elektor books

A Handbook on DIY

Electronic Security and Espionage

Luka Matic

elektor
design > share > sell

A Handbook on DIY Electronic Security and Espionage

Luka Matic

elektor
design > share > sell

an Elektor Publication

● This is an Elektor Publication. Elektor is the media brand of
Elektor International Media B.V.
78 York Street
London W1H 1DP, UK
Phone: (+44) (0)20 7692 8344

First published in the United Kingdom 2021

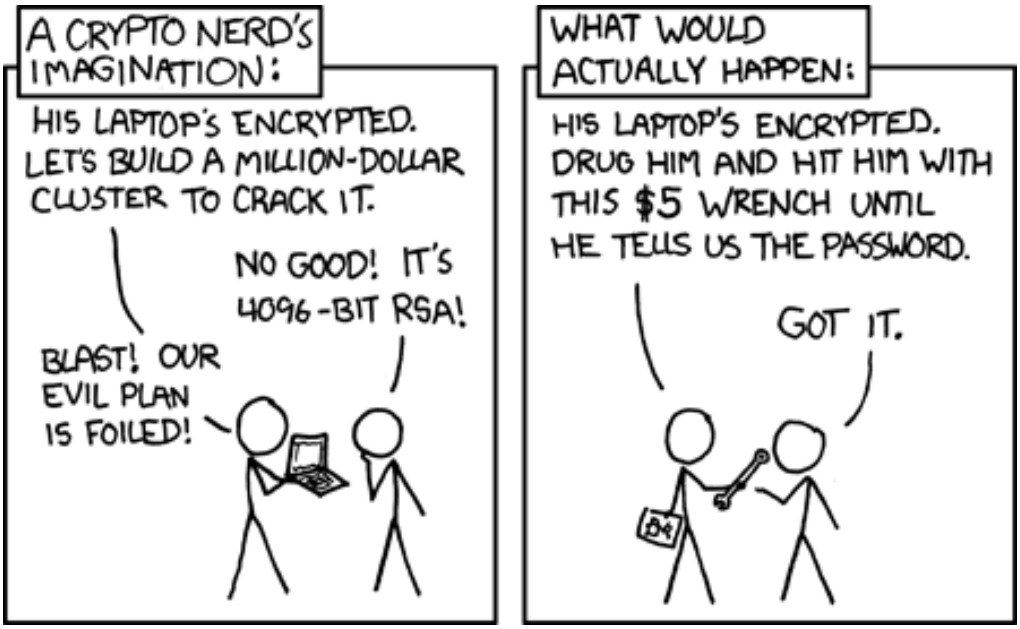
● British Library Cataloguing in Publication Data
Catalogue record for this book is available from the British Library

● ISBN: 978-3-89576-465-3

● EISBN: 978-3-89576-466-0

Prepress production: DMC ¦ dave@daverid.com
Printed in the Netherlands by Ipskamp


FOR ALICE AND BOB:
Stay vigilant.
Speed kills.
Trust no 1.
READY?



The author wishes to express his sincere thanks to XKCD (xkcd.com) for providing permission to include comic 538 in this book.

Table of Contents

Chapter 1 • All security problems solved perfectly - or perhaps not?

Here we are, in the 21st century, and the first 20 years have passed. All the electronics are cheap, fast, digital, highly reliable, highly integrated, and easily obtainable. Electronic components (once upon a time - I still remember) that needed extensive paper-catalogue shuffling, walking shop-to-shop and phone-call searching, and even smuggling across the Cold War borders, are now only a few clicks away. Books are relatively cheap, and fast internet is here for almost everyone - which means all information and knowledge required to design almost anything is also accessible to everyone interested.

On the other hand, **the more technology advances, the less secure it becomes**. This may not be so obvious as the facts in the previous paragraph, but it is exactly why I decided to write this book - I wanted to properly address routinely overlooked security issues of modern hi-tech. Let's first consider some other, also not so apparent facts about electronic technology nowadays.

Almost every electronic device we could have dreamt about (once upon that time) is now a few clicks away. Back then it was obvious that we needed faster computers, higher integration, better display resolution, more memory, faster refresh rates, lower prices, etc. Some technologies have already reached perfection (for all practical purposes) but are still being improved (for some unknown reason) - I am still thinking about buying the newest 800Hz wide-screen OLED, for Toxy, my feline lab assistant. We often watch spy movies together, so maybe he could inform me about the enhanced visual experience (only falcons and cats can process a video signal that fast in real-time) since the most perfect human eyes (like a fighter pilot's) can't notice any improvement above 150Hz.

This book is not about this sort of technology. Such discussion would quickly get boring, so I won't waste your time. Other technologies were suddenly shown to be extremely expensive and overrated hypes - **like invisible stealth aircraft** (almost always advertised as **invisible**, since the 1940s, in the strictest sense of this word, meaning **invisible** at any distance, for any radar frequency, mainly to justify enormous amounts of money spent). In theory, you can expose it yourself by carefully reading the first 50-100 pages of a basic microwave electronics textbook or any decent book on the basics of aerodynamics. In practice, after 50+ years and a probably still never-ending, multi-trillion waste of taxpayers' money was finally debunked in March 1999 with "obsolete" 1960s microwave RF and automation technology revamped by a small group of engineers operating on a shoestring budget. Needless to say, they started their remarkable project by reading their textbooks!

I have nothing original to write about this sort of technology, so I won't bother you with this. I will just remind you of the moral of the whole story - **please read your books carefully**. Don't rush to slap up something too quickly, don't do it to make money, and take your time to decide which project is worth working on in the first place. Don't be intimidated just because your opponent has more money and resources. Rely on your knowledge more than on expensive advertising as much as you can.

Considering the state of art today, it took me quite some time to decide what to work on. What is truly essential? Not available cheap-from-China? Not reliable enough? Above all this, what can be designed and assembled in an average home lab?

The answer is in this book. Simple, reliable, and secure encryption devices fully fit the aforementioned criteria! First, I will explain the basic problems of electronic security and present my solutions. I will try to relate the problems to real-world historical examples. You will see that for every problem solved, a few more also worth solving emerge. Therefore there are lots to work on.

1.1 ● Popular misconceptions

1.1.1 ● (Mis)understanding the basic principles of security

If many electronic devices have already reached the point of perfection, where any further development makes no practical sense, how does this reflect on electronic security and espionage? Hi-tech helps to spy on someone more discreetly and more effectively every millisecond of 24 hours a day - this is very easy to understand, but wait a minute... what happens **the other way around**? This is maybe not so obvious, but the situation is that a high-tech spy can be even more easily **spied upon**, or to put it in other words, the defence against spying becomes more and more complicated. Defending a modern complex system (like any PC or smartphone) is extremely complicated, if not impossible.

