University of Innsbruck

Institut of Computer Science

Security and Privacy Lab

Kerckhoffs' Forgotten Principles

Alex Hirsch

2015-11-05

1 Auguste Kerckhoffs

Auguste Kerckhoffs (⋆1835, †1903) was a Dutch linguist and cryptographer who is most commonly known for the Kerckhoffs' principle [8], which states:

> A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

But this principle is only one of six described in the first of two articles he published 1883 in *le Journal des Sciences Militaires*. The articles entitled *La Cryptographie Militaire* addressed the then state-of-the-art military cryptography and provided considerable improvements in French practices. Note that the original article was written in French and multiple English translations are available which are worded differently. [8]

The six principles translated from French [8]:

1. The system must be practically, if not mathematically, indecipherable;
2. It should not require secrecy, and it should not be a problem if it falls into enemy hands;
3. It must be possible to communicate and remember the key without using written notes, and correspondents must be able to change or modify it at will;
4. It must be applicable to telegraph communications;
5. It must be portable, and should not require several persons to handle or operate;
6. Lastly, given the circumstances in which it is to be used, the system must be easy to use and should not be stressful to use or require its users to know and comply with a long list of rules.

Claude Shannon formulated a similar principle (perhaps based on Kerckhoffs' famous principle) known today as *Shannon's maxim* [4]

> The enemy knows the system.

2 Argumentation

Kerckhoffs' argumentation built on war scenarios, despite this was before World War I. Cryptography (as well as steganography) are important aspects of a war and every battle. This was true *then* and still is *now*.

2.1 First Principle

The first principle allows for a lot of interpretation regarding the *practical indecipherable* part. From the article one could infer that this principle refers to setting a big enough timeframe in which message can be considered *not yet deciphered*.

A military general may for instance state that it's perfectly fine to use an encryption which cannot be broken in less than 5 hours if the transmitted information is only relevant for 3 hours. Kerckhoffs' reasoning, on the other hand, states that while we cannot ensure perfect security on all channels every time, the timeframe should be much bigger so the cryptographic system can be used in a more general way — not having to worry about the message getting deciphered anytime soon.

Also a follow-up to this, depending on the used cipher, the enemy may derive the key from a deciphered message, hence all further messages enciphered with the same key can be read instantly.

2.2 Second Principle

Imaging a war-like scenario where both, enemy and friendly units, change their position from day to day, equipment of one party may fall into the hands of the opposite party. A cryptographic system in place at an outpost may be acquired by the enemy during a raid. Now *the enemy knows the system*.

Kerckhoffs' (second) principle basically states that this common scenario should not improve the enemy's ability to decrypt messages using the *compromised* system.

This goes hand in hand with the next one.

2.3 Third Principle

Let's reuse the scenario above and assume Kerckhoffs' (second) principle is true.

The enemy has acquired parts (or all) of the system enabling it to encrypt and decrypt any message with a given key. If keys cannot be communicated or remembered, the odds of finding a set of keys (codebooks) near the system highly increases. Hence the enemy may not only have gained access to the system itself but may have also acquired a set of keys. Some of them may have been used for communication already since personnel had no ability to store the keys in their minds or periodically request new keys over a telegraphic channel.

Also if the enemy gets a hold of written notes this may help deriving keys.

After establishing that the key has to be kept secret at all costs, only a small number of messages should be encrypted with the same key to keep the consequences of a compromised key minimal. This requires the users of the system to change keys on a regular basis. This is also enforced by the third principle.

2.4 Forth Principle

Well, since all of this aims to be the minimum requirements for a cryptographic system used for telegraphic communication, the system in question should be applicable — otherwise it would be pointless.

2.5 Fifth Principle

Enforcing portability and single user operability will improve mobility and minimize response time. Both are key factors for the military especially during a battle.

2.6 Sixth Principle

Together with the fifth principle this also ensures usability. Usability is paramount when it comes to cryptographic systems since the wrongdoing of a user can drastically expand the attack surface. Keeping the steps required for encryption and decryption simple and to a minimum will enable many people to use the system in a secure manner.

3 Relevancy Today

Much has changed since the original publishing of Kerckhoffs' article, although our everyday devices possess more computing power than he probably imagined, his principles still hold relevance today.

3.1 First Principle

What Kerckhoffs (probably) refers to when talking about *mathematically indecipherability* is known today as the *perfect secrecy* property. [4] The most commonly known cipher which achieves this property is the one-time pad (OTP) first described by Frank Miller in 1882 [2]. While being impossible to break if used correctly it is oft impractical since a (truly random) key of the same length as the message is required — and reuse of the key is not allowed. This renders the OTP inapplicable for many scenarios.

The OTP cipher combines each character of the plaintext with the corresponding character from the key. Modern implementations use XOR for combining the two parts (XORing bitwise), this is known as the Vernam cipher issued by Gilbert S. Vernam in 1919 [5].

Other ciphers not satisfying the perfect secrecy property are more common since they work with shorter (fixed sized) keys. If the message is longer than the key, the key gets reused. But instead of simply combining character by character a whole *block* will be scrambled with the key. Therefore these types of ciphers are known as *block ciphers*[1] while the OTP is part of the *stream cipher*[2] family.

An attacker could try to decrypt an intercepted message with all possible values for the key and check whether the output looks like a possible plaintext. This may work if the plaintext contains enough redundancy to distinguish it from other outputs. This *exhaustion of the keyspace* is commonly known as *brute-force attack*. Modern ciphers are built in such a way that an enormous amount of computing power is required to try all possible combinations. Of course one may start such an attack by using keys in a lexicographical order, therefore a key with decent length is required to be considered *safe*.

