ARA Process Example

An Annex of the Cybersecurity Architectural Risk Analysis Process White Paper

May 2017

Alliance for Telecommunications Industry Solutions

Abstract

This annex includes an illustrative application of the Architectural Risk Analysis (ARA) Process to a hypothetical fitness service delivered as a managed service provided by an ICT Service Provider. The example is based on the WearFit example created by the IEEE Center for Secure Design.

Foreword

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information about ATIS and opportunities to participate in ATIS initiatives, please visit www.atis.org.

Published by

Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005

Distributed under Creative Commons BY-SA License

This document is distributed under a Creative Commons BY-SA license (< http://creativecommons.org/licenses/by-sa/3.0/legalcode >).

This license allows you to share (copy and redistribute) and adapt (remix, transform, and build upon) the content of this document, as long as you comply with the following terms:

Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may use any reasonable citation format, but the attribution may not suggest that the authors or publisher has a relationship with you or endorses you or your use.

"ShareAlike" — If you remix, transform, or build upon the material, you must distribute your contributions under the same BY-SA license as the original. That means you may not add any restrictions beyond those stated in the license, or apply legal terms or technological measures that legally restrict others from doing anything the license permits.

PLEASE NOTE THAT NO WARRANTIES ARE GIVEN REGARDING THE CONTENT OF THIS DOCUMENT.

Derogatory use of the content of this license to portray the authors, contributors, or publisher in a negative light may cancel the license under Section 4(a). This license may not give you all of the permissions necessary for a specific intended use.

This document contains information from "Avoiding The Top 10 Software Security Design Flaws," which was published by the IEEE Center for Secure Design document. This document is available here: < https://www.computer.org/cms/CYBSI/docs/Top-10-Flaws.pdf >.

Table of Contents

1 ARA Process Example 1

1.1 IEEE Center for Secure Design – WearFit: Security Design 1
1.2 WearFit Overview 1
1.3 WearFit Security Objectives 6
1.4 WearFit Use Cases 8
1.5 WearFit Architectural Diagrams 8
1.6 WearFit Threat Model 11
1.7 WearFit Abuse Cases 21
1.8 WearFit Risk Analysis and Mitigation 23

Table of Figures

Figure 1.1: IEEE Resources and WearFit 1
Figure 1.2: WearFit Design Example 2
Figure 1.3: WearFit Attack Categories, Part 1 3
Figure 1.4: WearFit Attack Categories, Part 2 4
Figure 1.5: WearFit Attack Categories, Part 3 5
Figure 1.6: WearFit Security Objectives 6
Figure 1.7: WearFit Security Objectives Details 7
Figure 1.8: Service Provider Managed WearFit Starting Point Assets 8
Figure 1.9: Architectural Diagram for WearFit Example 9
Figure 1.10: WearFit Use Case Asset Representation 10
Figure 1.11: Service Provider Managed WearFit Threat Model Scope 11
Figure 1.12: WearFit Device Threat Landscape 12
Figure 1.13: WearFit Device Target Tree 13
Figure 1.14: WearFit Device Weight and Path Metrics 14
Figure 1.15: WearFit Device Target Tree Inferences 15
Figure 1.16: WearFit Data Threat Landscape 16
Figure 1.17: WearFit Data Threat Landscape (cont.) 17
Figure 1.18: WearFit Data Target Tree 18
Figure 1.19: WearFit Data Weight and Path Metrics 19
Figure 1.20: WearFit Data Target Tree Inferences 20
Figure 1.21: WearFit Abuse Case Example 21
Figure 1.22: WearFit Abuse Case Traceability Matrix Example 22
Figure 1.23: WearFit Risk Mitigation, Summary of Analysis 23

1 ARA Process Example

This annex includes an illustrative application of the Architectural Risk Analysis (ARA) Process to a hypothetical fitness service delivered as a managed service provided by an ICT Service Provider. The example is based on the WearFit example created by the IEEE Center for Secure Design. The original WearFit solution description is used here, unmodified, to consider its delivery in a Software as a Service (SaaS) format.

1.1 IEEE Center for Secure Design – WearFit: Security Design

This clause provides a high-level example of the ARA Process, thus enabling the reader to see key steps of the process applied to an actual solution. The solution selected is called the WearFit solution, a fictional product and system that is documented by IEEE as part of a threat modeling exercise.

1.2 WearFit Overview

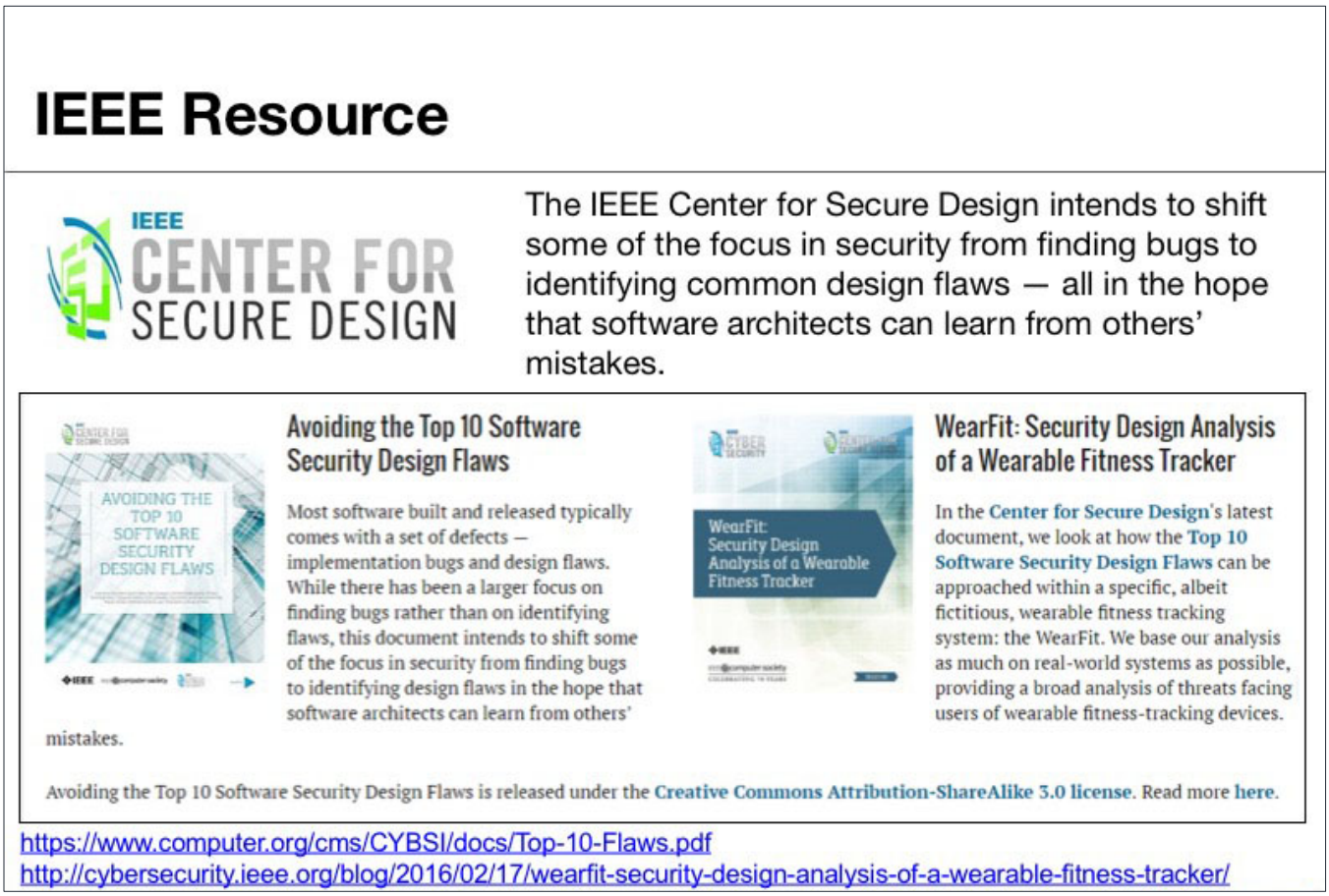

Figure 1.1: IEEE Resources and WearFit

The IEEE Center for Secure Design is an initiative in Cyber Security of the IEEE Computer Society. Information is available online at < http://cybersecurity.ieee.org/center-for-secure-design/ >. Two documents published on the website proved useful in the development and review of the ARA Process. The documents are "Avoiding the Top 10 Software Security Design Flaws" and "WearFit: Security Design Analysis of a Wearable Fitness Tracker." These documents are distributed by IEEE under a Creative Commons BY-SA license.