Let's first introduce a standard set of "crypto-characters" that are used in the security analysis of various hypothetic scenarios. Alice and Bob are two "good" spies trying to communicate and keep their comms secret. "Evil" Eve the eavesdropper is a passive spy who will try listening to their communications, cracking their codes, following them, dumpster-diving[1], or anything else without actively interfering with them. "Malicious" Mallory is an active spy who will actively interfere - by planting false messages, picking locks, breaking and entering, kidnapping, planting listening devices (bugs), planting viruses, planting pre-rigged electronic components to Alice's workshop, etc... These are four basic characters, and we may add a few more later, like **Trudy** the intruder, and **Walter** the warden.

It is much easier for Eve and Mallory to penetrate Alice's general-purpose PC - they need to find only one weak spot (a general-purpose PC has **many**, trust me), while Alice needs to defend them all simultaneously. Furthermore, she needs **to identify** all weak spots first (to prepare for any kind of effective defence), and this is even harder. This would first require Alice to be familiar with every piece of hardware and software used in her PC and how many lines of machine code Windows 10 OS has to begin with. How many top-class engineers do you know who are proficient with hardware and software, and also with the mathematics of cryptography? With analogue and digital electronics and then with machine code of their PC's particular CPU, and then comes the security...

Security is a chain that is as **strong as its weakest link**, which means that more complex

1 dumpster-diving: collecting information from physical items found in Alice's trash-can.

systems have many more potential links to rip - only one is enough, and evil Eve wins. A typical example of misunderstanding this basic principle of security is the PGP affair (we will address this later in more detail) from the 1990s. Phil Zimmermann did an exceptional job, of course, by programming the **PGP**[2] software, to effectively use the **RSA**[3] public-key encryption and provide good crypto protection to everybody. The real problem that arose is that many people started thinking that **good cryptography can solve all their security problems**. The mathematics of cryptography is perfect: RSA and El-Gamal can't be cracked in any reasonable time if properly configured, the PGP program that implements it on a PC can have a bug here and there, but even if perfectly debugged... it still runs on a general-purpose PC, right? Why should Eve waste her time trying to brute-force Alice's private key, or crypto-analysing the RSA, when it is much easier to send Mallory to plant a key-logger, or a screenshot-capture Trojan on Alice's PC? Or even to eavesdrop on a so-called **TEMPEST**[4] radiation from Alice's keyboard or monitor from across the street? Wim van Eck did it from several hundred meters away in 1980s. Why not record snapshots of Alice's PC's RAM when it multiplies large prime numbers for generating key pairs? Or install a hidden camera to record plaintext on her screen? This paranoid list goes on and on, and I have barely started to analyse it properly...

As we can now see, to fully secure a general-purpose PC or smartphone requires extensive knowledge and painstaking work - i.e. a highly paranoid analysis of every possible weak link in the chain - PGP itself is not enough. Very few top-class engineers have all the knowledge, and even fewer have time and patience to work this all out thoroughly. And yet, many more people need good security and privacy!

Does this mean that our poor, low-budget spies Alice and Bob should abort their operations and give up? Can they do anything DIY at all? Maybe they should start looking for a job in a major 3-letter agency... But wait, big companies have large and complex systems and consequently leak secret data even easier than a single Alice's or Bob's PC, which is already too complex itself!

The good news for Alice and Bob is they **can do a lot on a low DIY budget** - they just have to take a different approach! This is what my book is about. **My main idea is to help Alice and Bob**. I will explain it step-by-step in the following chapters. It will get more interesting, I promise!

1.1.2 ● Why design something new?

This has unfortunately become a very common rhetorical question, even within our community of electronic engineers. Everything is already improved up to the point of

2 PGP: Pretty Good Privacy.

3 RSA, besides El-Gamal, is the most important asymmetric encryption method-using a pair of public and private keys. RSA is based on quick and easy multiplication of two big prime numbers and slow and difficult factorisation of their product.

4 TEMPEST: residual signals inevitably generated and transmitted by all the electronic and even purely mechanical devices. Some consider the name an acronym, while others disagree. It poses a significant security risk. It will be analysed in more detail in chapter 2.

ultimate perfection anyway, so why bother. Maintenance, troubleshooting and repairing of the electronics on existing machinery brings decent money, so why bother with design engineering; it is too difficult, expensive, and time-consuming, and carries too much liability. Maybe just because some problem is there, so let me just try to solve it my way- will make at least a good practical exercise, just to boost my confidence.

After just a little thinking, in the case of electronic security and cryptography, it becomes apparent that the situation in this branch is quite opposite! Good cryptography software (like PGP) is easily available to everyone. Good anti-virus software (including all kinds of software protection, i.e. anti-spyware, anti-phishing, firewalls, etc.) is also easily available, but...

OK, but what about secure hardware? Somebody, please e-mail me a link to some online store to cheaply buy (preferably all in one place, to avoid too much clicking) a good true random number generator, a strong encryption/decryption device, a secure keyboard and monitor, a secure printer, a secure RF burst transmitter/receiver, a tamper-proof storage box, a CPU that I can trust 100% (i.e. 100% certified not pre-rigged with a hardware Trojan and with its silicon die microcircuit blueprints available), **zeroisable**[5] RAM, EPROM, HDD and SSD, a secure device to copy sensitive data between different memory media, reliable thin paper and invisible ink, a secure device to handle bitcoin payments... Most important of all, besides functionality, I want all devices to be fully documented, open-hardware and open-software (preferably with CPU single-stepper option pre-installed), implemented on PCBs with thick enough traces, all test points installed and fully accessible, **so I can check every analogue and digital signal and monitor every detail of every device's full operation in real-time**. The last sentence is my most important requirement (without it I can't trust the equipment to handle my sensitive secrets, sorry) - maybe you will find some well-advertised, very expensive, and overhyped stuff (like crypto-phones or stealth aircraft - remember?), but I am pretty sure that none will fulfil that crucial requirement, the most important one, conditio-sine-qua-non.

Checking a device's functionality is easy, but testing its security is very difficult, especially if it is a black box. If Alice can't test and check every aspect and scenario of its operation, it is simply not trustworthy - this is the way things are and it is regularly overlooked.

Most of the aforementioned hardware simply doesn't exist. It is much easier to design and assemble something trustworthy yourself than analyse another engineer's design. This is one very important fact, self-explained, but also vastly overlooked. This is simply the way things are. Many more devices that haven't come to my mind yet are also needed, but surely not readily available off-the-shelf.

This is exactly why it makes sense to work hard on your own designs.

5 Zeroise: to effectively fully erase a medium without any possibility of data recovery.

1.1.3 ● Moore's law and its corollary on security

Moore's law is a very well-known empirical fact - the number of transistors on the highest-integrated IC approximately doubles every year. This means that track width consequently decreases (from μm range in the 1970s to nm range today) and prices go down, while performance keeps increasing, practically everything in a favour of the customer.

There is also a less known Moore's second law which states that as prices for a customer decrease, prices for a producer (R&D, manufacturing, and testing) increase to fulfil Moore's first law.

