System IT Board Report

October 12, 2022

Update on Multi-Factor Authentication

The combination of a userid and password has been the standard means of authenticating access to computer systems since 1961. While passwords worked well for decades, the rise of phishing and similar credential harvesting attacks have rendered passwords insufficient as a means of authentication. Passwords, even strong passwords like CorrectHors3.BatteryStaple, are too easily stolen and re-used.

Multi-Factor Authentication (MFA) is one solution to this problem. MFA requires at least two independent pieces of information to authenticate a user. The most common choices are: something you know (a password), something you have (a phone or other device), or something you are (biometrics like fingerprints or facial recognition.) This combination of factors means that even when a password is stolen, it cannot be used by itself to gain illicit access to a computer system.

Online banking was an early adopter of multi-factor authentication. If you have ever received the message that your device wasn't recognized and the bank wants to send you a text message to verify your identity, you've seen MFA in action. The combination of password and cellphone was required to complete the login. CCCS has implemented Duo, a Cisco Systems product, as our MFA system. Duo works by prompting users to either confirm their login by pressing a button on a smartphone, or by entering a passcode that is sent via text message. Duo is extremely configurable and allows us to apply different security policies to individual applications.

CCCS has spent the past year implementing MFA including over the last few months configuring almost all of our systems to support multi-factor authentication. This includes our enterprise systems such as Banner and implementing DUO with our single sign-on methodologies. This is a key part of our overall cybersecurity strategy and an important part of preparing our application for cybersecurity insurance. As of the time of this writing, CCCS has implemented Duo MFA on 62 of our 71 enterprise applications. We plan to complete the remaining nine applications by the end of calendar year 2022. Over the next week or so, we will finalize our implementation of multi-factor authentication for all ways of accessing email. Email, of course, is a sector for phishing and other email-based cyber attacks.

Multi-factor authentication is a first, foundational step in creating a robust identity security architecture at CCCS. We will continue to evolve our authentication practices as attackers change tactics and technology adapts to meet new challenges.