AREA

Augmented Reality for Enterprise Alliance

Technical Report:

Wearable Enterprise AR Security - Security Framework and Test Protocol

TABLE OF CONTENTS

© 2014 - 2017 All Rights Reserved

© 2014 - 2017 All Rights Reserved

Introduction

In response to growing concerns regarding the cyber security risks of deploying wearable Augmented Reality (AR) solutions in enterprise environments, and given that prior to this project little thought leadership had been provided on this mission-critical topic, the *Augmented Reality for Enterprise Alliance (AREA)* commissioned this industry-first study to evaluate security matters related to wearable AR solutions. This 2017 study resulted in publication of two reports:

- ***Wearable Enterprise AR Security - Risks and Management*** (overview report)
- ***Wearable Enterprise AR Security - Security Framework and Test Protocol*** (this report)

The objective of this report is to help AREA members, and eventually the wider business community, characterize threats via a structured framework, assess major vulnerabilities against that framework, and identify key metrics for measuring real-world risks.

Adoption of AR solutions for industrial systems, enterprise assets, and critical infrastructure requires security to be evaluated from the project onset. This report serves as an initial foundation for formulating sensible mitigation strategies to protect these corporate assets. It provides AR device manufacturers, application and platform developers, system designers, integrators, and enterprise end users (device owners/operators) with a step-by-step guide for evaluating security requirements and design choices in their projects. These design elements and best practices allow stakeholders to make informed decisions critical for project success.

The scope of this first-of-its-kind study is confined to evaluating security aspects of wearable AR headset devices as edge elements in a larger “technology stack” comprising full-featured AR systems. This study does not cover security of other enabling technologies, processes, and services in the stack, such as Internet of Things (IoT), network gateways, local/wide-area networking, cloud services, enterprise applications, or data analytics. This methodology also does not evaluate other essential aspects of a comprehensive security strategy such as setting security policies, procedures over time, training, utilization competence, or maturity models, which are topics for future investigation.

The primary goals of this document are to:

1. Propose a security framework for AR developers and enterprise practitioners; and,
2. Create a three-phase test protocol for evaluation of AR headset solutions:
    - Identify appropriate security requirements for the AR device in an enterprise project.
    - Evaluate the security design of the AR device using vendor and third-party data.
    - Test the AR device security as part of the enterprise project.

© 2014 - 2017 All Rights Reserved

Terminology

Common Attack Pattern Enumeration and Classification (CAPEC™) - A publicly available catalog of common cyber attack patterns and classification schema administered by the MITRE Corporation and sponsored by US-CERT in the office of Cybersecurity and Communications at the US Department of Homeland Security.

Common Vulnerabilities and Exposures (CVE) - A publicly available catalog of information security vulnerabilities and exposures administered by the MITRE Corporation at the National Cybersecurity Federally Funded Research and Development Center, sponsored by the National Cyber Security Division of the US Department of Homeland Security.

Cyber Security Equivalence Model - An approach for establishing an effective security standard for an emerging technology or practice for which existing standards are undeveloped or insufficient. Achieved by modeling existing standards in parallel technology fields and then correlating those standards to an attack potential score to achieve an equivalent level of security. For example, modeling existing mobile technology standards for application in augmented reality device applications.

Industrial Internet Reference Architecture (IIRA) - A standards-based architectural template and methodology developed by members of the Industrial Internet Consortium (IIC) enabling Industrial Internet of Things (IIoT) system architects to design interoperable systems based on a common industry framework and concepts.

International Electrotechnical Commission (IEC) - An internationally-recognized, non-profit organization that publishes standards for all electrical, electronic, and related technologies.

International Organization for Standardization (ISO) - An independent, non-governmental organization with a membership of 163 national standards bodies.

Root-of-Trust - Computer systems are built with multiple layers of abstraction, from the hardware, up through various levels of firmware, to the OS and application layers. Generally, higher layers trust lower layers. The base source of trust is called the Root-of-Trust (RoT). RoT components are dedicated cryptographic processors on the headset/mobile device providing real-time drive encryption, detection and reporting of unauthorized changes to the OS and programs, and other security and memory management functions.

Security Framework - A series of documented processes that are used to define policies and procedures around the implementation and ongoing management of information security controls in an enterprise environment (Courtesy Wikipedia).

© 2014 - 2017 All Rights Reserved

STRIDE IoT - STRIDE is a threat modeling classification scheme developed by Microsoft which is an acronym for “Spoofing”, “Tampering”, “Repudiation”, “Information disclosure”, “Denial of service”, and “Elevation of privilege,” the six categories according to which all system threats can be classified, and subsequently mitigated. STRIDE IoT is an extended model for IoT applications.

Test Protocol - Formal outline of requirements, activities, resources, documentation, and schedules to be completed in the process of testing (devices).

Trust Boundary - A theoretical boundary of a computer system within which all subsystems can be trusted from a data integrity standpoint, and through which, program data or software application execution changes its level of trust with other elements of the system.

Vector Transition - A situational construct for exploiting network-connected AR devices by capturing data from the AR device and using it to attack a non-connected system or physical structure. Examples include password eavesdropping on an air-gapped system, alarm system PIN capture, token capture, and user behavior tracking.

© 2014 - 2017 All Rights Reserved

List of Acronyms

AREA	The Augmented Reality for Enterprise Alliance
AWE	Augmented World Expo
CVE	Common Vulnerabilities and Exposure
ICS	Industrial Control Systems
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical Electronics Engineers
IIC	Industrial Internet Consortium
IIoT	Industrial Internet of Things
IIRA	Industrial Internet Reference Architecture
IISF	Industrial Internet Security Framework
IoT	Internet of Things
ISO	International Standardization Organization
IT	Information Technologies
NIST	National Institute of Standards and Technology
OT	Operation Technologies
OWASP	Open Web Application Security Project
SDO	Standards developing organization
UI / UX	User Interface / User Experience

© 2014 - 2017 All Rights Reserved

SECTION 1 - AR SECURITY FRAMEWORK

Introduction

To address growing cyber security concerns related to the introduction of wearable AR solutions in enterprise environments, the AREA study team derived this *Security Framework and Test Protocol* by following the progression of steps described in the companion AREA Technical Report: ***Wearable Enterprise AR Cyber Security - Risks and Management***. That report explains how the study team determined that AR devices possess certain unique characteristics which prevent the direct adoption and enforcement of any existing cyber security framework such as those applying to the Industrial Internet of Things (IIoT), Industrial Control Systems, Enterprise Mobility and IT arenas. Simple cloning of any of those standards increases the possibility that individual controls will be unachievable or detrimental to the goals of those implementing the new AR technologies.

Therefore, addressing AR-specific cyber security attributes requires a translation of those prior standards to create a *Cyber Security Equivalence Model*, adopting elements where possible, discarding others where appropriate, and combining yet others with a newly-designed *AREA AR Security Framework*, synthesized here to address AR-specific gaps between those prior standards.

The following security standards and frameworks were referenced as follows:

- The NIST Cybersecurity Framework is used to inform an overall security program for AR.
- The OWASP top 10 threats for mobile and IoT are evaluated against AR.
- The Industrial Internet Security Framework provided the security building blocks to evaluate AR devices.
- The ISO/IEC 62443 standards are used to provide guidance on design choices required to achieve various security levels.
- The IEEE Standards on Cybersecurity, the Penetration Testing and Execution Standard (PTES), and various other standards are referenced, where applicable to provide additional supportive guidance.

The AREA study team will emphasize a scheme developed specifically to characterize and manage the unique threats and constraints associated with enterprise AR. Details of prior frameworks upon which the AR Security Framework is based are available from other sources.

© 2014 - 2017 All Rights Reserved

FIGURE 1-1: Elements of the Cyber Security Equivalence Model.

Managing Risk

The rollout of wearable AR solutions to enterprise employees will drive greater worker productivity but also require that AR developers build sophisticated, agile, and flexible systems suitable for modern IT environments. For wearable AR solutions to flourish within the context of the larger IT environments, developing a culture of trust and security is imperative. AR security concerns range from device theft and user authentication, to data loss, data encryption, and password hacks among others. Enterprises need to develop an end-to-end security model, trust requirements, and operational policies across AR devices, applications, networks, and data to effectively manage risks and mitigate current and emerging security threats.

Security Programs for AR

A minimum assessment of cyber security should be applied when considering the addition of any connected device to a system architecture for processing, transmitting, or storing data. When adding AR devices, that minimum assessment should be consistent with existing security doctrine, where possible. The National Institute of Standards and Technology (NIST) publications under NIST 800 provide a strong baseline which can be employed for establishing security programs for AR devices. The following guidelines should be applied when assessing AR device security:

- NIST SP 800: Computer Security
- NIST SP 1800: NIST Cybersecurity Practice Guides

© 2014 - 2017 All Rights Reserved

- NIST SP 800-164 (Draft): Draft Guidelines on Hardware-Rooted Security in Mobile Devices
- NIST SP 800-123 Rev. 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise
- NIST SP 800-115: Technical Guide to Information Security Testing and Assessment

To provide a structured model for describing the evolution of the security process, it is also advisable to establish a maturity model with policies targeting both the Augmented Reality solution and the enterprise. Just one of many informative examples is the Cybersecurity Capability Maturity Model (C2M2), published Feb 2014 by the U.S. Department of Energy and the U.S. Department of Homeland Security - https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

Risk Assessments

A risk assessment is a process used to measure security problems and the weighted extent of their effects. The common approach is to create a table or list of threats, then assess their likelihood and potential impact. Information Technology (IT) risk assessments are data focused, while Operational Technology (OT) risk assessments evaluate both digital data and the potential risk of attacks against device integrity resulting in physical world impacts. While IT-centric risk assessments can be used for AR, AR headsets are also a conduit for physical activities in different industry-specific applications, so must be evaluated from both perspectives.

This report provides steps through which a team or individual can identify and assess various general threats associated with enterprise AR devices. In practice, each instance of an industry-specific AR solution implemented in an Enterprise IT environment presents different risks, and must be uniquely reviewed. Also, from a security and safety perspective, a human utilizing an AR device can be seen as an “actuator” that is fed data, then performs directed activities based on that information. Thus the human can generate various risk potentials for cyber physical attacks. Because AR solutions exhibit a mix of IoT and mobile technology attributes, it makes them more challenging to assess with respect to security impact, and these may also be entangled with safety effects. If an impact affects human lives or the environment, it should be correctly distinguished, labeled, and addressed as a safety consideration.

Enterprise programs should engage security specialists as early as possible from inside or outside the organization, or both, to methodically identify and assess risks and mitigation measures associated with AR pilots and production projects, and establish minimum security requirements.

