Call For Papers

Call for Paper for the 2nd International Workshop on

Quality of protection - QoP 2006

Security Measurements and Metrics

Mon. Oct. 30 - Alexandria VA, USA

Affiliated with 13th ACM Conference on
Computer and Communications Security (CCS-2006)

EXTENDED DEADLINE: Fri. 23 June

1 WORKSHOP OVERVIEW

Information Security in Industry has matured in the last few decades. Standards such as ISO17799, the Common Criteria, a number of industrial certification and risk analysis methodologies have raised the bar on what is considered a good security solution from a business perspective.

Yet, if we compare Information Security with Networking or Empirical Software Engineering we find a major difference. Networking research has introduced concepts such as Quality of Service and Service Level Agreements. Conferences and Journals are frequently devoted to performance evaluation, QoS and SLAs. Empirical Software Engineering has made similar advances. Notions such as software metrics and measurements are well established. Processes to measure the quality and reliability of software exist and are appreciated in industry.

Security looks different. Even a fairly sophisticated standard such as ISO17799 has an intrinsically qualitative nature. Notions such as Security Metrics, Quality of Protection (QoP) or Protection Level Agreement (PLA) have surfaced in the literature but still have a qualitative flavour. The "QoP field" in WS-Security is just a data field to specify a cryptographic

algorithm. Indeed, neither ISO17799 nor ISO15408 (the Common Criteria) addresses QoP sufficiently. ISO17799 is a management standard, not directly concerned with the actual quality of protection achieved; ISO15408 is instead a product assessment standard and yet does not answer the question of how a user of a product assessed by it can achieve a high QoP within his/her operational environment. Both standards cover just one aspect of an effective QoP and even the combination of both would not address the aspect sufficiently. "Best practice" standards, such as the baseline protection standard published by many government agencies, also belong to the category of standards that are useful, but not sufficient, for achieving a good QoP.

Security is different also in another respect. A very large proportion of recorded security incidents has a non-IT cause. Hence, while the networking and software communities may concentrate on technical features (networks and software), security requires a much wider notion of "system", including users, work processes, organisational structures in addition to the IT infrastructure.

The QoP Workshop intends to discuss how security research can progress towards a notion of Quality of Protection in Security comparable to the notion of Quality of Service in Networking, Software Reliability, or Software Measurements and Metrics in Empirical Software Engineering.

The 1st QoP workshop was held in Milano in September 2005 and was affiliated with the 10th European Symposium on Research in Computer Security (ESORICS 2005) and the 11th IEEE International Software Metrics Symposium (METRICS 2005). The revised proceedings of the workshop are going to appear in the Kluwer (now Springer) Applied Security Series.

2 SUBMISSION TOPICS

Original submissions are solicited from industry and academic experts to presents their work, plans and views related to Quality of Protection. The topics of interest include but are not limited to:

- Industrial Experience
- Security Risk Analysis
- Security Quality Assurance
- Measurement-based decision making and risk management

- Empirical assessment of security architectures and solutions
- Mining data from attacks and vulnerabilities repositories
- Security metrics
- Measurement theory and formal theories of security metrics
- Security measurement and monitoring,
- Experimental verification and validation of models,
- Simulation and statistical analysis, stochastic modelling
- Reliability analysis

3 IMPORTANT DATES

- Fri. 23 June - Paper submissions (EXTENDED)
- Tue. 10 July - Authors' notification
- Thu. 17 August - Camera ready paper due
- Oct. 30 - Nov 3 - ACM CCS and QoP Workshop

4 PAPER SUBMISSION

Original RESEARCH PAPERS are solicited in any of the above mentioned topics describing significant research results based on sound theory or experimental assessment. Preliminary research results can be submitted in the form of SHORT PAPERS.

We also solicit INDUSTRY EXPERIENCE REPORTS about the use of security measurements and metrics in industrial environments. Industry papers should have at least one author from industry or government, and will be considered for their industrial relevance.

Industry and Research papers should be limited to 6 pages in the standard ACM conference format. Short Papers should be limited to 3 pages.

5 PUBLICATION

Authors of accepted papers will be expected to give full presentations at the workshop. The proceedings of the workshop will be published by ACM.

6 PROGRAM CHAIRS

- Guenter Karjoth - IBM Research - Zurich
- Fabio Massacci - University of Trento

7 PROGRAM COMMITTEE

- Alessandro Acquisti - Carnegie Mellon University (USA)
- Guenter Bitz - SAP (DE)
- Yves Deswarte - LAAS-CNRS (FR)
- Dieter Gollmann - TU Hamburg-Harburg (DE)
- Virgil D. Gligor - University of Maryland (USA)
- Judith N. Froscher - Naval Research Laboratory (USA)
- Erland Jonsson - Chalmers University of Technology (SW)
- Svein Johan Knapskog - The Norwegian University of Science and Technology (NOR)
- Helmut Kurth - ATSEC (DE)
- Bev Littlewood - City University, London (UK) Volkmar Lotz - SAP (DE)
- Roy Maxion - Carnegie Mellon University (USA)
- David M. Nicol - University of Illinois (USA)
- Mario Piattini - University of Castilla-La Mancha (SP)
- Anand Prasad - DoCoMo Communications Laboratories Europe (DE)
- Tomas Sander - HP Labs (USA)
- Shrivastava Santosh - University of Newcastle upon Tyne (UK)
- Ketil Stolen - SINTEF (NO) & Univ. of Oslo (NO)
- Vipin Swarup - The MITRE Corporation (USA)
- Marvin Zelkowitz - University of Maryland (USA)