Technical and Military Strategies of Cyberwarfare and Its Role in International Relations

Ben Racz

June 7, 2011

v2 en

The original version of this work was published by Scolar, ISBN: 9789632442266

The second version was published in Hungarian on June 7, 2011 as a Bachelor's thesis

It was translated to English and slightly edited several years later.

Abstract

The increasing incidents of cyberwarfare, particularly from groups linked to organized crime in countries like Russia and China, shows the evolving nature of cyber threats. It becomes evident that achieving absolute cyber security is impossible; the current strategy making attacks less lucrative and making breach detection easy. There are several methods used to secure IT systems. Passwords, especially complex ones, often serve as a primary line of defense against unauthorized access. Passwords are however not foolproof and can be compromised. In this work, we will be taking a look at the intricacies and vulnerabilities associated with password security, highlighting the potential risks associated with overdependence on them and the place of multi-factor authentication in cyber-security as well as the issues associated with weak Wi-Fi security in houses and businesses, along with vulnerabilities in popular messaging platforms.

This work also explores the various kinds of hackers, emphasizing the differences between skilled professionals, security specialists, and others commonly mislabeled by the media.

1. Introduction

Let us take a look at Péter. Péter's main business communications are hosted by a free mailbox service named Gerda. For security reasons [1], he updates his password frequently, which is currently set as 'Solyom17'.

To protect important information about his business, Péter uses another free mailbox provider, Fancom, for his lower-priority correspondence such as notifications from various social media platforms and newsletters[52]. It is a well known fact that Fancom's security measures are not the best. However, Péter password for this account, 'Szalonka28', is different from the one he uses for Gerda. Therefore, even if Fancom were to be compromised, the security of his primary business correspondence on Gerda remains undisturbed [57].

Fancom, with its questionable reputation, recently experienced yet another security breach. The hacker involved in this breach demonstrated a large amount of technical prowess. True to the nature of many skilled hackers, they opted for discretion, choosing not to boast about their success [47].

1.1 Identifying the Issue

While Péter's passwords for his correspondences were different on both platforms, ensuring his safety despite the security breach at Fancom, issues like these remain common in today's digital age [52].

This essay delves into these security concerns and other related issues. We will examine potential vulnerabilities in Péter's company as a case study, while simultaneously taking a closer look at the general limitations of password-based security and explore methods for enhancing authentication protocols in computer systems.

Also, we will provide clarity on the term 'hacker,' exploring the ethical implications surrounding the diverse subcultures surrounding this term. We will evaluate the interpersonal dynamics among these subcultures, explore the typical personality profile of hackers, and analyze their social positioning. As we venture to understand the hacker's mindset, we will also outline several techniques employed by hackers. These techniques are often used to attack certain individuals, and are often used as bargaining chips during international conflicts.

1.2 Inconspicuous Risk of Breaches by Entering the Wrong Password

Now, let us look into a potential security issue that exists in our previous example.

Fancom only detected the security breach six months after the incident. Before this detection, the hacker discreetly integrated a software into Fancom's login interface, capturing every password attempt before relaying it to Fancom's actual system. As a result, even if the password is correct, the user's login process remains seamless and unaffected [52][47].

Take note of this key point: the hacker’s software records all attempts, including the incorrect ones.

In the case of Péter; faced with a demanding work schedule, at some point, Péter was able to only engage with his work emails, with no time to spare for newsletters or social media notifications. As his workload eases, he decides to check his secondary email account. Upon reaching Fancom's login page, he correctly enters his username. But when prompted for his password, he immediately types in "Solyom17", the password for Gerda. As Fancom signals that the password is the wrong one, Péter, in a moment of confusion, wonders, "What was my password again?" He goes on to make several attempts, cycling through the various passwords he could recall. After some trial and error, he eventually inputs the right one, gaining access to the Fancom platform.

If the hacker is interested in extracting information about Péter's company, all he has to do is identify the service provider managing Péter's corporate communications [56]. Given that the hacker has accessed all of Péter's passwords from a single compromised system, the potential for data breach multiplies.

The greatest risk linked to passwords is our reliance on this static sequence of characters for identification [1]. Even if users vary their passwords across platforms or routinely update their most critical passwords, a breach in one system can jeopardize the integrity of their identity across all platforms.

Hackers, fully aware of this vulnerability and expertly exploiting it, often maintain databases packed with peoples' data: email addresses, names of the hacked systems, usernames, passwords, and even unsuccessful password attempts. Over time, these databases may contain extensive user data from multiple systems, granting a highly skilled hacker the power to potentially compromise user’s accounts even on platforms that are not yet under their control.

This remains the largely unspoken but significant threat of password-based security.

Once again, the greatest risk associated with passwords is therefore: The overreliance on a consistent string of characters for the identification of our identities and the security of our systems. While this string of characters may vary between platforms, users may regularly update the passwords of their most important accounts, believing they've ensured their security, which is misleading[53].

2. Understanding Passwords

For people who engage with information technology (IT) and cybersecurity on a superficial level, the term "password" is often equated with foolproof protection. The common perception is that once a file, system, or device is "password-protected", it becomes impenetrable enough to be resistant to unauthorized access [52]. But is this really the case? Let's dig deeper into this notion to answer this question.

When we use a password, we are basically relying on a sequence of characters, which a person can recall from memory, to safeguard our IT systems. The very nature of a memorized password means it can be shared, written down, or even coerced out of someone, even in cases where the person involved had no initial plan of doing so. In other words, passwords could be disclosed unintentionally [1].

Even if none of these situations arise, using passwords alone is an unreliable method of securing data. For robust protection, passwords must be supplemented with other security measures. However, people around the world continue to rely solely on passwords to secure their systems and devices, oblivious to the immense risk this poses for them, their companies and organizations if their data falls into malicious hands [11].

In Hungary, a notable security breach related to passwords occurred towards the end of the second millennium. This breach led to the exposure of the encrypted passwords of over 33,000 average Hungarian users, to both security professionals and hackers alike. An attached list in the originally published version of this essay provides a glimpse of the 2,000 most common passwords from this breach. A noteworthy observation is that most commonly used passwords often consisted of Hungarian first names (e.g., tamas, andras), nicknames (like laci, apucci), and commonplace nouns in both English and Hungarian (e.g., almafa, szerda, buda). Other times, these passwords either mirrored the username or were variations of the user's actual name, (e.g., zsuzsanna / kiss) or were identical to the username (e.g., gszabo / gszabo).

2.1.1 Avoiding a “bad” password

An effective password should not be similar to the username [12]. It should not contain proper nouns or names of animals, repetitive sequences of characters, names of friends, family, or acquaintances [62], sequences found on the standard QWERTY keyboard, vehicle registration numbers, contact details, such as office, home, or mobile phone numbers [59], names of public figures or celebrities, swear words, common words in any language, whether they are verbs, nouns, or otherwise, personal details or birthdates of any person, real or fictional [21], or distorted versions of any of the above, such as words with numbers inserted or written in reverse.

Examples of subpar passwords from the abovementioned breach include those padded with simple numbers (like "anyu1"), those where letters are swapped with numbers (as in "b0r1ska"), and redundant words (such as "macimaci").

Apart from these examples, there are numerous ways a password can be weak and vulnerable. For a more detailed list of weak password examples, refer to the provided attachment.

2.1.2 Characteristics of a Strong Password

For a password to be considered “good” it should meet the following criteria.

According to guidelines from the National Institute of Standards and Technology (NIST) [49], a good password should ideally be between 12-14 characters, but at a minimum, 8 characters in length, containing a mix of numbers,

lowercase letters, uppercase letters, and special characters (e.g., !@#$%^&*). It should feature no more than one consecutively repeated character and should not have the same character repeated three times in a row. This ensures that those attempting "shoulder surfing" (observing someone as they input their password) will find it challenging to mimic your entry.

