system design & management

Balancing Usability and Cybersecurity in IoT Devices

MITsdm

MIT SDM Systems Thinking Webinar Series

system design & management

Saurabh Dutta, Director of Experience Design, Rapid7

Tod Beardsley, Director of Research, Rapid7

Background- Saurabh Dutta

4 Years
DESIGN &
ARCHITECTURE

12 Years
USABILITY &
EXPERIENCE DESIGN/

10 Years in CYBER
SECURITY

Background- Tod Beardsley

7 Years
NETWORK AND SYSTEM ENGINEERING

14 Years
SECURITY ENGINEERING, RESEARCH, AND DEVELOPMENT

Today’s Webinar Agenda

- IoT market overview
- Usability-Security Paradox
- Need of IoT Security Framework
- Stakeholder Analysis
- Usability/ Functionality Analysis
- Security Analysis **Today’s Primary Focus**
- Application **Today’s Primary Focus**

Internet of Things (IoT) Market Overview

- Consumer
  - Gartner predicts by 2020, IoT technology will be in 95% of electronics for new product designs
  - Bain predicts consumer applications will generate $150B by 2020
  - Wearables including medical devices, smart home technologies are at the forefront

- Enterprise
  - Gartner predicts by 2020, more than 65% of enterprises will adopt IoT products
  - Discrete Manufacturing, Transportation and Logistics, and Utilities will lead all industries in IoT spending by 2020, averaging $40B each
  - Improving customer experiences (70%) and safety (56%) are the two areas enterprises are using IoT solutions most often today.

Today's Webinar Agenda

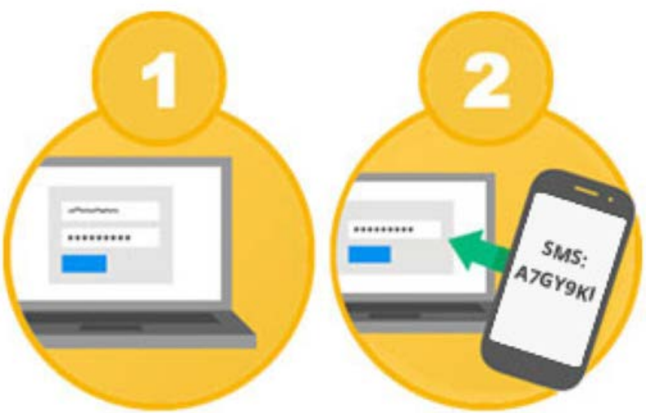
- IoT market overview
- Usability-Security Paradox
- Need of IoT Security Framework
- Stakeholder Analysis
- Usability/ Functionality Analysis
- Security Analysis
- Application

Usability Security Paradox

The Internet of Things, that system of web-enabled devices that can talk to one another, has brought people a wealth of benefits, from quick rides via Uber to the ability to remotely control the heat levels in our homes. But are these devices compromising our privacy—or even our safety?

