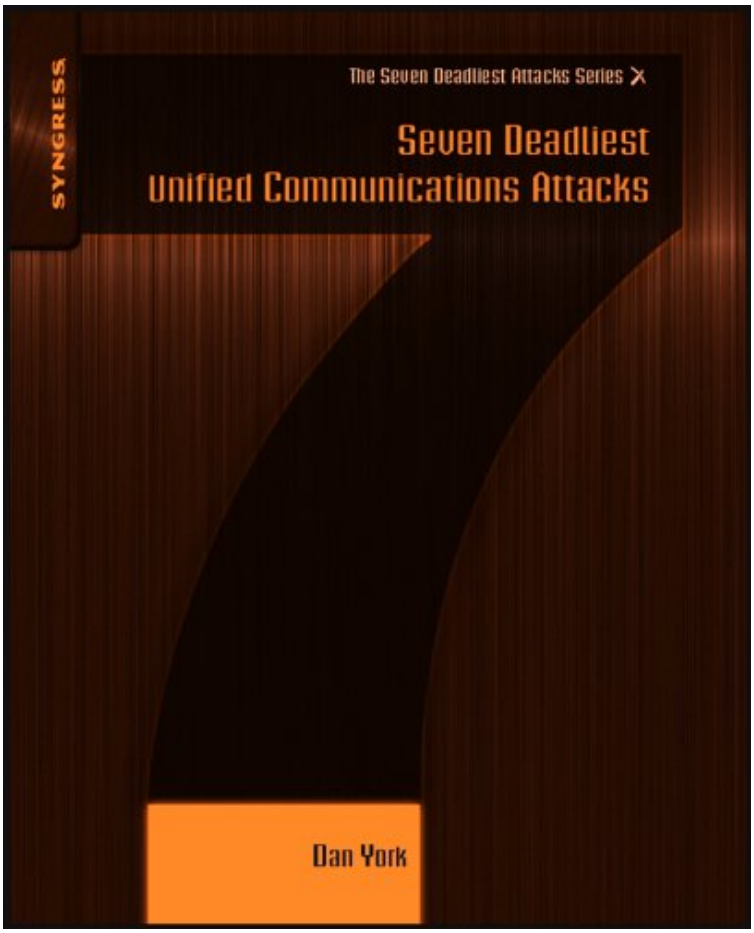
Seven Deadliest Unified Communications Attacks (Seven Deadliest Attacks)

Dan York
**Download PDF | ePub | DOC | audiobook | ebooks*



#2435662 in eBooks 2010-06-04 2010-06-04File Name: B003ZDNYWK | File size: 35.Mb

Dan York : Seven Deadliest Unified Communications Attacks (Seven Deadliest Attacks) before purchasing it in order to gage whether or not it would be worth my time, and all praised Seven Deadliest Unified Communications Attacks (Seven Deadliest Attacks):

0 of 0 people found the following review helpful. Good info; easy readBy TJ in TexasI wanted a good overview of VoIP security issues so that I could better position the aspects of security in our UC platform. I was able to read this in a few hours and better understand the issues and how to position our platform with respect to security. Although I do marketing now I have a technical degree and background as an engineer - the book was sufficiently technical enough but enjoyable to read.1 of 1 people found the following review helpful. Seven Deadliest Unified Communications AttacksBy Mario CamilienBook Title: Seven Deadliest Unified Communications AttacksISBN-978-1-59749-547-9Reviewer: Mario Camilien, CISSPAuthor: Dan YorkAttacks against communications systems have always been challenges that societies throughout the ages have tried to withstand in order to survive. The parallel exists between early societies and those of today. To remain a successful entity - a stable communications system was -- and still is --

