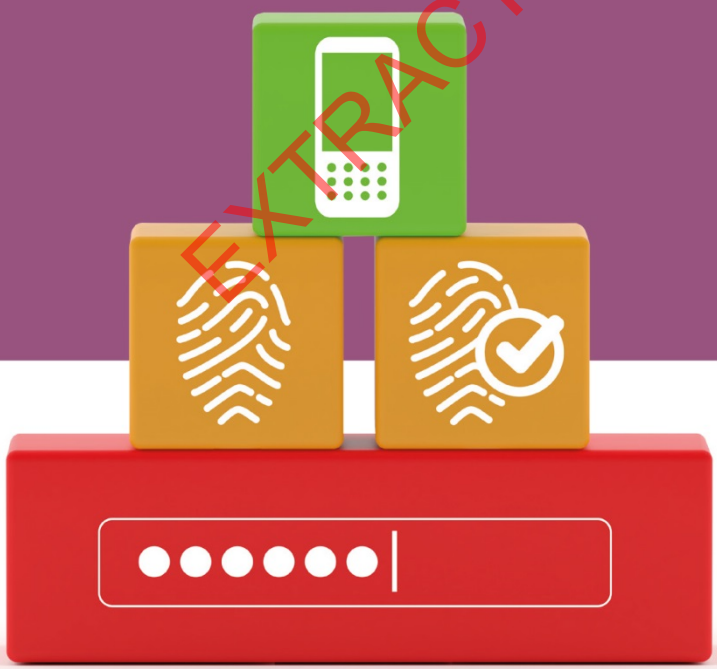
TWO-FACTOR AUTHENTICATION

Mark Stanislav



Information Security buzz

itgp™

Two-Factor Authentication

MARK STANISLAV

IT Governance Publishing

IT Governance Publishing
IT Governance Limited
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambridgeshire
CB7 4EA
United Kingdom
www.itgovernance.co.uk

First published in the United Kingdom in 2015
by IT Governance Publishing

ISBN 978-1-84928-733-3

FOREWORD

If there is a more hated, feared, or otherwise misunderstood word associated with information technology than ‘password’, I don’t know it.

My authentication-security baptism occurred in 1982 during my first commercial security project fixing the 30-line password algorithm of ACF2 (SKK, Inc.). Since then, I’ve only gone further down the rabbit hole of this critical area of information security.

Because ACF2 was the leading mainframe security product, and the primary product protecting US and other Western governments, we were heavily involved with trust certifications. These included C2 and B1 levels of assurance documented in the ‘Orange Book’ in the noted ‘Rainbow Series’ from the Department of Defense (DoD).

The ‘Green Book’ in the series dealt with password controls – this is where the commercial debate began in earnest. We at SKK, Inc. broke rank with our DoD counterparts and officially told our customers that the ‘Green Book’ controls were more dangerous than helpful for security.

For instance, implementers were told to store the last ten passwords of an account to determine if password reuse was occurring. At the time, we believed that sticky-note sales would skyrocket with such guidance – little did we know just how accurate that prediction was. Against our customers’ desires, we refused to budge on this issue and instead decided to act.

We opened our development doors inviting strong-authentication vendors to solve the problem. We introduced a new feature to ACF2/MVS 3.1.5 called Extended User Authentication Exit Facility, a.k.a. EUA Exit. The more notable companies we saw participate were Gordian Systems Inc., Enigma Logic and Security Dynamics. Today, these companies collectively represent the innovators behind many of the core one-time password (OTP) technologies you will read about in this book.

I personally tried my hand with a biometric startup in 1987 called ThumbScan. Our dream could not get out of the lab so we pivoted to 'plan B' and bought the failing Gordian OTP product and patents. ThumbScan/Gordian unfortunately failed as well, but years later I tried again under the Value Added Systems Company (VASCO) flag and finally got it right.

Ken Hunt, the CEO of VASCO, believed that security patents might be 'important someday', and I was still convinced the dreaded password was a scourge to computing. We set off in 1994 to change the world and this time we accomplished our goal by protecting banks across the globe – except for the US. We scratched our heads on that one for years.

