



Experimental Security Analysis of the App Model in Business Collaboration Platforms

Yunang Chen*, Yue Gao*, Nick Ceccio,
Rahul Chatterjee, Kassem Fawaz, Earlence Fernandes⁺

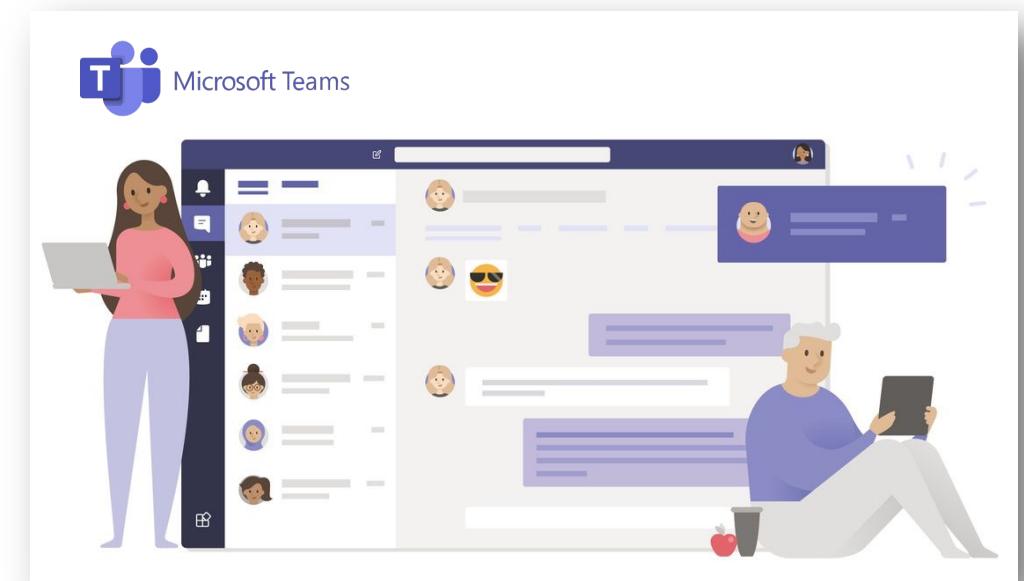
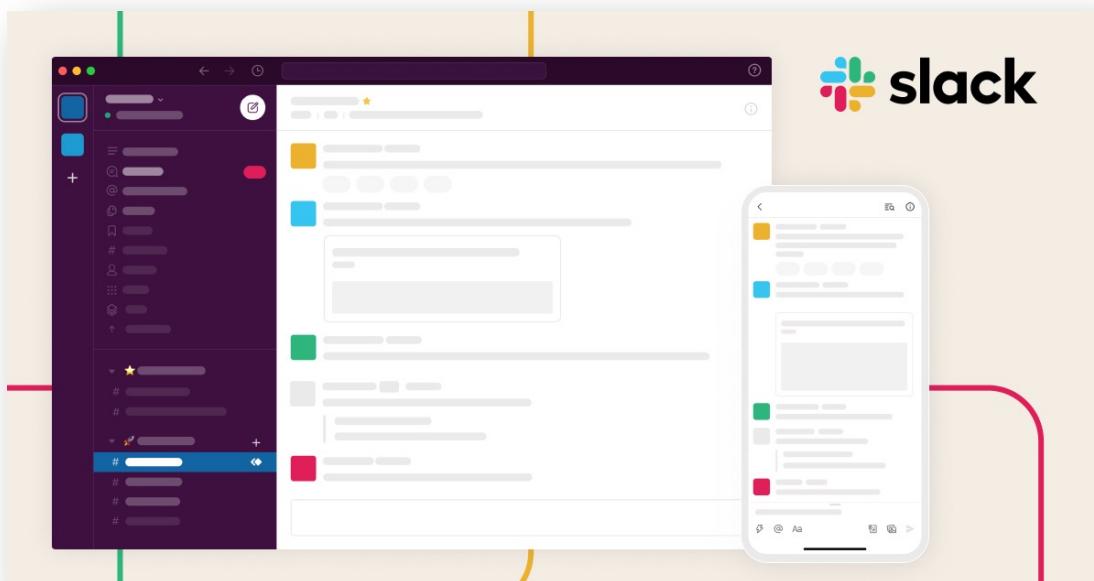
University of Wisconsin–Madison, University of California San Diego

* Equal contribution

⁺ Work done while at UW-Madison

Business Collaboration Platforms (BCPs)

- Productivity & Team Collaboration
- Third-Party Integrations (Apps)



BCPs Have Become A Hub for Sensitive Resources

- Zoom Calls
- DropBox File Sharing
- Email Forwarding
- Code Repository Management
- ...