ARA Process Example

The ten common software security flaws are summarized here. The "Avoiding the Top 10 Software Security Design Flaws" paper describes each in detail and offers guidance to avoid flaws in design and implementation:

1. Earn or give, but never assume, trust.
2. Use an authentication mechanism that cannot be bypassed or tampered with.
3. Authorize after you authenticate.
4. Strictly separate data and control instructions, and never process control instructions received from untrusted sources.
5. Define an approach that ensures all data are explicitly validated.
6. Use cryptography correctly.
7. Identify sensitive data and how it should be handled.
8. Always consider the users.
9. Understand how integrating external components changes your attack surface.
10. Be flexible when considering future changes to objects and actors.

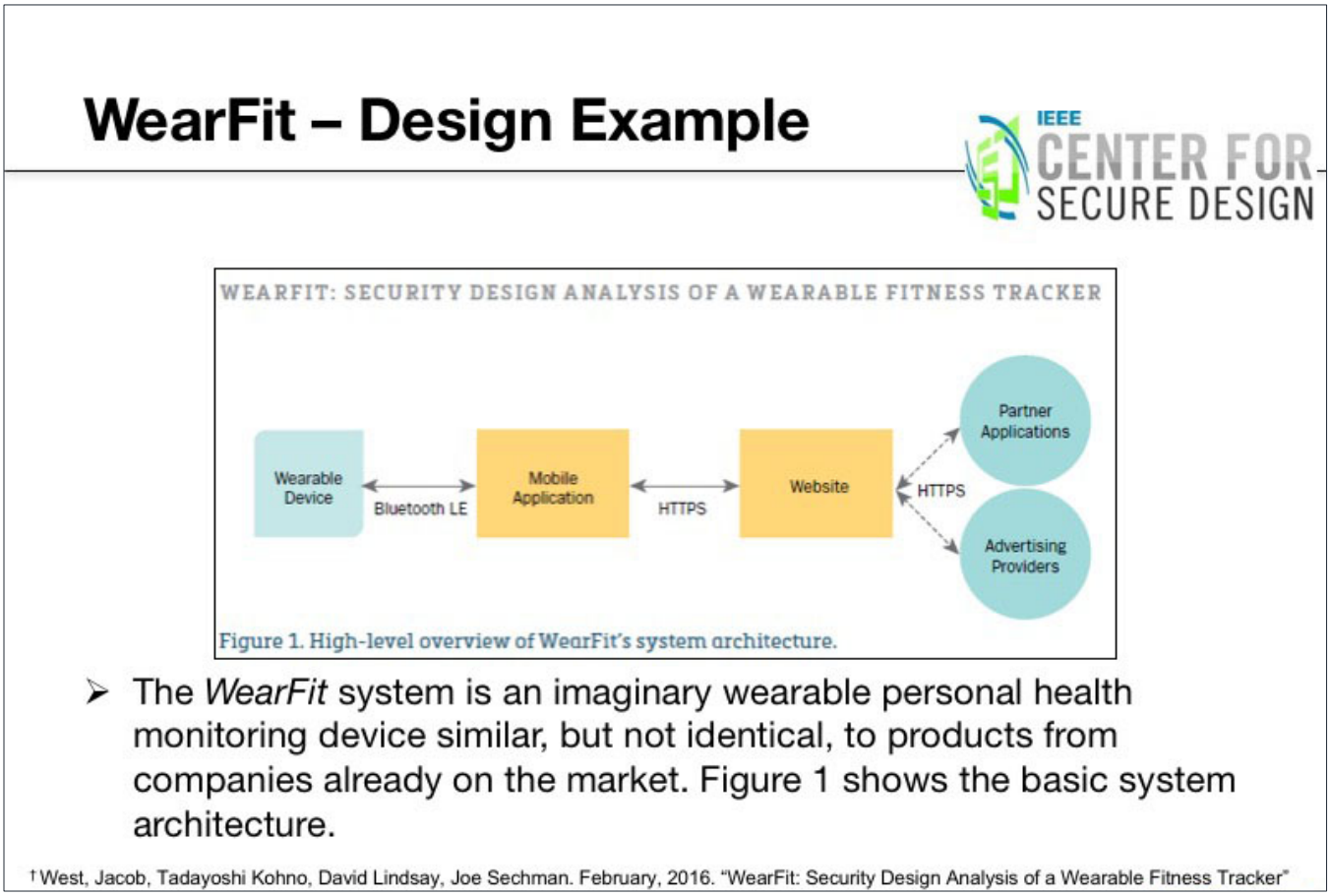

Figure 1.2: WearFit Design Example

The WearFit solution is a wearable fitness tracker similar to many fitness devices available on the market today. The solution consists of the wearable device, a mobile application resident on a smart phone or tablet, an associated web-site in a cloud that interacts with the mobile application over an Internet connection, and various partner applications connected over the Internet to the WearFit website. The wearable device connects to the mobile device over a Bluetooth LE interface.

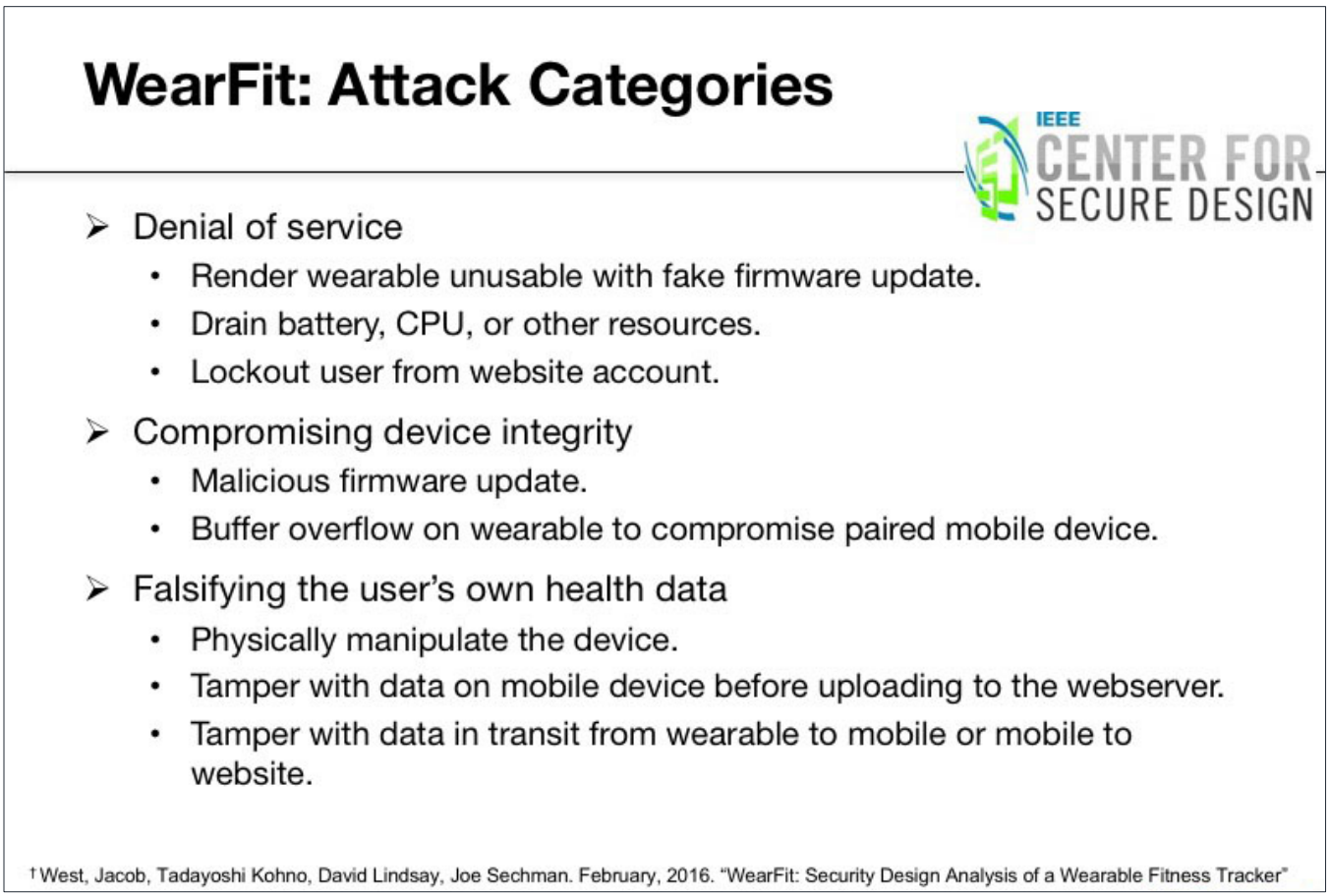

Figure 1.3: WearFit Attack Categories, Part 1

Six categories of attacks are presented in "WearFit: Security Design Analysis of a Wearable Fitness Tracker." Denial of service, compromising device integrity, and falsifying the user's own health data are presented here with additional details of each. The detailed sub-bullets are similar to abuse cases an attacker may use in attempting to compromise the WearFit solution.