Even as products were refined over the years, the industry barely noticed. Sure, some of us were successful but in the grand scheme of things the problems far outpaced solutions – things got worse, not better. Considering that, why *are* passwords so damning still today?

Foremost, the problem isn't the idea of a password but rather that most passwords are created and managed by

humans. A computer can generate and store a great password but humans will often create passwords that can be committed to memory. This leads to poor password selection and a high amount of reuse across systems.

Second, the number of accounts being created and maintained has exacerbated the aforementioned problems. We're at a point where a social network for knitting could have its passwords stolen and criminals will drain bank accounts around the US.

Lastly, we have all underestimated pain thresholds – just how bad does it have to get? Our craziest fear-mongering marketers at VASCO couldn't have written the headlines we see today. This last point, I'm afraid to say, is still with us, but a divide is happening where competitive advantages will separate winners and losers along trust lines.

The FIDO (Fast IDentity Online) Alliance – a not-for-profit consortium focused on open standards and interoperability around authentication security – has done a fantastic job in bringing many stakeholders to the table with the stated objective of killing passwords. Does anyone believe passwords will actually be 'killed'? Of course they don't. Can we bring far better solutions collectively to the industry than any one company? Absolutely.

The industry call to action is that application owners become activists. While no one entity can solve this, a class of entities can. It takes an activist, however, to start the ball rolling and two notable FIDO participants are PayPal and Google. When application owners realise that millions of existing end-user devices can be trusted, at no

additional cost to either party, things will finally change in this industry.

This is the way forward, and when coupled with advancements in contextual authentication and better open standards, the future looks quite bright. Not just for a single country or industry but for authentication security as a whole.

While I am not surprised, I am sincerely sad, that so many of our predictions from previous decades came true. It tells me that we, the security industry, failed to accomplish what we were tasked to do – protect users.

The good news is that many of us have never given up. We are a persistent bunch and we've welcomed new minds to the fight. I have never been as confident as I am today that everyday technology users will soon have great authentication security choices to protect themselves at scale.

It's been a long, hard-fought battle, but I hope that we're on the cusp of finally taking power away from the bad guys and putting it back in the hands of the end user.

John Haggard
Chief Business Officer, Yubico

PREFACE

Two-factor authentication is an ever-increasing necessity in information technology as the threats facing end-user security become more intense and powerful. As criminals continue to improve their techniques to steal user credentials and otherwise circumvent traditional, single-factor authentication security mechanisms, there's a pressing need for individuals and organisations to understand their options better when it comes to authentication.

It is my experience that much of the thinking regarding two-factor authentication is actually based on decades-old knowledge about how, why and when people should deploy such authentication security. Further, any matter already written about this topic is limited to a few pages of a book on overall information security and not a standalone effort to summarise this topic in a sufficient manner.

This book intends to provide an introduction to the topic of two-factor authentication for those technologists who have yet to be deeply engaged with this important subject matter. Still, even those with previous two-factor authentication experience may not be fully aware of the technologies available, or trends in progress, around the broad subject of authentication security.

The following subject matter will be covered:

- Chapter 1 aims to provide readers with important foundational knowledge to frame the subjects discussed in this book.
- Chapter 2 will address why two-factor authentication is so critical to IT and the concerning reality of password-only security.
- Chapter 3 provides readers with key two-factor authentication basics that are core to many of the discussed technologies throughout this book.
- Chapter 4 covers six key groupings of two-factor authentication technologies with a focus on their strengths, weaknesses and important nuances.
- Chapter 5 conveys international examples of standards and regulations that make two-factor authentication a component of security guidance.
- Chapter 6 details how everyday end-users are interacting with two-factor authentication and provides insight into the drivers behind their use.
- Chapter 7 suggests how two-factor authentication will continue to evolve and where we'll see increased adoption in the future.

My hope is that you, the reader, will gain a sense of understanding of the means with which you can not only protect your own accounts and technologies, but also help influence the decisions of the organisations you work with and for.

ABOUT THE AUTHOR

Mark Stanislav is an information technology professional with over a decade of varied experience in systems administration, web application development and information security. Mark is currently a Senior Security Consultant for the Strategic Services team at Rapid7.