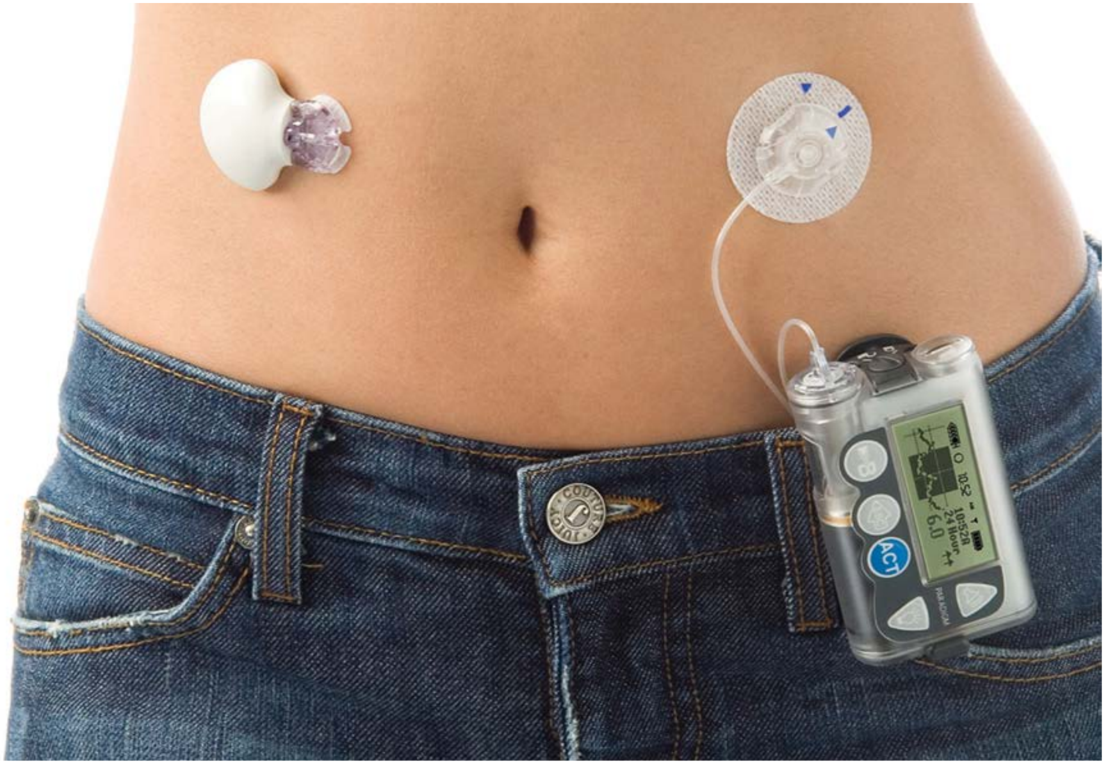
Usability Security Paradox

As per a study by distil networks, when CAPTCHA was present, people were on average 27% less likely to continue to the content.



Another experiment with 61 users showed how usability gets degraded with better security in 2 factor authentication over single factor

Usability Security Paradox



Insulin pump with always on bluetooth sensor

Today's Webinar Agenda

- IoT market overview
- Usability-Security Paradox
- Need of IoT Security Framework
- Stakeholder Analysis
- Usability/ Functionality Analysis
- Security Analysis
- Application

Antagonistic to Synergistic...

At first glance, it will always look like security and usability are antagonistic, but a deeper analysis suggests that by setting good practices, patterns and principles, security and usability can be improved synergistically

Good practices, patterns, principles example

Usability Pattern

- Copy and Paste
- Drag and Drop

Security Pattern

- Using the Secure Socket Layer (SSL) to “wrap” clear text protocols
- Email-Based Identification and Authentication for resetting passwords

