value
  - Based on a combination of attributes, designed to detect changes

- Examples:
  - Linux ‘hostid’ calculated via an open source algorithm
  - Windows activation
Responses Virtualized

- Sell direct to hardware manufacturers **FAILS**
- Bundle OS with device **FAILS**
- Gnu “copyleft” unaffected (and unhelpful...)
- NIC card (IP address or MAC) **FAILS**
- Trusted hardware **FAILS**
- Unix 'hostid' **FAILS**
- Calculated signature **promising...**
Calculating Signature – License Certificates

- Vendor can create a certificate using PKI signature
  - Include vendors identity certificate (from Certification Authority)
  - Include capability list
    - Features allowed, timeframes, capacity
  - Gather fingerprint data from customer
    - Satellite databases, smart card IDs (unique users), OS version
- Sign with vendor’s private key
  - Provide public verification key
Using License Certificates

- Software can compare to certificate at run time
  - Verify certificate using vendor’s public key
  - Compare fingerprint data from license to fingerprint in environment
Using License Certificates

- Example: Microsoft Windows
  - Windows ‘activation’ collects signature and sends to central authority
  - Activated copy is compared against environment
  - Detects major discrepancy (e.g. new motherboard)
Wrinkle: License Servers

- Count active license instances

- Additional level of indirection: only the license server is node locked
  - But it’s still node locked

- When nodes can be copied a ‘special’ node is problematic
Network Discovery (no special node)

- Multicast discovery using well-known ports
  - Standard implementation on Linux is mDNS ‘avahi’
  - Nodes with connectivity self-organize into a domain
- Can be used to implement decentralized count within a domain
Counting Things

- Computing resources per instance
  - CPUs/threads
  - Memory
- Number of instances within a network discovery domain
- Users
  - Simultaneous unique users
    - Smartcard certificates can proxy individuals
  - Simultaneous active API sessions
    - Hard to measure in a Web-services environment
- Domain resources
  - Telemetry streams
  - Spacecraft
  - Database size
  - Number of scheduled events
Mission Critical Applications

- Immediately crippling real-time application due to license failure is not acceptable
  - Avoid implications to Safety and Mission Assurance
- Gentle reminders are OK
  - Pop-up or visible reminder to accept EULA
  - Stop reminding after license installed and EULA accepted
Customer Networks are Closed

- May not be possible to send information to manufacturer for certificate generation
- Solution: trusted third-party license generation
  - Third-party proxy holds the certificate generation key for license
  - Combines the customer’s private data with the vendor’s license grant to produce a certificate that goes to the end user
  - Run-time software accepts third-party’s ID
Summary

- Node locking is **over**.
  - Software and certificates can and will be replicated.

- **Vendor or proxy generates license based on non-virtual fingerprint**
  - Spacecraft (database signature)
  - Unique end users (smart cards)
  - Capacity per instance or per network domain
  - Enabled product features
  - Embeds vendor identity

- Application software validates license at runtime
  - Compares licensed fingerprint to current environment
  - Provides only licensed features

- **Ground Systems have specific constraints**
  - No hard enforcement (gentle reminders OK)
  - Complications due to customer data privacy
Thank you

Jeremy Jacobsohn
jjacobsohn@usa.gmv.com
240 403-0185 x119