

AVIT

APPLIED VERIFICATION FOR INTEGRITY AND TRUST
METHODOLOGY

By Pete Herzog
avit<at>isecom.org

June 2006

1 Creating the Applied Verification for Integrity and Trust Methodology for OpenTC¹

Pete Herzog, ISECOM

pete@isecom.org

Purpose : Project Abstract
Date : January 15, 2006
Revised : June 7, 2006

1.1.1.1 Short Abstract

The Trusted Computing Group (TCG) and Trusted Platform Module (TPM) are the center of a paranoia level as high as any in conspiracy circles. The open, community-reviewed, methodology of *Applied Verification for Integrity and Trust* (AVIT) will apply tests to answer the core questions of Trusted Computing and dispel the catalytic myths assisting current paranoia. ISECOM, a non-profit, open source community for developing open methodologies under the Open Methodology License (OML) will develop AVIT as part of the EU-supported² OpenTC³ project to explore whether an open methodology can give guidance to designers, implementers, and independent evaluators to standardize tests for trustworthiness.

1.1.1.2 Trust and FOSS

What if you had to trust someone or something? If you were to, what would you require to do that? What would be the steps you would take to convince yourself that you can give trust? Can you define what those steps would be? Are you sure they're good enough or would you have second doubts about your own ability to devise that methodology yourself? Would you be more comfortable to know how others might do it as well?

Enter the Trusted Computing Group (TCG) and the Trusted Platform Module (TPM). The growing ubiquity of the TPM on computer motherboards has managed to put, at the very least, the Free/Open Source Software (FOSS) and LINUX communities on the defensive with the TCG. The movement to involve the TPM in commercially viable interests by members of the TCG have precluded these arguments with the uncertain future of TPM application with the exaggerations of wants and fears.

So how paranoid should we be? As part of OpenTC, an EU-supported, collaborative research and development project started in November 2006, ISECOM is approaching paranoia in a pragmatic fashion. Developing trust tests works best in the FOSS approach and as ISECOM approaches every methodology, we will take paranoia from everyone and devise the most thorough means to address all fears towards trustworthiness. That will also allow for tests which provide a metric for trustworthiness. Which, in turn, will allow

1 The content of this paper is published under the sole responsibility of the author. It does not necessarily reflect the position of other OpenTC members.

2 Project Nr. 027635

3 <http://www.opentc.net>

transparent rules of trustworthiness to be followed to conclusion and therefore decide STOP or GO. In conclusion, ISECOM will attempt to open the methods of trustworthiness much like it did for hacking and business integrity to discover what it takes to be less paranoid about trust.

1.1.1.3 How the FOSS Methodology Works for OpenTC

ISECOM has begun development of the methodology for *Applied Verification for Integrity and Trust* (AVIT) which will apply tests to answer the core questions of Trusted Computing: how can we arrive at an educated decision about whether a software component should be trusted for a particular purpose? And if we can, how can we convince ordinary users that this trusted platform is indeed fit for purpose and trustworthy? To confront this core issue, ISECOM will cooperate in the OpenTC project to explore whether an open methodology similar to ISECOM's *Open Source Security Testing Methodology* can give guidance to designers, implementers, and independent evaluators to standardize trustworthiness.

Developing a methodology for trust is a difficult thing as trust is difficult to define outside of its connotations. Deciding on what is an adequate level of trust requires measuring what is an adequate level of transparency and controls. How do you measure what feels right? Since this project is as much about defining when a system should "feel" secure based on what we know to "be" secure following Risk Assessment Value (RAV) metrics then we find that the true purpose of developing a methodology is to explore what Trusted Computing needs to be. This will no doubt be a struggle to prove when a system can be trusted by the user, the owner, and a third party. Especially in cases where it is the owner who must be trusted by the third party. Fortunately, the technology for defining a means for not trusting the owner (meaning the TPM is not designed to be secured from hardware tampering or owner-based attacks) does not exist to the state where we can do more than define parameters for "what-if" scenarios.