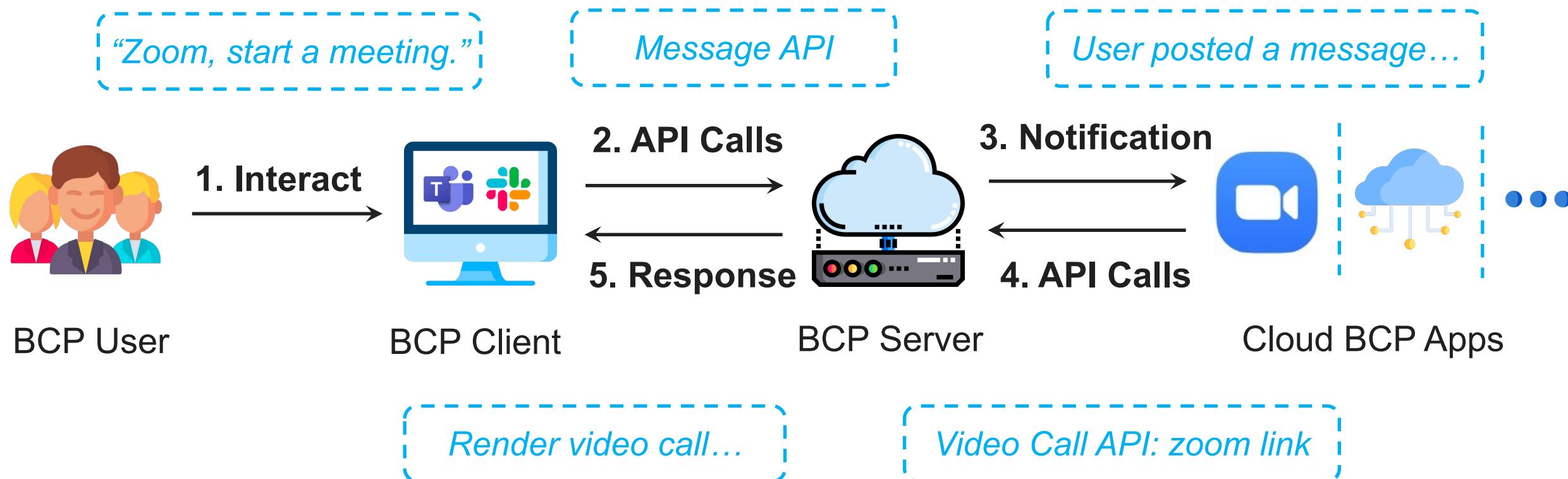
What if the apps are malicious?

Can BCPs enforce security correctly?



