AREA

Augmented Reality for Enterprise Alliance

Technical Report:

Wearable Enterprise AR Security - Risks and Management

ACKNOWLEDGEMENTS

The following organization, under contract to the Augmented Reality for Enterprise Alliance (AREA), prepared this report:

Brainwaive LLC
Huntsville, AL

Principal Investigators:

T Hodgson
R LaBelle
J Molina
F Cohee

This report describes research sponsored by the AREA, whose members and affiliate organizations include:

3Dstudio Blomberg
Aertec Solutions
AFC Hackathon
AMRC
Appearition
Atheer
Augmate
Boeing
Bosch
Brainxchange
Contextere
DAQRI
EPRI
Flatirons
Georgia Tech
Huawei
iQagent
JoinPad
Lockheed Martin
Newport News Shipbuilding
NVIDIA
Optech4D
PEREY Research & Consulting
PTC
RA Pro
RealWear
ScopeAR
UpSkill
VanGogh Imaging
Vision Star
Vital Enterprises
XMReality

ABSTRACT

There is a high level of concern and uncertainty regarding risks to data security when introducing mobile, wearable, AR systems into the enterprise. Enterprise managers want to reduce or eliminate potential security risks. AR vendors and system integrators want to ensure their devices, applications, and integrated solutions do not introduce dangerous threats to clients, or create new legal liabilities.

Because prior to this project very little thought leadership had been generated on the topic, the AREA sponsored this research of data security as it relates to wearable enterprise AR solutions. The objective is to help AREA members, and eventually the wider business community, better understand data security risks, communicate using a common vocabulary, characterize threats via a structured framework, assess major vulnerabilities against that framework, and identify key metrics to measure risks in the real-world.

The investigative team at Brainwaive LLC conducted comprehensive research, led multiple industry stakeholder interviews, and conducted hands-on evaluation of several market-leading headsets to develop and validate a comprehensive approach for assessing data vulnerabilities and formulating risk mitigation plans. Results of that work are provided in this AREA Technical Report, **"*Wearable Enterprise AR - Risks and Management.*"**

The companion AREA Technical Report, **"*Wearable Enterprise AR - Security Framework and Test Protocol,*"** builds on the first report, and draws on decades of experience by Brainwaive team members in developing global cyber security standards to generate a new ***AREA AR Security Framework***. The new *Framework* supplements key elements of existing standards with original work to cover security gaps introduced by emerging wearable AR solutions. A comprehensive ***Test Protocol*** is provided for enterprise users and supporting stakeholders to methodically evaluate their cyber security posture against the *Framework*.

By understanding and discussing the topics presented, and using the guidelines provided, enterprise stakeholders, AR solution vendors, and system integration partners can begin to deal with complex and important data security issues earlier in their project planning, speed venture funding and deployments, and improve the business impacts of their programs.

Keywords

Augmented Reality
Cyber Security
Data Security
Enterprise
Threat Analysis
Wearables

EXECUTIVE SUMMARY

TECHNICAL REPORT: Wearable Enterprise AR Data - Security Risks and Management

Primary Audience

- Enterprise business and technology teams tasked with implementing AR solutions.
- AR device vendors interested in hardening their solutions against cyber security threats.
- AR application developers deploying on head-worn platforms and smart glasses.
- AR system integrators designing and supporting AR systems for enterprise clients.

Overview

There is a high level of concern and uncertainty regarding risks to data security when introducing mobile, wearable, AR systems into the enterprise. Enterprise managers want to reduce or eliminate potential security risks. AR vendors and system integrators want to ensure their devices, applications, and integrated solutions do not introduce dangerous threats to clients, or create new legal liabilities.

Because prior to this project very little thought leadership had been generated on the topic, the AREA sponsored this research of data security as it relates to wearable enterprise AR solutions. The objective is to help AREA members, and eventually the wider business community, better understand data security risks, communicate using a common vocabulary, characterize threats via a structured framework, assess major vulnerabilities against that framework, and identify key metrics to measure risks in the real-world.

Research Methodology

From prior research conducted in 2016, and extensive literature studies and industry interviews that were part of this study, it was observed that no comprehensive, practical cyber security framework existed for AR solutions in the enterprise. Accordingly, the Brainwaive LLC study team combined their professional experience developing and exploiting related frameworks for Industrial Internet of Things (IIoT), Enterprise Mobile devices including smartphones and tablets, and Enterprise IT solutions to create a new *AREA AR Security Framework*. The Framework builds on best practices of those prior constructs, and adds new elements filling gaps presented by this unique AR digital medium.

Wearable enterprise AR solutions involve a suite of technical elements working in concert with headsets or smart glasses. These technical architecture elements (the AR solution stack) may include wireless networking capabilities, local and remote computing resources, cloud-based data analytics, reporting applications, integration with Enterprise IT and mobile device management resources, and more. For purposes of this report, the primary study focus was maintained on the head-worn device, itself. Follow-on studies should expand the cyber security review across all components of the AR solution stack to provide a comprehensive analysis.

While detailed testing and reporting on specific AR devices was out of scope for this study, the Brainwaive team did perform hands-on evaluation of multiple AR headsets of varying form-factors in a variety of application modes and environments to discern cyber-attributes of AR headsets, generally. Important observations from this first-hand testing permitted refinement and validation of the AREA Security Framework.

By evaluating several enterprise use cases, a framework for characterizing the cyber security posture of AR devices was derived and documented. A common vocabulary is suggested throughout for various system elements and concepts to enable stakeholders to communicate more effectively. An assessment of the vulnerabilities within that characterized environment is then provided. Key metrics are identified to measure vulnerability attributes in terms of real world impact potential.

Key Findings

- 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.
- Implementing AR cyber security will require a suite of tools and approaches to be effective. Assuming conventional Mobile Device Management / Mobile Application Management (MDM/MAM) tools or mobile security approaches can be easily extended to wearable AR solutions is both inaccurate and dangerous. MDM/MAM suites can help with some, but not all, aspects of securing AR headsets. Enterprise Mobility device certification and practices must be reevaluated to accommodate new factors and threats introduced by AR solutions.
- There is a tendency for stakeholders to “pass the buck” when it comes to taking responsibility for AR security: device vendors say it is the responsibility of the customer and can probably be handled by MDM applications; MDM providers have not seen enough deployments to extend their platforms to meet AR-specific needs, which would not be sufficient in any case; AR project teams look to Enterprise IT for guidance; Enterprise IT and Mobility departments hesitate to open up their networks to these

unconventional solutions without defined security criteria and processes for certifying and managing them.

- AR devices are tightly linked to the environment in which they operate, and 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 powered down. This data can include detailed spatial 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.
- Depending upon the application, in order to be most effective, wearable AR applications will often 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 can present complicated challenges for secure user authentication, especially when devices are shared among users.
- It is essential that the AR community, device vendors, and enterprise stakeholders work together to understand and protect against the new cyber threats enabled by wearable AR headsets and smart glasses. AR security specialists should augment existing Enterprise Mobility and security teams to create a comprehensive, methodical approach for identifying and mitigating risks to enterprise assets and operations.

Why This Matters

- Through this study and the two resulting AREA Technical Reports: ***Wearable Enterprise AR Data Security - Risks and Management***, and ***Wearable Enterprise AR Data Security - Security Framework and Test Protocol***, AREA Members are receiving new insights and expert guidance regarding how to define and communicate security requirements, evaluate AR solutions for vulnerabilities, and begin to measure important real-world security attributes.
- AR device vendors, AR application developers, and AR system integrators can evaluate and harden security aspects of their designs prior to market introduction. They can proactively generate comprehensive statements and specifications regarding the cyber security posture of their solutions prior to clients asking for them, distinguishing themselves from their competition.

- Enterprise AR teams can characterize their AR environments and intended applications from a security perspective to help understand and make informed decisions regarding which AR headsets to deploy and how.
- Enterprise IT and Mobility teams can use the framework and protocol to evolve device certification and management processes.
- Everyone can breathe a bit easier knowing formerly misunderstood and rogue AR projects can now be planned in a more organized fashion to meet security requirements of the organization.

How to Apply Results

By understanding and discussing the topics presented, and using the guidelines provided, enterprise stakeholders, AR solution vendors, and system integration partners can begin to deal with complex and important data security issues earlier in their project planning, speeding funding and deployments, and improving the business impact of their programs.

The *AREA AR Security Framework* can be used as a guideline by organizations to assess their existing AR cyber security program, or to build one from scratch. Plans and goals can be set and prioritized to maintain and improve the company's cyber security posture. The framework can also be used by enterprise executives to better understand their company's AR security practices and how they measure up to framework best practices, including understanding where vulnerabilities lie in order to properly address them.

AREA Contact

Mark Sage, Executive Director Mark@thearea.org

TABLE OF CONTENTS

Terminology

Cyber Security Equivalence Concept - 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 to achieve an equivalent level of security. For example, modeling existing mobile technology standards for application in Augmented Reality device applications.

Defense in Depth - A layered approach strategy that uses people, technology and procedures to protect an enterprise's network system.

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)

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

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. Examples include password eavesdropping on an air-gapped system, alarm system PIN capture, token capture or user behavior tracking.

