The Feasibility of Wearables in an Enterprise Environment

And

Their Impact on IT Security

Vincent Scotti Jr.[1]
Florida Institute of Technology, Melbourne, FL, 32904

This paper is intended to explore the usability and feasibility of wearables in an enterprise environment and their impact on IT Security. In this day and age, with the advent of the Internet of Things, we must explore all the new technology emerging from the minds of the new inventors. This means exploring the use of wearables in regards to their benefits, limitations, and the new challenges they pose to securing computer networks in the Federal environment. We will explore the design of the wearables, the interfaces needed to connect them, and what it will take to connect personal devices in the Federal enterprise network environment. We will provide an overview of the wearable design, concerns of ensuring the confidentiality, integrity, and availability of information and the challenges faced by those doing so. We will also review the implications and limitations of the policies governing wearable technology and the physical efforts to enforce them.

[1] IT Security Specialist II, IT Security, IT-B-II, Kennedy Space Center.

Nomenclature

Android Wear	=	*Google IOS Interface connecting Smartphones with wearables*
AO	=	*Authorizing Official*
API	=	*Application Programming Interface*
Apps	=	*Applications*
ATO	=	*Authorization To Operate*
Attacker	=	*A person or system trying to gain unauthorized access to a system*
BYOD	=	*Bring Your Own Device*
C&A	=	*Certification & Accreditation*
DaR	=	*Data at Rest*
DiT	=	*Data in Transit*
ECDH	=	*Elliptic Curve Diffie-Hellman*
FIPS	=	*Federal Information Processing Standards*
Compromise	=	*An event for which an attacker has tried or succeeded in gaining access to the system*
FISMA	=	*Federal Information Security Management Act of 2002*
HOST	=	*Any computer that has full two-way access to other computers on the Internet.*
Incident	=	*A violation of computer security, acceptable use, or standard computer security policies*
IoT	=	*Internet of Things*
IOS	=	*mobile operating system created and developed by Apple, presently powers many of the company's mobile devices*
LED	=	*Light Emitting Diode*
Legacy	=	*often implies that the system is out of date or in need of replacement*
MDMS	=	*Mobile Device Management System*
NIST	=	*National Institute of Standards and Technology*
Organization	=	*An entity of any size, complexity, or positioning within an Institutional structure*
PEnE	=	*Policy Enforcement Engine*
Piconet	=	*A small Bluetooth network created on an ad hoc basis that includes two or more devices.*
PII	=	*Personal Identifying Information*
PIN	=	*Personal Identifying Number*
RISK	=	*A measure of the extent to which an entity is threatened by a potential circumstance or event*
RMF	=	*Risk Management Framework*
RoT	=	*Root of Trust*
RTI	=	*Root of Trust for Integrity*
RTM	=	*Root of Trust for Measurement*
RTR	=	*Root of Trust for Reporting*
RTS	=	*Root of Trust for Storage*
RTV	=	*Root of Trust for Verification*
Safeguards	=	*Protective measures prescribed to meet the security requirements for an Information System*
SAR	=	*Security Assessment Report*
SDLC	=	*System Development Life Cycle*
Smart	=	*Having advanced circuitry, wireless connectivity and independent processing capability*
Smartwatch	=	*A wearable device which connects to Smartphone using Android Wear IOS Interface*
SP	=	*Special Publications*
SSP	=	*System Security Plan*
Threat	=	*Any circumstance or event with the potential to adversely impact organizational operations*
Vulnerability	=	*A weakness in a computer system which allows an attacker to reduce a system's information assurance*
Wearable	=	*Being worn for an extended period of time, with the user experience significantly enhanced as a result*
Wearable Technology	=	*Includes Smartwatches, Smartbands, Smartglasses, Smart jewelry, and Smart earbuds*

I. Introduction

THIS Study will focus around the LG G Smartwatch (Model #W100) and is the beginning of a series of studies to evaluate the different wearables and their impact in the Federal enterprise network environment and the associated security implications. With the advent of the Internet of Things and the push for enterprise environments to allow Bring Your Own Device (BYOD) on the network, it is only appropriate to study the impact and effect of wearables in such an environment. The need for this study is driven by the ever changing landscape of personal communication technology and the need to generate a best practices approach to using the wearables in an enterprise network environment. These best practices and the knowledge gained by evaluating the technologies used by the LG G Smartwatch will drive the IT Security practices and policies going forward to secure the enterprise network environment while simultaneously allowing the use of the LG G Smartwatch in such an environment. Smartwatches use Bluetooth to interface with Smartphones to connect with the outside world. Users do not realize Smartwatches are actually small GPS-enabled computers using applications (apps) housed on the Smartphone which allow the user to make phone calls, text, tape conversations, and take pictures. This drives the requirement to look at wearables in the enterprise network environment closely and develop a broader enterprise Mobile Device Management Plan.[2]

II. LG G Smartwatch

The LG G Smartwatch (henceforth referred to as "Smartwatch") is one of the first in a long line of new Smartwatches commonly known as wearables. It is a stylish Smartwatch with features which can ensure everyday tasks such as setting reminders, creating schedules, reading emails, and screening calls are easily accomplished. Some of the many things you can accomplish with the Smartwatch are as follows[3]:

Accomplish Tasks:

- Set alarms, timers and reminders
- Take notes
- Check your schedule
- Take a photo
- Record a conversation

Fitness Tracker:

- Set and keep track of fitness goals
- Track your step count per day/week/month
- Track your calorie count

Use Google:

- Check the weather
- Check sports scores
- Check Google for information or quick answers
- Get directions with Google Maps

Text Messages:

- Read and reply to emails
- Read and reply to text messages
- Screen incoming calls
- Send pre-written text messages to unanswered calls

Travel:

- GPS turn by turn navigation
- Airport flight status
- Get traffic info
- Get latest news alerts

[2] (Trend Micro, 2014)

[3] (LG, 2014)

The preceding is a partial list of the everyday tasks you can accomplish with the Smartwatch which can be expanded by downloading third party applications (apps) to your Android Smartphone. To use the Smartwatch, you must have an Android Smartphone running a 4.3 Android operating system or higher and the Smartphone must have Bluetooth enable. The Smartwatch (as well as every other Smartwatch) uses Bluetooth to connect with the Smartphone.

Connection is accomplished by downloading Google's Android Wear app from the Google Play Store[4]. The Google Wear app is essentially another operating system running on top of the Android Smartphone operating system. Once you download the Wear app and follow the installation instructions, you will see a list of nearby devices and the Smartwatch should be one of them if the app is installed correctly.

Once you select your Smartwatch from the list, you will be instructed on how to pair the device to the Smartphone. When you opt to pair the Smartwatch to the Android Smartphone, you will receive a pairing code on both the Smartwatch screen and the Android Smartphone screen. When you touch both screens, you will receive a confirmation message telling you that the pairing has completed successfully. You will now be able to use your LG G Smartwatch and the last step is to download any updates that the Smartwatch alerts you to being available.

Once the updates are installed, the next step is to configure the Smartwatch to take advantage of all of its features. This is done partly by turning on Google Now and Location, which enables the Smartwatch to use Google as its source of information for look ups using the Google Now feature. You would turn on Google Location to use GPS directions, local suggestions (like restaurants and traffic) and Maps. Lastly, you would turn on contact recognition to call, text or email your personal contacts stored on your Android Smartphone.

