1. Record Nr. UNINA9910713414203321

| | |
|---|---|
| Titolo | Federal preemption of state and local control of locomotives / / United States Environmental Protection Agency, Air and Radiation, Office of Mobile Sources |
| Pubbl/distr/stampa | [Washington, DC] : , : United States Environmental Protection Agency, Air and Radiation, Office of Mobile Sources, , 1997 |
| Descrizione fisica | 1 online resource (3 pages) |
| Collana | Regulatory announcement |
| Soggetti | Locomotives - Exhaust - Standards - United States<br>Air quality management - United States<br>Air quality management<br>United States |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Note generali | "EPA420-F-97-050."<br>"December 1997." |
| Nota di bibliografia | Includes bibliographical reference. |

2. Record Nr. UNINA9910782274703321

| | |
|---|---|
| Autore | Zou Xukai <1963-> |
| Titolo | Trust and security in collaborative computing [[electronic resource] /] / Xukai Zou, Yuan-Shun Dai, Yi Pan |
| Pubbl/distr/stampa | Hackensack, NJ, : World Scientific, c2008 |
| ISBN | 1-281-93358-9<br>9786611933586<br>981-279-088-8 |
| Descrizione fisica | 1 online resource (248 p.) |
| Collana | Computer and network security ; ; v. 2 |
| Altri autori (Persone) | DaiYuan-Shun<br>PanYi <1960-> |
| Disciplina | 005.8 |
| Soggetti | Computer security<br>Groupware (Computer software)<br>Computer networks - Security measures |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Note generali | Description based upon print version of record. |
| Nota di bibliografia | Includes bibliographical references and index. |
| Nota di contenuto | Contents; Preface; Acknowledgments; List of Figures; List of Tables; 1. Introduction; 1.1 Overview of Trusted Collaborative Computing; 1.2 Basic Concepts in Terms of Security; 1.3 Basic Concepts in Terms of Reliability; 1.4 Abbreviations and Notations; 1.5 Outline; 2. Secure Group Communication (SGC); 2.1 Overview of Secure Group Communication (SGC); 2.2 Typical Group Key Management Schemes for SGC; 2.2.1 Centralized Group Key Distribution; 2.2.1.1 Key Tree (Logical Key Hierarchy); 2.2.1.2 Other Proposed Schemes; 2.2.2 De-centralized Group Key Management; 2.2.2.1 Iolus 2.2.2.2 Other Proposed Schemes 2.2.3 (Distributed) Contributory Group Key Agreement; 2.2.3.1 Tree based Group Di.e-Hellman Key Agreement; 2.2.3.2 Other Proposed Schemes; 2.2.4 Distributed Group Key Distribution; 2.2.4.1 DGKD; 2.3 Enhanced Group Key Management for SGC; 2.3.1 SGC for Wireless and Mobile Ad Hoc Networks; 2.3.1.1 CRTDH; 2.3.1.2 Other Proposed Schemes; 2.3.2 Authenticated Key Exchange (AKE); 2.3.2.1 AUTH-CRTDH; 2.3.2.2 Other Proposed Schemes; 2.3.3 Self-Healing Key Distribution; 2.3.3.1 Self-Healing based on Polynomials and Secret Sharing; 2.3.3.2 Other Proposed |

Schemes

2.3.4 Block-free Group Key Management 2.3.4.1 BF-TGDH; 2.3.5 Secure Dynamic Conferencing; 2.3.5.1 KTDCKM-SDC; 2.3.5.2 Other Proposed Schemes; 2.4 Conclusion; 3. Cryptography based Access Control; 3.1 Overview of Access Control in Collaborative Computing; 3.2 An Efficient Differential Access Control (DIF-AC) Scheme; 3.2.1 System Description and Initialization; 3.2.2 System Dynamics and Maintenance; 3.2.3 Discussion; 3.3 Cryptographic Hierarchical Access Control (CHAC) Schemes; 3.3.1 HACModel; 3.3.2 Directly Dependent Key Schemes; 3.3.3 Indirectly Dependent Key Schemes
3.3.4 Polynomial and Interpolation based Schemes 3.3.5 An Efficient CHAC Scheme with Locality; 3.4 A Uniform CHAC Scheme Based on Access Polynomials; 3.4.1 Principle; 3.4.2 Key Computation/Derivation; 3.4.3 Node/Vertex Level Dynamics; 3.4.4 User Level Dynamics; 3.4.5 Security and Performance Analysis; 3.4.5.1 Security Analysis; 3.4.5.2 Performance Analysis; 3.4.6 An Illustrative Example and Experiment Results; 3.4.7 Discussion; 3.4.7.1 Enforcement of Other Access Models; 3.5 Conclusion; 4. Intrusion Detection and Defense; 4.1 Overview of Intrusion Detection and Defense; 4.2 Intruding Attacks
4.3 Intrusion Detection Models 4.3.1 Anomaly Modeling; 4.3.2 Misuse Modeling; 4.3.3 Specification Modeling; 4.4 Intrusion Response; 4.5 DoS/DDoS Attacks ; 4.5.1 Typical DoS Attacks; 4.5.1.1 DoS Flooding Attacks; 4.5.1.2 Redirection Attacks; 4.5.1.3 Service Exploits; 4.5.2 Distributed Denial of Service (DDoS) Attacks; 4.5.2.1 DDoS Attack Steps; 4.5.2.2 DDoS Tools; 4.6 Typical DoS/DDoS Defense Mechanisms; 4.6.1 Single-node Defending Method; 4.6.2 Multiple-node Defending Methods; 4.6.2.1 Path Identification; 4.6.3 Honeypot; 4.7 Defending against DoS/DDoS Attacks-Traceback; 4.7.1 ICMP Traceback.
4.7.2 (Probabilistic) IP Packet Marking

Sommario/riassunto

Computer networks are compromised by various unpredictable factors, such as hackers, viruses, spam, faults, and system failures, hindering the full utilization of computer systems for collaborative computing - one of the objectives for the next generation of the Internet. It includes the functions of data communication, resource sharing, group cooperation, and task allocation. One popular example of collaborative computing is grid computing.  This monograph considers the latest efforts to develop a trusted environment with the high security and reliability needed for collaborative computing.