Applying AI to the SDLC: New Ideas and Gotchas!

Leveraging AI Models to Improve Software Creation

Trac Bannon
Senior Principal
Software Architect & Digital Transformation Advisor
MITRE Advanced Software Innovation Center

April 2023

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

Tracy L. Bannon

"Trac"

Software architect | engineer | mentor | community leader

Who Am I?

/trās/

Metrics
Value Stream Design
#OpenSource
#DevOps
Continuous Testing
#StraightTalkforGovt
Agility
#DevSecOps
Continuous Improvement
#TDM
Ruthless Prioritization
Automation
CI/CD
Building Digital Workforce
Modernization
#CloudNative
CALMS
#RealTechnologists
Emersive Learning
Digital Transformation
Psychological Safety
Community
DoJo
#SomethingToNoodleOn
Current State Baseline
Low Code/No Code
CyberSecurity
Secure by Design
Minimum CD
#DesignPatterns
Modern Software Practices
Evolutionary Architecture
AI-Assisted SDLC
Value Stream Mapping

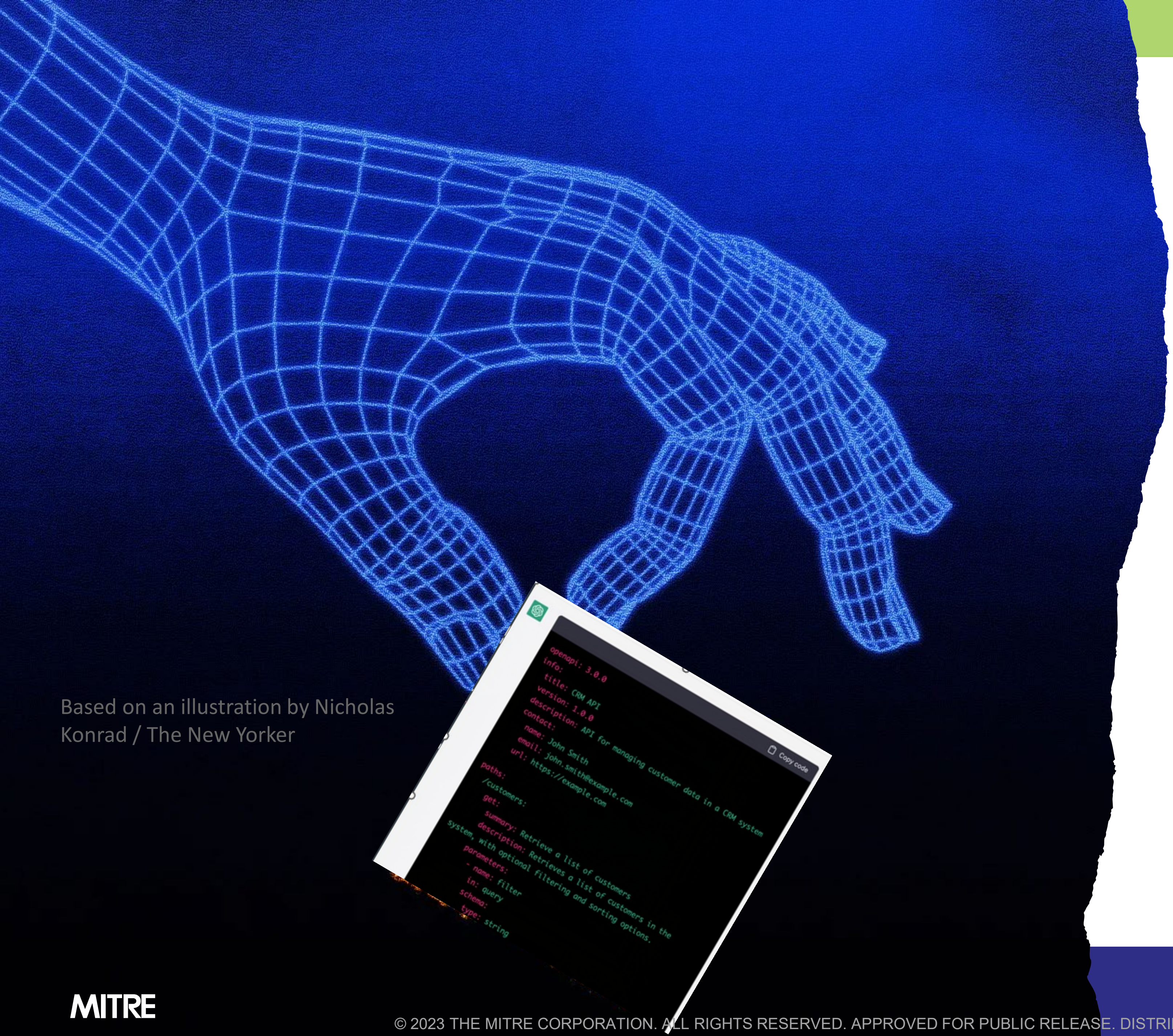
vsm consortium
Influencer

AMBASSADOR
DevOps Institute
ADVANCING THE HUMANS OF DEVOPS

IEEE
SENIOR MEMBER

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

Artificial Intelligence and Software Development



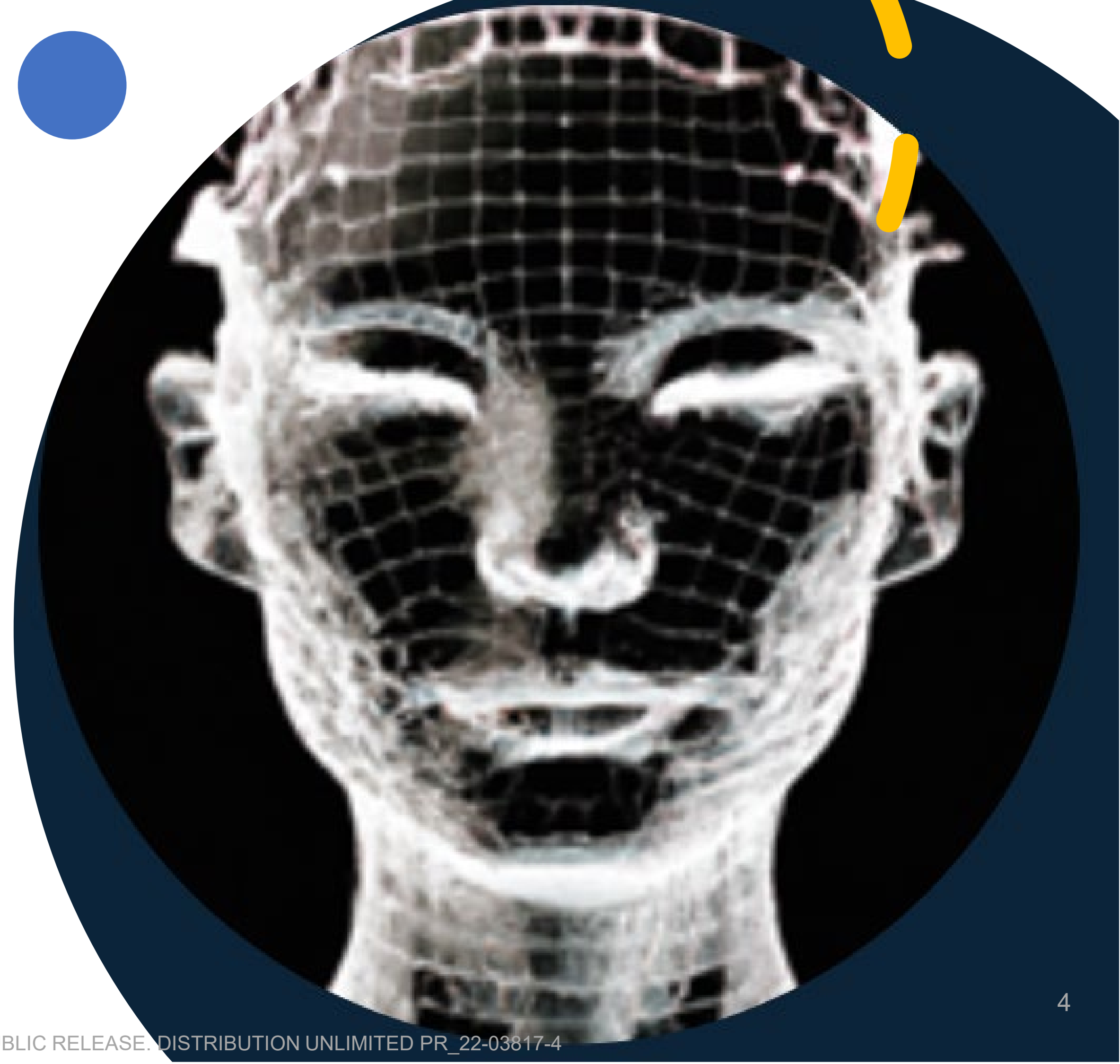
```
openapi: 3.0.0
info:
  title: CRM API
  version: 1.0.0
  description: API for managing customer data in a CRM system
  contact:
    name: John Smith
    email: john.smith@example.com
    url: https://example.com
paths:
  /customers:
    get:
      summary: Retrieve a list of customers
      description: Retrieves a list of customers in the
system, with optional filtering and sorting options.
      parameters:
        - name: filter
          in: query
          schema:
            type: string
```