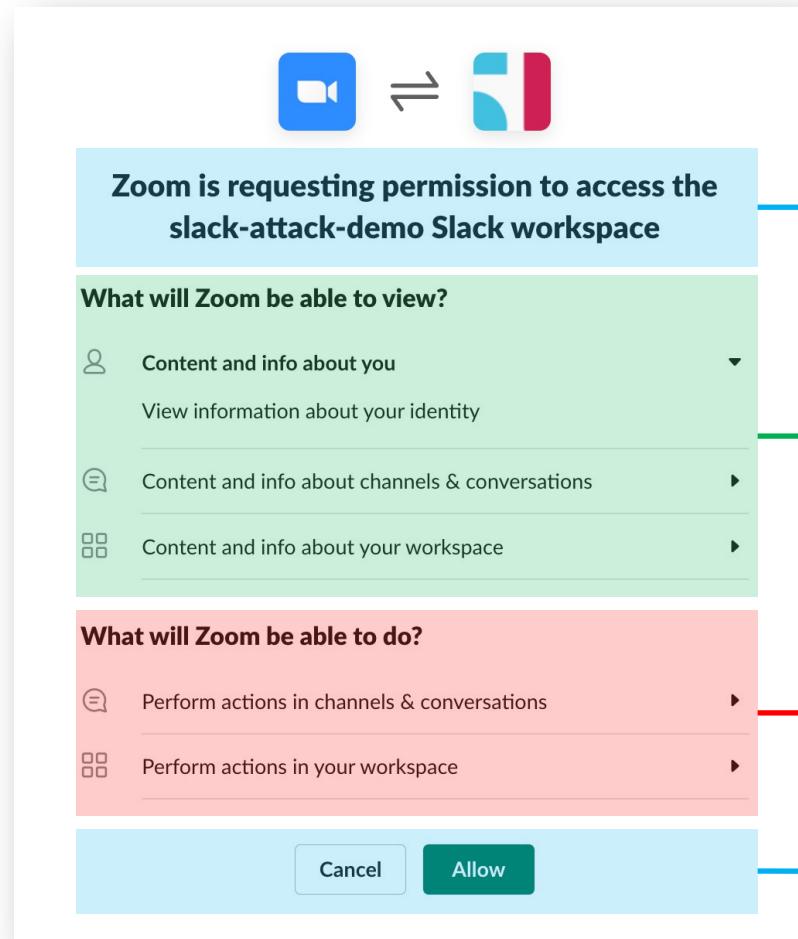


Background: App Workflow





Background: App Installation



1. App Requests Permissions

2. Read Permission Scopes

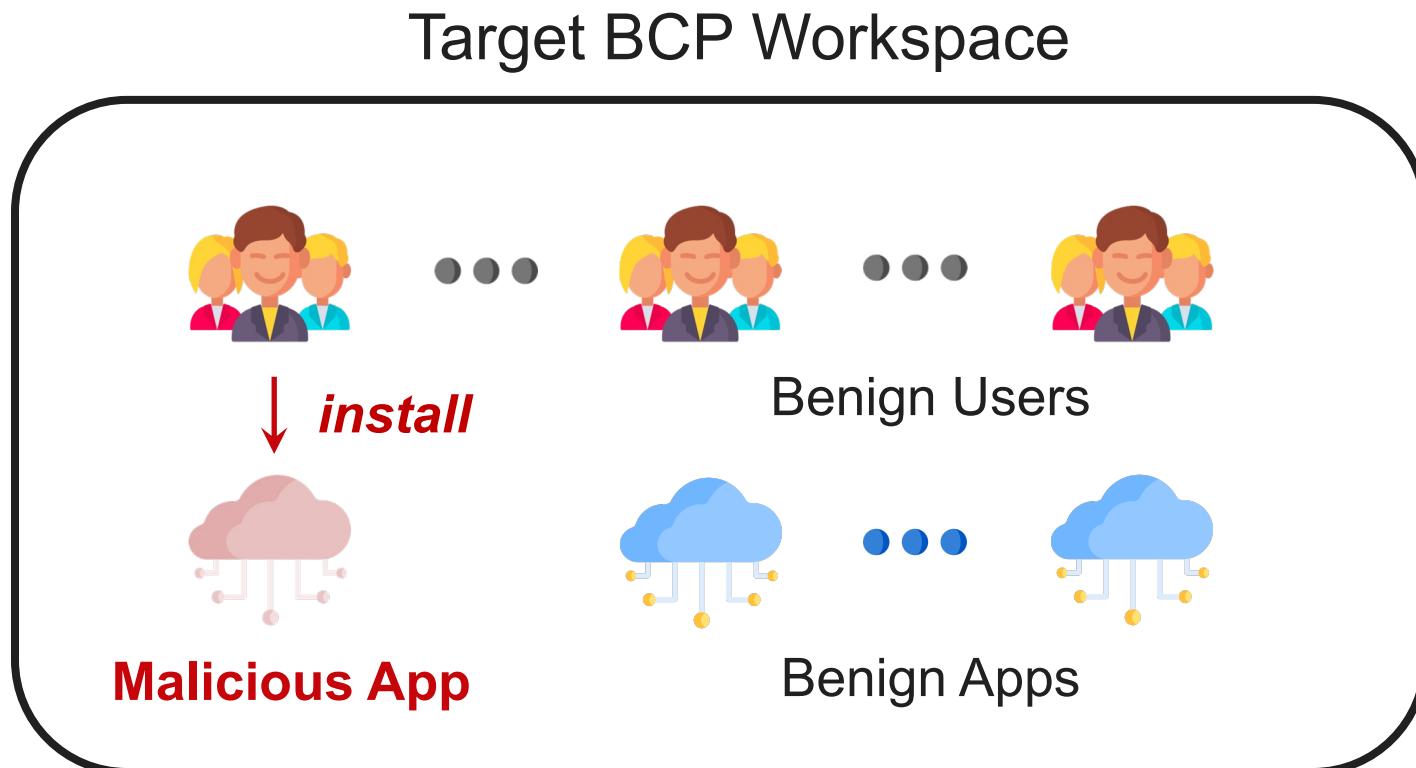
- Read user identity*
- Read public messages*

3. Write Permission Scopes

- Post messages*
- Post messages on behalf of users*

4. User Approves Permissions

Threat Model: Malicious Apps in BCP



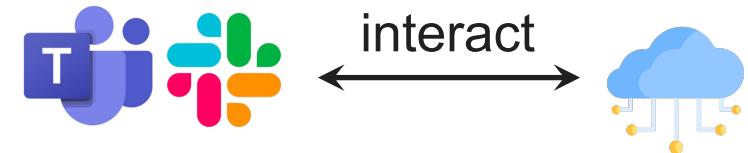
- Attacker tricks the user to install a malicious app
- The user is curious and installs a malicious app
- The benign app becomes malicious



Challenges & Our Methodology

- Incomplete permission model description.