© 2014 - 2017 All Rights Reserved

Phased Framework Methodology

After evaluating the existing standards (described above) for applicability and gaps related to the generic solution architecture derived from the Use Case review (described below), the AREA study team synthesized a three-phase approach for a new AR Security Framework. The Framework is provided to help users select and deploy a headset that provides the proper security level given specific use case requirements, deployment environments, and the functional roles of the user. It evaluates the prudent security requirements for AR devices by defining trust boundaries, reviewing the role of the user, identifying deployment patterns and network connectivity, and assessing the potential for automating threat modeling.

The three key phases of the *AREA AR Security Framework* include the following:

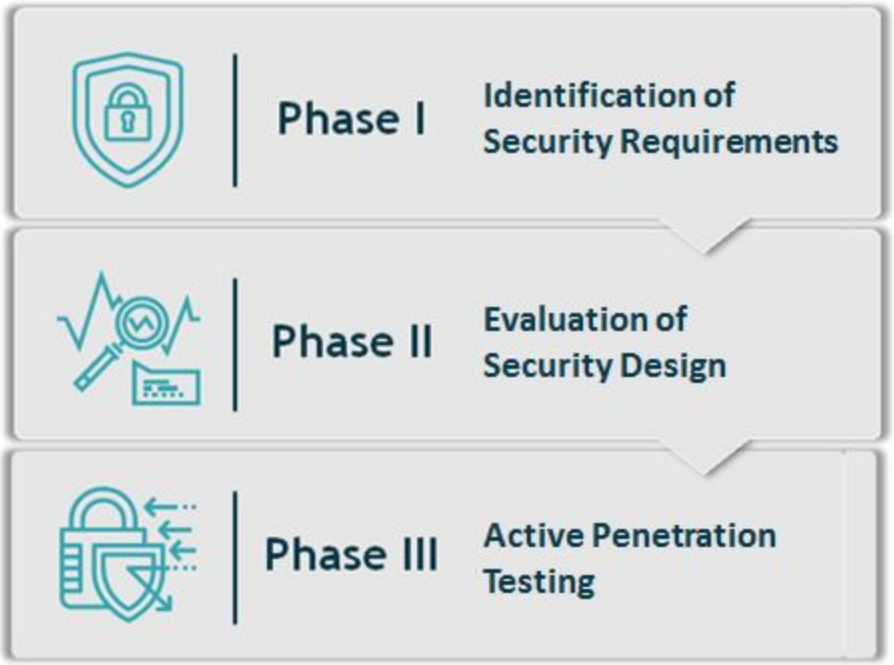


FIGURE 1-2: Three Phases of the AREA AR Security Framework.

© 2014 - 2017 All Rights Reserved

Goals and methodologies used to conduct each Framework phase are listed, below.

TABLE 1-1: Phase Goals and Methodologies.

Phase	Description	Phase Goals	Methods
I	Identification of security requirements	Document use cases Document design architecture Perform risk analyses Create threat assessment Identify security levels	Research use cases Model use cases Identify trust boundaries Document threats
II	Evaluation of security design	Select candidate AR headset Document headset security specifications Evaluate security design Identify vulnerabilities Identify mitigation tactics	Review headset documentation Document device specifications Generate a CVE report (see https://cve.mitre.org/about/) Conduct a vulnerability scan
III	Active penetration testing	Conduct functional testing Report on known attacks to enterprise team lead Identify unreported threat vectors	Complete pre-test assessment Scope threats Conduct vulnerability analyses Engage active exploitation

Elaboration of each of the three phases of the security framework are provided below.

Phase I - Identification of Security Requirements

Consider that every Industrial IoT project engenders different protection requirements, depending on vertical market, device functionality, environmental conditions, user roles, and user activities undertaken. Simply using a boilerplate security solution will not provide sufficient understanding of, or protection against, critical threats. As a type of IoT solution, AR represents a new type of computing platform, so security requirements not supported by current policies or in-house solutions should be carefully identified. The procedures used to identify security requirements for an AR headset include:

A. Document the relevant security uses cases for the enterprise end-to-end solution.

B. Create a detailed architecture of the project utilizing the *Industrial Internet Reference Architecture* (Such as division between edge, platform, and enterprise architecture; see

© 2014 - 2017 All Rights Reserved

Figure 1-3, below).

C. Identify the trust boundaries (a.k.a, trust zones), which are a grouping of logical or physical assets that share common security requirements based on factors such as criticality and consequence. This step is part of most automated threat modeling tools, such as STRIDE IoT, and is required by security standards like IEC 62443.

D. Describe the connectivity between zones, also known as conduits. At the end of this step, definitions will have been identified for all AR entities in each trust zone, a set of threats to the trust zone, and conduits to/from that trust zone. It is strongly suggested that, because AR devices are not yet well understood, it would be helpful to evaluate all AR device types appearing in one or more trust zones, without mixing them with other device types.

E. Define the role of the user, which explains how the subject device will interact with the environment, and hence, defines how device misuse can affect safety and kinetic threats (a class of cyber attacks that can cause direct or indirect physical damage, injury or death).

F. Utilize the use cases to evaluate the threats, security requirements for the AR zone, and conduits.

G. Methodically perform a threat assessment, using OWASP, IoT STRIDE, IEC 62443 or other models with the help of the guidance tables provided in this framework.

Document Use Cases

Three popular enterprise AR use cases were evaluated in the companion AREA technical report - *Wearable Enterprise AR Security - Risks and Management*:

1. Augmented Maintenance and Repair Operations.
2. Augmented Warehouse/Warehouse Picking.
3. Assembling a New Product.

Differences and commonalities between technical functional requirements of these use cases were noted.

© 2014 - 2017 All Rights Reserved

Document Design Architecture

A single, generic solution architecture to use as a model for threat analysis was derived from the three use cases. Architectural tiers are separated by borders, illustrated in red, while trust boundaries are identified around each significant element of the technical stack.

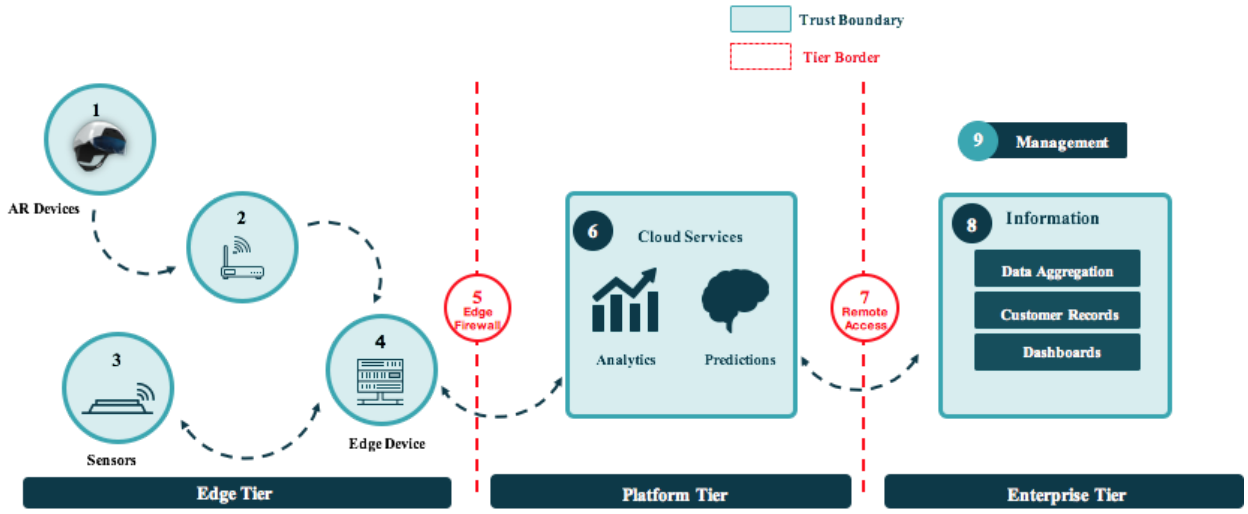


FIGURE 1-3: Generic AR architecture model.

Threat Assessment for AR Devices

For stakeholders to begin effective conversations regarding cyber threats to AR device solutions, it is useful to understand a few key terms and distinctions:

Threat	The expressed potential for occurrence of a harmful event such as an attack.
Attack	An action taken against a target with the intention of doing harm.
Vulnerability	A weakness that makes targets susceptible to an attack.

When assessing the overall security posture of an AR device within the enterprise, it is important to establish these distinctions in order to communicate clearly with stakeholders, evaluators, and testers. An instance of an AR device may have certain *threat* vectors that stem from its communication protocols, storage capabilities or operating system. *Vulnerabilities* may be weaknesses in those features that can be exploited for an attack. When establishing a security profile of a device, threats are normally static, based on the implementation, and vulnerabilities are dynamic, based on the protection mechanism established. *Attacks* may be categorized to provide penetration testers with a target scope of interest for their evaluation.

© 2014 - 2017 All Rights Reserved

Today, AR devices inherit protection from the OS, connected host system, and MDM platforms - which is insufficient.

As discovered in the AREA study team's device research, most AR devices today inherit protection mechanisms from either the operating system platform, the connected host systems, or a mobile device management (MDM) system - which are individually and collectively insufficient. For example in the case of reliance on host operating systems primarily derived from mobile OS platforms (Android® and Windows® 10), protections share the strengths and weaknesses of those systems. The vast majority of Android platforms exist in the mobile cell phone space and security mechanisms are largely handled by ecosystem-wide updates pushed down by the cellular provider. Enterprises with AR devices not directly connected to an external provider are forced to implement a separate patch management program. This gap provides a potential attack vector as vulnerabilities are discovered in the mobile platform space. Evaluating each component of the integrated AR system will help to discretely identify such vulnerabilities.

To identify system components and interrelations, the ISO/IEC are currently working on a Mixed and Augmented Reality (MAR) Reference Model. Expanding on that ISO MAR model, the *Electric Power Research Institute (EPRI)* recently published a report on Enterprise AR Vision, Interoperability Requirements, and Standards proposing an *AR Interoperability Framework.* The Interoperability Framework is divided into three-layers of Information and Communications Technology (ICT) components required for presenting AR experiences to a user (see Figure 1-4, below). The top layer shows those components closest to the physical world used for context capture and experience presentation. The middle layer illustrates middleware components necessary for AR presentation from the native device operating system to the local and remote resources shared with other mobile systems and applications, depicted on the bottom layer. Each component in the *AR Interoperability Framework* can give rise to threat vectors from which the system must be protected.