Based on an illustration by Nicholas Konrad / The New Yorker

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

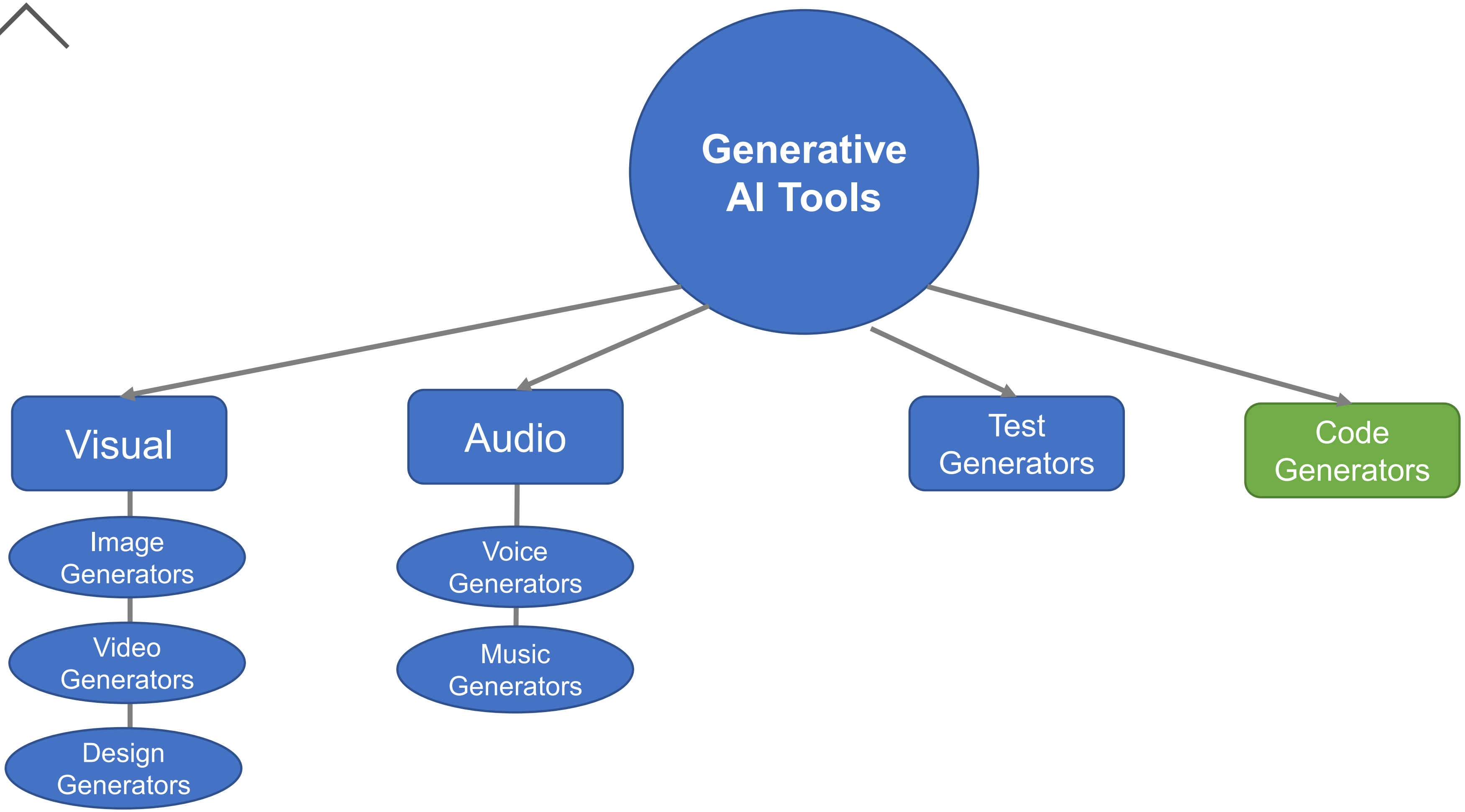
Some definitions to help our conversation