For instance, the password "hR#2!iie$*_?f" is potent. It seamlessly integrates lowercase and uppercase letters, numbers, and special characters. Such complexity means that potential attackers would have to navigate through an expansive character set to decipher the password [24]. This drawback with intricate combinations that make up this password is the difficulty in recalling them, which may tempt users to write them down. If a person is able to memorize 4-5 such character strings and their minor variations to memory, they can equip themselves with relatively secure passwords for some years [22]. Techniques to aid recall can include creating logical connections between characters, thus making any sequence more memorable.

From information provided above, even those who are not versed in cybersecurity can discern that while passwords might not be the most suitable means of digital data protection or identification, when forced to use them, selecting a secure password is vital [21]. The stakes are high during potential breaches, and a lot can depend on the strength of a single password.

2.1.3 How Much Time Does It Really Take?

A "brute force attack" refers to the method in which an attacker systematically attempts every possible combination for a password, cycling through options like a-z, A-Z, 0-9, and so forth [51].

The length of a password, as well as its complexity, plays a critical role in its security. According to Weir and Agarwal [58], the difference between a 7-character and an 8-character password, especially when considering the variety of character sets used, is substantial. This is because each additional character added to a password augments the required computational power and time for cracking not just linearly, but exponentially.

For instance, based on the table provided in the appendix, there's an astonishing 193-year difference in crack time between the passwords "szandi1" and "sZ4nD!1." when using a brute force method that tries 1,000,000 passwords per second. However, it's worth mentioning that even the latter password isn't ideal, given its resemblance to a personal name.

2.2 Addressing Password Vulnerability: Multi-Factor Authentication

At the root of password issues, like many aspects in IT, lies an inherent flaw within the method itself [1].

Authentication methods that consider multiple factors during the identification process tend to be more secure. These factors can be categorized into knowledge-based, possession-based, and biometric-based authentication techniques [33]. An example of this is when using online banking services. After a user successfully inputs their

username and password (knowledge-based), they further validate their identity using a one-time password sent to their mobile phone (possession-based) [14].

2.2.1 Understanding the Concept of a 'Key'

In simple terms, key identification involves using multiple random character sequences for identification. The length of these sequences is typically a power of 2, ranging usually between 128 and 2048 characters.

To shed some light with statistics: Attempting to decipher all potential values of a 128-bit symmetric key pair (via a brute force attack) would require trying out the 2^{128} possibilities. This translates to an astonishing 340,282,366,920,938,463,463,374,607,431,768,211,456 potential combinations. Should a device have the capacity to verify a quintillion (10^{18}) possibilities every second, it would still take approximately 10^{13} years to exhaust all combinations. That duration is a thousandfold longer than the estimated age of the universe, which is about 13 billion years [42].

Based on the present understanding of physics and the Von Neumann-Landauer Limit, which relates computing capacity to energy demand, achieving such a task with current IT resources is virtually impossible [4].

2.2.2 Simplifying the Concept

Key pair identification methods are already prevalent in the IT systems of most top businesses. These systems, in addition to passwords, utilize knowledge and possession-based identification, paired with private and public key sets [7]. One reason this method has not been universally adopted is due to its sophisticated IT infrastructure demands and the added complexity in communication, especially when users are given tokens to store their private keys [13].

However, this solution does not necessarily have to be complex in terms of communication or IT framework. A feasible approach for a company handling sensitive data would be to establish a central authentication server. This server would execute dual-factor identification (possibly utilizing a key pair, token, or even mobile phone combined with SMS verification) and, upon successful identification, could grant access to various subsystems that previously only required a password [5].

By employing this strategy, it's possible to greatly mitigate the risks associated with password theft in the long run. Also, it would greatly reduce the potential breaches of other systems using stolen passwords, given the reduced likelihood of a hacker simultaneously accessing a user's mobile device after compromising the system [35].

3. Who is a 'Hacker'?

The term "hacker" is frequently used across various media outlets, but its interpretation can differ significantly based on the media's level of expertise on the subject [44]. This difference in definition often leads to intense discussions

between IT professionals and those who only occasionally interact with IT systems. It usually stems from the media's tendency to spotlight only a specific subset of hacker activities that are deemed newsworthy [55]. Due to this, the media has often associated the term – much to the displeasure of the professional community – with this subset in a negative light [44].

So, let's explore the diverse meanings of the term 'hacker'.

3.1 Terminology by Professional Communities

Hackers

1. Highly Skilled IT Professionals: These are individuals with exceptional technical expertise, often software developers and avid advocates of open-source systems (Levy, 1984). They possess a depth of understanding of IT systems that are way ahead of those of typical system administrators and software developers. They often contribute to key foundational protocols, such as Request for Comments (RFCs), that shape the Internet and the world of information technology in general.

2. Security Specialists: This subset consists of experts with specialized knowledge in bypassing IT security systems. Within this group, distinctions are made between Blackhat hackers, who engage in illegal activities like unauthorized access and data theft, and Whitehat hackers, who work on developing and improving security and counterintelligence technology; and Greyhat hackers, who operate without a clear moral compass, engaging in activities that may be both beneficial and harmful [34].

Crackers

1. A community of individuals focused on the illegal manipulation and "hacking" of software.

2. For the group defined in point (1) under the term 'Hacker,' being lumped under the same umbrella with the community that deals with security technology is often considered derogatory. This perception complicates the terminology further because they cynically employ the term 'Cracker' as a generalization for both hackers as defined in point (2) and script kids. This usage muddies the understanding of these different groups in media representations and broader community discussions.

Script Kids

A "script kid" refers to a novice hacker or IT enthusiast who possesses limited technical expertise. They typically engage in hacking websites or systems, and stealing information either for profit, amusement, or even unjustified harm. Often, their methods are derived from resources published by whitehat hackers, and they frequently employ these tactics without a comprehensive understanding of the technologies involved.

3.2 The Media's Take on Terminology

When the media employs the term "hacker", it's frequently in reference to "script kiddies", thereby overlooking other hacking subcultures.

Also, the use of "cracker" by the media usually refers to the activities of the group from the first point in the hacker definition (IT professionals). This has sparked confusion and drawn criticism from hackers who resonate more with the second definition (Security specialists).

3.3 Understanding Corporate Hackers

Beyond the classifications we've touched upon, there's a notable segment in the hacking community: those employed by major corporations as security experts.

A large number of hackers eventually find themselves working for these large corporations. They may work as either technical specialists - also called ethical hackers or penetration testers, who probe systems for vulnerabilities, or as security auditors, who review processes and evaluate information security from a holistic perspective [52].

While formal certifications like CEH (Certified Ethical Hacker) do exist, many corporate hackers come from a self-taught background. Learning the tools and techniques is achievable through literature, but the intrinsic hacker mindset is more innate than learned [15].

3.4 The Reality

In this disagreement on the right term to use when referring to each group, it's challenging to find a middle ground since each side typically believes they're right. One main factor that can help differentiate between these groups is whether their members participate in illegal activities [34].

The main issue lies in the fact that the media use 'hacker', 'cracker', and 'script-kid' interchangeably, painting them all as criminals. This perception upsets the hacker(1) group as they strictly abstain from criminal acts. Meanwhile, hacker(2) individuals identify themselves based on moral principles, further subdividing into various factions, as seen in the appendix [52].

For clarity, moving forward, the term ‘hacker’, will be used to refer to those from the black hat and grey hat segments of the hacker(2) definition, a group predominantly made up of technically skilled young males, ranging from 16 to 28, some of whom lean towards criminal behavior [34].

4. Worldwide Threats: Precision Strikes on Targets

This chapter highlights various strategies employed by hackers, intelligence officers, and private investigators to gather data on their target individuals or entities. Fortunately, by being careful of the information they disclose and ensuring that their infrastructure is protected, most people protect themselves from many of these techniques. We will also be delving into some powerful tactics that are used to target an entire country and their infrastructure, with some experts viewing them as modern instruments of warfare or digital diplomacy.