© 2014 - 2017 All Rights Reserved

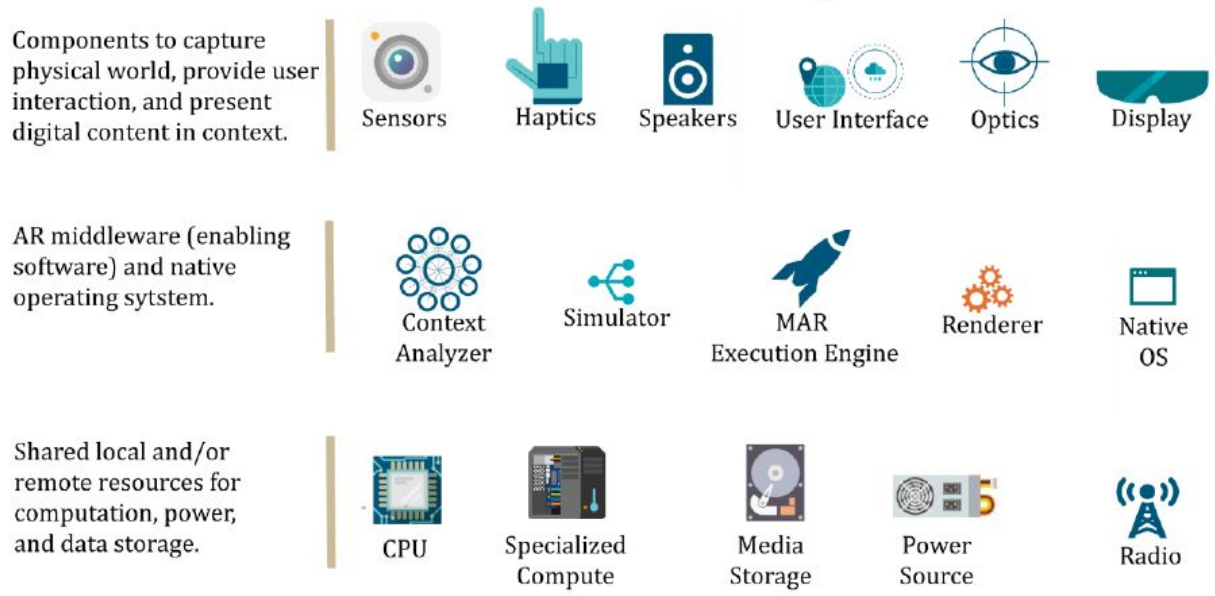


FIGURE 1-4: Component layers of the Augmented Reality Interoperability Framework. Courtesy EPRI and Perey Research and Consulting.

Taking a functional viewpoint on many of the same ICT elements shown above, the *ISO MAR Reference Model* offers the element schematic, shown in Figure 1-5, below. That viewpoint illustrates both the components and required connectivity to offline data sources, all of which expose potential attack vectors in the communication, authentication, authorization, and verification space. The connected nature and offloaded security mechanisms provide opportunity for interception, manipulation, and perturbation of data to/from the AR device.

© 2014 - 2017 All Rights Reserved

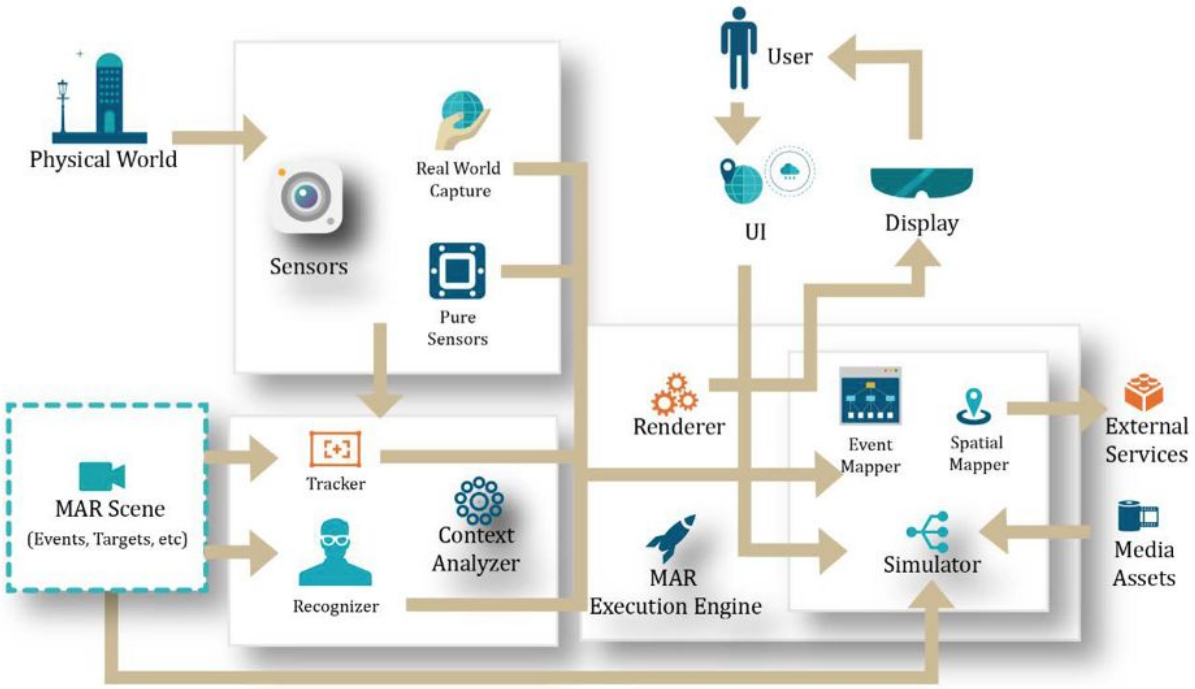


FIGURE 1-5: Component viewpoint of ISO Mixed and Augmented Reality Reference Model. Courtesy EPRI and Perey Research and Consulting.

To reiterate, when evaluating risks to the enterprise from introducing AR devices, one cannot simply inherit requirements directly from existing mobile and IoT frameworks. AR devices engender new and novel threats and impact risks. AR system threat boundaries cross into multiple product domains and share commonalities with a wide variety of devices. The majority of platform-based threats are inherited from common operating system threats, referenced above, and application threats in the enterprise will typically be customized software requiring traditional code analysis to determine data resiliency. Additionally, AR devices introduce bridges between cyber threats and kinetic factors similar to characteristics of devices in the IoT domain.

Mobile and IoT cyber security frameworks are insufficient for evaluating risks to the enterprise from introducing AR devices.

© 2014 - 2017 All Rights Reserved

AR-Unique Threat Vectors

The new threat vectors for AR devices in the domain are spread across systems and components in the ecosystem. These attack types highlighted below are derived from *MITRE CAPEC* attack categories but focus on the unique challenges introduced by AR devices. Figure 1-6 and following Table 1-2 highlight these novel attacks, their objective and where they exist in the overall system architecture.

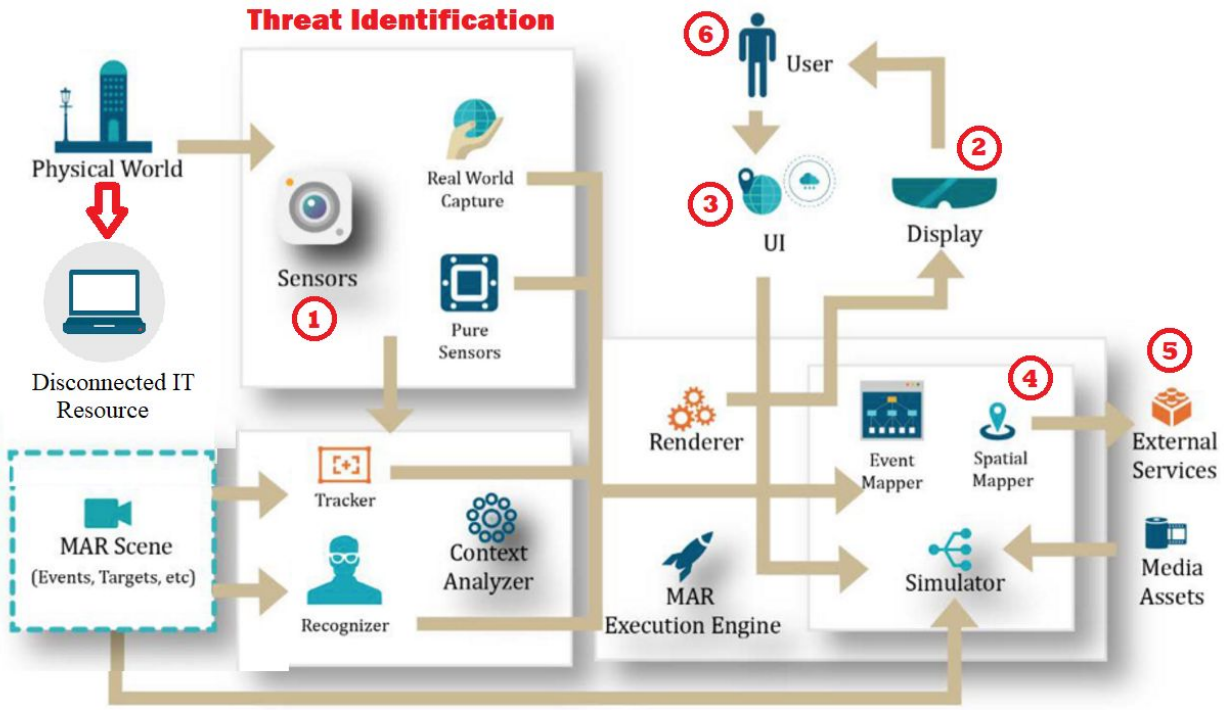


FIGURE 1-6: Threat vectors for AR systems.

© 2014 - 2017 All Rights Reserved

TABLE 1-2: AR-unique threat types.

	AR Threat Type	Target	Threat Objective
1	Data Extraction	Sensors	Obtain compromising information about air-gapped systems.
2	Environment Manipulation	Device	Inject false data into the environment to affect the user.
3	Object Manipulation	UI	Modify data elements in order to adversely affect real world objects.
4	Data Extraction	Spatial Mapping	Obtain compromising information about physical security mechanisms.
5	Trust Exploitation	External Services	Abuse trust relationship to host in order to attack connected networks.
6	Visual Manipulation	User	Inject visual/auditory data elements in order to confuse, injure or manipulate the user.