Acronyms

EMM	Enterprise Mobility Management
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical Electronics Engineers
IIC	Industrial Internet Consortium
IIOT	Industrial Internet of Things
IISF	Industrial Internet Security Framework
MAM	Mobile Application Management
MDM	Mobile Device Management
NIST	National Institute of Standards and Technology
SDO	Standards developing organization
UI	User Interface
UX	User Experience

SECTION 1 - BACKGROUND AND OVERVIEW

There is a high level of concern and uncertainty regarding risks to enterprise data security when introducing and using mobile, wearable, enterprise AR systems. Enterprise users want to reduce or eliminate the potential risks. AR vendors want to ensure their devices and applications do not introduce dangerous threats to their clients. Because prior to this project very little thought leadership and guidance has been generated on such a mission-critical topic, the AREA sponsored this research of data security as it relates to wearable AR solutions.

The objective of this research is to help AREA members, and eventually the wider business community, to better understand data security risks, communicate using a common vocabulary, characterize threats via a structured framework, assess major vulnerabilities against that framework, and identify key metrics to measure real-world risks. This report can then serve as an initial foundation for formulating sensible mitigation strategies to protect corporate assets.

Problem Statement

The benefits of Enterprise AR are quickly becoming recognized and proven globally through proof-of-concept trials and real-world pilot programs. For example, AR in the enterprise:

- provides vital information to designers, architects, engineers, and field personnel.
- employs high-quality graphics, pictures and two-way video to remote experts.
- engages an array of sensors to capture worker context (e.g., location, orientation), and activities throughout workplaces.
- allows access to remote data to support work tasks, maintenance and operations.

FIGURE 1-1: Benefits of Augmented Reality across market verticals.

However, these same valuable attributes can open doors to nightmare scenarios. Besides the vulnerability of the user and data on the device, itself, wearable AR systems open new threat doorways to the enterprise, creating risks to company intellectual property, personnel safety and privacy, operational resources and activities, and overall financial performance.

AR functionality opens doors to security threats.

Recent ransomware threats bring to mind just a few of many possible nightmare scenarios. For example, will ransomware soon be directed towards enterprise assets through AR headsets?

FIGURE 1-2: Nightmare scenarios.

In aircraft production facilities, what are the threats when the integrity of manufacturing data can be hijacked? What havoc might ensue if misinformation and misconfigurations are introduced by malevolent actors? What about attacks on national critical infrastructure? Can electric power plant worker location and activities, and use of unique peripherals be leveraged to gain sensitive information? Or what about offshore oil rig operations where nefarious characters exploit improper user authentication, collection of environmental data, and exacerbate safety risks?

It is time to have an adult conversation.
If security is not addressed, enterprise AR deployments will slow or stop.

Until now, the AR industry has been properly focused on development of technical capabilities and use cases to provide meaningful value. Headsets and software configurations have been left wide-open with regard to security in order to facilitate maximum exploration of features, functions, and applications. However, it is becoming obvious to AR solution leaders that none of their hard work will ever come to fruition in the enterprise if security is not assured. Headset makers will never sell at scale where their devices cannot be certified by the Enterprise Mobility team. App developers will never see their programs deployed in production unless they can demonstrate compliance with new security standards being developed. AR Pilot Program managers trying to implement their new solutions into the workforce will never gain Enterprise IT and executive approvals without a comprehensive security plan addressing the many concerns.

One of the main challenges to implementing enterprise AR projects is Enterprise IT team concerns about cyber security.

On top of it all, AR device vendors, application developers, and system integrators must understand that a flood of legal liability could now channel through them. If workers are injured or die using their solutions, or factory production grinds to a halt because of a breach, a clear, documented trail of steps taken to provide every measure of security and safety possible could prove invaluable. This applies to the full spectrum of AR applications and systems, including wearable devices. If new, AR-related security issues are not identified and addressed, they may compromise the enterprise with regard to compliance issues, brand reputation, financial loss, and perhaps even worker injury and death. Critical questions to be considered include:

- How do we characterize possible new threats introduced by AR solutions?
- How do we communicate with stakeholders and the industry, at large, about these issues?
- How do we defend ourselves and go on the offensive to protect our ventures and assets?

This 2017 study answers these questions through these two new AREA Technical Reports:

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

2016 AREA Security Survey Insights

In the early 2016 timeframe, it was perceived by AREA leadership that there were few, if any, reputable sources of guidance to help understand cyber security risks when introducing wearable AR systems to the enterprise. Solution providers and client companies also indicated a need for practical plans to address these threats.

To gain insight and establish a baseline regarding whether current enterprise ecosystem security standards, best practices, and modalities would meet the security challenges, a series of interviews with AREA members was conducted and summarized. The resulting 2016 survey report, *"AR Security Landscape Interview Preliminary Report: Insights, Perspectives and Opportunities from AREA Members,"* provided new awareness and distinctions about potential challenges and opportunities when AR interacts with existing enterprise systems (human and physical resources, financial applications, procurement functions, etc.). Although not specifically focused on wearable solutions, the survey provided insight into three overarching aspects that should be taken into consideration when addressing wearable AR:

1. Identifying Sources and Potential Magnitude of Security Risks

A security risk may be introduced which impacts the user experience, and then extends beyond, into company internal operations. Obstacles must be overcome using security models and applications that work with, or are integrated into, enterprise infrastructure. Risk mitigation protocols and processes must be established so the company is not compromised. It was noted that the customers and end users can play a significant role in understanding and addressing security risks and concerns.

Respondents felt that because, until that point, there has been such focus on the user interface (UI) and user experience (UE) to drive adoption of AR in general, focus was lacking on security. Unlike conventional information and communication technology, development and adoption drivers have not matured (including security elements) through iterative cycles. It was suggested that developers should examine, learn from and apply lessons learned through case studies with similar technologies and devices that are in effective use today to mitigate existing security risks.

Existing security models for adjacent technologies (Mobility, IoT, medical devices, etc.) were recognized, but respondents suspected these models would probably need improvement or adjustment for application in enterprise AR. For example, the risk models and enterprise management procedures for Bring Your Own Device (BYOD) mobile smartphone and tablet initiatives were probably somewhat applicable. However, respondents also speculated that in the short-term, AR devices are more likely to be enterprise-owned and confined to the physical corporate location, not removed and used personally. This would allow them to be

more stringently controlled by the company. The threat of users storing external data on company-owned AR devices was considered less than that for BYOD personal mobile devices.

The biggest security threats or concerns impacting enterprise AR adoption were seen as:

- Lack of active proposals or standards to enable effective user & device authentication.
- Lack of standard security measures for field use of AR.
- Stringent security measures could make it difficult for end users to practically use devices.
- Running open platforms on physical devices when data on those devices and platforms must be kept inside closed and controlled Enterprise IT environments.
- Current IT and/or security systems and infrastructure may not be prepared to accommodate AR technology.
- Relying on third party parties to provide technical support regarding capture, storage, and retrieval of sensitive corporate data.
- Even if AR systems didn't introduce unique new security threats or concerns, perhaps the scale of existing threats would increase.
- Deep questions exist about the extent to which existing security and risk models are applicable and must be modified.

2. Strategies for Security Risk Mitigation

In the examination of strategies for risk mitigation, interviewees expressed a general, but contextual, consensus that current enterprise system of standards, best practices and modalities could meet most AR security challenges:

- It would be best to keep the development of AR proof of concepts and testing in-house rather than outsource.
- When building proof of concept and testing of AR devices and systems and implementation, it is vital to include technical support teams and end users.
- While some AR solutions are built upon new, proprietary platforms, most appear to use existing mobile operating systems (e.g. Linux, Android, iOS), so one can leverage the many models and lessons provided for those systems.
- The ROI of adopting AR in the enterprise must be clearly understood before making investments in developing and documenting security measures, and engaging in

security standards and best practices development.

- AR developers and providers need to work directly with end users and client security teams to fully understand how the technology will be used, and the various possible security nuances of respective work environments.
- Considering “security by design” or building security into design is critical. One interviewee noted, “*Security is too critical to leave as an afterthought.*”

3. Strategies for Reducing Risk Mitigation Impact on AR Experience Delivery

When discussing whether integrating AR into enterprise infrastructure will cause more security concerns or introduce new "weak links" into enterprise systems, interviewees did not necessarily believe there would be an increase in concerns. They did note that tightly managing data transmission and storage - a core element of an enterprise’s risk mitigation strategy - could adversely impact AR experience delivery. Some common themes emerged:

- AR will probably not drive the need to re-invent data security practices or standards.
- Today’s data standards apply to AR, but data storage might pose a challenge.
- Decisions would need to be made regarding containing data on the device, with implications for broader access and use of that data.
- Decisions would need to be made on how “locked-down” AR device data should be based on deployment, use case, and industry. Organizations deploying AR will need to analyze what is required to secure data access given their specific application.
- Decisions would need to be made regarding cloud storage solutions. Some customers are more comfortable with data being stored in the public cloud, while others may require private clouds or keeping date on premise.
- There is a need for best practices or criteria for AR risk measurement and mitigation.

Far more questions than answers were generated by the 2016 survey. A better understanding of AR cybersecurity risks to the enterprise was needed.

The 2016 survey generated far more questions than it answered. It clearly illustrated the need for a better understanding of enterprise AR cyber security risks and the need to adopt - or develop - a methodical means for characterizing and mitigating the threats.

In response, in early 2017, the AREA issued a Request for Proposals to industry for this premier, comprehensive study regarding wearable enterprise AR security risks and management, and development of a security framework and test protocol.

2017 AR Security Study Overview and Objectives

In order to forge new ground in the field of enterprise AR security, the AREA commissioned this 2017 study. The intent was to gather insights and perspectives from AR device manufacturers, platform creators, IT and security professionals, end-users, and others regarding security risks from introducing mobile, wearable systems into the enterprise. By researching the state of cyber security development in the AR industry, and the security approach of enterprise users across various market verticals, AREA Members could potentially gain greater understanding regarding real and perceived risks and mitigation strategies.