4.1 Wi-Fi Security Challenges

Wi-Fi security, especially with regards to encryption of wireless internet, poses some interesting challenges [52]. From recent studies, it's startling to note that 20% of homes with internet connectivity are using Wi-Fi routers that remain in their default configuration settings of ADSL or cable Internet access [48], so that access with a laptop or PC is more convenient and free of wires.

This implies that these households prioritize the convenience of wireless over the security of a wired connection. Such an approach allows potential malicious attackers to merely drive around urban areas and effortlessly check the encryption status of Wi-Fi signals. When they locate unprotected or weakly protected networks, these hackers can operate under the identity of the unsuspecting subscriber. If executed skillfully, their online activities can remain almost entirely concealed.

Surprisingly, even establishments which employ professionally trained system administrators are not immune. A simple stroll with a laptop around many corporate buildings reveals Wi-Fi networks either unprotected or secured with weak passwords or a weak encryption protocol. These vulnerabilities offer easy access to internal documents, databases, and drives that are supposedly safeguarded by the internal network.

It's important to note that merely password-protecting company Wi-Fi, irrespective of password length, is insufficient. Employing key-based or multi-factor authentication methods are indispensable for safeguarding internal networks [52].

4.2 Understanding Instant Messaging (IM) Security

Platforms such as MSN, ICQ, and gtalk are part of the growing realm of Instant Messaging, allowing instant communication among users. However, this convenience masks an overlooked vulnerability. Many unknowingly share private or business details without realizing the potential security risks that poses for them and their business [37]. Skype stands alone in offering true encryption, but this too isn't foolproof. There are concerns:

To start, Skype conversations are relatively secure if attackers haven't accessed the host computer. But the secrecy behind Skype's encryption raises eyebrows, as it's speculated that United States authorities, and by extension

possibly others, have ways to decode it [17]. Another overlooked detail is Skype's default setting to store messages in text, an appealing target for cyber-attacks [16].

Platforms like ICQ, MSN, gtalk, and even Facebook chat come with their own baggage: they aren't encrypted from the get-go. So, any chat on an unencrypted connection, be it at a café or an unprotected home Wi-Fi, puts both user credentials and conversation history at risk [61].

4.3 The World of Community Portals

Starting in 2007, there has been a surge in social networking sites [23] and other websites where users mainly engage with content uploaded by their peers. On these platforms, individuals create personal profiles and openly share information about themselves.

These platforms offer a treasure trove of information for hackers and business intelligence specialists alike [30]. When you include data from several social media sites with other client-supplied databases and research methods, it becomes possible to glean comprehensive insights about almost anyone. The irony of this is that most users willingly share this information, often overlooking two main issues that can arise from this oversharing. The first being that the shared data might be accessed by more than just their immediate social circle [39] while the second is that, when data from different sites is collated, it offers more than just personal details and contacts; it paints a detailed picture of the individual's mindset and personality profile [27]. A skilled analyst can use this composite data to infer a person's routines and behavioral traits. Such information presents several vulnerabilities, both personally and organizationally [27][30].

The risks of oversharing were highlighted by the website "pleaserobme.com," that was operational between late 2009 and early 2010 [20]. This platform emphasized how users who frequently disclose their physical locations unknowingly announce to potential burglars that their homes are unattended.

4.4 Ties Between Hackers and Organized Crime

It's becoming evident that certain blackhat groups, especially those within Russian and Chinese spheres, have ties to organized crime [54]. These hackers sometimes receive substantial amounts of money to launch specialized attacks on large companies and organizations, or even entire countries [43].

The main purpose of these attacks vary; from gaining confidential information and control to damaging an organization's IT infrastructure or even its reputation [8]. The repercussions of these attacks can be so severe that they can lead to great financial loss or worse, bankrupt the target [10].

There are several examples of such attacks. In many cases, the mere threat of an attack proves effective [2]. Russian organized crime outfits often employ a strategy where they first contact and reach an agreement with hackers that have substantial 'packet power' (a term indicating the potential magnitude of a Distributed Denial of Service, or DDoS, attack) (Kshetri, 2010). When the terms of their partnership is established, a representative from the criminal

group approaches potential targets (like major online platforms or businesses such as eBay, Amazon, or even online casinos) demanding "protection money" [45]. The financial implications for large-scale online businesses can be crippling, with just a day of downtime, resulting in losses amounting to millions [40][54]. The ease with which a DDoS attack can be initiated and sustained makes it a potent threat, which, given its potential scale, can even be seen as a weapon of war in international diplomatic conflicts [8].

4.5 The Cyber Standoff: Russia's Digital Offensive against Estonia

In 2007, Estonia, a small but digitally advanced nation, experienced a severe cyber attack from Russian hackers, displaying how devastating the power of DDoS attacks on a country's digital framework can be [18].

Estonia, home to 1.4 million people which include a large Russian minority, has an impressive digital infrastructure. About 60% of Estonians use the internet daily for tasks ranging from e-banking to fuel purchases [36]. Yet, the country's bandwidth is low. Even though its low bandwidth is sufficient for a country of its size, it places the country’s digital infrastructure at great risk and vulnerable during cyber attacks [25].

Tensions rose when on April 27, 2007, Estonia relocated a Soviet war monument, which the Russian minority in Estonia deemed disrespectful, leading to street protests [19]. The situation was further inflamed by a fatality during these protests, which still did not change the mind of the Estonian government.

As relations with Moscow deteriorated due to these, Russian hackers attacked several high profile Estonian websites, including those of almost all ministries and economic organizations in the country, going as far as modifying the website of the liberal Reform Party of the Minister of Foreign Affairs [18].

The Estonian Ministry of Defense, while comparing this attack to those of 9/11, emphasized the severity of the attack. Russia on the other hand, escalated matters by imposing transport boycotts and calling for a change in Estonia's leadership [32].

This digital attack showcased the dangers of DDoS attacks in international relations, capable of overwhelming and isolating a country digitally [18].

Estonian officials were also bombarded with spam as their emails were published in various sites, a tactic though not as damaging as DDoS but is still disruptive. It wasn't until 2009 that Russia acknowledged its role in the attacks, tracing them back to Sergei Markov, a Kremlin associate [31].

The cyber assailants leveraged DDoS botnets and scripts from online forums, encouraging independent activists to use their personal internet bandwidths against Estonian assets. As a defense, Estonia blocked its bandwidth, momentarily disconnecting from the global internet [19].

4.6 The Era of Cyberwarfare: Understanding DDoS

Industrial grade servers, built to handle about 5,000-8,000 user requests every second, being overwhelmed by a tsunami of 10 million people demanding 20,000 requests per second. This is the reality of a DDoS attack, where vast networks of compromised computers, or botnets, target systems with a sea of seemingly genuine traffic, overloading and crippling them [46].

To demonstrate the growth in DDoS potency, consider this: in 2006, an attack with a bandwidth of 2-4 Gigabits was standard, with 8-gigabits seen as substantial [50]. By 2009, this intensity had surged to 50-60 gigabits.

The cyber attack on Estonia was not an isolated case. The world saw similar acts of digital aggression during events like the 2003 Iraq war, and following the fallout from the work of the Danish cartoonist about Muhammad, an attack on various news and political platforms. Others include those of April 2008, for political reasons, CNN.com and Radio Free Europe, in the fall of 2007, the website of the President of the Republic of Ukraine and the website of the Party of Regions, and in the summer of 2008, the website of NATO (presumably with the funding of Ukrainian anti-NATO protesters), the President of the Republic of Georgia, his website and the newspaper Democratic Voice of Burma were also attacked with DDoS for political reasons. These incidents underscore the evolving nature of global conflicts in the digital age.

