Chapter 26

WHY DIGITAL CERTIFICATES ARE USED

INTRODUCTION

More and more people are looking for solutions to the massive growth in phishing and other consumer fraud on the Net. Digital certificates, already vital for securing web sites and encrypting communications with consumers so they can't be intercepted and read in transmission, will be a major part of the solution. But how will this happen [1]?

Digital certificates that secure web sites (SSL server certificates) contain certain information submitted by the site that bought the certificate from a public Certification Authority (CA). Some have suggested greater display and reliance on this information to help consumers detect fraud. Can this work, or will it instead give rise to new phishing opportunities and even greater incidents of consumer fraud [1]?

This chapter takes a look at digital certificates (past, present and future) and their potential for deterring phishing attacks and online fraud. It demonstrates the severe pitfalls from First Generation manual vetting of certificate holders and the inherent unreliability of the identity information they contain (which can easily be faked). These certificates could create serious legal liability for the writers of browser software and for CAs if the identity information they contain is presented to end users as reliable data. Finally, this chapter lays out a path for the future, with a description of higher assurance Second Generation automated vetting of Web identities, and discusses ongoing enhancements that will provide a better solution for online identity authentication and reduction of consumer fraud [1].

UNDERSTANDING FIRST GENERATION DIGITAL CERTIFICATES

The technology surrounding SSL server certificates and Public Key Infrastructures has been well known since the 1970s, and will not be covered here. What's important for this chapter are the two main things that digital certificates can do to secure web sites and

help avoid consumer fraud: They encrypt communications between the web site owner and consumer, and they provide certain identity data about the web site owner [1].

As Internet use expanded during the 1990s from universities and the defense industry (a closed community) to online commerce and broad consumer use, the encryption function has worked brilliantly, but the identity function has not. Consumers have learned to trust the padlock symbol for sites protected by an SSL server certificate as meaning they can safely transmit their personal and financial data to complete a transaction. For the majority of consumers, they have never clicked on the lock to look "inside" the certificate at the limited identity data stored there by the issuer. A number of browser software makers are considering extracting that identity data and displaying it in the browser toolbar, but that is a flawed approach considering the inherent unreliability of that data [1].

So, where did the rules around digital certificates come from? Who made the rules?

The development of digital certificate and PKI protocols over the past 28 years was focused primarily on technical syntax and overall system structure and design, and paid only scant attention to the specific authentication steps to be followed by CAs prior to certificate issuance. The limited discussion of authentication processes during this period:

1. Was written mostly by technical PKI experts, and not by commercial users of PKI or by CAs themselves
2. Recognized that different authentication steps will be appropriate for different uses and communities (closed communities of enterprises who knew each other versus open worldwide communities)
3. Was very vague in nature, reflecting the limited expertise of the authors in business and commercial practices [1].

Early industry documents establishing digital certificate and PKI protocols skipped over specific authentication steps to be used prior to issuance of digital certificates, or made only general reference to some sort of authentication process.

> **Note:** See the early standards stated at the IETF's RFC 791 (1981), RFC 822 (1982), and RFC 1422 (1993). The standards for authentication were very weak and delegated. For example, RFC 1422 provides in part: 3.4.1.2 User Registration: Most details of user registration are a local matter, subject to policies established by the user's CA and the PCA (Policy Certification Authority) under which that CA has been certified. The CA will employ some means, specified by the CA in accordance with the policy of its PCA, to validate the user's claimed identity and to ensure that the public component provided is associated with the user whose distinguished name is to be bound into the certificate.

The technical experts who set up digital certificates and PKI as are known today worked only on the technical aspects and architecture; they "punted" on ultimate identity issues, leaving it to closed communities and public CAs to decide what authentication steps they would take before issuing a certificate to an enterprise or individual. They probably thought this was the easiest part of the online identity equation; in fact, it's the hardest [1].

> **Note:** RFC 2459, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" (1999), which set X.509 v3 standards for certificates in use today, likewise did not prescribe particular authentication standards: Requirements and assumptions: A certificate user should review the certificate policy generated by the certification authority (CA) before relying on the authentication