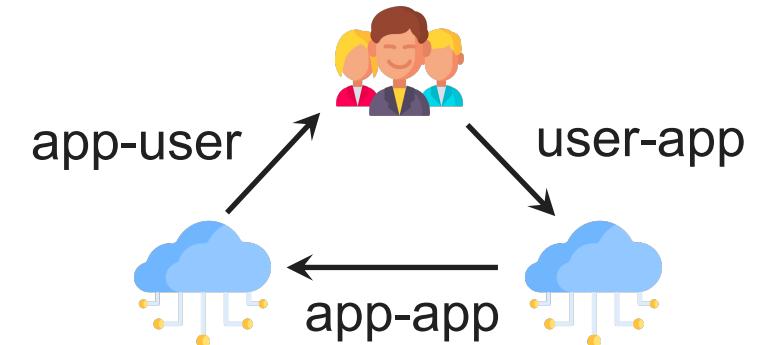
We extract a unified abstraction.



one permission model

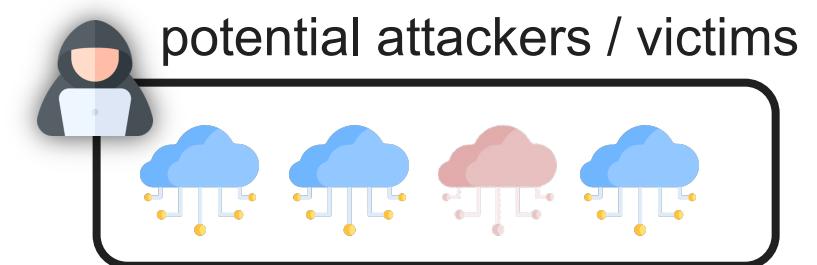
- Closed-source apps in the cloud.

We examine all possible interactions.



- Unscalable in-depth analysis.

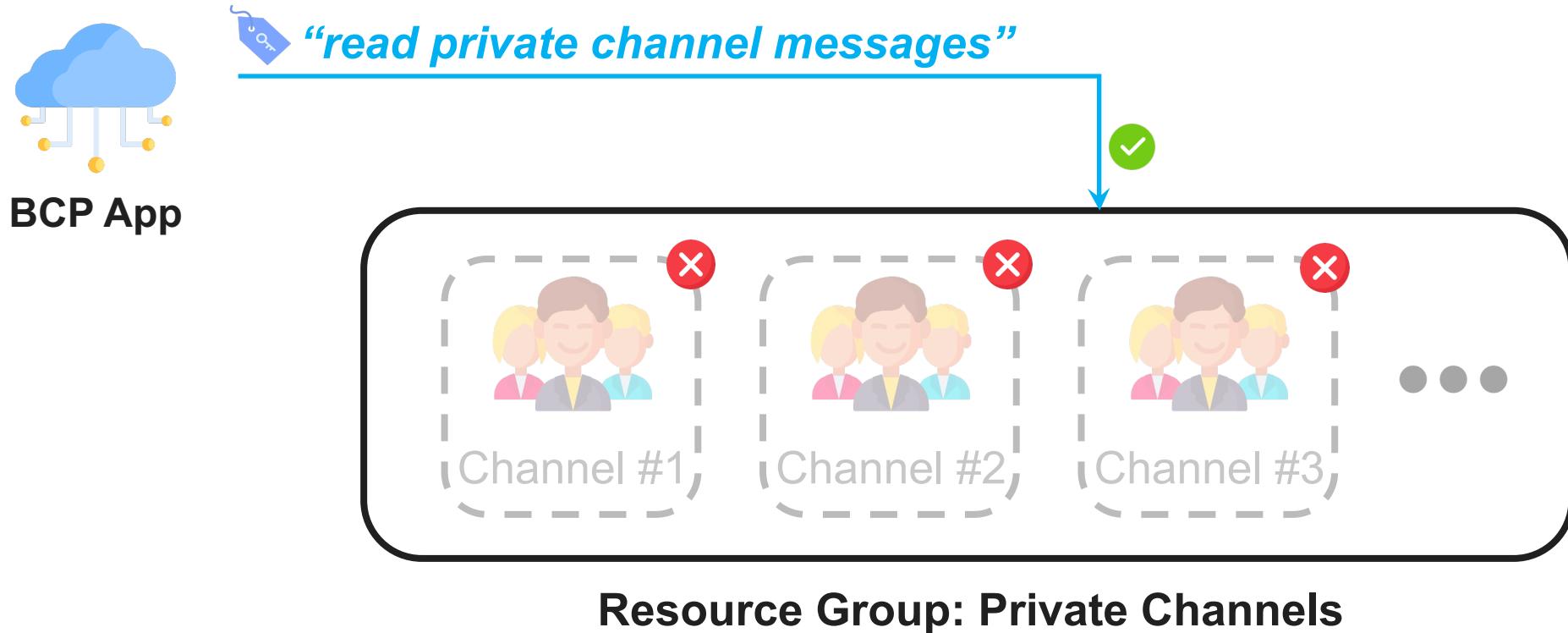
We estimate potential attackers & victims.





