1 Security: Introduction into my interests

I believe security is a good entrance into my current interests. It awards both attention to detail and high-level systematic view; its subfields connects directly with both theoretical and practical areas that fascinates me, and it offers effective tools to solve the imminent problems I face in real life.

The term *security* in computer science generally carries the sense of achieving *security goals* through *mechanisms or properties* of a system, despite the presence of adversaries in a *threat model*. The threat model has to be carefully chosen and reviewed; there would be no security against an omnipotent adversary.

Unlike in math, one cannot arbitrarily wiggle the threat model to one's desire. On the contrary, one's rights are increasingly threatened by the powerful digitally [21, 47, 43]. A prominent example is the continuous push for exceptional access to to people's data and communication in various forms by governments[1], ignoring expert opinions against such measures [2, 1, 3]. I unfortunately has suffered from more aggressive attacks, primarily systematic, comprehensive, and far-reaching censorship [4] [52, Sect. 5], because of my background.

How my security goal of being able to exercise my human rights in the presence of these powerful adversaries drives my interests will be explained by the following subsections, some of which also describes how my more pure academic excitements are intertwined with this realistic drive. Finally, the last subsection, 1.3, will lead the transition into the other areas of my interest.

1.1 Secure Systems: Understanding the mechanisms

1.1.1 A high-level view of the Internet

A high-level understanding of how the digital infrastructures work is essential to understand what enables these threats. The current networking infrastructure, in my opinion, has conflicting properties. On one hand, the fundamental problem of the impossibility to link every two computers requires sharing of links, a solution that welcomes centralization. On the other hand, the poor scalability of simple sharing schemes of a link (usually via a switch) necessitates a better scheme to extend a small network globally. The Internet relies on topological divisions in its address, and delegates most routing task to each individual networks (e.g. ISPs). Its BGP, opearing in between them, is mainly concerned exchanging reachability information, whereas its IGPs handle routing paths and allow different networks to implement different routing policies.

Therefore, the Internet has become a mixture of centralization and decentralization, where each end node is managed by an ISP network, yet no single ISP runs the whole Internet. Perhaps surprisingly, I found this hybrid structure more optimal for localized sabotage at the state level, creating "sub-Internet"s, each of which is crippled at a different level.

[1] For instance, EU revived the Chat Control proposal in 2025. See `https://eutechloop.com/time-is-running-chat-control/`.

Unfortunately, the lower layers of the Internet have proven to have a great inertia for change. Handley gave a nice discussion on it in 2006 [26], and the trend he described has mostly been the same since then: "*the core Internet protocols have not changed significantly in more than a decade, in spite of exponential growth in the number of Internet users and the speed of the fastest links.*" [26]. On the other hand, the protocols in the higher layers evolved to a much greater degree. As the transport layer welcomes QUIC[27], the application layer has accumulated an enormous amount of innovation and progress, in particular, onion routing and Tor[24, 12], Bitcoin[36], VPN protocols[38, 14] and decentralized instant chat[32, 46], that fight for digital rights and/or promote decentralization. Yet one must not overlook the crypto-constructs that lay the foundation for all of them, which I discuss in detail in Section 1.3.

Unfortunately again, because all of these are built on the Internet, a state-level censor could easily abuse its local authority to target them. A few regimes are notorious to have blocked a vast amount of them to various extents, employing complicated passive analysis and active probing techniques [16, 29, 49, 50, 18, 17], Although a state would need to consider the collatoral damage, a totalitarian regime would not hesitate to block an entire protocol before it can figure out how to block it selectively [54, 50]. Apart from state-level actors, because commerical local ISPs additionally have an incentive in income and profit, not only do they perform surveillance and censorship like state-actors [6, 5], they also implement unjust policies easily with their local control of the infrastructure, like unfairly limiting the use of certain P2P protocols [13, 39, 34, 6]. Although ISPs argue that these P2P protocols can consume too much bandwidth, the other side of the story is that ISPs often oversubscribe and fraudulently advertise the bandwidth of Internet service they provide [41, 8]. This essentially is a probabilistic exploit on its customers — when almost all of the users happen to use the maximal bandwidth the ISP sells to them, cogestion and throttling occur, and the users, not the ISP, ultimately pay the price — this is also the same kind of injustice imposed by airlines who oversell tickets.

