Making PASSWORDS SECURE

Fixing the weakest link in cybersecurity



DOVELL BONNETT
FOUNDER & CEO ACCESS SMART, LLC

Making PASSWORDS SECURE

Making PASSWORDS SECURE

Fixing the weakest link in cybersecurity

Dovell Bonnett

© 2016 Dovell Bonnett. All rights reserved.

Copyright © 2016 by Dovell Bonnett

All rights reserved. Except for appropriate use in critical reviews or works of scholarship, no part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or in any information storage and retrieval system without written permission from the author.

Library of Congress Cataloging-in-Publication Data
Bonnett, Dovell
Making Passwords Secure: Fixing the Weakest Link in Cybersecurity

ISBN: 978-1530164486

Cover Design: Fiona Jayde
Interior Design: Tamara Cribley

www.Access-Smart.com

1. Computers & Technology. 2. Security & Encryption. 3. Network Security.

To my beautiful, loving and supportive wife, Marguerite.
Without your support and encouragement, this book would not have been possible.

And to every business owner, IT manager, and employee
who experiences password fatigue.

DISCLAIMER

Because of the dynamic nature of the Internet, any Web addresses or links contained in this book may have changed since publication and may no longer be valid. The views expressed in this work are solely those of the author and do not necessarily reflect the views of the publisher, and the publisher hereby disclaims any responsibility for them.

The author of this book does not dispense legal advice or prescribe the use of any technology as a form of absolute protection from hackers. The intent of the author is only to offer information of a general nature to help you in your quest for computer security. In the event you use any of the information in this book for yourself, or your company, which is your constitutional right, the author and the publisher assume no responsibility for your actions.

PRAISE FOR *MAKING PASSWORDS SECURE*

I most highly recommend reading the timely and informative book by Dovell Bonnett, "Making Passwords Secure: Fixing the Weakest Link in Cybersecurity". As companies, individuals are increasingly being subjected to breaches and ransomware attacks, the need for cybersecurity awareness and safeguards have become paramount. Thankfully, Dovell, who has been creating computer security solutions for over 20 years, offers a one-stop guide book on how to mitigate cyber threats by explaining the basis and tactics of authentication security. The book is written in a concise style that provides useful information for both laymen and serious techies. It is a book that should be on everyone's reading list!

~ Chuck Brooks, Vice President, Sutherland Government Solutions

If you want to find out about the world of multi-factor authentication in a less technical and more informative way, I can genuinely recommend this book.

~ Sandra Jones, Principal, Sandra Jones and Company

Addictive... Introduces readers to this brave new world of technology, where hackers roam free, and victims include nearly anyone on the Web. Dovell presents this myriad of cyber weaknesses and attack examples in a matter-of-fact voice with intriguing real world examples throughout. It's both fun and informative.

~Eileen Kent, The Federal Sales Sherpa, President, Custom Keynotes, LLC

Understanding the weak points in cybersecurity allows IT to fill them, but not without a budget. CEOs need to understand what their CISOs are facing. No one points this out better than Dovell. Logging on to your computer network will have a new meaning after reading this book.

~Sherman Crancer, Microsoft PCDM

Dovell Bonnett urges business owners to take responsibility for their computer networks and cybersecurity. If you don't get your employees out of the position of network security administrator, then the responsibility of a data breach will be on the owners.

~ William Yeadon, CEO, Chase Security Solutions, Australia

This book is a MUST-READ for any manager in the IT industry. While there are many, competing priorities in information technology, being conversant on the notion of a "Password Authentication Infrastructure" is critical enough to demand everyone's attention. I have received so many "ah-ha" moments as I read this book; things that are right before my eyes that I have given little thought or to which I have paid little attention. Thank you Dovell for opening my eyes to the one commonly used, yet overlooked security vulnerability! Thank you for providing a road-map to addressing this is an effective way! Your writing style and appropriate humor made this topic very digestible!

~ Karen Clay, IT Director, Carlos Rosario International Public Charter School

Making Passwords Secure is a must-read for everyone. No matter what business you're in, strong passwords and effective password management are critical for maintaining secure networks. Dovell Bonnett has done us all a favor by combining his knowledge, helpful stories, and extensive research in an easy-to-read format. Get this on your bookshelf today!

~ Dietrich Wecker, Security Software Developer

Multi-factor authentication is essential for good security, with a remembered password as a common factor. Dovell Bonnett writes in a clear, easy-to-understand, non-technical style, with useful information. This book claims to be "A guide to understanding the weakest links, and appropriate solutions for cybersecurity." I feel it meets these claims, and more.

~ Hitoshi Kokumai, President, Mnemonic Security, Inc.

In this thought-provoking work, Dovell Bonnett digs into the nuts-and-bolts of the authentication challenge and talks about why username-and-password isn't going away anytime soon but can be made secure for many applications. As "The Password Guy," Dovell debunks many of the myths of infallibility surrounding multi-factor authentication and other high-technology solutions, in favor of a pragmatic approach to password management that is a 99% solution to this often vexing enterprise challenge.

~Chris Williams, co-author of *Enterprise Cybersecurity: How to Build a Successful Cybersecurity Program Against Advanced Threats*

ACKNOWLEDGEMENTS

I want to thank the many people who have helped make this book and my business possible. First and foremost, I want to acknowledge Dietrich and Christine Wecker, and Marc Jacquinot for their friendship and collaboration. They ignited my passion for secure password authentication and supported my mission to make ID badges "do more than make a door go beep."

