Alex Shah
EN.695.741.81.SP25 Information Assurance Analysis
Mod 6 Assignment
March 1, 2025

1 Ransomware

What is ransomware?

Ransomware is a malware that encrypts and locks a user out of their files in an attempt to extort a ransom in exchange for decryption of the files. For example, in 2017 Wannacry spread around the world using the Eternal Blue exploit to infect devices, encrypt files, and demand payment from companies and institutions in Bitcoin.

How does ransomware work cryptographically?

Ransomware involves a series of steps to encrypt a user's files. First some malware needs to infect a target, such as by phishing or exploiting vulnerabilities in the target remotely. Once the malware has infected the device, built in encryption functions are used to encrypt local files using a key controlled by the attacker. The attacker notifies the user that they are locked out of their files and demand a ransom, and if the user is able to pay the ransom, the attacker can provide the private key or the symmetric encryption key for the user to decrypt their files.

In your opinion are mobile devices more prone to ransomware attacks than desktops, why or why not?

Mobile devices are vulnerable to ransomware, but mobile devices aren't as valuable to attackers as desktops. Desktops usually contain more valuable information to target, are more likely connected to corporate networks, and are less likely to have backups or easy ways to restore the encrypted data. This makes it more likely that a victim would pay for decrypting their desktop than mobile device. Attackers want to target the most valuable resources that would get them their ransom, and desktops are more appealing to attackers than mobile devices.

What are some of the defenses that can be employed to defend against ransomware?

Ransomware is a threat if you have no way of recovering the files or restoring the infected device. Regular backups offsite/offline allows the encrypted files to be kept safe even if a device is compromised by ransomware. But vigilance and prevention are also important, such as host and network based IPS solutions to detect malware and prevent phishing from being successful. Regular patches can also prevent the vulnerabilities that some ransomware uses as the initial vector to infect a machine. Critical system can be further protected using a ZTA security model to prevent devices from compromising other resources by enforcing access policies, segmenting the network, and monitoring the network. Employees should also be trained to prevent phishing attempts that could compromise their machine.

2 Bluesnarfing & Bluejacking

What is bluesnarfing and bluejacking?

Bluesnarfing and bluejacking are Bluetooth based attacks that can steal information or cause disruption on devices that have Bluetooth enabled. Bluesnarfing involves stealing information from a target Bluetooth device without the user knowing, whereas Bluejacking involves sending disruptive requests and messages to a target.

How do they compromise bluetooth technology?

Bluesnarfing uses vulnerabilities in the OBEX (object exchange) protocol on Bluetooth devices used to share files in order to connect to a target and extract information from it. For example, Bluesnarfing can be used to copy contacts, email, passwords, and files from the device without the user knowing. Usually this requires the attacker to be within Bluetooth range of the device but there are also more powerful directed radios and antennas that can be used to target devices further away. Bluesnarfing attacks were reported as early as 2003, and vulnerabilities in older devices were able to be exploited. Today some Bluetooth low energy devices are also able to be exploited by similar methods, such as those commonly used in IoT devices.

Bluejacking similarly targets nearby bluetooth devices and attempts to brute force pairing pins in order to establish a connection to a device. Then the attacker can send bogus requests or messages like prank images or attempt to phish or extort their target.

In your opinion with the increasing number of Internet of Things (IoT's) being IP addressable and being able to connect to smart devices/phones, will these and other Bluetooth types of attacks increase? Support your answer.

While there are many more devices coming online with the Internet of Things, Bluetooth attacks are primarily proximity attacks. Being IP addressable will increase the number of attackable devices on the Internet, but the increase of Bluetooth devices will affect the number of nearby attackable devices like Bluetooth war driving. This is especially likely considering many IoT devices use cheap, older Bluetooth chips with weak or default security options and these types of devices are harder to keep up to date and receive security patches sporadically if at all. In addition, with devices in the field, it is more difficult to monitor IoT devices subject to proximity attacks.

3 Mobile Application Scanning

Static & Dynamic analysis scanning methods are a popular method to use against mobile devices. Static analysis includes assessing the security of Android or I-Phone Apps, detecting app clones, automating test case generations, or uncovering non-functional issues related to performance or energy. Dynamic analysis includes testing & evaluating a program by executing data in real-time. Discuss two (2) static and two (2) dynamic tools used for mobile applications?

