Exercise 1

Module 8 - Security Management

Knut Lucas Andersen
Master Applied Information Security
isits AG International School of IT Security

November 26, 2017

Contents

1 Facebook: Uploading naked photos for own security

Earlier this week, it was mentioned on both Gallileo and in the news how Facebook are currently testing out a new security feature. The aim for this security feature is to prevent others from uploading semi-nude or nude photos of you. However, for this feature to work, you must yourself upload naked photos of yourself to Facebook so that Facebook can recognize and warn you when it happens.

There are several issues I see with this. Putting aside the question whether or not one need this feature (ie. the "every day person"), what guarantees does the user have that this data is secure? Every day, there are stories about leaked sex videos, secret documents and corrupt employees breaking into their own company's system. Furthermore, would not this just make attackers even more interested in attacking and breaking Facebook? Hacking today is more about earning money than simply breaking things and showing off your skills.

From the users perspective, the user must not only be comfortable enough with taking potential nude shots of themselves, but also trust that Facebook keeps them safe. But what safety can Facebook really promise, and in what way would they process these images? Not to forget that Facebook changes their guidelines and terms of conditions so often, that it is nearly impossible to bother keeping up with the changes. Do we as users have any guarantee that Facebook will not later on "chop of your head" and sell the images as "commercial-ware"?

2 Network externalities to strengthen its market position

3 Information Goods

a) Non-rivalry

(Wikipedia, 2017d)

b) Low marginal costs of reproduction

When first launching a new product, the costs are high, but fixed. E.g. there might occur delays, machines breaking down and other (un-)expected errors occurring. When running the second to N-production round, we have what we refer to as "low marginal costs". This is because the costs for production is already known and one can avoid the issues that occurred during the first round. Another reason could be that the first production round sets up the requirements to use the product, whereas the second to N production round is simple "maintenance". An example is the Telecomms, as described in (R. J. Anderson, 2008, p. 624) where the first production round was creating the telephone network, and the marginal costs were handling phone calls.

c) Arrows information paradox

Arrows information paradox focuses mainly on patents and the users right to insight into the product (Wikipedia, 2017a; MbaSkool.com, 2017). When a customer buys (or considers buying) the product, they may want to know what "makes it tick". The problem is that this information might be unique to the company, and sharing this information is perhaps something they cannot claim payment for. Even if payment were claimed for this insight, the user could also claim that s/he had then bought the rights to use the information gained for own usage. Arrows information paradox takes into consideration additional processing steps during patenting to secure the products intellectual property.

d) Non-excludability

Non-excludability touches upon the question whether or not only valid (paying) customers have access to a given product (Wikipedia, 2017b; Treasury, 2005). (Treasury, 2005) states that:

> "... non-excludability means that once a good has been created, it is impossible to prevent other people from gaining access to it (or more realistically, is extremely costly to do so)."

An example of this could be operative systems. Windows and Mac are Excludable products, because you can only have access to their products through valid licenses (which are given through purchases/renewals). Unix and Linux are non-excludable because they are open-source, and mostly free to use (excluding enterprise versions).

e) Qualitative differentiation (uniqueness)

Qualitative differentiation is comparison of multiple products offering the same "services" (Wikipedia, 2017c; Answers, 2017; R. Anderson, 2001). In (R. Anderson, 2001, p. 5-6) used cars are one example, where they all look the same, but only a given amount of these are good cars. Here in Germany, the Rewe stores are another examples, where they offer original brands and their own cheaper version of the same product ("Rewe" and "Ja!"). The same goes for many Norwegian stores, where they sell their own cheap version of certain food and everyday usage items. To create a simple example, only three general rules can be set for distinguishing the products:

1. Brand: Larger, more known brands have higher prices than the less known ones (e.g. Rewe, Ja!)
2. Quality: Certain products can be more obvious in regards to usage. E.g. cheap soap for dish washers might create white/gray remains, laundry can be smelly or have colour damage.
3. Taste and looks (to same degree same as quality): E.g. meat that are less processed (more fat, bones, etc that requires to be cut off), chocolate that taste the same, but come from different brands, etc.

4 Information markets

5 Dynamics in information warfare

The dynamics for information warfare can be summarized as the following: "Attackers can attack everywhere, anytime. Defenders have to protect everything, everywhere, all at once" (R. Anderson, 2001).

Even though a security tester have the possibility to research and find more bugs and exploits then the attacker, the testers has no guarantee that they found the same as those found by attackers. For attackers, they can also simply trade or give away risks and exploits on Dark Web. For the security tester, the issue is that they can be blacklisted, get penalties and even risk prison sentence from the more larger companies.

The question is also for the discoverer of the bug/exploit what benefits them the most. You can report the exploit and risk 10 years in prison, or sell it anonymously on Dark Web and earn several thousands (maybe millions) of Euro. In (R. Anderson, 2001), his example was military intelligence and surveillance. His conclusion was basically that the smaller the population, the greater success of attacking other countries vs. others attacking them.

6 Information asymmetries

References

Anderson, Ross (2001). "Why information security is hard – An economic perspective". In: *Annual Computer Security Applications Conference (ACSAC)*.

Anderson, Ross J. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Second Edition. Wiley Publishing, Inc. ISBN: 978-0-470-06852-6.

Answers, Yahhoo! (2017). *Can somebody explain to me what 'qualitative differentiation' means please?* URL: https://answers.yahoo.com/question/index?qid=20101107081041AATOqUX.

MbaSkool.com (2017). *Arrow Information Paradox*. URL: https://www.mbaskool.com/business-concepts/marketing-and-strategy-terms/12644-arrow-information-paradox.html.

Treasury, The (2005). *Non-excludability*. URL: http://www.treasury.govt.nz/publications/research-policy/ppp/2005/05-05/05.htm.

Wikipedia (2017a). *Arrow information paradox*. URL: https://en.wikipedia.org/wiki/Arrow_information_paradox.

— (2017b). *Excludability*. URL: https://en.wikipedia.org/wiki/Excludability.

— (2017c). *Product differentiation*. URL: https://en.wikipedia.org/wiki/Excludability.

— (2017d). *Rivalry (economics)*. URL: https://en.wikipedia.org/wiki/Rivalry_(economics).