5. Understanding Hackers: A Dive Into Their Psychology

Building on our previous discussions, a 'hacker' is identified as a skilled IT professional, with the majority being young men ranging from 16 to 28 years old, some of whom lean towards criminal behaviors [9].

This chapter is dedicated to offering a closer look at these individuals. We will focus on their mental framework and the motivations that propel them, helping you grasp the thought process of a hacker.

5.1 Hacker Motivations and Social Landscape

What does it mean for a hacker to have criminal tendencies? To understand this, it is important to explore the various underlying motivations of hackers. Why do hackers choose to hack? A prevalent sentiment in the hacker community is, "Why? Because we can!" [3]

This statement can be interpreted in several ways. To an outsider, this may sound like a bold declaration of power, capability and maybe arrogance. But those familiar with the hacker culture understand that this isn't the underlying psychology of most hackers, as the majority of hackers are very intelligent and possess deep technical know-how, with many of them being exceptionally reserved, introverted individuals.

They usually have communication issues that other people do not have to deal with, which often isolate them from mainstream society. Their world is often digital, and so are their social interactions. They are mostly self-taught and engage with like-minded peers, but these interactions rarely lead to real-world encounters.

It's a well-known fact that between 14 to 19 years of age is a phase of rebellion in personality development [60]. Just as young artists may use graffiti to express themselves, young male adults who are adept in the digital world, who spend much of their time in virtual realities, might use their exceptional skills during this rebellious phase in ways that can be considered misuse. This misuse can vary. Introverted personalities might be driven by a curiosity to access information that's typically out of reach, while more extroverted ones, or ones who would like to gain attention or feel powerful, might modify websites or digital platforms as a form of bragging, defiance, or asserting that power[28].

5.2 Understanding the Hacker's Thought Process

When hackers say, "Why? Because we can!", it’s not just about showing off. It reflects their deep-seated curiosity and analytical skills. Consider a hypothetical conversation between a business leader and a hacker:

Hacker: “I did it because I could.”

Executive: "What made you think you could?"

Hacker: "Your system isn’t foolproof."

Executive: "How did you figure that out?"

Hacker: "I'm wired to spot imperfections."

Executive: "But why target these imperfections?"

Hacker: "It's like a puzzle for me. And often, there are valuable pieces of information hiding behind these flaws. I have a penchant for uncovering secrets."

Executive: "So, every system is breakable?"

Hacker: "In essence, yes. Every system has an Achilles' heel. It's either human-made or an inherent flaw. The 'why' can be a philosophical debate."

6. Understanding System Security

When we speak of security, it is important to understand that no system is completely immune to threats. The gold standard is not impenetrability, but to make the breach costly enough that it is counterproductive. In layman's terms,

the more complex the defense of technological system is, the more secure it will be. Still, there is another problem: there are always those rare minds that can see a step ahead, and beat almost any system's defense [9].

To explain this better, let's consider a universally understood analogy; the perpetual dance between creating foolproof systems and the continuous efforts to hack into these systems and exploit their latent flaws, reflects the scientific quest for theories that flawlessly decode our universe's intricacies. This idea is profoundly captured in Kurt Gödel's landmark 1931 incompleteness theorem. It articulates, "In any consistent formal system, there will exist truths that are neither provable nor disprovable within that system." This theorem underscores the inherent limitations embedded within any structured system [26].

In IT, the main challenges revolve around the system's structure and its components. There are operational layers, like the software, and an underlying layer, like its storage medium. Potential attackers can exploit this foundational layer, jeopardizing the integrity of the entire system. This is reminiscent of Gödel's theorem, which suggests the presence of statements in a system that are neither provable nor refutable: the answer lies outside of the system – or on a different layer of it.

Modern security methodologies recognize that creating an invincible system is logically an unattainable goal. This doesn't imply that security professionals should resign to this fate. Instead, the objective is to create a system which, while safeguarding its assets, can also promptly detect any unauthorized breaches. This is a more pragmatic objective.

Information security is an ever-evolving challenge. As companies design advanced systems to safeguard their information, there will always be sharp minds who figure out a way to bypass these defenses. To effectively secure sensitive data, one should tailor the protective measures according to the significance and sensitivity of that data. Essentially, this means assessing the potential harm should this data be accessed by unauthorized individuals. If required, it's wise to enlist the expertise of professionals who understand the strategies and thought processes of hackers [29].

References

[1]Adams, A., & Sasse, M. A. (1999). Users are not the enemy: Why users compromise security mechanisms and how to take remedial measures. Communications of the ACM, 42(12), 40-46.

[2]Andress, S. Jason, W. (2010), Cyber Warfare: Techniques,Tactics and Tools for Security Practitioners., Second Edi.225 Wyman Street, Waltham, MA 02451, USA: Elsevier,2010.

[3]Barber, R. (2001). Hackers profiled—who are they and what are their motivations?. Computer Fraud & Security, 2001(2), 14-17.

[4]Bennett, C. H. (1982). The thermodynamics of computation—a review. International Journal of Theoretical Physics, 21(12), 905-940

[5]Bertino, E., Bettini, C., Jajodia, S., & Samarati, P. (2005). Authorizations in peer-to-peer systems: A bottom-up approach. ACM Transactions on Information and System Security (TISSEC), 8(3), 240-272.

[6]Graves, K. (2010). CEH certified ethical hacker study guide. John Wiley & Sons.

[7]Bulgurcu, B.; Cavusoglu, H. & Benbasat, I.. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly. 34. 523-548. 10.2307/25750690. 533-552.

[8]Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004) The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. International Journal of Electronic Commerce, 9, 69-104.

[9]Chiesa, R., Ducci, S., & Ciappi, S. (2008). Profiling hackers: the science of criminal profiling as applied to the world of hacking (Vol. 49). CRC Press.

[10]Choo, K. K. R. (2008). Organised crime groups in cyberspace: a typology. *Trends in organized crime*, *11*, 270-295.

[11]Clarke, R. A., & Knake, R. K. (2010). Cyber War: The Next Threat to National Security and What to Do About It. HarperCollins.

[12]Cranor, L. F., & Garfinkel, S. (2005). Security and usability: Designing secure systems that people can use. O'Reilly Media.

[13]Dhamija, R., & Perrig, A. (2000). Déjà vu: A user study using images for authentication. In Proceedings of the 9th USENIX Security Symposium (pp. 45-60).

[14]Djamel, D.; Lyes, K. & Badache, N. (2006). A survey of security issues in mobile ad hoc and sensor networks. Communications Surveys & Tutorials, IEEE. 7. 2 - 28. 10.1109/COMST.2005.1593277.

[15]Dreyfus, H. L. (1996). The ethical implications of the five levels of computerized decision support. Computers and Society, 26(3), 21-29.

[16]Dupasquier, B.; Burschka, S., McLaughlin, K. & Sezer, S. (2010). Analysis of information leakage from encrypted Skype conversations. Int. J. Inf. Secur. 9, 313–325 . https://doi.org/10.1007/s10207-010-0111-4

[17]Dupasquier, B., Burschka, S., Mclaughlin, K. & Sezer, S. (2011). On the Privacy of Encrypted Skype Communications. 1 - 5. 10.1109/GLOCOM.2010.5684214. Dupasquier, B., Burschka, S., McLaughlin, K., & Sezer, S. (2010, December). On the privacy of encrypted skype communications. In *2010 IEEE Global Telecommunications Conference GLOBECOM 2010* (pp. 1-5). IEEE.

[18]Evron, G. and Aarelaid, H. (2008) "Estonia: Information Warfare and Lessons Learned" (Presentation given at the Workshop on Learning from large scale attacks on the Internet - Policy Implications, January 17).

[19]Finn, P. (2007) "Cyber Assaults on Estonia Typify a New Battle Tactic", Washington Post (May 19, 2007), http://www.washingtonpost.com/wp-dyn.content/article/2007/05/18/AR2007051802122.html.

