Summary

The Citizen Lab is an academic research group based at the Munk School of Global Affairs & Public Policy at the University of Toronto in Toronto, Canada.

We analyzed Xunfei Input Method on Android as part of our ongoing work analyzing popular mobile and desktop apps for security and privacy issues. We found that Xunfei Input Method for Android includes a vulnerability which allows network eavesdroppers to recover the plaintext of insufficiently encrypted network transmissions, revealing sensitive information including what users have typed.

Platform	**File/Package Name**	**Version analyzed**
Android	iFlyIME_v12.1.10.14983.apk	12.1.10

Table 1: The version of Xunfei Input Method analyzed.

Findings

We found that the payload of each HTTP request sent to `pinyin.voicecloud.cn` is encrypted with the following algorithm. Let *s* be the current time in seconds since the Unix epoch at the time of the request. For each request, an 8-byte encryption key is then derived by first performing the following computation:

$$x = (s \% 0x5F5E100) \wedge 0x1001111$$

The 8-byte key *k* is then derived from *x* as the lowest 8 ASCII-encoded digits of *x*, left-padded with leading zeroes if necessary, in big-endian order. In Python, the above can be summarized by the following expression:

$$k = \text{b'\%08u'} \% ((s \% 0x5F5E100) \wedge 0x1001111)$$

The payload of the request is then padded with PKCS#7 padding and then encrypted with DES using key *k* in ECB mode. The value *s* is transmitted in the HTTP request in the clear as a GET parameter named “time”.

Vulnerability

Since DES is a symmetric encryption algorithm, the same key used to encrypt a message can also be used to decrypt it. Since *k* can be easily derived from *s* and since *s* is transmitted in the

clear in every HTTP request encrypted by *k*, any network eavesdropper can easily decrypt the contents of each HTTP request encrypted in the manner described above.

Notably, we found that users' keystrokes were sent to `pinyin.voicecloud.cn` and encrypted in this manner, seemingly to implement the keyboard's cloud-based recommendation feature. Therefore, a network eavesdropper who is eavesdropping on a user's network traffic can observe what that user is typing by exploiting this vulnerability.

Finally, the DES encryption algorithm is an older encryption algorithm with known weaknesses, and the ECB block cipher mode is a simplistic and problematic cipher mode. The use of each of these technologies is problematic in itself and opens Xunfei Input Method's communications to additional attacks.

Mitigation

In order to address the reported issues, Xunfei Input Method should secure all transmissions using a popular, up-to-date implementation of HTTPS or, more generally, TLS instead of relying on custom-designed cryptography to secure the transmission of sensitive user data.