III. Google Android Wear Application

The Smartwatch uses Google's Android Wear Operating system. This operating system is what makes the Smartwatch work in connection with the Android Smartphone. The purpose of this Android Wear is to give you access to the same information on your Smartphone but without the hassle of searching for it. By having access to the information on your wrist, you can take a quick look at the Smartwatch to see the information in a fraction of the time it would take you to see the same information on your Smartphone.

Android Wear uses a type of what they call "Style Cards". Each of these cards contains different information and you pick which information you want to see by tapping the screen or swiping the cards either up, left or right depending on what you are trying to accomplish[5]. For example:

- Touch screen to wake up Smartwatch
- Tap on screen and say "OK Google", when OK Google appears, ask Google a question or give command
- Swipe the card from left to right to dismiss the card you don't want
- Swipe up from bottom of screen to view cards
- Swipe from right to left to see more information
- Swipe down half way to see remaining battery life
- Swipe down all the way to mute or unmute the vibration effects

Some of the things you can do with the Google Android Wear Operating system are as follows[6]:

- Make voice memos
- Use voice search (Google)
- Start navigation
- Control music
- Set reminders
- Track flights
- Track fitness
- Make calls using voice command
- Get reminders
- Get GPS support (turn by turn navigation)

[4] (LG, 2014)
[5] (LG, 2014)
[6] (Andriod, 2014)

- Track weather
- Check commuting times
- Play music offline
- Respond to email, text and instant messages by voice

These are just some of the apps installed by default when you pair your wearable device with your Android Smartphone using the Google Android Wear Operating system. This then allows you to download other third party apps made for wearable devices to expand the functionality of your Smartwatch. These third party apps allow you to play games, listen to music, read books, check flights, track fitness and health, check weather, check for availability of Wi Fi networks, record conversations, and take photos.[7] To date, there are 252 Wearable Apps on the Google Play Store with more being developed every day. Smartwatches are the second most popular wearable today with 5 percent of consumers planning to buy one in the next year and 23 percent planning to purchase one within the next 5 years[8]. This shows that the wearable Smartwatch is going to be a real concern when it comes to the implementation of policies and BYOD programs in an enterprise environment.

IV. Third Party Wearable Applications

A. Google

Google makes some of the most popular apps that are in use today. Apps like Gmail, used to check email, or Google Maps, used for directions to a destination, are by far some of today’s most used apps. Most of us do not even think of them as apps because we use them every day in our lives. Now with Google designing the Google Wear OS, these apps are going to be available on Android wearable devices. See the list of Google Apps below:

- Gmail: Gmail is built on the idea that email can be more intuitive, efficient, and useful. Gmail also lets you manage multiple accounts, view and save attachments, and set up label notifications.
- Google+: Google+ is a free app where you can explore ideas, connect with people, and share your interests. You can also find content using the search box, trending hashtags, what’s hot, and more. Simply follow someone you’re interested in to get their posts in your home stream.
- Google: The fastest, easiest way to find what you need on the web and on your device. Use your voice to quickly search the web on your Smartphone or tablet to get personalized results based on your location.
- Hangouts: Hangouts is a Communications app that lets you send and receive messages, photos and more; even start free video and voice calls — one-on-one or with a group!
- Maps: The Google Maps app for Android Smartphones and tablets makes navigating your world faster and easier. Find the best spots in town and the information you need to get where you want to go using voice activated GPS Navigation including live traffic conditions, incident reports and automatic rerouting to find the best route for your traveling needs.
- Google Keep: Speak a voice memo on the go and have it automatically transcribed. Grab a photo of a poster, receipt or document and easily find it later in search. Quickly capture what’s on your mind and get a reminder later at the right place or time for yourself. You can also share it with friends and family.
- Google Camera: Google Camera captures quick and easy photos and videos, and takes advantage of your Android device's computing power with image enhancing features like HDR+, Lens Blur, Wide Angle, Panorama and Photo Sphere. Control the camera from a distance using Android Wear.

B. Other Third Party Developers

Applications developed for BYOD by third party developers are at the same time a driving force in the use of wearables and a major concern for IT Security professionals. The developers are called on to develop apps which can drive the use for a technology to be accepted by the public at large. This is substantiated by the fact that there are more than 1.3 million Android apps in the Google Play Store and a similar number in the Apple App Store[9]. Going forward there will be a need to develop a policy similar to the Apple Store to ensure the apps on the Google Play Store live up to a set of standards. Apple’s App Store has a process by which they evaluate the app for usefulness, presentation,

[7] (Google, 2014)

[8] (acquitygroup,LLC, 2014)

[9] (Casey, 2014)

non-conforming content (this is open to debate, see website for more info), and intellectual property. If your app is rejected for one of the preceding reasons, Apple even has a review board for you to appeal your rejection.[10]

C. Applications Pros

As stated above, between the Google Play Store and the Apple App Store there are more than 2.6 million apps developed between the Android and IPhone platforms. With the advent of wearables and the Internet of Things, this is only going to increase. This brings us to one very big pro, Jobs. Since 2008, Apple has downloaded 75 million apps to users[11]. This means users will buy apps they think will make their life easier. Gartner has predicted users will have downloaded 268 billion apps by 2017[12]. This means that apps are going to be a driving force in the adoption of any new technology in the future. Since apps can make for a fast, mobile workforce which is not tied down to a desk, it will and should increase productivity.

D. Applications Cons

The applications developed for BYOD by third party developers are at the same time a driving force in the use of wearables and a major concern for IT Security professionals. The fact is anyone, from a developer working for a major corporation to a college student working in his parent's basement, can develop these apps and have them published on application market squares like Google Play and other app Stores which is a major security concern. The concern stems from the Google Play policies, which do specify what is an acceptable app in regards to appropriate content like: No hate speech, sexually explicit material, violence or bullying, impersonation or deceptive behavior to name a few, but do nothing to verify the developer themselves as being reputable[13]. This can cause a problem with allowing attackers to develop apps which look harmless, but have installed a backdoor or other Trojan horse like virus to steal data or credentials and use the device they are installed on to phone home with the information.

E. Business Enablers

The case can be made for wearables to be a business enabler due to the fact that by design the wearables make for a more agile workforce by allowing them to check and respond to messages while driving without having to pick up their Smartphone. Another business enabler would be the availability to read emails and get notifications of meetings by way of vibrations to notify you of an impending scheduled meeting or a new incoming email or message. This means the users will be more in contact with their daily schedule by way of alerts or vibrations making it hard to miss a notification. The last business enabler would be the reduced cost to the CIO or Owner of the enterprise environment by allowing the use of BYODs and by design, the advent of wearables. The Owners and CIOs could cut programs related to supplying mobile devices to employees and the cost of refreshes every couple of years saving them large sums of money. Gartner predicts that by 2017 half of all employers will require employees to use BYODs for work.[14] But this will only work with a sound BYOD policy and management plan in conjunction with the infrastructure to support a mobile workforce.[15]

F. Security Concerns

There are just as many security concerns about wearables as there are reasons for implementing them in the enterprise environment. But one good thing is they can be managed by the same BYOD policies and management programs. Some of the questions that need to be answered are as follows:

- Is there a need to connect or support wearables within the enterprise environment?
- What education will be needed for employees on the particulars of wearable IT Security?
- Should mobile devices connected to wearables be allowed access to enterprise data and applications?
- Should wearables be classified as less secure devices and considered separate from Smartphones?