I also want to thank those people who, over my 25 years in the industry, have contributed to my knowledge and understanding of smartcards, cryptography, and the business ramifications of technology. Thank you, John Corbett, Jody Zimmerman, Juergen Hammerschmitt, Chris Goeltner, Robert Merkert, Steve Hamilton, Anne Gregory, Bob Gilson, Alex Giakoumis, Shirley Gonzalez, Mark McGovern, Bryan Ichikawa, Bruce Ross, Mike Dusche, Mark Scaparro, and Dominic Piperno for sharing your time, knowledge, and insight.

I also want to thank the many people within the Microsoft community who encouraged me to write this book. I first need to recognize Casey Watson who had to put up with my badgering question, "So how do you log into Azure?" I also want to thank Sherman Crancer, Candy Stark, Justin Slagle, Maryam Al-Hammami, Kimberley Kenner, Jonathan Frieber, Lacy Finley, David Gersten, Dave Seibert, Veronica Place, Bill Hole, Eric Klauss, and all the other wonderful members of IAMCP. These people and many more who I am just getting to know are amazing, and it is my privilege to know them.

Finally, there are individuals whose guidance and insight have contributed to my business growth and professionalism who I also want to thank: Michael Jalaty, Diane Kehlenbeck, Eileen Kent, Chuck Brooks, Terry Gold, Chris Williams, Hitishi Kokumai, Tamara Bill, Denise Griffitts, Martin Kleckner, Dane Kinnear, Donald Kasle, Denzil Barber, Karen Clay, Mike Rudderow, Aaron Flick, Keith Cunningham, Tom Hope, and Dr. Neil Kalin.

I have been incredibly lucky to have so many people help me throughout my career. It would be impossible to thank them all. I offer this book in gratitude to them all, with my promise to pay it forward.

TABLE OF CONTENTS

Introduction 1
Chapter 1 5
The Real Problem with Passwords

Chapter 2. 17
The Current State of Passwords

Chapter 3. 25
The World of Ciphers

Chapter 4. 43
Authentication

Chapter 5. 53
Multi-Factor Authentication (MFA)

Chapter 6. 61
Cyber Attacks and Best Defenses

Chapter 7. 75
PKI: A Lock is Only as Secure as Its Key

Chapter 8. 89
Cyber Authentication Infrastructures

Chapter 9. 103
Return On Your Investment

Chapter 10. 111
Implementing A Multi-Factor Password Authentication Infrastructure

Chapter 11 131
The Bottom Line

About The Author 133
Resources. 135
Bibliography 137
A Closing Note from Me. 151

I BELIEVE...

...that an individual's personal information should ideally remain in their possession. When your identity is handed over to or managed by a third party, you can lose both your identity and your security.

Identity has become the technology that interfaces with digital devices, software, and the Internet. Technology has been changing and directing how we operate in the world for as long as it has been in existence. It's time to turn the tide and begin directing technology to operate in ways that work for individuals. Humans should be telling digital devices not just what we want them to do, but also how we want them to do it, not the other way around.

Secure authentication is no exception. Instead of being a slave to passwords and the technologies that require them, let me show you how to make technology bend to your will by ***Making Passwords Secure.***

Dovell Bonnett
Founder and CEO of Access Smart

INTRODUCTION

The information in this book is a game changer for both business people and technical people. Business owners, corporate officers, agency managers, and financial decision makers will gain a high-level understanding about what the IT administrator or Chief Information and Security Officer (CISO) worries about and needs in order to protect the business.

The CISO, IT Administrator, and other technology recommenders will gain a greater appreciation for what the business side must have to create purchasing approvals and be better able to communicate what they need, without bogging the business folks down with tech speak.

By arming you with targeted information to make informed decisions about cybersecurity technology, this book is designed to help you implement the best security solution for your organization, become a hero in the boardroom, and protect against a security breach that would seriously damage your company.

It is essential for everyone to understand the one link in your company's computer security chain that is the most ignored and overlooked hole in cybersecurity:

User Authentication and the Management of Passwords.

There are those in the computer security industry who claim that passwords are dead. They are wrong. You'll learn why in Chapter 1. There are those who believe passwords are insecure. They, too, are wrong. That's in Chapter 2. There are those who claim that certificate-based authentication is super-secure and is the only way to protect data. They are only partially correct because certificates are not as strong as they would like you to believe. That's in Chapters 3 and 7. In Chapters 4 and 5, you will learn how many companies, even ones with extensive backend security, could be leaving their virtual front door unlocked. And

if anyone ever tries to convince you there is no way to calculate cybersecurity's Return On Investment, have them read Chapter 9. Finally, Chapter 10 will give you a step-by-step plan to implement the right cybersecurity infrastructure for your situation. These are just a few reasons to read this book.

The many mistaken and incomplete understandings about cybersecurity that are commonplace today drove me to write this book. The truth in this book may not set you free, but it will save you time, money, and valuable resources.

In November 2014, I was invited by a very large computer software company to learn about their newest product and the latest security features they had implemented to protect their customers' information. While the presenter spoke, I sat quietly listening and nodding, but expressing no excitement or praise for what they were conveying. Afterward, the presenter came over to me and asked me point-blank if I was impressed with what they had done. I told him I was impressed, but I had one simple question. The conversation went something like this:

Dovell: "How do you log in to your software?"

