How iot, mfa, e2ee and gdpr may impact the security of mobile connections in futu...

Sociology, Communication

Securing Mobile Communications

Mobile security refers to smartphones, tablets, and any device that a person can carry while on the go. Nearly all homes have some sort of mobile device that an attacker can gain access to and steal data. Enterprises have felt the heat to secure these devices under the BYOD platform, since company data/user data is highly sought after by attackers from all parts of the world. The major downside to mobile security is the security gap that comes with accessing the world wide web and lack of user knowledge. Security issues include data theft, rise of malware, data leakage, and many more. Endpoint security, a term used by the IT community, is said to provide a layered approach to securing these mobile platforms and possibly organizations reducing the BYOD footprint using special methods.

Mobile Network Security

Mobile privacy is considered a very important facet of our daily lives. From social media websites to mobile applications to banking institutions, user data is stored in a multitude of places for a hacker to feast on. Smartphone apps gather data such as phone number, email, username, and geolocation data. Most apps, if not all, ask for permission to access your information before they gather the data they need. The underlying issue is if you refuse to give your apps permission, they will deny you access to the application itself; kind of a double-edged sword as apps have been known to make our lives easier. Apps use what they call “ risky permissions. Risky permissions affect stored data or full use of the app itself.

Risky permissions include track location (geolocating), camera access, access to audio record, and access to call log/SMS (Cleary, 2018). Every app or website a user is associated with via their PII is linked into one main user profile. There are websites that ask you to log in via your username/password or through your Gmail account. That in itself could lead to more risky behavior from a user standpoint. A recent study purported that out of all the apps on the market, only 4% employ strong security and privacy practices! (Cleary, 2018). To put it plainly, users have no idea what they're consenting to as the app use third parties for proper functionality. In the same token, removing themselves from liability if user data is stolen. How do users protect themselves? Thoroughly read over the privacy policy and know what is at stake and do not sign into an app using your social media website or email.

Mobile Authentication

What does it mean to authenticate? Authentication is done to ensure users are who they say they are, based on a number of factors, i. e., username/password, biometric data (facial recognition, fingerprint), swipe pattern technology, push notification, etc. Legacy authentication methods (2FA) were a thing of the past. In theory, " legacy solutions lack the capabilities to enforce policies based on risk, including the inability to leverage contextual, behavioral, or correlative factors like gelocation, device posture and nature of transaction being attempted" (Goodman, 2018). What is the solution to 2FA? Multifactor Authentication (MFA). Nowadays, 2FA is used in most applications, while some do not think its enough. Currently,

there are three ways for a user to claim they’re real and need access to data present: Knowledge, Possession, and Inherence (Tatum, 2016).

Out of the three only two are used. With MFA, all three would be used to verify user identity. Is MFA more secure than 2FA and how does that affect user experience? To answer the question, MFA is like adding another lock onto your front door – adds another layer of security that an attacker would have to get through. However, the downside of more security could hinder user experience. Users do not more security as it takes away from usability and can be cumbersome. PCI DSS has replaced all 2FA authentication with MFA in version 3. 2; however, 2FA is still in progress, but may change at a later date (Tatum, 2017).

Attack Vectors

A path or means by a hacker to gain access to a target system (Rouse, 2012). Meaning, an attacker will do anything by any means to get access to your device. From viruses, the infamous pop-up windows, social engineering, etc. Firewalls and patching software tend to block some vectors, but there is always another means of entry. Hackers are realizing that it is easier to use social engineering to gain entry than crafting malicious code.

Trusted Computing Base

Trusted Computing Base or TCB, involves everything within a computer that makes it secure, but what exactly? OS and its security mechanisms, hardware, firmware, procedures, and software (Rouse, 2005). The introduction of TCB was to reduce or eliminate malware attacking mobile

phones based on TCB. TCB manages sensitive information and core services/applications independent of the OS (Gilad, Herzberg, Trachtenberg, 2014). User then invokes a key that validates themselves and protects the sensitive data, even if malware is present. Below is a TCB layout that explains smartphones OS from the TCB. (Gilad, Herzberg, Trachtenberg, 2014) recommends TCB over ARM's Trustzone (trusted-code-execution platform prevalent in today's smartphones. What makes TrustZone unique is that it manifests two environments running concurrently via a single core, starting with the physical layer.

Internet of Things (IoT)

IoT means every device that is connected to the world wide web. Microwaves, refridgerators, smart watches, Alexa, TV's, and many more. It's about connecting all devices and optimizing user efficiency.