a basic tenet of survival.Successful attacks against communications systems, such as roads, waterways, caves, and today's digital media have always been detrimental. Empires such as the Romans --understood that notion well. Their ability to communicate effectively without hindrance, allowed them to succeed in the operations of state, commerce, and the dispatching of armies to the Mediterranean world, North Africa and the Iberian Peninsula. Well protected communications channels allowed the Roman armies to campaign as far East as Parthia -- known today as Iran. The Romans knew that any denial of service (DOS) was a hindrance, and did their utmost best to ensure that all lines of communications remained open. That's not to say -- establishing a secure communication system was an easy task. The Romans believed that "communication was what held their society together ". For that reason the Roman Empire put best security practices in place to protect their communications system. They maintained a protective security posture that incorporated adaptability to emerging threats. They saw all risks as potential dangers to established polity or areas of controls. In today's terms we call it a domain or a unified communications system.In the seven Deadliest Unified Communications (UC) Attacks, Author Dan York takes a close look at the various components which make up today's Communications Ecosystem. As the author puts it, the digital world is ending geography as we know it. Those who are bent on attacking communications systems live by their own rules - come from anywhere --and think differently. They have no configuration management, and no security plan, in others words --they are not overburdened by an organization structure of checks and balances.As outlined by Dan York, the digital world has changed the ways systems are interconnected. It is no longer a domain controlled by few providers (such as ATT, Verizon, and the various states owned telecommunications system such the PTT in France), where the rules of engagement are known and interconnectivities among systems are well established. We now live in a world dominated by heterogeneous endpoint devices which are no longer isolated to their own servers and systems. They are interlinked with a vast number of disparate systems. Systems are distributed and federated in a way that dictates a challenging security posture. Attacks against an existing communications system can be initiated from anywhere in the world.Again, as demonstrated by the early Romans, stable forms of communications remain the foundation for any successful society. However, Dan York states, " Today communication infrastructure is much more complex. You don't only have to worry about your PBX and wiring, you also have to worry about e-mail servers, Web Servers, business systems, desktop PCs...Oh, and of course the underlying network infrastructure". As narrated times and times by the Author " there are dangers associated with the UC Ecosystems.Chapter by chapter the author takes the reader and describes the various dangers such as protocol fuzzing, denial of service attacks, misuse of legitimate Session Initiated Protocol SIP) Signaling, registration erasure or modification, spam for internet telephony (SPIT), Toll fraud and so on. Just like technologies continue to evolve and so are the threats. Those attacks will continue to grow as unified communications continue to expand and interconnect. In closing, the author accomplished the objectives of bringing to the reader the reality that securing digital infractrures will be challenging. As he stated: " Complexity is the enemy of security in that the more complex a system becomes, the harder it is to secure".Mario Camilien, CISSPReferences:1. Gestures and Acclamations in Ancient Rome, Aldrete, Gregory2. French public administration of postal services and telecommunications3. The Session Initiation Protocol (SIP) is an IETF-defined signaling protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP). The protocol can be used for creating, modifying and terminating two-party (unicast) or multiparty (multicast) sessions consisting of one or several media streams. The modification can involve changing addresses or ports, inviting more participants, and adding or deleting media streams. Other feasible application examples include video conferencing, streaming multimedia distribution, instant messaging, presence information, file transfer and online games. From From Wikipedia)0 of 0 people found the following review helpful. Well worth the readBy Andrew ZmolekFor those that don't know Dan York, he helped get the Voice over IP Security Alliance [...] community going and started the Blue Box podcast on VoIP Security [...] so he's been well connected to Unified Communications Security community for many years. With "7DUC Attacks" (as the book has come to be known informally - [...]) Dan provides clear and thoughtful guidance for anyone charged with securing their enterprise UC systems.The hybrid security models that come into play with Unified Communications are not well understood by most enterprises today as we enter this era of massively interconnected communications solutions. There's no magic bullet for UC security, but Dan gives readers the next best thing: accessible security models and straightforward action plans that speak directly to the most unique aspects of UC security challenges.

Seven Deadliest Unified Communications Attacks provides a comprehensive coverage of the seven most dangerous hacks and exploits specific to Unified Communications (UC) and lays out the anatomy of these attacks including how to make your system more secure. You will discover the best ways to defend against these vicious hacks with step-by-step instruction and learn techniques to make your computer and network impenetrable. The book describes the intersection of the various communication technologies that make up UC, including Voice over IP (VoIP), instant message (IM), and other collaboration technologies. There are seven chapters that focus on the following: attacks against the UC ecosystem and UC endpoints; eavesdropping and modification attacks; control channel attacks; attacks on Session Initiation Protocol (SIP) trunks and public switched telephone network (PSTN) interconnection; attacks on

identity; and attacks against distributed systems. Each chapter begins with an introduction to the threat along with some examples of the problem. This is followed by discussions of the anatomy, dangers, and future outlook of the threat as well as specific strategies on how to defend systems against the threat. The discussions of each threat are also organized around the themes of confidentiality, integrity, and availability. This book will be of interest to information security professionals of all levels as well as recreational hackers.Knowledge is power, find out about the most dominant attacks currently waging war on computers and networks globallyDiscover the best ways to defend against these vicious attacks; step-by-step instruction shows you howInstitute countermeasures, donrsquo;t be caught defenseless again, andnbsp;learn techniques to make your computer and network impenetrable

"Anyone charged with securing their enterprise UC systems will find Dan York's clear and thoughtful guidance invaluable as we enter this era of massively interconnected communications solutions. There's no magic bullet for UC security, but Dan gives readers the next best thing: accessible security models and straightforward action plansnbsp;that speak directly to the most unique aspects ofnbsp;UC security challenges." - Andrew Zmolek, Sr. Mgr., Security Planning and Strategy, Avaya, Inc.About the AuthorDan York (CISSP) is the Best Practices Chair for the VOIP Security Alliance (VOIPSA) as well as the producer of "Blue Box: The VoIP Security Podcast" where since October 2005 he and co-host Jonathan Zar have discussed VOIP security news and interviewed people involved in the field. Dan is employed as the Director of Conversations at Voxeo Corporation heading up the company's communication through both traditional and new/social media. Previously, Dan served in Voxeo's Office of the CTO focused on analyzing/evaluating emerging technology, participating in industry standards bodies and addressing VoIP security issues. Since the mid-1980s Dan has been working with online communication technologies and helping businesses and organizations understand how to use and participate in those new media. Dan frequently presents at conferences, has authored multiple books on Linux and networking and writes extensively online at sites such as www.voipsa.org/blog and www.disruptivetelephony.com.