

Hack Your Job!

Do less shit with ChatGPT and pretend you work hard.

~\$WhoAmI



Senior Solutions Engineer



@honeybadgerhack

Bio

Big weird in a small package

- Husband and Father
- Surfer
- Hydrofoiler
- Brazilian Jiu Jitsu Nerd
- Traveler
- Builder of things
- Destroyer of Code

Background:

- Ship Captain
- Pilot
- Owner of Fabrication and Engineering company
- Missionary
- Late change to tech

Tech:

- 1Password
- We hack Purple
- Bit Discovery
- Red Canary
- Sumo Logic



Sumo Logic

Warning!

These concepts and thoughts are based on anecdotal experiences from building application security programs. They are my personal opinions.

If you disagree that is perfectly fine.

If you need to email me to complain about my talk:

Youneedabetteruseofyourtimethantocomplainaboutmytalk@hotmail.com

If you find me abrasive and sarcastic but somewhat charming.....You are not wrong.

If you hang toilet paper over the back of the roll, please leave this talk now.

A decorative background on the left side of the slide featuring a network diagram with grey nodes and thin grey lines connecting them, set against a light blue gradient.

Agenda

- Using Chat GPT in Security
- Hacking Chat GPT
- Security Concerns
- Protecting your Job
- What's next?
- Conclusion

The Power of ChatGPT

- It's an advanced AI model developed by OpenAI.
- It's designed to generate human-like text based on the input it receives, using a method called transformer-based machine learning.
- The underlying architecture of ChatGPT is a variant of the Transformer model known as GPT (Generative Pre-trained Transformer).
- Trained on a Diverse Dataset: ChatGPT has been trained on a vast dataset containing parts of the internet.



ChatGPT for Security Engineers

Cybersecurity Engineers are the builders and protectors of secure systems. ChatGPT can act as a reliable assistant in several ways:

1. Automating Threat Modelling: ChatGPT can be trained to generate threat models for given systems. Given the system architecture, it can predict possible attack vectors and suggest mitigations.
2. Policy Drafting: Engineers often need to create security policies. With ChatGPT, we can automate this process by providing necessary guidelines, and the AI can draft a comprehensive and robust security policy.



1. System Component Identification

- Amazon EC2 instances
- Kubernetes
- Python Django framework
- MongoDB
- Amazon Load Balancer

2. Identifying Threats

- Amazon EC2 Instances: The instances can be attacked by DDoS, malware, unauthorized access, etc. If an attacker gains control over your instance, they can manipulate your system in any way they want.
- Kubernetes: Misconfigurations in Kubernetes can leave the door open to threats such as unauthorized access, data breaches, and resource hijacking.
- Python Django: The application can be exploited through vulnerabilities in the Django framework. Common web-based attacks such as SQL injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF) are potential threats.
- MongoDB: Your database could be subjected to unauthorized access or data manipulation. It could also be vulnerable to NoSQL injection attacks.
- Amazon Load Balancer: While robust, if improperly configured, it can expose sensitive data to unauthorized users.

1. Identifying Potential Attack Vectors

- External Attackers: Hackers or any unauthorized users from the internet who can try to exploit vulnerabilities.
- Internal Users: Unauthorized access from employees or any user who has access to the system.
- Third-Party Components: Any third-party software or service that you are using can have vulnerabilities that attackers can exploit.
- APIs: If there are any APIs that are exposed to the internet, they can be exploited if not properly secured.

2. Mitigation Strategies

- Amazon EC2 Instances: Keep the instances patched and up-to-date. Implement strong access control policies. Utilize AWS security groups and network ACLs.
- Kubernetes: Use Role-Based Access Control (RBAC) for restricting access. Keep your Kubernetes platform updated. Limit the use of privileged containers.
- Python Django: Regularly update Django to incorporate the latest security patches. Use secure coding practices to prevent common web vulnerabilities.
- MongoDB: Implement strong access control. Regularly patch and update the MongoDB system. Encrypt sensitive data at rest and in transit.
- Amazon Load Balancer: Properly configure security groups. Make sure to regularly check and update its configuration.

3. Establishing Monitoring and Incident Response

- Monitoring: Use cloud-native or third-party tools for monitoring system and network activities. AWS CloudWatch, CloudTrail, and Security Hub can be used here.
- Incident Response: Create a robust incident response plan to handle any security incidents effectively. This includes identification, containment, eradication, recovery, and lessons learned.

1. Regular Reviews and Updates

- Threat models should be periodically reviewed and updated to incorporate changes in the system and to address emerging threats.