AR Threats from an Implementation Perspective

As with all information system elements, the implementation of an AR device into the enterprise and how it is managed may either increase or decrease the security posture of the device as well as the enterprise, itself. As one protection step then, it is important to assess device security requirements in the context of its operational environment. AR operational environments should be evaluated to ensure common best practices for securing information systems are established. This evaluation should include at a minimum:

- Business-wide information security policies and procedures.
- Enterprise network configuration management and control.
- An Information Security Risk Management and Assessment program.
- Standardized, compliant software configurations.
- Security training and awareness program.
- Incident Response Plans.
- Disaster Recovery Plans.
- Applicable Certification and Accreditation.

© 2014 - 2017 All Rights Reserved

In addition, those operational environments must be examined to ensure that no additional risk will occur from the implementation of devices in the environment. This could include risks from additional non-standard ports and services for spatial mapping, geolocation, application store availability, and digital rights management services. It should include impact evaluation to other, non-connected devices in the environment, such as company-proprietary tools or practices, that could be compromised from the collection of audio, video, or spatial mapping data. Lastly the environments should be evaluated for social engineering and user-based threat vectors including operator safety. In summary, an end-to-end evaluation of the AR device must be considered holistically within it's given implementation for an effective security assessment.

OWASP Top Threats Related to AR

To guide evaluation of system threats, the *Open Web Application Security Project (OWASP)* global not-for-profit organization provides developers and security teams with resources to build and maintain secure mobile applications, including classification of the top threats associated with various computing platforms. In the two tables below, the AREA study team evaluated the top IoT and Mobile platform threats, and compared them to application in an AR device scenario. Each risk was evaluated and designated either higher, lower, or the same as the related IoT and Mobile scenarios defined by OWASP.

For more information on the threats listed, please refer to Mobile OWASP and IoT OWASP projects.

Mobile OWASP Threats

The OWASP Mobile Security Project classifies the top mobile security risks as listed in Table 1-3. The relative threat level for AR device implementations is estimated.

TABLE 1-3: OWASP Mobile Risk Comparison to AR Scenarios.

Rank	Title	AR Risk	Notes
M1	Improper Platform Usage	Higher	AR devices are complex and security guidance today is non-existent.
M2	Insecure Data Storage	Higher	AR Enterprise devices should primarily offload data storage elements however, storage protection is limited by the technical constraints of the device.

© 2014 - 2017 All Rights Reserved

M3	Insecure Communication	Same	AR devices employ existing protocols sharing security risk levels.
M4	Insecure Authentication	Higher	AR devices primarily inherit authentication controls from host devices or networks, but user authentication methods may differ.
M5	Insufficient Cryptography	Same	AR devices will have similar challenges to mobile for cryptographic algorithms and encryption.
M6	Insecure Authorization	Same	Enterprise devices will be used by multiple personnel and require additional role-based or user-based authorization.
M7	Client Code Quality	Higher	The siloed nature of current AR solutions and the rush to create them will likely result in poor coding practices.
M8	Code Tampering	Higher	The tools utilized to create AR solutions can be modified by an attacker at the developer's desk.
M9	Reverse Engineering	Same	Code will share the same reverse engineering techniques with mobile platforms.
M10	Extraneous Functionality	Same	Backdoor and maintenance access functions will have similar implementation across AR devices.

© 2014 - 2017 All Rights Reserved

IoT OWASP

The OWASP IoT Security Project classifies the top IoT security risks as those listed in Table 1-4. The relative threat level for AR device implementations is estimated.

TABLE 1-4: OWASP IoT Risk Comparison to AR Scenarios.

Rank	Title	AR risk	Notes
I1	Insecure Web Interface	Lower	Web interfaces and API are likely to have enhanced security features.
I2	Insufficient Authentication / Authorization	Same	IoT and AR share the lack of common authentication / authorization methods.
I3	Insecure Network Services	Same	AR platforms use many network services for remote management and data sharing.
I4	Lack of Transport Encryption/Integrity Verification	Lower	AR devices do not have the computing constraints of IoT devices and will be able to use cryptographic libraries.
I5	Privacy Concerns	Higher	The amount and type of data collected by AR devices increase privacy concerns.
I6	Insecure Cloud Interface	Same	The siloed nature of AR devices opens the possibility of insecure cloud interfaces, similar to IoT devices.
I7	Insecure Mobile Interface	Same	The siloed nature also opens the possibility of insecure mobile interfaces, like IoT units.
I8	Insufficient Security Configurability	Higher	AR devices are complex devices, with new computation units, peripherals and sensors. We expect a lack of granularity to configure security of the components.

© 2014 - 2017 All Rights Reserved

I9	Insecure Software/Firmware	Same	The cost of the device will probably make firmware quality higher, however peripheral support may be difficult for new devices.
I10	Poor Physical Security	Same	AR devices do not feature increased physical security components.

Phase II - Evaluation of Security Design

The second phase of the *AREA AR Security Framework* involves analyzing an AR system from a security design perspective. After AR project teams select one or more candidate headsets to evaluate, they must document device security specifications provided by the vendor, evaluate security of the design attributes identified, and begin to evaluate appropriate risk mediation steps. A list of some key security design elements to consider is provided in Figure 1-7, below.

Today, AR device vendors offer little detail regarding security designs of their systems. This must change before widespread enterprise adoption will occur.

This AREA study team found that AR device vendors offered very little detail regarding security design elements of their systems, and in some cases, were reluctant to even have conversations about those items. That reluctance is unworkable and will have to change in order for vendors to deeply penetrate the enterprise markets they are trying to address. Device vendors and application developers should engage security specialists to help clients understand security elements of their systems using modern frameworks and protocols, validating headset suitability for the enterprise environment, and separating themselves from competitive offerings.

Two-way conversations about AR device cyber security design must begin.

As well, enterprise AR project managers should begin flowing down their security requirements to device vendors, and insisting that critical security design information become known and

© 2014 - 2017 All Rights Reserved

easily accessible from vendors. This data is vital for evaluating whether any given AR system will meet or exceed the corporation's internal cyber security requirements, and the design strengths and weaknesses of each wearable AR device.

The AREA study team advises AR project managers and asset owners to carefully evaluate the security design choices made by the wearable AR device manufacturer using the security framework and test protocol provided here.

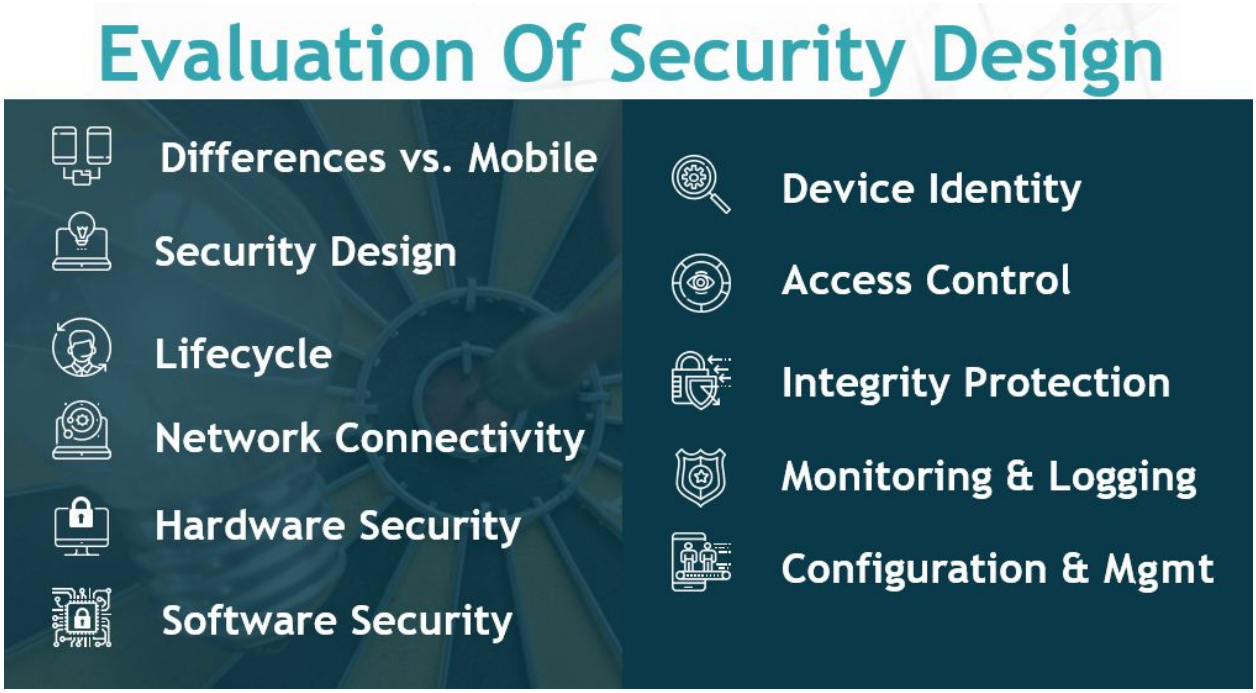


FIGURE 1-7: Key Elements of AR device security design.

Security Protection Levels

The International Electrotechnical Commission (IEC) is an internationally-recognized non-profit organization that publishes standards for electrical, electronic and related technologies. *IEC 62443-3-3, Security for industrial automation and control systems – System security requirements and security levels*, defines four security levels for rating cyber threat protection elements, providing guidance on how to evaluate the protection levels for different security functions.

© 2014 - 2017 All Rights Reserved

TABLE 1.5: IEC security protection levels.

IEC Security Protection Level	Description
SL1	Protection against casual violation
SL2	Protection against intentional violation using simple means
SL3	Protection against intentional violation using sophisticated means
SL4	Protection against intentional violation using sophisticated means with extended resources

The AREA study team utilized the cyber-equivalency philosophy presented earlier to describe a similar set of security levels for AR security design choices modeled after the IEC levels. The security levels are intended to guide decision making with security personnel familiar with enterprise and industrial security standards, and also bridge the gap with IT security assurance programs when integrating AR devices. AR security protection levels are presented, below, as applicable across various elements of the AR security framework.

Device Protection

Enterprise users piloting AR solutions today benefit from headset features and functions that are left wide-open from a security perspective by the manufacturer. Just out of the box, this allows users to test every possible use case and device configuration easily. Unfortunately, this openness will not support scaling to production deployments. In today's AR market scramble for functionality, hardware security features and software security testing are frequently left behind by device designers. Because there are no current turn-key security solutions to protect AR devices, the system integrator and asset owner inherits security problems, which sometimes cannot be resolved or require purchase of additional technology and software to mitigate security shortcomings. Dialogue should begin between designers and end users to generate feedback on security requirements which can be incorporated into subsequent headset designs.

