The Use of the Simple Certificate Enrollment Protocol (SCEP) and Untrusted Devices

Essay

Authors – Ted Shorter, CTO, Certified Security Solutions, Inc.
Wayne Harris, PKI Practice Lead, Certified Security Solutions, Inc.

About Certified Security Solutions, Inc. (CSS)

CSS is an information security company with operations throughout North America, and is headquartered in Independence, OH.

For more information and for a complete list of branch offices, please visit www.css-security.com.

Authors:

Ted Shorter, CTO, CSS

Wayne Harris, PKI Practice Lead, CSS

Abstract

In this essay, we describe what may be a serious IT security issue for many organizations that use the Simple Certificate Enrollment Protocol (SCEP). Organizations that leverage SCEP to provide certificates for mobile devices such as tablets or mobile phones may be exposed to a Privilege Escalation attack, which would allow the issuance of certificates representing a user or device of the attacker's choice. The problem can exist even when the SCEP server is protected by a proxy or firewall, and even if the SCEP server has been configured to enforce dynamic SCEP challenge passwords. The issue is not caused by a vulnerability in a single product, but rather by a combination of features, configurations, and new use cases that, together, open up an unforeseen avenue of attack.

Background

A detailed description of the vulnerability will require some background information on the various components involved.

About the Simple Certificate Enrollment Protocol

The Simple Certificate Enrollment Protocol, or SCEP, was developed by VeriSign, Inc. for Cisco Systems, Inc., primarily to allow network administrators to easily enroll network devices for certificates in a scalable manner.

Because these network devices are unlikely to have their identities represented in an enterprise directory or credential store, SCEP includes no provision for authenticating the identity of the requester. Instead, SCEP allows for two different authorization mechanisms for the initial enrollment:

- ***Manual***, where the requester is required to wait after submission for the CA operator or certificate officer to approve the request
- ***Pre-shared secret***, where the SCEP server creates a "challenge password" that must be somehow delivered to the requester and then included with the submission back to the server

The overall security model surrounding SCEP's creation is that of a relatively well-controlled environment. In the situations for which SCEP was initially designed to handle, challenge passwords would be retrieved by a highly trusted CA administrator, and given to a highly trusted network administrator, to generate certificates for highly trusted network devices. In fact, in many organizations, it is likely that these two tasks were performed by the same trusted administrator. This assumed security context of the tightly controlled environment made up of only highly trusted users and devices no longer aligns with the use cases for which SCEP is now being pressed into service. This shift in security models is important, and will be mentioned again later.

SCEP and the Microsoft CA

Microsoft has supported SCEP for its Certification Authority software since Windows Server 2003 – first as a freely downloadable add-on component, and later with Windows Server 2008 as a native component (via the "Network Device Enrollment Service" role, or "NDES" feature of Active Directory Certificate Services). Microsoft's SCEP implementation is relatively full-featured, and allows for a variety of configuration options, including:

- Setting the length of the SCEP challenge passwords
- Turning the requirement of SCEP challenges on or off
- Allowing or disallowing the re-use of SCEP challenges
- Maximum time that an unused SCEP challenge should be considered valid

It is important to mention that many, perhaps even most, default installations of Microsoft Certification Authorities are set such that the CA can issue Domain credentials. This is because Enterprise CAs are automatically included in the Active Directory Enterprise "NTAuth" store, which allows Domain Controllers to map AD identities based on the content of authentication certificates.

iOS Support for SCEP

Starting with iOS 4, iPhones, iPads, and iPod Touch devices have included support for SCEP. When a configuration profile is delivered to an iOS device that includes SCEP configuration parameters, the device generates its own RSA private key, and then uses that key to construct a PKCS#10-formatted certificate request, which is then in turn delivered to the SCEP server.

The actual certificate content that the iOS device requests, as well as the SCEP challenge password, is determined by the configuration information that gets delivered to the device. Because the rest of the information in the configuration profile tends to be more of a "one-size-fits-all" variety, it can become tempting to re-use the same SCEP settings for multiple devices. This practice has led some implementers to require that the SCEP server be configured to allow the re-use of challenge passwords, or even worse, no passwords at all. The mishandling of SCEP authorization information in this manner is a serious security risk in and of itself; however, even dynamically created SCEP challenge passwords do not solve the problem that is the primary focus of this essay.

When Apple added SCEP to iOS, it increased the global count of SCEP-speaking client devices by several orders of magnitude. Additionally, it moved SCEP away from the security-friendly environment in which the protocol was initially used. Instead of issuing certificates to tightly controlled network devices under the direction of highly trusted administrators, many SCEP deployments are now being architected to allow enrollment of "less-trusted" devices and their users, often over the Internet.

Mobile Device Management (MDM) Systems and SCEP

Mobile Device Management systems that support iOS can make use of SCEP-based certificate enrollment in two different ways. Each of these will be discussed in its own section.

Initial Device Enrollment for iOS

Nearly every MDM system implements this capability in accordance with Apple's published vendor guidance for creating an over-the-air configuration profile enrollment product. In this case, the resulting certificate is used to authenticate the device to the MDM system, and also to encrypt the configuration profiles delivered to the device.

Some MDM implementations leverage Microsoft's implementation of SCEP (*aka* "NDES") for this initial certificate. Others ship with an embedded SCEP server and Certification Authority, or make use of a third-party SCEP server.

Enterprise Authentication Certificate Enrollment

Not every MDM supports the issuance of user authentication certificates through SCEP, but many do. Because iOS natively supports certificate authentication for 802.1X, VPN, and ActiveSync, and because SCEP-issued certificates through iOS have their private keys generated on the device, this is an attractive feature for many organizations that already leverage an in-house PKI for authentication or other purposes.