- **Generative AI** is a category of AI algorithms that focus on generating new content, data, or patterns after being trained on existing information.
- Generative AI includes text, images, video, or even music (tool names)
- **Large language models (LLMs)** are a subset of Generative AI trained on vast amount of text data
- LLMs calculates probability distribution over sequences of words and scores the likelihood of word sequences
- Parameters in LLMs help the model to understand relationships in the text, which helps them to predict the likelihood of word sequences
- By sampling over the probability distribution, the models can write text mimicking human-like language understanding
- **AI-assisted** development often refers to using LLMs to improving developer productivity



MITRE

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4



Generative AI Tools

Visual

Image Generators

Video Generators

Design Generators

Audio

Voice Generators

Music Generators

Test Generators

Code Generators

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

Generative AI and the SDLC

LowCode/NoCode

- Faster adoption into the LC/NC platforms
- Purpose of the platforms are to simplify and accelerate
- Equipping non-IT personas
- Leveraging AI *before* the recent GPT surge
- Suggests users are more likely to adopt new tech

Custom Development

- Improving quality
- Jumpstart code segments
- Repetitive tasks
- Investment in **Hyperautomation**

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

By 2026, 80% of developers will be outside formal IT departments[1]

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

What to use it for right now

- Documentation and knowledge sharing
- Personalized learning and training
- Inspiration
- Natural language translation

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

Generative AI and LC/NC

- Automated app generation (OutSystems, Appian)
- User interface (UI) design. (UI Bakery, Wappler)
- Workflow optimization (Mendix, Microsoft Power Automate)
- Integration support (Zapier, Integromat)
- Domain-specific language (DSL) generation (Betty Blocks, Retool)
- Customizable AI components (Appgyver, Quick Base)

Artificial Intelligence and Low Code/No Code: https://youtu.be/8Vat_jRt128

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

Using LLMs to help with Coding

Some ways to provide AI-assistance with LLMs:

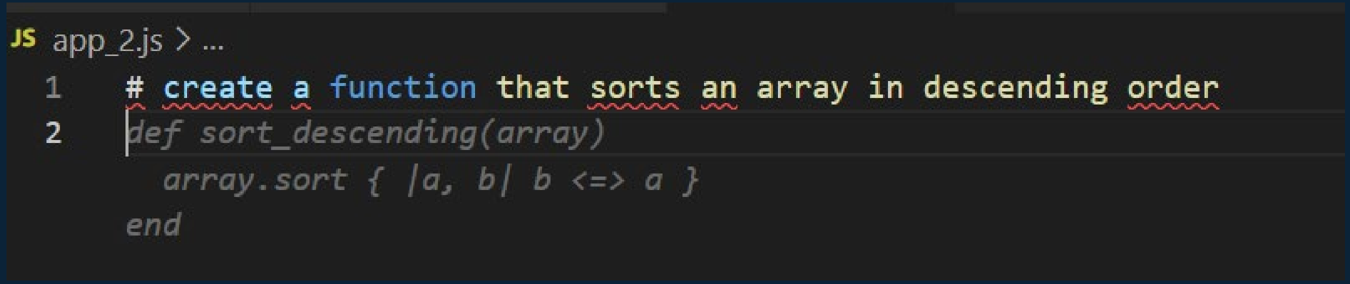
- Code Completion
- Code Review
- Code Generation
- Style Checking
- Issue identification and debugging
- Code Refactoring

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

Generative AI – Code Completion - 1

Platform: Tabnine – AI Autocomplete Generative Feature

Faster Code Completion



```
# create a function that sorts an array in descending order
def sort_descending(array)
  array.sort { |a, b| b <=> a }
end
```