WearFit: Attack Categories-part 2

IEEE CENTER FOR SECURE DESIGN

- Falsifying another user's health data
  - Rewrite health data on device.
  - Tamper with data on a mobile device when used as a passthrough.
  - Spoof data uploads using a known device or user identifier.
  - Tamper with data in transit from wearable to mobile or mobile to website.
  - Direct attacks against the website (for example, SQL injection).
  - Phishing, cross-site request forgery (CSRF), and other indirect attacks against end users.
- Abusing health data that are intentionally shared
  - Employer or insurer penalizes behavior seen through WearFit Corporate Benefits.
  - Users of the WearFit Social System unintentionally view sensitive activities.
  - Advertising partners target over-personalized ads.
  - Share configuration that becomes out-of-sync with changes in real-world relationships.

† West, Jacob, Tadayoshi Kohno, David Lindsay, Joe Sechman. February, 2016. "WearFit: Security Design Analysis of a Wearable Fitness Tracker"

Figure 1.4: WearFit Attack Categories, Part 2

Falsifying another user's health data and abusing heath data that are intentionally shared are two additional attack categories presented here.

WearFit: Attack Categories-part 3

- Stealing a user's health data
  - Guess or steal a user's authentication credentials.
  - Direct attacks against the website (for example, SQL injection).
  - Eavesdrop on communication on mobile device when used as a passthrough.
  - Eavesdrop on communication from wearable to mobile or mobile to website.
  - Malicious insider uses internal, or otherwise "privileged," access.
  - Phishing, CSRF, and other indirect attacks against end users.
- Observations:
  - The analysis presented in the IEEE paper is similar to the ATIS process concepts except for the lack of detailed diagrams.
  - Functional descriptions are provided which is similar to Use Case analysis.
  - The threats seem well thought out based on common industry threats and abuse cases.
  - The top 10 list (avoid part) serves as a general reference to security controls.

† West, Jacob, Tadayoshi Kohno, David Lindsay, Joe Sechman. February, 2016. "WearFit: Security Design Analysis of a Wearable Fitness Tracker"

Figure 1.5: WearFit Attack Categories, Part 3

The final attack category, stealing a user's health data, is presented here. The Security Design Analyses presented in the paper use similar approaches as defined in the ARA Process with the major exception that it lacks detailed diagrams that clarify the solution architecture and data flows.

1.3 WearFit Security Objectives

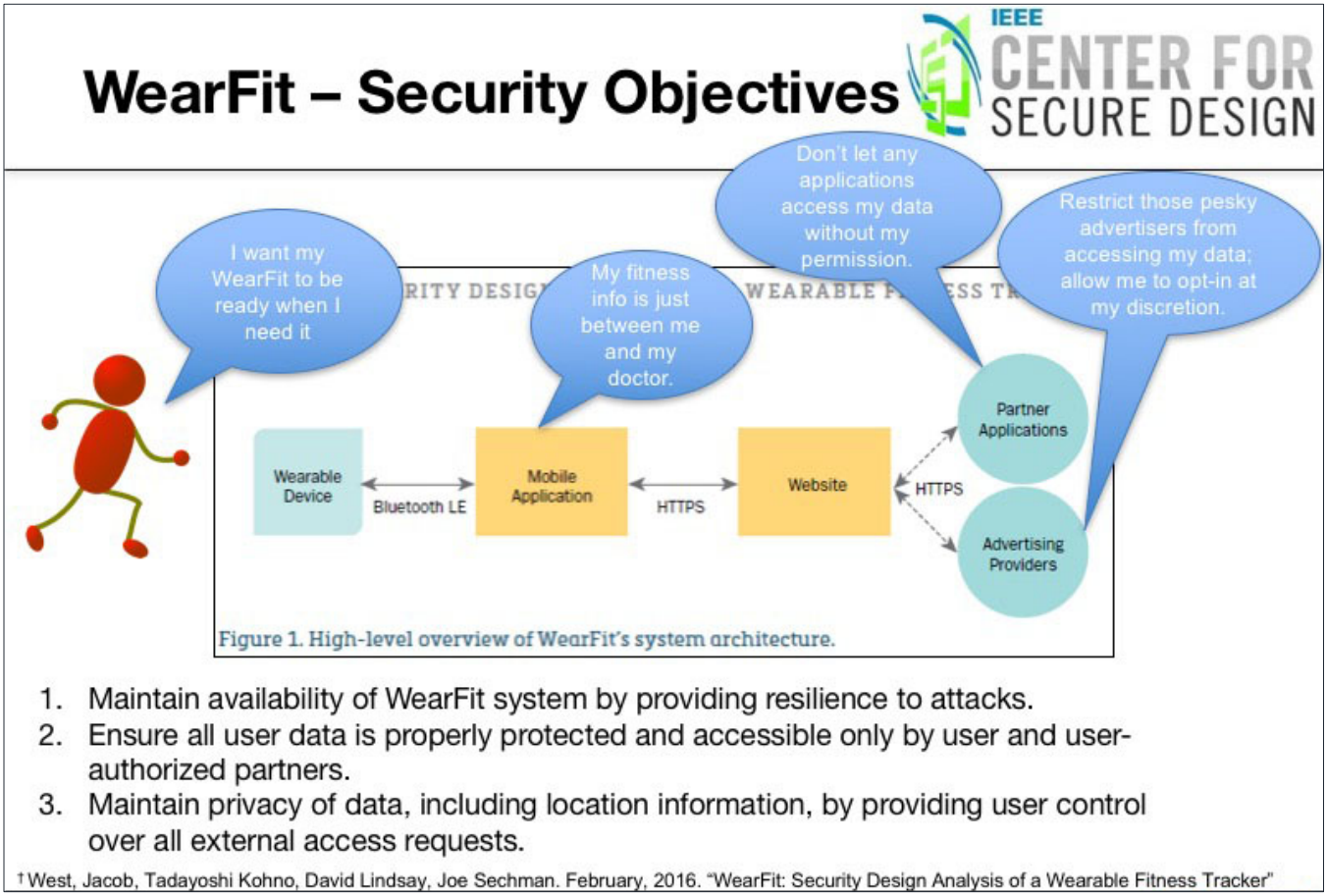

Figure 1.6: WearFit Security Objectives

The user's perspective of the WearFit solution is superimposed on the solution architecture diagram to help identify the importance of security to the consumer. Users want the solution to be available whenever they desire to track fitness activities which could be anytime day or night. Users also view the data generated, collected and stored by the WearFit solution as private health data that should be access restricted to the user and his/her doctor. Interaction with other partners should be restricted with full control being given to the user through opt-in choices.

Security Objectives - Details

1. Maintain availability of WearFit system by providing resilience to attacks.
   - Configure OS web-server to mitigate common DoS/DDoS threats.
2. Ensure all user data is properly protected and accessible only by user and user-authorized partners.
   - Employ access and authentication controls
   - Configure system to comply with least privileges principle
   - Enforce strong password management
3. Maintain privacy of data, including location information, by providing user control over all external access requests.
   - Restrict access and encryption

Figure 1.7: WearFit Security Objectives Details

Using the high-level user perspectives, three security objectives with underlying details are identified. These constitute the primary objectives that developers of the WearFit solution should address in order to satisfy the expectations of prospective customers. However, they do not represent all objectives that should be considered. From this starting point, however, other security requirements may be derived.