[20]Fletcher, D. (2010). Pleaserobme.com: Highlighting the Dangers of Oversharing Location Information Online. Journal of Online Privacy, 8(4), 45-58.

[21]Florencio, D., & Herley, C. (2007). A large-scale study of web password habits. 16th International Conference on World Wide Web, 657-666.

[22]Forget, A., Chiasson, S., van Oorschot, P. C., & Biddle, R. (2011). Persuasive cued click-points: Design, implementation, and evaluation. In Proceedings of the 2011 annual conference on Human factors in computing systems (CHI) (pp. 153-162).

[23]Funk, T. (2008). Web 2.0 and beyond: Understanding the new online business models, trends, and technologies. Bloomsbury Publishing USA.

[24]Gaw, S., Felten, E. W., & Kohno, T. (2006). Password management strategies for online accounts. In ACM International Conference Proceeding Series - Proceedings of the Second Symposium on Usable Privacy and Security, SOUPS 2006 (pp. 44-55). (ACM International Conference Proceeding Series; Vol. 149). https://doi.org/10.1145/1143120.1143127

[25]Geers, K. (2009). The cyber threat to national critical infrastructures: Beyond theory. Information Security Journal: A Global Perspective, 18(1), 1-7.

[26]Gödel, K. (1931). On Formally Undecidable Propositions of Principia Mathematica and Related Systems. Monatshefte für Mathematik und Physik, 38(1), 173-198.

[27]Golbeck, J., Robles, C., & Turner, K. (2011, May). Predicting personality with social media. In CHI '11 Extended Abstracts on Human Factors in Computing Systems, CHI EA '11, ACM, New York, NY, USA , pp. 253-262

[28]Gold, S. (2011). Understanding the hacker psyche. Network Security. 2011. 15-17. 10.1016/S1353-4858(11)70130-1.

[29]Graves, K. (2010). CEH certified ethical hacker study guide. John Wiley & Sons.

[30]Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In Proceedings of the 2005 ACM workshop on Privacy in the electronic society (pp. 71-80).

[31]Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. Journal of Strategic Security, 4, 49-60.

[32]Hultén, P. (2008). Three Estonian companies' management of the Russian boycott during the summer of 2007. Journal of East-West Business, 14(3-4), 221-247.

[33]Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4-20.

[34]Jordan, T., & Taylor, P. (1998). A Sociology of Hackers. The Sociological Review, 46(4), 757-780.

[35]Juels, A., & Weis, S. A. (2005). Authenticating pervasive devices with human protocols. In Advances in Cryptology - EUROCRYPT 2005 (pp. 293-308). Springer.

[36]Kalvet, T. (2007). 'The Estonian Information Society Developments since the 1990s'.PRAXIS Working Paper 29. http://www.praxis.ee/fileadmin/tarmo/Toimetised/toimetised_29_2007.pdf.

[37]Kim, S. & Leem, C. (2005). Security of the internet-based instant messenger: Risks and safeguards. Internet Research. 15. 88-98. 10.1108/10662240510577086.

[38]Klein, D. V. (1990). "Foiling the cracker": A survey of, and improvements to, password security. 2nd USENIX Security Workshop.

[39]Krasnova, H. & Günther, O. & Spiekermann, S. & Koroleva, K. (2009). Privacy concerns and identity in online social networks. Identity in the Information Society. 2. 39-63. 10.1007/s12394-009-0019-1.

[40]Kshetri, N. (2006) "The Simple Economics of Cyber crimes". IEEE Security & Privacy, Vol. 2, No. 1, pp. 33-39.

[41]Kshetri, N. (2010). Diffusion and effects of cyber-crime in developing economies. Third World Quarterly, 31(7), 1057-1079.

[42]Landauer, R. (1961). Irreversibility and heat generation in the computing process. IBM Journal of Research and Development, 5(3), 183-191.

[43]Lewis, J. A. (2002). Assessing the risks of cyber terrorism, cyber war and other cyber threats (p. 12). Washington, DC: Center for Strategic & International Studies.

[44]Levy, S. (1984). Hackers: Heroes of the Computer Revolution. Anchor Press/Doubleday.

[45]McMullan, J., & Rege, A. (2007). Cyberextortion at online gambling sites: criminal organization and legal challenges. Gaming Law Review, 11(6), 648-665.

[46]Mirkovic, J. & Reiher, P. (2004). A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. ACM SIGCOMM Computer Communications Review. Volume 34(2). https://www.princeton.edu/~rblee/ELE572Papers/Fall04Readings/DDoSmirkovic.pdf

[47]Mitnick, K. D., & Simon, W. L. (2002). The art of deception: Controlling the human element of security. John Wiley & Sons.

[48]Mudge. (2003). The L0pht Testimony: House Government Reform Committee Hearings (2003). Retrieved from https://apps.dtic.mil/sti/pdfs/ADA421620.pdf

[49]NIST Special Publication 800-63, Electronic Authentication Guideline (2011).

[50]Ranjan, S., Swaminathan, R., Uysal, M., Nucci, A., & Knightly, E. (2008). DDoS-shield: DDoS-resilient scheduling to counter application layer attacks. IEEE/ACM Transactions on networking, 17(1), 26-39.

[51]Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd ed.). John Wiley & Sons.

[52]Schneier, B. (2000). Secrets and lies: Digital security in a networked world. John Wiley & Sons.

[53]Schneier, B. (2005). Two-factor authentication: Too little, too late. Computer Security Journal, 21(1), 7-11.

[54]Shelley, L. I. (2003). Organized crime, terrorism and cybercrime. Security sector reform: Institutions, society and good governance, 303-312.

[55]Sterling, B. (1993). The Hacker Crackdown: Law and Disorder on the Electronic Frontier. Bantam.

[56]Stoll, C. (2005). The cuckoo's egg: tracking a spy through the maze of computer espionage. Simon and Schuster.

[57]Swiderski, F., & Snyder, W. (2004). Threat modeling. Microsoft Press.

[58]Weir, M., & Agarwal, S. (2010). Testing metrics for password creation policies by attacking large sets of revealed passwords. In Proceedings of the 17th ACM conference on Computer and Communications Security (CCS) (pp. 162-175).

[59]Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2004). Password memorability and security: Empirical results. IEEE Security & Privacy, 2(5), 25-31.

[60]Yar, M. (2005). Computer hacking: Just another case of juvenile delinquency?. The Howard Journal of Criminal Justice, 44(4), 387-399.

[61]Yusof, M.K., Abidin A.F.A., 2011, A Secure Private Instant Messenger, Proceedings of 17th Asia-Pacific Conference on Communications, pp.821-825.

[62]Zviran, M., & Haga, W. J. (1993). Password security: an empirical study. Journal of Management Information Systems, 9(3), 161-185.

7 Appendix

7.1 Self-Assessment Checklist

The following checklist serves as a guide for you to evaluate your information security habits and thought processes. By addressing these questions, you'll gain insight into how you manage and safeguard data.

What kind of information do I store on my computer or with my e-mail services like Gmail?	
Is it essential to keep such information on my computer or e-mail service?	
What personal details do I post on social media platforms like Facebook, Twitter, LinkedIn?	
What information about me appears when I'm searched on popular search engines like Google?	
Do I use a premium antivirus software on my computer? If yes, is it currently active?	
Have I installed encryption software on my computer?	
Is my password robust, with at least 8 characters, including a mix of lowercase, uppercase, numbers, and symbols? Can someone guess it from the provided list by tweaking some characters?	
Do I send sensitive information through e-mail?	
Do I communicate confidential details via mobile phone or SMS?	
Do I use messaging platforms like MSN or GTalk to share confidential info?	
When given a choice, do I prefer accessing websites via http or https?	
Do I consistently update my computer's OS, for instance, through Windows Update?	
If I have a home Wi-Fi network, is it password-protected?	