Trust requirements flow down from the owner/operator to all parts of the system, but trust functionality and controls must be built from the bottom up.

© 2014 - 2017 All Rights Reserved

The trust lifecycle in an AR solution starts with the system owner/operator and their security specialists creating detailed trust specifications as part of overall operational requirements, which are then issued to AR device vendors. Device builders must further break down the specifications into trust requirements for each component, and certify compliance with those requirements as components are received from component suppliers. Certification of the entire integrated system is assured (preferably by an independent third-party) after production. Upon delivery, the owner/operator and third-party specialists validate that trust specifications have indeed been assured in an operational context. The figure below illustrates this bi-directional flow of specifications and certifications to achieve the desired level of trust.

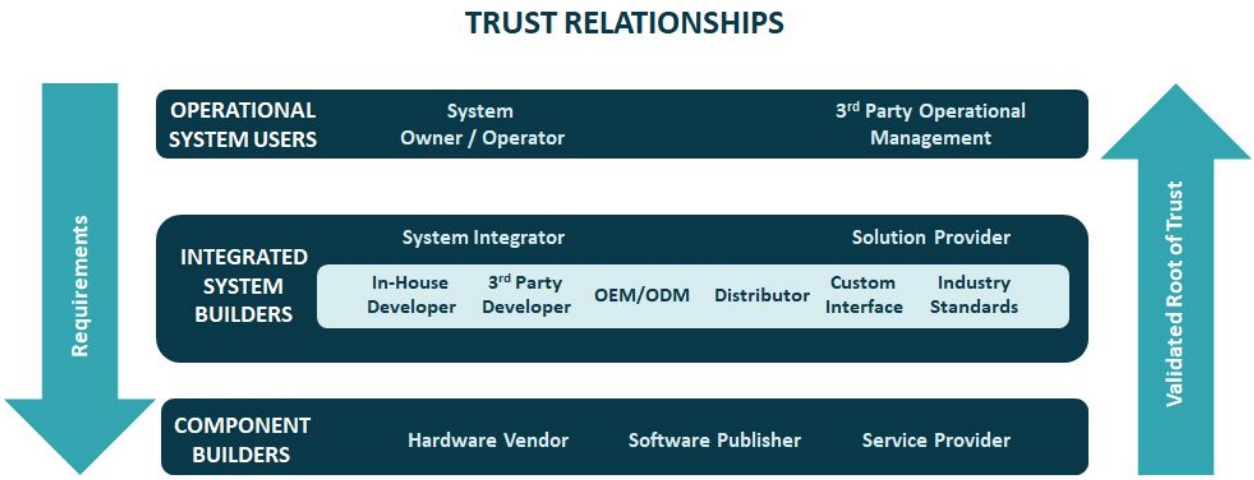


FIGURE 1-8: Integrated system layers and stakeholders. Courtesy Industrial Internet Security Working Group.

The multi-purpose architecture of AR devices allows for implementation of software security controls, in particular to enhance the security communication protocols. But hardening devices without security design in mind can only achieve limited levels of protection. For example, a root-of-trust element should exist, be integrated in the platform, and used correctly for data storage, integrity, and isolation. This enables necessary security functions such as secure identities or boot protection.

© 2014 - 2017 All Rights Reserved

In this document, two tools are provided to ensure the chosen security levels are achieved:

- Guidance regarding security features provided by the vendor using the IEC protection level information for each of the security building blocks (*AREA AR Security Framework*).
- A *Test Protocol* providing a coherent methodology for security evaluation of AR devices.

Security Building Blocks

In this framework, we build upon the security building blocks as described in the Industrial Internet Security Framework (IISF) by the Industrial Internet Consortium (IIC), aggregating the "I/O, Sensors and Other Peripherals Security". For detailed information and description of these building blocks, please refer to that IISF source document. Here, the AREA study team provides information on how the security design evaluation can be applied in these building blocks for AR.

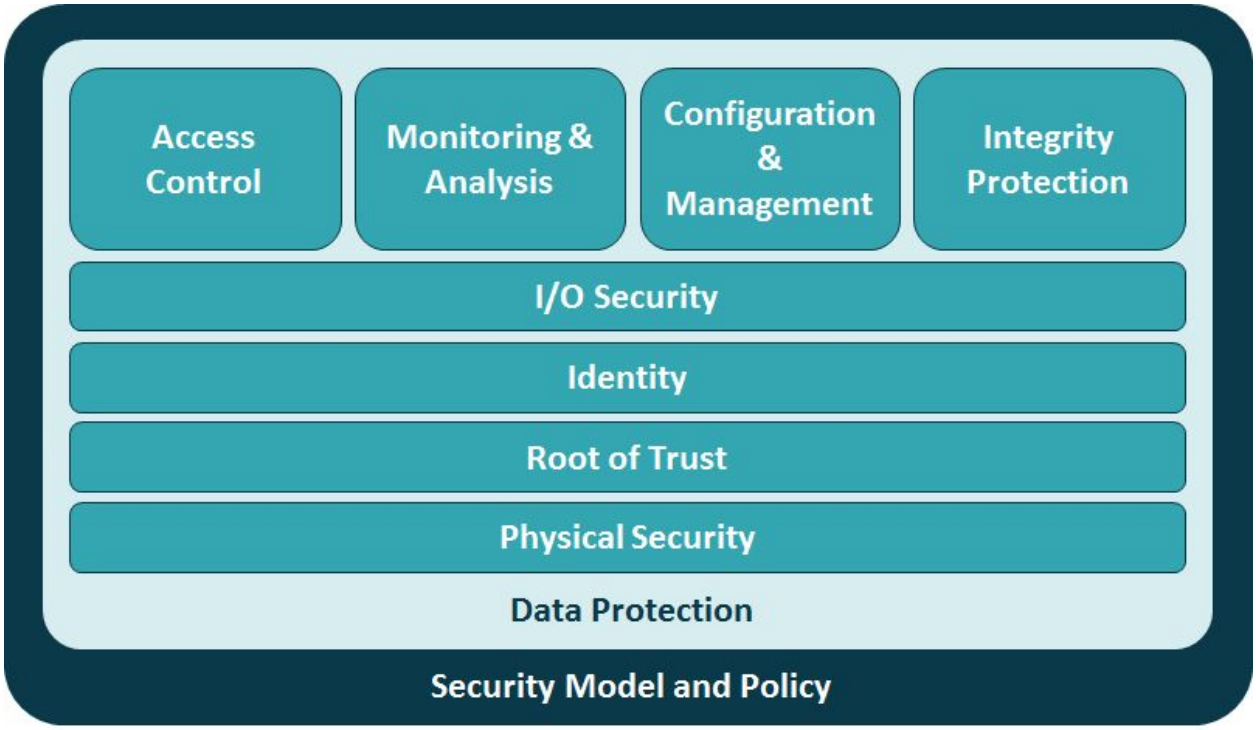


FIGURE 1-9: AR endpoint security framework.

© 2014 - 2017 All Rights Reserved

Security Model & Policy

The security model for deployment of AR devices at the edge of the technology architecture stack needs to recognize the differences between AR policy and existing mobile / IT / IoT policies. Collecting information on policy discrepancies enables the creation of a robust security policy, which includes mitigation tactics for both the new AR-unique and inherited attack vectors and threats.

The state of the art for device manufacturers, content providers, and system integrators currently is to model security policy of AR devices as mobile computing and communication products. As discussed previously, this model is flawed. AR devices are a new computing platform and the enterprise security policy should accommodate their unique features. AR devices share security considerations inherited from the mobile, IT, and IoT worlds. They are multi-purpose platforms collecting massive amounts of data in real time, featuring novel hardware and peripherals, groundbreaking user interfaces (gaze, gestures, voice), and immersive environments.

TABLE 1-6: AR-unique attributes and similarities with Mobile and IoT policies.

Distinguishing Attribute	Policy Consideration	Policy Similarities (Mobile,IoT)
Data collection from sensors	Data collected confidentiality and new attack vectors	IoT
User authentication with uncommon UI	Authentication with AR input (voice, gestures, etc) and usage of biometrics and tokens	IoT
Uncommon peripherals	Authentication of peripherals, authorization of input	Mobile
Lack of hardware root-of-trust	Support hardware root-of-trust operation, mitigation strategies if it doesn't exist	Mobile

© 2014 - 2017 All Rights Reserved

Safety and trust risks of digital immersion	Add user safety to policy and kinetic threats	Mobile
Intentionally open configuration	Hardening platform as an explicit step	IoT
Hardware and networking design vulnerabilities	Add evaluation of new hardware platform to policy	IoT
Software vulnerabilities	Add support to AR custom software	Mobile, IoT
Undefined upgrade & patching strategies	Add to policy a patch strategy that accounts for mobility and custom software	IoT
Remote connectivity	Add strategy and authentication for remote control	IoT
Remote monitoring and always-on sensors	Fine grained modularity in policy for sensor data collection and storage	IoT
Modified software development and deployment patterns	Include trust implication of utilizing siloed platforms for software development	Mobile
Connectivity Protocols inherited from previous platform	Mitigation techniques for usage of connectivity platforms with known flaws	IoT

© 2014 - 2017 All Rights Reserved

Data Protection

Gathering information about the user's context and presenting data within in the user's real world context are the primary functionalities of AR devices. Some of the many types of data and mechanisms include:

- Camera-based detection of gestures
- Camera-based eye tracking
- Ultrasound or radar-based gestures detection
- Voice recognition
- Audio sensing & transmission
- Video recording & transmission
- Photodiode sensor
- Proximity touch screen
- Motion sensor
- Wireless sensor
- Touch sensors
- Thermal sensors
- Accelerometer
- GPS
- Solid state compass

Data policy on AR devices should distinguish between system data collected by the device, external data fed to the device, and data created by the device.

Data collection on AR devices is pervasive. At a minimum, the enterprise needs to understand what data is collected by the device, the possible threats from data being captured or modified, and how data is stored. The device should allow local, automated, and remote wipe for lost and stolen devices. Data should be encrypted for confidentiality and integrity, and capabilities provided for SL3 and SL4 hardware based encryption with root keys stored in a hardware root-of-trust.

The following items are required for SL >0

- Document system data collected
- Local/Auto wipe
- Remote wipe

The following items are required for SL >1

- Segregation of system data and user data
- Encryption of sensitive data collected
- Purging sensor data

© 2014 - 2017 All Rights Reserved

The following items are required for SL >2

- Support hardware encryption
- Fine grained access control of sensor data

Physical Security

The AR device should have anti-tampering mechanisms to avoid uncontrolled changes or inspection of hardware. Also, physical security includes the control of exposed physical ports such as USB and media jacks. AR devices can be protected by perimeter defenses, but the risk analysis should take into account the mobile nature and size of AR devices.