Presenter: With a confused, but also 'you're an idiot' look on his face, he said, "With your computer."

Dovell: "Yes, I understand. But how do you log in to your software?"

Presenter: In a perturbed voice, he said, "With your user account information."

Dovell: "Right. That's great. But how do you log in to the software?"

Presenter: Now, in a tone of almost pure disgust and a 'Why am I wasting my time with you' attitude, he said, "With your user name and password."

Dovell: "Exactly! And as soon as my password is stolen, all that amazing backend security no longer matters."

That was the moment when he finally understood the importance of secure authentication. The software was Microsoft's Azure. After that meeting, I worked

with Microsoft to put out a press release announcing how Power LogOn® and Azure together secures your data from fingertips to storage.

Cybersecurity needs to start when the computer is first turned on. If just anyone can turn on your computer, all security bets are off. If you wait until the user is past the firewall to authenticate him, you are too late.

As the owner, manager, or chief officer of a business or agency, you are responsible for funding cybersecurity investments. If you don't understand what you are buying and why you need it (or don't need it,) then how can you know if you are making the right choices?

According to the National Cyber Security Alliance, forty percent of small- to medium-size businesses are victims of a cyber breach. Sixty percent of those SMBs go out of business within six months. And while large enterprises may be able to weather an attack, they will spend hundreds of thousands to millions of dollars in damage control and trying to shore up their computer networks. Even then, money cannot solve all the issues of a successful data breach.

No matter what size business or agency you are dealing with, this book will lead you step by step along a path to protect your data, your company, and yourself by understanding and building secure, trusted identity authentication. That trust begins by first... **Making Passwords Secure.**

CHAPTER 1

THE REAL PROBLEM WITH PASSWORDS

"I am concerned for the security of our great Nation; not so much because of any threat from without, but because of the insidious forces working from within."

~ General Douglas MacArthur

Today's computer networks are complex and decentralized, creating multiple points for hackers to attack. This fact alone makes cybersecurity both important and difficult for information technology (IT) administrators to achieve. These managers not only have to deal with keeping servers, operating systems and applications up-to-date, but now they are also tasked with managing Bring Your Own Devices (BYOD), Clouds, phishing, pharming, social engineering, and many other threats.

Because we live in the Internet age, IT managers also worry about the network security of other companies, something they have zero control over. Sending a simple email from one person to another may involve hundreds of vulnerabilities.

Despite all these attack points, whenever a data breach is reported in the news, the lack of strong passwords often gets blamed first. The main reason passwords are the easy scapegoat (especially in the media) is because people actually know what passwords are and everyone is frustrated with trying to manage them.

Password authentication is not the problem.

The *management* of passwords is the real security nightmare.

In our world of ever-increasing cyber-attacks, IT invests massive amounts of time, resources, and money to secure corporate networks and data, train employees to be wary of attacks, and perform 24/7 monitoring of data traffic to spot anomalies. Because there are no silver bullets, many different security technologies are utilized to address each potential threat, and often not in a coordinated fashion.

With so many vulnerability points for hackers to target, where should cybersecurity start? The first line of defense must be **trusted authentication of the user.** User authentication has to start when you turn on the computer, *before* the operating system is fully loaded. If authentication takes place behind the firewall, where Single Sign-On and One-Time Password technologies reside, it's too late. For the vast majority of computers in the world today, an end-user implements authentication via a user name and password. That makes password authentication the elephant in the room everyone is ignoring.

There are three considerations when evaluating the security of passwords:

1. Password Authentication;
2. Password Management; and
3. Password Infrastructure.

When these three considerations are successfully integrated, making passwords secure is not only possible, but passwords actually become a very effective, cost-efficient, and user-friendly feature contributing to robust cybersecurity.

Password Authentication is Secure! Password Management is the Beast!

IT managers, along with a multitude of costly network security protections, frequently cannot prevent a breach because a legitimate user name and password is used. How do hackers and criminals acquire legit user names and passwords? The easiest targets are employees.

The ten most common criticisms levied against passwords include:

1. Passwords are not long enough to be secure
2. Passwords don't always include different cases, numbers, and special characters
3. Passwords use words that can be found in a dictionary
4. Users choose passwords that include personal information
5. The same password is used on multiple sites
6. Passwords are not changed frequently
7. Users write passwords on notes or store them in smartphones, computer files, etc.
8. People can look over your shoulder as you type passwords
9. Malware programs like keyloggers capture passwords as a user types them
10. Users disclose passwords to hackers through social engineering tricks

Think about it. Are these complaints the fault of password authentication viability, or how and who manages those passwords? It makes no difference what authentication method you use, including certificates and biometrics (the ability to use anatomical, physiological, or behavioral characteristics as unique identifiers). If the authentication methodology can be compromised, the system will be breached.

Where passwords were used to gain unauthorized access, investigators eventually discovered that hackers simply took advantage of poor password management or social engineering tactics. These breaches had nothing to do with whether passwords are a secure and viable means of authentication. When corporations task their employees with managing their own passwords, they inadvertently put the most insecure element of security in charge of security. Since no manager wants to blame his/her employees, passwords take the hit.

