Team Members: Sahib Bajwa – [sahib.bajwa@colorado.edu](mailto:sahib.bajwa@colorado.edu) – completed the entire assignment.

(note on group members at the end of the assignment)

Niemiec

CSCI 3403

6 February 2020

Project 1

**Explaining Your Event:**

The event I chose to analyze was the abuse of Twitter’s API to uncover user identities, written by Lindsey O’Donnell from Kaspersky Labs’ Threatpost. This happened due to a “large network of fake accounts abusing a legitimate API function on its platform that, when sued as intended, allows accounts to find users that they may already know by matching phone numbers to their Twitter Account names.” In essence, people’s real names could be figured out due to a security vulnerability on Twitter’s API. This relates to cyber security because the whole point of cyber security is to now allow for these types of breaches to occur in the first place.

Twitter can find Twitter accounts of people that you know by searching for accounts that have phone numbers linked to them that correspond to phone numbers in your contacts. Twitter’s API that helps them accomplish them was breached unknowingly, allowing for unauthorized people to access other user’s personal data.

Even big companies like Twitter make mistakes and do not realize it for a while. Twitter is one of the most used sites on the internet yet had a security vulnerability that most people would agree should not have happened in the first place. The event wasn’t breaking into Twitter’s API, it was exploiting a vulnerability in its design.

**The CIA Triad:**

Confidentiality: The confidentiality of user’s information was breached during this event. The attackers were able to access and see other’s personal information that they did not intend to be seen by others.

Integrity: Based on this article, integrity was not breached during this event. The attackers were not able to change any user’s data, thus their information stayed trustworthy.

Availability: Twitter never went down during this event, thus Availability was not breached. Their API was not taken down and neither were any of Twitter’s functions.

**Common Design Principles:**

Least Privilege: That specific portion of the API should not have been quarriable by everyone. This would have made it so that no one other than Twitter could have accessed people’s sensitive personal information.

Defense In Depth: Don’t allow for bot accounts to exist on the website. Bot accounts should be accounted for by removal from the site. This would include adding authenticators to accounts so attackers could not make massive amounts of accounts.

Complete Mediation: Similar to least privilege, make sure that every API query is checked. This would prevent people who should not access private sections of the API from doing so. If a query is made to this section of the API, either flat out deny the request or mislead the attacker into thinking they got what they wanted (but it really being garbage).

Sources

<https://securityscorecard.com/blog/top-10-information-security-websites-to-follow>

<https://threatpost.com/twitter-api-abused-to-uncover-identities/152521/>

<https://www.us-cert.gov/bsi/articles/knowledge/principles/complete-mediation>

**Note on Group Members** (from Sahib Bajwa)**:**

As far as I know, I do not have team members? I have not been contacted by anyone and do not know how to contact my prospective group members. I will send an email shortly to the class email asking about this, but I submitted my google form saying that I did not have any group members, so I am hoping that I get to work solo on my project. If I do in fact have group members (I see on this assignment’s turn in page that I am in group T78, but it does not link to anywhere), I will contact them after this assignment. I hope that points won’t be taken off due to this fact as I have not been able to find a group listing on the Moodle site or on Piazza.