So how does this reflect on the security of electronic hardware? Moore's second law may give you a hint - the expenses of **testing** a higher-integrated IC are getting higher. OK, but this refers only to testing of that IC's **functionality**, not **security**. If the cost of testing functionality of a more complex IC becomes higher, it unfortunately, means the costs of fully testing its security become exponentially higher! Why? Functionality test of an electronic device is a test to confirm only if its performance within **normal operating conditions** (which is a set of pre-defined specs) simply meets these specs. A security test is much more complicated -mainly because this is not a test within the scope of the pre-defined specs of some normal conditions. To test security, we need to think of a much wider scope of conditions. Attackers don't play by the rules, and definitely not within the range of any pre-defined specs. They are devious and unpredictable. Testing security requires many independent experts and lots of time. New designs (higher integration, narrower tracks) are more vulnerable than old ones that are robust and already tested and re-tested over a long period. Furthermore, integrating a device makes it less secure than physically splitting it into multiple ICs or modules - a highly integrated version will have much fewer accessible test points to test various signals and will also provide more opportunity to Mallory to plant hardware Trojans undetected.

Testing the security is much more complicated and hence more expensive than testing the functionality - this means that it requires extra financial investment that is rarely justified and never returned in a reasonable amount of time.

To sum it all up, as technology advances and the level of integration, speed, and overall performance increases, the level of security decreases even faster! We will analyse this in more detail later, as we continue to reveal many other pitfalls of modern highly integrated electronics. All modern trends of electronic technology progress tend to work against security! Seems a bit unintuitive? Well, there will be more to it - I have barely started…

1.1.4 ● Espionage in the past and present

Now we will make a comparison between the level of technology and methods of espionage and counter-espionage available to Alice, Bob, Eve, and Mallory with a focus on the distinction between the 20th (and before that) and 21st century. We will see that advanced technology in the 21st century changed not only the technical aspects but also the basic methods and principles of espionage compared to the previous era.

I was born in Yugoslavia - a communist dictatorship, not so technologically advanced like the Soviet Union or East Germany. Unlike them, Yugoslavia was very short on highly educated and trained personnel in its 3-letter agencies. As a member of the **Non-Aligned Movement**[6], it wasn't actively involved in the Cold War between East and West Bloc (or more precisely, Warsaw Pact and NATO) and the high-tech arms race. Consequently, it didn't need any high-tech espionage to keep its regime in power. Its 3-letter agencies dealt only with spying and intimidating Yugoslav citizens, using mostly very "low-tech" methods. With nothing of interest going on in my neighbourhood, I started reading books. Good spy movies were difficult to get. In 1985, when I got my first computer, a Spectrum ZX-48, smuggled from Trieste (Yugoslav civilians were not allowed to buy computers, because "an enemy might get a hold of them"), a crossword-puzzle magazine "Kviz" by "Vjesnik" from Zagreb started publishing a series of fictional spy-story puzzles under a very catchy name - **"A crash-course on clandestine diplomacy and espionage"**. They caught my attention immediately: the puzzles were extremely difficult to solve. I started buying every new issue of Kviz the day it arrived at the local kiosk, although it got me wondering how it slipped through communist censorship since this could also provide the "enemy" with a lot of useful knowledge, the same as it did for me.

Now heavily armed both with illegal high-tech from the West, and newly gained knowledge, I decided to try to do some cryptography on my Speccy. I made BASIC programs, first for **Caesar's cipher**, and then more advanced **Vigenere's cipher**, and then ran into problems with truly random numbers for **Vernam's one-time pads**[7]. To get ready for Morse Rx/Tx (any Cold War spy's long-range tool of trade), I made a program to convert ASCII text to Morse dit-dit-daah and the other way around. Then I hacked my Sinclair joystick to connect my Morse key to its fire button… At least I got my first nice taste of "forbidden" and learned what an "enemy" might use it for.

In 1989. The Berlin Wall went down, followed by Yugoslavia later in 1990, and we finally got first democratic elections, only to get another dictator (one of the last in Europe), until he died in 1999. At the time, I was 23 years old, a student at FER Zagreb, now with the experience of living under two different dictatorships and more technical knowledge, so I started thinking of ways and means to make some use of it.

And then came the 21st century: I started my cooperation with Elektor, and finally got to start solving real cryptography problems in practice (that I was thinking over and over for quite some time then) and publishing articles with working prototypes. New methods and threats appeared, requiring a new approach.

To start solving security problems, we need to properly identify the threats first. This is

6 NAM was a 3rd Bloc during the Cold War. Enabled a certain business cooperation among the 3rd World countries, independently of NATO or WP Bloc. Yugoslav president Tito, Jawaharlal Nehru of India and Fidel Castro of Cuba were the key persons. NAM actually survived the end of the Cold War, but its political influence nowadays is not significant.

7 OTP, or Vernam's cipher is the only method that can be mathematically proven as unbreakable, if properly used. Its key is a very long sequence of random numbers, as long as a plaintext message. Each random number is used only once, to encrypt one letter of the plaintext, usually by bitwise XOR-ing. All encryption methods will be explained later.

why it is important to make a clear distinction between 20th and 21st centuries. In the 20th century, technical resources were limited, which required more manpower. Consequently, it was possible to spy on and survey only a limited number of citizens. A tape recorder had to be hooked to your phone line, and an agent had to replace the tapes (they had limited capacity, up to several hours). A radio transmitter bug (a covert listening device) had to be placed hidden inside your office. Then some unfortunate agent had to listen to kilometres of tapes, just to conclude that your "discussions" with your wife, mistress, and mother-in-law contained nothing security-critical for the government. Cameras were still big, unwieldy, and expensive and hence only used in some special situations. Following a suspect on a street required physically tailing him on foot or by car, and such surveillance could be evaded. Most important of all, you had to be engaged in some suspicious activities first, before STASI[8] would dispatch a team to follow you and record your conversations. This means that it wasn't dangerous to tell a political joke over an analogue telephone, because the conversation was probably not monitored. One more important detail - civilian and military systems used different hardware, software, and communication channels. Real-time encryption of telephone communications was seldom used, mainly because of the too expensive hardware required. On the other hand, although getting the radio frequency assignment chart from the government was usually difficult, after re-tuning your AM or FM receiver out of their standard bands, it was possible to listen to e.g. police or air-force conversations because they were not encrypted in real-time. Most of the high-tech equipment was very expensive and hence not available to low-budget rogue spies.