<u>Ideas and Gotchas:</u>

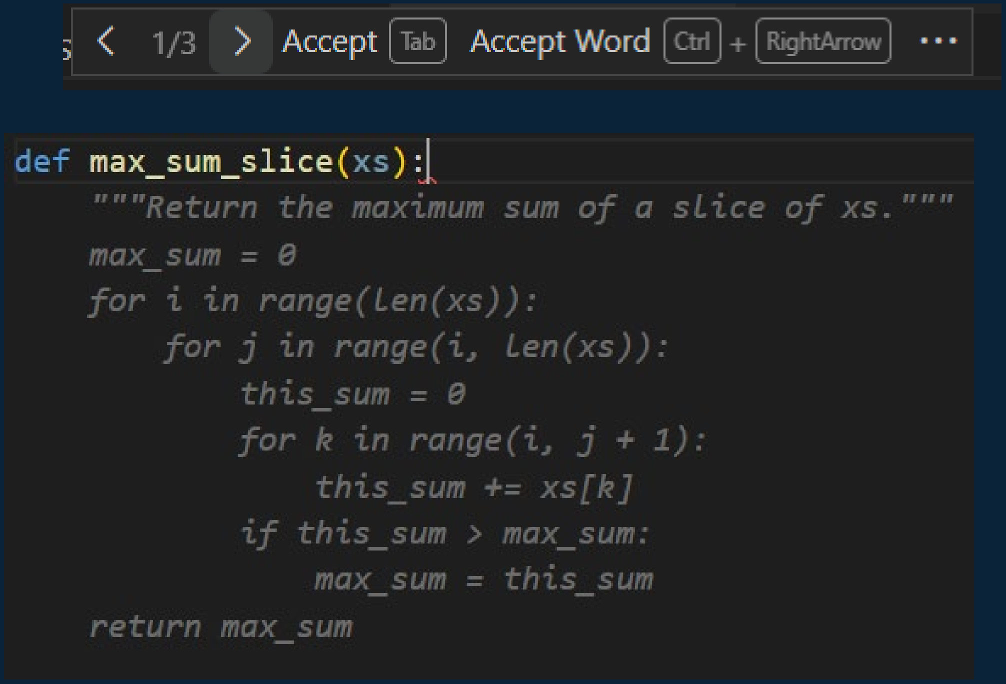
- Overreliance may fail to develop their own skills or may not explore other more innovative /creative options
- Possible security vulnerabilities may go unnoticed
- Tools lack context; suggestions may be syntactically correct but semantically incorrect
- Be mindful of performance hit to development machine/environment
- Doesn’t make use of functions defined in the code elsewhere
- For now, always use in tandem with quality scanning tools

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

Generative AI – Code Generation - 2

Platform: CoPilot – Alternative Solution Generation Feature

Generating Code



```
def max_sum_slice(xs):
    """Return the maximum sum of a slice of xs."""
    max_sum = 0
    for i in range(len(xs)):
        for j in range(i, len(xs)):
            this_sum = 0
            for k in range(i, j + 1):
                this_sum += xs[k]
            if this_sum > max_sum:
                max_sum = this_sum
    return max_sum
```

Ideas and Gotchas:

