1

Introduction

Stop! Right now, think of how many passwords and personal identification number (PIN) codes you have to remember. Now, think back to when you started using passwords and PIN codes. How many did you use then compared to now? For most of us, the number of passwords and PIN codes we currently have is somewhere between 5 and 8. For some, that number can be as high as 12 to 15. How often do you forget them? It is very inconvenient to remember those codes. Now, do you have your fingers, eyes, voice, and face with you? The answer hopefully is yes! Have you ever forgotten any of those body parts? Not very likely! What if we could use those body parts instead of passwords and PIN codes to verify who you are? Would that not be more convenient? It also seems logical that it could be a more secure way of authenticating a person.

Biometric technology uses a physical or psychological trait for identification and/or authentication. By using physical traits, the provider of the trait always has them with him or her.

This book is about using those physical traits for providing access to computers and their networks. *Biometrics for Network Security* is a book dedicated to helping those interested in the use and implementation of biometrics systems for access control to be successful the first time.

This book is based on my own real-world experiences. The methodologies, observations, and suggestions are based on several years of real-world, in-the-field experience. Everything I talk about in this book really happened to me. I did not get the information from a presenta-

tion or hear a story secondhand from a friend; I have been in the trenches and have the scars to prove it!

What Makes This Book Different?

As outlined above, it is my real-world experience in delivering biometrics for network security that will differentiate this book from others. You will not find in here the same tired examples used in other books–examples that have been rehashed endlessly as case studies to be learned from. I want to teach you and prepare you for taking on a biometrics project–not only to evaluate the technology and understand it, but to actually get it deployed and thus deliver on the promise that biometrics can deliver.

The Structure of This Book

The book has four sections:

Section 1–Introduction and Background

While this section title is seen in many other books, this book tries to provide a different view. The first chapter in this section is about authentication technologies. If you are to use and deploy biometrics, you need to understand where they fit in relative to other types of authentication, and also where one authentication method may be better than another for a given use. Chapter 3 describes privacy issues. While other books tackle privacy, it is normally from the user's perspective. In this chapter, I contrast and balance the needs of privacy for the employer, employee, and customer with biometrics as both an enabler and a compromiser of privacy.

Section 2–Biometric Technologies

This section deals with different types of biometrics and biometric devices. The devices described in these chapters were selected by me to reflect, at the time, what I believed to be the best suited for network security. Each chapter in this section has the same format so that it is easy to compare one biometric device's features versus another's. Before any discussion on technologies takes place, it is important to define what makes a good biometric for network security and which

features of a biometric are most important to evaluate for network security. The final two chapters of this section discuss the mathematics of biometrics and how a complete biometric system can be secured.

Section 3–Implementing Biometrics for Network Security

This section is what truly sets this book apart. In three chapters, the reader is led through the proof of concept, the pilot, and lastly, the rollout. In the chapters of this section, the stories of Martin and Jason will be told. Martin and Jason personify the right and wrong ways to deploy biometric technology. Martin is the culmination of my experience when the outlined steps are followed and the biometric project is delivered. Jason is the culmination of my experience when the different stages of the methodology are skipped or not taken seriously. It is these chapters that will make or break the success of a project.

Section 4–Future and Conclusions

With the serious aim of the book out of the way, it is fun to try to predict what the future holds in store for biometrics. I have seen some of this technology myself, and can say without any doubt, it carries a high "cool factor."

Everything You Need to Know about Biometrics to Understand the First Three Chapters

Biometrics, like any other technology, have their own nomenclature and acronyms. While these are covered in great detail throughout the book, below is a primer on basic biometric technology and terminology to get you started. What is covered here will be just enough to get you going.

What Is a Biometric?

As mentioned earlier, a *biometric* is a physical or psychological trait that can be measured, recorded, and quantified. By doing this, we can use that trait to obtain a biometric enrollment. This way, we can say with a degree of certainty that someone is the same person in future biometric authentications based on their previous enrollment authentications. The degree of certainty will be discussed in greater detail in Section 2.

Enrollment, Template, Algorithm, and Verification

In a biometric system, a physical trait needs to be recorded. The recording is referred to as an *enrollment*. This enrollment is based on the creation of a template. A *template* is the digital representation of a physical trait. The template is normally a long string of alphanumeric characters that describe, based on a biometric algorithm, characteristics or features of the physical trait. The *biometric algorithm* can be viewed as the recipe for turning raw ingredients–like a physical trait–into a digital representation in the form of a template. The algorithm will also allow the matching of an enrolled template with a new template just created for verifying an identity, called a *live template*. When a stored template and a live template are compared, the system calculates how closely they match. If the match is close enough, a person will be *verified*. If the match is not close enough, a person will not be verified.

FAR, FRR, and FTE

As described above, when a stored and live template are compared, they either match or they do not match. What happens if it is not you who is trying to match to your template? In this case, someone else is trying to verify as you. If that person were to match as you, it would be classified as a *false acceptance*. The probability of this happening is referred to as the *false acceptance rate*, or *FAR*. The FAR normally states, either in a percentage or a fraction, the probability of someone else matching as you. Thus, the lower the probability, the less likely a match. That means that a match needs to be closer to the original template. As the closeness of a match increases, what does this mean for you when you try to verify as yourself? It means that your live template must match even closer to the enrolled template. If you fail to match against your own template, then you have been *falsely rejected*. The probability of this happening is referred to as the *false rejection rate*, or *FRR*. Thus, the higher the probability of false rejection, the greater the likelihood you will be rejected.

Lastly, when you are new to a biometric system and need to enroll but cannot, this is called a *failure to enroll*, or *FTE*. The FTE normally states, either in a percentage or a fraction, the possibility of someone failing to enroll in a system. A discussion in a later chapter will cover the relationship among FAR, FRR, and FTE as it relates to choosing a biometric device and algorithm.

Who Should Read This Book?

This book was written for the network manager or network security manager. There are others who could benefit from reading it. Below is a list of chapters that each particular person in a company would benefit from reading:

- Chief executive officer (CEO)–Chapters 2, 3, 4, and lastly, skim Chapters 12, 13, and 14. These chapters will provide a solid understanding of the technology and its applicability to an organization.
- Chief information officer (CIO)–Chapters 2, 3, 4, 10, 11, and lastly, skim Chapters 12, 13, and 14. In reviewing these chapters, you will be best prepared to talk about and articulate the issues concerned with using the technology and the preparation required for successful deployment.
- Project manager–Chapters 2, 12, 13, and 14. By reading these chapters, a project manager can become familiar with biometrics and the special project management tasks required to deliver a successful biometric project.
- Network administrator or security specialist–Chapters 2–10, and skim Chapters 11–14. This way, the technology can be examined in greater detail and the project management chapters can be left for the use of the project manager.

Conclusion

This book was written to provide a guide and roadmap for the successful deployment of biometrics for network security. The book is broken down into sections to keep the related information contained, and to allow the different groups of people reading this book to get the most out of it.