This is not to say that employees are bad people or are out to defeat cybersecurity. Far from it. Because of staffing cutbacks, most employees today are working harder than ever. They have more responsibilities and more stress than ever before. Managing the average 50 to 100 user names and passwords while trying to follow complex password policies can become so cumbersome that employees look for shortcuts to create what they see as efficiencies. Unfortunately, those shortcuts can wreak havoc on a company by creating vulnerabilities that thieves exploit to steal customer credit card information, customer passwords, company confidential data, and more. All you have to do is listen to the news reports after a data breach to hear the horrors. Many of those could have been

prevented by incorporating a robust enterprise password manager that takes the employee out of the business of securing the network.

Passwords Are Not Going Away Anytime Soon

Computer authentication is made up of three parts (called "factors"): something you Have, something you Know, and something you Are. Together, the industry refers to these as "the three factors of authentication."
Passwords are the something you *know*. If passwords disappeared completely, then authentication would be left with only two factors. This is something no security professional would ever support. Finally, passwords are the only factor of the three that can be easily, cheaply, and frequently changed. That's why, as an authentication methodology, passwords are both effective and here to stay.

> **Note:** A new authentication factor is under discussion since the introduction of GPS-enabled smartphones. The new proposed factor is "Where you Are."

What *Needs* to be Fixed is How Users Manage Passwords

Employees (or end-users) are the weakest link in any computer network for three reasons. First, they do a very poor job of generating passwords. The passwords they choose are easy to crack. Second, they can't remember their passwords, so they write them down and store them in places where they (and others) can find them. And third, end-users are susceptible to social engineering schemes (aka human hacking) which hackers use to get people to voluntarily give up their passwords.

> When employees are given the responsibility to generate, know, remember, type, and manage passwords, IT has inadvertently given employees the job title "Network Security Manager."

SOMETHING TO THINK ABOUT

You may remember the movie "Catch Me If You Can" staring Leonardo DiCaprio, Tom Hanks, and Christopher Walken. The movie was about

Frank Abagnale, who in 1963 started as a con artist (social engineer.) Fast-forward to the computer age where the poster kid for computer social engineering has to be Kevin Mitnick. Kevin was a hacker and fugitive, breaking into computer networks, creating false identities, and running from authorities for years. At one point when the FBI was closing in to arrest Kevin, he escaped, but not before leaving a fresh box of donuts in the refrigerator marked "FBI donuts."

In his book *The Art of Deception*, Kevin shares how he used social engineering, not hacking tools, to discover passwords so he could break into computers. Kevin also says, "Testifying before Congress not too long ago, I explained that I could often get passwords and other pieces of sensitive information from companies by pretending to be someone else and just asking for it." He goes on to explain that social engineering takes advantage of people's gullibility, naiveté, ignorance, and stupidity. A quote from Albert Einstein sums up Kevin's philosophy: "Only two things are infinite, the universe and human stupidity, and I'm not sure about the former."

Like Frank Abagnale, Kevin was eventually caught, served his time and now runs a computer security consulting firm where he helps businesses secure their computer networks. I'm sure Kevin would agree that one of the best ways to prevent data breaches is to get the employee out of the role of network security manager!

Myth: Users Must Know Their Passwords

The concept of a password or pass phrase dates back to ancient times. They were required for access into places like a castle, camp or even a professional guild, such as the Freemasons Society. A guardian would challenge the visitor for the password. If the stranger answered correctly, he was recognized as a friend and allowed to pass. If the wrong password was used, swords were drawn.

During World War II, Americans used passwords like "Lollypop," "Licorice," or "Lollapalooza" because the Japanese language does not have the "L" sound, which made it difficult for Japanese soldiers to pronounce these words.

In modern times, computer passwords have become the digital authentication representing the "something you know." Where and how a person reveals their

password has changed significantly (from a sentry to a computer) and it's time for an update to our understanding of how passwords should and can function in the twenty-first century.

The current definition of "password" according to Dictionary.com is:

Password: noun

1. A secret word or expression used by authorized persons to prove their right to access, information, etc.

2. A word or other string of characters, sometimes kept secret or confidential, that must be supplied by a user in order to gain full or partial access to a multiuser computer system or its data resources.

One of the biggest misconceptions about passwords is that passwords must be the thing that a person *knows, types, or speaks.* That is literally an ancient and false belief! In the wake of massive computer advancements, why are humans still being asked to generate, know, and reveal passwords? Shouldn't technology be doing that?

Here's my take on an updated definition of "password:"

Password: noun

1. A shared secret expression or other string of characters exchanged human-to-human, human-to-computer, or computer-to-computer for the purpose of authenticating access to facilities, services, computer networks, and/or data.

Not only does a user *not* need to know his password, he also *shouldn't* have to remember it or type it. This is good for both the end-user and network security because it diminishes the effectiveness of social engineering hacks. How can an employee reveal something he doesn't even know?

Hackers vs. Crackers

The media has confused hackers and crackers. Not all hackers are crackers, but all crackers are hackers.

A hacker (also called a White Hat hacker) is someone who is able to analyze, take apart, and then re-assemble a device or code to make it do something it was never intended to do.

A cracker (also known as a Black Hat hacker) is an individual with the same skills as a hacker, but they use their knowledge to do harm for personal or financial gain. The harm or devastation they do to businesses, governments, and individuals is of no concern to them. In this book, when I use the word "hacker," I am referring to that person's ability to break a system. However, when the break is used for illegal or malicious purposes, I use the term "cracker."

Identity Theft

The theft of an individual's computer credentials is fast outpacing the theft of credit card data. Credentials allow unfettered access to accounts and services. With the identity theft epidemic, how can one really be sure that a person is who they say they are?