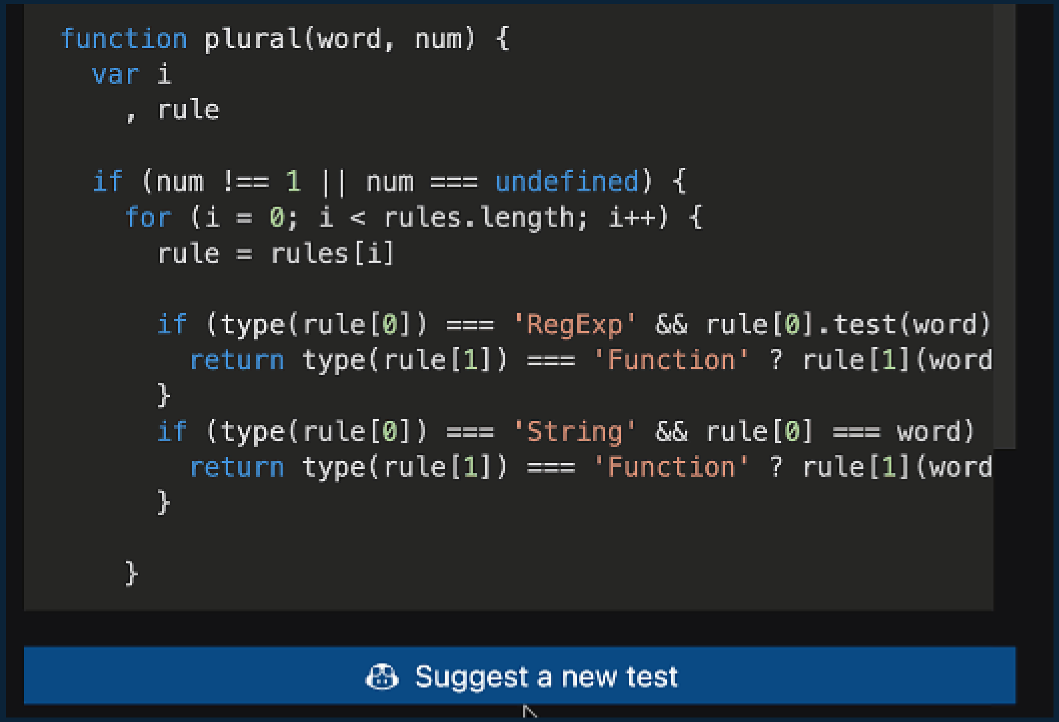
- Defects abound - if you are new in career and can't easily identify defects, you will waste time
- Start the code yourself and be as explicit as possible
- Limited context: doesn't make use of functions defined in the code elsewhere
- Users accepted on average 26% of all completions shown by GitHub Copilot
- GitHub recommends precautions "to ensure its suitability" :
  - Rigorous testing
  - IP scanning
  - Checking for security vulnerabilities

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

Generative AI – Code Generation - 3

Platform: CoPilot – Unit Test Generation Feature

Generating Unit Tests



```
function plural(word, num) {
  var i
    , rule

  if (num !== 1 || num === undefined) {
    for (i = 0; i < rules.length; i++) {
      rule = rules[i]

      if (type(rule[0]) === 'RegExp' && rule[0].test(word)
        return type(rule[1]) === 'Function' ? rule[1](word
      }
      if (type(rule[0]) === 'String' && rule[0] === word)
        return type(rule[1]) === 'Function' ? rule[1](word
      }

    }
```

Ideas and Gotchas:

Generates based on the context of the code sample you are writing

Accelerated developer learning by suggesting more comprehensive tests

Not a unit testing framework

Tabnine has release a BETA test generation feature

MITRE

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

Not quite ready for prime time

- **Current** tools show tremendous potential
- Developing a generative AI model is resource intensive and **currently** out of the question for all but the biggest and best-resourced companies[4]

These use cases are exploding and by late summer, expect new tools, pricing model, and benefits

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

Questions to ask your vendors

How does the platform ensure the security and privacy of data used by the generative AI models?

What measures have been taken to prevent the AI model from generating malicious or vulnerable code?

How does the platform manage and control access to the generative AI models and their generated outputs?

How does the vendor handle AI model updates, and what steps are taken to evaluate and maintain the security of the generative AI models over time?

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

The Hype around ChatGPT

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

ChatGPT – Quick Context

- ✓ Released in November by Open AI
- One million subscribers in first 5 days; over 100 million users now
- Funded, in part, by Microsoft and hosted on Azure
- Creative usage in myriad domains from education to contracting to art to copy
- Spitting out copy with tremendous literary flare

MITRE

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

The ChatGPT Attraction

The model and the interface essentially understands and responds to natural language text

