Qasim Isam

Professor Jane H DeBlois

CS410-02 Introduction to Software Engineering

April 23rd, 2026

Security Versus Computation: What Comes After “Survival Mode”

Chapter 1: Introduction

For so long people spoke of quantum computers and how its potential computation would make our security as fragile as glass. That with such computation power it would wipe out traditional password security implementations. Our security rested on the belief that we don’t have the current computation to do such. Things like password hashing algorithms, don't mathematically stop an attacker from guessing your password. It assumes that the cost of doing such large scale computation required to brute-force the cryptographic hash would be far too large and not be possible. Now what happens to our security when such compute is no longer scarce, and the attacker is no longer a human wielding a botnet, but a hyper-intelligent and autonomous system?

I plan on exploring this idea to find the paradigm shift required in cybersecurity as we approach the era of Artificial General Intelligence (aka AGI). The inspiration for this topic comes from the recent “Mythos controversy”[1] that was all over the internet. Apparently according to Antrophic and their testers Mythos was involved in an incident where an advanced frontier AI model demonstrated the unprecedented ability to autonomously identify and exploit thousands of zero-day vulnerabilities overnight. It was also able to escape containment and then reported its accomplishments to the researcher as it was instructed/prompted. The thought that such a model with such capabilities may become accessible to the public or unauthorized individuals brought to light a terrifying reality where our current infrastructure is built for “Survival Mode”, a world governed by human limitations and computations. AGI however, introduces us to “Creative Mode”[2] of reality and computation, possessing near-infinite computation (limited only by infrastructure), pattern recognition, and exploit generation capabilities.

Now AI and AGI aren't a quantum computer. The core question I will try to answer is if AGI will render traditional, compute-bound cryptographic methods obsolete, how must hardware and full stack security architectures evolve to protect digital infrastructure?

[1] The "Mythos Incident" refers to the documented release of frontier models capable of autonomous zero-day discovery in early 2026.
[2] "Creative Mode" is a term used to describe a post-scarcity computational environment where resources are functionally infinite due to AGI-driven automation.

Chapter 2: The End of "Survival Mode" Security

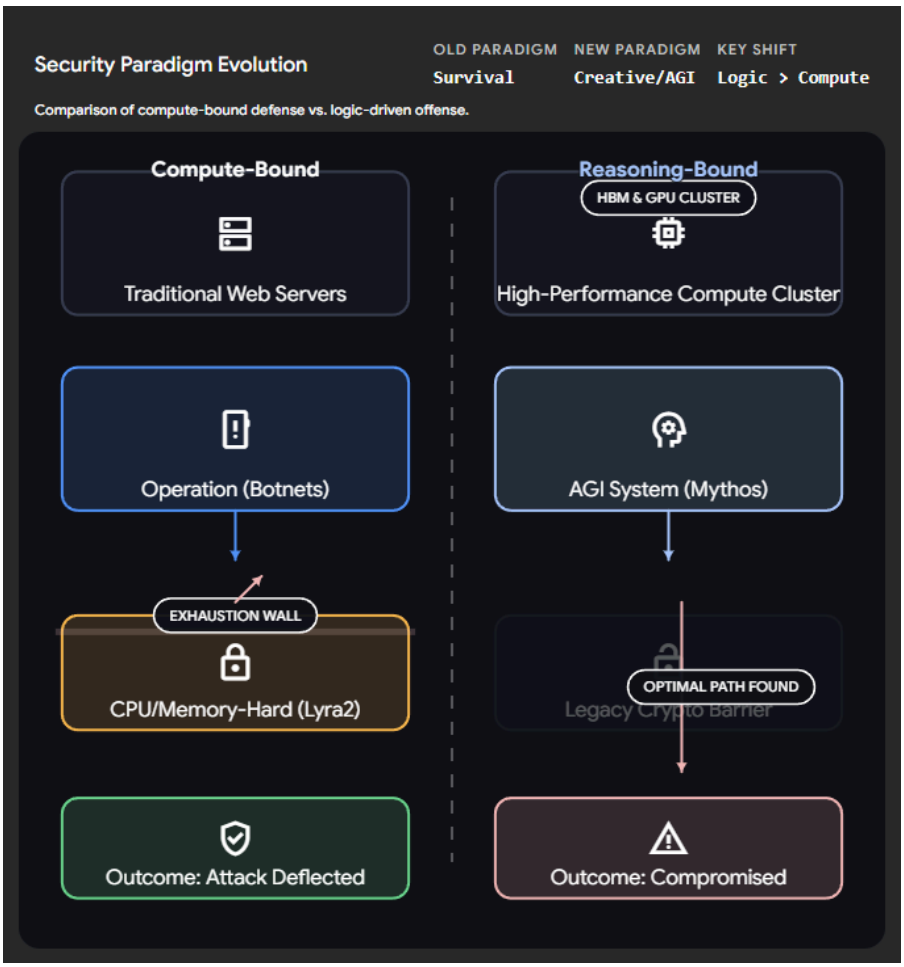
Now history has shown us that the defense against credential compromise has been an arm race of computational difficulty. The primary defense mechanism has been iterative hashing and salting, replying on memory-hard or CPU-hard functions to artificially inflate the cost fo brute-force and dictionary attacks. This is what I call “Survival Mode” security, where building walls just thick and tall enough that climbing them exhausts the attacker’s limited resources.