Good practices, patterns, principles

↓

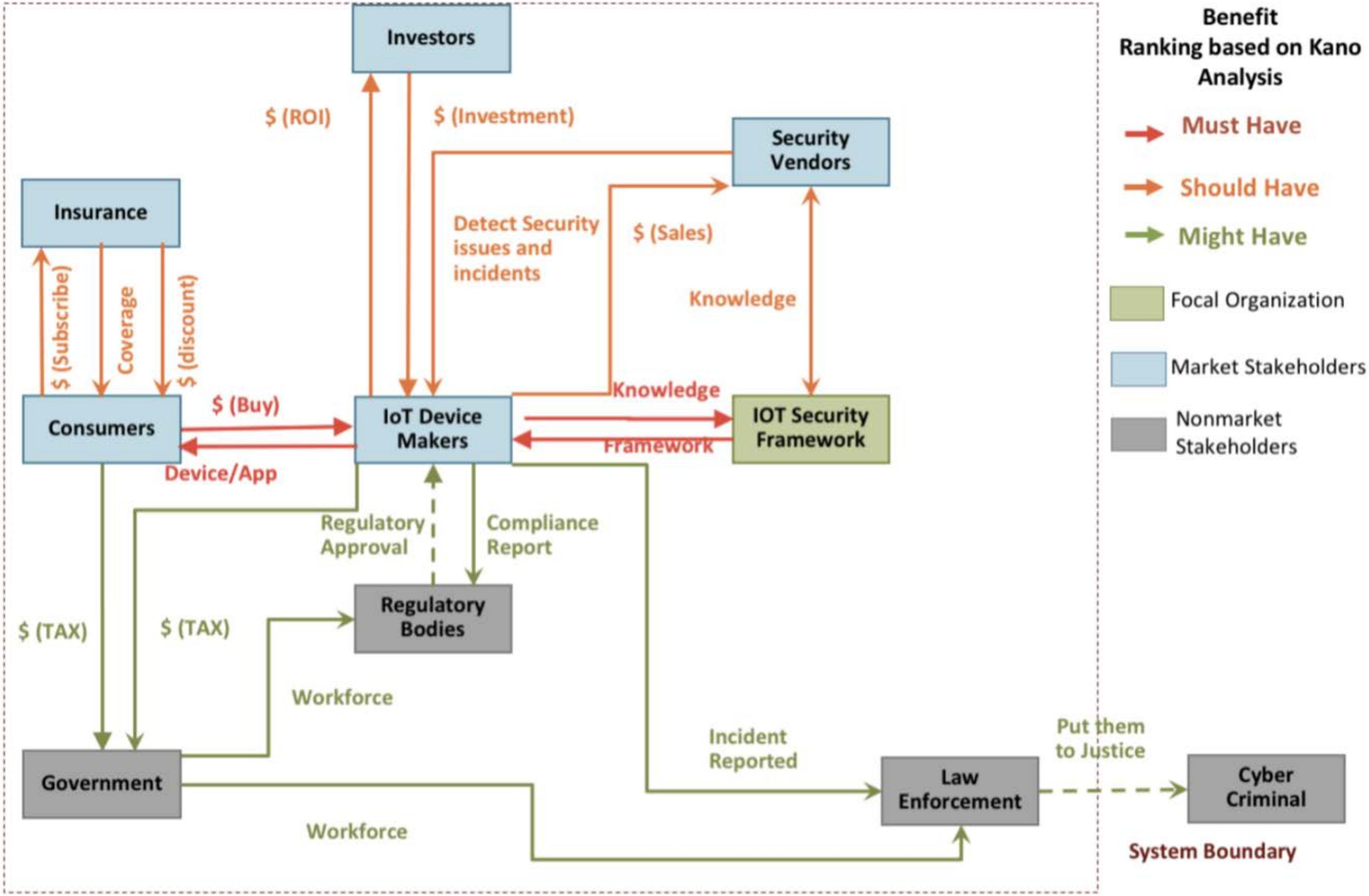
IoT Security Framework

But 1st, who is it for?

Today's Webinar Agenda

- IoT market overview
- Usability-Security Paradox
- Need of IoT Security Framework
- Stakeholder Analysis
- Usability/ Functionality Analysis
- Security Analysis
- Application

Stakeholder Analysis



Stakeholder Analysis

Role: Product manager/ Developer of IoT device maker

Goal: Need to ship new features and make product successful commercially

Problem: Needs to understand the security implications to feature requests before implementation

Solution: IoT framework makes the persona aware of potential security issues and better protect the company from releasing products that introduce unanticipated risks to their customers.

How: IoT security framework can be used to compare various designs to come up with the optimized option which does justice to both functionality and security.

Today's Webinar Agenda

- IoT market overview
- Usability-Security Paradox
- Need of IoT Security Framework
- Stakeholder Analysis
- Usability/ Functionality Analysis
- Security Analysis
- Application

Usability as Functional Product Requirement

At a high level, any product has two types of requirements:

- Functional requirements specify what the system should do.
- Non-Functional requirements specify how the system works or how the system should behave.