1.4 WearFit Use Cases

WearFit Use Case Assets

Starting Point for Threat Analysis

Category	Use Case	Potential Solution Assets														
		Inter-Component Comm.	Configuration Data	End User Data	APIs	Service/Traffic Handling	Encryption Keys	Inter-Domain Admin Procedures	NFV Components	Customer Application SW	End-User	Compute Environment	Endpoint Device	Physical Assets, Power, Cooling	Staff	Brand and Reputation
Service Provider delivered SW as a Service (SaaS)	IoT/M2M Application – Service Provider Managed WearFit	S	S	P	P	P	S			P	P		P			P

P = Primary Asset
S = Priority Secondary Asset

Figure 1.8: Service Provider Managed WearFit Starting Point Assets

The Use Cases associated with the WearFit hypothetical solution are documented as part of the IEEE WearFit material and will not be repeated here. As indicated previously, the sample application of the ARA process focuses on WearFit delivered as a service provider managed services in a SaaS context. This step begins with the selection of the IoT/M2M application use case in the service provider-delivered SaaS category as a basis for identifying the ***Primary*** and ***Priority Secondary*** assets. The items marked with a P in the figure above are the ***Primary Assets***. The template set of ***Priority Secondary Assets*** has been reduced to a subset which are relevant for service provider managed WearFit. Two of the ***Primary Assets*** – ***End User Data*** and ***Endpoint Devices*** will be further developed in the threat analysis examples which follow.

1.5 WearFit Architectural Diagrams

The WearFit Architectural Diagram depicts the assets deployed for the delivery of network services utilizing 3rd party or service provider SaaS for the WearFit hypothetical solution. Within this architectural framework, assets can be identified in both a physical and virtual context. The diagrams will attempt to visually show operational, physical or virtual areas where the ***Primary*** and ***Priority Secondary*** assets can be exposed. Figure 1.9 shows the WearFit device and its interconnection to the service provider network and SaaS hosted facilities.

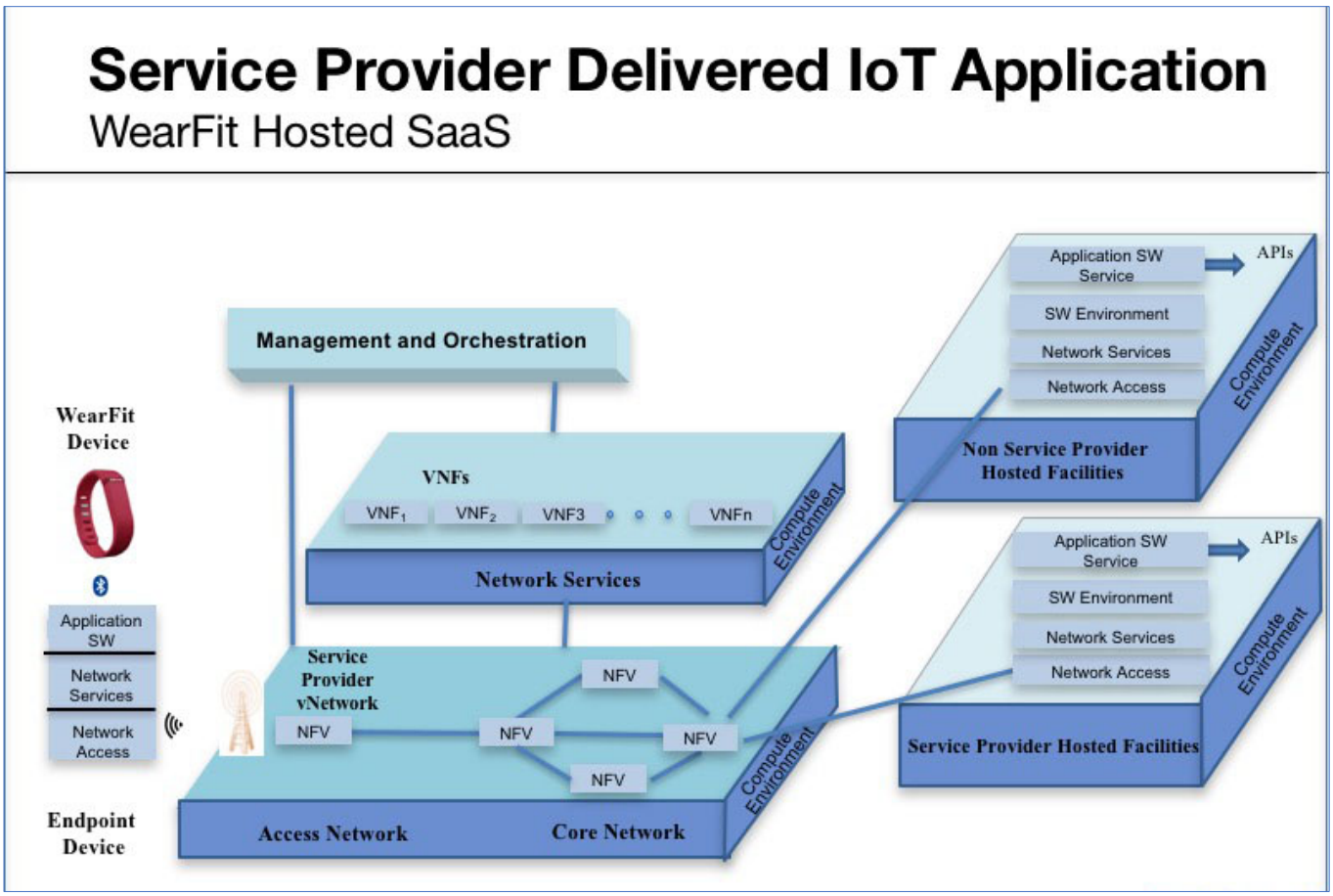

Figure 1.9: Architectural Diagram for WearFit Example

The use case demonstrating the threat analysis for the primary assets of end user data and end device(s) is reflected in the network diagram below. End user data is reflected as residing in the WearFit device, end device, and application software service function in the hosted facilities. The diagram reflects a representative implementation of WearFit and provides a reference for the primary assets that are described in the use cases selected. These assets, USD (End User Data) and EPD (End Point Device), are highlighted below.

