==========

Call for Paper for the 1st International Workshop on

QUALITY OF PROTECTION - QoP 2005
Security Measurements and Metrics
http://dit.unitn.it/ qop/

Milano, Italy, Thu. 15 September 2005.

Affiliated with 10th European Symposium on Research in Computer Security (ESORICS 2005) in Milan (12-14 Sep).
http://esorics05.dti.unimi.it

and

the 11th IEEE International Software Metrics Symposium METRICS 2005 in Como (19-22 Sep)
http://www.swmetrics.org/metrics2005

==========

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 stan-

dard 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.

SUBMISSION TOPICS:

Original submissions are solicited from 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

INVITED SPEAKERS

- Stefano De Panfilis - Engineering SpA (IT)
- TBA

IMPORTANT DATES:

- Fri 10 June (deadline is extended till Thu 23 June) - Paper submissions
- Fri 8 July - Author's Notification
- Wed 12 Sep - Fri 14 Sep ESORICS
- Thu 15 Sep - QoP Workshop
- Mon 19 Sep - Thu 22 Sep IEEE METRICS in Como

PAPER SUBMISSION:

Original RESEARCH PAPERS are solicited in any of the above mentioned topics. Research papers should be limited to 12 pages in the standard Springer Verlag format, describing significant research results based on sound theory or experimental assessment.

We also solicit INDUSTRY EXPERIENCE REPORTS, limited to 6 pages, 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.

PUBLICATION:

Authors of accepted papers will be expected to give full presentations at the workshop. Revised versions of the papers presented at the workshop will be published by Kluwer/Springer in the Applied Security Series.

STEERING COMMITTEE

- Imrich Chlamtac - UTDallas (US) & CreateNet (IT)
- Gerhard Eschelbeck - QUALYS (US)
- Dieter Gollmann - TU Hamburg-Harburg (DE)
- Helmut Kurth - ATSEC (DE)
- Bev Littlewood - City University, London (UK)
- Fabio Massacci - Univ. di Trento (IT)
- Ketil Stølen - SINTEF (NO) & Univ. of Oslo (NO)
- Lorenzo Strigini - City University, London (UK)
- Jeannette Wing - CMU (USA)

PROGRAMM COMMITTEE

- Alessandro Acquisti - Carnegie Mellon University (USA)
- Matt Bishop - U. California Davis (USA)
- Imrich Chlamtac - CreateNet (IT)
- Yves Deswarte - LAAS-CNRS (FR)
- Paolo Donzelli - University of Maryland (USA)
- Gerhard Eschelbeck - QUALYS (USA)
- Dieter Gollmann - TU Hamburg-Harburg (DE) — Co-chair
- Erland Jonsson - Chalmers University of Technology (SW)
- Audun Jøsang - University of Queensland, (AUS)
- Svein Johan Knapskog - The Norwegian University of Science and Technology (NOR)
- Helmut Kurth - ATSEC (DE)
- Bev Littlewood - City University, London (UK)
- Fabio Martinelli - Institute of Informatics and Telematics (IT)
- Fabio Massacci - Univ. di Trento (IT) — Co-Chair
- Roy Maxion - Carnegie Mellon University (USA)
- Flemming Nielson - Technical University of Denmark (DE)
- Mario Piattini - University of Castilla-La Mancha (SP)
- Ketil Stølen - SINTEF (NO) & Univ. of Oslo (NO)
- Lorenzo Strigini - City University, London (UK)
- Edgar Weippl - Vienna University of Technology (AU)
- Jeannette Wing - Carnegie Mellon University (USA)
- Marvin Zelkowitz - University of Maryland (USA)