The question of how to build protocols and systems that preserves one's rights on top of the Internet that powerful adversaries control, fighting against surveillance, censorship, and overall other unfair practices which the infrastructures of the current networks happen to enable, is central to my interest in secure distributed systems.

1.1.2 Low-level system details

Beside the threat model, when we talk about security, we also implicitly assume another model, environment, or host, that encapsulates the problem. For instance, in the context of isolation,

- The host that encapsulates process isolation is the operating system kernel.
- The host that encapsulates virtual machine isolation is the hypervisor, often including hardware support.

- The host that encapsulates air-gapped machine isolation is the physical world, or more abstractly, the physical laws.

Moreover, these hosts also form a hierachy; the physical world, as the ultimate host, contains all the others directly or indirectly. Take as example processes running in an OS from a virtual machine, physically on an air-gapped machine: in this case, the host OS is contained by the host hypervisor, the hardware, and finally the physical world.

As a result, a security researcher has to understand these hosts, each to a different degree, depending on how secure she wants her systems to be. Even if a system is formally verified to be secure within a host, it can still be attacked from interactions with an outer host. That is well examplified by the Meltdown attack, which breaks both kernel and hypervisor's isolation of memory, because an outer host, the hardware, has a vulnerability [31]. In fact, Meltdown touches more than logical flaws in hardware; it relies on the timing difference of cache accesses to extract information from it [53], one that directly connects with the physical world. Indeed, other than timing, a running secure systems leaks information in so many other ways such as power and radiation via physical effects, which opens to a large range of attacks [30, 7, 19, 53], collectively defined as side-channel attacks.

Although there's little hope to understand and model the universe thoroughly in one's life-time, a good understanding of the most common hosts, the operating systems and the hardware (including the architecture), will prove invaluable for me as a security researcher. Additionally, figuring out how to perform clever hacks (as in the hacking culture of MIT, not the mainstream meaning of cracking) based on knowledge of details of a system gives a great sense of achievement to me. Finally, this is one major place where cybersecurity connects directly with a broad range of other fields, including software engineering, systems architecture, networking, and physics. These together contribute to my interest in the low-level details of secure systems.

1.2 Data-driven analysis: Lights through artifical clouds

Despite my intention to understand systems, many of them are not open for analysis, for various reasons. In particular, the aforementioned systems for digital surveillance and censorship are not only proprietary but often state secrets. On the other hand, similar to side channel attacks, these systems inevitably leak information in different ways.

By observing their operation and actively testing how they react under controlled conditions, we will gain an insight into such systems. Combined with data scientific approaches that extract hidden structures, we could often obtain a reasonably good knowledge on a specific aspect of such systems.

The process usually involves 1) raising questions and claims about some properties of a target system 2) conducting experiments (often involving purchased servers within such as Aliyun) 3) analyzing data 4) answering questions and verifying claims. As a simple example, Sheffey et al. very recently studied the IP addresses injected by the GFW censorship system. By first finding injected IPs and then probing them within the GFW, they found three categories of such IPs [45].

Thanks to continuous work from both academic scholars and dedicated organizations, (e.g. [51, 37, 17]), I and a small set of others who suffer from such systems and who are fortunate enough to know these works, could know what we are facing everyday better. Conversely, I strongly hope to contribute to the free-side of the arms race, making the free Internet reachable to everyone.

1.3 Cryptography: A mathematical savior

Security is often described as an arms race — that who controls more resources tends to discover more vulnerabilities, devise more attacks, and harden their systems more. Where is hope, then, when most self-censor and give up fighting the regime [9, 35, 48] and even fewer of them have sufficient skills to join in the crypto war [40, 28]?