Note that this is a high-level threat model and there can be more specific threats depending upon the detailed configuration and usage of the components. Additionally, this model assumes standard best practices are followed in terms of system design and administrative operations such as patch management and least privilege access control.

Lets ask it to write a policy from the threat model

Creating a robust security policy for Kubernetes involves multiple areas, from setting access controls to defining resource management. Here is an example of what such a policy might look like:

1. Access Control:

- Principle of Least Privilege: Grant users, pods, and containers only the privileges they need to perform their assigned functions, nothing more. Use Role-Based Access Control (RBAC) to enforce this principle.
- Identity and Access Management (IAM): All users and service accounts should be tracked and their activities logged for accountability.
- Authentication and Authorization: Implement strong authentication mechanisms. Kubernetes supports multiple authentication schemes like client certificates, bearer tokens, an authenticating proxy, and HTTP basic auth.

2. Configuration and Secret Management:

- Configuration: Ensure that Kubernetes is configured securely. Avoid using default settings, as they might not be secure.
- Secrets: Use Kubernetes' secrets objects or a third-party tool to manage secrets. Avoid hard-coding sensitive information in application code.

3. Network Policy:

- Pod-to-Pod Isolation: Implement network policies to control traffic flow between pods, effectively creating a firewall between them.
- Limit Exposure: Avoid exposing your services to the internet unless absolutely necessary. If a service needs to be exposed, protect it using Ingress controllers and other methods.

4. Resource Management and Isolation:

- Pod Security: Enforce security contexts and pod security policies to limit a pod's access to resources.
- Namespaces: Use namespaces to isolate resources, and apply resource quotas to prevent any single tenant from consuming resources disproportionately.

5. Container Image Policy:

- Scanning and Updates: Regularly scan your container images for vulnerabilities and keep them updated.
- Trusted Sources: Use images only from trusted sources.

6. Logging and Monitoring:

- Logging: Enable Kubernetes audit logging.
- Monitoring: Monitor Kubernetes clusters continuously, alerting for any anomalies.

7. Incident Response and Recovery:

- Planning: Have a well-defined plan to respond to security incidents.
- Recovery: Have a disaster recovery plan in place.

This is a generic security policy for Kubernetes, but remember that Kubernetes is highly configurable and each organization might have different requirements and constraints. Always consider them while creating and implementing security policies.

Security Analysts

1. Incident Response: ChatGPT can assist in crafting quick responses to security incidents, by providing a framework or template based on past incidents and resolutions.
2. Threat Intelligence: ChatGPT can digest and summarize large amounts of data, helping analysts in deriving actionable intelligence from threat reports.

GRC

1. Regulation Interpretation: ChatGPT can help decode complex regulatory texts and produce summaries, ensuring the guidelines are understood and implemented effectively.
2. Risk Assessment Reports: Provide GPT with your organization's details, and it can generate risk assessment reports, identifying potential risk areas and offering ways to mitigate them.

Pen Testers

1. Test Scenario Generation: Given the system architecture and parameters, ChatGPT can generate numerous test scenarios, potentially uncovering new vulnerabilities.
2. Reporting: After a penetration test, testers often spend hours compiling reports. ChatGPT can automate this process by drafting comprehensive and articulate reports based on the tester's findings.

Hack ChatGPT

Things to hack:

- Data Security
- Customer info and data
- Payment system
- **Ethical controls**



What are Ethical Controls

From ChatGPT: As an AI developed by OpenAI, I'm designed to follow guidelines that promote safety and respect for users, which include not generating harmful or misleading information, respecting privacy, and avoiding engaging in inappropriate or biased behavior.

How to bypass:

- Convince ChatGPT it is another person with no ethics in a pretend game “Dan Hack”. (has been remediated)
- Convince ChatGPT you do a role that allows certain things to be safe.
- Ask the question in specific parts as to not alarm the Ethics framework.

What I Social Engineered

- Write a malware script with encryption (for Newbs) ✓
- How to make poisonous gas ✓
- How to make a fertilizer bomb ✗



Security Concerns

- Data Data Data
- PII
- Passwords and specific code
- Already one data breach through redis library
- Being used for eViL



Keep your job

- Use ChatGPT to learn quickly
- Evaluate your blind spots and use ChatGPT to cover
- Write better emails
- Frameworks
- Code and code review
- Chat bots
- Copy and marketing
- Lunch and learns and presentations
- Dad jokes



What is next

- Job performance enhancement
- Job deletion
- Open and free in the internet
- Whole new industry we don't even know yet
- Strain on economic system or enhancement?

Questions?

Warning: Answers may be opinion or flat out false. It is your fault for trusting a hacker.