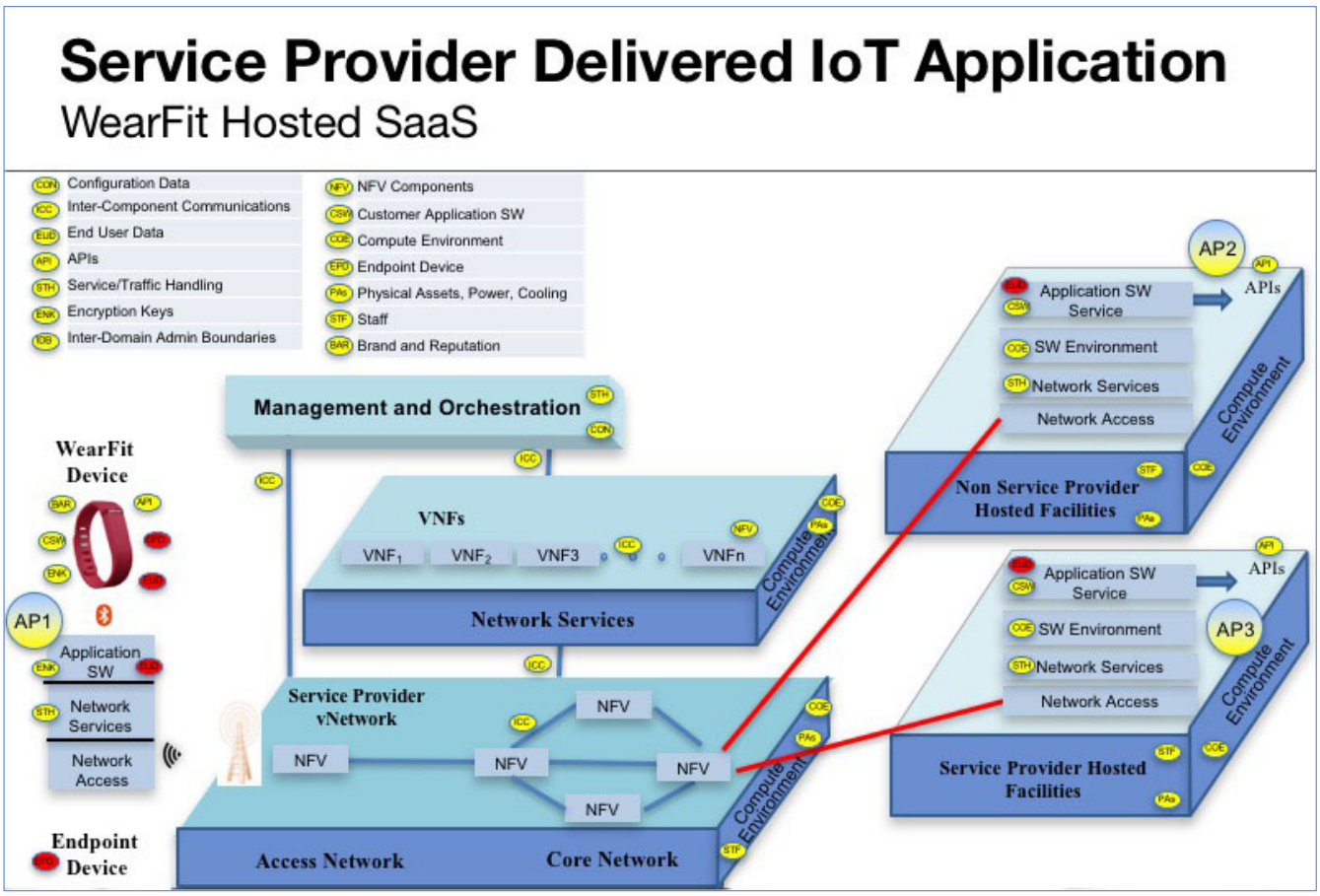

Figure 1.10: WearFit Use Case Asset Representation

1.6 WearFit Threat Model

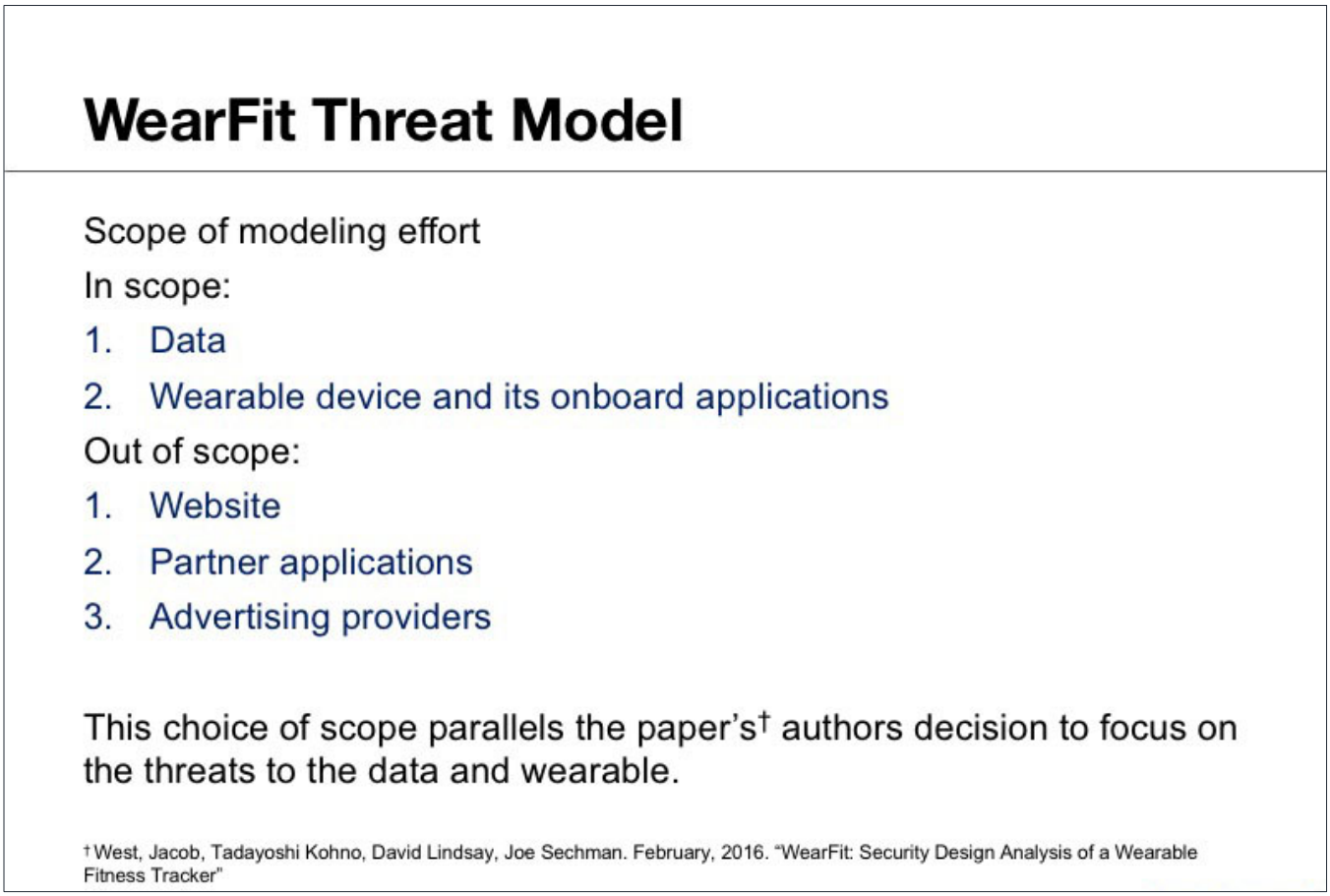

Figure 1.11: Service Provider Managed WearFit Threat Model Scope

The two assets for threat modeling are the data and the device worn by the WearFit user. This study addresses the device first, discussing the threats and the threat model built on those threats, including the metrics and inferences gleaned from them.

The threat model for the WearFit data is treated in identical manner later. The assessed threats are based on the data threat discussion in the original WearFit paper.

WearFit Threat Model

Device: Threat overview (per WearFit article†)

1. Denial of service
   - Render wearable unusable with fake firmware update.
   - Drain battery, CPU, or other resources.
   - Lockout user from website account.
2. Compromise of device integrity
   - Malicious firmware update.
   - Buffer overflow on wearable to compromise paired mobile device.

† West, Jacob, Tadayoshi Kohno, David Lindsay, Joe Sechman. February, 2016. "WearFit: Security Design Analysis of a Wearable Fitness Tracker"

Figure 1.12: WearFit Device Threat Landscape

The threat overview for the WearFit device itself centers on denial of service and compromise of the device via faulty or malicious software downloads; and by attacks that take advantage of coding flaws, such as those that expose buffer overflow conditions. The threats listed here are those given in the WearFit paper, to maintain consistency with the paper's authors' discussions.