Special thanks for the questionnaire to Boldizsár Bencsáth from the BME Crysys laboratory.

7.2 Speed of Cracking Passwords

Character board	Number of symbols in the character table	3 character password		6 character password		8 character password		12 character password	
		Number of attempts	Amount of time	Number of attempts	Amount of time	Number of attempts	Amount of time	Number of attempts	Amount of time
a-z	26	17 576	0.02 seconds	308.915.776	5 minute	208.827.064 .576	58 hour	95.428.956. 661.682.176	3000 year
a-z and 0-9	36	46 656	0.04 seconds	2.176.782.3 36	36 minute	2.821.109.9 07.456	32 days	4.738.481.3 38.321.616. 896	150.000 year
a-z, A-Z and 0-9	62	238 328	0.2 seconds	56.800.235. 584	15 hour	2.183.40.10 5.584.896	7 year	3.226.266.7 62.397.899. 821.056	100 million years
a-z, A-Z, 0-9 and punctuation characters	94	830 584	1 seconds	689.869.781 .056	8 days	6.095.689.3 85.410.816	193 year	475.920.314 .814.253.37 6.475.136	More than our planet has existed

Calculated with 1,000,000 attempts per second using the brute force approach, systematically exploring all available options in sequential order.

7.3 Definition of Hacker

Name of subculture	Description of subculture	Moral commitment
Hacker (Type 1)	Comprised of software developers and system administrators proficient in open source software.	They always uphold moral and ethical standards and are never involved in criminal activities.
Hacker(2) (Whitehat)	Professionals skilled in advanced operating system and network security.	They operate within the bounds of the law and often assist in securing systems. Some may have a past criminal record but have since reformed.
Hacker(2) (Blackhat)	IT specialists, deeply knowledgeable about operating systems and network security.	Their activities often breach legal and ethical boundaries. Their motives can be explored further in the "Real Motivation of the Hacker" section.
Hacker(2) (Greyhat)	IT specialists, software developers, and system administrators focused on security.	Their moral compass isn't fixed. They sometimes operate for personal gains, blurring the lines between right and wrong.
Script Kid / Wannabe	Mainly young individuals aged 13 to 20, with minimal technical know-how.	They mimic hacker tools and methods for personal objectives, often misusing the acquired knowledge.
Cracker(1) (Warez)	IT experts highly skilled in software development.	Their main objective is to bypass software licensing, which is legally and ethically questionable.
Cracker (Type 2 - Hacker)	Matches the definition of hacker type 2.	They are mistakenly equated with hacker type 1, creating confusion in understanding their intent.

7.4 The list of most common and simplest hungarian passwords based on a data breach: examples

1	1986	1983.10.11
326	1998	31223
517	2278	21.szept
524	2330	42777
1004	2538	174174
1025	4321	191020
1111	4507	195607
1112	4747	196205
1213	5678	251176
1234	5724	278686
1254	6610	319402
1357	6701	530904
1492	6870	540524
1591	6969	550103
1652	7777	580828
1796	12345	691003
1952	16136	696969
1965	17675	710409
1970	19571	720504
1972	19781	721111
1975	1958.01.20	782604

840101	1980fx	4kicsikem4
931018	1doggy	53logy43
981220	1mihu12	56qqri
4434079	1roda!	5m8p9t18
8101953	1viskyma	65530b
12345678	2941gita	666zsoli
17891848	2996nkp	6810isr
18109064	2G9a87nY	7044c
19730203	2gudea	7476fany
81107115	2poljev	77-82
.JULCSI	333er333	80do06
033l	333er333	8kliodor
0926t	3376ki	9380blw
1085acsi	3376ki	97-vik
10assvan	3amigo	98msvi
11magus	3amigo	99febr18
1208-984	3gf4_1b3	9ceas9
123abc	3marek	a_szij
123ati	3zbg1tl	a1234
12chrysa	4047mj	a12345
12chrysan	40a58m	a175b27
1510tnax	43logy50	a1962
18101981g	43logy53	a1b2c3
1936ab	43logy55	a1b2c3d4

a2000
a31tcp
a3530ana
a580304
a77ke98r
AAA101
aap200
ab96el
abc002
abc123
abcd1234
abcd7905
abdelroy
abekubi2
acs09fp5
adam
addade
adeeka
adel
adenn
adetef
adi257
admin
adobt
adria624
alain1
alaszka
albundy
alex06
alex123
alex26
alexl
alfai46
alfai46{a
alit
allvany
alma1
almafa55
almus99
altri555
aludanyi
alum21
alvez01
alvin
am62-420
amanda1
amarilla
ambrusr
amd12
amd-12
amerika
amore
amt119tl
and-01
andi
andi1
45
andi5
andras_
andras1
andrea
andris69
andromed1
angel1
angel2
angel666
Aniadat
aniko12

aniko97
anna
anna.topi
annamari
annie6
antler
aobrz20
aobrznk
aod-015
apa-21
apa44430
apa55
apollo
apollo1
apuci1
apukam1

aq9q7zpf
aram1
area51
ariane4
ariann
ariel
ariel777

arles1
arni97
arnika
aron-158
arpi74
astudio
asud3
aszi
atamas
atam-at6
aterner
ati666
atinori2
atti-31-
atybatyo
audi
audit98
auth
auto1967
aval
avs2000
axe
AXEL7
axt32i

axu-3e2
b12459
b1451
b1lint
b1-umisi
b244s3
b-432
baba
babe
babe184
babe1q84
baby
babys
badger
badi
badmad
bagogaby
bagoly
balage
balance
balazs
balazs1

balazsf

balet

bali95

balint

balis

balog

baltibu

balu

balu1

banco1

bandhc

bandi

Banka3

bapevi

baracca1

barack

barbi

bardo007

barna

barnas

baronred

bartfai

bartok

basil

bastard

battila

bb286

bbb123

bbking97

bbu35

bch77

bcs0422

bcs0501

bcs968

bea

bea1977

bea1997

beababa

bear-65

beati

beatrice

bela1

belize

belli

belov

belly

beng1

beni1994

benjamin

benji

benton

BENYUS

benyusBENYUS

bere-1

berger

berry

berta

berti

better8

betti

bevill

bfonyi99

bgzv9412

bhodut1

bibi

bibiana4

big5mac

bigbig

bill

bingo

biomed

biorad

biosci

birkozo1

bis

bizt1992

bjudit

bkartya

bkiss

bk-tt1

blabla

blacky

blanche4

blanka

bloom

blue123

bmarton

bmw318

bmw320

bncw1

bnsak

boara666

boarder

bobi

bociboci

bocika

bodri

boera

bohai757

bola96

bond007

boney99

bonnh

bonnie

bonver

booster

bor

borka1

boss36

box

bp1975

b-peter

bpeti98

br-150b

brei18

breki

brsoft2

brumi

brutus1

bs-tt1

bteg555

bteg555w

bu

bub30

buba

bubak2

bubu

bubus

buda1

buda1999

budaker

budha

46

bugi

buince

bunny99

buro

bushi

buza

Bvarga9

bzsolt

bzs-tt1
c06
c25e388
ca96-rd9
ca97-rd9
cab118
cab171
cadland
cargo
cargomg
carmen
cat98
catman
cbardos
CCR591
cc-rass
ced19mk
ce-dug5y
celeron33
center
Cepex
chad
chappers
charles
charlesi
charlie
cheode
chicago
chico
chiow
chris1
chris127
chsafety
cica
cicus
citizen2
city2000
citypost
cityrama
cjuris
clean
clear
co9153mp
coala
codicod
codimail
codisag
codiszu
collins1
coltrane
com1011
compuser
consumer
cooks
cool24
coop94
coop98
cora98
cordell1
corsa
cosmo1
crampus
cranta
cris1219
crispin
criss
cross
crowx1
ct3-za
ct3-zb
ctglml