Mark has spoken internationally at nearly 100 events including RSA, DEF CON, SecTor, SOURCE Boston, ShmooCon, and THOTCON. News outlets such as the *Wall Street Journal*, *Al Jazeera America*, *Fox Business*, *MarketWatch*, *CNN Money*, *Yahoo Finance*, *Marketplace* and *The Register* have featured Mark's research, initiatives and insights on information security.

Mark earned both his Bachelor of Science degree in networking & IT administration and his Master of Science degree in technology studies, focused on information assurance, from Eastern Michigan University. He also holds CISSP, Security+, Linux+, and CCSK certifications.

CONTENTS

CHAPTER 1: INTRODUCTION

Everything old is new again

Existing information-security technologies and processes often resemble historical methods to provide confidentiality, integrity and availability.

In the Middle Ages, the use of castle walls, gates, and drawbridges allowed for certain people to come or go only as desired by those in charge. Today, a firewall ensures that data can only enter or leave specific network ports as defined by configured filtering-rule sets. Similarly, Julius Caesar utilised primitive cryptography thousands of years ago to transmit instructions and guidance to his Roman army. While cryptography still has its place among military engagements, it also helps us protect everything from our private photos to credit card numbers for online shopping.

Authentication is no different, with a rich history of methods proving that you are who you say you are before certain privilege or authorisation is granted.

If you've ever seen a signet ring, you may have been intrigued that it could provide a means to ensure that a document was sealed by a certain party whose ring symbol you knew of. What if you received a letter from a person that was sealed with a signet ring and then met them in person? Would presenting their ring as proof of identity satisfy you? What if the letter they had sealed included information about a scar on their face and a code word they'd say to you upon first meeting?

Within authentication security, the method to prove identity breaks down into three 'factor classes', each with their own pros and cons. The previous example involving the signet ring and letter actually encompasses all three of the factor classes rather succinctly.

1 **The signet ring** represents 'what you have'.
2 **The facial scar** represents 'what you are'.
3 **The code word** represents 'what you know'.

Today, authentication factor classes are better represented by a slightly more tech-forward list:

1 **A smartphone** represents 'what you have'.
2 **A fingerprint** represents 'what you are'.
3 **A password** represents 'what you know'.

The capabilities afforded to us by modern technology provide a wealth of means to handle our existing factor classes in new ways. As you'll read, this opens up exciting possibilities for authentication security as we've known it for decades.

You've been using two-factor for years

For the majority of people worldwide, passwords and personal identification numbers (PINs) are how users authenticate themselves to systems and services in their daily lives. These values are representative of the 'what you know' factor class. Much like a predetermined code word, a password is really an agreement between a system and a user that, each time they 'meet', the password will validate that the user coming back to the system is who they claim to be.

However, if you've used an ATM or bought something with a debit card, you've actually engaged in using two-factor authentication. By possessing the debit card (what you have) and typing a PIN (what you know), you've utilised two factor classes for one authentication process.

Mixing factor classes leads to better security because it's unlikely that a criminal could compromise both authentication mechanisms. Imagine if someone stole your wallet at a bar one night. They may now have your debit card (something you had), but without the PIN (something you know) they are unable to withdraw funds. If, one day, someone saw your PIN over your shoulder as you entered it into an ATM, they may know that value but still not have the card they need to present to the machine.

Since the ATM security we know today was patented back in the 1960s, it would seem reckless if the banking industry took away one of those factors of authentication to access your financial accounts. Amazingly, though, the majority of people who have used online banking for decades still wield only a password as their means to achieve the same goal.

Many of the technologies we use today (like online banking), have grown organically as capabilities to provide advanced functions to customers have become more realistic. Indeed, 15 years ago there were few cheap, reliable, easy-to-use and efficient means for two-factor authentication to be added to everyone's online banking experiences. As a result, we're now seeing financial institutions play catch-up in the digital world to gain parity with their physical banking counterparts.

Authentication security's naming problem

One of the biggest issues with authentication security is the inability of the industry to name the technology clearly and concisely. Further, even well informed technologists and companies quite often use authentication security terms incorrectly, leading to unnecessary confusion. This point is well noted by the usage of so-called 'security images'.