Driver's licenses can easily be forged, Social Security numbers stolen, and fake passports printed, resulting in trusted documents being brought into question. Legitimate and honest registration authorities and certificate authorities are having a difficult task trusting the documentation and identity of individuals requesting certificates. Fraudulent documents lead to fraudulent certificates, which lead to serious cyber-attacks and data breaches.

Identity theft is much more than a stolen credit card. Many laws require companies to report breaches, and the penalties are far more severe for the business than they are for the criminals utilizing the false identity. Additionally, there are very few laws to help victims and make the recovery process manageable. The number one way individuals are exposed to identity theft is through corporate data breaches, making this a massive problem.

Companies need to understand both the direct and indirect costs of a data breach. While different organizations calculate the costs in different ways, the Ponemon Institute is the most widely quoted research firm that analyses the costs of a data breach to companies. According to Ponemon's *2015 Cost of Data Breach Study* report, the average cost to a company *per sensitive record* lost or stolen in the United States over the last few years is:

- **2013:** $188 per record for a combined average total cost of $5.40M per company

- **2014:** $201 per record for a combined average total cost of $5.85M per company

- **2015:** $217 per record for a combined average total cost of $6.53M per company

Defending against data breaches and identity theft is outside the scope of this book. There are books on the market that address that topic specifically. From my perspective, data security must start before the firewall when a computer is first turned on. Having a strong, secure Password Authentication Infrastructure (PAI) is a key component to safeguarding computer networks.

Chain of Trust

A chain of trust is built on the premise that within a computer network, all hardware and software is authorized and disperses information only to authorized users or places. The problem with networks today is that they are so complex and decentralized. One weak link within this chain becomes a portal hackers can exploit to gain access to other parts of the network, until they eventually achieve full system administrative rights. Then, all confidential data and private information becomes available for the hackers to use as they wish.

Crackers are highly motivated to access private information for their own personal, financial, political, or social gain. And they have a vast arsenal at their disposal to penetrate a network: technology, social engineering, careless employees, indirect network connections, and more.

The best IT can do is to try to protect against known attacks, which is an almost futile endeavor. Trying to protect against every known attack is not only cost prohibitive, but hackers and crackers constantly make minor modifications to their attacks in their efforts to get past security. They have copies of every antivirus software on which they test their malware over and over, tweaking it until it gets through. Then they release it before anyone has a defense. This fact alone gives crackers a huge advantage. It also creates the greatest fear of the Chief Information Officer (CIO) and Chief Information Security Officer (CISO): the unknown attacks.

When a hacker decides to break into a network, what do you think he wants most? What does he go after first? Ideally, he wants the network administrator's authentication credentials because he knows that will give him complete access. He starts wherever he sees the weakest link, using that point to burrow his way

in. Once he gets the desired credentials, he has free rein of the entire network to access confidential data, inject malware, or reprogram peripheral hardware to perform unintended tasks.

SOMETHING TO THINK ABOUT

I recently heard a White Hat hacker tell a shocking story. A bank hired him to test their network. In a matter of minutes, he was in their network snooping around. That was his first task. While in the network, he came across some IP addresses that he didn't recognize. After a quick investigation, he discovered they were the IP addresses for the bank's network of ATMs. Wanting to test the security of the ATMs, he wrote and uploaded a program into the network to have a specific ATM spit out a twenty-dollar bill the next day at 12:02 a.m. At the appointed hour, he hopped in his car and drove to the remote location. Just before midnight, he set up a video camera and pointed it at the dark ATM machine. He waved at the camera and waited. At 12:02 a.m., right on schedule, the ATM magically came to life. The screen lit up, the cash door opened, and the machine spit out a twenty-dollar bill.

It doesn't matter how or where a breach occurs, once the hacker has broken in, the entire network loses the chain of trust.

Password Alternatives

The plethora of computer breaches and password database thefts has caused some security pundits to rail against passwords. Michael Daniel, Special Assistant to President Obama and the U.S. Cybersecurity Coordinator (Cyber Czar), said recently, "One of my key goals in my job that I would really love to be able to do is to kill the password dead." But, what would replace passwords? Certificates? Biometrics? Smartphones? Or something else?

A digital "certificate" is the combination of cryptographic functions (symmetric and asymmetric ciphers, hashing, and digital signature) with infrastructure components (Registration and Certificate Authorities, encryption acceleration hardware, Key management, HSM, and smartcards) used to generate an electronic "passport." This passport or certificate allows individuals, computers, and organizations to trust each other over the networks and to securely exchange information.

Certificate authentication, which can be expensive and is not necessary for every business environment, offers high levels of assurances that the identity of a person or device really is who they say they are. However, there are many cases where sloppy identity authentication, poorly managed keys, and the subpoenas of Private Keys make certificate-based systems just as weak and vulnerable as poorly managed password systems. Because of the overall infrastructure complexity of certificate-based systems and the false sense of security some IT managers place in digital certificates, they can be more vulnerable to an attack than some security experts are willing to acknowledge.

Biometrics also have cost and implementation considerations. And smartphones require charging and monthly service fees. All these alternatives do have a place in specific environments, but they cannot replace the humble password across the board.

That is why I am introducing a new concept I call "**Password Authentication Infrastructure**" (PAI.) Like all security infrastructures, PAI is based on combining and utilizing the strengths of many different technologies and techniques which, when taken together, become stronger than their parts.

