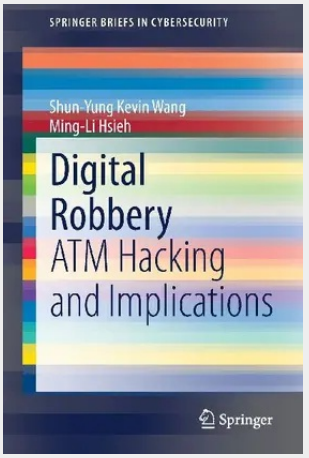
Wang / Hsieh

Digital Robbery

ATM Hacking and Implications



This book begins with a broader discussion of cybercrime and attacks targeting ATMs and then focuses on a specific type of cybercrime named “ATM Hacking.” It discusses ATM Hacking from a more full scope of aspects, including technology, modus operandi, law enforcement, socio-economic and geopolitical context, and theory development. After unpacking a classic case of ATM Hacking and its modus operandi, implications for cybersecurity and prevention, intra- and inter-agency collaboration, and theory development are presented.
This book also demonstrates the analysis of extensive qualitative data collected from a high-profile case in which European criminal group hacked into a London voice mail server belonging to a Taiwanese financial institution – First Commercial Bank,. Then it programmed dozens of ATMs to “spit out” millions of dollars of cash. The successful crackdown on this type of crime is rare, if not unique, while the number of similar crimes has increased enormously in recent years and the trend seem to continue unabatingly. Further, the implications go beyond a country or a continent. Intra- and inter-agency collaboration among players of law enforcement is essential to the case especially in the police context of “turf jealousies.”
The authors seek to document the ways in which agencies collaborate, as well as the perceived benefits and challenges of cooperation. Whether the broader political and contextual climates in which these agencies operate, limit the extent to which they can cooperate.
This book is useful as a reference for researchers and professionals working in the area of cybercrime and cybersecurity. University professors can also use this book as a case study for senior seminars or graduate courses.

This book begins with a broader discussion of cybercrime and attacks targeting ATMs and then focuses on a specific type of cybercrime named ¿ATM Hacking.¿ It discusses ATM Hacking from a more full scope of aspects, including technology, modus operandi, law enforcement, socio-economic and geopolitical context, and theory development. After unpacking a classic case of ATM Hacking and its modus operandi, implications for cybersecurity and prevention, intra- and inter-agency collaboration, and theory development are presented.
This book also demonstrates the analysis of extensive qualitative data collected from a high-profile case in which European criminal group hacked into a London voice mail server belonging to a Taiwanese financial institution ¿ First Commercial Bank,. Then it programmed dozens of ATMs to ¿spit out¿ millions of dollars of cash. The successful crackdown on this type of crime is rare, if not unique, while the number of similar crimes has increased enormously in recent years and the trend seem to continue unabatingly. Further, the implications go beyond a country or a continent. Intra- and inter-agency collaboration among players of law enforcement is essential to the case especially in the police context of ¿turf jealousies.¿
The authors seek to document the ways in which agencies collaborate, as well as the perceived benefits and challenges of cooperation. Whether the broader political and contextual climates in which these agencies operate, limit the extent to which they can cooperate.
This book is useful as a reference for researchers and professionals working in the area of cybercrime and cybersecurity. University professors can also use this book as a case study for senior seminars or graduate courses.

74,89 €
69,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783030707057
Medium: Buch
ISBN: 978-3-030-70705-7
Verlag: Palgrave Macmillan
Erscheinungstermin: 21.04.2021
Sprache(n): Englisch
Auflage: 1. Auflage 2021
Serie: SpringerBriefs in Cybersecurity
Produktform: Kartoniert
Gewicht: 108 g
Seiten: 53
Format (B x H): 155 x 235 mm

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)