Confirming initial AREA leadership assumptions, after extensive research and scores of interviews and conversations by this AREA study team, it was verified there is exceedingly limited prior research or practical guidance on the topic.

This 2017 study was designed to create the primer providing an overview of wearable enterprise AR cyber security to orient corporate and vendor teams. Throughout the analysis and development of the security framework and testing protocol presented, a common vocabulary is suggested for facilitating communication on this important topic. The objectives are to facilitate understanding of cyber security vulnerabilities by AREA Members, and educate them on how to characterize, test for, and measure the impact of these new threats.

SECTION 2 – AR SECURITY LANDSCAPE

To understand the extent to which the topic of enterprise AR cyber security has already been addressed, this AREA study team began the investigation with an extensive online search and case study review. The team also conducted interviews with representatives across the AR stakeholder spectrum, from enterprise managers and end users, to device vendors, application developers, and more. While results of the literature search and industry interviews influenced the direction, scope, and findings of this final report, they also confirmed that, prior to this research, no directly-relevant sources of information were available on this important topic.

> ***No prior sources of information were found to be directly-relevant and sufficient regarding wearable AR cyber security.***

The literature review and case studies provided below necessarily focus, then, on technologies and applications related to Augmented Reality. For example, case studies on use, security, safety, and privacy for wearables in the enterprise, and IoT & Enterprise IT security studies.

Literature Review

To gain insight regarding the risks to enterprise data security from mobile, wearable AR systems, a collection of white papers, academic research papers and industry articles were reviewed (See Appendix B - Literature Review). A few key findings include the following:

- Various white papers present a range of real-world case studies for enterprise wearables classified by vertical market, including smart AR glasses, voice-controlled headsets or clip-on devices, smart watches, body sensors, wearable cameras, fitness trackers, and other devices.

- Embedded wearable medical devices are evaluated, noting that the data is both extremely private and highly vulnerable to theft. The study posits that current approaches to data security do not provide a pragmatic framework for end-to-end protection so a new security architecture with end-to-end encryption is both required and proposed.

- Best practices and frameworks for enterprise data security should address more than just the cyber security perspective (physical security, operating procedures, personnel security & training, visitor management, IT security). IoT security is a shared

responsibility between the various entities in control of the system, applications, and development tools at the various vendor, customer and public levels.

- The Industrial Internet of Things (IIoT) offers multiple characteristics and best-practices, and unique security and privacy challenges, that mirror AR wearable devices. For example, components like controllers, sensors, and actuators are based on technologies that are uncommon within most IT architectures. Lack of interoperability complicates and slows adoption.

- Four of the most dominant IoT architectures are analyzed from security and privacy perspectives, and shown to meet only mediocre requirements. Traditional IT cyber security methods are found to be insufficient. Exclusively relying on use case evaluation to identify security threats is insufficient because unique, broader-scale system vulnerabilities and threat vectors operate outside those use case models. Defense in Depth practices providing layers of redundant security controls are essential to protect personnel, procedures, technical and physical security across the system life cycle.

- Because technology will continue to evolve, enterprises must develop an agile security plan which calls for regular maintenance, constant network monitoring, system failure alerts, and established and adaptable incident response protocols.

- Existing standards for networked low-power wireless IoT devices (ZigBee, BLE) do not support secure pairing of new devices into a network and are vulnerable to man-in-the-middle attacks. Three aspects for improving secure pairing of IoT devices are proposed:

    - functionality allowing users to manually approve/abort/sever associations;
    - a new message recognition protocol which allows devices to exchange authenticated messages without the use of public-key cryptography (which exceeds the capabilities of many IoT devices);
    - message exchange requires robust definition of security based on universal composability for analyzing cryptographic protocols and guaranteeing very strong security.

- Mobile device usage by employees of the U.S. Federal Government is regularly reviewed and the global mobile ecosystem is categorized into a threat model. Each element of the ecosystem is evaluated with detailed summaries of the greatest threats in each area, and current mitigations and defenses described. A framework for modeling mobile threats to assist in identification of attacker tactics and techniques is provided, and several emerging threats are analyzed.

Case Studies

The availability of public case studies on the security of wearable AR devices in the enterprise is scarce. Given this, the AREA study team drew upon several relevant case studies in technology realms related to wearable AR devices - Enterprise IT, Mobility, and IIoT:

Nonprofit Under Attack: A Cyber Defense Case Study
https://redmondmag.com/articles/2017/04/01/defense-in-depth.aspx

> This case study addresses threat detection and remediation related to cyber attacks targeted against Planned Parenthood (PP), a national organization providing health care services to millions of women across 650 U.S. clinics. Representative of many large healthcare and commercial enterprises, Planned Parenthood is a decentralized organization required to protect highly sensitive customer information and comply with a host of regulations. Facing an ethical and political firestorm regarding their services, the organization needed to defend against potential data breaches and system compromises which could harm patients, physicians, or other support personnel. In this case study, organized as a series of interviews over two years, PP shares challenges faced in modernizing their IT services:
>
> - A unique coordinated threat vector and attack types.
> - Difficulty finding and retaining skilled security professionals.
> - Creation of a Center of Excellence (COE) blueprint based on National Institute of Standards and Technology (NIST) and SANS Institute best practices.
> - Evaluating and developing deep partnerships with the right suppliers.
> - Finding suitable, extensible, and secure collaboration tools and an Enterprise Mobility and management (EMM) platform.

Garage Door Openers: An Internet of Things Case Study
https://www.computer.org/web/computingnow/content?g=53319&type=article&urlTitle=garage-door-openers-an-internet-of-things-case-study

> This case study examines how connecting garage door openers to the Internet can make them easy targets for hacking and pose serious risks to property owners. For example, what if an attacker could indiscriminately open doors nearby, or hack email accounts to learn a user's home address and credentials to open their doors? What if an attacker downloaded an entire database of user credentials? These possibilities make home intrusions virtually inevitable, and similar to AR wearables as a form of connected IoT devices, could turn the products sold by long-standing, trusted, companies into unwitting cyber attack vectors.

Virtual Machine Security Challenges: Implementing malware with virtual machines
http://www.citeweb.info/20130165118

> This case study profiles various methods used by cyber attackers, whose core objectives are to gain control of systems and either seize important information or destroy it. Research indicates hackers are sometimes using low-level operating system techniques and programming codes, or a new class of rootkit that makes detection and defense very difficult. Through these attacks, system administrators can suffer huge losses in both the short and long run. Using such methods, it becomes quite difficult for defenders to predict and gauge the intensity of an attack. More specifically, this new type of malware is known as a virtual-machine based rootkit (VMBR) - code installed in a virtual machine monitor (VMM) that operates under an operating system of a computer. This malware converts the OS into a virtual machine, which makes the code extremely difficult to remove. These VMBRs also facilitate the spread of more general malicious services and shields them from the target system in a separate OS. The authors evaluated the new threat using two VMBR proof-of-concept attacks to to subvert target systems running Windows XP and Linux.

Mobile OS Security and Threats: A Critical Review
http://research.ijcaonline.org/volume86/number9/pxc3893293.pdf

> Case studies are presented on various smartphone operating systems, which are similar to the OS used on many AR headsets. The power of modern smartphones comes, in part, because they are multi-purpose, portable devices supporting a vast number of third party applications augmenting the device's functionality. Unfortunately, the toolkits and programming libraries provided by the platforms to support application development can also be their weak point. This paper provides a comparative analysis of various proof-of-concept attempts made by undergraduate and postgraduate computer science students to implement and distribute location-tracking malware on various smartphone platforms.
>
> Observations show that most smartphone platforms could not stop even average developers from successfully launching privacy attacks, harvesting data from the device without the user's knowledge and consent. It illustrates the ease with which malware can be developed and spread. Unfortunately, no silver bullet solution is available. Existing smartphone security models facilitate mechanisms for controlling the installation and execution of third party apps, but this approach is not sufficient to thwart many modern attacks vectors. The paper proposes that, in addition to implementing secure application distribution procedures, administrators can at least try to prevent the spread some attacks by increasing user awareness regarding security and privacy risks and best-practices.

Enterprise Mobility Management

When evaluating how enterprise teams might manage wearable AR devices, a close analogy would be how companies manage smartphones, tablets, and laptops for their employees, today. Organizations are increasingly engaging in coordinated and evolving Enterprise Mobility Management (EMM) strategies to carefully balance the potential risks and benefits of leveraging these powerful mobile resources. A solid EMM approach involves one or more of the following elements:

Mobile Device Management (MDM)

Initially, companies desired full control over all devices and applications, so established a Mobile Device Management (MDM) control policy only allowing use of very tightly restricted, corporate-owned phones. This approach often resulted in employees carrying around two phones – one corporate and one personal – which proved somewhat impractical. MDM refers to the software platforms and the corporate policies used to centrally administer company-owned smartphones, tablet computers, and laptops across all popular mobile device operating systems. MDM provides a unified software administration console for device activation, enrollment, and provisioning, and decommissioning. It also provides a layer of security for locking down, monitoring, and controlling SD card encryption, geo-tracking, and creation of policies and connectivity profiles. MDM also provides the IT department with the ability to enforce policies by restricting user authentication modes and software loads, and enabling remote locking and wiping of the device.