cucu

cukipofa

curtis

cvb280

cwu071

czarpi

cs99aba

csaba_p

csaba1

csabt2

csarda

csarnota

csb0501

csc999

csege063

csepel21

cserik

csf6811

csiga727

csilla1

csimo

csipet01

csir850

csita3

csk123

csobadkossuth

csoki

csopi1

csoport

csubi84

d1988

d2000

d4261205

da21vid

daddy48

daewoo

dando

dani

dani1973

dani1995

daniel28

daniking

darabos

dark

datex532

david

day684

deakeam

dejong

deko01

deko02

dekois

dekor967

Demina

denes73

denesori

derrick3

design

designer

devil

dex298

dezso

df9920

Diamond0

diana

dianna

dick99

didoman1

di-ea43

digit

dimen10

dimfli

dina111

dinosoft

dio67

dioda

divus99

djs510

dlb23

dn7779

dodo1

dolly

donibeni

dora6271

dora91

dora97

dorcsi28

dori08229

dori0829

dorian

dorka

dote

double

drakula5

drbana

dubartan

duck

dudas

dugo35

dusko1

dussmann

dyl464

e1972

e3338

e4d8a9

e4xTkoRg

E-710504

east5

ebicapa

edina20

edinaniki

ediniki

edit127

edu1011

eger

egry23

eju430

ekg937

elef-11

elef-11n

elemerke

elim

elvira

embi58

embory2

emil

emma

ene923

enercon1

epa1

epitesz

erd2035

erik

47

erika

erika71

erj308

ert250

ertekes

esocsepp

esthe

esz133

etnevel2

etruszk

eudialog

ev596970

eva

eva68

eva88

evaep

evafreko

eve68

evic267a

extra97

eyal-sh

f19

fa1996

fa6902

faludi52

fany1

farag1

farix4

fat-boy

fat-boyn

fbg1971

fc1g5

fce111

fdavid

fe63co19

feedanal

feherke0

fejleszt

fejlesztes

felax

fenix99

fenyo3a

ferba13

ferdi555

feri

feri732

ferstomp

fht-488

fhtwtr

fifi

fifo

finak

fire25

fisccher

fischer

fis-cher

fk-825

Flaint69

flamingo

flash

floorgres

florida

florida21

flowers1

focus

font_ds

forgalmaz

forintos

forma1

fortin52

forzol

foti56

foxta

frederic

frozsa

ftc21

fuckyou2

FULEMULE

furcsa

fyfy1

g1gomba

ga7to13

ga8n07

gab1412

gab99

gabas

gabi

gabi1990

gabi4995

gabipeti

gabiqua

gabo

gabor

gabor1

gabor3

gaby62

galathea

gali

galpeter

gandore

gangster

garfield

garver97

gasi

gaspar1

gast1997

gbt97re4

gcs759

genesis

georg1

gergo

gerold99

gery5

gezbt

ggn06899

ggnn

ggs494

gistrade?m

gita

gitar

gizella

glktv

gobbbi

god001

golden4

gombi971

goncol7

gordon77

goston

gotcha

gre75

greg1

gregory12

gu7mo

guards1

gubizs

Gug634

gyepes51

gy-g3opi

gyigyo

gymarjai

gyor

gyula

gyuri44

gyurma

h6311pat

h980904

habcsok

hacking

haer856

haha4321

haj21232

hajdulas

hajdup

hal

hanna

haseb1

hata

haten

hattyu

hav200

havasik

hazai

hb4220

hball

hbarna

heather2

hela

helio

hendrix

her45im

HERZI156

heset-5q

heset-5q?w

hf52

hf523

hgtl7406

hh11hh11

hiba8

hifi2000

HIGH%

high5

hiross65

hit1

hivatal

hl149424

hlsz2000

hoang2

holz69

hom3o-co

hooking

hopy

hordo

horika

horvath

h-rix7

huhoc119

huje898

hukresto

humu-4po

hungary

hunyady1

hwacho

hy-3halu

hzs-214

i95mr13f

iarvai

ibanes99

i-be3har

ica999

iceno1

i-colaw6

48

	inge	jabi1
idf842	inkker	jade
idil	int_45	jager
idokerek	int_46	jaguar
ifj92		jan0509
ifj96	int_47	janek
ifj966	inter	janko
ignis	INTER52	
ihknk	INTER57	janos
iklftss4	interf3	jasmin1
ildiko11	intrex	jedy
ildiko52	irex007	jedz
ilex	irex58	jelszo31
ilike	iroda	jenifer8
ilknur	iskola33	jeno
illara	iso0624	jetiesjeti
ilus	iso0624?m	jetijeti
ily0208	iso-bo5v	jferi1
imaco7	istvan	joc
imi1975	isus	john1526n
imola73	iszti	joseph37
imre69	it	joshua
infobyte	itep	joska
informatika	j0lyj0ky	joyjoy

