Concept for Summer Research Focus: An Adaptive AI Framework for Ransomware Defense

Alex Towell
atowell@siue.edu
Department of Computer Science
Southern Illinois University-Edwardsville

May 10, 2025

I've been developing some ideas for an advanced AI framework to tackle ransomware, and I'm excited about its potential for our research. I wanted to outline the core concepts and propose exploring this further as a 3-credit independent study or focused research course this summer. This could be a great way to make substantial progress and also align with broader interests, perhaps even involving Dr. Gultepe.

The Big Idea: Intelligent, Adaptive Ransomware Defense

The core concept is an AI system that learns to proactively and intelligently handle ransomware threats. Instead of static defenses, this system would feature:

- **A Cognitive Core**: An RL-trained policy (e.g., based on a DNN) that learns optimal strategies for detection, response, and mitigation.
- **Deep Contextual Understanding**: The policy operates on rich context (from logs, network activity, etc.) represented as latent embeddings. This allows it to discover and act on subtle patterns.
- **An LLM as a Dynamic Tool**: This is a key part. The RL policy itself would learn to ”prompt engineer” a Large Language Model. The LLM would be used by the policy to:
  - Dynamically rewrite and augment the context (e.g., pulling salient examples from an associative memory).
  - Analyze the current environment to generate useful metadata, enriching the policy's state awareness.

The emphasis is on a system where the policy doesn't just act, but actively learns how to best gather and process information using the LLM as a powerful, adaptable assistant. We can also incorporate non-latent features or DBN-style variables where useful, but the primary thrust is leveraging learned latent representations.

Promising Extensions to Explore

Two particularly exciting avenues we could investigate as part of this research include:

- **Ransomware-Specific LLM**: Pretraining/fine-tuning the LLM on cybersecurity data to make it a ”ransomware expert,” significantly boosting its effectiveness within the framework.
- **Adversarial Training**: Developing the defense policy by pitting it against an AI-driven attacker. This would push the defender to become exceptionally robust and adaptive to novel threats.

Summer Research Focus (3-Credit Project/Course)

I propose dedicating the summer (as a 3-credit independent study, directed research, or a custom online course module) to formally dive into this. The main goals would be:

- To further develop the theoretical underpinnings of this framework.
- Potentially prototype key components (e.g., the policy-LLM interaction loop or the context embedding strategy).
- Lay the groundwork for future publications.

Given my self-driven nature, I’m confident I can make significant headway. This would directly contribute to my dissertation research and our group’s objectives.

Next Steps

I’d love to discuss this with you further at your convenience to see if this aligns with your vision for my summer research and how we might best structure it.