Security and Privacy Foundations of Internet-Scale User-Centered Automation

PI: Earlence Fernandes, University of Wisconsin-Madison



Challenge

• Trigger-action platforms (TAPs) enable automation rules between wide variety of services



Scientific Impact

- Understand and measure the two levels of overprivileges caused by the current designs of TAP
 - 1. Access to redundant APIs
 - 2. Access to unnecessary data attributes
- Automatically ensure *data minimization* when executing trigger-action rules
 - w/o sacrificing usability or compatibility
- But they are *overprivileged* to ensure ease of use
 - IFTTT
 Trigger a rule when I upload a new file to Google Drive
 Give me a token that can read files, share files, delete files ...
 IFTTT
 Only when the file's name matches [...]
 Tell me every file and their name, content, modified time ...
- *against* a compromised TAP
- Towards the design of an authorization system with *dynamic access control*



Solution



- Develop a practical data minimization model for trigger-action rules in TAPs
- Apply static and dynamic data-flow analysis to compute minimizer function for rules
- Sandbox execution environment to protect services from maliciously programmed rules

Trigger Service

Trigger-Action Platform

minimized trigger data = m (trigger data) m

minimized trigger data

action data = f(minimized trigger data)

action data

Action Service

Estimated Impact

Prevent all unnecessary leakages of user data to TAPs



----attributes ----sanitized highly-sensitive attributes

Other Impact

- Allow service providers to have fine-grained control of their data
 - Reports indicated that some service providers were unwilling to be integrated into TAPs due to excessive data access
- Help service providers convert their existing APIs to privacy-aware ones that adhere to the principle of data minimization required by GDPR/CPRA

The 5th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting (2022 SaTC PI Meeting) June 1-2, 2022 | Arlington, Virginia