Usability vs. Security: The Everlasting Trade-Off in the Context of Apple iOS Mobile Hotspots

University of Erlangen, Department of Computer Science, Tech. Rep. CS-2013-02 (author's preprint) June 2013, 10 pp.

Available: https://www1.cs.fau.de/filepool/projects/hotspot/hotspot.pdf

Summary

The paper studies the usability/strength trade-off of machine generated passwords that are designed to be exchanged by humans.

Looks specifically at the method used by iOS to generate default passwords when using the device as a mobile WiFi hotspot.

WPA2 security in the context of mobile hotspots is always based on a password, which is used to generate a pre-shared key (PSK). Capturing the PSK during the initial handshake allows an attacker to then perform brute-force or targeted dictionary attacks upon it **Offline**.

Summary cont.

The authors analysed the method used by the iOS system to create default passwords in order to see if they could reduce the set of possible passwords.

Passwords generated are a 4-6 character English word followed by a 4 digit random number, the authors traced the words to a wordlist of 52,500 entries and were able to bruteforce a correct password in 49mins with 525mil permutations.

Hoping to reduce the attack time further, they found that the iOS system uses a function suggestWordInLanguage(), which is normally used to predict user input while typing, to select an English word from 1842 appropriate words. Furthermore the process is not random with some words having high frequencies of use.

Summary cont.

Now the attack space has been reduced to 18.5mil permutations, with a skewed frequency distribution.

#	Word	RF	#	Word	RF
1	suave	0.80%	6	coal	0.41%
2	subbed	0.76%	7	ohms	0.40%
3	headed	0.61%	8	coach	0.40%
4	head	0.53%	9	reach	0.38%
5	header	0.50%	10	macaws	0.29%

Now the attack space has been reduced to 18.5mil permutations, with a skewed frequency distribution. Using a GPU cluster the authors were able to find the password in **less than 50 seconds.**

What can we learn (the Good)

The paper shows that the same limitations that apply to user generated passwords can also apply to machine generated passwords.

Just like a user choosing passwords based on things relative to them (name of a pet) iOS creates passwords that follow a predictable format. But in this case the danger is higher because the weakness exists in **every** default password and the users are likely to expect that machine generated passwords are very strong and trust the defaults.

In this case the attempt to generate more memorable and readable passwords has affected the security greatly, not just for a single user but for all using the generated passwords.

cont.

Even passwords containing random portions, or appearing to be random can have an underling pattern of generation.

Probably best to change default passwords in case the underling system has flaws, especially if the method used is obscured.

Critisism

In the conclusion for the paper the authors state that the mobile hotspot feature of smart phones increases the attack surface of the device. And at other points recommend minimising it’s use.

However the material covered in the paper only shows a weakness in the password generation of some devices, this is not a problem that is related to any technical detail of the wireless hotspots themselves and is applicable to other scenarios in which default passwords are generated.

Question

Can you think of any other platforms that may include this venerability?