Augmented Reality Security White Paper

by Tony Hodgson, CEO, Brainwaive LLC (Nov. 2017)

Augmented Reality (AR) headsets and smartglasses are tightly linked to the environment in which they operate. They sense, process, store, and possibly expose a large range of important information related to business facilities, personnel locations, resources, and activities related to planning, operations, production, maintenance, and more. To a much greater degree than conventional mobile devices, AR headsets nearly constantly gather data while in use, in standby mode, and sometimes even when “shut down.” This data can include detailed contour maps of user surroundings and captured audio, video, locational and positional data. Some of this data can be accessed remotely without the user even being aware it is happening.

While in some regards, AR systems exhibit the strengths of some similar technology areas like industrial control systems, wireless / mobile computing, the Industrial Internet of Things (IIoT), and conventional Enterprise IT, a more-sober characterization recognizes that AR solutions also share many of the weaknesses of these other systems, essentially presenting the worse of all worlds from a risk perspective.

- What happens if an AR target is compromised or the data the user is seeing is not real or accurate?
- What are the implications if a bad actor intentionally corrupts AR interfaces or procedures?
- What damage could be done if the massive amount of geospatial, multimedia data gathered by AR headsets ends up in the wrong hands?

Augmented Reality headsets open up new, unique, and significant threat potential to enterprise assets. They represent doorways through which bad actors can surveille, infiltrate, and potentially commandeer and misdirect critical resources and functions. Security on enterprise AR projects is critical, and no pilot program should be scaled up to production without completing a methodical, comprehensive security design and review. Unfortunately, when it comes to Enterprise users wishing to reduce or eliminate potential security risks, most IT and mobility teams are not specialized in AR solutions, nor on how to establish critical confidence levels when initiating pilot projects, rolling out production deployments, and maintaining systems over time.

Integrated Security Approach

It is a common occurrence in many enterprises that information security solutions are designed, acquired and installed on a tactical basis, where needs and requirements are identified, specifications developed, and solutions sought to meet particular situations. Unfortunately, in this approach, there is no opportunity to address strategic dimensions, resulting in design inefficiencies, lack of compatibility or interoperability, and unnecessary management burdens.

AR cyber security require a suite of tools and approaches to be effective. Mobile Device Management platforms and Enterprise IT tools can help with some, but not all needs. Mobile device certification and practices must be reevaluated to accommodate new factors and threats introduced by AR solutions. Additionally, in order to be most effective, wearable AR applications will require access to data stored remotely or in the cloud, increasing the number and types of trust boundaries that must be protected beyond the device, itself. Voice, gesture, and biosensor interfaces, and team-sharing of AR headsets, will present complicated challenges for secure user authentication and device management.

Recently, an internationally-recognized industry organization named the **Augmented Reality for Enterprise Alliance (AREA)** commissioned the Brainwaive LLC team to complete the first-ever study of AR cyber security related to enterprise deployment of smartglasses and headsets. Drawing from adjacent technology areas where security processes are already established, including industrial control systems, wireless / mobile computing, the Industrial Internet of Things (IIoT), and conventional Enterprise IT, the AREA study team created a comprehensive **AR Security Framework and Test Protocol** for wearable headsets which filled gaps in existing standards and best practices. The report is available on a limited basis and to members of the AREA (www.thearea.org).

Security by Design

The implementation of security requirements in mobile and AR programs should mirror the same general methodology used in implementing other IT systems. Design should start at the beginning of the project and at a high level before working down into details and implementation. “Security by Design” is a methodology which puts security first. Requirements are defined early, and controls are built into products and services and their installations which eliminate ineffective and costly security retrofits. This approach significantly decreases the risk for vulnerabilities and subsequent unauthorized access or attack by malicious actors. Taking a comprehensive, preemptive approach for security is critical, especially when considering compliance and regulatory requirements, as well as the extensive technology supply chain for hardware, equipment and software. Establishing security requirements early will help inform selection of the most compatible AR devices and software options.

AR Security Framework Support

Engaging AR cyber security subject matter experts can help educate your organization regarding data security risks, define program and system requirements, assist with selection of hardware and software elements, validate integrated system effectiveness and security, and recommend best practices to strengthen your existing enterprise IT and mobility program landscape and portfolio.

In any event IT and Mobility teams should be interviewed to understand the organization's current security policies and measures already in place (e.g. firewalled systems, profiles & IT processes, best practices, root of trust, intrusion protection, etc.). Risk areas for adding new AR devices should be identified, and considerations regarding gaps and modifications provided to the IT environment & program. To the degree possible, every effort should be made to utilize existing standards and frameworks. Examples include:

- NIST Framework for Improving Critical Infrastructure Cybersecurity
- OWASP Mobile Security Project
- IEEE Cyber Security Initiative
- ISO/IEC Information Security Management Systems Standards
- Industrial Internet Security Framework
- AR for Enterprise Alliance (AREA) Security Framework and Test Protocol

The number-one reason enterprise IT managers nix new mobility and AR programs is because of cyber security concerns. Rather than allow security risks to stall or kill projects, follow an industry-specific protocol for identifying and addressing the topic head-on and comprehensively with project tools and guidance. Doing so will aid in communication about the project, demonstrate proactivity, cover key bases required for management and IT stage-gate approvals, speed development and deployment, and boost the business results of the program.

To learn more about how you can work with Brainwaive to address your AR security questions and needs, please contact us at +1 832.317.3703 or email thodgson@brainwaive.com.