Alice and Bob could safely use payphone-to-payphone calls to securely exchange encrypted messages. After finishing the call and wiping their fingerprints, they could safely leave. Many more payphones were in service than nowadays, and waiting for a call beside a payphone wasn't considered suspicious behaviour - especially while cellphones were not yet available (or still too expensive). Landline connections were still very expensive in some areas; so many houses didn't have a phone line installed. Payphones were not under 24/7 video surveillance - so Alice and Bob didn't even have to bother wearing a disguise. Even if the conversation was taped, this meant nothing, because they wouldn't use the same payphones twice. If intercepted by Eve -a human operator, a payphone-to-payphone conversation sounding something like **"Bravo-3-6-8-7, Oscar-5-0-9-1, Yankee-4-9-6-4, Lima-2-7-5-1…"** during the Cold War would immediately alert the counter-espionage, but the time needed to trace the call, locate both payphones and dispatch the police was surely more than 10 minutes- so Alice and Bob were safe as long as they kept their conversations shorter than 5 minutes. Btw, this is exactly why Yugoslav communists **disabled** payphone-to-payphone calls. An "enemy" could definitely have tried using them.

Now, in the 21st century, most of the aforementioned has changed. Cameras and microphones are everywhere, almost all online (some are not 24/7, but you usually don't know which, where, and when) and networked. Every smartphone, PC, and even old GSM phones can easily become personal listening devices, by only uploading and activating a software Trojan. No need for Eve to waste time listening to bugs planted under your desk. Everything is recorded and kept. HDD storage space is almost unlimited, so Eve doesn't

8 Ministerium für **STA**ats**SI**cherheit - East German intelligence until 1989. Not 3, but 5-letter agency known for their very high-tech methods, many invented by their own experts.

need to bother with connecting tape recorders and replacing tapes. Artificial intelligence can analyse the conversations and flag them if there is something suspicious, so it can be reviewed later by a human operator. No need for agents to follow you around, on foot or by car, since cameras are everywhere, and more and more of them are being installed. Your activities are recorded and kept even if you are not under any suspicion. Today, civilian and military systems often use the same hardware. A NATO officer's laptop may be a "Toughbook", but is still a general-purpose PC running under Windows OS. Almost all conversations are digitally encoded and encrypted (GSM, VOIP, different protocols), so just knowing the RF frequency of the GSM signal will not enable Eve to listen in. The prices of modern high-tech came down to the point where they became affordable for our low-budget spies.

I mentioned the payphone-to-payphone calls previously just to point out how drastically some security aspects have changed. Being one of the **safest** methods of the 20th century, this has now become one of the **least safe** methods! Now, with cheap cellphones available to almost everybody, Alice will need to have a very good excuse for standing by a CCTV-monitored payphone waiting for Bob's call. She will also need a very good disguise, actually several disguises ready to change quickly, and an even better escape plan, since she can expect every street in an average urban area to be at least partially monitored by at least one camera. The total number of operational payphones today is down to 5% of the maximum reached at the turn of the century, so Alice and Bob will have a hard time finding a new pair of payphones for each contact. Their conversation, now surely recorded and monitored by Eve the Artificial Intelligence will be immediately flagged, mainly because nowadays it is an extremely rare payphone-to-payphone call, and secondly due to unusually high percentage of numbers and spelled letters. Detection of location and reaction can be practically immediate, and evading the video surveillance after the call is very difficult.

With this in mind, it is important to get tuned to the rules and state-of-art of the 21st century - from my experience, I can tell that most people, even those born in the 21st century are still adopting a 20th century's mindset and this is not good. Alice and Bob must adapt their actions to the new rules, or they are lost.

1.2 ● Omnipresent, unrecognised, and unaddressed problems

Proper identification of threats is crucial before we start to solve security-related problems. Otherwise, it is pointless. In this section, we will see how important it is, and unfortunately routinely overlooked.

1.2.1 ● Liability problem

Maybe not the best one to start with, but the main reason is that almost nobody is aware of it. Let's start with a basic definition: an entry from the Oxford Dictionary, to be **liable** means to be held **legally responsible** for something.

This is relatively easy to understand in areas like e.g. civil engineering, shipbuilding, or electrical power engineering. A civil engineer is held liable if a bridge built according to

his drawings collapses, e.g. because he made bad structural calculations. A construction contractor is liable if he cuts corners and builds a cheaper bridge not according to design plans from the civil engineer. A facility manager is liable for refusing to evacuate a building that started to structurally fail hours before the main collapse (happened with the Sampoong Department Store in Seoul in 1995, along with lousy structural calculations and even worse construction job). A ship's captain is liable for the sinking of a ship because of disregarding safety procedures, etc.

Bad **safety** practice makes you liable for an accident, but what about bad **security**? Safety and security are two different things: I learned this in the 5 years I spent on board offshore construction vessels and oil drilling rigs. Safety means protection against **accidents**, while **security** refers to **deliberate attacks**.

There is much less liability in the world of security. I don't know much in detail about the legal side, but this is just a common practical fact. Police or private security guards are not liable for failing to protect you if you get wounded during a bank robbery. The police chief may be fired or demoted for failing to solve a string of bank robberies. Bad security guards can be sacked and replaced. My offshore construction company used to hire highly unreliable security for sailing through the Gulf of Aden (luckily, I never sailed on board one of those ships). They used to leave their loaded handguns everywhere around the ship, but they were much cheaper than professionals.

The situation in the world of electronic security (both hardware and software) is even worse. Vendors of bad security software (anti-virus, anti-spyware, firewall...) are **not liable** for any damage caused by malicious hacker attacks. Software security companies have another possibility that others don't have - if there is a security weakness exploited in ver 4.2, a patch will be uploaded to this company's website for everyone to download and upgrade the firewall to ver 4.3. They will consider the problem solved. Civil engineers or shipbuilders don't have this "luxury". Our ship sank due to structural failure, but ver 2.0 will be unsinkable, we promise. This is another reason why electronic security is often taken too lightly, by everybody involved - designers, vendors, and end-users.

Until something changes from the legal side, Alice and Bob will have to take more care about their security themselves, especially regarding hardware security - reliance on software security products is not enough. Anyway, they can't buy insurance against damage caused by leakage of their critical data to Eve, especially not if their operations are **illegal**.

1.2.2 ● Failure to recognise important problems to solve

Before we start to design any security features, we first need to identify the real threats. The full scope of threat to defend against is seldom as obvious as it may seem. A simple example is wasting money and time installing a brand new 10-pin pick-proof lock on a plywood door, while also forgetting to put steel bars over a glass window in your basement. Why would anyone try to pick the expensive lock with mechanical pick-proof features when is it easier to slam on that weak door or even more discreetly break the basement window?

This is a very simple example, but the following are not that obvious:

1. Alice uses one-time pads, with perfect true random numbers sequences to communicate with Bob, so Eve can't crack the encryption. Alice uses the pen-and-paper method to encrypt messages before transmitting them by keying in manually the Morse code to a long-range shortwave radio transmitter. She prefers manual operation to prevent electronic leakage of data (more about this later). First, we will set it up in the Cold War stage. Let Alice be a Soviet spy in a safe place in Moscow. Bob is an illegal operating in the USA, and Eve is FBI. In this setup, Eve will have a very hard time trying to catch Bob. The communication is only one-way, and the encryption is unbreakable. Eve can try radio-locating Alice's transmitter (may be difficult at long distance, after several ionospheric reflections and refractions). Eve can tape Alice's transmissions as samples for later comparison. Bob can securely receive Alice's transmissions without drawing any attention from his neighbours - maybe he will suspend a few wires in his wooden attic to make a better shortwave antenna if the signal is weak. Eve could theoretically pick weak residual radiation coming from his **superhet**[9] receiver's local LO-RF oscillator, only if she is very close in his neighbourhood- but he can also use a **TRF**[10] receiver to mitigate this if he reaches that level of paranoia.