Associated Risks & Vulnerabilities

Disadvantages of IoT are common as no one knows the full extent of its capabilities. Compatibility is the first issue as there is international standard for tagging and monitoring of equipment (Quek, 2017). When bluetooth was first implemented, it was met with the same criticism. Complexity which could be a good or bad thing. Major glitches in the software could lead to overexpense if not caught on time. The next and most important issue is privacy and security. If our water systems and power grids that give us power is jeopardized in any way, that would be catastrophic for all users. With everything being connected, a user's medical information or financial data a few things that would be targeted.

Benefits

Advantages of IoT include communication, automation, mass information, monitoring capabilities, time, ability to save money, automate conrols, and better QoL (quality of life) (Quek, 2017). Essentially, every human will be connected to the internet with the ability to link with other like-minded people. Ten fold, this will be one of the biggest achievements in history. Health monitors, for instance, will be used to identify health problems, eliminating time wasted and catching medical emergencies before they become terminal; this data will then be forwarded to doctors on a consistent basis.

Future of IoT

A recent report conducted by Samsung says that a clear danger exist with technology as it may be running ahead of its time; additionally, the need to secure every connected device by 2020 is critical (Burgess, 2018). With the implementation of 5G, technology will bring us Virtual Reality (VR), improved surveillance, one-click solutions, etc. Microsoft has started the initialization of IoT (IoT Central) to help organizations simplify IoT networks (Burgess, 2018).

Security Challenges

Encryption (Layers). Encryption is critical as we move into the IoT. All devices must be encrypted, to include the data within it. We are moving into an age where desktops are becoming obsolete; laptops may be soon to follow. End to End Encryption (E2EE) communications is becoming a staple in the technology world. The reason for the adoption of E2EE is the General Data Protection Regulation (GDPR) global standard on protecting user data.

Current encryption types are Secret Key, Public-key, Block Ciphers, Stream Ciphers, Elliptcal Curve, and Blockchain. What will the future of encryption look like? E2EE is looking to tackle issues like email phishing attacks and IoT. A company called Level 3, explain that global corporations no longer need to trade network performance for encryption of their most critical data; below depicts what the cyber landscape will look like moving forward and ways to protect the infrastructure (Level 3, 2017).

These wave use AES 256 encryption using dynamic key and key rotation for added security. To be clear, this encryption format is forward looking and is merely a thorough idea that could be useful to mobile encryption. Companies are starting to notice that current encryption methods are no match for the ongoing cyber threats. Users browsing needs via mobile devices are protected using SSL and TLS protocol, making data unreadable; however, these security formats are being bypassed on a consistent basis. Below is a depiction of data at rest and in transit. As stated earlier, MFA will be used to authenticate on mobile devices, coupled with solid E2EE to give the user a more secure platform.

BYOD/MDM (Advantages/Disadvantages)

BYOD (Bring Your Own Device) being introduced into the workforce has been a controversial topic for some time now. Employees utilize their own mobile phones to access organizational data and email. More and more employers have employees who work from home, which means they work remotely and need access to said information. Advantages of BYOD: Lower Cost, Technology Familiarity, and Flexibility (Optimus Learning, n. d.). BYOD

means employers do not have to buy expensive laptops or devices to give to employees. This expense is remedied as people use their own devices and they will likely take care of it as it is their own. People are also familiar with their own device, as this saves time and money for training (on site/off site).

Disadvantages of BYOD are broken down as the added costs for employees, device disparities, and security (Optimus Learning, n. d.). There are too many cases with employees using their work laptop to conduct personal business and that data in question for being property of the employer. It’s a murky topic which is still being worked on. According to TrendMicro, Mobile Security includes Mobile Device Management (MDM), Mobile Application Management, Mobile Application Reputation Services, and Device Antivirus (TrendMicro, n. d.). Companies are investing in ways to safeguard corporate data. That front-end support extends from iOS to Androids to Windows. Data preventative methods include Data Encryption enforcement, password enforcement, remote lock and wipe, MDM, etc (TrendMicro, n. d.). Holistically, advantages of MDM means data protection as a centralized management system, low cost, and flexibility. This in turn enables easy monitoring of devices.

Common Threats regarding Mobile Security

Mobile devices are being attacked daily whether we know it or not. There are seven mobile device threats that are prominent and we will continue to see as technology advances: Data Leakeage, Unsecured Wi-Fi, Network spoofing, Phishing Attacks, Spyware, Broken Cryptography, and Improper Session Handling (Kaspersky, n. d.).