Mobile Application Management (MAM)

As employees demanded more flexibility and use of their personal devices for work, companies examined Bring Your Own Device (BYOD) strategies. This gave rise to Mobile Application Management (MAM) tools, aimed at controlling just the corporate applications loaded on employee-owned phones rather than attempting to manage the entire device. MAM allows IT departments to lock down, secure, and control only their corporate applications such as email, calendar, contacts, and expense reporting. Companies can provide access to corporate-approved applications through customized app stores. MAM handles software licensing and delivery, configuration management, app maintenance, policy enforcement, and usage tracking of corporate applications, while everything else on the phone remains under the control of the user. The company can remotely control encryption, policy management, and wiping of corporate data and applications, leaving the employee's personal apps and device usage alone. MAM also presents some challenges, including trying to run various secure and unsecure applications on the same device.

Mobile Information Management (MIM)

Most recently, companies have explored leaving the device and applications alone, and only concerning themselves with encrypting and managing corporate data utilized by those applications. Theoretically, a standard mobile app could then interact with both personal and enterprise information, the later done securely. MIM provides for access and identity management, giving IT managers the ability to monitor and control which employees have mobile access to sensitive information. Unfortunately, this approach is fraught with complications related to device and software integration which have not yet been ironed out.

In these early days of AR, where the cost of wearable headsets is high and functionality limited, one might reasonably expect most AR devices will be owned by the company rather than the employee. In that case using an MDM approach, companies could tightly control the device and applications, and help secure corporate data and functionality, although additional tools and policy revisions would be required to create a comprehensive solution. Increasingly over time, the cost of headsets will drop, their general availability and functionality will expand, and employees will begin using the smart glasses in both their personal and professional lives.

Wearables and smart glasses are expected to assume all functionalities of contemporary smart phones and tablets, making earlier mobile devices effectively obsolete for some, and then gradually, most applications. Companies should anticipate how MAM, MIM, and newer models of mobile management might be employed for these emerging communication and computing tools. Offering a couple of promising first steps, in Nov 2015 at the Mobile World Congress, *Good Technology* announced support for wearable devices, and in Oct 2016, *VMware AirWatch* announced what they claim is the first unified solution for AR smart glasses management. The extent to which these management platforms can meet security requirements for wearable enterprise AR devices is uncertain and is an important topic for follow-on research.

Additional Market Areas to Consider

Additional market areas which may give rise to case studies and best practices that could possibly be transferred to the wearable AR arena include the medical device market, cloud services, and enterprise data management arenas. For this study, these areas were seen as less likely to yield practical results than those investigated, above, and so they were left for future research.

SECTION 3 – SECURITY FRAMEWORK & TEST PROTOCOL

> ***Gaps exist between contemporary security protocols and requirements for securing wearable enterprise AR solutions. A new framework is required.***

Although valuable concepts and best practices were discovered across the literature search, case study reviews, and industry interviews conducted by this AREA study team, there are still many gaps between current security protocols and guides for comprehensively securing wearable enterprise AR solutions. To evaluate and fill these gaps, the AREA study team drew on professional experience gained from co-authoring and exploiting several high-profile methodologies and frameworks developed for secure Enterprise IT, Mobility solutions, and Industrial IoT applications.

Use Cases and Vulnerability Evaluation

In order to begin the development of a new security framework and test protocol for wearable enterprise AR devices, this AREA study team began with a review of three common enterprise use cases for AR wearables leveraged from the prior AREA Technical Report: *User Experience Design for Enterprise Augmented Reality.* The three use cases were further reduced and a common technology architecture was defined, and associated security threats identified. Important data security similarities and differences were also identified between wearable AR headsets and other multi-purpose mobile devices, like smartphones and tablet computers. Although mobile devices also have collections of sensors, are connected through digital networks, and are location aware, critical distinctions between systems are highlighted, below.

#1 - Augmented Maintenance and Repair Operations

Maintenance and repair operations (MRO) are procedural tasks that involve the revision of the status of a piece of equipment, the diagnosis of a problem and/or the repair of an identified fault. MRO procedures can be performed on any type of component and in potentially any location. The procedure often follows these steps:

- Receive notification of a maintenance order
- Identify the location
- Identify the object
- Diagnose the status of the object
- Identify the fault
- Perform repair procedure
- Notification of successful completion of procedure

FIGURE 3-1: AR-assisted maintenance. Courtesy US Space and Naval Warfare Systems Command.

The repair procedure can include the replacement of a part of the equipment and the disassembly/reassembly of many adjacent parts. The AR application via wearables such as a headset can assist workers during the assembly process. For example, it can highlight existing parts involved, display virtual parts to assemble, show animation illustrating the operation to perform, display an arrow pointing to the direction of an industrial closet, and highlight the bin containing the required fixtures when it becomes visible.

Similarly, the AR application can help users perform maintenance and repair operations in situ or in the field. In the case of field service in remote areas, a remote expert can efficiently support the technician by actually seeing what the operator sees on-site and collaborating with him. In a consumer scenario, customers that need to perform a repair task at home are able to download instructions to their AR device.

#2 - Augmented Warehouse/Warehouse Picking

AR-assisted warehouse systems support users through the use of wearables in picking and sorting processes. AR scanners recognize and match part or package codes and provide instructions via graphical overlays for sorting and delivery. The user interface for AR-assisted warehouse picking wearables can be speech recognition, gesture recognition, eye-gaze recognition, and touch screens.

There are many benefits of augmented warehouse picking as part of the overall warehouse management system. Notably, wearable technology is fully mobile and enables hands-free processing; a rich graphical user interface without the need to carry a handheld device; voice-controlled processing; barcode scanning and image capture; vision-aided processing that assists with the accuracy of supply chain operations; and built-in GPS systems for navigation. The use of Augmented Reality via wearables in the warehouse has the potential to significantly reduce costs by increasing speed and reducing or eliminating errors in the picking process. It can also help with the training of new or temporary warehouse staff, and aid warehouse planning.

FIGURE 3-2: Automated warehouse picking. Image courtesy Augmate.

As noted in the AREA Technical Report: *User Experience Design for Enterprise Augmented Reality*, AR-assisted warehouse picking is effectively utilized when integrated into parts and inventory databases and workflow, and customer management technologies. In an advanced deployment, they can support remote expert interaction and feedback with integrated video conferencing and collaboration tools. AR can help warehouse staff navigate large facilities with thousands of items to efficiently locate and collect them. Presentation of route optimization steps and product scanning can replace handheld device procedures used today.

#3 - Assembling a New Product

AR system architecture can be effective for assisting assembly workers by providing visual information superimposed on the physical assembly parts. Such AR methods are particularly well suited for complex, short manufacturing series or in a customized production factory

environment. Each individual product may have a slightly different configuration: the order of assembling parts may vary for different products and/or the number of phases in the assembly line may be large. The traditional approach is to use assembly drawings (blueprints) and possibly instruction manuals with guiding pictures to describe the content of each work task. As the assemblies become even smaller, the need for guiding the worker with all available tools becomes increasingly important. The AR system can reduce assembly times, accelerate learning of the assembly tasks and provide more quality assurance to the factory floor.

AR-based manufacturing or assembly instructions affect different information processing systems of the enterprise in several ways. The implementation of AR-based assembly instructions via wearables needs to consider the information processing architecture. The majority of product data is created in design systems and stored to a PDM/PLM system. Sales teams can provide input to configure and customize the individual product, which is also stored to the PDM/PLM system from which AR-assisted instructions will be created. The ERP system controls production planning, and the assembly server, which manages augmented instructions sent to the worker.

FIGURE 3-3: Augmented electronics assembly. Image courtesy Zentech Mfg, Inc.

Use Case Commonalities

Certain common characteristics apply across many use cases.

From these three use cases, a common technical architecture was mapped and considerations identified which are relevant to security of AR wearables in most enterprise applications. Figure 3-4 illustrates the technology stack required. Tiers of the stack are identified, and trust boundaries are established around each significant entity. This process of modeling the architecture of an enterprise AR solution, then establishing trust boundaries and threat vectors is described in detail in the companion AREA Technical Report: *Wearable Enterprise AR Security - Security Framework and Test Protocol*.

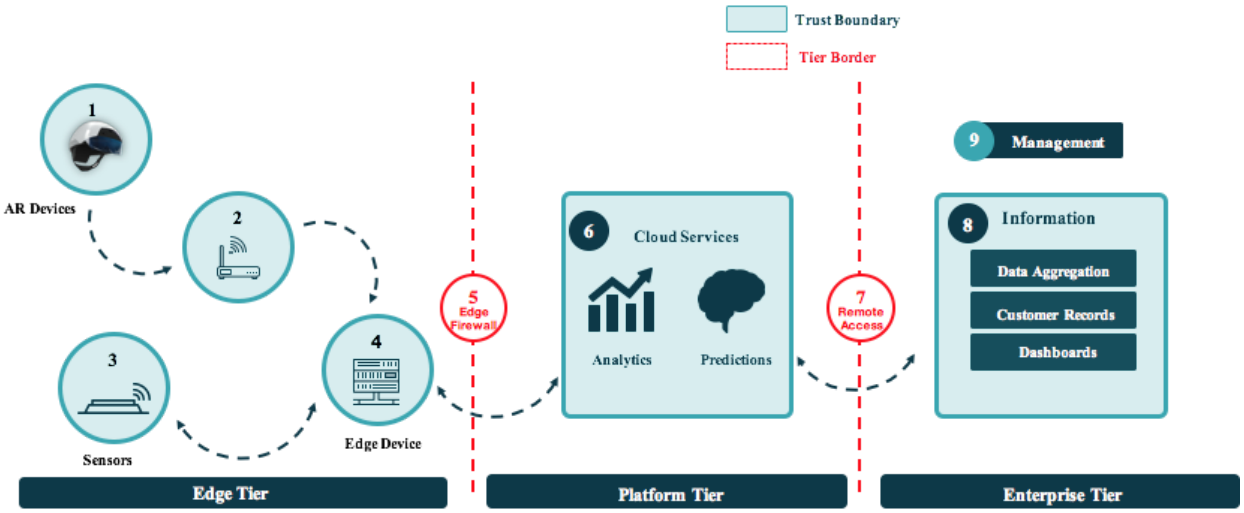


FIGURE 3-4: A common AR technical architecture model.

