Software Assurance Tips

A product of the Software Assurance Tips Team[1]

Generated Friday 7th May, 2021

Jon Hood

Monday 10th May, 2021

1 Homoglyphs and Homographic Attacks

Do you have an OS X system and would like to get our totally trustworthy, Apple-certified software on your machine? Then be sure to run the command in Listing 1!

```
sh-3.2# softwareupdate --set-catalog http://osx.com
```

Listing 1: Totally Legit-Looking OSX Update Site

If you were to copy+paste that address in your browser, you'd be taken back to our Software Assurance Tips page. It's not the real OSX.com! Attackers often use *homoglyphs*–characters that look identical to the end user but are actually a different character set. Our eyes may think that "osx.com" and "osx.com" look identical (and pixel-for-pixel, they are identical). However, the first one uses Cyrillic characters, meaning that they are two different addresses!

1.1 Attacks

In the past, attackers used a technique known as "soundsquatting" to reserve homophonous domains to trick unsuspecting users. An attacker would register a homophone (eg: "whether" vs. "weather") and set up a mirrored attack site to gleen credentials from their victims.[2]

Suppose that a system makes sure that only trusted friends can request a "Call for Fire" to an enemy location. What would happen if an enemy were able to send the unfiltered "Call for Fire" where the "a" character has been replaced with the Cyrillic character "а"?

1.2 Conclusion

Maybe you think you're too good and wouldn't have been fooled by the fake OSX address at the beginning of this article. But I bet you were fooled with the fact that nearly every letter "a" has been replaced with the Cyrillic character "а" throughout this article. And you didn't even notice!

References

[1] Jon Hood, ed. *SwATips*. https://www.SwATips.com/.

[2] Nick Nikiforakis et al. “Soundsquatting: Uncovering the use of homophones in domain squatting”. In: *International Conference on Information Security*. Springer. 2014, pp. 291–308.