   Now if Bob needs to transmit a message to Alice, things will get complicated. Eve still can't break his encryption, but the mere fact that he is transmitting an encrypted message may put him in trouble, after a successful triangulation of his position. This still doesn't flag him as a Russian spy, especially if he has a radio-amateur license - there is still no evidence that the message was sent to Alice, so he can get away with it.

   The situation will get tough if Alice comes to the USA to operate as an illegal afterwards and starts transmitting. Eve will immediately know that she is a Russian spy after comparing her new transmissions with previously recorded samples sent from Russia. Every telegraph operator has a distinct rhythm of keying - like a signature or a fingerprint. The normal ratio of duration between dash and dot is 3:1, while a space between should be the same duration (1:1) as a dot. Some operators will have more like 2.8:1 for dash/dot ratio and 1.2:1 for dot/space. Besides these ratios, there are spaces between letters and words, and you get the operator's full signature. Since a Morse key also exhibits a button-bounce effect (like any mechanical switch), it is also

9 superheterodyne receiver: by mixing the RF signal received in antenna with a sinewave RF from a variable local oscillator (LO), a signal of the same baseband, but much lower carrier frequency (IF-or intermediate frequency equals a difference between LO frequency and received RF carrier frequency, typically 455kHz for 3-30MHz shortwave RF) is generated. Unlike TRF, the following amplifier stages need to be tuned to one fixed IF frequency only once, without the need to re-tune during operation. Tuning a superhet receiver to a transmitter station is done simply by varying the LO frequency.

10 tuned radio frequency receiver: no local oscillators, no IF. Every amplifier stage must be tuned and re-tuned to RF carrier repeatedly during operation. Variable RF tank circuits are much less selective than fixed-frequency IF filters. Low IF is easier to amplify than a much higher RF. TRF receiver is difficult to manually re-tune in operation (too many variables), but this may not be needed, if listening to the same RF frequency most of the time. Outperformed in any technical quality aspect by a superhet, except for the security - LO can always leak a few nW RF power to an Rx antenna. A good TRF has absolute zero RF leakage.

possible to identify the telegraph operator by dynamics of his hand's motion! With this in mind, Alice will have to quickly relocate and conceal her transmitter and antenna after each transmission.

The moral of this story is that even perfect encryption is not enough to secure your communications. Yet many people don't understand this - many thought PGP running on a PC would solve all the problems.

The threat of cracking the encryption in this example was solved perfectly, but if Alice and Bob didn't recognise the threat of radio-location and identification of operators by their Morse transmissions, they would lose.

This is why, besides encryption, RF engineers needed to invent burst-transmitters, spread-spectrum, frequency hopping, and other methods to conceal communication itself.

Besides the three threats in this scenario, perhaps there are even more threats from Eve and Mallory. Can you think of any?

2. With this in mind, it is easy to see that the same can happen if Alice and Bob try the same with an analogue modem on a classic telephone landline - the messages are encrypted, but the switching information for the telephone exchange is still sent in plain and therefore the call can be traced and located.

3. Even without encryption, many people think that if Alice and Bob buy cellphones for cash in a street, with a SIM card with top-ups also paid in cash that this will conceal their identity. Radio-location today is even faster, especially when aided by a smartphone's GPS, and analysis of contacts dialled can reveal the identity-especially if apart from the two of them they call other people, whose phones are registered. Above all, the identification of an individual human's voice is even easier than his Morse transmissions. Even if they decide to use some kind of voice distortion, they need to know that some distortion algorithms are reversible, and they, therefore, need to choose carefully one that reliably and irreversibly removes the redundant information from the human voice signal.

4. Telephone companies, both landline, and mobile invested a lot to prevent theft of their services. Even then it was not 100% effective (remember the Blue-box, Red-box, cracked stored-value payphone cards...) The point is that theft of cheap phone calls is a much lesser problem than the theft of identity and making phone calls with the stolen identity of legit users. Much less has been invested to solve this problem.

5. Sometimes, solving one security problem will cause another more dangerous one to arise - **but you may be unaware of it**. Car alarms became popular in the 1990s, mainly due to them becoming more affordable. **Car theft** was increasing steadily during that time, while I studied on FER. What car owners failed to realise is that investing to mitigate a car theft, even if 100% possible with a perfect car alarm immediately

puts them in danger of **carjacking**[11], which is a way more dangerous attack. Some carjackers in Zagreb resorted to killing drivers (!) instead of forcing them to drive at a gunpoint, which they considered less practical. Then one company started advertising footswitch-operated **flamethrowers** as protection against carjackers. I solved this problem by buying a 1979. Citroen GS for 1000 DEM. It served well until the end of my studies, (both for driving and learning about non-electronic hydraulic-pneumatic control loops on a piece of practical machinery - I was at the automation branch) and no decent car thief would ever try to steal it. This is another example of what can happen because of poor threat identification.

6. Now it's your turn. Try to analyse the possible problems for Alice and Bob if they use newspaper ads to secretly communicate. This method was allegedly popular during the Cold War, although I don't know of any confirmed real-life instances. Anyway, the overall concept seems very secure and difficult to detect. It goes something like this: Alice places an ad in a newspaper with a message for Bob. Some of the ad's text is meaningless, but some part contains an encrypted message (concealed to look like a normal plain text). Bob buys the newspaper (in paper form) at a local kiosk, then reads the ads without drawing any suspicion whatsoever. He knows how to recognise a message from Alice - to all other 100.000 people who bought the newspaper today (including Eve and Mallory) it looks just like an ad to sell an old second-hand Ford. No traces left.

   Movies have been made about some "Eves" of the Cold War who had become maniacally obsessed trying to decode non-existent concealed messages in newspapers' advertisements (and crossword puzzles as well).

   Now, to point out another important problem - encrypting a message is one problem, concealing it (hiding the fact that an encrypted message is what is being sent) is another problem. As we have just seen previously, concealing Alice's and Bob's true identities, and/or the mere fact that they are communicating is yet a third problem. Besides our usual set of four crypto-characters (**Alice and Bob**, trying to secretly communicate, **Eve** eavesdropper, passive spy, **Mallory** malicious active spy) we need to add **Walter a warden**, **guarding Alice and Bob**. He may be a prison warden if Alice is in his jail and still wants to communicate with Bob. It may also be a 3-letter agency of a repressive dictatorship. In this case, all Alice's messages are checked by Walter. He doesn't bother decrypting them (Eve will try to do this part), his job is to check Alice's messages for possible concealed ciphertext. Alice will not do well if her message looks something like "143-231-525-BV, 45-834-56-AF, ..." -Walter will immediately notice something suspicious. If she tries writing a normal-looking love letter to Bob, where e.g. every first letter in every word is a character of a ciphertext, then Walter will probably not notice anything suspicious and pass it on. This is called **steganography**: hiding secret messages in other messages.