Common considerations across wearable AR devices in the enterprise include:

- Use context of the wearable device (how it is being used? where it is being used? by whom is it being used? etc.).
- Human factors arising from wearable devices in which the AR system dynamically follows the user's point of view and keeps virtual objects aligned with real world objects.
- Level of processing power of the wearable device.
- Degree of physical and mental constraint imposed by the wearable device.
- Connectedness of the wearable device to other devices, systems, etc. and cross platform system interaction and interoperability.
- Security protocols for network communication.
- Integration of AR wearables with legacy systems.
- Maintaining name directories for authentication.
- Attack surfaces (social engineered or reversed engineered).
- Unreliable content and data, especially content created and delivered by other systems or even third party vendors and applications.
- Web browsers that do not fully support AR functionality, and AR developer disabling of Web browser security filters to make new tools and APIs available.
- Lack of universally approved security standards for AR.
- Different versions of Operating Systems (Android™,Windows™,etc).
- Potential use/integration with biometrics and new emerging security-related technologies.

Security Requirements Development

> ***Boilerplate security solutions are not appropriate for AR use cases.***

Although common considerations were identified for the use cases studied, it's important to recognize that every industrial connected-device project demands different protection requirements, depending on intended function and vertical. It is critical that security teams not approach the problem from a boilerplate security solution perspective. AR is a new computing platform. As such, security requirements not supported by current policies or in-house solutions should be carefully identified. The procedures to identify security requirements for an AR headset are as follows, and elaborated upon in the companion AREA Technical Report: ***Wearable Enterprise AR Security - Security Framework and Test Protocol***.

1. Document the relevant security uses cases for the enterprise end-to-end solution.
2. Create a detailed technical architecture of the project, such as that provided, below.
3. Identify the trust boundaries (also known as trust zones), which are defined as a grouping of logical or physical assets that share common security requirements based on factors such as criticality and consequence.
4. Describe the connectivity between zones, also known as "conduits."
5. Identify the set of threats to all AR devices in each particular trust and related conduits.
6. Define the role of the user in order to evaluate how the device will interact with the environment, and hence, how device misuse may affect safety and kinetic threats.
7. Utilize the use cases to evaluate the threats, security requirements for the AR zone and conduits
8. Perform a threat assessment, using OWASP, IoT STRIDE, IEC 62443 or others, with the help of the Test Protocol tables provided in this framework presented in the companion report.

AR vs. Mobile vs. IIoT vs. IT Security

At first glance, it would seem logical to assume that AR devices are very similar to conventional enterprise mobile devices like notebooks, smartphones, and tablets from a security perspective. Also in some regards, AR headsets might be considered a type of "thing" similar to industrial Internet of Things devices. As well, aspects of head mounted devices are similar to other Enterprise IT elements like desktop computers or peripherals like printers, scanners, video

cameras or projectors. So can AR solutions be managed using cyber security methods and tools used for these related devices? The AREA study team found this assumption to be both highly inaccurate and dangerous. A more accurate characterization recognizes that AR solutions share both the strengths and weaknesses of these systems, which actually embodies the worse of all worlds.

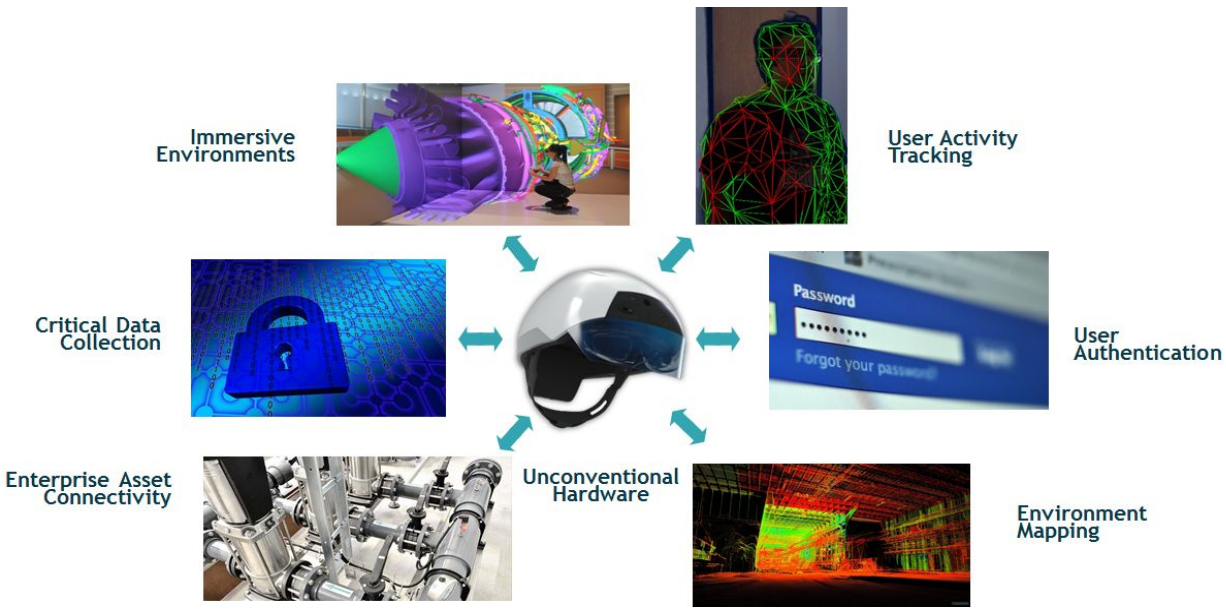


FIGURE 3-5: Some unique functional attributes of AR headset solutions.

> ***Unique attributes of wearable AR solutions give rise to a complicated security posture and threat profile.***

The combination of both similar and unique attributes characterizing wearable AR solutions versus conventional Mobility, IIoT, and IT solutions gives rise to a complicated security posture and threat profile. For example, designing and managing security at the AR edge-computing device is unique relative to typical Enterprise IT and Mobility deployments where users and applications are managed, security tools and permissions are established, computing elements are secured, ports are closed, and user activities are logged and audited.

Critical differences between AR solutions and other enterprise connected device modalities include the following, which must be addressed:

1. **Massive data collection and environment mapping** - To maximize functionality, AR devices collect data regarding user location, orientation, connection to equipment and assets, and 3D environment mapping.

    a. **Recording of sensitive data** - Concern is increasing regarding the security of AR headset cameras recording sensitive corporate assets and activities.

    b. **Immature security protocols** - Strong security protocols have yet to be defined or employed to manage data captured and use by AR system camera and other sensors, including a lack of proper practices for users and the ability to track compliance.

    c. **Undefined data logging and encryption policies** - Data logging and encryption methods to audit and restrict access to critical information have not been established.

    d. **Uncertain data ownership** - In order to establish effective security measures, another key concern involves resolving who owns all of the gathered headset data. Does the enterprise, the device operator, the AR platform provider, or cloud application vendor have rights to some or all of the data? Are managed service providers authorized to access streaming and stored client data? Is there a succession plan for data transfer if the company facility is sold? For example, do 3D environment maps generated by AR headsets stay with the new owners, and how are they practically erased off seller servers and AR systems? Could be legal implications if stakeholders are cut off from their digital property?

2. **User authentication with uncommon UI** - In order to increase flexibility or to have company-owned AR devices shared by multiple users, depending on their tasks, these devices may be configured with limited or modified user authentication. Passwords may be generalized or shared between work groups, resulting in less secure user authentication. Unconventional authentication methods using voice or gestures are easily observed and spoofed by cyber criminals.

3. **Mutual and role-based authentication** - To enable deep team collaboration, devices must be able to mutually authenticate, which might happen most effectively in a peer-to-peer mode rather than relying on cloud-based authentication methods. Role-based authentication must also be enabled to authorizing users to appropriate

levels of data access, functionality, and interactions.

4. **Uncommon peripherals** - A plethora of innovative peripheral devices are appearing in the market to enhance user interaction with wearable AR devices, in addition to the unique environmental sensors integrated into the headsets, themselves: positioning systems tracking the wearer's geographic and relative position in the work area, head position and orientation tracking, eye tracking, gesture recognition and hand-tracking including smart-gloves, tangible user interfaces similar to game controllers with haptic feedback, voice and multi-touch interactions, and more. Connectivity and communication with these peripherals is through a variety of networking protocols and procedures. Pairing and authentication of these unique peripherals is susceptible to intrusion and corruption. Signals and data may be subject to adulteration, evisceration, or transformation.

5. **Lack of hardware Root-of-Trust** - Root-of-Trust (RoT) functions provide the necessary foundation for security function such as integrity, isolation, and storage. Most AR headset hardware does not appear to have included this vital security system component, or it is not properly supported by firmware and OS. Without these critical hardware components, some critical protection features cannot be enabled such as on-the-fly encryption, detection and reporting of unauthorized OS and program changes, detection of rootkits, memory curtaining to prevent program memory read/write impropriety, and hardware-based digital rights management for digital media copyright protection.