[10] (Apple Inc., 2014)
[11] (Casey, 2014)
[12] (Gartner, 2014)
[13] (Google, 2014)
[14] (Gartner, 2013)
[15] (Casey, 2014)

- Do existing policies for mobile devices address any of the above issues concerning enterprise data?
- Do BYOD policies or management programs have the ability to include the wearable technology?
- Are there legal issues concerning the manageability of wearable devices?
- How much end user evaluation/input is needed for the consideration, development or testing of wearable apps?
- Which wearable platform to support Apple? Android? Or both?
- What will be the best way to deploy apps and updates to OS and apps? Will it be possible?
- How would the organization track the usage of wearables in an enterprise environment? Is it possible?
- Since it uses Bluetooth, should you allow enterprise data on a wearable Smartwatch?

These are all legitimate concerns when dealing with any new technology, but with the advent of wearables, you have to wonder if technology is moving too fast for the adopters to realize. With the advent of the Internet of Things, new avenues are going to open up for new devices and the need for new security controls or policies. There has been a buzz phrase of late in the IT Security community, IT is the "Holistic Approach" to IT Security. This means you can no longer look at just the firewall and password policies and expect to secure your network. Now you must look at the whole picture. This means we have to look at not only Smartphones, but Smartwatches, Smartglasses and who knows what else in the future.

We can't expect to keep all technology out of the enterprise environment, but we have to take a look at the whole picture to see how we can or if we can develop a management plan and policies to keep up with this new technology and at the same time secure the enterprise environment.

V. Computer Security

Computer security is a section of Information Technology known as information security as it is applied to computers and computer networks. The purpose of computer security includes protection of information and property from theft, corruption, or natural disaster, while at the same time allowing the information and property to remain accessible and useful to its intended users. Computer system security is the combined processes and mechanisms by which sensitive and valuable information or services are protected from exploitation, tampering or destruction by unauthorized activities instituted by untrustworthy or even authorized individuals or unplanned events respectively. The strategies and methodologies of computer security, known as best practices outlined in the NIST[16] Special Publications documents or Defense in Depth[17] Methodology, often differ from most other computer technologies because of its somewhat elusive objective of preventing unwanted computer behavior instead of enabling wanted computer behavior.

Both of these methodologies use the risk management method when designing a computer system life cycle, which should be applied to all computer systems. The better the design and the earlier in the process, the easier it is to implement the best practices or methods. The System Design Life Cycle[18] design process starts with:

1. Initiation Phase: What is the need for the system?
2. Development or Acquisition Phase: The system is designed, bought, developed, and constructed.
3. Implementation Phase: System security is configured and enabled.
4. Operation and Maintenance Phase: The system is put into operation with ongoing support.
5. Disposal: This is the phase where information, hardware, software may be discarded.

The disposal phase is the last phase of the risk management best practices methodology. For the purpose of this paper, the focus will be limited to the NIST Risk Management Framework and its implementation in a Federal Government environment.

A. Introduction - Why the Need for Computer Security

The need for computer security is one of the most important issues to be considered when planning on using a computer system in a Federal environment. Most people today take computer security for granted; they think by

[16] (National Institute of Standards and Technology, 2006)
[17] (Jordan, 2012)
[18] (National Institute of Standards and Technology, 2011)

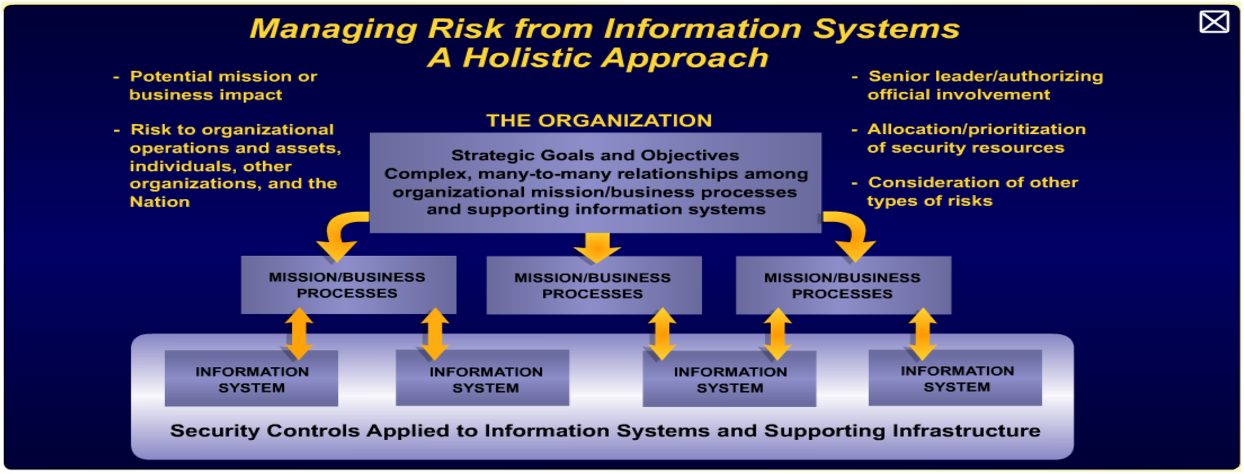
installing anti-virus software on the computer, the system will be protected. The reality is far from the truth.

Computer security must take into account the multiple threats and vulnerabilities to which computer systems are exposed. The first is the design aspect of the system. A system should be designed from the beginning with computer security in mind. By applying the NIST Risk Management Framework towards securing your system, it will ensure a better security posture.

Next is the most challenging by far: the human aspect of computer security. The human factor has to deal with people not following guidelines set forth by NIST, the host system administrator or corporate/government policies. A user not securing their password or changing their password regularly is a big problem in computer security. Another problem pertains to phishing links in an e-mail. Users can’t resist clicking on these links, even when they are expressly told not to in their yearly IT Security training.

Lastly, social engineering attacks are where attackers ask users for personal information, which to them seems harmless, but helps an attacker gain access to your system. This is a major problem with people who use social networks such as Facebook and Twitter. Hackers surf these sites looking for information, which will help them approach the user already possessing some information, asking (and getting) more, and infiltrating their computer system.

Additional challenges include the technological aspect of Computer Security. We live in a world where technology grows by leaps and bounds. Every time a company comes out with a new piece of hardware to help you secure the computer network against intrusions, there is another piece of hardware or software which enables hackers to gain access. This is a cat and mouse game in which the mouse (hackers) seems to be winning. The effort it takes to keep up with the latest technology seems insurmountable at best, which is why the role of information security risk management policy for information systems is critical to the success of an organization in achieving its strategic goals and objectives. The risk management concepts establish a relationship between aggregated risks from information systems and the mission and/or business success. The chart below shows the organizational relationship between the mission/business risk and specific information security risks.