I believe one solution to what might sound like a power struggle lies within (modern) cryptography. For thousands of years since the use of the earliest symmetric encryption methods like the Ceasar cipher, the ability to securely communicate through an insecure channel had still been mostly limited to the privileged who could afford persistent access to physical secure channels to exchange the keys and reliable safeguarding of the keys. A stunning turning point was found in what was widely regarded as the beginning of modern cryptography, Deffie and Hellman's *New Directions in Cryptography* [11], where they gave a practical mathematical procedure to Merkle's original idea for establishing a key known only to both parties over an insecure channel.

At first glance, the idea sounded so impossible that Merkel himself faced rejections when presenting the idea to his then professor Hoffman and to the CACM [33]:

> "I am sorry to have to inform you that the paper is not in the main stream of present cryptography thinking and I would not recommend that it be published in the Communications of the ACM."
>
> "Experience shows that it is extremely dangerous to transmit key information in the clear."[33]

The rejections represented a concensus of the old cryptography community that even Shannon concurred with: "*The key must be transmitted by non-interceptible means from transmitting to receiving points*" [44, p. 670], which demonstrates how "paradoxical" the idea was.

Such "paradoxical" ideas of modern cryptography are what attract me most to it, because they are the enabler that underlies those systems mentioned in section 1.1: TOR, Bitcoin, OpenVPN, Matrix, etc., and the catalyst that leads to the massive adoption of society advancements such as e-commerce. Remarkably, in less than 50 years since 1976, we already have a number of such discoveries in addition, and here's a list of some of them.

Pseudorandom functions The kind of deterministic algorithms whose outputs look like that of a random oracle, by block ciphers like AES[10] or other ways [22], has a strong link with various other essential constructs like one-way functions.

Zero-knowledge proofs By interactively leveraging challenges that only a true prover could easily solve, zero-knowledge proof [25] enables one to verify that the prover knows a witness of a problem in NP [23] without revealing the witness.

Homomorphic encryptions Doing computation on encrypted data has been a very desirable property for many years. Although many earliest public-key encryption schemes, such as RSA [42] and ElGamal [15], already natively supported limited homomorphism like modular multiplication, by their design, the first full scheme that allowed arbitrary computation on encrypted data was only proposed in 2009 [20].

These discoveries have many applications and implications, two of which I pay most attention to. One is that they update our understanding of certain theoretical lower bounds of how much security one can achieve in the face of strong adversaries, no matter the power difference between them. The other is how they help minimize the trust required to perform global-level of collaboration that involves people from vastly different backgrounds and beliefs; such a collaboration that would typically require a strong central authority to organize, now only requires the participate to trust a few foundamental assumptions of cryptography.

Personally, I would go a step further. I believe modern cryptography offers not only technical tools, but a possible solution for addressing one of the deepest challenges our democracies face today: fragmentation, polarization, and the erosion of shared trust. By design, cryptography redistributes power — it makes mass surveillance prohibitively costly, even for state-level actors, by forcing them to target individuals rather than populations. For example, if breaking one person's encryption, on average, required even a single day of dedicated effort (through side-channels, vulnerabilities, or social engineering rather than mathematics), that constraint alone would prevent massive surveillance, since no adversary has that many days or resources to do this on everyone. In this way, encryption does something profound: it automatically and passively unites individuals, protecting each not by active coordination that is increaingly difficult, but by the collective shield of widespread adoption. Fortunately, as many modern infrastructures already deploy encryption and other crypto schemes by default, this "passive solidarity" is not a dream but a reachable reality, one that shows how mathematics can serve as a safeguard for democracy in an increasingly divided world.

To end this section, cryptography not only flows towards my passion for purer philosophical understanding, because of its deep connection with theoretical computer science and mathematics, to which I turn in Section 2, but also carries my hope to break free from the strong grasp of the tyrannies today, one that represents my free will which refuses to lose my agency and independence, in a world that too often seeks to reduce us into interchangable screws for the system.