Security images are really a staple of the online financial industry's attempt to provide additional protection to customer accounts without frustrating their users. Typically, a customer will select an image from a list of perhaps twenty that will be shown to them upon logging into their account. The usage of that image, however, is often conflated with the wrong type of security focus.

A security image can actually provide a benefit to customers by appearing when they are prompted to type their username and password into a site. If a user doesn't see their specific image shown, they can be implicitly warned that a criminal may be attempting to steal their credentials through the usage of a fraudulent website. Unfortunately, this security benefit is often used incorrectly by treating it as a 'second factor', which it most certainly is not.

Remember, two-factor authentication requires two different factor classes to be used for one authentication transaction. A password is something the banking customer knows – and so is the security image. As a phishing-mitigation technique, security images may suffice, but do not accomplish the goals of two-factor authentication. While two steps from the same factor class

isn't necessarily bad, it's not as secure as using two factor classes.

This leads us into the other aspect of naming that goes sideways for people: 'I thought two-factor authentication was called [insert phrase or acronym] instead!' Here's a quick breakdown:

- **Two-factor authentication:** use of two factor classes to provide authentication. This is also represented as '2FA' and 'TFA'.
- **Multi-factor authentication:** use of two or more factor classes to provide authentication. This is also represented as 'MFA'.
- **Two-step verification:** use of two independent steps for authentication that might not involve two separate factor classes. This is also represented as '2SV'.
- **Strong authentication:** authentication beyond simply a password. May be represented by the usage of 'security questions', or could be layered security like two-factor authentication.

Factor classes, when used together, are often referred to as primary and secondary methods of authentication. This book will typically discuss the secondary form of authentication used and implies that a password or PIN is the primary method. While certain facilities, government agencies or even corporations may not use a 'what-you-know' factor in their authentication process, most readers will likely do just that for the foreseeable future.

Looking down a road to greater adoption

I would suspect that many readers of this book have been using computing technologies for perhaps decades and likely had little to no interaction with two-factor authentication up to this point. The reason for this could vary wildly, but one reason is that unless your employers made you use it, few people would ever think that they could or should use such a level of authentication security for their day-to-day activities. Part of this reasoning goes to the fact that, until rather recently, the cost and complexity of deploying and using methods in this technology space were very prohibitive for most people's lives.

Technologies best known to existing users of two-factor authentication will likely be hardware-based. That's to say, their second factor would be 'what you have', such as a hardware token that would generate a one-time password (OTP) value. These devices typically range between US$25 and US$100, and for a business that you were a customer of, it's unlikely they would just give them out to everyone (for free, anyway). Further, even if your financial institution or stock-trading company offered you one, you may have been annoyed at the prospect of having to carry a device on your keyring or in your wallet to log in online.

These two points (cost and end-user frustration) have unfortunately been traits of authentication security for decades. This isn't to say that successful authentication vendors were doing anything wrong, simply that technology was not yet at the level necessary to reduce the costs and complexity associated with making security

applicable for most users' needs. Could you imagine the effort and cost of supplying the millions of customers of a multinational bank with hardware tokens? Taking on the overheads of purchasing, shipping, managing and supporting such an effort would be extremely unwise.

The road to adoption, while slow overall, has sped up within just the past decade due to technologies such as Cloud computing and smartphones, relieving much of the cost and complexity of widely deploying and managing a proper two-factor authentication solution. The addition of open standards for OTP generation has allowed vendors to build hardware that works on any number of platforms, helping to reduce cost and create more incentive for organisations to make the investment to buy devices they can use with a number of vendors.

As you learn more about the technologies, standards, risks and use cases of two-factor authentication throughout this book, be mindful to figure out what will work best for *your* needs. There are a wide variety of vendors, methods and implementation styles available to complement the specific goals that you or your organisation have.

<<< END OF EXTRACT >>>

Two-Factor Authentication

- An introduction to the topic of two-factor authentication.
- Provides a comprehensive evaluation of popular secondary authentication methods.
- Presents international examples of standards and regulations that make two-factor authentication a component of security guidance.

Buy your copy today

www.itgovernance.co.uk/shop/p-1693-two-factor-authentication.aspx

www.itgovernanceusa.com/shop/p-1470-two-factor-authentication.aspx

www.itgovernance.eu/p-1120-two-factor-authentication.aspx