Managing Risk from Information Systems
A Holistic Approach
- Potential mission or business impact
- Risk to organizational operations and assets, individuals, other organizations, and the Nation
- Senior leader/authorizing official involvement
- Allocation/prioritization of security resources
- Consideration of other types of risks
THE ORGANIZATION
Strategic Goals and Objectives
Complex, many-to-many relationships among organizational mission/business processes and supporting information systems
MISSION/BUSINESS PROCESSES
MISSION/BUSINESS PROCESSES
MISSION/BUSINESS PROCESSES
INFORMATION SYSTEM
INFORMATION SYSTEM
INFORMATION SYSTEM
INFORMATION SYSTEM
Security Controls Applied to Information Systems and Supporting Infrastructure

[19](Technology, National Institute of Standards and, 2013)

By taking an organizational view of risk management as in the chart above, we see:

- Potential mission or business systems impact
- Risk to organizational operations and assets, individuals, other organizations, and the nation (should the organization’s system be compromised)
- Consideration of other types of risks
- Allocation/prioritization of security resources
- Senior leadership/authorizing official involvement
- Facilitates prioritization of security requirements and allocation of information security resources
- Promotes development and dissemination of common security policies and procedures
- Increases the information security knowledge base

[19] (Technology, National Institute of Standards and, 2013)

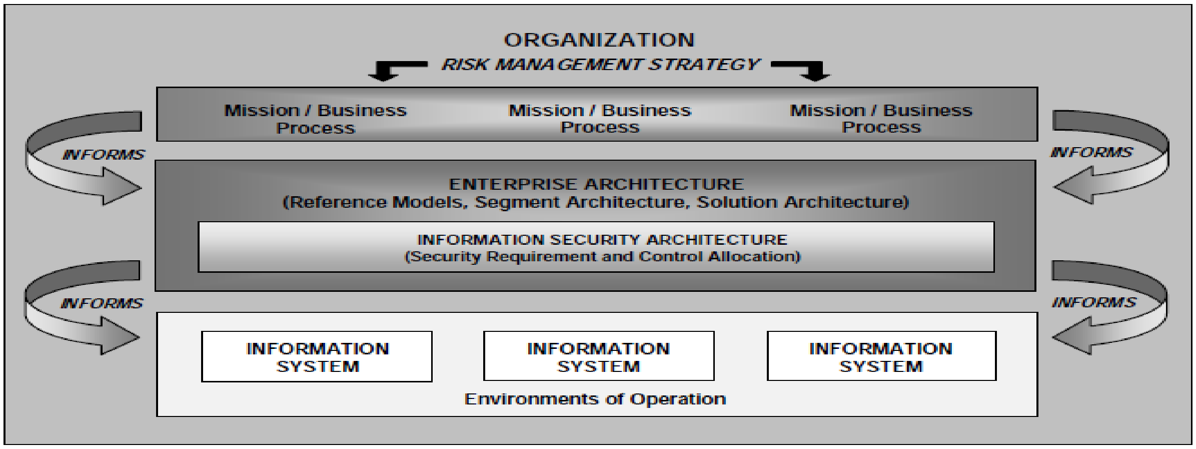
- Facilitates decisions on risk mitigation activities
- Promotes development of organization-wide solutions to information security problems
- Facilitates consolidation and streamlining of security solutions across the organization

Obviously it is very important to look at the whole picture when applying the Risk Management Framework, and that it should be a major priority right from the beginning.[20]

B. NIST: Risk Management Framework

The following section outlines the NIST Risk Management Framework and the concerns taken into account when designing and implementing the RMS on the system. There are many concerns which are not normally thought of when devising a risk management plan, unless you reference NIST Special Publication SP800-37 Rev.1: *Guide to Applying the Risk Management Framework to Federal Information Systems*.

- **Business Drivers:** Most organizations do not spend sufficient time clearly defining the critical business issues or mission drivers that create the necessity for a risk management program. These drivers must be aligned with business objectives, regulatory requirements, organization directors and executive management directives. Without such alignment, there is the potential for confusion in coordinating various agendas and communicating the overall enterprise risk vision.
- **Risk Strategy:** The risk strategy is a high-level, concise plan that articulates the vision, scope and direction for the risk management plan within the organization. The risk management plan should encompass risk tolerance guidance, risk processes, expectations for the risk management function, and the integration of risk processes such as IT Security into standard IT operations. Ideally, the risk management plan is representative of the enterprise's risk strategy and organizational charter.
- **Risk Governance:** The cornerstones of a risk management program are ownership, accountability and oversight. The risk governance aspect of a successful risk management program should include a strong executive leader, who can handle both strategic and tactical enterprise initiatives across diverse and distributed IT environments.
- **Policies and Standards:** The Risk Management Framework defines the policies, standards, and guidelines in which the organizational management can apply to the existing risk management and business IT risk functions. The decision making process should include all stakeholders to be fair to all concerned parties, while ensuring that the application and execution of all of the policies and standards are managed effectively.
- **Risk Identification and Profiling:** The NIST Special Publications SP800-39 Risk Management Framework uses a security life cycle approach to implement the System Development Life Cycle process.


ORGANIZATION
RISK MANAGEMENT STRATEGY
Mission / Business Process
Mission / Business Process
Mission / Business Process
INFORMS
INFORMS
ENTERPRISE ARCHITECTURE
(Reference Models, Segment Architecture, Solution Architecture)
INFORMATION SECURITY ARCHITECTURE
(Security Requirement and Control Allocation)
INFORMS
INFORMS
INFORMATION SYSTEM
INFORMATION SYSTEM
INFORMATION SYSTEM
Environments of Operation

[21] Information Security Requirements Integration

[20] (Technology, 2013)
[21] (National Institute of Standards and Technology, 2011)

To summarize, risk management considerations can be addressed as an integral part of the enterprise architecture by:[22]

- Developing a segment architecture linked to the strategic goals and objectives of organizations, defined missions/business functions, and associated mission/business processes;
- Identifying where effective risk response is a critical element in the success of organizational missions and business functions;
- Defining the appropriate, architectural-level information security requirements within organization-defined segments based on the organization's risk management strategy;
- Incorporating an information security architecture that implements architectural-level information security requirements;
- Translating the information security requirements from the segment architecture into specific security controls for information systems/environments of operation as part of the solution architecture;
- Allocating management, operational, and technical security controls to information systems and environments of operation as defined by the information security architecture; and
- Documenting risk management decisions at all levels of the enterprise architecture.

Enterprise architecture provides a disciplined and structured approach to achieving consolidation, standardization, and optimization of Information Technology assets that are employed within organizations. Risk reduction can be achieved through the full integration of managerial and technical processes, organization-wide, thereby providing greater degrees of security, privacy, reliability, and cost-effectiveness for the missions and business functions being carried out by organizations. The above model of risk management is based on the NIST Special Publications document SP800-39[23] Final, which is titled *Managing Information Security Risk: an "Organizational, Mission, and Information Systems View"*. This document is broken up into three levels and addresses the risk as it pertains to the organization level, the mission/business level and lastly the information system level.

C. NIST SP800-163:
Technical Considerations for Vetting Third Party Mobile Applications

Today's commercially available mobile devices (e.g., Smartphones, tablets) are technically handheld computers with wireless capabilities, geographic localization, cameras, and microphones. Similar to traditional computers such as desktops and laptops, the user experience with a mobile device is tied to both the manufacturer, vendor third party software apps, and the tools and utilities available. The purpose of this study is to provide guidance for vetting third party software apps for mobile devices. Mobile app vetting is intended to assess a mobile app's operational characteristics of secure behavior and reliability (including performance) so that organizations can determine if the app is acceptable for use in their intended enterprise environment.[24]

The purpose of this study is to encourage organizations to develop requirements and policies concerning the mobile apps to be used on the BYOD devices used by employees on the enterprise environment. This will allow the organization to verify or vet the application by testing it to see that it meets the requirements and policies set forth by the organization concerning the amount of risk they are willing to accept with the use of mobile apps. The testing configurations will include the app version, type of devices and operating systems configurations.

