Challenges and Innovations in Security

Theme: Security

By Adam Paul 11/29/2020

Code Injection – What is the threat?

- Code injection is a type of cyberattack which involves the injection and subsequent execution of a malicious software attack.
- With the rise in popularity of smartphones in recent years, many developers have collaborated to build an HTML-5-based framework for development across several platforms.
- However, having a cross-platform framework also means that these apps will be vulnerable to the same cyberattacks.
- As development for this framework is still relatively new, it’s necessary that software be built to detect and pinpoint the code injection vulnerabilities in it.

SCANCIF – What is it?

- SCAN Code Injection Flaws (SCANCIF) is an automated code injection detection tool created by Tuong Phi Lau (2018).
- In past research into HTML-5 vulnerabilities, such as with programs like DroneCIA, only one type of vulnerability was concentrated on (Chen, et al., 2015).
- Instead of focusing on singular vulnerabilities, SCANCIF opts to identify APIs, known or unknown, that these vulnerabilities originate from, flagging them via a tag system.
- SCANCIF then “slices” out these tagged APIs, showing them and their tags to the user.
- This allows for manual code review in order to identify how these vulnerabilities are caused.
- However, SCANCIF is incapable of identifying individual apps that are vulnerable, as it simply identifies and slices APIs.

SCANCIF - Outcomes

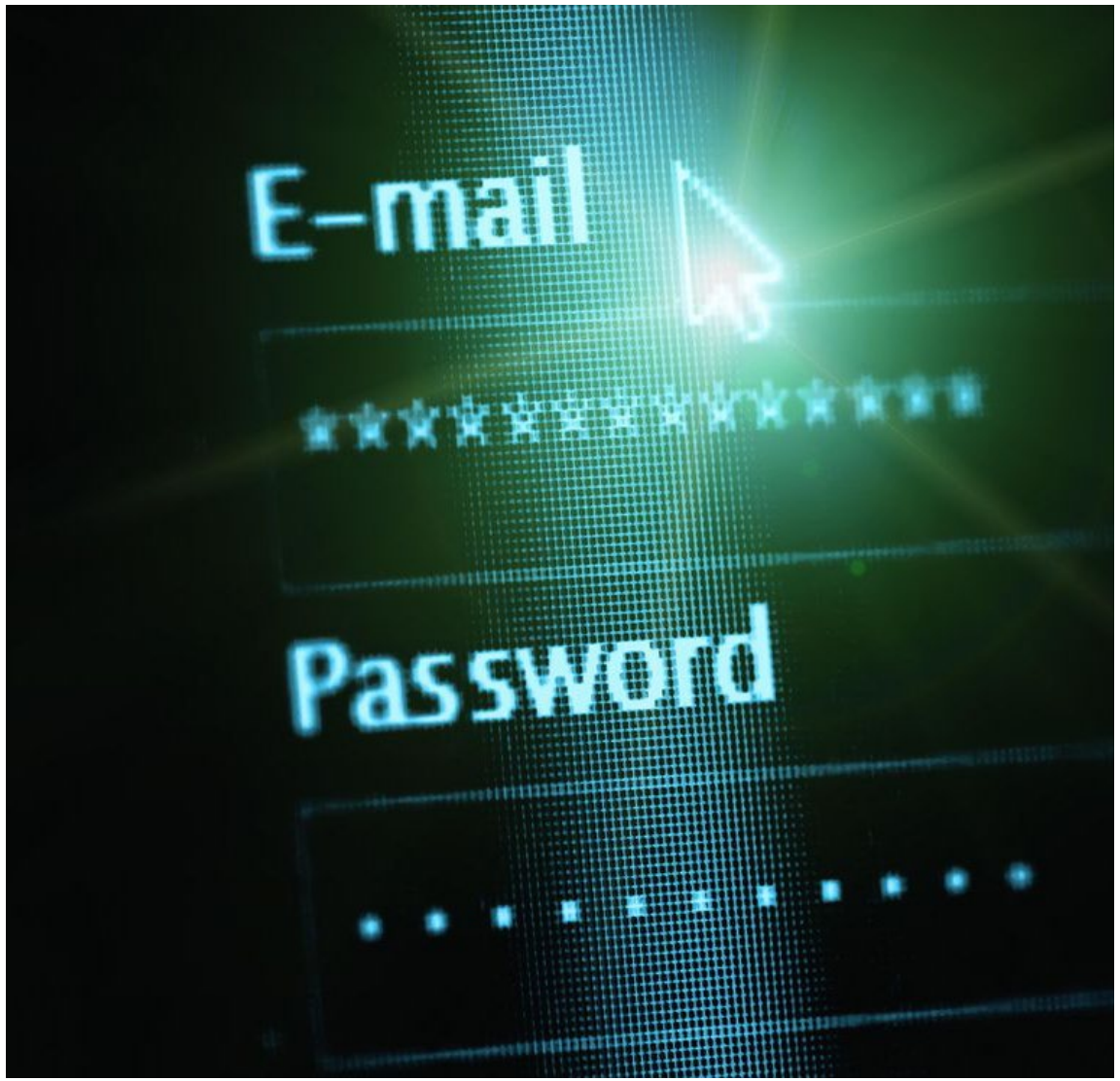
- SCANCIF scanned a total of 3,204 apps downloaded from the Google Play store.
- Of the 3,204 apps scanned, 220 were found to be vulnerable and 4 new vulnerable plugin APIs were able to be found (Lau, 2018).
- As time passes, HTML-5 code injection attacks will only get more complex and harder to identify.
- When this time comes, programs like SCANCIF will be crucial to ensure that some of the most widely-used APIs will be safe and secure for their plethora of users.
- In the future, SCANCIF will be able to serve as either a foundation for or a piece of a larger, more comprehensive code injection diagnosing software.

