

AutoPGT: LLM-Driven Security Policy Generation

Jiahui Lim, Wen Shei Ong, Dr. Rochelle Xenia Mendoza Santos, Dr. Utku Tefek, Dr. Ertem Esiner

Motivation

The **intricate ecosystems** of Industrial Control Systems (ICS) often possess **complex, system-specific vulnerabilities** that necessitate **tailored cybersecurity measures**. Traditional one-size-fits-all security policies are typically inadequate for addressing the unique challenges in these heterogeneous environments. However, **manually designing** customized security policies remains a **labor-intensive, error-prone, and time-consuming** process.



Specialized Expertise

Technical knowledge and skills are required to develop **effective security measures**.



System Customization

Security policies must be **tailored** to the system's **unique vulnerabilities**.

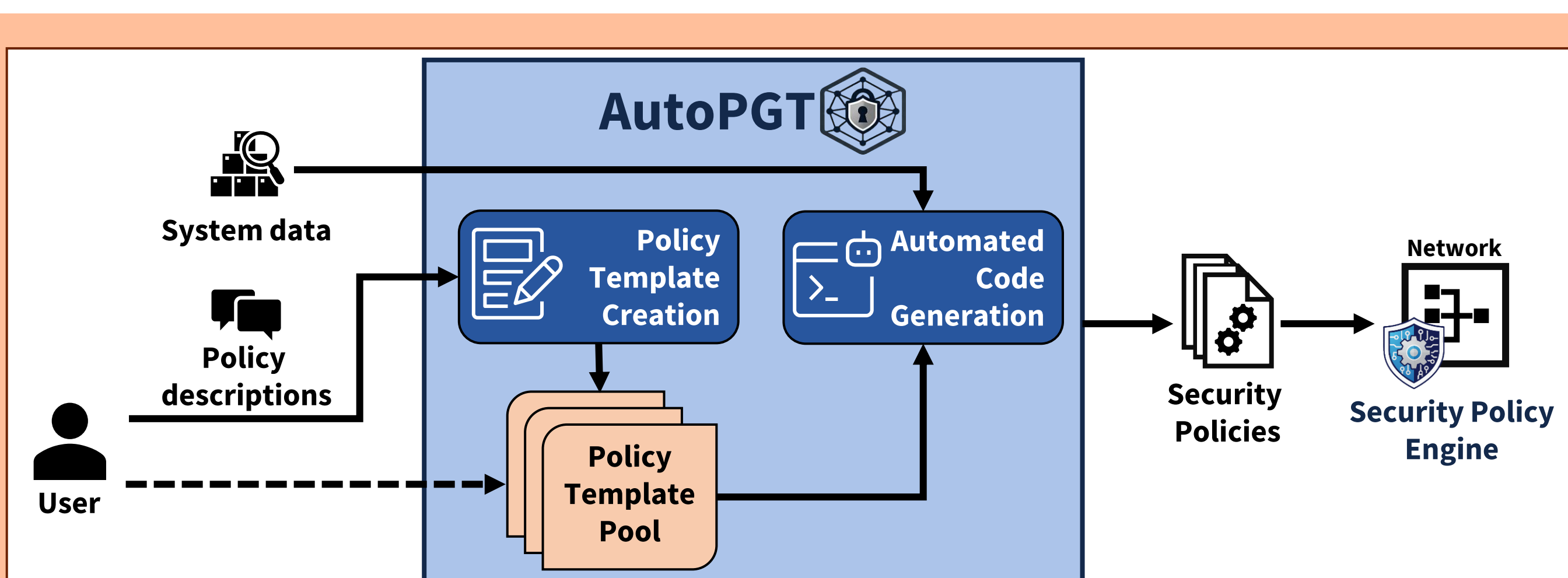


Limited Agility

Manual development can take **weeks to months**, making it **slow to adapt** to threats.

Solution Overview

The **Automated Policy Generation Tool (AutoPGT)** accelerates security policy development by generating **customized security policies** from **user descriptions** and **network data**.



High-level Overview of AutoPGT

Security Policies are **developed** through the following procedure:

- 1 **Craft Security Policy Templates**
Describe and refine security policies with **AI Assistance** through the **chat-based interface**.
- 2 **Compile Security Policy Templates**
Utilize your own custom policies or import from the **template library**.
- 3 **Import Network Data**
Provide **representative sample data** to AutoPGT for analysis.
- 4 **Generate Security Policy Code**
Wait for AutoPGT to **generate code tailored** to your system.
- 5 **Deploy Security Policy to the Engine**
Enforce your policies in real-time with the **Security Policy Engine**.

AutoPGT Key Features



Smart Policy Drafting

AutoPGT's **LLM-driven pipeline** and **chat-based interface** helps users quickly define and refine security policies, **reducing manual effort**.



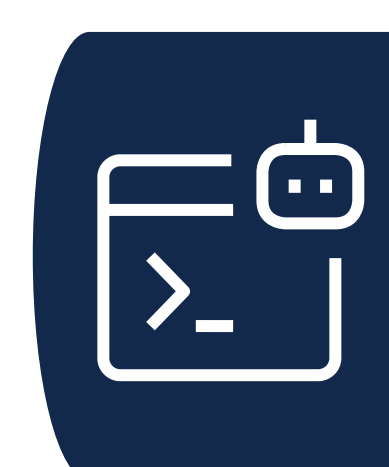
Template-Based Policy Design

Drafted policies are stored as **system-agnostic templates**, allowing them to be **reused, imported** from template libraries, and **tailored** to different systems.



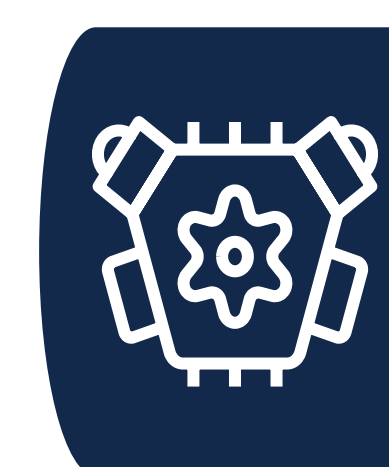
Data-Driven Customization

By **analyzing** sample network data, AutoPGT identifies **underlying network properties** to automatically **customize policies** to each system.



Automated Code Generation

AutoPGT's generated **Security Policy** consists of **executable code** and a **parameter database**, based on the policy template and insights obtained from sample data.



Security Policy Engine Integration

Generated policies are **fully compatible** with the Security Policy Engine, enabling **immediate deployment and enforcement**.

Video Demonstrations and Digital Resources



Product Brochure

A digital copy (PDF) presenting AutoPGT's problem statement, solution overview, key features, and demonstrations.



Technical Overview

An introductory video for AutoPGT covering its overall workflow and step-by-step policy generation pipeline.



AI-Assisted Policy Drafting

A video demonstration of drafting security policies using AutoPGT's chat-based interface and LLM-driven pipeline.



Policy Drafting with Automated Custom Conditions

An advanced demonstration of security policy drafting, showcasing AutoPGT's detection and guided creation of Custom Conditions.