By developing a comprehensive mobile device management plan for the organization, they will ensure that when they deploy a new technology like Smartwatches, they will have a process by which to assess the capabilities of the new technology and its security impact to the enterprise environment. Part of this management plan is to have or develop a vetting approach to third party apps which will be repeatable, consistent and limit false results.[25]

This will allow the organization to provide a comprehensive mobile device management plan including training on how to install, configure and identify mobile apps meeting the enterprise requirements and policies. This will ensure that the apps will work as intended, while limiting the security risk usually faced by installing unvetted apps.

[22] (NIST: JOINT TASK FORCE TRANSFORMATION INITIATIVE, 2011)
[23] (NIST: JOINT TASK FORCE TRANSFORMATION INITIATIVE, 2011)
[24] (Christoph Michael, 2014)
[25] (Christoph Michael, 2014)

D. NIST SP800-124 Rev.1:
Guidelines for Managing the Security of Mobile Devices in the Enterprise

This NIST publication is designed to help organizations centrally manage and secure mobile devices, such as Smartphones and tablets. This particular document provides recommendations for selecting, implementing, and using centralized management technologies. It explains the security concerns inherent in mobile device use and provides recommendations for securing them throughout their life cycles. The scope of this NIST document includes both organization-provided and personally-owned (BYOD) mobile devices.

As with any new computer technology, no solutions should be put into production without testing it in a limited environment, like a pilot test to evaluate the device and its effects on the network environment and its security implications. This should begin with the development of a mobile device security policy, where the policy describes the types of devices allowed on the network and the resources they will be allowed to access. Since mobile devices are an inherently high threat, an analysis should be done to identify their security shortcomings and the controls needed to make them more secure when accessing the network.

The organization can then develop comprehensive mobile device solutions which should address some of the following areas:[26]

- General Policies: Develop enterprise security policies to enforce restrictions to the type of hardware, software and wireless network settings allowed when connecting to the enterprise network. Other policies would address violations of these policies by implementing monitoring, detecting and reporting procedures when the policies are violated.
- Communications Policy (Data and Storage): This policy would address the type of encryption to be used and how to store the data on mobile devices. Another concern is the procedure for remote wiping of the device if lost or stolen to prevent unauthorized access of data by unauthorized users. This would also include the wiping of the device to reissue it to another authorized user.
- Device Authentication (Device and User): Require two factor authentication for the user in addition to requiring the device to authenticate itself to the credential authority before being allowed to access the organizational network resources. Provide a means to lock or remote wipe the device in case it is lost or stolen.
- Applications: Restrict the download of apps to an approved list from approved apps stores. The approved app should have a default installation configuration with permissions restricting downloads, updates and connection to synchronization services limited to organization approved application functionality.

By developing and implementing system specific policies similar to the ones mentioned above and taking a proactive approach to BYOD by securing mobile devices and wearables. This can be accomplished by making sure the organization issues fully secured mobile devices and provides a means to protect individual personal mobile devices by ensuring they are configured and conform to the best practices and policies of the organization.

E. NIST SP800-164:
Guidelines on Hardware-Rooted Security in Mobile Devices

Today's mobile devices are taking the place of the laptops and other traditional hosts. The problem is that the mobile devices lack the hardware based "roots of trust" that are normally built into laptops and other types of traditional hosts. Mobile devices by design are not capable of providing strong security assurances to the end user.[27] This Special Publication goes on to address the roots of trust needed to provide a strong security assurance using the mobile device provided by the organization and the end users.

There are three mobile security components and three mobile security capabilities that mobile phones need to have and implement to ensure that hardware rooted security is being addressed in mobile devices. This will provide a measure of integrity in establishing a strong security assurance for the end user mobile device. The three components are Roots of Trust, Application Programming Interface, and a Policy Enforcement Engine.

The Security components and the security capabilities have to work in tandem to be effective in establishing hardware rooted security in mobile devices like Smartphones and wearables. Here is a breakdown of the security components and Capabilities:

[26] (Souppaya, 2013)

[27] (Lily Chen, 2012)

Security Components:

- Roots of Trust (RoT) – Security primitives that provide a set of trusted security-critical functions, which are comprised of hardware, firmware, and software entities which provide Roots of Trust security by design.[28]
  - Root of Trust for Integrity (RTI): Provides a protected interface, storage, and integrity protection to store and manage assertions.
  - Root of Trust for Measurement (RTM): Measurements used by the assertions protected by the Root of Trust for Integrity and confirmed by the Root of Trust for Reporting.
  - Root of Trust for Reporting (RTR): A protected interface and environment to sign assertions and manage identities.
  - Root of Trust for Storage (RTS): Provides a protected interface and repository to store and manage keying material.
  - Root of Trust for Verification (RTV): A protected interface and engine to verify digital signatures associated with firmware and software used to create assertions based on the results.
- The Application Programming Interface (API): Exposing the Root of Trust to the platform by using the Application Programming Interface to provide applications a Root of Trust by interacting with the device and the operating system to establish a chain of trust.
- Policy Enforcement Engine (PEnE): Provides a means by which policies can be managed, processed and maintained to provide the user with control over the information to ensure a level of security by accessing the configuration state of the device and applying the security policies.

Security Capabilities:

- Device Integrity: A mobile device can provide evidence (absence of corruption) that it has maintained integrity by using hardware, firmware, and software configurations to provide a device in a state to be trusted by a relying party.
- Isolation: This provides a secure environment to allow the device to separate and prevent unintentional interaction by separate users of the device.
- Protected Storage: This is provided by enabling a Data at Rest (DaR) application to ensure the integrity and confidentiality of the user's information while not in use and prevent any unauthorized access to the sensitive information when it is being accessed.

These components and capabilities allow a higher level of trustworthiness of a device by providing a baseline of security technologies that can be implemented across a wide range of devices to help secure both organization provided and personal owned devices in an enterprise environment.

F. NIST SP800-121: *Guide to Bluetooth Security*

Bluetooth is a form of radio frequency communication used to provide a method of communication to personal Smartphones, wearables, laptops, automobiles and office devices. It provides a short range of communication between devices by establishing a personal area network.[29] Bluetooth is the means by which wearables communicate with their corresponding Smartphones to which they are linked. There are many versions of Bluetooth, but for the purpose of this study, we will just call them all Bluetooth.