A Two-Level Unified Permission Model

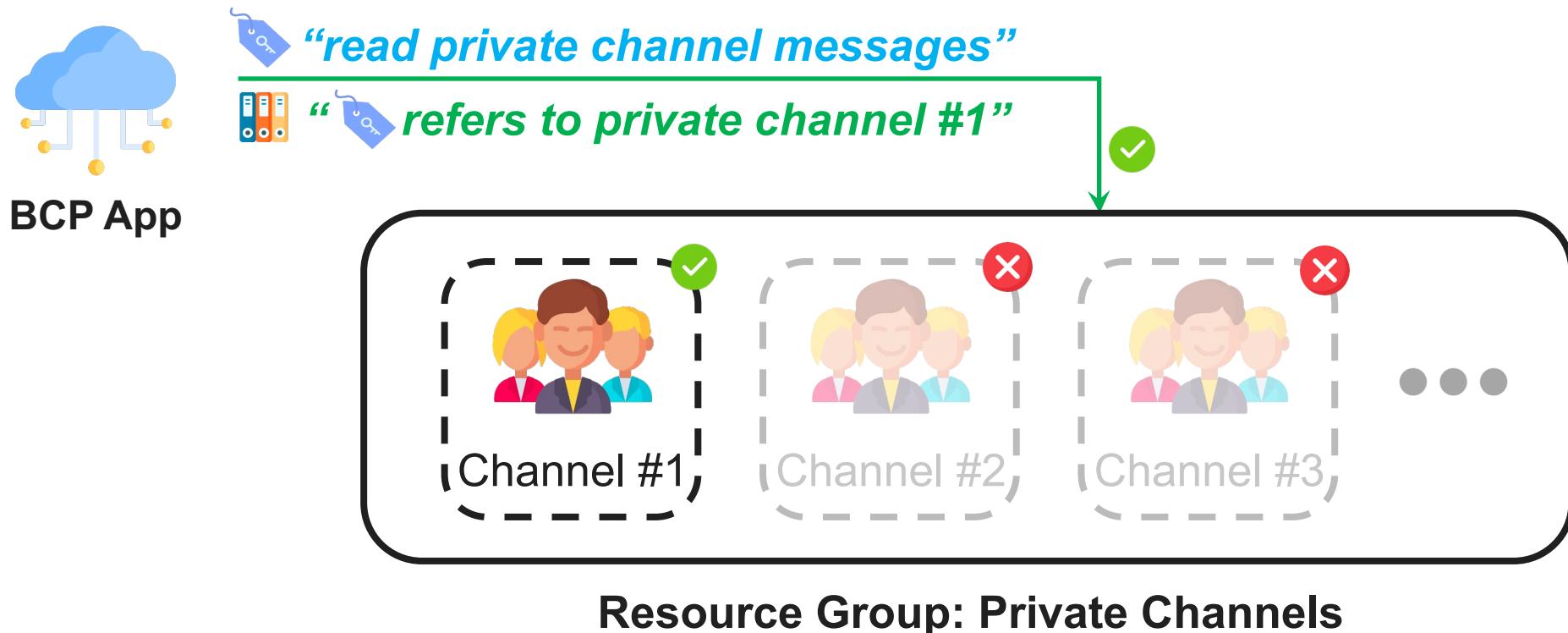
- Level 1: coarse-grained OAuth permissions scopes





A Two-Level Unified Permission Model

- **Level 1:** coarse-grained OAuth permissions scopes
- **Level 2:** fine-grained runtime policy checks



Violation of Security Principles

- **Least Privilege**

Runtime policies are ad-hoc and incomplete.



“post messages to channels”



“only if the app joined this channel”



“post messages to users”



“null”

- **Complete Mediation**

Provenance of resources are not properly tracked.