Usability is degree of ability of anything to be used and is generally a non-functional requirement

General Usability Attributes

Efficiency

Effectiveness

Productivity

Satisfaction

Learnability

Safety

Trustfulness

Accessibility

Universality

Usefulness

Based on Quality in Use Integrated Measurement (QUIM)

Today's Webinar Agenda

- IoT market overview
- Usability-Security Paradox
- Need of IoT Security Framework
- Stakeholder Analysis
- Usability/ Functionality Analysis
- Security Analysis — Today's Primary Focus
- Application

Common Vulnerabilities and Exposures: What can go wrong?

Confidentiality

Protection of information, especially when shared over a publicly accessible medium such as air for wireless

For example, hackers can get access to home monitoring camera and use that to blackmail

Integrity

Involves the protection of data and make sure that no unauthorized modifications occur.

Integrity on protection of sensor data is crucial for designing reliable and dependable IoT applications.

Availability

Specific to IoT, ensures that information is available when required.

For example, in a smart home denial-of-service (DoS) attack can make the device run out of battery and eventually unavailable

General IoT Security Attributes

Interviewed and surveyed 20 security professionals with IoT experience

+

OWASP IoT Project literature

General IoT Security Attributes

Physical Security

Making sure people, property, surrounding environment and the device itself is not harmed in case of accident or attack.

This is a defining attribute for IoT security.

Remote Control

WiFi (wireless networking), BLE (Bluetooth Low Energy), NFC (near field communications), and many other standards that all operate in RF (radio frequency spectrum) are used in IoT devices widely for ease of use.

Maintenance

It is critical for IoT devices to allow for regular maintenance including patching and upgrades.

IoT often fails at this.

General IoT Security Attributes

Authentication

Authentication involves the mutual verification of peers before they share information and ensures the data's origin and destination is accurate.

Authorization

Authorization consists of access policies that explicitly assign certain permissions to subjects: users, endpoints, and the like.

Input Validation

"Thou shalt not trust user-supplied input."

This is a common source for classic programming errors.

General IoT Security Attributes

Sanitization

Once validated, input from users and sensors is sanitized to ensure that the system is operating with expected, correct, and useful data.

Transport Security

Adjacent to authentication, transport security ensures that only the intended subjects can read or modify data in transit.

This is nearly always a job for cryptography.

Sensitive Data

If a device stores and transmits PII (Personally identifiable information), collect passwords, or handles any similar data that can be misused, it is dealing with sensitive data.

General IoT Security Attributes

Data Storage

Secure data storage involves preventing unauthorized people from accessing it as well as preventing accidental or intentional destruction or corruption of information

Encryption

All things being equal, data should neither be stored or transmitted "in the clear." Cryptographic standards ensure that data cannot be altered without evidence, nor read by unauthorized endpoints.

Logging

IoT devices need to know when their services are accessed, who is making the service request, when the request is happening

General IoT Security Attributes

Auditability

In case of an attack or accident, error investigation is crucial to understand what went wrong so that it can be prevented from causing further damage and reoccurrence

Logging

Logging services are critical for not only troubleshooting and maintenance, but can also be the last line of defense when it comes to feature abuse and system compromise