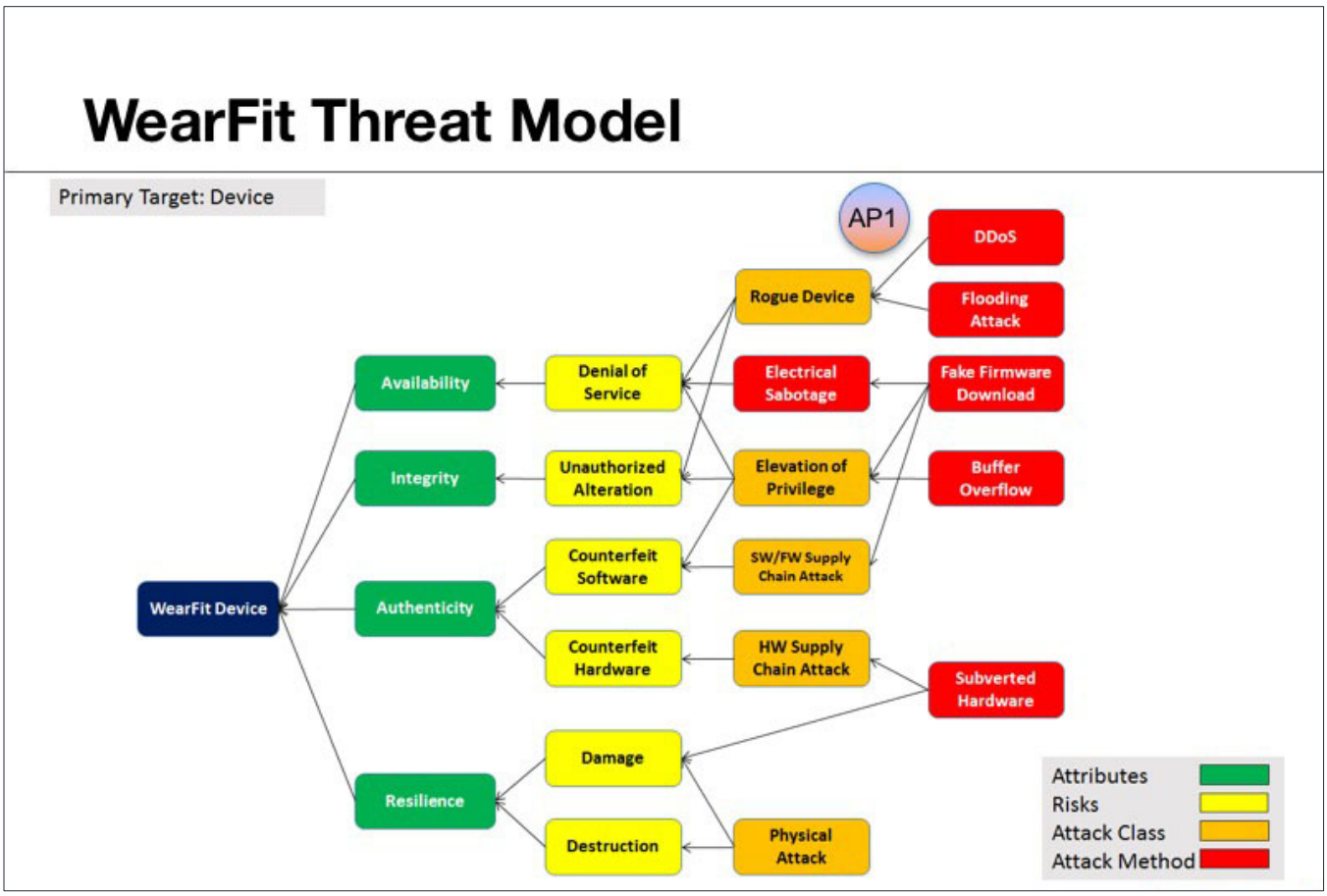

Figure 1.13: WearFit Device Target Tree

The WearFit device itself is at risk from attacks on its availability, the integrity of its software, the authenticity of its software and hardware components, and its resilience; i.e., its resistance to physical attack.

Figure 1.14 illustrates the attack tree for the device. The yellow nodes indicate the risks to each of the four attributes (the green nodes). The orange nodes list the attack classes associated with each risk; the red nodes are some of the attacks that could be waged against the device. The concepts of attack classes and attacks are described in Clause 3.2.1 of the Cybersecurity Architectural Risk Analysis Process white paper

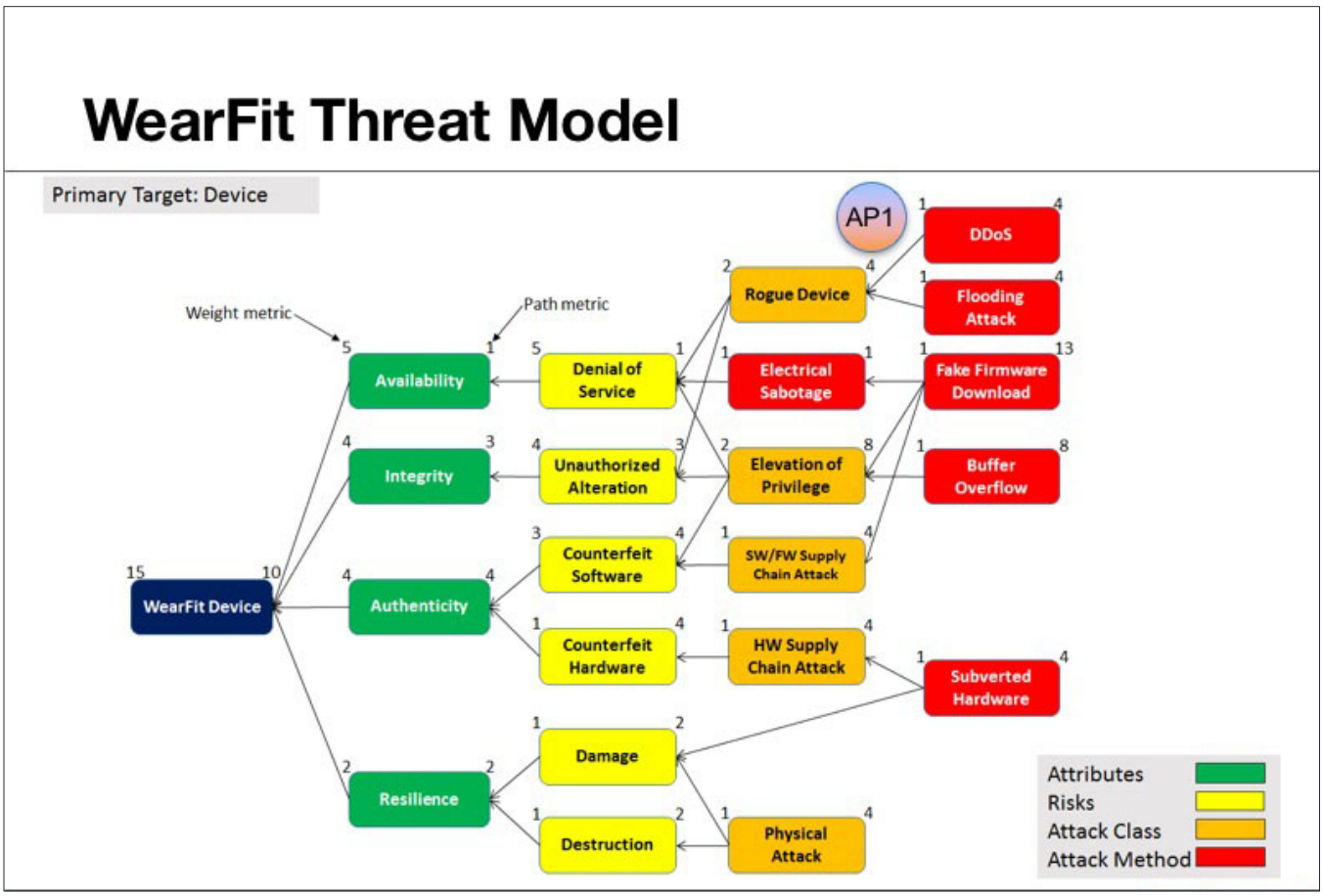

Figure 1.14: WearFit Device Weight and Path Metrics

The weight and path metrics are shown in Figure 1.15. They are computed as described in Clause 3.2.1 of the Cybersecurity Architectural Risk Analysis Process white paper. The weight metrics are based on a ranking of the WearFit device's attribute rankings, which rank device authenticity highest at 4, integrity 3, resilience 2, and availability 1. These rankings are based on foregoing discussion of the device.

The path and weight metrics allow us to make certain inferences about the protective measures the device needs. They are summarized in Figure 1.15.

WearFit Threat Model

The following inferences can be made from the device metrics:

- The path metric values for the four attributes (top left of each node) suggest that Availability is the most threatened attribute, while Resilience (resistance to physical attack) is the least threatened. This makes sense in light of the causes of physical attack; e.g., subverted hardware and direct attack (say, with a hammer) and the unlikeliness of each.
- The low ranking (1) of Availability would seem to offset the high weight metric, suggesting that some laxity in the defenses against Availability attacks is a viable security strategy.
- The high path metric values for “buffer overflow” and “fake firmware download” suggest that Elevation of Privilege is an attack class that must be strongly defended against, particularly since the model shows that that attack class affects Authenticity and Integrity, the two most highly ranked attributes.
- These points suggest that:
  - secure programming practices be in place in the development shop of the WearFit device, to lower the incidence of programing errors that can lead to problems like buffer overflow.
  - The security of the firmware update process needs to be strong; .e.g., encrypted downloads, integrity checking, and good access control into the WearFit device.

Figure 1.15: WearFit Device Target Tree Inferences

WearFit Threat Model

Data: Threat overview (per WearFit article†)

1. Falsifying the user's own health data
   - Physically manipulate the device.
   - Tamper with data on mobile device before uploading to the webserver.
   - Tamper with data in transit from wearable to mobile or mobile to website.
2. Falsifying another user's health data
   - Rewrite health data on device.
   - Tamper with data on a mobile device when used as a passthrough.
   - Spoof data uploads using a known device or user identifier.
   - Tamper with data in transit from wearable to mobile or mobile to website.
   - Direct attacks against the website (for example, SQL injection).
   - Phishing, cross-site request forgery (CSRF), and other indirect attacks against end users.

† West, Jacob, Tadayoshi Kohno, David Lindsay, Joe Sechman. February, 2016. "WearFit: Security Design Analysis of a Wearable Fitness Tracker"

Figure 1.16: WearFit Data Threat Landscape

The WearFit data can be threatened in the ways shown in Figure 1.16 and Figure 1.17. As before, these threats are taken from the text of the original WearFit article. Item 3 in Figure 1.17 is highlighted in gray because the items listed do not appear to represent threats, so much as consequences—a departure from the other items in the threat list. The gray items do not contribute to the threat model, and hence the highlighting. However, they *do* suggest that intentional exposure of data is a serious danger; and so, represent, at a high level, risks to data confidentiality and possibly data integrity. For that reason, confidentiality and integrity are included as attributes of the WearFit data in this portion of the threat model, as part of the target tree.