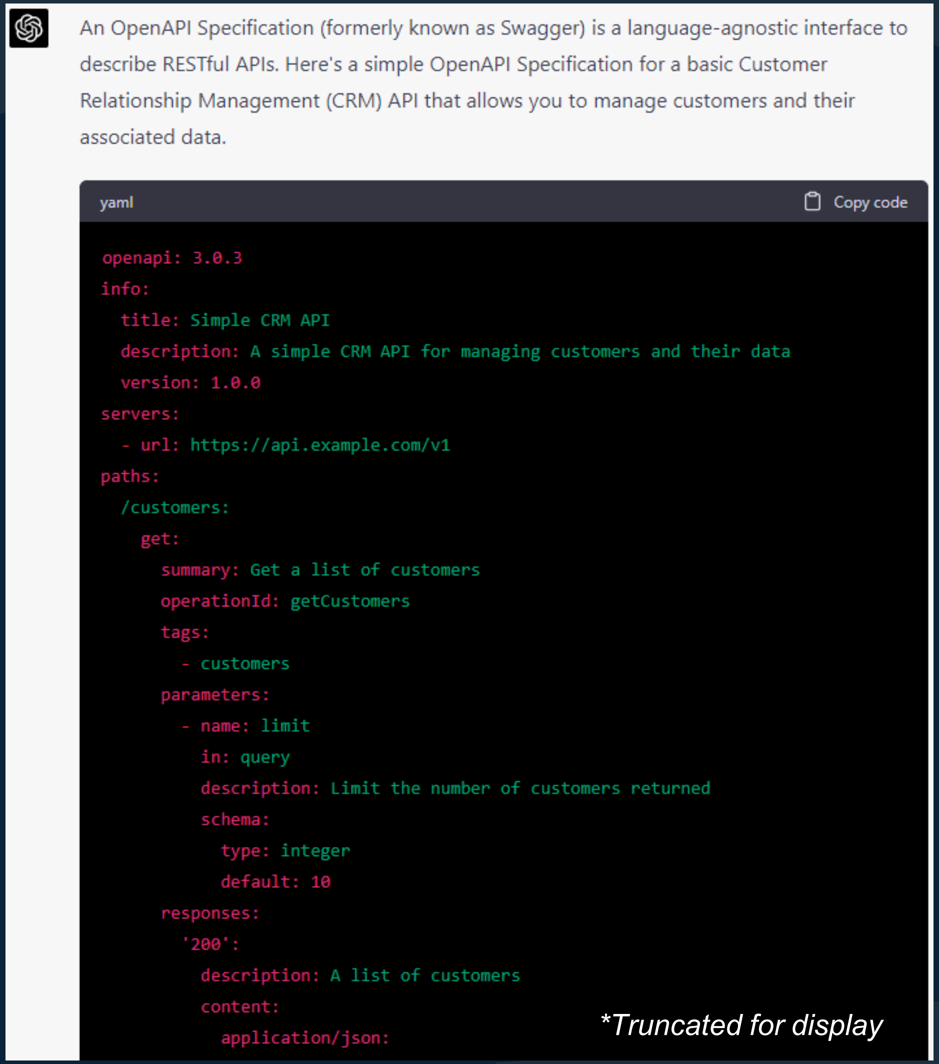
ChatGPT responses are both eerily entertaining and oddly educational

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

ChatGPT for API Generation

Actual ChatGPT Prompt: “*write an OpenAPI Spec for a CRM API*”

Generated Response:***



An OpenAPI Specification (formerly known as Swagger) is a language-agnostic interface to describe RESTful APIs. Here's a simple OpenAPI Specification for a basic Customer Relationship Management (CRM) API that allows you to manage customers and their associated data.

```yaml
openapi: 3.0.3
info:
  title: Simple CRM API
  description: A simple CRM API for managing customers and their data
  version: 1.0.0
servers:
  - url: https://api.example.com/v1
paths:
  /customers:
    get:
      summary: Get a list of customers
      operationId: getCustomers
      tags:
        - customers
      parameters:
        - name: limit
          in: query
          description: Limit the number of customers returned
          schema:
            type: integer
            default: 10
      responses:
        '200':
          description: A list of customers
          content:
            application/json:
```

**Truncated for display*

Ideas and Gotchas:

- *ChatGPT understood CRM domain*
- *Understood HTTP methods (Get, POST, PUT, DELETE)*
- *Easily addressed syntax errors when code ported to OpenAPI Generator*
- *Little value to using for unit test generation over OpenAPI.Tools*

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

Commonly Claimed ChatGPT Benefits

Faster Results

Focus on higher-level problems, delegate boiler plate code to the platform

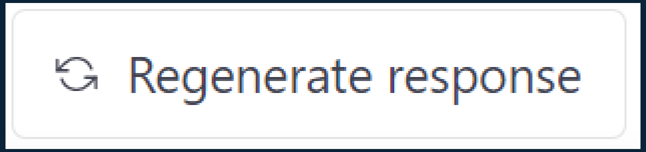
Work on problems in domains where you are not an expert

Learn new programming languages

Use AI to explain what a piece of code does

Assisted debugging, code reviews, PR content reviews

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4



ChatGPT is very good for coming up with new things that don't follow a predefined script. It's great for being creative... but you can never count on the answer.