2 Mathematics: My purer philosophical pursuits

References

[1] Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Callas, J., Diffie, W., Landau, S., Neumann, P. G., Rivest, R. L., Schiller, J. I., Schneier, B., Teague, V., and Troncoso, C. Bugs in our pockets: the risks of client-side scanning. *Journal of Cybersecurity 10*, 1 (01 2024), tyad020.

[2] Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P. G., Rivest, R. L., Schiller, J. I., Schneier, B., Specter, M. A., and Weitzner, D. J. Keys under doormats: mandating insecurity by requiring government access to all data and communications ‡. *Journal of Cybersecurity 1*, 1 (11 2015), 69–79.

[3] Anderson, R. Chat control or child protection? 2210.08958, 2022. `https://arxiv.org/abs/2210.08958`.

[4] Anonymous. The internet coup. Technical analysis, InterSecLab, sep 2025. `https://interseclab.org/research/the-internet-coup/`. Accessed 25 Sept 2025.

[5] Becker, E., and Djuitcheu, H. Could your mobile broadband internet provider threaten your digital privacy? In *2022 Workshop on Next Generation Networks and Applications (NGNA 2022)* (2022).

[6] Bendrath, R., and Mueller, M. The end of the net as we know it? deep packet inspection and internet governance. *New Media & Society 13*, 7 (2011), 1142–1160.

[7] Boneh, D., DeMillo, R., and Lipton, R. On the importance of eliminating errors in cryptographic computations. *Journal of Cryptology 14* (mar 2000), 101–119.

[8] Cachon, G. P., and Feldman, P. Pricing services subject to congestion: Charge per-use fees or sell subscriptions? *Manufacturing & Service Operations Management 13*, 2 (2011), 244–260.

[9] Chen, X., Xie, J., Wang, Z., Shen, B., and Zhou, Z. How we express ourselves freely: Censorship, self-censorship, and anti-censorship on a chinese social media. In *Information for a Better World: Normality, Virtuality, Physicality, Inclusivity* (Cham, 2023), I. Sserwanga, A. Goulding, H. Moulaison-Sandy, J. T. Du, A. L. Soares, V. Hessami, and R. D. Frank, Eds., Springer Nature Switzerland, pp. 93–108.

[10] Daemen, J., and Rijmen, V. Aes proposal: Rijndael. Gaithersburg, MD, USA, 1999.

[11] Diffie, W., and Hellman, M. E. *New Directions in Cryptography*, 1 ed. Association for Computing Machinery, New York, NY, USA, 2022, p. 365–390.

[12] Dingledine, R., Mathewson, N., and Syverson, P. Tor: The Second-Generation onion router. In *13th USENIX Security Symposium (USENIX Security 04)* (San Diego, CA, Aug. 2004), USENIX Association.

[13] Dischinger, M., Mislove, A., Haeberlen, A., and Gummadi, K. P. Detecting bittorrent blocking. In *Proceedings of the 8th ACM SIGCOMM Conference on Internet Measurement* (New York, NY, USA, 2008), IMC '08, Association for Computing Machinery, p. 3–8.

[14] Donenfeld, J. A. Wireguard: Next generation kernel network tunnel. In *NDSS* (2017), pp. 1–12.

[15] Elgamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory 31*, 4 (1985), 469–472.

[16] Elmenhorst, K., Schütz, B., Aschenbruck, N., and Basso, S. Web censorship measurements of http/3 over quic. In *Proceedings of the 21st ACM Internet Measurement Conference* (New York, NY, USA, 2021), IMC '21, Association for Computing Machinery, p. 276–282.

[17] Ensafi, R., Fifield, D., Winter, P., Feamster, N., Weaver, N., and Paxson, V. Examining how the great firewall discovers hidden circumvention servers. In *Proceedings of the 2015 Internet Measurement Conference* (New York, NY, USA, 2015), IMC '15, Association for Computing Machinery, p. 445–458.

[18] Ensafi, R., Winter, P., Mueen, A., and Crandall, J. R. Analyzing the great firewall of china over space and time. In *Proceedings on Privacy Enhancing Technologies* (2015), vol. 2015, pp. 61–76.