3.2 Second Principle

As already elaborated in section 2 security should not rely on keeping a system hidden from the enemy. Doing this however (and therefore infringe Kerckhoffs' principle) is often referred to as *security through obscurity* or *security by obfuscation*. Even though considered bad practise by cryptographers such system are still used today.

You'll commonly encounter such systems when looking at digital rights management (DRM) enforcement techniques. Using an open system where all security relies on the key is hardly an option in scenarios where DRM access control technology is used. This comes from the fact that key extraction is simple in most cases and must only be achieved once per access control technology. Additional steps of obfuscation are required to make key extraction much harder and unprofitable for the enduser.

DRM is not considered uncrackable, oft it is only a matter of time until a new system is reverse-engineered and cracked. This is an ordinary chain of events in the video game industry among others. A recent example would be Denuvo, an anti-tamper technology built into the PC releases of *Metal Gear Solid V: The Phantom Pain*, *Batman Arkham Knight* and *Mad Max*. [7] It took *warez groups*[3] more than two weeks after release to build a working crack. This is what related publishers were aiming for since they know every DRM technology can be broken given a certain amount of time. This amount of time is proportional to the amount of obfuscation the DRM system introduces.

[2] see https://en.wikipedia.org/wiki/Block_cipher
[2] see https://en.wikipedia.org/wiki/Stream_cipher
[3] see https://en.wikipedia.org/wiki/Warez_group

3.3 Third Principle

Generally keys are just bit streams which can be send over a channel (hopefully encrypted) just like normal messages. Nevertheless key distribution is a common topic in modern cryptography. For symmetric encryption the Kerberos protocol[4] is a typical example. On the side of asymmetric encryption we have the public key infrastructure (PKI) for TLS / SSL certificates, which works nice theory but more like hell in practise. [3]

Most protocols have some directives for switching the key, even during a session. Generating a key once per session and switching the key whenever one endpoint wants to is common practice, take a look at TLS / SSL for example. [1]

3.4 Forth Principle

Telegraph communication back then evolved to the internet now, thus as long as your messages can be encoded somehow into bits you satisfy this one. Kerckhoffs did not really talk about latency and bandwidth so I suggest keeping your message format within reasonable boundaries will prevent you from running into channel related problems.

You may consider using compression techniques, but be aware, they may extend the attack surface.

3.5 Fifth Principle

Portability seems to be the easiest of the six achievable today. Laptops, tablets, smart phones, smart watches, smart cards, … electronic devices get smaller and smaller every year and gain more power and capabilities too. Hardware additions like crypto chips and secure key storages are added for performance and security. This chips are often integrated into the CPU or surrounding chipset.

Modern computers come with a Trusted Platform Module (TPM)[5] which can be used for platform integrity, disk encryption, key storage and more.

3.6 Sixth Principle

While portability seems easy to achieve this one may be the hardest of the stated principles. Many crypto systems work perfectly in theory but fail in reality because the required rule set is not practical or user friendly enough.

We achieved best possible usability with smart cards: holding a piece of plastic against another piece of plastic and you're done. It doesn't get much simpler than that.

In contrast take a look at Pretty Good Privacy (PGP) which has been around since 1991. While key management is a very important topic better left for the user, hardly any interface tries to guide a new user through the sequence of steps to correctly acquire, verify and use public / private keys. Despite the recent improvements to enigmail (Thunderbirds PGP addon)[6] it's still a long way to go until unfamiliar users can use the system reliably. [6]

[4] see http://web.mit.edu/kerberos/
[5] see https://en.wikipedia.org/wiki/Trusted_Platform_Module
[6] see https://www.enigmail.net/home/index.php

4 Conclusion

Looking at the Enigma and its success in World War II one can easily see the importance of Kerckhoffs' principles, all of them apply to the Enigma itself. Yes, the Germans did not respect the condemnation of written notes / codebooks, but the system allowed for short and memorable keys while the keyspace was big enough to prevent bruteforce attacks.

Because of technological advancements and new insights in cryptanalysis Allied Forces were able to break the encryption during the war, nevertheless the Enigma can still be considered a success.

As elaborated in section 3 all of the stated principles are still of importance today. Some of them can be achieved for free, others still require a lot of engineering in modern systems to be satisfied.

References

[1] Tim Dierks and Eric Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2, August 2008. RFC 5246.

[2] Frank Miller. *Telegraphic code to insure privacy and secrecy in the transmission of telegrams*. C.M. Cornwell, 1882.

[3] Bruce Schneier. Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure. *Computer Security Journal*, 16(1), 2000.

[4] Claude Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 1949.

[5] Gilbert Vernam. Secret signaling system, 1919. URL https://www.google.com/patents/US1310719. US Patent 1,310,719.

[6] Alma Whitten and J Doug Tygar. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *Usenix Security*, volume 1999, 1999.

[7] Wikipedia. Denuvo, 2015. URL https://en.wikipedia.org/w/index.php?title=Denuvo&oldid=689469015. [Online; accessed 2015-11-01].

[8] Wikipedia. Kerckhoff's principle, 2015. URL https://en.wikipedia.org/w/index.php?title=Kerckhoffs%27s_principle&oldid=656551689. [Online; accessed 2015-11-01].