WearFit Threat Model

3. Abusing health data that are intentionally shared
   - Employer or insurer penalizes behavior seen through WearFit Corporate Benefits.
   - Users of the WearFit Social System unintentionally view sensitive activities.
   - Advertising partners target over-personalized ads.
   - Share configuration that becomes out-of-sync with changes in real-world relationships.
4. Stealing a user's health data
   - Guess or steal a user's authentication credentials.
   - Direct attacks against the website (for example, SQL injection).
   - Eavesdrop on communication on mobile device when used as a passthrough.
   - Eavesdrop on communication from wearable to mobile or mobile to website.
   - Malicious insider uses internal, or otherwise "privileged," access.
   - Phishing, CSRF, and other indirect attacks against end users.

Figure 1.17: WearFit Data Threat Landscape (cont.)

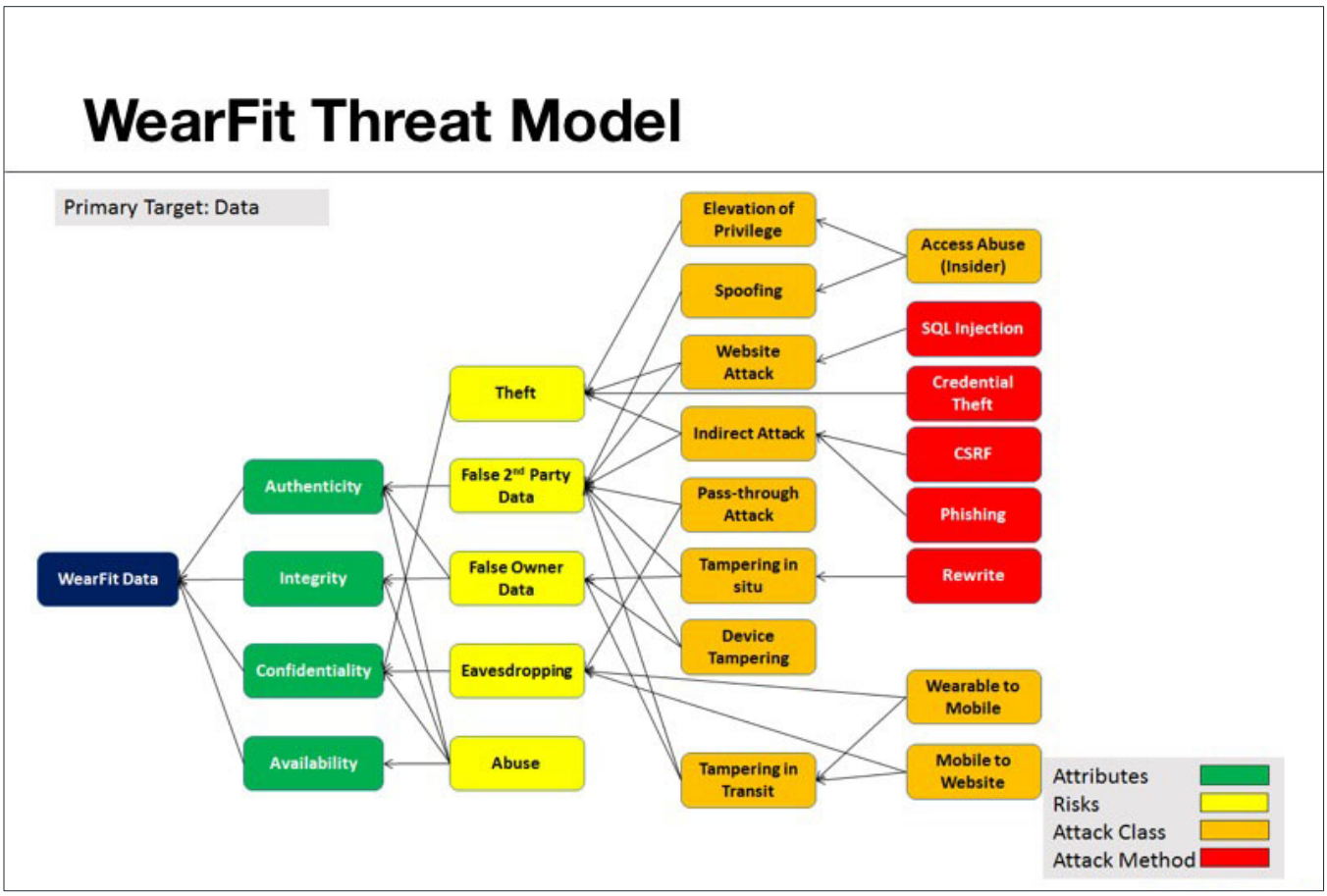

Figure 1.18: WearFit Data Target Tree

The target tree for the WearFit data is formulated in terms of the data's authenticity, integrity, confidentiality, and availability. The normally included fifth attribute of data, non-repudiation, is omitted from this assessment because there is no evidence from the WearFit description that situations could arise in which a party would deny having provided the data.

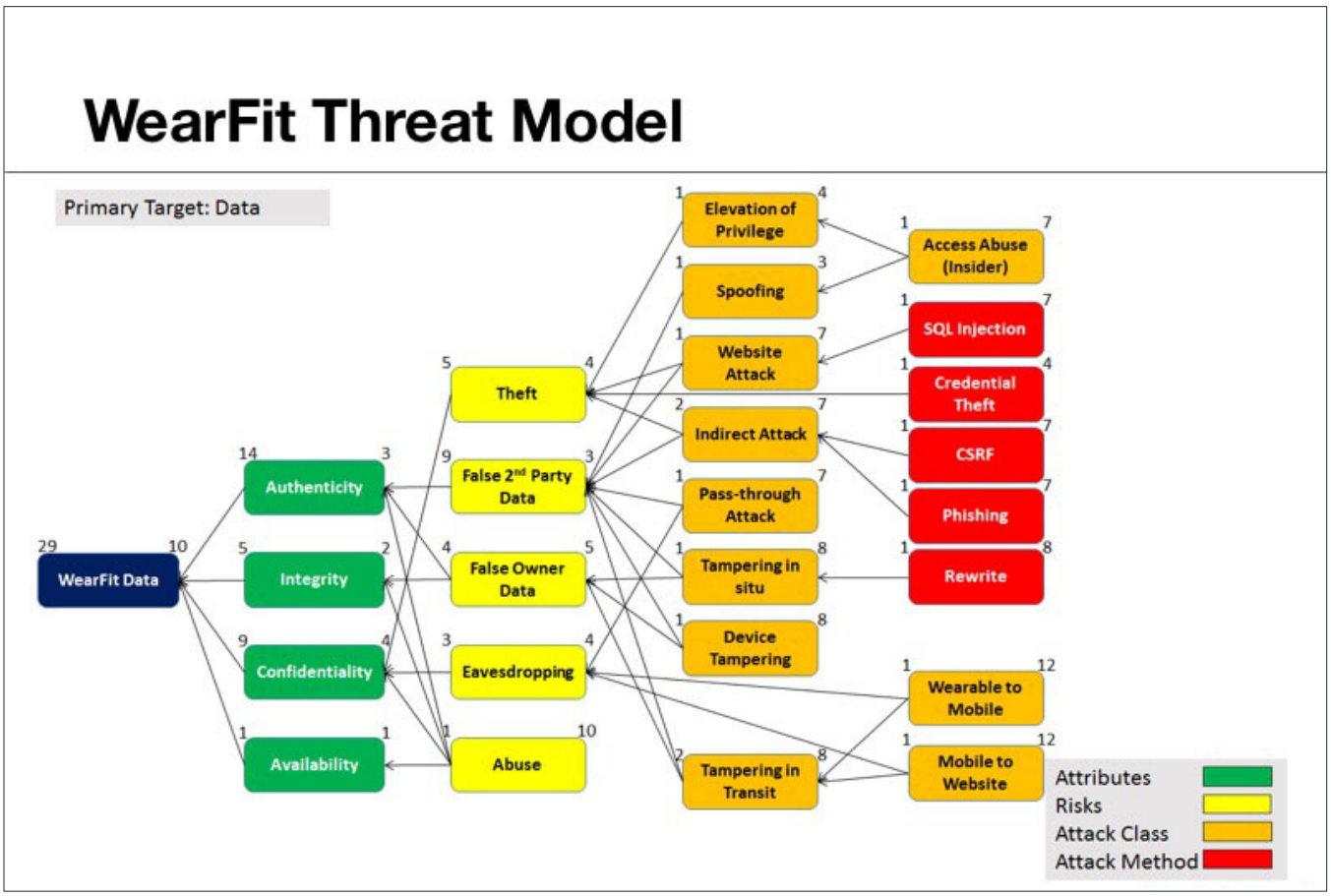

Figure 1.19: WearFit Data Weight and Path Metrics

The target tree metrics for the data are arrived at in the same fashion as those of the device target tree. The data's attributes are ranked as follows: Confidentiality is the highest at 4, with authenticity, integrity, and availability following in descending order of importance. The ranking is based on foregoing discussion of the WearFit data and the threats to it.