SCANCIF - Impacts

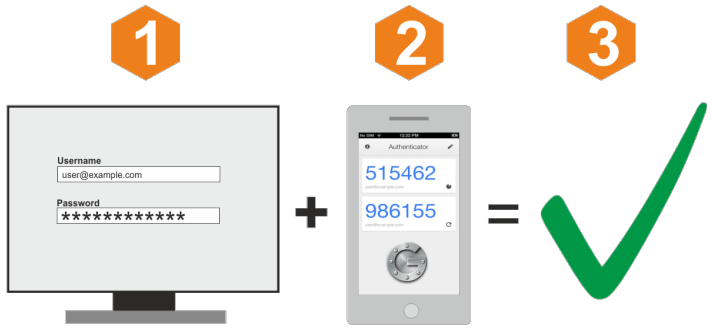
- **Economic:** SCANIF's use in identifying vulnerabilities can prove extremely useful for bank app developers who are using the HTML-5 framework for their app, allowing for the creation of a more secure app.
- **Cultural:** SCANIF's identification capabilities also benefit regular users and their social media accounts. Code injection can lead to personal data being leaked, which can lead to personal social media accounts being compromised.
- **Political:** In a similar vein, SCANIF can indirectly prevent the hacking of a politician's website that would cause them to lose credibility via the spread of false information.

Account Security Breaches – What is the threat?

- As time goes on, traditional methods of login for most websites become less secure overall.
- Oftentimes, these systems are based on a username and password, with no other form of barrier between an attacker and an account.
- This lack of extra security means that brute-force password-guessing systems are a viable way for hackers to gain access to others' accounts.
- These password-guessing scripts only get more advanced over time.
- In order to defend against these attacks more effectively, account login systems must implement more thorough security checks.



Two-Factor Authentication – What is it?



