Short Paper Review of:

Application-Level Reconnaissance: Timing Channel Attacks Against Antivirus Software

Citation:


Author(s) Affiliation(s):

- University of New Mexico, Department of Computer Science

Claims:

- It is possible to check how up to date a client machines AV is.

Likes:

- I dug into the authors a bit and discovered that they also presented at the New Security Paradigms Workshop. It doesn't really have anything to do with this paper review but I found it interesting non-the-less.

- A lot has been done in browser based fingerprinting, but it interesting to see that an external application such as AV can be tested as well because it's linked to the browser.

- I like that the technique can be applied to any OS running AV or at least ClamAV.
- A timing channel attack is an interesting way to go about this, it's been done before to determine other aspects of applications linked to the browser but AV complicates this significantly.

Dislikes:

- The example attack that they developed was based on ActiveX which doesn't run on Linux/MacOS natively. I realize that it could be re-written but when choosing to create an attack for a multi-platform AV like ClamAV wouldn't you make your example attack multi-platform as well?

- The authors never discussed how they determined if the computer was running ClamAV. How do they go about fingerprinting the AV running on the client, the browser ID string will not have that information in it.
Repeat / Add to Work?

- I enjoyed this paper, it was well put together and covered the topic in fairly good detail. I would have liked to see more code but at least the illustrations were well explained. They make the point that ClamAV is Open Source and that's why they chose to work with it but I would have liked to see at least one more AV's analyzed even if an exploit wasn't written for it.

- I could see myself reproducing this paper, it would be interesting to be to recreate the attack for at least 2-3 different AV programs and make sure that it worked on multiple OS's. In addition I would be interested in creating a fingerprinting mechanism to see which AV the client system was running as well.