Password Authentication Infrastructure (PAI) for enterprise networks addresses four basic principles:

1. Removal of the user as a network security manager
2. Creation of IT centrally managed secure passwords and policies
3. Installation of a strong password manager
4. Utilization of multi-factor authentication

When cracking passwords becomes as difficult as cracking cipher keys, then passwords will be secure.

This book does *not* compare the operational functions or benefits of ciphers versus passwords, because they are unrelated. Ciphers are software algorithms used to encrypt data. Passwords are a means of user authentication.

This book *does* analyze an important cipher component that the security industry goes to great lengths to protect: the keys. Keys are the secrets you need to know to unlock the cipher algorithm. If a Key is ever compromised, it will not matter how great an algorithm is because it will have been made instantly worthless. In my opinion, cipher keys are really just glorified passwords. In fact,

the only thing distinguishing keys from passwords is that far more time and money is spent securing keys, while password protection is often ignored.

> When security is cumbersome to use, end-users will circumvent security for convenience. But, convenience without security is neither convenient nor secure.

Password security is easy to fix and far more economical to implement than a cumbersome and complex Public Key Infrastructure (PKI). I admit, there are environments where PKI is appropriate, but it is not an efficient or appropriate use of resources for most companies. The good news is, there are other choices along the computer security spectrum between simple user-managed passwords and PKI.

At the opposite end of the spectrum from PKI, simple password managers may be convenient, yet how they are implemented can be anything but secure. Using an Internet browser to secure passwords is extremely insecure because anyone using that computer can access them. Companies like Trend Micro, Google, and LastPass have all experienced security breaches. Password security involves so much more than just a password manager. Robust password security requires an infrastructure.

In this book, you will discover exactly how symmetric and asymmetric keys are similar to passwords, what makes these encryption key methodologies appropriate for select environments, and how the same security techniques can be deployed to protect passwords for everyone else. A Password Authentication Infrastructure (PAI) can drastically improve a company's return on investment (ROI). And yes, it really is possible to make employees, executives and IT professionals happy, secure, and productive.

It's time to tame the password beast!

CHAPTER 2

THE CURRENT STATE OF PASSWORDS

"Our problems stem from our acceptance of this filthy, rotten system."

~ Dorothy Day, American Journalist

Password data looms as a primary target for nefarious crackers because it is the easiest way to gain access into a company's network. Just because data are stolen does not mean it has been used to commit a fraud. Fraud begins when criminals exploit stolen credentials to gain unauthorized network access.

In my first book, *Online Identity Theft Protection for Dummies*®, I explained the difference between "identity theft" and "identity fraud." The same holds true for password theft vs. password fraud:

Password data *theft* is the actual stealing of passwords through data breaches, social engineering, and a multitude of other means.

Password authentication *fraud* is the act of using someone else's identity to gain unauthorized access into a computer network.

Securing a company against theft involves different protocols than securing against fraud. Password Authentication Infrastructure (PAI) addresses both.

IT first needs the tools to safeguard password data. If password data becomes compromised, IT should have the capability of making it all useless. Second, the

system needs to be able to authenticate that the real authorized user is actually presenting the password entered. This is where multi-factor authentication comes in.

Who Should Manage the Password?

IT can inadvertently be its own worst enemy when it comes to security. Employees often see security policies as a hindrance to their jobs, which forces them to circumvent security for their own personal convenience. In my experience, IT appears to overlook this fact.

I talk to many Chief Information Security Officers (CISOs) and I always ask them if they have a secure log-on policy. They all give me the same resounding "Yes!" According to these CISOs, they have implemented a password policy made up of the same old requirements we've been hearing about since the 1990s: use eight to nine characters, different character types, change them every sixty to ninety days, and do not allow the reuse of the last five passwords. When I ask those same CISOs *how* the employees *manage* their policy, they have no idea. Their only concern seems to be that they have a "strong" policy in place.

The Weakest Link

What IT is missing is that network security is only as strong as its weakest link. They themselves put the weakest link—the user—in charge of implementing IT's policies. Employees tend to create shortcuts and workarounds that include using the same password in multiple places, writing them down, or trying to come up with something that is easy to remember and type. This combination of security policies and users' habits is what makes computer networks inherently insecure. My concern is that these CISOs are thinking only from the perspective of their side of the security fence, about meeting security compliance requirements, and not about how the employee/end-user is going to manage those policies. The implementation (not the existence) of strong policies determines a company's network vulnerability.

Today, the average number of accounts that each user has to manage is somewhere between fifty and a hundred. When I combine both my personal and professional accounts, I have closer to three hundred different places that require me to enter a user name and password. How many do you have? Even on the low end, twenty-five to fifty unique user names and passwords are way too many for a human being to manage securely.

As I mentioned earlier, passwords are just one factor of authentication. So, what does one single factor actually get you? It only proves that the person or

machine entering the code knows the secret. It does not prove that the person or machine is authorized to know that secret. While some security experts believe that frequently changing passwords and having complex passwords ensures authentication by making it much harder for hackers to discover their password, that really does very little. With the tools hackers have at their disposal, they can know a new password almost as soon as the user generates it.