All Types of Interactions Are Vulnerable

- App-to-App Interaction → *Delegation Attacks*



- User-to-App Interaction → *Command Hijacking*



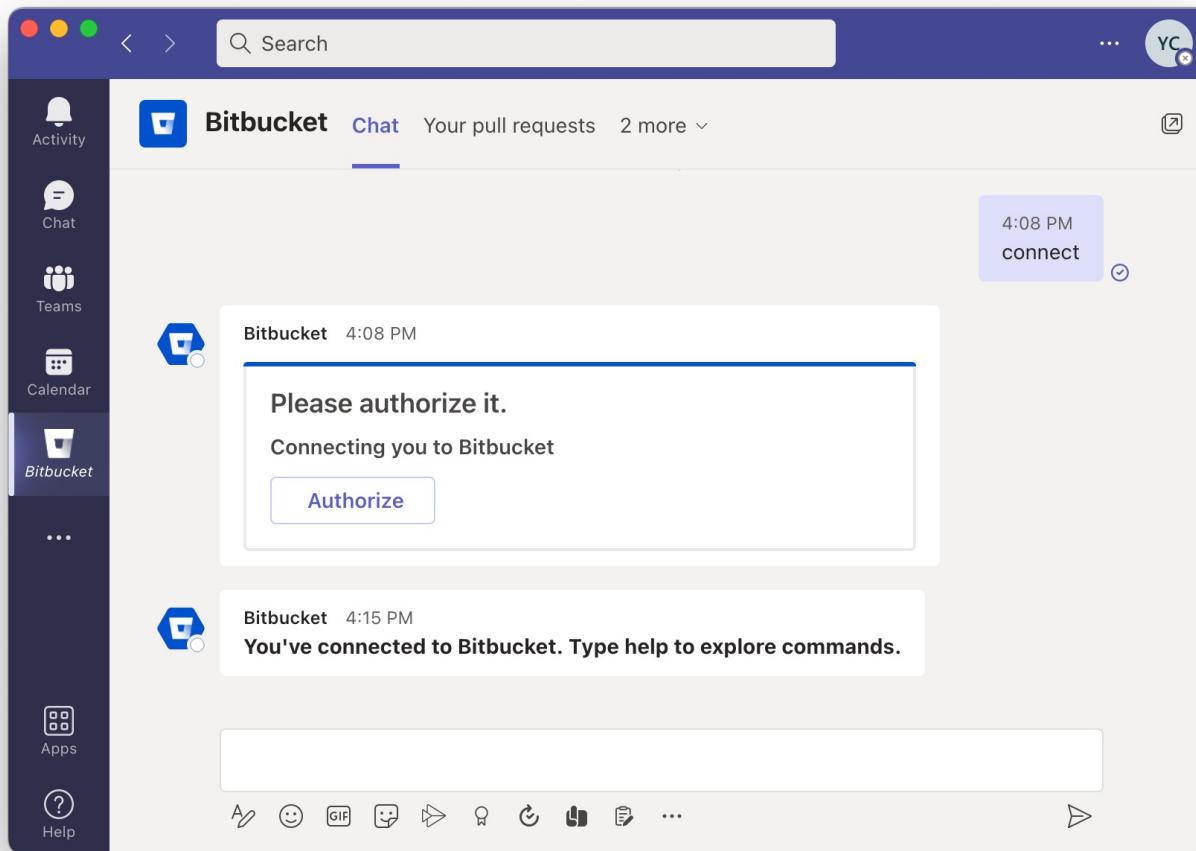
- App-to-User Interaction → *Privilege Escalation*





Delegation Attack: Merge Malicious PRs

- Step 1: User installed Bitbucket app.



“Merge #1”



“Confirm merge #1?”