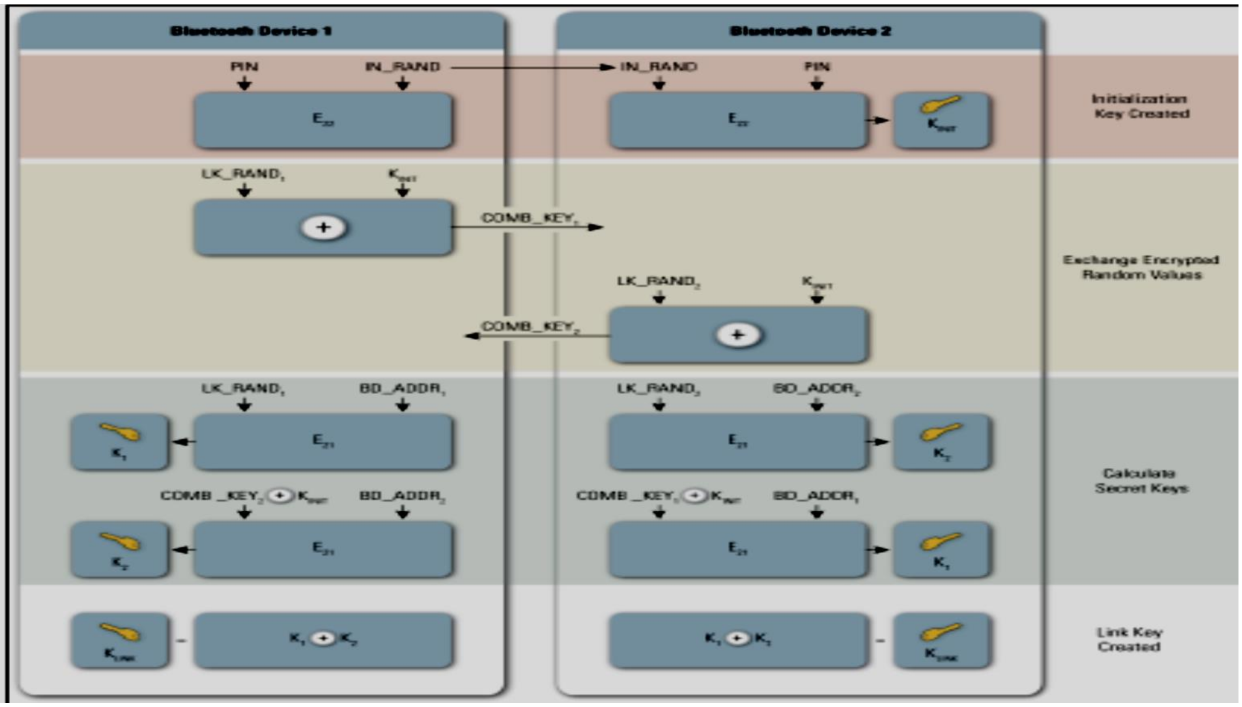
Bluetooth is the means by which the Smartwatch connects to the Android Smartphone. The connection is made by way of pairing the devices by generating a code and then entering the code into the wearable for the purpose of completing the connection process. Bluetooth has some security features which an organization should require before allowing wearables on the network. One such security feature is to require that the Bluetooth connection should be encrypted. This can be enabled at the time of setting up the connection between the Smartwatch and Android Smartphone.

[28] (Lily Chen, 2012)
[29] (Lily Chen J. P., 2012)

The highest and strongest security mode should be selected by the organization that is available for the Smartwatch and Android Smartphone pairing in question. A secret symmetric key (PIN code) is established to be used to link the two devices together. When used with a link level security mode, it will authenticate and encrypt the connection when the symmetric key is entered to complete the connection. The PIN code can vary between 1 and 16 bytes of binary and is usually 4 digits in length.[30]

Authentication of a Bluetooth device is done in the form of the challenge and response scheme. One device will act as the claimant, who is attempting to prove the identity; the other device will act as a verifier, who will validate the identity of the claimant.[31]

Below we see a figure representing the process from key generation to device pairing. After the key is generated, the devices authenticate and encrypt themselves by using the generated key. When this is accomplished the devices will then be able to communicate with each other.



[32](Lily Chen J. P., 2012)

These settings should be addressed in the organization's security policies and should be changed to reflect these policies. Part of developing the policies for the use of Bluetooth is to address user awareness to the shortcomings of Bluetooth security and the user's responsibilities regarding their use of Bluetooth enabled devices.[33]

Even addressing these issues will not totally protect the Bluetooth from vulnerabilities or attacks. By now we know that no system can be fully protected. However we can make them secure enough to deter the attacker by making the time it takes to perpetrate an attack unacceptable.

G. DoD Bluetooth Peripheral Device Security Requirements

This document from the NSA website[34] specifies requirements necessary for the secure use of unclassified Bluetooth peripheral devices in the U.S. Department of Defense. The NSA has broken down the guidance into Basic, Connectivity, Authorization, Pairing and Authentication, and lastly Encryption requirements.

[30] (Lily Chen J. P., 2012)
[31] (Lily Chen J. P., 2012)
[32] (Lily Chen J. P., 2012)
[33] (Lily Chen J. P., 2012)
[34] (National Security Agency, 2013)

Basic Requirements:[35]

- Devices must use easily-understandable connection, configuration, and link activity status indicators like LEDs or icons.
- Devices must only support the minimum number of Bluetooth services required for operational use of approved Bluetooth peripherals. Services should be enabled only while needed. Devices or administrators must reliably disable or delete all unneeded Bluetooth services.
- Devices or administrators must reliably disable or delete all unneeded Bluetooth user controls, drivers, application programming interfaces, executables, and applications.
- Devices must use random number values and public/private key pairs that achieve maximum entropy for all cryptographic functions as mandated and defined in the Bluetooth specifications and based on applicable NIST guidelines

Connectivity Requirements:

- Discoverability - Bluetooth devices must not be discoverable unless absolutely necessary and never for more than two minutes at a time. Best case, the devices should never be discoverable.
- Connectability - Bluetooth devices must not be connectable unless absolutely necessary. Devices should initiate Bluetooth connections only when absolutely necessary. Best case, only one device per Bluetooth piconet should initiate connections to other devices in that piconet and the devices should become unconnectable once the connection is established or disable the connection function, if possible.
- Auto-Reconnect - Page frames from devices attempting to automatically re-establish Bluetooth links to peripheral devices must be transmitted periodically and not continuously. The time for reconnect frames should be limited to 30 seconds at any one time, frequency of no more than once every 5 minutes with a 20 minute total limit overall.

Authorization Requirements:[36]

- User must authorize all incoming Bluetooth connection requests before allowing any incoming connection request to proceed after being prompted by device. Users must never accept connections, files, or other objects from unexpected, unknown, or untrusted sources.

Pairing and Authentication Requirements:[37]

- General Pairing and Authentication Requirements - recommend when establishing the initial Bluetooth connection requests, all Bluetooth devices must pair (mutually authenticate) and store the resulting link key, which must be stored securely based on applicable NIST guidance. All Bluetooth pairing should be done as infrequently as possible, prior to establishing a new link, Bluetooth devices must again mutually authenticate each other during all connection requests. Users or administrators must never enter or confirm pairing passkeys when unexpectedly prompted by device. Best case, when pairing is in a secure location away from windows and behind physical access controls where attackers cannot realistically observe entry of the passkey or intercept transmitted pairing messages. Bluetooth devices must use either legacy pairing Security Mode 3 link level security or Secure Simple Pairing Security Mode 4 service level security and unused, lost, stolen, or discarded Bluetooth devices must be removed immediately from the paired device lists by the user or administrator to protect integrity.
- Legacy Pairing Requirements – require Bluetooth 2.0 and earlier devices must use Security Mode 3 link level security, legacy pairing must not use or accept unit keys and must use combination keys for link key establishment, must use completely random Bluetooth passkeys at least eight digits in length that are newly generated for each pairing exchange.
- Secure Simple Pairing Requirements – This recommends Bluetooth 2.1 and later devices should use the Passkey Entry SSP association model. Bluetooth devices supporting SSP must use Elliptic Curve Diffie-Hellman (ECDH) public/private key pairs that are unique for each device and must originate from a trusted source, devices must store SSP ECDH public/private key pairs securely and Host protocol stacks in devices using Security Mode 4 must be sufficiently robust to prevent denial of service and other attacks based on anomalous frames

[35] (NSA: Systems and Network Analysis Center, 2011)
[36] (NSA: Systems and Network Analysis Center, 2011)
[37] (NSA: Systems and Network Analysis Center, 2011)

Encryption Requirements:[38]

- ➢ All Bluetooth Devices must initiate Bluetooth encryption immediately(Links must use 128 bit Bluetooth Encryption) after the successful completion of mutual authentication.