[19] Genkin, D., Shamir, A., and Tromer, E. Rsa key extraction via low-bandwidth acoustic cryptanalysis. In *Advances in Cryptology – CRYPTO 2014* (Berlin, Heidelberg, 2014), J. A. Garay and R. Gennaro, Eds., Springer Berlin Heidelberg, pp. 444–461.

[20] Gentry, C. Fully homomorphic encryption using ideal lattices. In *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing* (New York, NY, USA, 2009), STOC '09, Association for Computing Machinery, p. 169–178.

[21] Głowacka, D., Youngs, R., Pintea, A., and Wołosik, E. Digital technologies as a means of repression and social control. *Policy Department for External Relations, Directorate General for External Policies of the Union 1* (2021), 1–106.

[22] Goldreich, O., Goldwasser, S., and Micali, S. How to construct random functions. *J. ACM 33*, 4 (Aug. 1986), 792–807.

[23] Goldreich, O., Micali, S., and Wigderson, A. Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof systems. *J. ACM 38*, 3 (July 1991), 690–728.

[24] Goldschlag, D., Reed, M., and Syverson, P. Onion routing. *Commun. ACM 42*, 2 (Feb. 1999), 39–41.

[25] Goldwasser, S., Micali, S., and Rackoff, C. *The knowledge complexity of interactive proof-systems.* Association for Computing Machinery, New York, NY, USA, 2019, p. 203–225.

[26] Handley, M. Why the internet only just works. *BT Technology Journal 24*, 3 (2006), 119–129.

[27] Iyengar, J., and Thomson, M. *RFC 9000 QUIC: A UDP-Based Multiplexed and Secure Transport.* Internet Engineering Task Force (IETF), may 2021. https://www.rfc-editor.org/rfc/rfc9000.html.

[28] Kazansky, B. Digital security in context: Learning how human rights defenders. https://cdn.ttc.io/s/secresearch.tacticaltech.org/pages/pdfs/original/DigitalSecurityInContext.pdf.

[29] Knockel, J., Crandall, J. R., and Saia, J. Three researchers, five conjectures: An empirical analysis of {TOM-Skype} censorship and surveillance. In *USENIX Workshop on Free and Open Communications on the Internet (FOCI 11)* (2011).

[30] Kocher, P., Jaffe, J., and Jun, B. Differential power analysis. In *Advances in Cryptology — CRYPTO' 99* (Berlin, Heidelberg, 1999), M. Wiener, Ed., Springer Berlin Heidelberg, pp. 388–397.

[31] Lipp, M., Schwarz, M., Gruss, D., Prescher, T., Haas, W., Horn, J., Mangard, S., Kocher, P., Genkin, D., Yarom, Y., Hamburg, M., and Strackx, R. Meltdown: reading kernel memory from user space. *Commun. ACM 63*, 6 (May 2020), 46–56.

[32] Matrix.org. Matrix for instant messaging. https://matrix.org/docs/chat_basics/matrix-for-im/, 2023. Accessed 26 Sept 2025.

[33] Merkle, R. C. Publishing a new idea. https://ralphmerkle.com/1974/. Accessed 25 Sept 2025.

[34] Mondal, A., Trestian, I., Qin, Z., and Kuzmanovic, A. P2p as a cdn: A new service model for file sharing. *Computer Networks 56*, 14 (2012), 3233–3246.

[35] Moore-Gilbert, K., and Abdul-Nabi, Z. Authoritarian downgrading, (self)censorship and new media activism after the arab spring. *New Media & Society 23*, 5 (2021), 875–893.

[36] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Available at SSRN 3440802* (2008).

[37] Niaki, A. A., Hoang, N. P., Gill, P., Houmansadr, A., et al. Triplet censors: Demystifying great {Firewall's}{DNS} censorship behavior. In *10th USENIX workshop on free and open communications on the internet (FOCI 20)* (2020).

