Paper Details

Author details:

Milijana Surbatovich Email: Phone: Collaborative Innovation Center,	Jassim Aljuraidan Email: Phone: Collaborative Innovation	Lujo Bauer Email: Phone Collaborative Innovation Center,
Anupam Das Email: Phone: Institute for Software Research,	Limin Jia Email: Phone: Collaborative Innovation Center,	

Title: Some Recipes Can Do More Than Spoil Your Appetite: Analyzing the Security and Privacy Risks of IFTTT Recipes

Abstract: End-user programming services such as *if-this-then-that* (IFTTT) allow users to easily create new functionality by connecting arbitrary Internet-of-Things (IoT) devices and online services using simple *if-then* rules (trigger-action pairs), commonly known as recipes. However, such convenience at times comes at the cost of security and privacy risks for end users. For example, a recipe that automatically uploads email attachments to a user's Google Drive folder seems a reasonable way to manage attachments, but this recipe could allow a malicious attachment to be automatically synced to all of the user's connected devices, thus increasing the likelihood of being infected by malware.

To gain an in-depth understanding of the potential security and privacy risks, we build an information-flow model to analyze how often IFTTT recipes involve potential secrecy or integrity violations. This model assigns each trigger or action a *secrecy label* and an *integrity label*. The labels themselves are arranged in a lattice that represents which flows between labels are safe and which are potentially unsafe. We use this model to identify recipes that potentially leak information or allow outsiders control over a user's data or IoT devices. Our analysis finds that around 50% of the 19,323 unique recipes we examined are potentially unsafe, as they contain a secrecy violation, an integrity violation, or both. The most common type of integrity violation allows triggers from untrusted, public services to indirectly control the actions of or on trusted devices. For example, a recipe that automatically changes a user's phone's wallpaper to a top voted photo on a photography sub-reddit effectively gives the participants in that sub-reddit explicit control over the user's wallpaper. The most common type of secrecy violation allows

private information to be leaked to online services, such as a recipe that uploads all phone camera photos to Flickr as public photos.

We next categorize the types of harm these potentially unsafe recipes can impose on users. After manually examining a random selection of potentially unsafe recipes, we find that recipes can not only lead to harms such as personal embarrassment, but can also be exploited by an attacker, e.g., to distribute malware or carry out denial-of-service attacks. While it is possible that users may purposely use some violating recipes -- a recipe that posts Fitbit step counts to Twitter is perhaps intentionally leaking private information -- it is not clear to what extent users are aware of or consciously choose to accept the accompanying risks. We plan to carry out human subjects experiments to study users' perceptions and understanding of security and privacy risks as they create and use IFTTT recipes.

To the best of our knowledge, our work is the first to provide an analytical framework to better reason about the security and privacy risks associated with end-user programming platforms such as IFTTT. Our framework can help users discover and mitigate threats to which they could be unwittingly exposing themselves, and can help analysts and policymakers understand the risks to the population of users using IFTTT and other end-user-programming services.

Publication details: M. Surbatovich, J. Aljuraidan, L. Bauer, A. Das, and L. Jia. Some recipes can do more than spoil your appetite: Analyzing the security and privacy risks of IFTTT recipes. In *Proceedings of the 26th International World Wide Web Conference (WWW)*, pages 1501–1510, 2017 (dl.acm.org/citation.cfm?id=3052709)