Computers » Computer Systems

Robust Detection of Stepping-Stone Attacks

Authors: Ting He; Lang Tong; CORNELL UNIV ITHACA NY SCHOOL OF ELECTRICAL AND COMPUTER ENGINEERING

Abstract: The detection of encrypted stepping-stone attack is considered. Besides encryption and padding, the attacker is capable of inserting **chaff** packets and perturbing packet timing and transmission order. Based on the assumption that packet arrivals form renewal processes, and a pair of such renewal processes is also renewal, a nonparametric detector is proposed to detect attacking traffic by testing the correlation between interarrival times in the incoming process and the outgoing process. The detector requires no knowledge of the interarrival distributions, and it is shown to have exponentially decaying detection error probabilities for all distributions. The error exponents are characterized using the Vapnik-Chervonenkis Theory. An efficient algorithm is proposed based on the detector structure to detect renewal processes with linearly correlated interarrival times. It is shown that the proposed algorithm is robust against an amount of **chaff** arbitrarily close to the amount of **chaff** needed to mimic independent processes.

Limitations:	APPROVED FOR PUBLIC RELEASE
Description:	Conference paper
Pages:	9
Report Date:	NOV 2006
Contract Number:	DAAD190120011, NSFCCF04244422
Report Number:	A354184

Keywords relating to this report:

- *CRYPTOGRAPHY
- *DETECTORS
- *INTRUSION DETECTION
- ALGORITHMS
- CHAFF
- DETECTION
- DISTRIBUTION
- EFFICIENCY
- ERRORS
- PACKETS
- PROBABILITY
- TEST AND EVALUATION

« Back to search