[38] OpenVPN, Inc. Openvpn. https://openvpn.net/, 2025. Accessed 26 Sept 2025.

[39] Piatek, M., Madhyastha, H. V., John, J. P., Krishnamurthy, A., and Anderson, T. E. Pitfalls for isp-friendly p2p design. In *HotNets* (2009).

[40] Rahman, Z., Thompson, N., Walker, T., and Kaminski-Killany, K. Technology tools in human rights. Tech report, The Engine Room, 2016. www.theengineroom.org/wp-content/uploads/2017/01/technology-tools-in-human-rights_high-quality.pdf.

[41] Raju, A., Gonçalves, V., Lindmark, S., and Ballon, P. Evaluating impacts of oversubscription on future internet business models. In *NETWORKING 2012 Workshops* (Berlin, Heidelberg, 2012), Z. Becvar, R. Bestak, and L. Kencl, Eds., Springer Berlin Heidelberg, pp. 105–112.

[42] Rivest, R. L., Shamir, A., and Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM 21*, 2 (Feb. 1978), 120–126.

[43] Rosson, Z., Anthonio, F., and Tackett, C. Emboldened offenders, endangered communities: internet shutdowns in 2024. Technical report, AccessNow, feb 2025. https://www.accessnow.org/press-release/keepiton-internet-shutdowns-2024-en/. Accessed 25 Sept 2025.

[44] Shannon, C. E. Communication theory of secrecy systems. *The Bell System Technical Journal 28*, 4 (1949), 656–715.

[45] Sheffey, J., Zohaib, A., Kang, D., Durumeric, Z., Houmansadr, A., and Wu, Q. Extended abstract: I'll shake your hand: What happens after DNS poisoning. In *Free and Open Communications on the Internet* (2025).

[46] TokTok. A new kind of instant messaging. `https://tox.chat/`, 2025. Accessed 26 Sept 2025.

[47] Wagner, B., Bronowicka, J., Berger, C., Behrndt, T., et al. Surveillance and censorship: The impact of technologies on human rights. EESC: European Economic and Social Committee, 2015.

[48] Wang, M., and Mayer, J. Self-censorship under law: A case study of the hong kong national security law, 2023.

[49] Wendzel, S., Volpert, S., Zillien, S., Lenz, J., Rünz, P., and Caviglione, L. A survey of internet censorship and its measurement: Methodology, trends, and challenges, 2025.

[50] Wu, M., Sippe, J., Sivakumar, D., Burg, J., Anderson, P., Wang, X., Bock, K., Houmansadr, A., Levin, D., and Wustrow, E. How the great firewall of china detects and blocks fully encrypted traffic. In *32nd USENIX Security Symposium (USENIX Security 23)* (Anaheim, CA, Aug. 2023), USENIX Association, pp. 2653–2670.

[51] Wu, M., Zohaib, A., Durumeric, Z., Houmansadr, A., and Wustrow, E. A wall behind a wall: Emerging regional censorship in china. In *2025 IEEE Symposium on Security and Privacy (SP)* (2025), pp. 1363–1380.

[52] Xue, D., Ablove, A., Ramesh, R., Danciu, G. K., and Ensafi, R. Bridging barriers: A survey of challenges and priorities in the censorship circumvention landscape. In *33rd USENIX Security Symposium (USENIX Security 24)* (Philadelphia, PA, Aug. 2024), USENIX Association, pp. 2671–2688.

[53] Yarom, Y., and Falkner, K. FLUSH+RELOAD: A high resolution, low noise, l3 cache Side-Channel attack. In *23rd USENIX Security Symposium (USENIX Security 14)* (San Diego, CA, Aug. 2014), USENIX Association, pp. 719–732.

[54] Zohaib, A., Zao, Q., Sippe, J., Alaraj, A., Houmansadr, A., Durumeric, Z., and Wustrow, E. Exposing and circumventing {SNI-based}{QUIC} censorship of the great firewall of china. In *34th USENIX Security Symposium (USENIX Security 25)* (2025), pp. 783–802.