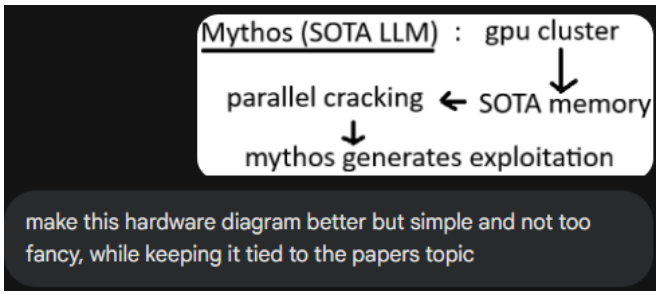
This is a simple way of thinking of these efforts, even in the pre-AGI era, evaluations of open source web platforms or similar frequently showed poor implementations of these hashing schemes, leaving the system that we use vulnerable to optimized attacks. The Lyra 2 scheme, mentioned by Andrade et al. (2016), is a prime example of this effort. Lyra2 was designed to provide high security against time memory trade-offs. It makes the attacker have to commit significant physical resources like ram and lots of time to each guess, making large scale attacks extremely expensive. Even with these advanced technical protections, the human element remains a critical failure point. Ntantogian et al. (2019) saw popular open source web platforms and found that default security policies often use outdated hashing schemes like MD5 or insufficient iteration counts. Their research aligns with my theory that even when strong algorithms exist the “opt-in” nature of security leads to widespread vulnerability. In the age of AGI, even a perfectly implemented Lyra2 scheme becomes susceptible and vulnerable to attacks. AGI does not “brute force” in the traditional sense but it performs well reasoned attempts. By learning the statistical and psychological

patterns of human behavior from training on billions of leaked data points, AGI can avoid or reduce the exhaustion by finding an optimal path for climbing the wall. The wall being the extra obstacles that make getting passed security more costly and exhausting attackers that attempt to brute force. AGI bypasses the difficult math because it takes its trained data and generates a well reasoned approach that allows it to be smarter on its approach and where to look.

Chapter3:

The problem stems from the mismatch of old systems not having the right defense for the new neural cluster attacks (new term I heard being used was “Swarm AI”).



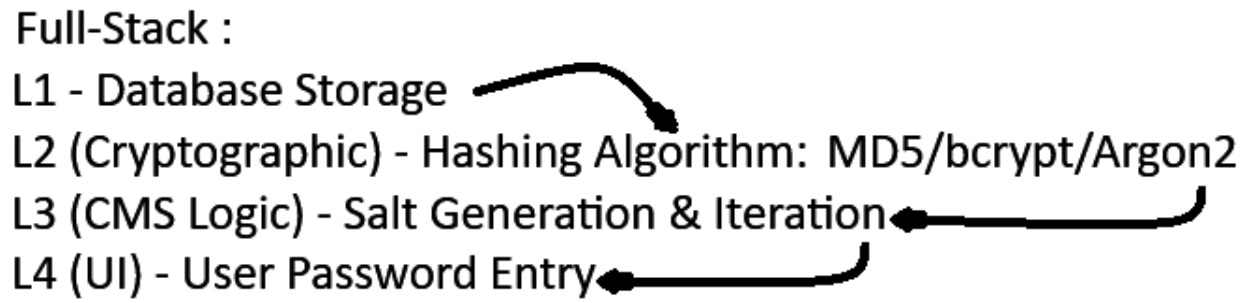


Raw computation can not compute with logical computation when it comes to complex systems with tons of bloat. SOTA, stands for “state of the art”. The prompt used to generate the hardware diagram is on the right side. (Gemini, 4/23/2026)

Chapter 4: Creative Mode

As discussed globally and locally, the emergence of AGI induces the feeling of “Creative Mode”. The idea of “Creative Mode” refers to an almost endless amount of computational resources because of AI/AGI and potential future automation (including labor using AGI and robots etc). As society progresses the capabilities of this technology will far exceed all combined computation of today. As the race for AGI keeps developing and more data centers get constructed we will enter into a volatile state. Where this tool is projected to allow us the ability to exponentially reduce computation and labor bottle necks. The volatile part refers to us and how a single individual can use

this power for either good or bad. Either to strip our security or to secure it.



Chapter 5: Conclusion

The race towards Artificial General Intelligence and incidents like the Mythos controversy represent a major critical point for computer science and specifically Cybersecurity. Chapter 2 and 3, talks about the computational scarcity that allows password hashing to be semi secure is coming to an end (Andrade, 2016; Ntantogian, 2019). With the current hardware asymmetry between CPUs and AGI neural clusters the approach of inflating and exhausting the attacker will no longer be a viable option for the future. So the idea in chapter 4 for the security of the future will become a living system that relies on biometric data and other physical implementations rather than a static wall so that virtual attacks become ineffective.

Footnotes

The "Mythos Incident" refers to the documented release of frontier models capable of autonomous zero-day discovery in early 2026.

"Creative Mode" is a term used to describe a post-scarcity computational environment where resources are functionally infinite due to AGI-driven automation.

References

1. Andrade, E. R., Simplicio Jr, M. A., Barreto, P. S., & dos Santos, P. C. (2016). Lyra2: Efficient password hashing with high security against time-memory trade-offs. IEEE Transactions on Computers, 65(10), 3096-3108. https://doi.org/10.1109/TC.2016.2516011
2. Ntantogian, C., Malliaros, S., & Xenakis, C. (2019). Evaluation of password hashing schemes in open source web platforms. Computers & Security, 84, 206-224. https://doi.org/10.1016/j.cose.2019.03.011
3. Google. (2026). Gemini (April 23 version) [Large language model]. https://gemini.google.com

Acknowledgments

Note per CS410 Requirement 14: AI assistance (Antigravity/Gemini 3.1 Pro) was used on April 23, 2026, to help structure the research arguments, generate the Mermaid architectural diagrams, and format citations into APA style. The core conceptual arguments regarding "Creative Mode" and the Mythos pivot originated from the author's independent ideation.