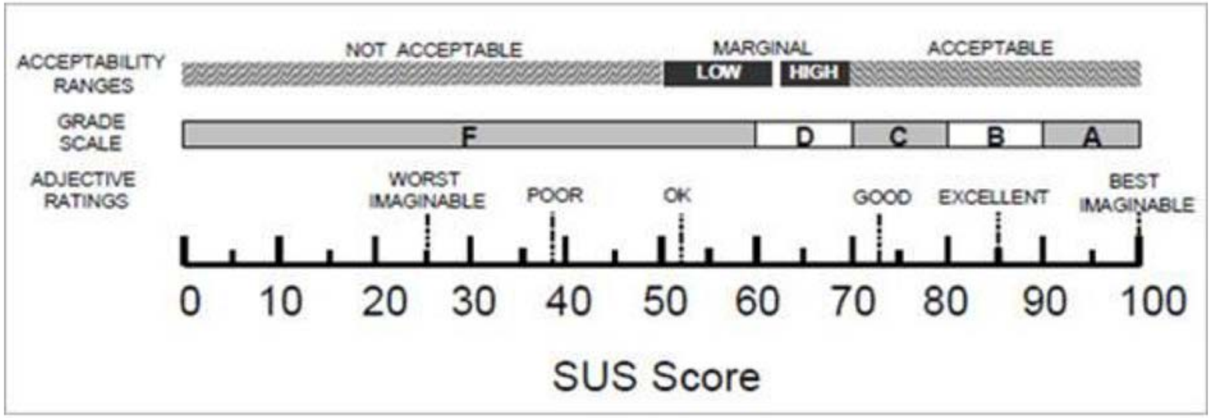
Transparency

While it may not be practical for a completely open source model for every feature and application, software should be reviewable by an independent auditor

Today's Webinar Agenda

- IoT market overview
- Usability-Security Paradox
- Need of IoT Security Framework
- Stakeholder Analysis
- Usability/ Functionality Analysis
- Security Analysis
- **Application** Today's Primary Focus

Application 1- System Security Scale



The System Usability Scale (SUS) provides a “quick and dirty”, reliable tool for measuring the usability. It consists of a 10-item questionnaire and evaluates a wide variety of products and services, including hardware, software, mobile devices, websites and applications.

Proposing- System Security Scale...

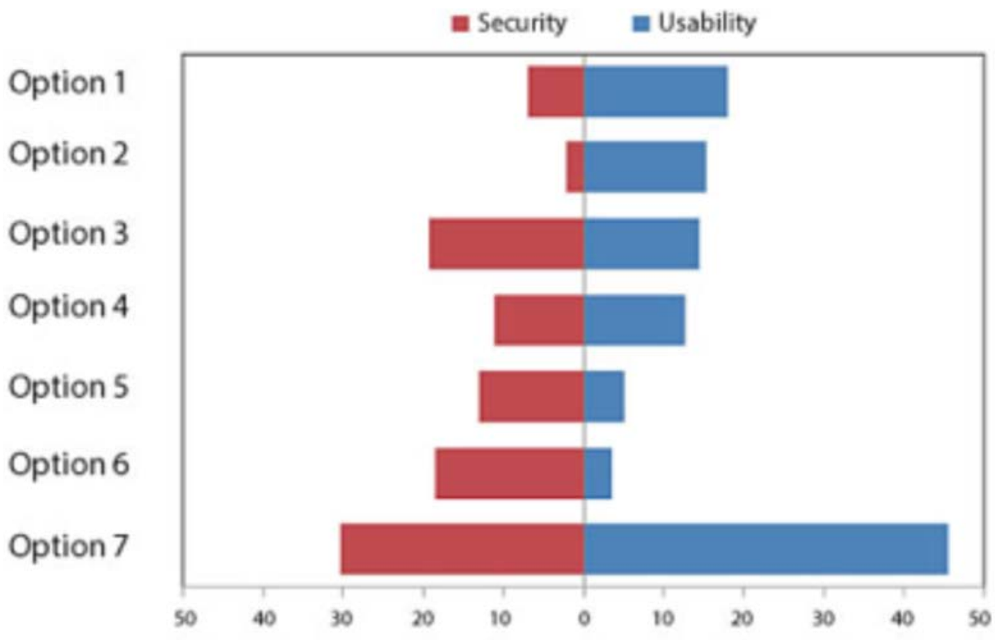
Application 1- System Security Scale

System Security Question	Affects (C,I,A)	Improvement Recommendation	Security Attributes
Is it impossible for the feature to affect the health and safety of people or property?	availability	Provide safety guarantees for failure conditions	Physical Security
Does the feature require a local, physical interface to access it?	availability	Lock down all control and data input interfaces	Remote Control
Can authorized users or devices patch or update the feature in the future?	integrity	Build and maintain a patch / update service	Maintenance
Can only authenticated, authorized users or devices access the feature?	availability confidentiality	Construct and enforce authentication and authorization policies	Authentication Authorization
Is all received data automatically inspected and validated?	availability integrity	Validate all input	Sanitization Input Validation

