A mechanism for automatic digital evidence collection on high-interaction honeypots

An investigation of a compromised host on a honeynet being used to increase the security of a large enterprise network

Application of a methodology to characterize rootkits retrieved from honeynets

Honeypot forensics

Misleading attackers with deception

Overview of a high assurance architecture for distributed multilevel security

Defending against traffic analysis attacks with link padding for bursty traffics

Limitations of on demand secure routing protocols

Anomalous packet identification for network intrusion detection

Searching covert channels by identifying malicious subjects in the time domain

Protocol anomaly detection and verification

Windows NT one-class masquerade detection

Context-based adaptive control in autonomous systems

LSB steganalysis using support vector regression

Modeling critical infrastructure requirements

The trusted computing exemplar project

Honeyfiles: deceptive files for intrusion detection

NoSEBrEaK - attacking honeynets

UML extensions for honeypots in the ISTS distributed honeypot project

Determining the strength of a decoy system: a paradox of deception and solicitation

Public key cryptography with matrices

On the security of random key pre-distribution scheme

Matrix based asymmetric bulk encryption algorithm

Evolution of in-line network encryptors toward the high assurance Internet protocol interoperability specifications (HAIPIS)

Simplified protocol capture (SIMPCAP)

The new criteria for covert channels auditing

Architecture of the reconnaissance intrusion detection system (RIDS)

Dimension reduction using feature extraction methods for real-time misuse detection systems

Security feature comparison for fibre channel storage area networks switches

Towards the specification of access control policies on multiple operating systems

Dynamic document reclassification for preventing insider abuse

Measuring IT security - a method based on common criteria's security functional requirements

Secure communications in ad hoc networks
Developing and delivering hands-on information assurance exercises: experiences with the Cyber Defense Lab at UMBC

A biometric authentication approach for high security ad hoc networks

Tactical bandwidth exhaustion in ad hoc networks

The application of a low pass filter in anomaly network intrusion detection

Battery-based intrusion detection: a first line of defense

A game theoretic approach to modeling intrusion detection in mobile ad hoc networks

Network abuse detection via flow content characterization

Agent based multilevel dynamic multimedia security system

SILT: integrated logging management for security-enhanced Linux

Advancing assurance for security distributed communications

The Manuka project

Qualitative and quantitative analytical techniques for network security assessment

Simulation for training computer network operations

Enhanced secure dynamic DNS update with indirect route

Analyzing the security and survivability of real-time control systems

Fuzzy dependency and its applications in damage assessment and recovery

Anomaly intrusion detection using one class SVM

Classification of computer attacks using a self-organizing map

Limitations of on demand secure routing protocols

Security in software architecture: a case study

Forensics for advanced UNIX file systems

A secure logging scheme for forensic computing

Developing forensic computing tools and techniques within a holistic framework: an Australian approach

Mining data relationships for database damage assessment in a post information warfare scenario

Who has the keys to the vault?: protecting secrets on laptops

Investigation of pushback based detection and prevention of network bandwidth attacks

Recursive data mining for masquerade detection recursive data mining for masquerade detection

Markov chains in network intrusion detection

GSWLAN: a new architecture model for a generic and secure wireless LAN system

Attack attribution in non-cooperative networks

IP-traceback based attacker tracking: a probabilistic technique for detecting Internet attacks using the concept of hidden Markov models

Iterative incentive scheme for outsourced IA

Adding the fourth "R"

Towards a trusted immutable kernel extension (TIKE) for self-healing systems: a virtual machine approach
CLIQUE clustering approach to detect denial-of-service attacks  p. 447
Designing an information security system  p. 449

*Table of Contents provided by Blackwell's Book Services and R.R. Bowker. Used with permission.*