The methodology will begin as a set of questions to be answered in the form of an outline. The outline will be provided openly at ISECOM's website and a call for volunteers and reviewers will be made publicly. The outline will begin under the Open Methodology License which protects a person's Trade Secrets (a methodology is considered a Trade Secret by law) in an open manner to foster development and use in much the same way that the GPL protects copyright. Furthermore, the content itself will be provided under the Common Criteria copyleft to facilitate research and open dialog. Contributions are added to the outline and pass through an editorial review board and then to the open document. Credit is not given as part of the submission rather as part of the whole document. In this manner, we allow researchers to provide information which may not be mainstream thought without having to be afraid of repercussions. In cases of corporate reprisals, researchers may remain anonymous as long as the information is not protected by the company as some companies require extensive paperwork for an employee to assist such projects even off-hours.

As researchers contribute their expertise in the various questions, the methodology will grow. Verification will take place at ISECOM and with the partners of OpenTC to assure facts are correct. Further public participation is advertised as the document takes form and the transparent process is necessary to garner general public support if not participation. The

goal being a set of tests and tasks to assure trust not just for OpenTC but as a living standard for all Trustworthiness open and closed. Therefore, any individual or organization should be able to apply the tests and determine if it not only is trustworthy but also how much so.

With public acceptance being a major obstacle for a trusted platform, FOSS has all the advantages.

1.1.1.4 Obstacles

The obstacles to trust begin with fears and uncertainties. If there is a chip, how will it be used? If there is a software, will it take control? If everything is in place, how do I know it's doing only what it's designed and intended to do if I can't verify for myself?

The three main obstacles are:

1. fears behind trustworthiness
2. the human problem with trustworthiness
3. the technical problem with trustworthiness

The next issue is public acceptance and the human problem with trust. More so than that even is individual preference. Public acceptance may be something bought and connived. But individual preference for trust is much more delicate and requires convincing.

The third obstacle is the technical one. If we have the appropriate hardware in place for trust, how can we be sure it's appropriate? If we need software for trust, can we be assured the software operate correctly? Who determines how the hardware and software interact and that what they accomplish can lead to trust as the conclusion? For this reason, the methodology needs to come before the hardware and the software. As this is not the current state, the methodology needs to include metrics to determine how close the current state is to the methodology and where precisely it fails to match. In this regard we are both fortunate and unlucky. While we have a model to follow and the development in this area is not new, we run the risk of determining current models as untrustworthy and losing public acceptance. Furthermore, we run the risk of relying on status quo to build the methodology and by not reaching further we will commit ourselves to the same mistakes as those before us. Therefore the only appropriate solution is a public and open methodology that is based on the questions we need answered to find trust and not on the current research and implementations.

The AVIT methodology is based on that which the person can control for trust to first, exist, and second, to be beneficial. From the three main obstacles to trustworthiness, the first two are easiest to find control over by an individual. The third, technical design and implementation, will require more as not even the average technically-inclined individual will be able to ascertain trustworthiness without support. For this reason, the AVIT methodology will focus on tests for the technical problem of trustworthiness to overcome both the fears and the human problem.

Basic AVIT tests:

1. Choice and finality of controls,
2. Openness of design and implementation,
3. Transparency of communication and action, and
4. Clarity and usability of operations.

1.1.1.5 The Open Methodology to Trust

It is only with a publicly-supported standard for determining trust that we can actually achieve trustworthiness. To achieve such a standard we need not just the thoughts and ideas of a few who have commercial interests both at heart and on their minds and therefore closed into a particular space of thought but we also need to include the interested, the hobbyists, the worried, and the paranoid. ISECOM will apply the principles and communities of open source to finding a solution to trust. Over time, there should be no reason to trust any component as our ability to evaluate against a thorough methodology should be possible-- if not by us then by a source that we trust. And that source we need to be able to evaluate to gain our trust. Therein lies the chain nature of trust that needs to be designed on stronger ground than currently exists. As you see, we don't need trust to gain trustworthiness; we need a methodology of trust.