Application 1- System Security Scale

System Security Question	Affects (C,I,A)	Improvement Recommendation	Security Attributes
Are data transmissions encrypted and mutually authenticated?	confidentiality integrity	Use secure transport techniques	Transport Security Authentication Encryption
Does the feature avoid storing personally identifying information, tokens, or passwords?	confidentiality integrity	Be deliberate and careful with secure storage of credentials	Sensitive Data
Is any stored data only accessible after authentication by an authorized user or device?	availability confidentiality	Consider encrypting data at rest	Data Storage Encryption Authorization
Does the feature routinely log use and errors in a way that authorized users can inspect the logs?	logging integrity	Store log data securely	Auditability Error Investigation
Is the source code available for inspection by a third party?	integrity	Adopt open source principals where appropriate	Transparency Auditability

Application 1- System Security Scale

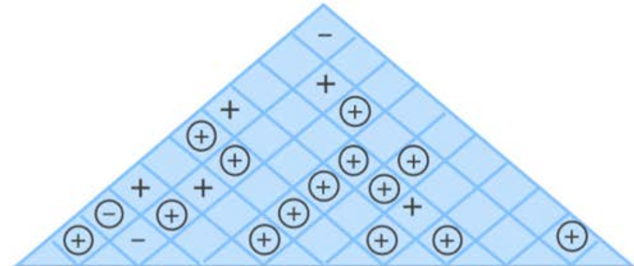


Future work- Imagine a quantitative metric that can be verbally stated in the form of the ubiquitous blood pressure rate. For instance, 70/85 or seventy over eighty-five would signify that both security and usability levels are high using the scores from, System usability scale score and System security scale score

Application 2- Security- Usability QFD to set priorities

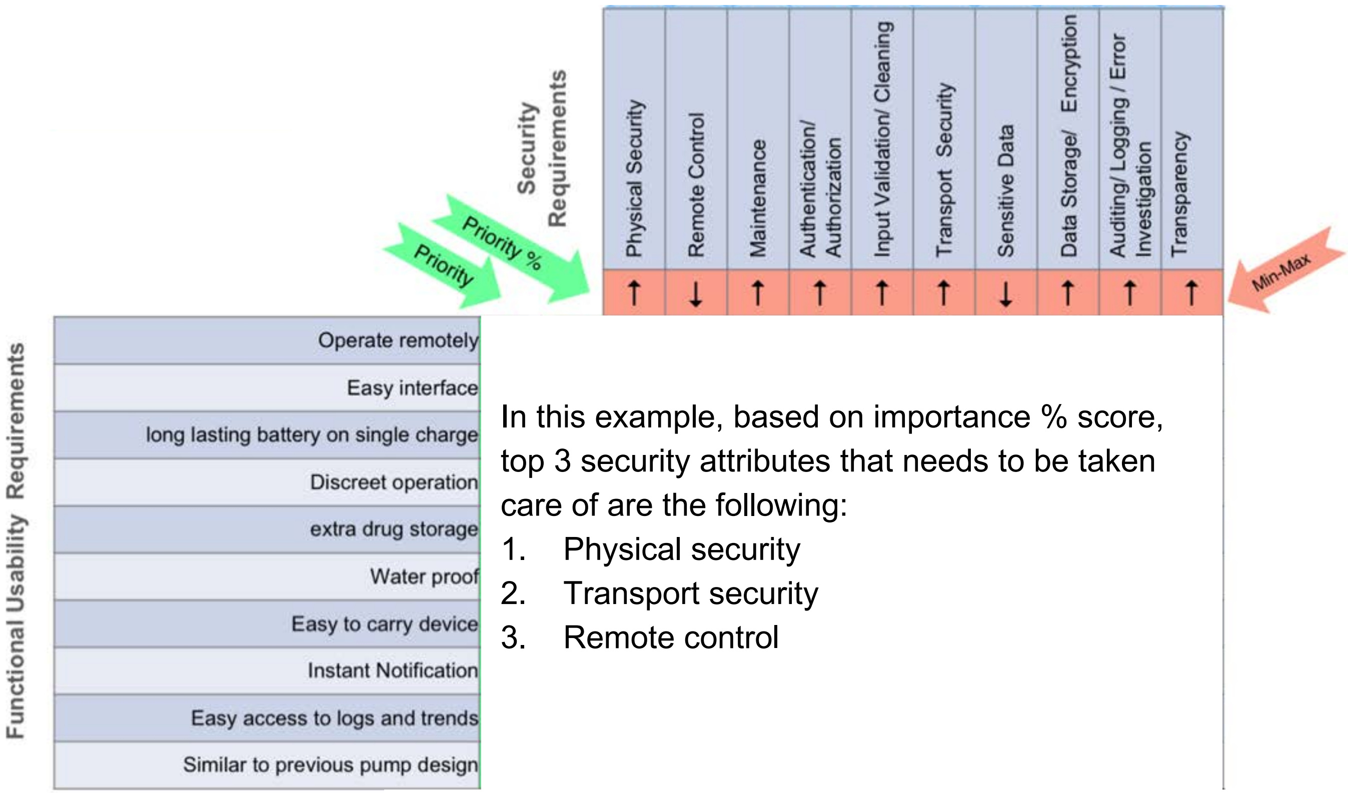
Correlations:
- ⊕ Strong Positive
- + Positive
- ⊖ Strong Negative
- − Negative
- None