6. **Safety and trust risks of digital immersion** - In contrast to use of AR on mobile devices, a strength - and weakness - of AR headsets is their inherent ability to provide an enhanced immersive experience for the user. Workers wearing headsets and experiencing rich visual, auditory, and haptic interactions will tend to trust the information being delivered as an integrated element of their operating environment. Ques in their surroundings which might otherwise warn users of dangerous, obviously-incorrect information, or security risks may be obscured or overlooked. Trusting digital representations of the real world versus physical realities can cause life-threatening mistakes and misfortune.

7. **Intentionally open configuration** - AR devices come out of the box with either a proprietary Operating System (OS), or a stock OS without security hardening of any kind (Android, iOS, Linux, Windows Mobile). System designs and configurations are wide-open from a security perspective, for example ports are commonly left open by default to encourage access. Configurations can be corrupted. Protective features and functions are rarely/never clearly identified, explained, pre-configured, or addressed by the vendor from a threat mitigation standpoint.

8. **Hardware and networking design vulnerabilities** - Rather than relying on onboard data storage exclusively, headsets may record data on SD cards which can be forcibly removed, deleted, or exchanged. I/O ports and communication protocols are open including audio jacks, micro USB ports, WiFi and Bluetooth(™) networking.

9. **Software threat vulnerabilities** - Some AR headsets utilize the closed, proprietary architecture and development tools, and are fundamentally susceptible to desktop-type attacks. Loading of utilities protecting against viruses, spyware, and malware requires extra effort and cost. The applicability of mobile or desktop versions of protection utilities for AR systems is unknown at this time and a suggested topic for further research.

10. **Undefined upgrade and patching strategies** - As use of AR devices becomes more more widespread, it becomes increasingly likely hackers will exploit vulnerabilities if developers can't remotely upgrade systems to protect against evolving threats. Developers of AR solutions will have to integrate periodic software update capabilities into the systems. Scalable and secure patch distribution strategies must be effective and flexible enough to operate across a variety of device makes and models, including tools to identify and correct roll-out anomalies.

11. **Remote connectivity** - There are many benefits from establishing remote connectivity with AR systems. For example, bi-directional, real-time voice, video, and sensor data streams between wearable AR units and offsite personnel, data repositories, and applications can provide important value. However, the preponderance of enterprise representatives surveyed indicate strong reluctance to allow connectivity between AR systems and offsite/cloud data repositories, applications, and resources. AR systems fundamentally require access to large amounts of data that exceeds onboard storage capabilities, creating an additional conflict. Is access to the open internet critical for field workers to retrieve equipment vendor schematics and repair processes? Alternatively, what happens if access to remote resources is intentionally cut off by hackers, stranding the end-user? More-trusted conventional mobile devices do not face the same degree of restriction.

12. **Remote monitoring and always-on sensors** - AR headset cameras, microphones, and sensors were found to engage in pervasive background collection of data, in some cases, even when in standby and powered-down modes. This AREA study team was able to remotely access data being collected in real-time by headsets without the user's knowledge, including collecting progressively higher-fidelity 3D contour maps of the user's surroundings posing a clear threat to enterprise intellectual property, facilities, assets and personnel. Future AR systems may be able to redact certain details in video and sensor feeds, such as automatically blurring everything except the equipment and

surroundings contextually relevant for tasks being performed by the user, but that is thought to be some ways off.

13. **Remote management** - In the near term, AR solutions are most likely to be corporate-owned, restricted-use systems, as opposed to employee-owned devices serving both personal and professional functions. Remote management requirements will clash with the desire to restrict remote connectivity to protect sensitive data. Third-party device management may be unfavorable by the enterprise, thereby challenging contemporary strategies for managing employee smartphones and tablets. Hackers may simulate routine software updates in order to infect systems.

14. **Modified software development and deployment patterns** - Software settings in a development environment allow a much greater degree of access than in production environments. Although prudent software development practices typically require that teams maintain strict isolation between development code and code ready for deployment into production, enterprise hardware devices on which that code runs (like PC workstations) are not typically reconfigured between environments because they are typically stationary and assigned to a specific user or confined to a lab. The mobility of AR devices, however, increases the likelihood that units used in development might actually transition to production, enterprise, and guest networks over their lifecycle.

15. **Restricted use encouraging relaxed security** - In the near-term, unlike traditional BYOD mobile devices which are often managed via MDM/MAM data compartmentalization schemas, AR devices will likely be corporate-owned and tightly managed from a use case perspective. There is a recognized paradoxical tendency for corporate asset managers to relax security measures on assets they consider to be exclusively on-premise and restricted use.

Supplementing existing Enterprise IT, Mobility, and IIoT security measures with a new AR security framework is essential.

What is critical for AR systems to be deployed at scale in production environments is the thoughtful design and methodical implementation of a collage of security measures incorporating the best approaches from Enterprise IT, Mobility, and IIoT supplemented by a new AR security framework filling the gaps remaining to cover AR-unique system characteristics.

Cyber Security Equivalence Concept

Although information systems have always existed on a spectrum of technological constraints, connectivity and capabilities, the emergence of a new breed of device or implementation necessitates an analysis of the applicability of standards and guidelines for that device. Ideally standards and requirements within a framework would be consistent and comprehensive according to accepted best practices within the domain. However limitations in processing power, data storage, connectivity and other technical constraints often render such standards impossible. In addition, standards which may be technically feasible, may have a reduced effect or adverse complications within specific architectures or implementations.

Therefore, it is appropriate and advisable to establish a security framework in which individual standards are reshaped to achieve an equivalent level of security posture in spite of technical challenges. We specifically refer to this as the concept of *Cyber Security Equivalency*. This practice requires the evaluation of vulnerabilities in a vacuum which are then applied to realistic threat probabilities as would arise in a penetration test. The result is an “equivalent” level of probability by which we can strengthen or edit security controls in order to achieve strong protections that are feasible, achievable, and effective. Figure 3-6 illustrates the existing security standards on top of which the AREA Enterprise AR Cyber Security Framework is built:

FIGURE 3-6: Elements of the cyber security equivalence model.

NIST Framework for Improving Critical Infrastructure Cybersecurity
https://www.nist.gov/cyberframework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST CSF) was established through government and private sector collaboration to provide a set of industry standards and best practices for managing cybersecurity risks. Originally published in 2014 and aimed at critical infrastructure operators, various updates have since been deployed and the framework is now utilized by a wide range of businesses and organizations. The flexible and technology-neutral framework uses a common language to cost-effectively address and manage various degrees of cybersecurity risks, and is composed of three parts. Each of the three framework components reinforces the connection between business drivers and cybersecurity activities, and can be customized to meet organizational conditions and priorities:

- *Framework Core* - a set of cybersecurity activities, outcomes, and informative references common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational profiles to help align cybersecurity activities with business requirements, risk tolerances, and resources.
- *Framework Implementation Tiers* - a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk. Tiers describe the degree to which an organization's cyber risk management practices align with the Framework (e.g. risk and threat aware, repeatable, and adaptive).
- *Framework Profiles* - cybersecurity outcomes based on business needs that organizations select from framework categories and subcategories. The profile aligns standards, guidelines, and practices to the framework core in a particular implementation scenario. Profiles can be used to compare a "current" profile with a "target" profile.

OWASP Mobile Security Project
https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

The Open Web Application Security Project (OWASP) is a worldwide not-for-profit organization focused on improving software security. The OWASP Mobile Security Project provides developers and security teams with resources to build and maintain secure mobile applications by classifying mobile security risks and providing developmental controls to reduce their impact or likelihood of exploitation. The primary focus is at the application layer, though the project also takes into consideration the underlying mobile platform and carrier inherent risks, and addresses both applications on the mobile device and remote servers. OWASP placed heavy focus on the integration of mobile application, remote authentication services, and cloud platform features.

IEEE Cyber Security Initiative
https://cybersecurity.ieee.org/

The Institute of Electrical and Electronics (IEEE) Cybersecurity Initiative was launched in 2014 by the IEEE Computer Society and the IEEE Future Directions Committee to:

- provide the go-to online presence for security and privacy (S&P) professionals, including a growing collection of thought leader interviews.
- improve the comprehension of cybersecurity by students and educators through the Try-Cybsi sandbox for users to try out cyber security attacks, tools, and exercises.
- improve S&P designs and implementations by professionals through the Center for Secure Design facilitating identification of common design flaws, and hosting the IEEE SecDev annual conference to expand knowledge around creating secure systems.

ISO/IEC Information Security Management Systems Standards
https://www.iso.org/standard/66435.html

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) joint technical committee (JTC1) established the ISO/IEC 27000 family of standards to help organizations keep information assets secure through implementation of information security management system (ISMS) requirements. The family includes more than a dozen standards to help systematically manage sensitive financial information, intellectual property, employee details, entrusted third-party information, and more. This includes risk management processes for people, organizations, and IT systems. Bringing information security deliberately under overt management control is a central principle of ISO/IEC 27000 standards.

Industrial Internet Security Framework
http://www.iiconsortium.org/IISF.htm

The Industrial Internet Consortium (IIC) was founded in March 2014 to bring together the organizations and technologies necessary to accelerate growth of the Industrial Internet by identifying, assembling, and promoting best practices. Membership includes small and large technology innovators, vertical market leaders, researchers, universities and government organizations. Members of the IIC published the *Industrial Internet Security Framework (IISF)* in September 2016 as a common framework, approach, and best practices for assessing and managing cybersecurity in IIoT systems. The IISF identifies, explains and positions security-related architectures, designs and technologies, as well as identifies procedures relevant to trustworthy IIoT systems. It describes security characteristics, technologies and techniques that should be applied, methods for addressing security, and how to gain assurance that the appropriate mix of issues have been addressed to meet stakeholders' expectations.