Static code analyzers scan code bases for security vulnerabilities to discover and prioritize the root cause of potential security problems for developers to fix quickly as part of the development cycle. Fortify is a static code analyzer by NDM that has plugins for popular IDEs for Java and Android development, as well as Swift and iOS. SonarQube is an open source static analyzer that finds issues with code quality and some security vulnerabilities in many languages and deployment types. Compared to Fortify, the security analysis is not as strong with the free edition but the support for more languages and use cases makes SonarQube a versatile analysis tool and is open source. Dynamic analyzers run code and monitor real time behaviors and vulnerabilities to potentially discover more vulnerabilities than static analyzers by enabling analysis at run time. ZAP is a dynamic analysis tool used for mobile and web security and performance analysis by analyzing traffic in between as a proxy or “manipulator in the middle”. ZAP can be used as a penetration testing software to passively scan pages and capabilities and then attack the discovered features and parameters. The Android Debugging tools that come with the Android SDK like ADB Android Debugging Bridge, allows Android developers to interact with devices and emulators to inspect and monitor resources for debug and security analysis. Whereas ZAP can be templated and used in an automated way, ADB is typically a manual tool used to investigate apps running locally.

With respect to cost & implementation, is there any differences between them?

Commercial products can be expensive, but like for like (such as using open source) it is more expensive to set up a dynamic analyzer that needs an environment to run the application and the analysis tool in. A static analyzer can run as part of CI/CD by analyzing the artifacts and files of a project, that take fewer resources to run on. It also takes more effort to set up and use a dynamic tool as the APIs and other functionality need to be live, the environment needs to be set up for the application, and the necessary time and resources need to be dedicated to testing the running application and services.

Discuss any cloud solutions which exist for performing this type of analysis?

There are static code analysis tools to integrate with CI/CD available like Fortify’s cloud solution. Since static analyzers require some resources/environment to run and analyze a code base, executing the analysis in a cloud instance is easily deployable, especially coupled with version control and automated builds. Dynamic tools can also be run in the cloud with some initial setup, and by offloading to cloud instances, teams can save local resources to run test suites. Solutions like Veracode offer SaaS implementations of black box testing for teams to start up dynamic testing more easily for mobile development.

4 OWASP Mobile Vulnerabilities

Go to the following link; https://owasp.org/Top10/ You will see a list titled Top 10:2021 List on the left hand side of webpage. Then review the ICS-CERT FY 2016 Annual Assessment Report Sections 2.1 & 3.2 found here; https://www.cisa.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf as well as review pgs 7-15 and Figure 11 & Figure 12 on pg 13 & pg 14 respectively in the attached Dragos pdf. (found in assignment section of CANVAS).
How do the ICS vulnerabilities differ from typical IT/enterprise web based application vulnerabilities? Pick two (2) mobile 2021 vulnerabilities (i.e., A01 through A10) that you feel are the most significant and explain why they are and how they can be guarded against?

ICT/OT attacks are considered more disruptive and have the potential to cause physical destruction and have critical real world consequences when they fail or experience downtime. Compared to traditional IT that focuses on data at rest and in transit, ICS systems make real time changes and have physical inputs and controlled physical actions as output. ICS systems are also different technically than traditional systems in that they support critical, sometimes proprietary or not traditional, devices and infrastructure that operate in a variety of physical environments. ICS systems also prioritize passive asset and threat detection, and have low bandwidth sites. These systems prioritize availability and safety over the traditional CIA triad.

Of the 10 mobile 2021 vulnerabilities, I feel that A02 Cryptographic Failures and A07 Identification and Authentication Failures are the two most significant vulnerabilities. With insecure encryption, data can be exposed at rest or in transit, which can lead to compromised credentials and the ability to access sensitive data such as using outdated TLS which leaves data vulnerable to man in the middle attacks. Similarly, weak authentication methods can allow unauthorized access to user data or can allow an attacker to compromise multiple accounts. These problems can be guarded against with proper implementation of secure methods. For insecure encryption, stronger and up to date encryption methods like larger AES or newer TLS methods should be used as well as avoiding common mistakes like hardcoding keys or using expired or compromised certificates. Authentication can be strengthened with the addition of multi factor authentication or using strong authentication protocols like up to date OAuth.

Read "Top 10 Mobile Risks- Final List 2016 found here; https://owasp.org/www-project-mobile-top-10/2016-risks/ Which mobile OS are attacks more successful against: Android or iOS, and why?

Both Android and iOS have vulnerabilities and can be compromised by the same poor design decisions. The article notes iOS has some additional default security, depending on the devices, such as encrypted code, and secure storage of biometrics. However both Android and iOS are subject to users modifying their devices to achieve root or at least some system level access through jailbreaks which can be used to circumvent protections and obfuscation methods to compromise app and device security like data storage, code tampering, reverse engineering, and other functionality that could further compromise encryption and authentication as well as communication with endpoints. Overall, the fragmentation of Android versions, which determine how up to date the security is, and the wide variety of devices and less controlled default security makes Android more vulnerable than iOS.

5 Application Program Interfaces (API's)

A foundational element of innovation in today’s app-driven world is the API. APIs are a critical part of modern mobile, SaaS and web applications and can be found in customer-facing, partner-facing and internal applications. By nature, APIs expose application logic and sensitive data becoming targets for attackers. Click on Blue API to drill down further. API list can be found here; https://owasp.org/www-project-api-security/
Pick two (2) items from the "API Security Top 10 2019" list that you feel are the most significant and explain why they are and how they can be guarded against?