11 Carjacking: hijacking a car, usually along with a driver, typically at a traffic light or parking lot.

In the case of secret messages in newspaper ads, the newspaper's editorial staff takes the role of Walter - they will certainly not publish a meaningless sequence of numbers as an ad. If Alice puts a non-existent 10-digit phone number as a contact (which is an encrypted message to Bob), this will probably be passed off as a typo. On the other hand, if Walter is on high alert, he may request the dialling and checking every phone number...

Your turn to continue this analysis! Are there any possible dangers for Alice and Bob? What methods of concealing the messages can they use? What are the possible traces they could leave? What is better from a security standpoint- printed newspaper or internet ads? Try to identify as many threats as possible!

1.2.3 ● Black box problem: Why should I care HOW my super-gizmo gets its work done?

Well, you should. As long as it does what it is supposed to do, nobody cares. This is OK for most of the devices you use today - because we are mostly concerned about functionality, not security. If it fails to work, you can claim a warranty and request a new item. But if it leaks your critical secret, you can do nothing - you should have thought of security and done something beforehand.

I will address the black box problem again in more detail several times in the following chapters; I must start here because it is increasingly **omnipresent**, regularly **unrecognised**, and almost always **unaddressed**.

If it is a black box, you can't analyse its security- this is the main problem. Furthermore, opening a black box device will surely cancel any warranty, put you in a breach of a contract, and may even be illegal. One of the best solutions is to design something new, open-source, so it can be tested, and constantly improved and contributed to by other independent experts.

1.2.4 ● Reluctance to properly address the "impossible" scenarios

This may look like another case under sub-section 1.2.2, but it isn't. In this case, Alice is aware of a possible threat. She properly recognises it, but doesn't point it to Bob because she thinks it is almost impossible, or because she thinks Bob would consider it ridiculous. Therefore, the threat is disregarded, and the consequences may follow.

The point is that many dangerous scenarios in this world are "not impossible- just highly improbable" (my favourite line from "The Hitchhiker's guide to the Galaxy"). Let's analyse a few examples and see in which way the highly improbable threats were considered:

1. During the Cold War, the actual invasion of West Europe by the Soviet army (and other members of the Warsaw Pact) was considered improbable, but still possible. The scenario of full occupation and collapse of West Europe, especially along with Great Britain (hasn't been invaded for almost 1000 years), where only small guerrilla armies are left to fight, sounds impossible today - especially for those of you born after

the Cold War. In the 1980s it became obvious that the Warsaw Pact started facing serious economical problems, although they were still keeping up with the West in high-tech engineering and arms race. Some NATO analysts considered though that the Warsaw Pact armies were in much better combat readiness at that time than NATO. Consequently, some of them concluded that WP might attack first, to use this temporary advantage before their communist economy collapsed.

Following this line of logic, to prepare for this worst-case scenario, the **FS-5000 Harpoon project** was started and finished with a fully functional portable long-range radio-communication system. It was designed and produced by well renowned TELEFUNKEN AG, not by some crazy conspiracy theorist, basement-dwelling social outcasts.

The design requirements were set very high:

- several thousand kilometres ranges, **without any land-based or satellite repeaters**
- to be operable by unskilled operators i.e the guerrillas fighting in occupied West Europe
- the size of a briefcase, battery-powered, lightweight, with portable antenna

Sounds "impossible"? Scenario or design requirements? Or both? Well, I know very few RF engineers nowadays who could tackle this, and I know even fewer engineers who would ever try to follow this line of security analysis.

2. Some people working in very tall skyscrapers allegedly keep **parachutes** in their offices. This idea is of course ridiculed by the vast majority, even after 9/11. More than 200 serious skyscraper fire incidents have been reported throughout the world, often with fatal consequences. Big skyscrapers are several hundred meters tall, and successful parachute jumps have been reported from heights as low as 30 meters. A fire brigade chief once remarked to a civil engineer designing a 200-meter tall skyscraper - "Excuse me, sir, there is no safe way to fight a fire above the 10th floor - and yet you keep building them higher and higher". Is a skyscraper fire (and also any other skyscraper disaster) a scenario so "impossible" that a parachute and a parachuting course are a waste of money?

3. Small knives and many other innocuous objects are strictly not allowed to be carried onboard an airplane. On the other hand, **lithium batteries** are perfectly OK, 2-3 pieces on an average passenger nowadays. They are consumer-grade mass products without any serious certification. Any one of them (if it fails) is a potential **incendiary bomb**[12], **poison gas-smoke bomb**, and even an **explosive bomb** if you are very unlucky. Imagine the mayhem that it can cause inside an airliner's cabin (and in a luggage hold as well). Try searching YouTube for "lithium battery explosion" and enjoy

12 Unlike "**flammable**", which denotes a high tendency to accidentally catch fire, the adjective "**incendiary**" actually refers to weapons deliberately designed to cause fire like napalm or thermite bombs or Molotov cocktails.

watching. Is the hazard of a Li-ion battery catching fire so low that it can be considered "highly improbable" or even impossible?

4. The danger of TEMPEST eavesdropping (more in detail later) is regularly neglected, even in high-security buildings. A usual excuse is that it requires too high-tech which is expensive. The first accidental TEMPEST eavesdropping dates back to 1916 - the equipment used was very low-tech. Most deliberate TEMPEST attacks have been mounted with less than $20.000 of equipment.

5. Try watching the "Doomsday Preppers" series. Almost all disastrous scenarios are at least theoretically possible. At least 50% are correctly worked out with good quality solutions proposed, and from at least 25% you can pick up nice ideas from an engineering standpoint. Yet, most people will consider it to be "an impossible" conspiracy theory nonsense, even those with a real-life experience of **full-scale war**.

Electronic security, if mixed with espionage in any way is the last place where a "highly improbable" scenario can be neglected by Alice and Bob. Unlike natural forces, their enemies Eve, Mallory, and Walter must be considered unpredictable, devious, cunning, extremely patient, and well-funded, and expected not to play by any rules or laws whatsoever.

1.2.5 ● The problems that electronic engineers can't solve

Cryptography solves only one part. Good electronic hardware design solves another. The same goes for carefully elaborated security procedures regarding the use of electronic equipment. Also for good technical education of your personnel. Electronic engineers can only build better electronic devices – everyone has to educate himself to attain a security-conscious mindset.

Apart from this, there are many other aspects of security that have nothing to do with electronic engineering or mathematics. Good electronic devices are necessary, but security is not all about high-tech.

For security to work, the end-user must be aware of threats- most of an average company's employees (even of one directly involved in security business) are either unaware or not motivated enough. This leads to negligence - the best crypto-electronics can't help here.

