CU WiFi Position Statement
CU IT Student Governance Board
Fall 2014
06/15/2014

Summary

At our 06/06/14 meeting, we received an overview of current and planned UCB Wireless network infrasture. We believe the current unencrypted UCB Wireless networks are inadequate to properly protect and facilitate secure student WiFi use. We are supportive of the University's plans to migrate to a WPA Enterprise based encrypted WiFi system in the near future. We also believe, however, that students should have the option of using a secondary, public, and open WiFi network suited for the maximization of student anonymity while online. Finally, we would prefer the University avoid mandating the installation of third party software on student-owned machines as a requirement for use of the new WPA Enterprise network.

Background

On 04/10/14, the ITSGB met with Dan Jones, CU OIS Chief Information Security Officer. Dan spoke with the Board regarding CU's plans and policies surrounding the University's WiFi network offerings. Dan covered the existing unencrypted "UCB Wireless" and "UCB Guest" networks currently offered on campus. "UCB Wireless" is an internal, authenticated WiFi network used by students, faculty and staff. It provides largely unrestricted access to both the Internet as well as to various internal CU resources. The "UCB Wireless" network uses a captive portal based authentication system to authenticate and associate a user's MAC address with their IdentiKey credentials. "UCB Guest" is a public WiFi network designed for use by individuals without CU IdentiKey accounts (e.g. campus visitors, etc). It restricts access to public Internet-based resources and only allows traffic on common ports and protocols (e.g HTTP, HTTPS, FTP SSH, etc).

Dan also described the planned rollout of a new WPA Enterprise secured eduroam-affiliated campus WiFi network. This new network will eventually replace the existing "UCB Wireless" network as the primary network used by CU-affiliated individuals. Unlike the current "UCB Wireless" network, the new network provides WPA encrypted WiFi connections and cryptographically secure authentication. In addition, the new network's use of the eduroam system will provide CU-affiliated individuals with WiFi network access when visiting other eduroam-affiliated institutions using their normal CU credentials. Likewise, guests to the CU campus from other eduroam-affiliated institution will be able to use their home credentials to access the new CU WiFi network. In order to ease the setup burden of using a WPA Enterprise encrypted WiFi network, CU will be providing non-Free (e.g. closed source) WPA supplicant software that individuals will be asked to install on their machines.

Position

We believe that providing secure, accessible, and unfettered Internet access to all CU-affiliated personnel should be a top priority of the OIT and the OIS. Thus, we are supportive of the University's efforts to replace the existing insecure “UCB Wireless” network with the new, cryptographically authenticated and encrypted WPA Enterprise based eduroam WiFi network. The MAC-based authentication scheme used by the existing “UCB Wireless” network is trivial to subvert and provides no encryption of WiFi network traffic. If anything, the existing MAC-based authentication method puts users at a greater risk than using no authentication system at all by providing the illusion of security. We urge the university to replace the existing “UCB Wireless” network with the new WPA Enterprise based network as soon as possible.

While we support the move toward a WPA Enterprise based WiFi network, we also believe that University-affiliated Internet users have a right to pseudo-anonymous, open, and untracked Internet access, similar to what they could achieve if they were living off campus and buying residential Internet access from a provider like Comcast. Thus, in parallel with the rollout of the new WPA Enterprise based internal WiFi network, we believe the University should deploy an unauthenticated, open, and public WiFi network for use by individuals who do not wish their Internet usage to be affiliated with their CU IdentiKey. It is possible that the existing “UCB Guest” network could serve this purpose, but we would prefer to see a “guest” network without a click-through landing page (which interferes with devices lacking a browser and poses accessibility concerns) and with support for all standard Internet protocols.

In short, our ideal WiFi network deployment would offer two options to all students:

- An authenticated and encrypted network providing both unrestricted access to the public Internet, as well as restricted access to private internal University resources.
- An unauthenticated and open network providing only unrestricted access to the public Internet. This network should support all standard Internet ports and protocols.

We are also concerned about the use of third party WPA supplicant software to “enhance” the end-user experience on the new WPA Enterprise network. We feel it is inappropriate for the University to mandate the installation of specific software on end-user machines not owned by the University, especially as a prerequisite to the use of services as fundamental as secure Internet and network access. Furthermore, we fear that such software may impose unnecessary accessibility burdens on end users. Thus, while the University is welcome to provide users with the *option* of installing the suggested WPA supplicant software to ease their configuration burden, we do not believe that such software should be required. The university should provide users with alternative configuration options requiring no extra software beyond the normal WPA Enterprise support built into all modern operating systems.

Finally, we would like to thank Dan Jones for taking the time to discuss CU’s current and planned WiFi infrastrue with us. We greatly appreciate his openness, his efforts, and his time.