H. MaaS360: Mobile Device Management System

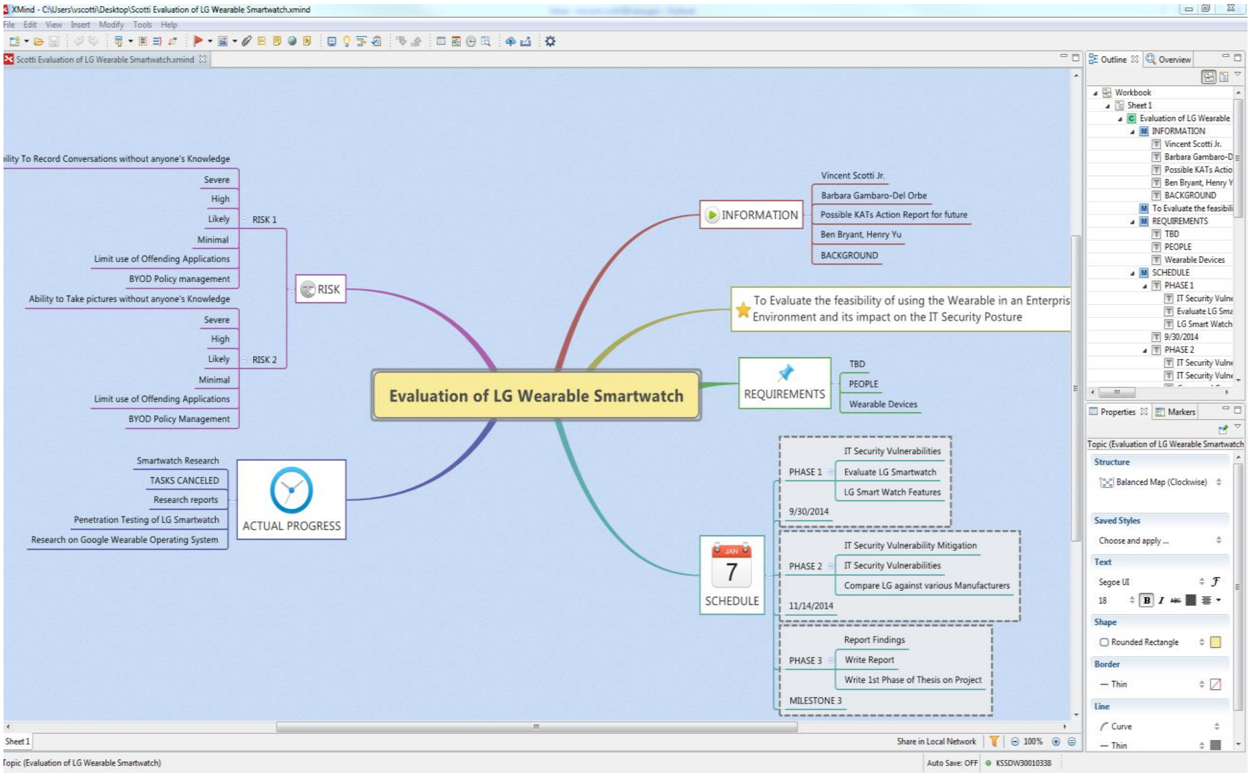
The MaaS360 mobile device management system is used to provide big business and government a way to enable mobile devices on their network, while at the same time provide a way to make the devices compliant and tractable. A mobile device management system should be easy to administer. Some of the questions to consider when developing policies for BYOD are as follows:[39]

- ➢ What mobile devices will be allowed on the network?
- ➢ What regulations and policies cover the data being accessed by the devices?
- ➢ What security measures are needed?
- ➢ What applications will be allowed and which ones will be forbidden?
- ➢ What network services will be accessible by the device?
- ➢ How will employee privacy be protected?

MaaS360 allows the administrator to set up policies, track, and remotely wipe the device if lost or stolen. It provides a way to back up the device and keep track of its usage. It also provides a way to separate the user's personal data from organizational network data by means of a sandbox to secure and separate the two.[40]

As of this time, MaaS360 has no way of tracking wearables, but is working on the issue. I was informed of this from a MaaS360 Webinar I attended in December and was the answer to a question I posed to the presenter of the webinar on the functionality of the MaaS360 mobile device management system.

I. Images, Figures, and Tables


XMind - C:\Users\vscotti\Desktop\Scotti Evaluation of LG Wearable Smartwatch.xmind
File Edit View Insert Modify Tools Help
Scotti Evaluation of LG Wearable Smartwatch.xmind
Evaluation of LG Wearable Smartwatch
RISK
RISK 1
ility To Record Conversations without anyone's Knowledge
Severe
High
Likely
Minimal
Limit use of Offending Applications
BYOD Policy management
RISK 2
Ability to Take pictures without anyone's Knowledge
Severe
High
Likely
Minimal
Limit use of Offending Applications
BYOD Policy Management
ACTUAL PROGRESS
Smartwatch Research
TASKS CANCELED
Research reports
Penetration Testing of LG Smartwatch
Research on Google Wearable Operating System
INFORMATION
Vincent Scotti Jr.
Barbara Gambaro-Del Orbe
Possible KATs Action Report for future
Ben Bryant, Henry Yu
BACKGROUND
To Evaluate the feasibility of using the Wearable in an Enterpris
Environment and its impact on the IT Security Posture
REQUIREMENTS
TBD
PEOPLE
Wearable Devices
JAN
7
SCHEDULE
PHASE 1
IT Security Vulnerabilities
Evaluate LG Smartwatch
LG Smart Watch Features
9/30/2014
PHASE 2
IT Security Vulnerability Mitigation
IT Security Vulnerabilities
Compare LG against various Manufacturers
11/14/2014
PHASE 3
Report Findings
Write Report
Write 1st Phase of Thesis on Project
MILESTONE 3
Sheet 1
Share in Local Network
100%
Topic (Evaluation of LG Wearable Smartwatch)
Auto Save: OFF
KSSDW30010338
Outline
Overview
Workbook
Sheet 1
Evaluation of LG Wearable
INFORMATION
Vincent Scotti Jr.
Barbara Gambaro-D
Possible KATs Actio
Ben Bryant, Henry Y
BACKGROUND
To Evaluate the feasibili
REQUIREMENTS
TBD
PEOPLE
Wearable Devices
SCHEDULE
PHASE 1
IT Security Vulne
Evaluate LG Sma
LG Smart Watch
9/30/2014
PHASE 2
IT Security Vulne
IT Security Vulne
Properties
Markers
Topic (Evaluation of LG Wearable Smartwatch)
Structure
Balanced Map (Clockwise)
Saved Styles
Choose and apply ...
Text
Segoe UI
18
Shape
Rounded Rectangle
Border
Thin
Line
Curve
Thin

[38] (NSA: Systems and Network Analysis Center, 2011)
[39] (MaaS360 by fiberlink, an IBM company, 2014)
[40] (MaaS360, 2014)

VI. Conclusion

In Conclusion, I was very pleased with the use of the Smartwatch and the way it enhanced the way I approached my day. It was very refreshing not having to pick up my phone every time it rang or I received a notification of an email or text. All I had to do was look at the Smartwatch to read the email or text on the screen, answer or discard a call with the swipe of a finger. This made it very easy to keep my concentration on my work. The Smartwatch is also very useful in travel situations by allowing you to receive turn by turn directions on the screen or check the status of a flight by flipping through the cards on the screen. I used this when I attended a conference in New Orleans, where it made catching my connecting flights or getting to the airport from the hotel very simple and stress free.