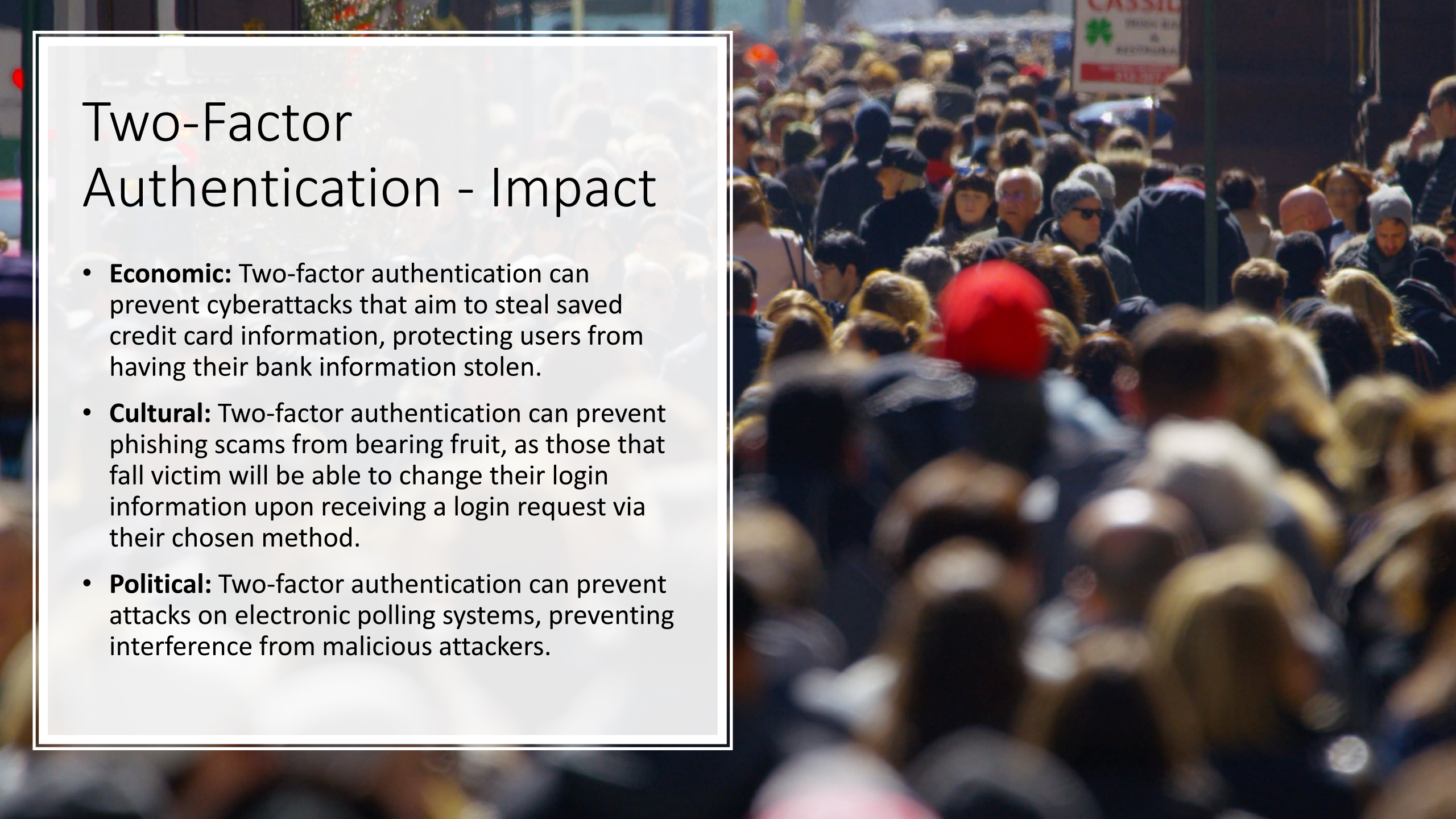
- Two-factor authentication increases account security by requiring users to present two of the following types of authentication factors: something they know (traditionally a password), something they have (such as a phone or hardware to-ken), or something they are (referring to biometrics, such as a fingerprint) (Reese, et al., 2019).
- The most frequent combination of these three are password verification and hardware verification.
- Two-factor authentication often employs one of five different methods: SMS, TOTP, pre-generated-codes, push, and U2F security keys (Reese, et al., 2019)
- Short Message Service (SMS) involves the user being sent a short code via text message that must be input to login.
- Time-based one-time password (TOTP) is the most complex, syncing a key generator on the user's mobile device with the login system of the website. Every 30 seconds, a new login password is generated that is only valid for 30 seconds after generation.
- Pre-generated codes are typically generated when the user initially sets up two-factor authentication, used in an emergency wherein the user lost access to their typical authentication method.
- Push involves push notifications from one's smartphone being sent, requiring the user to press "Approve" or "Deny" to log in.
- Universal 2nd Factor (U2F) involves connecting an authentication device to their computer via USB, having them activate the device when prompted.

Two-Factor Authentication – What's next?

- Two-factor authentication proves to be far more secure than traditional login means, as hackers are far less likely to have access to multiple systems of a single user.
- However, two-factor authentication isn't a be-all end-all solution for security.
- To this day, efforts are underway to improve the existing two-factor authentication systems through both new innovations and new applications.
- One suggestion utilizes yet-to-be completed quantum computing technology as a means to make one-time passwords generated by two-factor authentication systems more secure for both the user and the server (Sharma & Nene, 2020).
- Another suggests the utilization of a "virtual smart card" that leverages the security features of the Android OS to protect cloud data in a unique manner of two-factor authentication (Derhab et al., 2020).

Two-Factor Authentication - Impact

- **Economic:** Two-factor authentication can prevent cyberattacks that aim to steal saved credit card information, protecting users from having their bank information stolen.
- **Cultural:** Two-factor authentication can prevent phishing scams from bearing fruit, as those that fall victim will be able to change their login information upon receiving a login request via their chosen method.
- **Political:** Two-factor authentication can prevent attacks on electronic polling systems, preventing interference from malicious attackers.



Works Cited

- Chen, Y., Lee, H., Jeng, A. B., & Wei, T. (2015). DroidCIA: A Novel Detection Method of Code Injection Attacks on HTML5-Based Mobile Apps. *2015 IEEE Trustcom/BigDataSE/ISPA*. doi:10.1109/trustcom.2015.477
- Derhab, A., Belaoued, M., Guerroumi, M., & Khan, F. A. (2020). Two-Factor Mutual Authentication Offloading for Mobile Cloud Computing. *IEEE Access, 8*, 28956-28969. doi:10.1109/access.2020.2971024
- Lau, P. T. (2018). Scan Code Injection Flaws in HTML5-Based Mobile Applications. *2018 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*. doi:10.1109/icstw.2018.00032
- Reese, K., Smith, T., Duston, J., Armknecht, J., Cameron, J., & Seamons, K. (2019). A Usability Study of Five Two-Factor Authentication Methods. *Proceedings of the Fifteenth Symposium on Usable Privacy and Security*. Retrieved November 30, 2020, from https://www.usenix.org/system/files/soups2019-reese.pdf
- Sharma, M. K., & Nene, M. J. (2020). Two-factor authentication using biometric based quantum operations. *Security and Privacy, 3*(3). doi:10.1002/spy2.102 https://onlinelibrary.wiley.com/doi/pdf/10.1002/spy2.102