Ajay Agarwal, a professor at the University of Toronto whose research focuses on the economics of AI

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

The way forward

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

Rapid Growth Areas

- Natural language-to-code translation
- Rapid Prototyping
- Intelligent Development Assistants
- Analytics Automation and Error Handling
- Automatic Code Refactoring
- Forecast Precise Estimates
- Strategic decision-making
- User experience/Human factor analysis

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

AI Assisted or AI replaced?

- Augmentation to start
- Coding as we know it is forever changed
- AI-powered automated code generation
- Free up humans from routine tasks
- Creativity still resides with the humans
- In 10 years, developers will need to understand semantics, concepts, and logical sequences… and prompt engineering

This isn't new… in 1950's, Grace Hopper and her team developed FLOW-MATIC that used English-like statements[3]

Don't panic!

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

Considerations

- SBOM ramifications & tracing lineage
- Detecting generated code
- Tradeoffs of training a private model
- Costs:
  - Free tier becoming more feature poor
  - SaaS billing per user
- Beware tool explosion

MITRE

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

More Gotchas

Overreliance on generative AI, which can lead to a lack of creativity and innovation

Lack of understanding of the technology, which can lead to unrealistic expectations and disappointment

Failure to mitigate the risks of applying AI, such as ensuring transparency and accountability

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

Fix Icons

Concerns

- AI “sounds” authoritative, it car flat-out wrong
- Quality of the model training: data quality and context
- Availability and access by nefarious threat actors;
- Model training by non-US citizens

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

Possible Benefits

Fix Icons

Rapidly onboard large groups c
developers

Make developers more fungible

Make corporations less beholden to developers of their legacy codebase[6]

Use offshore resources more effectively

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

More questions to ask your vendors

What are the pricing options and licensing terms for using the generative AI features?

Are there any hidden costs or usage limitations we should be aware of?

How does the tool handle edge cases or unexpected inputs?

Are there any built-in fail-safes to prevent the generative AI from producing harmful or problematic code?

Can the generative AI model be fine-tuned or customized to our organization's specific coding standards and practices?

Is it possible to extend the model's capabilities to address our unique requirements or use cases?

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

We need to understand

- Prompt engineering as a discipline; turning human factors on its edge
- Human-Machine teaming
- Software team performance
- Trust and reliability in software outcomes when driven by AI-assisted or AI-generated software
- Automating decisions and software development workflows
- Ethics of prompts and who owns the data once created

We can't put the genie back in the bottle; we need to discuss, research, and understand

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

Call to Action

Your next steps:

- Connect with your tool and platform vendors to ask model quality and security questions
- Ask your vendor about their AI roadmap
- Pulse your organization to see if and how LLMs are being used
- Enable research and discovery or LLM usage with Cybersecurity as your highest priority
- Establish on reasonable guardrails

What I need from you:

- Share your organization’s story and lessons learned
- Continue to share out new use cases and new tools

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

Tracy L. Bannon
tbannon@mitre.org

in https://www.linkedin.com/in/tracylbannon

@TracyBannon

www https://tracybannon.tech

Disclaimer: The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

MITRE

SOLVING PROBLEMS
FOR A SAFER WORLD®

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4

References

[1] https://www.gartner.com/en/newsroom/press-releases/2022-12-13-gartner-forecasts-worldwide-low-code-development-technologies-market-to-grow-20-percent-in-2023

[2] https://spectrum.ieee.org/ai-code-generation-language-models

[3] https://www.codecademy.com/resources/blog/programming-languages-created-by-women/

[4] https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-generative-ai

[5] https://www.marktechpost.com/2022/08/25/researchers-develop-ticoder-framework-for-code-generation-using-user-feedback-with-90-4-consistency-to-user-intent/

[6] https://advisory-marketing.us.kpmg.com/speed/pov-generativeai.html

[7] https://youtu.be/8Vat_jRt128 (Artificial Intelligence and Low Code/No Code - Leveraging AI models to improve software creation)

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_22-03817-4