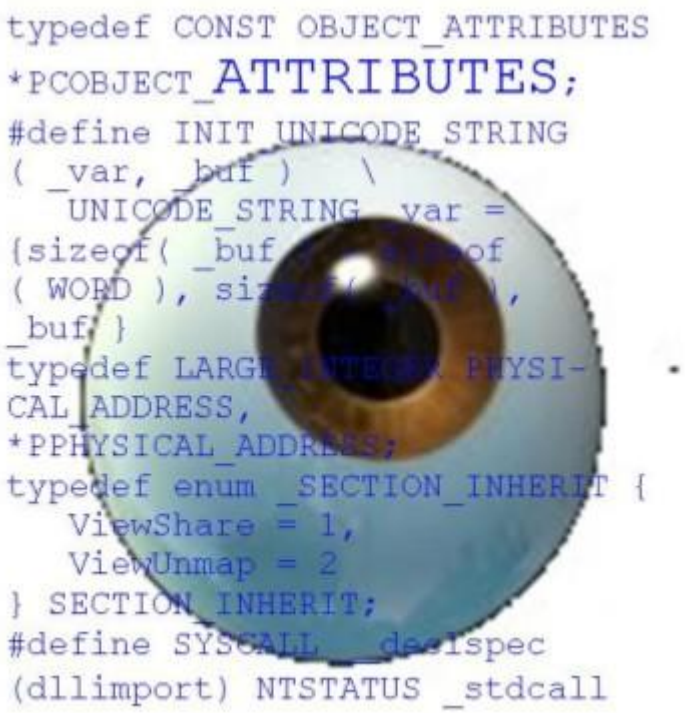

Second International Alternative Workshop on Aggressive Computing and Security

iAWACS 2010: the Revelation Edition

- * -

The no-limit workshop

- * -

"Enhancing security with the attacker's mind

"Orthodoxy and self confidence are weaknesses"

"There is no such thing as forbidden knowledge, only forbidden use of knowledge"

ESIEA - Paris – May 2010

Thinking security cannot be done without adopting a preferential mode of thought of the attacker. A system cannot be defended if we do not know how to attack it. If the theory is still an interesting approach to formalize things, the operational approach must be the ultimate goal: to talk about security is meaningless if we do not actually do security.

In recent years the major security conferences in the subjects preferred to select papers according to fashion topics, conforming to something like orthodoxy and organize selection as beauty contests. As a result excellent yet unorthodox scientific papers are often rejected and sink into oblivion.

The second *international Alternative Workshop in Aggressive Computing and Security* (iAWACS'10) aims to focus on this vision and to allow researchers and specialists to present relevant research works, with interesting results and operational (theoretical and/or applied) in the field of security. The different points of view, away from unconventional fashion and orthodoxy are particularly welcome. The aim is also to promote discussion of ideas around these topics. Articles or contributions submitted will be selected according to the following criteria:

- Interest and scientific/technical correctness/accuracy,
- New results,
- Operational quality

Regarding this last point, the authors should give all information and conditions for reproducibility of results they intend to present. This may include, during the selection phase by the reviewers, assessments based on challenges to the authors by the reviewers. iAWACS is not just another hackers workshop where the last exploit is disclosed. The aim of the conference is to make security concepts evolves through both the attacker's view AND a thorough formalization backed by experimental results.

The main topics covered (list not exhaustive) are:

- Cryptanalysis techniques
- Steganalysis techniques
- Malicious cryptography
- Advances computer virology techniques (malware, backdoor…)
- Active security product analysis and testing
- Active security auditing
- Mathematical concepts and applications with respect to the attacker's view.
- Cyber warfare techniques.
- Digital data counterfeiting
- Cryptographic and steganography techniques
- Invisible trap/backdoor techniques in algorithms and applications
- Implementation attacks
- Interception/eavesdropping techniques
- Forensics and anti-forensics techniques.
- Tempest and anti-tempest techniques
- InfoOps techniques.
- Satellite hijacking.

Articles should be submitted in electronic format, preferably in LaTeX format, in English. Submissions of Word/OOwriter documents are accepted. The address for submission is iawacs@esiea.fr Submissions under hidden identities or aliases are not allowed.

Technical challenges will be organized during the conference. Attendees who want to participate must register either now or on site. For this second edition, two challenges will be organized:

1. **Antivirus evaluation challenge (PWN2KILL).** The aim will be to bypass (and therefore practically evaluate the reality of) antivirus software protection. More details will be published later (when the list of accepted papers will be published) but challenge settings will be: Windows 7 and user mode only. The organizers reserve the right to choose freely the virus to be tested. A jury composed of a bailiff and journalists (from the computer technical press) will be responsible for technical control of the challenge.
2. **Cryptographic challenge (The Taliban AntiHackers… reloaded).** This cryptanalysis challenge aims at recovering secret information in a real context of use. More to come but interested people can refer to the first edition of the challenge we organized at Hack.Lu 2009 http://2009.hack.lu/index.php/CryptoChallenge

Workshops will also be organized (lock picking, soldering and free hacking technical session and tutorials...). We also intend to invite hacker spaces to come and present their work, initiatives...

Important dates:

- Submission deadline: Feb 20th, 2010
- Notification deadline: March 15th, 2010
- Final manuscript submission for inclusion into the pre-proceedings: April 15th, 2010
- Conference dates: May 12th – 14th, 2010

The conference proceedings will be published with ISBN by the Presses Techniques of ESIEA. They will be given to registered participants at the conference and can then be bought on the conference homepage. The conference will be held at *Ecole Supérieure en Informatique, Electronique et Automatique,* in Paris from Wednesday 12th to Friday14th, 2010. Each author will have 45 minutes of speaking time; each presentation will be followed by a technical discussion between speakers and listeners.

Conference registration amount to 200 Euros (includes proceedings, coffee breaks, lunches, cocktail reception and social events). Students fee are 100 Euros.

Organizing committee:

- ✓ Program Chair : Éric Filiol (ESIEA)
- ✓ Program Co-Chair : Anthony Desnos (ESIEA)
- ✓ Program Co-Co-Chair Robert Erra (ESIEA)
- ✓ Eddy Deligne (DCNS/ESIEA)
- ✓ Christophe Grenier (DCNS/ESIEA)
- ✓ Nicolas Bodin (ESIEA)
- ✓ Mickaël Salaün (ESIEA)

Contacts:

- Program chair: iawacs@esiea.fr
- Organization committee: iawacs_orga@esiea.fr
- Press contact: iawacs_press@esiea.fr