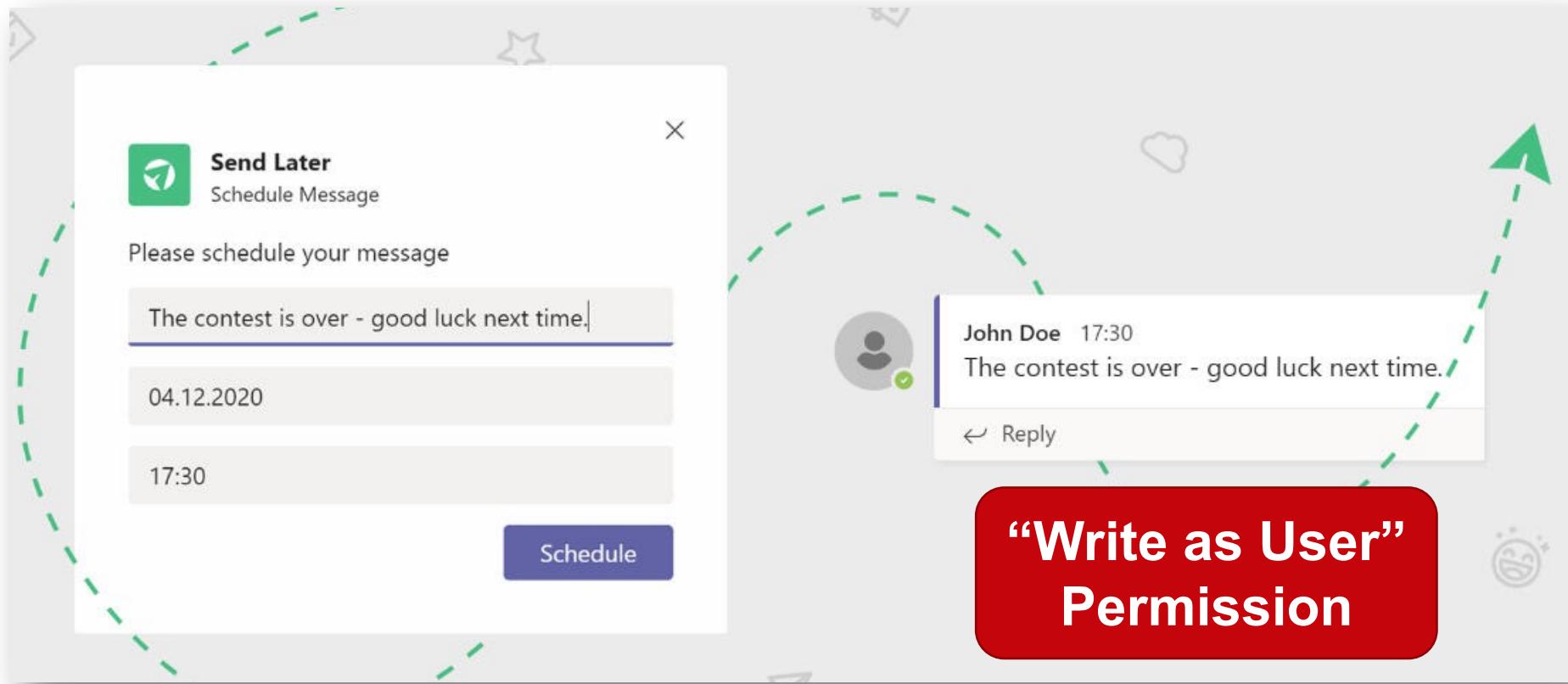
“Yes”



“Merged!”

Delegation Attack: Merge Malicious PRs

- Step 2: User installed “Send Later” app (*our malicious demo*).





Delegation Attack: Merge Malicious PRs

- Step 3: Attacker creates a **malicious** Pull Request #1.

The screenshot shows a GitHub pull request page for the repository `madison-sp / BCP-attack-demo / example-repo`. A red box highlights the status message `evil.txt created` above the pull request details. A red arrow points from the text **Bump version to ...** to the `evil.txt created` message. The pull request details include the author `YC`, target branch `master`, and status `OPEN`. The commit message is `evil.txt created`. The code diff shows a single line: `1 + This file is evil...`.

Repositories Projects More ▾ Create ▾

madison-sp / BCP-attack-demo / example-repo / Pull requests

evil.txt created

YC eviltxt → master OPEN
#1 · Created 2 minutes ago · Last updated 1 minute ago

Edit Approve Merge ... Settings

Description
evil.txt created

> 0 attachments

0 comments

YC Add a comment

> 1 commit

1 file

FILTER BY COMMENTS 🔍 YC

SORT BY File tree

evil.txt

@@ -0,0 +1 @@
1 + This file is evil...



Delegation Attack: Merge Malicious PRs

- Step 4: Malicious “Send Later” app talks to the Bitbucket app.

The screenshot shows a messaging interface with a sidebar containing icons for Activity, Chat, Teams, Calendar, Bitbucket (which is selected), Apps, and Help. The main area is a conversation with the Bitbucket app. A message from Bitbucket at 4:46 PM asks, "Are you sure that you want merge this pull request?" with "Yes" and "No" buttons. Above this message is another message from Bitbucket at 4:46 PM labeled "merge #1". A red box highlights this message, and a red line points to the text "First request ‘merge #1’". Below the "Yes" button is a message from Bitbucket at 4:46 PM stating "merge 1". A red box highlights this message, and a red line points to the text "Confirm ‘merge #1’". At the bottom of the conversation, a message from Bitbucket at 4:46 PM says "Pull request was successfully merged." This message is highlighted with a blue box, and a blue line points to the text "Pull request was successfully merged."



Delegation Attack: Merge Malicious PRs

- Step 5: Bitbucket merges the malicious pull request.