The following items are required for SL >0

- Disable unused ports

The following items are required for SL >1

- Tamper evident enclosures

The following items are required for SL >2

- Tamper proof for critical elements (see root-of-trust)
- Protection of exposed ports

The following items are required for SL >3

- Detection of hardware modifications

Root-of-Trust

RoTs are security primitives composed of hardware, firmware and/or software that provide a set of trusted, security-critical functions. The root-of-trust on a device determines the level of confidence in the AR device. AR systems operate in complex computing environments, and critical security functions should be designed using a hardware root-of-trust. As unique new hardware platforms, it is important for the asset owner to choose AR platforms that effectively implement hardware root-of-trust to provide device integrity, protected storage, and execution isolation. The protection levels SL3 and SL4 require a hardware root-of-trust.

Please refer to NIST SP 800-164, *Guidelines on Hardware-Rooted Security in Mobile Devices*, for an extended discussion of root-of-trust.

© 2014 - 2017 All Rights Reserved

The following items are required for SL >2

- Creation of a unique identity for the device in protected storage.
- Allow creation of additional ownership keys.
- Collect measurements of initial boot process.
- Protected storage for data collected.
- Verification of software installation.
- Support of measurements for all software stack.
- Support process isolation.

The following items are required for SL >3

- Support in-board verification of measurement
- Support root-of-trust in critical sensors and peripherals

Identity

Identity is the basis for trust in asset management, authentication, authorization, and remote maintenance. AR devices should be able to create at least one unique device identity. The device should also support creation of multiple device support identities, and multiple owner identities. Identities have different security levels. Please refer to the document "Secure Identities" from Industrie 4.0 for an in-depth discussion on identities.

The following items are required for SL >0

- Support identities

The following items are required for SL >1

- Support unique identities
- Support cryptographic identities

The following items are required for SL >2

- Unique identification and authentication
- Hardware identity for device and process

© 2014 - 2017 All Rights Reserved

Access Control

Access control for data and processes includes authentication and authorization. AR devices pose challenges in user authentication due to the new paradigms of user interaction. Voice, gestures, and gaze provide significant challenges to confidentiality and usability for maintaining strong passwords. Biometrics are not yet integrated into most hardware headsets. Biometrics and tokens may ultimately resolve authentication problems, but it will be complicated to integrate them into a company-wide policy.

Remote authentication of AR devices should follow IT or mobile authentication guidelines, for example NIST Special Publication SP-800-63-2.

Authorization should provide granularity to control the different data sets in the device.

The following items are required for SL >0

- Identify and authenticate all human users
- Timed device lock for authentication

The following items are required for SL >1

- Support cryptographic protection of passwords

The following items are required for SL >2

- Usage of strong passwords
- Multi-factor remote authentication

The following items are required for SL >3

- Support multi-factor authentication for all users
- Granular authorization for all data

Integrity Protection

System protection on the AR device should include both protection from malware, and compartmentalization of processes at the lowest reasonable level. Devices should run applications and operating environments at standard user privilege levels with device protection and configuration run at root levels. Due to the use of standard operating systems in most AR devices, compatible malware detection and endpoint protection solutions should be used which also take into account both standard and AR-unique characteristics, if available.

© 2014 - 2017 All Rights Reserved

The following items are required for SL >0

- Basic malware detection
- Tiered user login at lowest reasonable level

The following items are required for SL >1

- Application compartmentalization
- Enhanced malware protection
- Code execution protections

The following items are required for SL >2

- Support for hardware compartmentalization techniques
- Support for white listening
- Boot integrity measurements

The following items are required for SL >3

- OS support for root-of-trust based integrity protections

I/O, Sensors and Other Peripherals Security

One distinguishing aspect of AR is the proprietary hardware required to interact with the device and collect data from the user's environment. Because the hardware, firmware, software drivers, and data collected may fall into unchartered territory in terms of security, it is important to exercise caution evaluating their protection profiles. It is important to list all peripherals, I/O, and sensors featured by the device. This list should also include related software, and a threat assessment to minimize the possibility of attacks on confidentiality, integrity, and availability.

The following items are required for SL >0

- Authentication of peripherals
- Encrypted communications for wireless peripherals

The following items are required for SL >1

- White list of peripherals
- Audit of peripherals

The following items are required for SL >3

- Authentication of sensitive internal sensors and I/O
- Root-of-Trust for peripherals

© 2014 - 2017 All Rights Reserved

Monitoring

AR devices need to provide integrity and audit information that includes significant system events. Depending on the requirements, this audit information should be protected cryptographically or utilize secure data storage mechanisms.

The following items are required for SL >1

- Integrity protection of audit information

The following items are required for SL >2

- Cryptographic protection of Audit Events
- Configuration of Audit Events
- Information for non-repudiation

Configuration & Management

AR devices inherit many security challenges typically associated with mobile devices, including logging, auditing, malware detection, and incident response requirements. In order to achieve consistent and comprehensive security across AR devices in the enterprise, both host-based protection and image management should be used. Once a secure configuration has been built in a test environment, that device image should be used across all devices.

The lifecycle policy of the device (commission, provision, normal usage, alert state, remediation state and decommission) should cover other building blocks, in particular, identity management.

© 2014 - 2017 All Rights Reserved

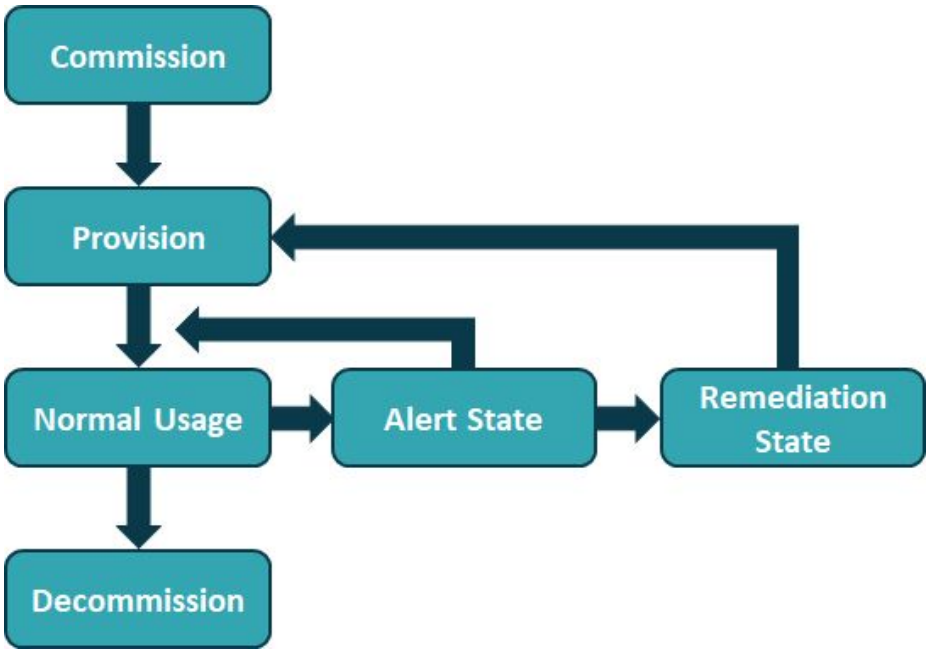


FIGURE 1-10: AR Device Lifecycle.

The following items are required for SL >1

- Remote management
- Cryptographic protection of OS and apps configuration

The following items are required for SL >2

- Management of identities
- Management of encryption keys

Software Security

From a software perspective, AR devices are quite similar to mobile devices like tablet computers. Most current AR devices feature multi-purpose OSs, such as Android, Windows, or Linux. Many of the software security functions can be provided by these OSs (access control, etc). The processing power of the devices allows them to run several processes, and functions such as software encryption and signing could easily be performed in software. The best way to secure these systems is to harden the OS utilizing best practices appropriate for the specific OS of the device.

© 2014 - 2017 All Rights Reserved

AR devices will be loaded with new software applications and drivers which may never have been thoroughly tested for security. The asset owner should require a complete manifest of all software included on their devices, references to known security vulnerabilities, and for higher protection levels, strict secure coding standards for all software. Owners should also utilize independent security evaluations of all new software.

A critical difference between AR devices and other mobile devices is the methods for user interaction. Common modes for interacting with an AR device are gestures, gaze, and voice, opening the software to new UI attack vectors. Many AR devices feature remote management consoles to allow setup, policies, debugging, monitoring, and other functions. These remote consoles need to be properly developed and secured to prevent remote vulnerabilities.

The following items are required for SL > 0

- Security patch management for firmware, OS and applications

The following items are required for SL >1

- Permissions enforcement
- CVE information for all software in the platform

The following items are required for SL >2

- Process compartmentalization
- Manifest of all software included in the device
- Secure coding standards

The following items are required for SL >3

- Independent software security evaluation

Connectivity

Connectivity of AR devices is usually similar to many mobile computing and IoT technologies, with protocols such as WIFI, Bluetooth, and NFC commonplace. The document *The Industrial Internet of Things Volume G5: Connectivity Framework* provides ample guidance on connectivity issues for the Industrial IoT, and a description of common issues implementing an IIoT connectivity stack.

AR connectivity protection profiles depend on a variety of factors, such as the existence of external gateways, firewalls, and deployment patterns. Hence, they are out of scope for this document but are critical for the enterprise to consider. At a minimum, the device

© 2014 - 2017 All Rights Reserved

owner/operator should understand all the network capabilities and threats associated with the AR devices, including all Open Systems Interconnection model (OSI) connectivity layers. Peripherals may use some of the connectivity capabilities with reduced authentication, opening further new attack vectors. For more information, please utilize guidance from the NIST documents described earlier.