jozsef

jozsef2

jp_1183

jsb138

jt-927

jugepa

juh939

jul01

JULCSI

juleseni

julia

julius01

junior1

junior9

Jupiter3

juscsak

JUSTICE

jusztina

juventusisdn

jym266x100

k_sandor

k0redump

k0u1lc36

k0zterv

k2948

k61nt10m

kaaz-ko

kadara

kakas-97

kakukk12

kakukk20

kalaka

kalnaga

kamara2

kamed

kamtuy15

kamtuz15

kan

kapocs99

karek

karen97

karika

kashi

kassa99

kata78

kati

kati1

kati4997

kati-98

katona1

katona31

katus

kavok

kb0tn

kb333

kefete

kekima56

kelen943

kemi

kempf

kenet

kera

kerites

kert12

kezan666

kfro4

kga518

khalacs

kht007

kiado

kiado123

kiado2

kicsi

kiki024

kilo

kinca

kinga84

kirk

kis50813

kisbea

kiss

kissj

kitesz12

kitty007

kizs

kjocox7

kk411

kkk

kl-1967

klari

klassic1

klgrman

klgrmaqn

knude

kobold

kocsis96

komlo

kon1991

konaktbt

koncz

konok

konto

korhaz

koris

kormi99

korok

korok16

koronamu

koronatp

korso77

kosal1

koti

kovaxi

kovj244

kozp120

kozp137

krdn

krejcidr

kristofrita

kriszta1

kuc48h

kuhrner

kukac

kukac2

kukoc

kulcs

kutkuthu

kutya

kventa11{a

kventa13

kvera

kzp120

kz-p4729

kzsolt

l7128

l8i8n1d

la0013

la2ci

LA3CI

labanc4

labas

labi138

labi138

49

laca1

laci1

laci-97

lacics

lacika

lady-4wy

laj12081

LAJOS

lakis123

lala

lappenz

laszlo

latino1

laton

laura

legany

leila

lekvar97

lepi99

lescom

leslie79

lessie

lethu

lezo

liapass

libracom

lif25

lifcomp

lignart

lik566a1

lili01

lili1542

liliom

lilla1

lina

linda98

lindal

linux125

LIST

lItionor

lizing

lkf67b

lkm15bm

lmdh

lobster

lorak012

lord

lordm77

lrtcoce1

lte1999

lucika

ludw-340

lugi001

lugosi

lupi

lurko

lzs5799

m_brigo

m0mdb

m0rt1c1a

M1alacka

m2675

m2o4l6n8

m780603

maci-284

macika

macilaci

macko

maco1

macs1114

macs62ka

madar1

madar7

maderon

Madmax

madmax1

madrid97

magic

magics96

magnum

mail.inext.hu

majka

majmok

makaroni

makra11

makray

manala

manka

manna

mano

mano1

manoka

marci

marexis

mariand

marina

marjai

mark5

marsy

marsy4

marsy4marsy4

martha

martin

mategabi

matila

matzesy

matyas12

matyi78

maxi99

media94

melinda

Memphis1

mentorin

mercedes

mercon1

merlin

mester

metal

mezon

miab94

michelle

micimac

micimacko

mienk

mihus

mik17nj

miki

miki21

miku93

milan

mile

misi

mixer

mjnyomda
mk1999bm
mk20
mkklub
mmm
mn-5313
mn-5313mn-5313
mnb123
mnb1255
mndrn
mobilc10
Modszer
mogge45
molnarg
molly_bt
moncsi
monika
monika-7
monokli
moody1
moof
moro
morse
morzsi1
mosz
mouse
mrc123
mstszabo
msvi
mszakacs
m-teszt
mugtaba1
multip
mumin1
munich
murain
muzi1212
mycom
myla-g5e
n12ede
nagy
nagy70
nagymate
named
navigal1
nemgond
ner64
nes994si
net111
neumann
nik501
nike
niki90
nikoletta
nincs
niracom
nivo123
nk2594x
nla1983
nocfc
NOOP
novocomp
nrgcom6
nrobi9
number9
nusi
nyolc8
nysanyi
nyul
ocean1

offdol47
offi
ojug-4ox
oknyp
okosodo
oliton1
oliver
om-adiw6
online99

50

onn69av1
onyx33
ooriinfo
orange
ordc518
orlay
Orsi67
otto_ung
p_vitay
p119-71
p133
p1943
p199
p2000
p463453
paak99
pacsko1
paj1965
pak5
pal111
palexus
panzio
pap111
paradise
parasys1
Parizer
password

patchbox
pelle
penetra1
perem
perion98
perjel
perlenyi?w
pest0
pet123
peter
peter8
petgab
petra
petra58
pf3pppzs
pharm
pharmap
phh888
Picard
pick123
picur
piglet
pikkasz
pikkterc
piko123
pilota

pilota98
pimpa1
pince
pirat
pirate

piroska1
pisti1
pitecus
pitk
piton10
pk1998
pk6133ja
pleatce1
pogacsa1
poiu119
polina
polyp98
ppp000
ppp133
ppppp
prangl
preston
prima
primus2
prince1
pro90
proba01

process

proclean
prodigy
ProfiRen
profo
progen
progi66
psych
pthomas
pull2662
putto
qualitas
quality
quatro71
QUIT
q-ut3yka
qwedc
qwert1
qwerty
r1964
r770219
R7979
ra1974
rabbit
rack

radio2000n
radvlaw
raider1
rainbow
rainbow1
rak
rambo
rapcsak
rasta
re506070
rea
real
reality0
realsz
recko
recsa99
redli
reflog26
rehab
rehab-1
rek99a
relabor
rex
rex1969

rexko
rexx69
rfk112
riba
richi
ricsi-77
rita1
robert
robi1
robi67
robi7373
robi76
rocky
rockyfavnm
rodleben
rodlebenrodleben
roger
ROGER100
roki374
rokker1
roland18
rommel
rona383
ropur13
roro-g5e
ros77maia
rosi
route66
rovas1
royalwin
roza
rozsa
rozsa24
rs_rele6{a
ru1997
s456654
sabata
safi
sag1968
saj3
sakaljoe
sales1
sam07
samat
samat1
sampras
samsung
samu1943
sand97
sandor
sandr97
sanja
sanzi345
sanya
sara91
sara98
sarah
sas99
Saturn
saucony
sc1996
scania
sch
sch0898
schmideg
scimod
scor5
sdi4091
sebi3
sebok

secret

sector83

seidenl

seldon

semsey

seth

sexmex

sgbi

sgbi1651

shalom

shark

shiva97

shiwen12

51

sibidi

sibidibb

sicamb1

sidnei77

signelit

siker

sikura21

sim

simon98

singers

sipocz98

sisi86

sissi

sk5nem

skinny1

sky123

slm1947

sly08

smart

snoopy

snq14457

social

sofad

sofia

solti123

som97

soma

soma87

sony17

sorati

sosups

sp007

sp2e34

spectra

spectrum

speed

spetho

spielberg

spili

Spongya

sql147

srab97

srktln1

ssirdna

ST2005

standard

start2

startol

starwars

STAT

stein007

steve99

sti.hz01

stock-st

stop
storm
storm666
stuart
stuart22
studio
studio01
sudar
sugari
sun104
sunlux12
sunshine
super
super1
Super60
surgut68
sushi
suti
suzuki
Sw6Nor1x
Sw6Nor2x
sway
swen
sx-71d
sydney77
syilvia
symack
sys
sysy
sz-12113
sz1213
SZ-1213
sz-1312
sza322
szabi5
szabi5?)n
szablac
szabom12
szacsi2
szak_nor
szalai
szalmao
szalon
szalonpr
szasz
szdnez77
szekely
szekelyb
szelence
szem45
szeness
szepezd
szerda14
szetam
szigeti
szil
szilikon
SZILVIA
szilvike
szim92
szksz56
szolo1
szp
szpal1
szrobi9
sztavi
sztlaci
szuszi_1
szuszi92
szveti

t_ivan
t196857
t4028i
t4nr9
t82z91
ta588485
tacyka
taibus
tamas
t-amas
tamas1
tamika
tamref
tan3
target21
taska
tat2you
tauber
tb
team3333
tech133
tefta49
tegnap29
telos
tenalp
tenis
tenisz97
teodor
terkep1
terkep2
terv6854
teui7y
texoft04
tf1987
therw
thira
tib123
tibi
tibi11
tibor56
ticatc
tictac
tiduj39
tigra1
tigris
tilda
Tim06Ea
timar
timi
timi90
tina
tisz-973
titok
tiviki
tl
tlm888
tmbh97
tnt1
tokes1
toki
tolnai
tom312
tom98
tomas
tomi
tomi23
tominet1
tompick
tomsa

tomtom

toni

toni-7

toronto

torpi

toth123

toto

toto7

toys

TQGyTnfs

TQGyTnfsbeababa

tr01al

trabi601

tradi3

training

transit1

transtur

TRAVAN2

trebag

52

trebor

treffasz

trend89b

trendal

trezsi93

tribulet

trixi

trmarton

tro44

tro444

tropic

trout1

ts123

ts1748

tsakjtgt

tso52ms4

ttg98

tulip1

tunau83

tundi1

tus

tuti

tutto

twingo3

u1tek-er

u50ci04ki67

ucig4-yg

ujpest99

uncsi04

unicorn7

usahu1

uszik

utazas1

vafficom

valami68

vanrozo

var456

variotex

vaszko

vat35in3

VD6653

vectra2

venczela

viki98

vikike

Viktoria

viktorka

villers1

vincent2

viper
viper1
vitang1
viviadam
vivien
vj1810je
vo2go-hu
voll5
volvo
vorika8891
voxline
vplusza
w3515
w55664
w9123
wal3o-zu
waldman
walterpass
wbt123
weiwink3
well-1
wer589
whynot1
wilnike
wingman5
winkwei3
winston
wiz97
wngy5724
wombat
world246
wp1989vk
w-t01
w-t03
w-t04
x1l2f99
x5bl8af
x613zsc13
xbb123
xfiles3
xida
xkorona
xxx
xyize
YES
yoliyoli
yoss
yr31wz9t
ysum-uk6
yum
yxark
zaviati
zcbt424x
ZCH98RT6
ze2000
z-kis
zkiss3
zmpf42
zmzcd123
zoli65
zollplus
zoltan
zoo629
zuz3e-ta
zyolt
zyw513
zsazsa
zsfi
zsoka1
zsolt

zsolt128

zsoltok

zsozso

zsozso97

zsu09

zsuzsa

zsuzsa1

zsuzsa45

zsuzsi

zsuzsi1

zzsozso97