The Missing Link

Another problem with today's password security is that the onus is on the user to maintain strong security practices. Think about it. Have you ever used the same password more than once? Written them down or typed them into a spreadsheet? Or used something like your child's birthday? How many times a day do you think employees and end-users circumvent security for their personal convenience? Virtually every computer user and company in the world face this serious problem. Unfortunately, nearly all of them have their heads in the sand about their most overlooked and under-solved problem. The missing link in network cybersecurity is an integrated set of tools that make passwords both secure and manageable *for the user*.

Humorous Ways Users Manage and Generate Passwords

After being in the password authentication business a very long time, I have collected a long list of zany ways people manage their passwords. One of the most common is the Word document or Excel spreadsheet titled "Passwords" and placed on the computer desktop. Of course, no hacker breaking into their computer would ever find this document, let alone open it, right?

Then there is what I like to call "Sticky Note Security." This is the writing of passwords on sticky notes and placing them on the computer monitor for easy access. Users trying to create some sense of security may hide their notes under the keyboard. Writing down passwords may free users from trying to remember all of their passwords, but then they have to remember where they hid them.

A few years back, the CEO of a marketing firm bet me a steak dinner that I could not find any of his employees' passwords because he had a written policy against writing them down. Not wanting to miss a dinner at Ruth's Chris, and hoping that he really did have security in place, I took the bet. To give him even better odds of winning, I let him choose which employee's cubical I was to search.

In less than two minutes, I found the password-laden sticky note hiding under the tissue box on the bookshelf. Over a juicy, medium rare, sixteen-ounce prime rib, we talked about how to improve his network security. The policy is not the challenge, it's the implementation.

I came across another example of poor password management in a slight variation of sticky note security. An executive at a large hotel chain wrote all her passwords on her white board. According to her, since hidden sticky notes will be found, and replacing them only adds to the landfill, she might as well make log-on easier on herself by just writing them on the white board in front of her desk.

The way employees generate passwords is equally creative. There's a joke going around that when I asked a client what his password was, he answered, "MickeyMinnieDonaldPlutoDocSleepyHappyDopey." When I asked why such a weird password, he replied, "It has to be eight characters long." While that may sound goofy, it's even worse when people use their anniversary date, kids' names, or the place where they met their spouse. All that information can usually be found by hackers in employees' Facebook, Google+, Twitter, or some other social media profile.

Here are some other similarly absurd password recommendations from so called "password experts:"

- Find a book title, poem, phrase, or favorite quote and then use the first letter of each word of the phrase or quote. According to the expert, you now have a complex password you can remember. What's wrong here is that the same password will be used at multiple sites; otherwise, the user has to remember a different quote for each site.

- Another one is to replace a known password with the letter in the alphabet just to the right or left of each character. I don't know about you, but when I sit down at a computer, the last thing I want to do is run a cipher algorithm in my head. Besides, even the entry-level hacker knows this trick and has automated tools that check for it.

- Perhaps the most ridiculous one is where the user picks the password based on the site's log-on message. When you visit a site, the screen might say, "Please enter password." So the password the user types in is, "PleaseEnterPassword." To keep passwords unique, they might choose,

"GooglePleaseEnterPassword" and "AmazonPleaseEnterPassword." While it meets most of the password requirements, it's another well-known trick.

These examples would be funnier if they weren't true. Generating and managing passwords is extremely important. These examples hopefully show you just how poorly your employees do it.

How Are Your Passwords Protected?

Many IT administrators will protect their password database the same way they protect all their other data. The data are stored behind a firewall, may require another password to access it, and are on the same server that also stores the company's marketing collateral, general reports, and other non-critical data. If the main goal is to prevent password theft, why would the password data file be stored on the same server that requires very limited security?

A more security-conscious IT manager will build on additional layers of security. They realize that at some point, a hacker may get the password data. The next layer of security should make the data unreadable and worthless. Here is where data encryption is applied. The savvy IT manager will implement encryption, hashing, and a host of other technologies that I will explain in a later chapter, and will also have a dedicated server just for passwords and other log-on credential information. Segregating sensitive data allows IT to monitor access, watch for anomalies like excessive pinging, and block URLs that are suspicious. By segregating data, IT can better monitor and prevent attacks, which could otherwise get lost in the noise of non-critical traffic.

SOMETHING TO THINK ABOUT

Recently a healthcare center IT administrator, who wishes to remain anonymous, did an independent network security audit. After a few hours of testing, the auditor presented his findings. The provider received a failing grade. However, they passed the government's HIPAA compliancy requirements because their security policies and procedures were all documented. The problem was that IT failed to monitor how their employees actually implemented and managed those policies. It was discovered that every healthcare worker used the exact same password: "Nurse123." The IT administrator could

> never truly authenticate a user, and if there ever was a breach, the audit reports would be useless.
>
> The main disjoint between policies and implementation is the human factor. While it is true that long, complex, unique passwords that change frequently offer greater security, an employee frustrated with trying to remember all his passwords will do silly things that circumvent security for convenience. That is what hackers exploit.

These examples remind me of an old saying: "Computer security is easy. That is, easy to do poorly." Whatever issue you're dealing with, remember to ask yourself, "Are these password *authentication* problems? Or are they password *management* problems?

Laying the Foundation

Before jumping into how to create the Password Authentication Infrastructure (PAI) that meets your specific needs, I first want to build a foundation. All infrastructures bring together multiple components. Each component has its own strengths and weaknesses. The goal is to capitalize on one component's strength and then leverage in other components that address remaining weaknesses.

