The Technology of Tamper Detection: Mechanical Security

By Matt Kwan, ECE '16

Through the process of building a security device, two extremely significant factors have been identified in the design criteria for mechanical security: (1) environmentally appropriate casings for protection against environmental intrusion, and (2) secure design against compromising inputs. Ultimately, thorough testing to discover flaws at the design phase is crucial when considering the above factors. This overview shows that mechanical security cannot be accomplished without addressing these factors.

Introduction

Security devices are held to some of the highest levels of scrutiny due to the nature of security applications. Such devices can be based in a variety of fields, all of which have useful literature, e.g. chemical-based, electrical-based, and mechanical-based (see the Tech Notes by Green Team members Catherine Kravchenko and Patricia O'Connor for discussion on chemical- and electrical-based applications). This scrutiny should come under two perspectives – environmental intrusion and purposeful intrusion. Between these two perspectives, engineering design gaps in a product such as insecure device inputs and insufficient casing warrant thorough testing before it is released to the market. This paper will introduce the concerns and standards in mechanical security through explanations and examples so that readers can possibly relate the material to current or future work in similar fields.

Protecting from Environmental Intrusion

Environmental intrusion to the product can come in a number of forms – the most common being liquids, grime, and dust which can be found under normal environmental circumstances. Unfortunately, if intruded into the product, they can corrode electronic terminals, break connections, and divert current. Thus, they can significantly hinder the lifetime of an electronic device. Furthermore, due to these invasive substances, electronics can fail in physically dangerous ways. For example, they could send current through the casing, possibly causing an electric shock or short-circuiting of the power source which could ultimately cause a burn or fire.

For safety devices that are used directly by humans, a level of protection against the elements is a must. A safety device that fails when subjected to normal environmental harm should not be recommended to anyone.

Significance of Ingress Protection (IP rating)

The engineering label of protection from environmental harm is described in the standard known as Ingress Protection rating, or *IP rating*. The rating (formally codified in the *IEC 60529 technical standard: Degrees of protection provided by enclosures (IP Code)* (IEC, 2013), describes how much protection is offered by the casing against liquids, dust, and other solid foreign objects. Its number system is IP## such as IP54 where the first digit represents the electronic casing's protection from solid foreign objects like dust or a tool (ranging from 0 [not protected] to 6 [protected against objects smaller than 1 mm]), and the second digit represents the casing's protection from liquid ingress (ranging from 0 [not protected] to 8 [protected from continuous immersion in water]) (Jowett, 2004).

These ratings can be found in the specifications of an array of devices (Table 1).

Table 1: IP Ratings for a Selection of Commercial Products

Name	IP Rating	Description
Fiilex P180E LED light	IP24 without Rain Shield IP25 with Rain Shield	LED Light for photography illumination [2] Protected against access with jointed finger (12 x 80 mm) [4] Protected against ingress of splashing water, any direction [5] Protected against jetting water, any direction
Netgear Arlo	IP65	Indoor/Outdoor battery-powered cameras for home security [6] Protected against access with a wire (1.0 mm) [5] Protected against jetting water, any direction
Cat S40	IP68	'Rugged' cell phone for outdoor lifestyles by Cat(R) construction company [6] Protected against access with a wire (1.0 mm) [8] Protected against continuous immersion in water

Sources: Bullitt Group (2015); Netgear Arlo (2015); Ryan (2014);

Protecting from Purposeful Intrusion

Purposeful intrusion is different from environmental intrusion in that it is an assailant's attempt to get past the device's security, whether by clever workarounds or brute force. The designers of safety devices must consider the routes that assailants would employ – avoiding a sensor, exploiting a software bug, destroying critical functions of the device, etc. The process of taking apart a device to figure out how it functions is known as *reverse-engineering*, and must be taken into consideration by the original design engineers.

Redundancy

A way to hinder reverse-engineering efforts would be to add a layer of *redundancy*. The idea of redundancy is to identify confident hits by checking if the incident triggered more than one layer. One can be confident of the result if multiple detection schemes reacted to the same incident.

One of the best redundancy measures for security devices are electromechanical components – that is, materials that work/react mechanically and electrically. For example, conductive rubber can be employed to both tighten around an object and detect expansion/contraction.

However, these components come at a price, not only monetarily but also physically. Design engineers are faced with the challenge of maximizing security while maintaining a usable form, matching the application with the level of practicality.

Conclusion

As evidenced, appropriate casing must be chosen that can protect the internal electronics against environmental factors such as dust and/or water ingress; otherwise, the security device could fail when it's needed. In addition, a secure design must take into consideration any buttons or switches that the user is intended to use such that illicit tampering cannot occur by these means. Even with this amount of consideration, thorough testing must be done with people from various backgrounds, not just design engineers. While engineers may fill in most holes, it is

inevitable that they will miss some things – perhaps things that others may find obvious. These necessary concerns should be addressed to ensure their integrity.

References

Bullitt Group; Cat(R) Phones Launches Cat S40 for U.S. Market. (2015). *Telecommunications Weekly*, 67-67. Retrieved December 1, 2015.

International Electrotechnical Commission (IEC). (2013). *IEC 60529 Ed. 2.2 b:2013. Degrees of protection provided by enclosures (IP Code)*. [Technical Standard]. ISBN 978-2-8322-1086-4

Jowett, J. (2004, June 1). What does instrument IP rating mean? *Plant Engineering*.

Netgear Arlo. (2015, July 22). *Computer Active*, 24-24.

Ryan, P. (2014, August 1). H2O TIGHT. *Popular Photography*, 18-18.