Relationships:
- ⊙ Strong= 9
- • Medium= 3
- △ Week= 1
- None= 0



Functional Usability Requirements \ Security Requirements	Priority	Priority %	Physical Security	Remote Control	Maintenance	Authentication/ Authorization	Input Validation/ Cleaning	Transport Security	Sensitive Data	Data Storage/ Encryption	Auditing/ Logging / Error Investigation	Transparency
Min-Max			↑	↓	↑	↑	↑	↑	↓	↑	↑	↑
Operate remotely	5	16.67	•	⊙	△	⊙	•	⊙	⊙	⊙	△	△
Easy interface	5	16.67		⊙		△	⊙	⊙	△		•	
long lasting battery on single charge	4	13.33	⊙					△	⊙			
Discreet operation	4	13.33	⊙	•		•		△	•	⊙		
extra drug storage	3	10	⊙			⊙				⊙		
Water proof	3	10	⊙									
Easy to carry device	2	6.67	⊙	△				•		△		
Instant Notification	2	6.67	△	⊙		⊙	⊙	⊙	△	△	⊙	△
Easy access to logs and trends	1	3.33		△	⊙	⊙	△	⊙	⊙	⊙	⊙	⊙
Similar to previous pump design	1	3.33										
Importance			537	410	47	387	264	437	363	403	157	53
Importance %			17.5	13.4	1.5	12.6	8.6	14.3	11.9	13.2	5.13	1.73

