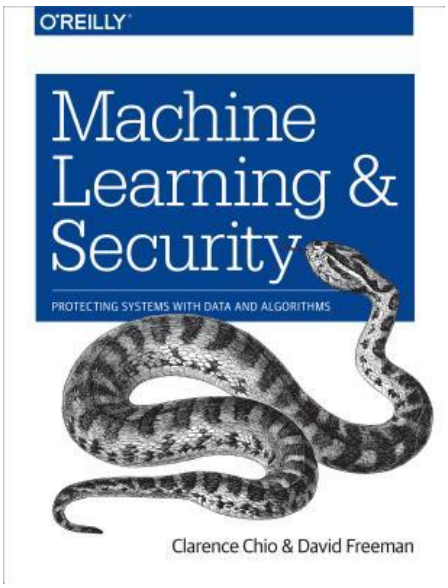

Machine Learning and Security: Protecting Systems with Data and Algorithms

Clarence Chio , David Freeman

Machine Learning and Security: Protecting Systems with Data and Algorithms

Clarence Chio , David Freeman

Machine Learning and Security: Protecting Systems with Data and Algorithms Clarence Chio , David Freeman
Can machine learning techniques solve our computer security problems and finally put an end to the cat-and-mouse game between attackers and defenders? Or is this hope merely hype? Now you can dive into the science and answer this question for yourself. With this practical guide, you'll explore ways to apply machine learning to security issues such as intrusion detection, malware classification, and network analysis.

Machine learning and security specialists Clarence Chio and David Freeman provide a framework for discussing the marriage of these two fields, as well as a toolkit of machine-learning algorithms that you can apply to an array of security problems. This book is ideal for security engineers and data scientists alike.

Learn how machine learning has contributed to the success of modern spam filters
Quickly detect anomalies, including breaches, fraud, and impending system failure
Conduct malware analysis by extracting useful information from computer binaries
Uncover attackers within the network by finding patterns inside datasets
Examine how attackers exploit consumer-facing websites and app functionality
Translate your machine learning algorithms from the lab to production
Understand the threat attackers pose to machine learning solutions

Machine Learning and Security: Protecting Systems with Data and Algorithms Details

Date	:	Published February 17th 2018 by O'Reilly Media
ISBN	:	9781491979907
Author	:	Clarence Chio , David Freeman
Format	:	Paperback 386 pages
Genre	:	Science, Computer Science

From Reader Review Machine Learning and Security: Protecting Systems with Data and Algorithms for online ebook

Delhi Irc says

Location: PTI IRC
Accession No: DL030007

Ben Rothke says

Machine learning and security are all the rage. With the RSA Conference a little more than 2 weeks away, there will be plenty of firms on the expo floor touting their security solutions based on AI, deep learning, and machine learning.

In Machine Learning and Security: Protecting Systems with Data and Algorithms, authors Clarence Chio and David Freeman have written a no-nonsense technical and practical guide showing how you can avoid that hype, and truly use machine learning to enhance information security.

After a brief introduction to what machine learning is, the authors candidly write of the limitations of machine learning in security. They note that the notion that machine learning methods will always give good results across different use cases is categorically false. In real-world scenarios there are usually factors to optimize for other than precision recall or accuracy.

For those that think that machine learning is the latest information security silver bullet, as good as this book is, it certainly won’t help them. But for those that know the limitations of machine learning, the authors suggest approaching it with equal parts enthusiasm and caution, remembering that not everything can instantly be made better with machine learning.

Machine learning works alongside areas such as pattern recognition and computational statistics, and as such, the book is made for those with a strong background in programming, math, and statistics. Most of the programming samples are in Python.

Current technologies like malware and virus classification, intrusion detection, malware classification, network protocol analysis and more are imperfect science. The promise of machine learning comes with many challenges. For those who are willing to invest in doing that, Machine Learning and Security is an indispensable reference.

This is a serious book for those serious about integrating machine learning into the overall information security framework. The reader is expected to know the underlying mathematics and statistics, Python and other languages, and more importantly – how to integrate these into their security architecture. Titles like Machine Learning For Dummies may provide a good introduction to the topic, but it’s books like this that will take you there.