Most MDM products that support this feature allow issuance of these certificates from a corporate Microsoft PKI via SCEP, even if the initial device authentication certificates are created from another source.

The Problem

A critical aspect of the SCEP challenge password is that, while it provides *authorization* to submit a PKCS#10-formatted certificate request, it does not actually *authenticate* the requester, nor does it even *identify* the requester. Furthermore, neither the SCEP challenge nor the SCEP server makes any substantial statement about the content of the request that may be submitted. In essence, possession of a valid SCEP challenge password entitles the bearer to submit a certificate request with content *entirely of their choosing* to the SCEP server. This is not a serious issue in the original "admin-only" security model for which SCEP was initially created, but is cause for concern when SCEP challenge passwords are delivered to users or devices outside of that trust boundary, as is often the case with MDM systems or "Bring Your Own Device" (BYOD) scenarios.

Because SCEP contains no authentication mechanism, it may be possible for a user or device to take a legitimately acquired SCEP challenge password, and use it to obtain a certificate that represents a *different user or device* (e.g., one with a higher level of network access), or to obtain a *different type of certificate* than what was intended. If challenge passwords are re-used or disabled, the consequences are severe, as the attacker would not need to be a legitimate user.

It is important to note that the exploitation of this issue does not necessarily require the use of an Apple device. It only requires:

- a valid SCEP challenge password, **and**
- the ability to communicate with the SCEP server.

Both the SCEP challenge password, and the URL of the SCEP server, are a part of the communication between the device and the MDM system, and could be obtained with software masquerading as a user's device, or by sniffing a legitimate connection with a man-in-the-middle proxy.

Given the above two conditions, even internally deployed SCEP servers, or servers protected by a proxy or firewall, can also be susceptible.

The Impact

The security impact of this issue varies on several factors, including:

- The nature and potential content of the fraudulent certificates that can be issued (cert subject, subject alternate name, extended key usage, etc.)
- The set of systems that trust the potentially fraudulent certificates

In organizations that are leveraging SCEP-issued certificates for authentication to enterprise infrastructure such as wireless networks, VPN, or ActiveSync, a fraudulent certificate could allow an attacker to authenticate as a different user – thus allowing them access to email, trusted networks, or a mutually authenticated SSL website with someone else's identity.

For MDM implementations that leverage SCEP only for enrolled device authentication, the impact can still be similar to the above, *if* the SCEP server being used is *also* a part of an organizational PKI. And even in cases when SCEP is handled internally by the MDM system, the possibility may still exist for a user to obtain a certificate that represents another user's device. For cloud-based MDM systems that leverage the same PKI to issue certificates to devices belonging to multiple customers, one potential concern would be for a user of one company to receive a certificate that identifies a device that belongs to another company.

Remediation

This issue is not the singular "fault" of Apple, Cisco, Microsoft, or even of the Mobile Device Management systems that leverage SCEP. Rather, it is brought about by a combination of several factors:

- That SCEP challenge passwords give someone *permission* to submit a certificate request to the SCEP server, but make no claims or enforcement over the *content* of that submission.
- That iOS devices' support of SCEP has opened up avenues for SCEP requests to originate from untrusted networks, and from less trusted (non-administrative) users, and in turn, many MDM systems operate under this expectation.
- That many enterprise Certification Authority installations, including most default installations of Microsoft's Certification Authority, are being used to issue certificates that serve as network authentication credentials.

Our guidance respect to the use of SCEP in conjunction with untrusted devices is as follows:

- Avoid the use of systems that require the re-use or disablement of SCEP challenge passwords.
- Avoid the use of systems that require delivering SCEP challenge passwords to untrusted machines or individuals. Firewalls or proxies may not be enough: the key is to ensure that no one can request a fraudulent certificate using a legitimate challenge password.
- iOS supports in-person, tethered registration through the use of the iPhone Configuration Utility (iPCU). In-person registration schemes allow personal vetting of the user's identity and the accuracy of their enrolled certificate content. However, iPCU requires manual entry of the SCEP enrollment parameters such as the certificate subject, subject alternative name, and SCEP challenge, which must be obtained from the SCEP server at the time of enrollment. In large-scale deployments, this approach is very labor-intensive.
- Starting with iOS 5.1, there is support for a SCEP return status of "PENDING", which allows a SCEP implementation to require the use of a Certificate Officer role, where requests could be inspected and approved later. The Certificate Officer role is responsible for assessing the validity of the request. In many circumstances, however, the Certificate Officer may not have enough information within the request itself to be capable of determining if the request is legitimate.
- If you must use a system that delivers SCEP challenge passwords to untrusted machines or users, make sure that the CA or PKI that issues the corresponding certificates is not trusted by the rest of the organization. If some trust is required, ensure that the level of trust given to these certificates, and the number of systems that trust them, is minimal. For example, the Issuing CA's certificate should be removed from the Microsoft "NTAuth" store if possible. This approach does not constitute a solution, however; it simply reduces the level of exposure.

- Certified Security Solutions, Inc. (CSS) has created a “SCEP Validation Service” that allows for the safe use of SCEP in this new model. The service dynamically enforces the pairings of each unique SCEP challenge password against a set of expected certificate content. This approach allows for the “pre-vetting” of SCEP certificate requests, and enables continued use of SCEP enrolled certificates while protecting against the risk of fraudulent certificates. The components of this system include:
  - A Validation Service that receives, from trusted sources (such as MDM systems or other issuance authorities), a series of *n*-tuples that combine a SCEP challenge password with expected certificate request content.
  - A Policy Module for the Microsoft CA that performs real-time vetting of SCEP requests by contacting the Validation Service for verification of the requested content and SCEP challenge to determine whether the request is valid.

For more information regarding the SCEP Privilege Escalation attack, please contact CSS at business@css-security.com or visit our website at www.css-security.com.