Read any of the books on Kevin Mitnick. Most of his exploits were about **social engineering**, the rest about programming and electronics. The social engineers' main rule is "If you don't have information, it's because you haven't asked for it yet." An amazing amount of secret information can be extracted by simply **asking for it**. This circumvents any electronic security and cryptography - a target under deception usually has all the passwords and security clearance required. Electronic engineers can't help here. Sorry.

Kim Philby spent more than 30 years in the top ranks of the British intelligence spying for the Soviet Union. He was a spy who inflicted more damage to the west than any other. No cryptography or electronic engineering could have been of any help here. He had access

to all codes and passwords. British electronic engineers and cryptographers were highly skilled, of course. It wasn't about them, but other professions, like e.g. psychologists, to make a careful screening of job candidates to detect those suspicious.

Detecting possible spies is very difficult because people of very different psychological profiles start spying for very different reasons. Some spies did it simply for money- some of them were drug addicts who had to support their habit, others had a too demanding mistress. Others were social outcasts in the west who falsely believed that communists would always be on a side of an underdog. Some people feel that they don't belong to **any nation** - not directly associated with the usual national divisions of this world, they will cooperate with any side that seems OK. Some people simply believe in a certain ideology (a belief which is usually a self-generated justification) but based on different past experiences. Some spies ended WWII on the Axis side and survived - when they became involved in the Cold war, they did it mainly because they wanted to get a taste of victory (some on WP, some on NATO side!) - having lost one war was too much frustration they couldn't handle. Some did it because they found it exciting and high-tech. The list of unusual psychological profiles goes on and on.

This might be interesting, but as you can see, this is a job for someone else. In this book, I will concentrate on the problems that we **electronic engineers can solve**.

1.3 ● Low tech rules - very unintuitive

Having read up to now, this should have become a little less unintuitive. In 1.1.3 we analysed how a higher level of integration of an IC decreases security. To prove the point, or to expand it a bit, let's make a security comparison of various long-term memory storage technologies throughout history. The main comparisons will be concerning:

- density of data storage
- price
- long-term storage reliability
- the possibility of fast and practical irrecoverable destruction of data (irreversible erasure or so-called zeroization)
- the possible existence of uncontrolled secret storage space
- susceptibility to TEMPEST eavesdropping
- possibility of detecting the author based on residual data

1. **Pen and paper** - cheap technology with the lowest density of data storage. If stored properly, will keep information for more than 1000 years - we've had enough time since the beginning of civilization to test it in every way. **Longer than any other technology**. Information on paper can be very easily zeroized by fire, ingestion, micro-shredders, or strong acid. There are no secret sectors on a sheet of paper, although there are technologies (like micro-dots and invisible ink) to hide information on paper -this will burn along with all other data when lit. Without any energy radiated, it can't be attacked by any means of TEMPEST. The only downside is that an author can be easily detected based on handwriting (learning to write with your other hand helps here). Altogether, **very reliable technology** from a security standpoint!

2. **Mechanical typewriter** - with a much better speed performance than pen and paper and a slightly higher price, it keeps most of the positive traits of its predecessor. It is also much harder to trace the text back to its author (analysis of handwriting is much easier), but still possible - the STASI were very good at this. Not only that they could link a typewritten paper to a particular typewriter, but also determine **the language** in which most of the plaintext was written. If the typewriter was used to write **ciphertext instead of plaintext**, it was even easier to detect, putting Alice immediately in a lot more trouble! How? Try analysing it yourself. If you are not sure, try again after reading the whole book: it will give you many leads!

3. **Electromechanical typewriter** - worse than 2.) - also transmits residual electrical pulses for another type of RF TEMPEST, and adds a possibility of planting an electronic key-logger as well.

4. **Analogue film tape** - stores more information per mm^2 than paper or magnetic tape, for a higher price. Requires chemical processing and can't directly convert information to electrical signals (like magnetic tape). Holds data reliably for more than 100 years. Burning or dissolving in a strong solvent will quickly destroy the data. **Microfilm** form (a film with higher storage density) has been any savvy spy's standard tool of the trade for many years. There is no possibility of secret storage space. An analogue camera has no useful TEMPEST radiation. On top of all this, it is very difficult to trace a film back to a camera! **A very reliable technology indeed**.

5. **Audio and video magnetic tapes** - both have been successfully used in past to store digital data. Reliable for more than 50 years, but prone to wear and tear, especially on low-quality tape decks. Special variants have been made to directly record digital data, required specially designed tapes and drives, for a much higher price. Fire or strong solvents quickly and effectively zeroize the data. Video tape systems with bandwidths up to 6MHz store data with much higher density than audio tape systems (up to 20kHz), but as a consequence, they radiate much more RF TEMPEST. There is no secret data space on audio tapes, but the latest generation VHS VCRs had some

metadata[13] recording features. Because of this metadata, a certain VCR could leave its "fingerprint" to be detected later, which is almost impossible with audio cassette tapes. As you can see, **audio compact cassettes** are a more favoured tool: cheap and still easily available in the 21st century. We will address them later.

6. **CD and DVDs** - considered to be very suitable for long-term data storage at the beginning, but is now apparent they degrade after 25-30 years. Although their data density is much higher than tapes and the price may be even lower, they are not very favoured from a security standpoint. First of all, they are difficult to destroy. Hidden sectors are difficult to mount, but secret metadata (to identify the drive and author) can easily be hidden because the user loses direct control over data recorded to CD/DVD. TEMPEST radiation, especially when burning a disc, is high. Existence of read-only and read/write drives gives a possibility of ensuring data integrity after writing - can't be tampered with by use of a Trojan when used inside a read-only drive.

7. **UV EPROM** - easily available even nowadays, cheap, with an average data density, and very good from the security standpoint. Can reliably hold data for up to 30 years. Illumination with strong UV light destroys the data, but it takes up to 10 minutes. No secret sectors, maybe on some newest type, but not on standard ubiquitous 27C type that is still straightforwardly available. Metadata for identification is difficult to hide because users can easily control every memory block written. TEMPEST radiation is less than CD/DVD. Tampering with data in runtime by a Trojan is not possible, because 12-14 volts must be connected to a Vpp pin to write digital zeros, and UV light is required to revert all bits to digital ones.

8. **HDD discs** can reliably hold the data for up to 20 years, but it is recommendable to make earlier backups. Data density is very high, price is satisfactory. With the old types in CHS[14] mode the user could have had some control of writing individual physical sectors, but this is fully lost with the new LBA[15] mode. This means that undetected hiding of secret sectors and metadata is very easy, and difficult to detect. Secure zeroization is difficult, the only method to ensure irreversible deletion is heating up to Curie temperature, which is very impractical. Above all this, TEMPEST radiation is high due to the high frequencies involved. **A bad technology from a security standpoint**.