Cybersecurity infrastructure systems include the following elements:

- Ciphers
- Safeguarding Secrets
- Authorization
- Multi-factor Authentication
- Secure Hardware Modules
- Secure Channels of Communications

After a brief overview of each of these components, I will show you how easily you can incorporate these same principles into password security.

The best way to implement security is to first understand the attacks and methods hackers use against the different security components. In the next chapter, the flaws in current attempts at password security will become very clear, along with how PAI addresses each of them.

Finally, security implementation involves more than just technology. There is a business component that has to justify IT expenditures to the CFO and CEO.

That's why I also cover the return on investment (ROI) for password authentication security in a later chapter.

It is only when security is designed with a holistic, comprehensive approach that security really works. Nothing can be left to chance or taken for granted. And while no security system will ever be completely foolproof, when enough security layers are implemented, most hackers get frustrated by the barriers and go elsewhere. Layered security also gives IT more time to discover anomalies and kick out intruders before a breach occurs.

ABOUT THE AUTHOR

Dovell Bonnett – "The Password Guy"

Dovell Bonnett has been creating computer security solutions for over 20 years. His passionate belief that technology should work for humans, and not the other way around, has lead him to create innovative solutions that protect businesses from cyber-attacks, free individual computer users from cumbersome security policies, and put IT administrators back in control of their networks.

He has spent most of his career designing solutions to solve business security needs, incorporating multiple applications onto single credentials using both contact and contactless smartcards. The most famous example of his work is the ID badge currently used by all Microsoft employees.

Back in 2000, Dovell was contacted by Indala (a division of Motorola) as a consultant to help them solve a security problem for one of their largest customers. The customer had just experienced a major cyber breach and the hacker had stolen important source code. The requirement was to create a single employee ID badge that would allow the employee secure authorized access into buildings and secure authorized access into computer networks.

After he explained to Indala how simple that would be, they immediately made Dovell their director of smartcard development. The customer turned out to be Microsoft and the project was the first time physical and logical access had been combined on a single corporate ID badge.

When the Indala division was sold by Motorola, the outgoing president told the new CEO he could get rid of all the upper management except Dovell because, "He is your visionary that will take you out five to ten years into the future." Dovell offered his new company the vision that businesses have two front

doors: the physical and the virtual, opening up a whole new market potential. Unfortunately, the new CEO pushed back, saying, "Dovell, you don't understand our business. We make doors go 'beep.'" That eventually led Dovell to exit the corporate world so he could manifest his vision.

In 2005, he founded Access Smart LLC to provide logical access control solutions to businesses. His premiere product, Power LogOn, is a multi-factor authentication enterprise password manager used by corporations, hospitals, educational institutions, police departments, government agencies, and more.

Dovell has held positions at National Semiconductor, Siemens (Infineon), Certicom, Motorola, and HID. In addition to his involvement with Public Key Infrastructure (PKI) and Elliptic Curve Cryptography, he has also held a Top Secret security clearance with the United States Navy while working on communications for nuclear submarines at GTE Systems.

Dovell has contributed to numerous papers for the Smart Card Alliance organization; magazines, including *Card Manufacturing Magazine*; and is the author of two books, *Online Identity Theft Protection for Dummies®* and *Making Passwords Secure: How to Fix the Weakest Link in Cybersecurity*. Dovell is a frequent speaker and sought-after consultant on the topic of passwords, cybersecurity, and building secure, affordable and appropriate computer authentication infrastructures especially PAIs.

He can be contacted at:

Dovell Bonnett
Founder and CEO, Access Smart LLC
(949) 218-8754
Dovell@Access-Smart.com
www.Access-Smart.com

A CLOSING NOTE FROM ME

As you probably can tell, I love passwords and believe through proper management they are secure. One of the best ways to start is by reviewing Chapter 10: "Implementing a Multi-Factor Password Authentication Infrastructure" again. If you are interested in learning more about how a PAI can work in your company, agency or small business, then I have a free gift for you.

The one common denominator when it comes to all computer networks is that there is no one common denominator. I am offering you a free, one-hour consultation where you can ask me anything about secure authentication, smartcards, or combining physical and cyber access control. If I don't know the answer, I will point you to the people or companies who will.

All you have to do is navigate over to http://www.MakingPasswordsSecure.com/contact-us/, Select "**Consultation**", type "**My free 1hr session**" in the email subject line, and fill in your contact information. Let me know your preferred day and time you would like to talk. Please include a couple of alternative days and times to help coordinate both our schedules.

Contact me now and you could have a PAI system up and running within days. Really!

Have a look at https://www.access-smart.com/power-logon/ if you want to research a PAI solution that includes everything to start a test pilot.

Making PASSWORDS SECURE

Passwords are not the problem.
The management of passwords is the real security nightmare.

User authentication is the most ignored risk to enterprise cybersecurity. When end users are allowed to generate, know, remember, type and manage their own passwords, IT has inadvertently surrendered the job title Network Security Manager to employees - the weakest link in the cybersecurity chain.

Dovell Bonnett reveals the truth about the elephant in the room that no one wants to mention: Expensive backend security is worthless when the virtual front door has a lousy lock!

Dovell proves that making passwords secure is not only possible, passwords can actually become an effective, cost efficient and user friendly feature of robust cybersecurity. After examining how encryption keys are secured, this book introduces a new strategy called Password Authentication Infrastructure (PAI) that rivals digital certificates.

Passwords are not going away. What needs to be fixed is how passwords are managed.