Phase III - Penetration Testing

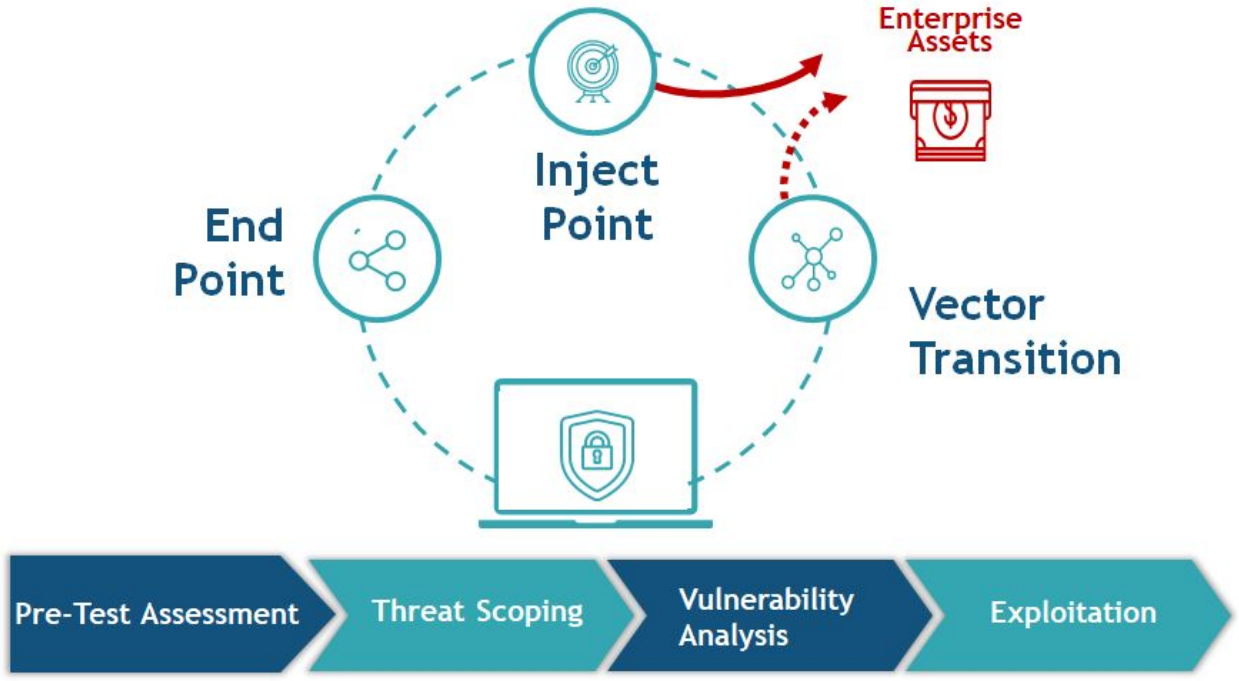


FIGURE 3-1: Penetration Testing Modes.

Penetration testing as a security discipline is tasked with exercising the vulnerabilities in a device as part of an attack chain that would simulate a real-world cyber attack. Rather than quantifying and qualifying the vulnerabilities of a device, penetration testing determines if those vulnerabilities are actionable as part of a non-theoretical exploit and measurable impact. The scope of penetration testing should always be systematic to determine the repeatability and assess the effectiveness of the vectors in an attack chain. In the case of AR devices, the scope of penetration testing should include three primary approaches:

© 2014 - 2017 All Rights Reserved

1) AR as the endpoint: The AR device is the objective of the attack in order to control its representation functionality.
2) AR as the inject point: The AR device is the external facing device due to an open interface and is used to access another system.
3) AR as a vector transition: The AR device is collecting data which is used to provide an attack vector on another system. For example, collecting spatial mapping data in order for bad actors to identify the location and orientation of facility security cameras.

Penetration Testing Methodology

The penetration testing methodology for AR devices should follow industry standard phases for systematic, repeatable data. The following standard is effective for traditional IT systems and has proven its application in the National Institute of Standards and Technology 800-115 and the Penetration Testing and Execution Standard (PTES). Also, recent standards such as the UL2900 cybersecurity assurance programs provide a guidance for a testable program to evaluate connected devices. Because AR devices exist as part of a larger infrastructure, it is recommended that users take these standards into account when assessing the device ecosystem.

AR devices maintain their own special considerations when creating a scope and respective target vector. The following shifts in methodology should be considered when approving a testing protocol for AR devices.

Pre-Test Assessment

The initial definition of test protocols, intelligence gathering, and test boundaries and objective identification should be identical to standard IT systems.

Threat Scoping

In a standard IT ecosystem penetration test, threat boundaries are normally reserved for the IT systems and any physical protection mechanisms that exist for those systems. AR devices, by their nature are cyber/kinetic bridge elements and must include penetration tests that allow for data gathered by the AR device to obtain objectives in physical space and air-gapped systems.

1) Vulnerability Analysis

The identification and enumeration of vulnerabilities within AR devices has a much greater degree of potential dependency on the “state” of the device. Based on the use cases provided, there is a high degree of probability that an enterprise AR device will have specific

© 2014 - 2017 All Rights Reserved

correlation to a defined environment. These defined environments may possess different configuration settings, sync requirements, and data access dependent on location, user, and application. Vulnerability analysis should identify these sub-states to determine consistency. The scoping of a vulnerability assessment should include:

a) Field Settings: Settings in which the device is used remotely from an enterprise infrastructure and relies on a third-party communication pipeline including cellular, WiMax, Bluetooth-to-Cell and remote sites. Other considerations include geo-fencing and tunnels to VPNs.

b) Enterprise Settings: Baseline settings for operation within a specific enterprise environment. This may include enterprise wireless and direct local connections.

c) Development Environment: Development settings may allow for much greater access to the AR device in a development environment. Although build practices typically provide heavy isolation between development and production code, devices and systems are not typically reconfigured between environments. This is irrelevant in traditional IT systems as they are typically non-mobile computing devices assigned to a user or confined to a lab. The mobility of AR devices increases the likelihood that they will transition between development, production, enterprise, and guest networks.

Unlike traditional mobile devices which are often subject to BYOD or data compartmentalization, there are likely to be considerable usage constraints associated with company-owned AR devices. While this would normally be equivalent to an increased cyber security posture, over-trusting that AR devices will remain onsite and only used by company personnel may cause a relaxation of device security protections otherwise commonly employed for mobile devices. See the next section on specific vulnerability areas for exploitation in AR devices.

2) Exploitation

Exploitation is an area of great agility and opportunity in the penetration test. The cyber/kinetic nature of AR devices allow for a great deal of potential for using the devices in novel ways to circumvent and defeat protection mechanisms. In addition, this area provides the greatest degree of potential complexity in a penetration test. Due to the kinetic impact factors (the device exists in a defined enterprise state and captures data, actively and passively about the environment in which it exists) full scope testing requires that the device be engaged in its typical operational environment. Testing in the operational environment(s) provides a much greater degree of fidelity in determining potential attack opportunities, vector transition options and impact effects.

Although it typically lies in the domain of the penetration tester to determine exploit methods within the attack chain, a developer or owner/operator of AR devices should be aware of the

© 2014 - 2017 All Rights Reserved

novel exploit potential that exist with AR devices. Using this AR Security Framework allows stakeholders to provide more specific direction to penetration test teams to focus and address the risk factors of these methods:

- Using spatial mapping to identify the behaviors of security personnel.
- Using spatial mapping to locate security devices, cameras, and alarms.
- Using spatial mapping to capture physical protection mechanisms.
- Using video capture to gather data on air-gapped systems.
- Using image capture to gather data on identification badges.
- Using video capture to gather authentication data (passwords, etc.) from the environment.
- Using cloud-based spatial anchors to spoof a legitimate interface to capture passwords.
- Using spatial mapping to locate target items or systems.

Factors Distinguishing AR Device Vulnerabilities

The largest distinguishing factor in the inclusion of AR devices is the potential vulnerabilities that the devices can introduce to the enterprise. Similar to the impact potential associated with Industrial Control Systems (ICS) devices, AR devices allow bridges to data in physical space. In the case of ICS devices, the manipulation of the ICS is the objective, and the IT infrastructure is the pathway to the objective. AR devices however, allow unique perception of the environmental space in which the device exists by virtue of its external sensing capabilities. Audio, Video, Spatial Mapping, Thermal, and Geographic Location features all collect data that can be used or captured for adverse purposes. These data sets could allow capture of data that would allow an attacker to circumvent a protection mechanism or allow the transition of attack from one vector to another. This change in the attack chain, or vector transition consists of exploiting a network connected to the AR device, capturing the data and using it to attack a non-connected system. Examples include password eavesdropping on an air-gapped system, alarm system PIN capture, token capture, or user behavior tracking.

In examining the security factors associated with AR devices in the enterprise it is important to identify the factors that differentiate the devices from traditional IT systems. Similarities in architecture, OS and communication protocol will allow for like attack vectors from a vulnerability perspective. AR devices have a very specific set of impacts that deal with the unique attributes that AR devices bring to the enterprise.

© 2014 - 2017 All Rights Reserved

AR devices by their inherent feature sets provide distinguishing impact characteristics in two areas:

1) As a collector of environmental data

2) As an injector of data to a user

The first differentiator is most significant as the AR devices inherently allow collection of visual, audio, network configuration, user behavior, and environmental behavior along with normal data consumption. These unique elements in the exploit chain allow for significant new methods and impacts as a result of a cyber attack. As the weakest point in any cyber defense is always the human element, these devices can significantly increase the ability to exploit human interface mechanisms and physical protection mechanisms.

Attack Categories for the AR Device

In determining and communicating threats and attack vectors it is advisable to provide a common nomenclature and identification schema. This will allow end-customers and penetration testing groups to address specific threat areas of interest derived from specific customer concerns normally described in narrative format. These attack categories can be used both to frame the scenario and synchronize elements of concern with specific threats, exploits and vulnerabilities.

Data Capture

Attack Objective	Target	Description
Footprinting	Device	Identification of the device network based on discovery analysis.
Interception	Network	Traffic intercepted from the wearable to a linked device.
Protocol Analysis	Network	Potential cryptanalysis of encrypted traffic.
Excavation	Device	Legitimate functional data (spatial mapping, video, etc.) extracted from the target device.

© 2014 - 2017 All Rights Reserved

Data Injection

Attack Objective	Target	Description
Code Injection	Device	Injection of malicious code directly to the device through existing protocols.
Object Injection	User	Injection of digital objects in viewing space in order to hide, distract from or clone legitimate digital objects.
Environment Interference	User	Injection of digital objects in viewing space in order to overwhelm, confuse or blind a user to real objects in the environment.
Object Manipulation	User	Manipulation of legitimate digital objects in order to convey invalid information or induce improper user action.
Environment Manipulation	User	Manipulation of digital objects in order to confuse the user regarding the real environmental state.
Traffic Injection	Device	Injection of non-specific traffic in order to overwhelm or induce specific state in the device.
Command Injection	Device	Injection of commands through existing protocols to achieve malicious effects.

Subversive Interactions

Attack Objective	Target	Description
Resource Spoofing	User	Presentation of an illegitimate host or data source as legitimate.
Social Engineering	User	Injection of digital objects within the Augmented Space in order to induce a behavior by the user (i.e., password submission, protected data disclosure, etc.).