A number of inferences can be made from these metrics, as listed in Figure 1.20.

WearFit Threat Model

The following inferences can be made from the data metrics:

- The path metric values for the four attributes (top left of each node) suggest that Authenticity is the most threatened data attribute, while Availability is the least threatened. Confidentiality is the next most threatened attribute.
- Worth noting is that attacks against the interfaces ("Wearable to Mobile" and "Mobile to Website") represent the most significant attack class, which in turn are primary threats to Confidentiality. This might be considered either a finding or (since we usually suspect this kind of thing anyway) a validation of the threat model.
- The high weight metric values for "Wearable to Mobile" and "Mobile to Website" suggest that Tampering and Eavesdropping are attack classes that must be strongly defended against. Although the other weight metrics are roughly equal (except for "Credential Theft"), their affect on so many attributes indicates that their effects must be dealt with.
- These points suggest that:
  - secure interfaces must be a key component of the WearFit security architecture.
  - The significant risks of false data must be mitigated by defenses that cover many attack classes, indicating a need for thorough risk assessment to determine the actual risks versus cost of defenses.

Figure 1.20: WearFit Data Target Tree Inferences

1.7 WearFit Abuse Cases

WearFit Abuse Case Example

Stolen Device Used for DoS and Flood Attacks

- Abuse Case Summary
  - Stolen WearFit Device is reverse engineered to determine device data transfer protocol
  - Attacker creates DoS attack by simulating multiple unregistered transfers of data to near-by mobile devices in a densely populated public area (example shopping mall or equiv.)
  - Goal is to compromise delivery of service (Primary Asset)
- Use Cases Covered
  - Unregistered device data transfer
  - Authentication attempt from mimicked WearFit device
- Attack Points
  - RF interface to nearby mobile devices (AP1)
  - Flood mobile devices with invalid unregistered wearable traffic
  - Flood mobile devices with high rate of unregistered access attempts
  - Attacks may include mimicking other nearby WearFit devices

Figure 1.21: WearFit Abuse Case Example

Figure 1.21 shows a sample example outline for a possible WearFit solution abuse case. In addition to identifying how the example threat is manifested, the abuse case documents the use case functionality covered/used, as well as the possible attack points within the solutions' architecture.

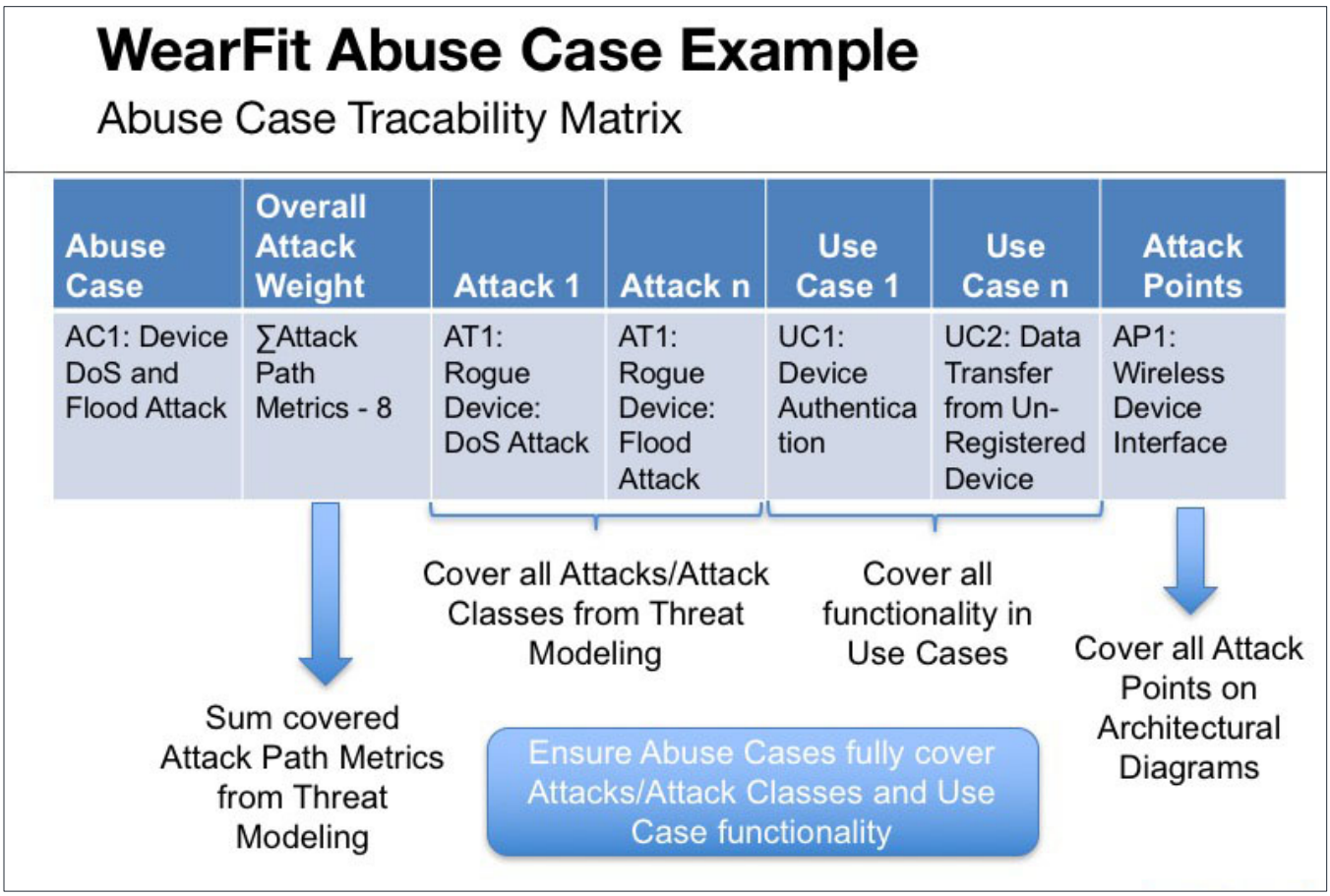

Figure 1.22: WearFit Abuse Case Traceability Matrix Example

Figure 1.22 illustrates the abuse case traceability matrix for the WearFit solution. The figure shows how example abuse cases cover a sub-set of the specific attacks identified as part of the threat analysis step, what use case functionality is exercised to mount the attack, and the attack point(s) in the solution's network diagrams where the attack can be applied. The attack weight metrics associated with the attack in the threat model is summed up and included to indicate the relative importance/risk that the example abuse case represents.

1.8 WearFit Risk Analysis and Mitigation

Risk Mitigation
Summary of Analysis

Risk Mitigation Step	Overall Priority	Attacks Mitigated (from Threat Analysis)	Overall Attack Weight	Ease of Exploit	Impact of Exploit	Cost Impact of Exploit	Attack Points
1	H	**Threat**: Brute force attack to steal credentials	4	H	H	H	AP3
		Impact: Attacker steals users LoginID and Password	**Security Control**: Enforce use of strong passwords and periodic update; PWs are salted and hashed with strong hashing algorithms. Authentication also provided via Google+ and Facebook		**Recommended Action**: Ensure hashing algorithms are strong and can be updated. Recommend that Google+ and Facebook authentication be used to supplement, not replace direct auth.		
2	M	**Threat**: Rogue device flooding network	4	H	M	M	AP1
		Impact: A rogue device could mimic numerous WearFit devices creating traffic floods leading to DoS	**Security Control**: Trusted authentication of device using certified credentials (certificates, etc.); WearFit does include the use of certificates and carefully managed keys		**Recommended Action**: Ensure all secrets are sufficiently protected, robust, and easily changed if compromised.		

Figure 1.23: WearFit Risk Mitigation, Summary of Analysis

Figure 1.23 represents a summary of the architectural risk analysis exercise for the WearFit solution. The table serves as an example of how analysis results can be summarized. Three entries are presented with a threat name, threat description, applied security control, assessment of control, and action for improving or ensuring effectiveness of control. Threats are also annotated with attack point references and abuse case references for convenience.