In the 2023 updated version of the OWASP API Security breakdown, API1:2023 - Broken Object Level Authorization and API2:2023 - Broken Authentication are both very significant API security problems that are commonly exposed in the wild. In Broken Object Level Authorization, endpoints that expose object identifiers and handling serving them can create a wide attack surface, since the implementation needs to be considered with the use of data source and identification methods in every function. Guarding against this type of attack surface involves careful consideration of the methods being used as well as strict access control policies to prevent the unintended access to sensitive data in the object store. The authorization mechanism should check if the user has access to every action when a function calls the API with user input. The design of the application should also involve testing for vulnerabilities in the access control/authorization mechanisms. Even large companies are vulnerable to API compromise, for example in 2019 Facebook had millions of users' records compromised due to improperly secured API access. A vulnerability generated an access token for a target user by improperly implementing a feature meant to show what a profile looked like to other users.

This leads into the next significant security problem with Broken Authentication, where authentication and access control are implemented incorrectly. This can allow attacks to compromise access tokens or the resources through exploiting vulnerabilities in the authorization implementation which can give unintended access to user data. Safeguarding authorization control involves analyzing all possible authorization flows including password resets and consider brute forcing limitations like rate limiting and locking out failed attempts. And authentication, tokens, and storing passwords should be done with strong standards including not using API keys as authentication. If possible, multi factor authentication should be used as well as requiring continuous authentication and reauthenticating for sensitive data or making changes like the account email or 2fa.

6 Protecting Work Information System & Data

Many organizations provide standard image laptops, require secured VPN connections using HID tokens, run VDI & RDP software from a trusted device, and allow BYOD's. Pretend you're the CIO of a fortune 500 company. Describe to me in 3 to 4 paragraphs your method/plan on how you would implement a BYOD policy. Have your plan focus on protecting the security of the company's assets, systems, and sensitive/proprietary data, and PII/PHI of the employees for when BYOD's are used at work and off-site/home. BYOD's are considered any mobile device. Have your plan cover work situations/environments for outbreaks/pandemics (i.e., COVID-19).

If I were the CIO of a Fortune 500 company in charge of a BYOD policy, especially during a time where offsite work is likely such as during a pandemic, the plan would need to provide strong security for employee devices to protect company assets. This could be accomplished with good policies and software enforcement, training and compliance, and strong security for corporate networks and endpoints.

Employee devices should only access company networks via a secured VPN and use strong authentication which should involve multi factor authentication. And devices should be locked down with device management software in addition to having employees follow strict device policies for how their devices should be kept and used. Device software can enforce encryption, provide remote wiping, and blacklist certain applications. Enforcing policies like keeping software up to date, and segmenting corporate apps and functions by the use of management software can prevent common vectors for compromising company assets.

Employees should be in compliance with device policies through regular training, which can help prevent phishing attacks, unauthorized use of other resources like cloud storage for storing sensitive data, and keep legal and regulatory requirements for handling sensitive data at the forefront. Policies should be regularly evaluated for these types of compliance like HIPAA and GDPR, and the network and systems should be monitored continuously through the use of intrusion prevention systems to detect anomalies and prevent attacks like lateral movement from a compromised employee device.

Protecting the corporate network can be further enhanced with a ZTA security model where strong authentication is coupled with strict access control, segmentation to further prevent unauthorized access, and continuous monitoring to help ensure protection for sensitive data and assets even if an employee BYOD device is compromised.

Sources

https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/

https://www.trellix.com/security-awareness/ransomware/what-is-ransomware/#:~:text=How%20does%20ransomware%20work%3F,stored%20on%20the%20attacker's%20server

https://us.norton.com/blog/mobile/bluesnarfing

https://www.techslang.com/definition/what-is-bluesnarfing/https:/nordvpn.com/blog/bluejacking/

https://nordvpn.com/blog/bluejacking/

https://ndm.net/fortify/static-code-analyzer/

https://digitalvarys.com/install-and-configure-fortify-static-code-analysis-tool/

https://www.zaproxy.org/getting-started/

https://www.veracode.com/security/dast-test

https://owasp.org/Top10/

https://owasp.org/www-project-api-security/

https://www.pingidentity.com/en/resources/blog/post/facebook-data-breach-highlights-api-vulnerabilities.html

ICS-CERT FY 2016 Annual Assessment Report
https://www.cisa.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf

Survey_ICSOT-Cybersecurity_Dragos.pdf, The State of ICS/OT Cybersecurity in 2022 and Beyond Written by Dean Parsons October 2022

https://owasp.org/www-project-mobile-top-10/2016-risks/