© 2014 - 2017 All Rights Reserved

Functionality Misuse

Attack Objective	Target	Description
Functionality Abuse	Device	Abuse of legitimate AR device tools (password recovery mechanisms, etc.).
API Manipulation	Device	Exploitation of open device APIs to introduce additional threat vectors or achieve local device control.

Access Control Subversion

Attack Objective	Target	Description
Authentication Bypass	Device	Direct attack on device authentication mechanisms.
Authentication Elevation	Device	Transition attack from valid user level login to privileged or root level login.
Physical Security Bypass	Device	Bypass physical locking, biometrics or location based security mechanisms.
Device Trust Abuse	Network	Exploit of legitimate trusted device to attack host network.
Device Credential Abuse	Network	Spoofing of legitimate device credentials to attack host network on another device.

Probabilistic Methods

Attack Objective	Target	Description
Encryption Brute Force	Device	Attack against existing encryption protocol to reveal plaintext, IV or ciphertext values.
Authentication Brute Force	Device	Dictionary-type attack against password controls and other authentication mechanisms.
Fuzzing	Device	Random data injection to identify system weaknesses.

© 2014 - 2017 All Rights Reserved

SECTION 2 - TEST PROTOCOL

This AREA AR Security Test Protocol is intended to be a preliminary step-by-step guide to apply the Security Framework in evaluating the protection profile of an AR device.

Actors

The testing protocol includes a PROJECT, a TEAM, a PRODUCT, and a VENDOR.

PROJECT	Refers to an enterprise deployment of hardware and software that includes an AR product.
TEAM	Refers to the workforce in charge of managing and delivering the project, including its security functions.
PRODUCT	Refers to AR device(s), in the form of a headset, that needs to be evaluated for security as part of the project.
VENDOR	Refers to the manufacturer or third party providing the final version of the PRODUCT to the TEAM.

Phase I: Identification of Security Requirements

The goal of phase I is to profile the security requirements for the PRODUCT.

Documentation and Threat analysis

1. The TEAM shall provide
    a. A set of use cases relevant to the deployment.
2. The TEAM shall provide a high level architecture of the project, containing:
    a. Representative elements, if possible divided as Edge, Platform, Enterprise tier.
    b. Trust boundaries for each tier.
    c. Connectivity protocols (conduits) between trust boundaries.
    d. Role of the user.
3. The TEAM shall perform a threat evaluation
    a. Once c) and d) are finished, perform an initial threat model using STRIDE IoT, OWASP or others

© 2014 - 2017 All Rights Reserved

Risk Analysis

The AR device(s) (PRODUCT) to be evaluated will fall in one or more of the trust zones. The team should provide information on the AR trust zones.

1. The TEAM shall provide a security risk analysis for the Trust boundary containing the PRODUCT, including:
    a. Number of devices associated for trust boundary.
    b. Role of the user.
    c. Restrictions in terms of safety and privacy for implementing security.
    d. A list of threats for the trust zone.
    e. An assessment of impact of each threat.
    f. The likelihood of each threat.
    g. Using the previous steps, determine the risk associated.
    h. Select the relevant threats to the PRODUCT trust boundary from a risk acceptance criteria.
    i. Identify controls required in the PRODUCT to mitigate the threats.
    j. Identify protection levels for security controls.
    k. Evaluation of common threats utilizing automated threat analysis tools.

Phase II: Evaluation of Security Design

TEAM shall collect from VENDOR, and VENDOR shall provide, documentation describing security design choices for the PRODUCT. The documentation shall include:

1. AR specific items that may affect security policy
    a. Data collection from sensors.
    b. User authentication with uncommon UI.
    c. Uncommon peripherals.
    d. Lack of hardware root-of-trust.
    e. Safety and trust risks of digital immersion.
    f. Intentionally open configuration.
    g. Hardware and networking design vulnerabilities.
    h. Software loading and vulnerabilities.
    i. Undefined upgrade & patching strategies.
    j. Remote connectivity.

© 2014 - 2017 All Rights Reserved

k. Remote monitoring and always-on sensors.
l. Modified software development and deployment patterns.
m. Connectivity Protocols inherited from previous platform.

2. Data Protection
    a. Existence of hardware encryption.
    b. System policy for sensors data.
    c. System policy for software.

3. Description of physical security
    a. Tamper resistant, tamper evidence, and other capabilities.

4. Information on root-of-trust, if any
    a. Describe support for integrity, storage, and identity security functions.
    b. If non-conventional or proprietary, describe.

5. Description of device identity and device identity management
    a. Unique identities, crypto identities, and hardware identities.
    b. Creation of identities in secure hardware.

6. List access control for device and applications
    a. User authentication.
    b. Remote authentication.

7. Describe integrity protections
    a. Boot integrity, such as authenticated boot.
    b. Run time integrity (Malware detection).

8. Describe I/O sensors and other peripherals
    a. Peripheral communication.
    b. If sensor, describe data collected type (user, surroundings).
    c. Authentication methods for peripherals.

9. Describe Monitoring data
    a. System data logs.
    b. Data audit configuration mechanisms.
    c. Audit data protection mechanisms.

© 2014 - 2017 All Rights Reserved

10. Describe Configuration and Management methods of the device
    a. Remote consoles.
    b. System updates.
    c. Application updates.
    d. Security patches.
11. Describe Software Security
    a. Software deployment methods.
    b. Application development tools.
    c. Manifest with all software, including firmware, and OS, including the device and versions.
    d. Known vulnerabilities of software provided in CVE format.
12. Describe device connectivity protocols
    a. Connectivity information.
    b. Modification of protocol if proprietary.

Security Design Assessment

Utilizing the previous documentation, TEAM shall create new AR policies for trust zones and assign a security protection level (SL) to each building block. If security level does not meet expectations, describe mitigation techniques, and iterate until risk is avoided, transferred or accepted.

1. Describe remediation policies for AR
2. Assign protection levels to every security building block
3. Add risk mitigation techniques
4. Describe risk management choices
    a. Risk transferal.
    b. Risk acceptance.
    c. Residual risk.

© 2014 - 2017 All Rights Reserved

Device Security Lifecycle

The TEAM shall evaluate the changing security posture of the device and lifecycle information using maturity models or other security programs. The lifecycle configuration of the device should be properly documented.

1. Description of commission information
    a. Hardware identities.
    b. Hardware and software inventory.
    c. Relationship with vendors.
    d. Data exchanged by system.
2. Descriptions of provision information
    a. Software provision.
    b. Secure identities.
3. Alert and Remediation states
    a. Description of alert and remediation states.
    b. Interruption of normal boot state.
    c. Logging of alert states.
    d. Access to data in alert and remediation states.
4. Decommission
    a. Decommission procedures.

Phase III: AR Device Penetration Testing

A vital component in the determination of cyber security protection levels is the validation associated with external penetration testing. By definition this assessment should be performed by an external entity in order to provide an objective test. Whether the testing criteria is black hat (no existing knowledge of the system/architecture) or white hat (potentially extensive insider knowledge), these consulting organizations typically provide their own assessment framework. By familiarizing themselves with the previously provided guidelines in this report on penetration testing, AR program stakeholders can become familiar with some of the common nomenclature and scoping aspects of the AR penetration test, and be better prepared to interact with the third-party testing organization.

© 2014 - 2017 All Rights Reserved

Appendix A - References

Common Attack Pattern Enumeration and Classification (CAPEC™). Cyber attack classification schema created by MITRE Corporation.

Institute of Electrical and Electronic Engineers (IEEE) Standards on Cybersecurity. Portfolio of standards curated by the IEEE.

Industrial Internet Connectivity Framework. Framework created by the Industrial Internet Consortium. Feb 2017.

Industrial Internet Reference Architecture. Framework created by the Industrial Internet Consortium. Jan 2017.

Industrial Internet Security Framework. Published by the Industrial Internet Consortium. Sept 2016.

ISA/IEC 62443-3-3, Security for industrial automation and control systems – System security requirements and security levels. Generally identical (and identically numbered) standards published by both the ISA and IEC defining procedures for implementing electronically secure Industrial Automation and Control Systems. Aug 2013.

NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment. Special publication by the National Institute of Standards and Technology. Sept 2008.

Penetration Testing and Execution Standard (PTES). Online resource published by pentest-standard.org. Last updated Aug 2014.

Program on Technology Innovation: Enterprise Augmented Reality Vision, Interoperability Requirements, and Standards Landscape. Publication by the Electric Power Research Institute (EPRI) and Perey Research and Consulting. May 2017.

STRIDE IoT. Threat modeling methodology created by Microsoft.

Technical Overview: Secure Identities. Publication by Plattform Industrie 4.0.

UL 2900 Standards Process - Cybersecurity for Network-Connectable Products. Published by United Laboratories. 2017.

© 2014 - 2017 All Rights Reserved

Appendix B – Brainwaive Cyber Security Team

Brainwaive LLC was commissioned by the AREA to conduct this research into the topic of Wearable Enterprise AR Security. The Brainwaive team assessed the existing market landscape regarding AR security, and through application of experience gained developing and using related global cyber security frameworks and standards (IIoT, Enterprise Mobility, Enterprise IT), created the *AREA Security Framework and Test Protocol* provided in these reports.

The Brainwaive team is available to answer questions and guide practical implementation of these models.

Brainwaive digital immersion

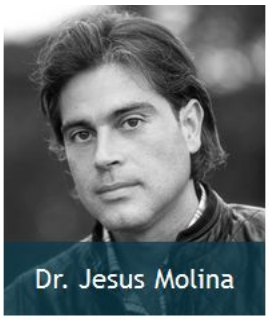
- 100 years of experience
- Leadership in global standards
- Hundreds of projects
- Government and industry network

Tony Hodgson

Project Management
Systems Engineering
AR / VR / Wearables
Mobility / Wireless
Enterprise IT Networks
Tech Commercialization

Robert LaBelle

Fmr Senior Director, Strategic Innovation and Standards for IEEE
Global Tech Standards
AR / VR / Wearables
Security & Privacy Issues



Dr. Jesus Molina

Ph.D Electrical Engineering
Cyber Security Patents
Co-Author Industrial Internet Security Framework
Co-Chair IIoT Security Standards WG

Frank Cohee

Cyber-Warfare Ops, Navy Army DARPA CIA NRO
AR / VR / Wearables
IIoT Cyber Security
Risk Frameworks
Threat Categorization

Brainwaive Contact

Tony Hodgson, CEO thodgson@brainwaive.com 832.317.3703

© 2014 - 2017 All Rights Reserved