The AREA AR Security Framework Overview

After evaluating the existing frameworks, described above, for applicability and gaps related to the generic AR Use Case defined, this AREA study team synthesized a three-phase approach for a new AR Security Framework. Details are presented in the companion AREA Technical Report: *Wearable Enterprise AR Security - Security Framework and Test Protocol*.

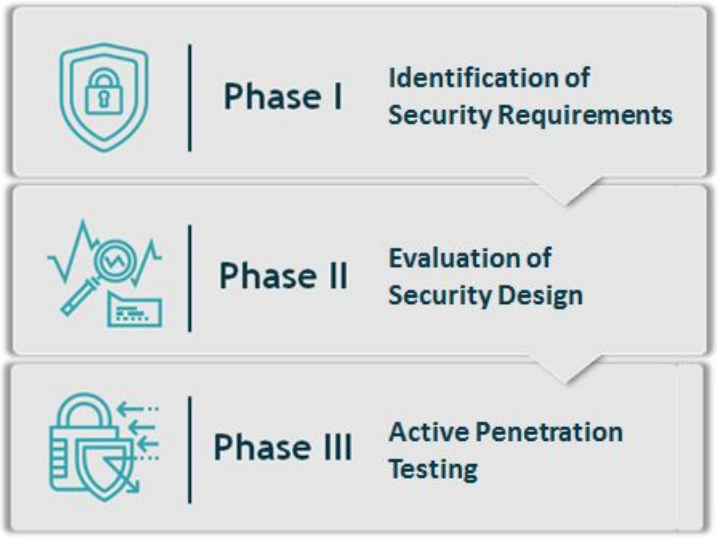


FIGURE 3-7: Three phases of the AREA AR Security Framework.

The AREA AR Security Framework and Test Protocol are designed to provide a repeatable approach for assessing the security of an industrial project utilizing AR headsets. Initially, the focus of the framework and protocol is on evaluation of the AR headsets and their role in enterprise solution deployment. Comprehensive security protection also requires sound policy development, user training, and effective governance procedures to guide deployment and use of the systems throughout their lifecycle. These latter factors, while critical to protect enterprise assets, are out of scope for this initial AREA project and are suggested for further study.

Use of the AREA AR Security Framework can aid in the selection and deployment of AR wearables in the enterprise.

The AR Security 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 role 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 the potential for automating threat modeling.

Please refer to the companion report for a detailed explanation of the AREA AR Security Framework.

The AREA AR Test Protocol

The AR Test Protocol is also offered in the companion AREA technical report, and defines a methodology to identify security requirements for an AR device, evaluate functional features, and broadly review operational testing guidance. Functional features for evaluation of devices include hardware and software security elements such as firmware, OS, middleware, applications, and methods for establishing device identity, access control, integrity protection, monitoring, and configuration and management. Operational elements include:

- Developing a trusted software repository.
- Evaluating software and remote access capabilities.
- Encrypting data at-rest and in transmission.
- Software testing techniques to identify deployment bugs and anomalies..

Please see the companion report for details of the AREA AR Security Test Protocol.

Validation of the Framework and Protocol Through Device Evaluations

The AREA study team physically examined and used several popular AR headsets as part of this research project. These activities helped the team formulate and validate the AR security framework and evaluation methodology. It was out of scope for this study to meticulously document performance of these devices against the new Test Protocol, which is an area for recommended follow-up study. Rather, hands-on testing of these headsets and smart glasses helped illuminate functional and use idiosyncrasies, and confirm theories on the part of this AREA study team.

FIGURE 3-8: Framework validation through hands-on device testing.

FIGURE 3-9: Framework validation through industry interviews.

SECTION 4 - KEY FINDINGS AND LESSONS-LEARNED

FIGURE 4-1: Key findings of this study.

Key findings of this AREA study include the following:

- 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.

- AR cyber security will require a suite of tools and approaches to be effective. Assuming conventional Mobile Device Management / Mobile Application Management (MDM/MAM) tools or mobile security approaches can be easily extended to wearable AR solutions is both inaccurate and dangerous. MDM/MAM suites can help with some, but not all, aspects of securing AR headsets. Enterprise Mobility device certification and practices must be reevaluated to accommodate new factors and threats introduced by AR solutions.

- Augmented Reality security is a shared responsibility. There is a current tendency for stakeholders to "pass the buck" when it comes to taking ownership: device vendors say it is the job of the customer and can probably be handled by MDM applications; MDM providers have not seen enough deployments to extend their platforms for AR-unique needs, which would not be sufficient in any case; AR project teams look to Enterprise IT for guidance; and Enterprise IT and Mobility departments hesitate to open up their networks to these unconventional solutions without defined processes and practices for

certifying and managing them. It is essential that the AR community, device vendors, and enterprise stakeholders work together to understand and protect against the new cyber threats enabled by wearable AR headsets and smart glasses. AR security specialists should augment existing Enterprise Mobility and security teams and create a methodical approach to identify and mitigate risks to enterprise assets and operations. Stakeholders should initiate coordinated studies to instill cyber security elements early into AR proofs-of-concepts and pilot programs, not wait until right before production roll-outs.

Securing the enterprise that contains AR wearables is a shared responsibility.

FIGURE 4-2: AR security is a shared responsibility. Ecosystem cooperation is required.

A methodical approach to identify and mitigate risks to enterprise assets and operations is a must.

- AR devices are tightly linked to the environment in which they operate, and 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 even when powered down. This data can include detailed 3Dmaps 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.

- In order to exploit the many benefits of establishing remote connectivity with AR systems, wearable AR applications will require access to data stored in public / private / hybrid cloud computing environments, 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, can present complicated challenges for secure user authentication because they are easily observed and can potentially be spoofed by cyber criminals.

- It is essential that the AR community, device vendors, and enterprise stakeholders work together to understand and protect against the new cyber threats enabled by wearable AR headsets and smart glasses. AR security specialists should augment existing Enterprise Mobility and security teams to create a comprehensive, methodical approach for identifying and mitigating risks to enterprise assets and operations.

- Finally, this report is only a preliminary step in the direction of a comprehensive security framework and practical test protocol for AR solutions in enterprise environments. Recommendations for follow-on opportunities are presented, below. Ecosystem cooperation in continuing to build out these tools will prove invaluable for facilitating more near-term deployments.

SECTION 5 - RECOMMENDATIONS FOR FURTHER STUDY

- The research behind these reports will continue and the framework and test protocol will evolve and strengthen. The AREA study team encourages every reader to go to the following survey link and provide their own perspective on the topic. All roles and levels of experience are needed in order to refine the models and processes:

  https://www.surveymonkey.com/r/ARSecurity

- The focus of this study was primarily on cyber security characteristics and threats related to the head-worn device, itself, and did not touch in any detail on the other critical communication and computing elements comprising a complete “AR solution stack” (e.g. the wireless network, the cloud, data analytics and reporting applications, etc.). Follow-on studies should expand the security review across all relevant components of the AR solution stack to provide a comprehensive and complete analysis.

- Similarly, this study did not evaluate other essential aspects of a comprehensive security strategy such as setting security policies, procedures over time, training, competence of utilization, or maturity models, which should be topics for future study.

- It is difficult to create meaningful AR solutions without Cloud access. Effort should be invested to develop recommendations and best practices for storing data and applications for AR experiences locally on the device, on-premise at the user’s facility, and remotely in the cloud.

- One major challenge to implementing AR projects in the enterprise is IT’s lack of understanding and mistrust of data security aspects of these solutions. In order to promote rapid proliferation in the enterprise, business unit managers and AR pilot program leaders should be provided with a structured data security analysis guideline and planning template created by the AREA. The reporting template would be a key element in AR business cases required by management in order to fund projects. By proactively and methodically characterizing cyber security elements of their proposed AR solutions, project leads could specifically report on attributes of highest concern to Enterprise IT and executives. The result would be faster communication, review, and decision-making on whether, and how, to proceed.

- Energy should be focused on evaluating the applicability and effectiveness of popular desktop and mobile antivirus, antispyware, antimalware utilities for use on AR headsets. Determine configuration parameters and optimization.

- Thorough evaluation of the capabilities and limitations of leading Enterprise Mobility Management platforms should be conducted so a clear understanding can be developed of how these important software tools can provide security support, and where they fall short.

- In cooperation with AR device vendors and enterprise owner/operators, a full suite of leading wearable enterprise AR headset solutions should be evaluated in detail using the new AREA AR Security Framework and Test Protocol. Results should be documented and published to help guide member selection of devices for various applications. Results would support further hardening and usability of the Framework and Protocol.

Appendix A – List of References

Request for Proposals: Wearable Enterprise AR Cyber Security Risks and Mitigation. Sponsored by the AREA. Jan 2017.

AR Security Landscape Interview - Preliminary Report: Insights, Perspectives and Opportunities from AREA Members. Survey of AREA Member perspectives regarding AR cyber security; member-exclusive report. Feb 2016.

Good Technology announces support for wearables and connected devices. PR-Newswire release. Mar 2015.

User Experience Design for Enterprise Augmented Reality. AREA Technical Report. Nov 2016.

VMware AirWatch Adds Industry's First Unified Solution for Smart Glasses Management for Augmented and Mixed Reality Experiences. Press release by VMware. Oct 2016.