9. **SD cards, SSD, FLASH**, anything based on solid-state. The situation is bad enough with HDD, and here is much worse, in almost all aspects. They can't hold the data

13 metadata: additional data created to provide information about the main data stored on a medium. In case of a VCR, the main data is audio and video signal (or digital data encoded like PAL video, if VHS tape is used to backup digital data). Metadata could be a unique serial number of the VCR and time and date of recording, inserted by the VCR itself. Metadata inserted without Alice's knowledge can be very dangerous, especially if created by Mallory's Trojan planted to VCR's firmware.

14 CHS: Cylinder-Head-Sector - an old method of accessing data on a HDD by directly addressing its physical location on a disc.

15 LBA: Logic Block Addressing - a new method, addressing logic blocks, not physical locations directly. They can be routed to different physical locations on a disc.

reliably for more than 10 years. Price and data density are practically the best, but every other property is worse. Because individual memory cells tend to fail over time (an inherent property of SSD devices), the internal MCU keeps rerouting the data to alternative physical locations. The user here absolutely loses control of which physical sector of the SSD device is written and erased- the internal MCU takes care of this dynamically. A 16GB SD card is likely to contain more than 32GB of raw memory space - the rest is a reserve to gradually fill in the bad sectors as they fail. Some sectors are copied to several physical locations, all without any control from the user -this process is called **write amplification**. A secure zeroisation is possible, but only by heating to at least 1300ºC, which is much higher than any material's Curie temperature and hence even more impractical. The presence of ABUNDANT storage space is necessary for SSD technology to OPERATE, for the reason of the inherent physics behind all low-voltage SSD devices. Abundant storage space is not needed for HDD, UV EPROM, cassette tape, and any other memory technology, but it is needed for SSD devices (like flash memory, SD cards, SSD drives...)
Secretly recording metadata for identification is also simple. Secretly changing critical data in runtime is very easy - unlike with 27C UV EPROM - FLASH and EEPROM can be erased and written with low voltage. **All in all, Alice's and Bob's nightmare, but Eve's and Mallory's sweetest dreams**. Regardless of all this, an SD card can still be used in secure applications, but only by observing certain limitations strictly. I will address this later as well.

Conclusion: Despite what James Bond movies say about high tech, it is low tech that rules when it comes to security.

1.4 • My design philosophy and approach to security

Now I will simply summarise the first chapter. These are the rules that Alice and Bob, our DIY spies on a low budget should follow to get good results:

- **use low-tech** whenever possible: it is still easily available, Eve can't monitor it, Mallory can't subvert it against you. Low-tech has managed to beat high-tech many times throughout history already. Even the old trustworthy Zilog Z80 will come in later to fill some security gaps, you'll see.
- **use a lower speed** of data transmission whenever possible - crucial messages are almost always short. Although Gb/s are available today, kb/s are often enough. There is less residual radiation for Eve to pick at a lower frequency because longer wires are required to effectively transmit RF energy at longer wavelengths. Filter square waves to basic harmonic sinewaves for the same reason if possible.
- **use a DIY approach**, don't always buy readily-made, off-the-shelf products
- **keep everything as simple as possible** - complexity is the main enemy of security
- **use easily obtainable, general-purpose components** whenever possible. Alice and Bob need to be able to get them everywhere, and without drawing much attention (purchasing special-purpose secure ICs will raise a flag for Eve).
- **use an open-source, open-hardware** approach, with a low level of integration, so every signal can be checked. This way you can test the security, which is necessary.

- **try to physically separate electronic modules** for different phases of crypto operations. This increases security, in the same way as low-level integration, enabling Alice to check and monitor more variables.
- **carefully read books and train yourself**, also on subjects other than electronics and cryptography - they alone can't solve your security problems.
- this will expand your scope of awareness and help you to **identify the real problems**
- never disregard any **"impossible scenario"**
- try identifying the problems that I and **other engineers may have overlooked**, and try to work them out.
- learn the basics of **microwave electronics**, although this may seem complicated (especially the mathematics behind it) - you need to understand the basics of the RF world to build proper defences.
- always remember that your security is primarily **your responsibility**
- build a security-conscious mindset - get into a head of a spy, learn to think like a spy. This means becoming a **professional paranoid**, while still keeping excessive paranoia away from your everyday life. Doesn't seem easy, and indeed it isn't.

This concludes the first chapter. The basic DIY principles of electronic security have now been outlined. In the next chapter, we will address specific problems and methods of attack that Eve, Mallory, or Walter can mount. We need to properly recognise the problems before solving them. We will also introduce Trudy, the intruder...

Emma: - Eileen, you are late! Your boyfriend is here already!

Eileen: - My boyfriend? What have you...

Emma: - You were right, can't call him "Kestrel". His hands are as gentle as a cat's paws...

Who are these charming ladies? What are they talking about? Chapter 1 should have given you a lead to figure out. This was allegedly a true event. No worries, in case you give up, you'll find the full story inside this book. The same goes for some puzzle anecdotes that will come later.

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z

elektorbooks

A Handbook on DIY

Electronic Security and Espionage

Nowadays, security problems are rarely properly solved or correctly addressed. Electronic security is only part of the chain in making a system secure. Electronic security is usually addressed as network or software security, neglecting other aspects, but the chain is only as strong as its weakest link.

This book is about electronic hardware security, with an emphasis on problems that you can solve on a shoestring DIY budget. It deals mostly with secure communications, cryptosystems, and espionage. You will quickly appreciate that you can't simply buy a trustworthy and reliable cryptosystem off the shelf. You will then realise that this applies equally to individuals, corporations, and governments.

If you want to increase your electronic security awareness in a world already overcrowded with networks of microphones and cameras, this is a book for you. Furthermore, if you want to do something DIY by designing and expanding upon simple electronic systems, please continue reading. Some of the devices described are already published as projects in the Elektor magazine. Some are still ideas yet to be worked out.

Complexity is the main enemy of security, so we'll try to keep to simple systems. Every chapter will analyse real-life espionage events or at least several hypothetical scenarios that will hopefully spark your imagination. The final goal is to build a security-conscious mindset (or "to get into a head of a spy") which is necessary to recognise possible threats beforehand, to design a truly secure system.

Don't bother reading if:

- you think you and your secrets are 100% safe and secure
- you think somebody else can effectively handle your security
- you think conspiracy theories only exist in theory –Telefunken's masterpiece the "FS-5000 Harpoon" was built on one!

Luka Matic was born in Rijeka, Croatia in 1976. After graduating from the Automation department of FER Zagreb, Luka started to design secure crypto electronics in cooperation with Elektor. He also gained valuable electronic and physical security experience while working in offshore construction and oil drilling. He now works as a researcher at FER Zagreb, where he hopes to obtain a Ph.D. in secure crypto electronics. Hobbies of Luka are sports, movies, reading, and his beloved cat Toxy.

Elektor International Media BV
www.elektor.com

ISBN 978-3-89576-465-3
9 783895 764653

elektor
design > share > sell