Application 2- Security- Usability QFD to set priorities

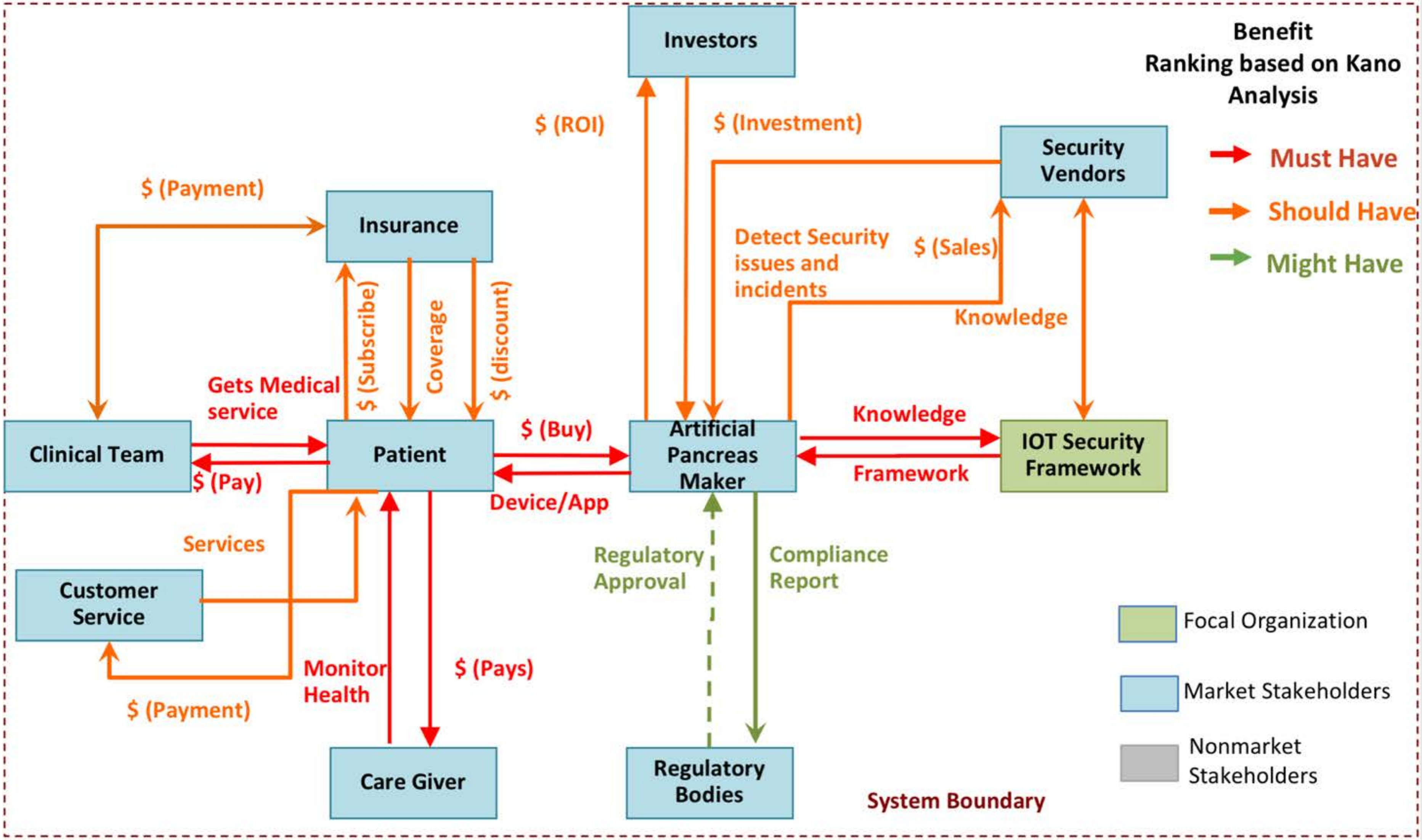


In this example, based on importance % score, top 3 security attributes that needs to be taken care of are the following:

1. Physical security
2. Transport security
3. Remote control

Appendix

Stakeholder Analysis- Artificial Pancreas



Functional Usability Attributes- Artificial Pancreas

Functional Usability Features	Stakeholder Priorities						
	Patients	Doctors	Caregivers	Customer Service	Sum	Avg. Priority 1-5, 5 being highest	QUIM Most relevant attribute
Easy to carry device	2	7	6	9	24	2	Efficiency, Accessibility
Operate remotely	4	1	2	1	8	5	Productivity, Efficiency
Easy interface	3	3	1	5	12	5	Satisfaction, Efficiency
long lasting on single charge, peace of mind	5	4	7	2	18	4	safety, Trustfulness
Instant Notification	8	8	3	6	25	2	Safety, Usefulness
extra drug storage	7	2	4	8	21	3	Productivity, Safety
Discreet operation	1	6	5	7	19	4	Satisfaction
Easy access to logs and trends	10	9	10	3	32	1	Learnability, Universality
Similar to previous pump design	9	10	9	10	38	1	Learnability
Water proof	6	5	8	4	23	3	Trustfulness, Effectiveness

Based on Quality in Use Integrated Measurement (QUIM)