Appendix B - Literature Review

To gain insight regarding the risks to enterprise data security from mobile, wearable AR systems, a collection of white papers, academic research papers and industry articles were reviewed. A few key examples include the following:

Tractica Enterprise Wearable Technology Case Studies
https://www.tractica.com/resources/white-papers/enterprise-wearable-technology-case-studies-2016/

> This white paper presents a diverse range of real-world case studies for enterprise wearables, classified by vertical market, to provide a flavor of the level of enterprise wearable activity currently taking place and opportunities being created for the future. The white paper covers the enterprise wearable technology market and case studies in automotive, construction, corporate wellness and insurance, field services, food industry, medical and healthcare, logistics and distribution, manufacturing, mining, oil, and gas, retail and marketing, and transportation, travel, and hospitality markets. Devices covered include smart AR glasses, voice-controlled headsets or clip-on devices, smart watches, body sensors, wearable cameras, fitness trackers, and other devices.

An End-to-End Security Architecture to Collect, Process and Share Wearable Medical Device Data
https://web.njit.edu/~rohloff/papers/2015/Rohloff_Polyakov_Healthcom_2015.pdf

> This paper addresses embedded wearable medical devices, noting that the data from these devices is both very private and highly vulnerable to theft. It posits that data needs to be collected from multiple devices to improve the effectiveness of treatment and that the medical devices, data processing sites and intended caregivers are often geographically distributed. They also operate on different time scales, with collected data being aggregated for days or months before analysis and usage. It posits that current approaches to data security do not provide a framework for end-to-end protection, where data can be encrypted but still used effectively. This paper presents a security architecture with end-to-end encryption that supports 1) secure collection of data from embedded medical devices, 2) protected computing on this data in low-cost commodity cloud environment and 3) restricts access exclusively to designated recipients. The basis of the architecture comes from recent advances in lattice encryption technologies, leveraging recent breakthroughs in Homomorphic Encryption (HE) and Proxy Re-Encryption (PRE) that would practically support specific data aggregation, processing and distribution needs of a secure medical data architecture.

Security Use Cases
http://www.jot.fm/issues/issue_2003_05/column6/

The premise of this paper is that focusing exclusively on use cases to help define security requirements for a system limits the effectiveness of those requirements and usually results in specification of security architectural mechanisms (e.g. the use of user identifiers and passwords) rather than actual security requirements (e.g. mandating some level of identification and authentication). The distinction is crucial. For example, a use case approach evaluating automatic teller machines might include initial interactions for inserting an ATM card to identify the customer and entering a PIN number. A resulting security requirement might then reasonably include scanning the card and validating the PIN for authenticity. This approach unnecessarily precludes the use of other, perhaps improved means of access control such as biometrics (e.g. face recognition, fingerprint analysis, or retinal scan).

Utilizing use cases to analyze security threats is highly effective, but using them exclusively is inappropriate for thorough specification of security requirements. Two concepts are discussed: “Integrity” (the extent to which an entity ensures that its data and communications are not intentionally corrupted) and “Access Control” (the extent to which an entity controls access by its external human users and applications; consists of identification, authentication, and authorization). The paper documents example paths through a highly-reusable essential security use case that specifies access control requirements.

Warehouse Security Best Practice Guidelines Customs-Trade Partnership Against Terrorism
http://www.iwla.com/assets/1/6/IWLABestPractices.pdf

This paper presents best practices and a framework for warehouse security developed by the International Warehouse and Logistics Association (IWLA). Its Security Plan addresses the following components:

- Physical Security
- Standard Operating Procedures
- Personnel Security & Training
- Visitors
- IT Security
- Customer Evaluation

IoT Security: How to Protect Connected Devices and the IoT Ecosystem
http://www.engineering.com/IOT/ArticleID/12554/IoT-Security-How-to-Protect-Connected-Devices-and-the-IoT-Ecosystem.aspx

> According to AdaptiveMobile, a mobile network security company, up to 80 percent of connected devices on the IoT do not have the security measures they need to protect users. This paper notes that human interactions with all IoT devices is not scalable: humans can not be there to hit "Okay" for an update or to manually override a processes. IoT has a diverse number of devices, operating systems and protocols making it hard to consolidate and standardize as companies grow and products change. The article discusses differences between IoT and Cloud security, and proposes that IoT security is a shared responsibility between the various entities in control of the system, applications, and development tools at the various vendor, customer and public levels. Defining roles for each of user type is critical, and dividing the system into protected subsystems helps protect against hacker compromises. Secure, controlled provisioning and decommissioning of each device is essential, as is understanding where all data will reside and who owns and controls the data. Program leaders must strive to manage the complex interactions between devices and users, find ways to patch security updates to devices in an easy and secure fashion, and mitigate cyber attack risks by preventing them from finding connected devices in the first place.

Key Challenges for the Industrial Internet of Things (IIoT)
https://www.tripwire.com/state-of-security/featured/5-key-challenges-for-the-industrial-internet-of-things-iiot/

This article addressed IIoT with several perspectives that can potentially be applied to AR wearable devices. It notes that the final control components (controllers, sensors, actuators, etc.) that bridge the cyber-physical space are still based on technologies that are not common within most IT architectures. The most fundamental challenges involved with IIoT today is the different set of device capability available to manufacturers and process control operations, with many solutions and opportunities for machine-to-machine interconnectivity and communications. When deploying these technologies considerations include what information is being collected and how the information is stored and accessed.

1. Settle on device capability requirements.
2. Maintain the integrity of the supply chain.
3. Consider how to integrate cyber threat protection solutions into the network.
4. Work together and break down silos between different disciplines and departments.
5. Traditional IT cyber security is not sufficient. Collaborate.

The 5 Steps to an IIoT-Ready Industrial Network
http://www.belden.com/blog/industrialsecurity/Industrial-Networking-5-Steps-to-Benefitting-from-the-IIoT.cfm

This paper presents five steps that enterprises can take to help ensure that their industrial networks benefit from IIoT-based manufacturing and process control applications, noting that all of the steps revolve around ensuring that communications infrastructures are secure:

1. *Assess and Map Industrial Networking Infrastructure* - Early-on in assessment, enterprises need to make sure they know what they have, where it is, what it does, and who owns and manages it. In a large system, enterprises can save time and effort by using Network Management Software (NMS).
2. *Migrate / Update to Ethernet* - Make Ethernet the foundation of communications infrastructure and to upgrade bandwidth, memory, switches and routers to support it. For existing components such as sensors, actuators and electric motors that communicate using fieldbus, plan migration to Ethernet.
3. *Update Network Design for Scalability and Security* - A well organized and segmented network is essential for scalability and security. ISA IEC 62443 (formerly ISA 99) best practices explain how to divide up a network into zones of devices with similar cybersecurity requirements and protect them with appropriate conduits.
4. *Protect Reliability and Resiliency with Defense in Depth* - The majority of industrial cybersecurity incidents are unintentional, resulting from human error, device flaws, and accidental malware introductions. Good network segmentation with security conduits contributes to Defense in Depth, as do many other measures. Defense in Depth practices are essential for high system reliability and resilience.
5. *Monitor for Changes, Anomalies and Malware* - Technology changes, which means the network will change. Therefore, enterprises must make a plan which calls for regular maintenance, constant network monitoring and system failure alerts. In addition, incident response protocols need to be established.

Secure Association of Internet of Things
https://eprint.iacr.org/2015/940.pdf

This paper posits that existing standards for networked low-power wireless devices (ZigBee and Bluetooth Low Energy) do not support secure pairing of new devices into a network and are vulnerable to man-in-the-middle attacks. This paper addresses three essential aspects for pairing such devices:

- User-interface functionality which allows users to approve authentic associations and abort compromised ones. The paper distills and generalizes several existing approve/abort mechanisms.
- New Message Recognition Protocol (MRP) allows devices associated using “oblivious comparison” to exchange authenticated messages without the use of public-key cryptography (which exceeds the capabilities of many IoT devices).
- Robust definition of security for MRPs that is based on universal composability.

On the security and privacy of Internet of Things architectures and systems
https://www.slideshare.net/manishaluthra94/on-the-security-and-privacy-of-internet-of-things-architectures

> A plethora of security and privacy challenges need to be addressed for the IoT to be fully realized. In this paper, the authors identify and discuss properties that constitute the unique security and privacy challenges of the IoT. They also construct requirements induced by the aforementioned properties. The authors survey the four most dominant IoT architectures and analyze security and privacy components with respect to the requirements. Their analysis shows a mediocre coverage of security and privacy requirements.

Study of Mobile Devices - US Dept of Homeland Security with the National Institute of Standards and Technology (NIST).

https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf

This report covers the use of use of mobile devices by the U.S. Federal Government. It categorized the global mobile ecosystem into a threat model organized along clear lines of logical function that follows industry roles. This report addresses each element of the ecosystem with sections providing a detailed summary of the greatest threats in each area as well as current mitigations and defenses:

- Mobile device technology stack, including mobile operating systems and lower level device components
- Mobile applications
- Networks (e.g., cellular, Wi-Fi, Bluetooth) and services provided by network operators
- Device physical access
- Enterprise mobile services and infrastructure, including mobile device management, enterprise mobile app stores and mobile application management

The report identifies a framework for modeling mobile threats to assist in the identification of attacker tactics and techniques, which in turn informs areas where current mitigations fall short of protecting mobile devices and information. This report also provides an analysis of emerging threats that are likely to happen based on past trends in crime, the general evolution of cellular network attacks, and advances in academic and public sector security research.

Appendix C – 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

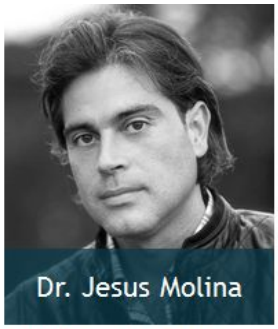
- 100 years of experience
- Leadership in global standards
- Hundreds of projects
- Government and industry network

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