Automatic Quality Testing And Distribution Of AV Updates

Andreas Marx

amarx@gega-it.de

AV-Test.org

University of Magdeburg, Germany

Introduction

Full automatic testing is impossible, but...

- A lot of things can be done automatically, reliable and very fast!

Why automatic testing?

- AV programs need regular updates
- Software is unsteady (small changes can cause a lot of side effects)
- Not only Engine-related, but all signature file updates have to be tested, too

Two main test categories

1. AV functions:

- Normal, regular updates:
  - Released every few weeks, tested regularly
  - Time to test: 2-3 days or more
- Emergency Updates:
  - Only a few minutes to test!

2. Other functions (GUI etc.):

   - Blackbox, Whitebox tests etc.

What should be tested?

- New virus detection should be higher than the last update
- Virus names should be unchanged (log file comparison)
- Same disinfected files (compared with old disinfection collection)
- No false positives

etc.

Automation I

Only a few computers are needed (10-15)...

- With different hardware, OS and slightly other configuration

-At best, like "usual" customer computers

Important: The GUI version has to be tested too, not only the command-line scanner.

Automation II

- Doing the same things on all computers at the same time should give the same results (one person is able to test 15 different configurations at the same time)
- Remote control (using scripts) of computers to start GUI scan jobs etc.

Don't forget...

- GUI tests on different language versions (both program and OS)
- Tests on OS that look nearly the same (Windows 98 vs. 98 SE or Netware 4.20 vs. 5.10)
- More than just one test for each issue (using different ways)
- Include formerly false positives
- Test all supported engines with the latest signatures

Variation of tests

- Create new test files
- Invite new testers
- Change the way of testing
- Include destroyed or other invalid files (what happens?)

Update Distribution

Problem: The AV company is fast enough to release an updates, but...

- The user don't know about it!
- In emergency situations (think about Nimda or Vote) the server of av companies are overloaded
- And the update has to be distributed to everyone in the company

What's the best update time?

- Manually pressing one button?
- Once a month, week, day or hour?
- During outbreak situations: IMMEDIATELY!
- What about an "Outbreak Service" - the server will be notified that a new, important update is available using standard ways, like e-mail

... but if 100.000 customers are notified at the same time?

Outbreak Updates

- Send out a notification slightly delayed to everyone (starting with the biggest customers)
- Use more than just one big server at one location (not only USA, but Germany too - special providers exist!)
- Use small, incremental emergency updates (1-2 KB only)

Update strategies I

Old: Always everything:

- *BIG* and *BIGGER* and *much BIGGER*

→ Not very useful in the times, where updates can be 1-2 MB big

Better way:

- *BIG* and *small updates*, and the small update patches the big one to the most current version

→ No big code changes necessary!

Methods of patching

- Using easy, generic methods: Big updates, but small program code
- Using specialized methods for a known file structure: Much smaller updates possible, but a lot of code has to be written and if the file structure changes, it has to be rewritten...

Of course, all patched files should be checked – using MD5 or other cryptographic methods instead of CRC32

Update strategies II

One time BIG and *small* and *slightly bigger* etc.

→ Only one file has to be updated, easier to handle

BIG and *INC* and *INC* and *INC* etc.

→ A lot of files have to be handled (which ones are needed?)

Distribution

- Old: All computers communicate directly with the download server at the av company
- Better: Special in-house update server (only this server communicates with the outside server), distributes it to all servers and clients
- (E-Mail-, HTTP- and FTP-) Gateway or Groupware systems can still be updated directly

Important: Not only signature files have to be updated, but the engine and the programs need to be updated too!

Usual problems

- Push vs. Pull (restart for login scripts?)
- FAT vs. NTFS on:
  - Daylight saving time
  - Only even seconds

Questions?

AV-Test.org

:-)