

SecuCode

Workshop on Secure Execution of Untrusted Code



In conjunction with
**ACM Conference on Computer and Communications Security 2009
(CCS 2009)**

November 9, 2009
Hyatt Regency Chicago, IL, USA

Call for Papers

The workshop aims at bringing together researchers and practitioners from industry and academia working on the protection of software systems against untrusted code. The workshop will be a platform for presenting and discussing recent developments and future directions.

Broadband access to the Internet is a key factor to the increased availability of untrusted code. Typically, various applications are downloaded and executed locally. All these applications have in common that their origin is often unknown or their trustworthiness cannot be assessed. The user wants to be sure that his system is not harmed when executing untrusted applications from an unknown source. Thus, the applications should only access those resources and only call those functions that are considered as non-security-critical. However, to allow applications to execute properly, they need a minimal set of rights which differs from application to application. The proliferation of malware and the increment of flaws in program code require securing systems against untrusted code to prevent unauthorized access to resources. The workshop addresses various topics of this field.

Topics of Interest

Intermediate languages (Java and .NET)

- Programming language safety
- Intermediate languages (e.g. Java bytecode, .NET CLI) safety
- Security applied to intermediate language code
- Intermediate language code verification and secure class loading
- Runtime environment security and security extensions
- Policy definition and policy enforcement
- Access control
- Information flow control
- Security of distributed computing

Interpreted languages (Python, PHP, ...)

- Programming language safety
- Interpreter security
- Access control
- Information flow control
- Security of distributed computing

Runtime monitoring (identifying prohibited resource accesses or function calls at runtime)

- In-lining of code in applications
- External monitors not running inside the application
- Sandboxing: preventing applications from escaping their restricted environment

Static analysis (identifying prohibited resource accesses or function calls prior to execution)

- Source code analysis
- Intermediate language code analysis
- Reduction of the number of security checks at runtime
- Policy generation

Security architectures (sound, coherent and holistic security approaches for a system)

- Protecting the system against untrusted code
- Security policies

Miscellaneous (touches all the before mentioned topics)

- Insufficiency of known security mechanisms and concepts
- Security activities at standardisation organisations (e.g. JCP)
- Performance loss due to security mechanisms (especially in resource constraint devices)
- Hot topics and future topics in securing systems against untrusted code

Submission Instructions

Please consider to submit your contribution to the workshop. Submissions shall be original, previously unpublished and not currently under review by another conference or journal. Theoretic work and pragmatic approaches are welcomed. Submissions that are usable and applicable in practice are especially welcomed. Your contribution should either cover your current research in progress, your research results, your experience from practical deployment of security features, or it should be a position paper containing your thesis and comprehensible reasoning. It should be written text at most eight pages double-column ACM format (<http://www.acm.org/sigs/publications/proceedings-templates>), including references and appendices. Authors of accepted papers must guarantee that their papers will be presented at the workshop.

Please submit your paper in PDF format at EasyChair:

<http://www.easychair.org/conferences/?conf=secucode09>.

Important Dates

Paper submission (extended)	Fri Jun 19, 2009	Camera ready version	Tue Aug 25, 2009
Author notification	Fri Aug 14, 2009	Workshop	Mon Nov 9, 2009

Publication

Accepted papers will be published in the ACM Digital Library and in the workshop proceedings on CD.

Organisation Committee and Program Chairs

Sven Lachmund, DOCOMO Euro-Labs, Germany

Christian Schaefer, DOCOMO Euro-Labs, Germany

Program Committee

Jörg Abendroth (Nokia Siemens Networks, Germany)

Mads Dam (Royal Institute of Technology (KTH), Sweden)

Jochen Haller (SAP, Germany)

Antonio Lioy (Politecnico di Torino, Italy)

Fabio Martinelli (National Research Council (IIT-CNR), Italy)

Fabio Massacci (University of Trento, Italy)

Chris Mitchell (Royal Holloway University of London, U.K.)

Frank Piessens (Katholieke Universiteit Leuven, Belgium)

Anand Prasad (NEC, Japan)

Alexander Pretschner (Fraunhofer Institut für Experimentelles Software Engineering, Germany)

Thomas Quillinan (Vrije Universiteit Amsterdam, Netherlands)

Yves Roudier (Institut Eurecom, France)

Frederic Stumpf (Fraunhofer Institut Sichere Informationstechnologie, Germany)

Eric Vetillard (Trusted Labs, France)

Dan Wallach (Rice University, USA)

Alf Zugenmaier (DOCOMO Euro-Labs, Germany)

Contact

SecuCode Web-Site: <http://www.docomoeurolabs.de/secucode/>

SecuCode E-Mail: Please obtain from SecuCode Web-Site.

CCS 2009 Web-Site www.sigsac.org/ccs/CCS2009/