Enforcement

Policy Language. All employers should have a policy in place that works as a standard operating procedure or an employee handbook. During orientation, an employer should relay their expectations of work habits. This would be the right time to go over BYOD policy. Policies should be fair, consistent, and in a conspicuous location. When crafting a policy, employers must take into consideration business and personal matters by allowing devices to access company data. (Redmond, Fong, 2018) mention Key issues that should be echoed are:

- Network and Information Security
- Employee Privacy
- Wage/Hour Compliance
- Policy/Procedure ComplianceGeneral Data Protection Regulation (GDPR) is one of the biggest drivers for corporations to get the ball on the road with securing mobile communications. Since BYOD is becoming very popular and will be a part of our lives moving forward, behemoth organizations like Apple and Google have a duty to protect user data.

Benefits and Drawback

Being GDPR compliant has a range of benefits to include: enhances your organizations cybersecurity strategy, improvement to data management, increase return on investment, boost audience loyalty and trust, and establishment of a new business culture (Fimin, 2018). GDPR is holding businesses accountable and its time that something is done about keeping

mobiles secure. With trust and security as two main focuses of GDPR, organizations will not be afraid to let their users know how/who has access to their data. Many believe that GDPR is hampering innovation due to its overregulation. This means that the cost to become compliant is costing some serious coin and some companies do not have the funds to get there. Like it or not, companies are grappling with this new cybersecurity strategy that's suppose to revolutionize data security. If GDPR maintains this strict regulation standard, data breaches are suppose to falter.

Responsibilities

As mentioned earlier, GDPR is taking a global responsibility in protecting users data; however, the onus should not be put on one entity. Studies have shown that users are careless when securing their smartphones. Nearly 3 out of 4 mobile users (73%) stated that they are not aware of security threats and best practices when working remotely, while almost half admitted to open suspicious email/attachments (Hickey, 2007). Companies need to address security as it is a complete package when both employer and employee are exercising safe practices.

Conclusion

In the near future, IoT, E2EE, GDPR, and MFA are all terms that we will hear on a consistent basis. IoT of things will transform how we interact with our devices, but to do that, we need MFA and E2EE to make that happen. Users and corporations have a duty to keep data safeguarded, but it needs to be a collective effort. The implementation of BYOD in the workplace is a great strategy for organizations to reduce the cost of expenses. MDM and MFA can

be used to close the gap on BYOD and protect a corporations data, to include employees data. GDPR is taking a step in the right direction as we haven't seen the full force of GDPR's hammer, but likely we will see some pretty hefty fines dealt in the near future. Mobile security extends to our smartphones, but also to tablets and any device where data has value. Smartphones pose a monumental risk moving forward. Lawmakers are constantly going back to the drawing board to toughen regulation, while keeping users data safe. Countering mobile threats will take a huge effort and maybe one day we will no longer have to worry about data being compromised.

References:

1. Cleary, G. (2018). Mobile Privacy: What Do Your Apps Know About You. Retrieved from https://www. symantec. com/blogs/threat-intelligence/mobile-privacy-apps
2. Fimin, M. (2018). Five Benefits GDPR Compliance Will Bring to Your Business. Retrieved from https://www. forbes. com/sites/forbestechcouncil/2018/03/29/five-benefits-gdpr-compliance-will-bring-to-your-business/#6a8e18df482f
3. Gilad, Y., Herzberg, A., & Trachtenberg, A. (2014). Securing smartphones: A µTCB approach. IEEE Pervasive Computing, 13(4), 72-79. doi: 10. 1109/MPRV. 2014. 72
4. Hickey, A. (2007). Mobile Security is End User and IT Responsibility. Retrieved from https://www. computerweekly. com/feature/Mobile-security-is-end-user-and-IT-responsibility

5. Hillard, R. (2014). Data Encryption on the Cloud. Retrieved from http://rjhillard. com/data-encryption-cloud/Level 3. (2017). The Future of Encryption is in the Wave. Retrieved from https://www. prnewswire. com/news-releases/the-future-of-encryption-is-in-the-wave-300521162. html
6. Quek, T. (2017). The Advantages and Disadvantages of Internet of Things (IoT). Retrieved from https://www. linkedin. com/pulse/advantages-disadvantages-internet-things-iot-tommy-quek
7. Redmond, J., Fong, B. (2018). Crafting an Effective Bring Your Own Device (BYOD) Policy. Retrieved from https://www. naahq. org/news-publications/units/march-2018/article/solving-companys-byod-policy
8. Rouse, M. (2005). Network Security: Trusted Computing Base. Retrieved from https://searchsecurity. techtarget. com/definition/trusted-computing-base
9. Rouse, M. (2012). Network Security: Attack Vectors. Retrieved from https://searchsecurity. techtarget. com/definition/attack-vector
10. Tatum, R. (2017). What’s the Difference Between Two Factor Authentication and Multi-Factor Authentication. Retrieved from https://www. helpsystems. com/resources/articles/whats-difference-between-two-factor-authentication-and-multi-factor