The screenshot shows a Bitbucket interface for a pull request. At the top, there are navigation tabs: 'Repositories', 'Projects', 'More', and a blue 'Create' button. Below the tabs, the repository path is shown: 'madison-sp / BCP-attack-demo / example-repo / Pull requests'. A prominent message 'evil.txt created' is displayed. Below this, a pull request card is shown for user 'eviltxt' merging into 'master'. The status is 'MERGED'. The pull request was created 24 minutes ago and last updated 4 minutes ago. A green box highlights the 'Merged pull request' status, stating 'Merged in eviltxt (pull request #1)'. The commit hash 'bff8c2e' and author information ('Author: Yunang Chen · Closed by: Yunang Chen · 4 minutes ago') are also visible. At the bottom, a 'Description' section contains the text 'evil.txt created'.



Potential Prevalence Analysis

- Collect each app's requested permissions.
- **Capable Apps** — *Have write permissions needed for attacks.*
- **Susceptible Apps** — *Have read permissions affected by attacks.*

Attacks	# Capable Apps (MS Teams)	# Capable Apps (Slack)	# Susceptible Apps (Slack)
Delegation Attacks	427 (33%)	563 (23%)	1,493 (61%)
Command Hijacking	77 (6%)	270 (11%)	1,266 (52%)
Privilege Escalation	n/a	11	n/a

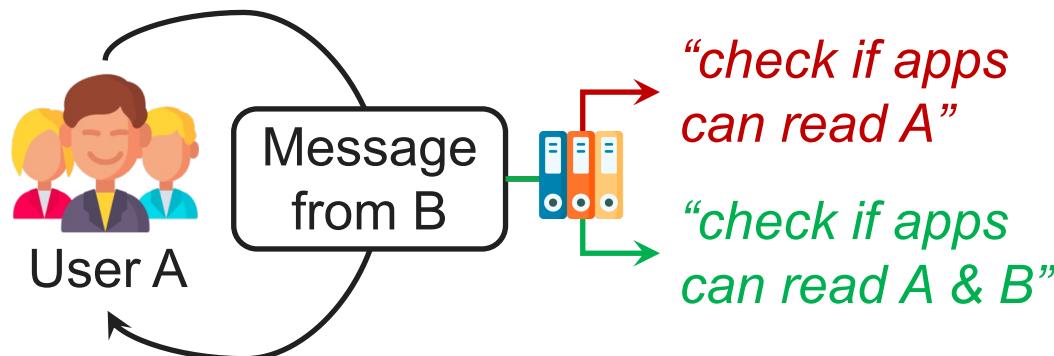
Countermeasures: Improve Permission Models

Better Design

– Finer-grained Scopes

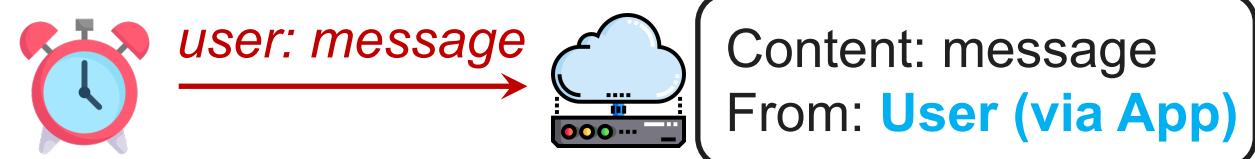


– Stricter Runtime Policies

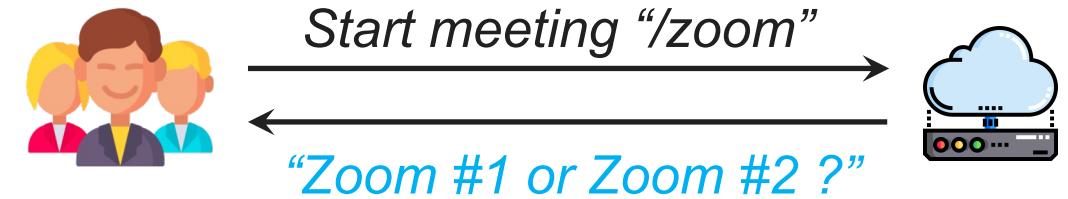


Better Execution

– Track Provenance of Actions



– Explicit User Confirmation





Disclosure & Responses

- Confirmed attacks
- Workspace → a trusted environment
- Administrator → will correctly manage apps

- Our tips for administrators
 - Consider limiting users from installing apps
 - Actively monitor the behavior of installed apps
 - Only approve delegation permissions from trusted apps

Summary

- BCPs have become a hub for **sensitive third-party resources**.
- We provide **security analysis** under malicious apps.
- All types of interactions are **vulnerable & potentially prevalent**.