I also used the Smartwatch to take pictures and record presentations at the conference without having to navigate my phone apps or screen by just tapping on the screen and asking Google to start the recording or take a picture using my phone camera on my hip. This allowed me to keep my hands free to help students at the conference. Another important application on the Smartwatch is the weather app, it can be set to give you weather notifications, which can be very important in Florida with their lightning storms.

There is so much more that the Smartwatch can do with the advent of the additional apps being developed for wearables on a daily basis. Wearables are going through a renaissance, they are being developed by more companies and the technology is progressing by leaps and bounds. From all the reading I have been doing and the research I have completed, I see wearables being the next big issue for government network environments. I recently read that BMW is developing an app, which would allow you to park your BMW with your wearable Smartwatch and the technology built into the automobile.

That being said, there is also a security concern with the integration of any new technology into the government network environment. When you have a new technology being deployed where you have no policy or security controls in place, it causes concerns for all parties. With any new technology, it should be rolled out in a limited capacity to be studied and evaluated to discover the vulnerabilities and to develop a policy and mitigation strategy. The biggest vulnerability I see are the apps that can be used by the Smartwatch and Android Smartphones. The apps should be evaluated before being allowed on the network. The good thing about the Smartwatch is it is paired to an Android Smartphone, which can be part of the BYOD mobile device management plan and by proxy controlled with some of the same policies and security features provided by the MDMS.

This technology is going to be a driving force in policy development for both the Federal and private sector to keep up with the new technology and its features. I see this being a big drain on IT resources or a big benefit to the IT Budget depending on the stance the organization takes in the adaption of this new technology we call the Smartwatch or more precisely wearables.

Acknowledgments

I would like to thank Ben Bryant and Henry W. Yu for selecting me and allowing me the time and latitude to evaluate this new technology at my own pace to get a good look at its potential and the possible security concerns which always arise with the advent of new technology. I also want to thank Barbara Gambaro-Del Orbe for working with me to clarify any questions or concerns I had with the directions of this paper. I also want to thank Annmarie Keim, who helped me with the research.

Bibliography

acquitygroup,LLC. (2014, Aug. 18th). *The Internet of Things: The Future of Consumer Adoption: ACQUITY GROUP'S 2014 INTERNET OF THINGS STUDY.* Retrieved from www.acquitygroup.com: http://www.acquitygroup.com/docs/default-source/Whitepapers/acquitygroup-2014iotstudy.pdf?sfvrsn=0

Andriod. (2014, Dec. 5th). *Andriod Wear*. Retrieved from Andriod: http://www.android.com/wear/

Apple Inc. (2014, Dec. 9th). *App Store Review Guidelines*. Retrieved from developer.apple.com: https://developer.apple.com/app-store/review/guidelines/

Casey, K. (2014, Sept. 11th). *Computer Associates:HDI.* Retrieved from Every Business is a mobile Business: http://www.ca.com/us/~/media/Files/whitepapers/ca-hdi-every-business-is-a-mobile-business.pdf

Christoph Michael, S. Q. (2014, Aug. 18th). *NIST SP800-163: Technical Considerations for Vetting 3rd Party Mobile Applications (Draft).* Retrieved from NIST Special Publications: http://csrc.nist.gov/publications/drafts/800-163/sp800_163_draft.pdf

Gartner. (2013, May 1st). *Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes*. Retrieved from Gartner: Newsroom: http://www.gartner.com/newsroom/id/2466615

Gartner. (2014, Jan. 22nd). *Gartner Says by 2017, Mobile Users Will Provide Personalized Data Streams to More Than 100 Apps and Services Every Day*. Retrieved from Gartner: Newsroom: http://www.gartner.com/newsroom/id/2654115

Google. (2014, Mar. 28th). *Google Play Developer Program Policies* . Retrieved from Google Play: https://play.google.com/about/developer-content-policy.html

Google. (2014, Dec 9th). *Wearable Apps*. Retrieved from Google Play Store: https://play.google.com/store/search?q=wearable%20apps&c=apps&docType=1&sp=CAFiDwoNd2VhcmFibGUgYXBwc3oCGACKAQIIAQ%3D%3D&hl=en

Jordan, S. (2012, Nov. 16th). *SANS Institute InfoSec Reading Room.* Retrieved from www.SANS.org.

LG. (2014, Dec. 9th). *Mobile Product support:W100 Owners Manual.* Retrieved from LG: http://www.lg.com/us/support-mobile/lg-W100#

Lily Chen, J. F. (2012, October 23rd). *SP800-164: Guidelines on Hardware-Rooted Security in Mobile Devices (Draft).* Retrieved from Computer Security Division Information Technology Laboratory: http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf

Lily Chen, J. P. (2012, June 24th). *NIST: SP-800-121 Rev.1- Guide to Bluetooth Security.* Retrieved from NIST: Computer Security Division: Computer Security Resource Center: http://csrc.nist.gov/publications/nistpubs/800-121-rev1/sp800-121_rev1.pdf

MaaS360. (2014, Feb. 6th). *MaaS360: The ten Commandments of BYOD.* Retrieved from MaaS360: http://content.maas360.com/www/content/wp/wp_maas360_mdm_tenCommandments.pdf

MaaS360 by fiberlink, an IBM company. (2014, Feb. 7th). *Mobile Device Management:Your Guide to the Essentials and Beyond.* Retrieved from MasS360: http://content.maas360.com/www/content/eb/ebook_mdmEssentials.pdf

National Institute of Standards and Technology. (2006, Feb. 10th). *SP800-18 Rev.1 Guide for Developing Security Plans for Federal Information Systems.* Retrieved from NIST: Computer Security Division- Computer Security Resource Center: http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf

National Institute of Standards and Technology. (2012, Feb. 6th). *SP800-39:Managing Information Security Risk.* Retrieved from NIST:Computer Security Division Information Technology Laboratory: http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

National Security Agency. (2013, July 11th). *Information Assurance/Mitigation Guidence/Security Configurations Guides/Wireless Guides.* Retrieved July 4th, 2015, from National Security Agency: https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/wireless.shtml

NIST: JOINT TASK FORCE TRANSFORMATION INITIATIVE. (2011, Mar. 3rd). *NIST: SP-800-39: Managing Information Security Risk.* Retrieved from NIST: Computer Security Division- Computer Security Resource Center: http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

NSA: Systems and Network Analysis Center. (2011, April 15th). *DoD Bluetooth Peripheral Device Security Requirements.* Retrieved July 5th, 2015, from NSA:: https://www.nsa.gov/ia/_files/wireless/BluetoothDoc.pdf

Souppaya, M. (2013, June 24th). *SP 800-124 Revision 1:Guidelines for Managing the Security of Mobile Devices in the Enterprise.* Retrieved from NIST: Computer Security Division- Computer Security Resource Center: http://dx.doi.org/10.6028/NIST.SP.800-124r1

Technology, N. I. (2013, Nov. 26th). *NIST: Computer Security Division- Security resource Center.* Retrieved from http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/rmf-training: http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/rmf-training/index.html

Technology, National Institute of Standards and. (2013, Nov. 26th). *http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/rmf-training.* Retrieved from www.NIST.gov: http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/rmf-training/index.html

Trend Micro. (2014, Jan. 14th). *BLURRING BOUNDARIES:2014 Security Predictions for Small and Midsize Businesses.* Retrieved from Trend Micro: http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp01_threat_predictions_smb_140127.pdf