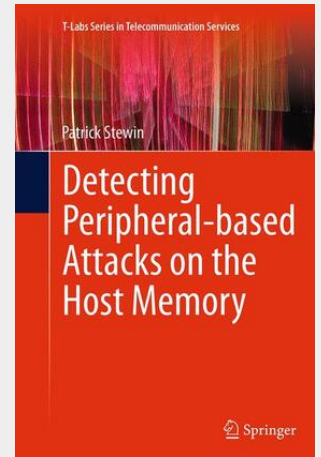


Detecting Peripheral-based Attacks on the Host Memory

This work addresses stealthy peripheral-based attacks on host computers and presents a new approach to detecting them. Peripherals can be regarded as separate systems that have a dedicated processor and dedicated runtime memory to handle their tasks. The book addresses the problem that peripherals generally communicate with the host via the host's main memory, storing cryptographic keys, passwords, opened files and other sensitive data in the process – an aspect attackers are quick to exploit. Here, stealthy malicious software based on isolated micro-controllers is implemented to conduct an attack analysis, the results of which provide the basis for developing a novel runtime detector. The detector reveals stealthy peripheral-based attacks on the host's main memory by exploiting certain hardware properties, while a permanent and resource-efficient measurement strategy ensures that the detector is also capable of detecting transient attacks, which can otherwise succeed when the applied strategy only measures intermittently. Attackers exploit this strategy by attacking the system in between two measurements and erasing all traces of the attack before the system is measured again.

This work addresses stealthy peripheral-based attacks on host computers and presents a new approach to detecting them. Peripherals can be regarded as separate systems that have a dedicated processor and dedicated runtime memory to handle their tasks. The book addresses the problem that peripherals generally communicate with the host via the host's main memory, storing cryptographic keys, passwords, opened files and other sensitive data in the process – an aspect attackers are quick to exploit. Here, stealthy malicious software based on isolated micro-controllers is implemented to conduct an attack analysis, the results of which provide the basis for developing a novel runtime detector. The detector reveals stealthy peripheral-based attacks on the host's main memory by exploiting certain hardware properties, while a permanent and resource-efficient measurement strategy ensures that the detector is also capable of detecting transient attacks, which can otherwise succeed when the applied strategy only measures intermittently. Attackers exploit this strategy by attacking the system in between two measurements and erasing all traces of the attack before the system is measured again.



99,98 €

93,44 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783319386188

Medium: Buch

ISBN: 978-3-319-38618-8

Verlag: Springer

Erscheinungstermin: 24.09.2016

Sprache(n): Englisch

Auflage: Softcover Nachdruck of the original 1. Auflage 2015

Serie: T-Labs Series in Telecommunication Services

Produktform: Kartoniert

Gewicht: 273 g

Seiten: 108

Format (B x H): 155 x 235 mm

