How to Install The New (GoLang) Fabric Client

Build and Watch Your Personal AI Ecosystem

Dexter Miller
Dec 14, 2025
5 min read

Contents

- Backgrounder
- GitHub - danielmiessler/fabric | README | Installation
  - Get Latest Release Binaries
  - Install Go
    - Install Homebrew (if not already installed)
    - Install Go using Homebrew
    - Verify the installation
  - Install Fabric
    - Install Fabric directly from the repo
    - Run install.ps1 script from danielmiessler/fabric
  - Set Environment Variables
    - Edit the zshrc file
    - Save and close the editor
    - Source the zshrc file
  - Setup
    - Run the setup to set up your directories and base models
    - Update .zshrc
  - Add aliases for all patterns
  - Test 1: Analyze Paper
    - Input
    - Output
  - Test 2: Extract Wisdom
    - Input
    - Output

Backgrounder

This step by step tutorial on how to install the fabric client builds on a previous explainer video.

Check that post out first if you haven't already seen it, then come or back for a pretty crazy installation demo so you can flex and show your friends what you can do.

GitHub - danielmiessler/fabric | README | Installation

fabric is an open-source framework for augmenting humans using AI. It provides a modular framework for solving specific problems using a crowdsourced set of AI prompts that can be integrated anywhere.

Get Latest Release Binaries

```
# Download the latest binary for your platform
curl -L -o fabric
https://github.com/danielmiessler/fabric/releases/latest/download/fabric-$(uname -s | tr '[:upper:]' '[:lower:]')-$(uname -m | sed -e s/x86_64/amd64/ -e s/aarch64/arm64/)
# Make it executable
chmod +x fabric
```

Install Go

Install Homebrew (if not already installed):

Open your terminal and paste the following command. This will install Homebrew, a package manager for macOS:

```
/bin/bash -c "$(curl -fsSL
https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
```

Install Go using Homebrew:

Once Homebrew is installed, you can install Go by running:

```
brew install go
```

Verify the installation:

To ensure Go is installed correctly, you can check its version by typing:

```
go version
```

Install Fabric

Install Fabric directly from the repo

```
go install github.com/danielmiessler/fabric@latest
```

Run install.ps1 script from danielmiessler/fabric

```
curl -fsSL
https://raw.githubusercontent.com/danielmiessler/fabric/main/install.ps1
| iex
```

Set Environment Variables

For Apple Silicon based macs:

1. Edit the zshrc file

```
nano ~/.zshrc
```

2. Add the environment variables:

```
# Fabric AI framework paths
export GOROOT=/opt/homebrew/opt/go/libexec
export GOPATH=$HOME/go
export PATH=$GOROOT/bin:$GOPATH/bin:$HOME/.local/bin:$PATH
export DEXPY_ANALYZER_VAULT="$HOME/Dexpy-Vault"
```

Make sure each export line is on a new line in the file.

3. Save and close the editor:
   - Ctrl+X
   - Y
   - Enter
4. Apply the changes:

```
source ~/.zshrc
```

Setup

```
# Run the setup to set up your directories and base models
fabric --setup
```

Add aliases for all patterns

In order to add aliases for all your patterns and use them directly, an command-line is called `fabric-pattern-symlink`. You can add the following to your `.zshrc` or `.bashrc` file:

```
# Load fabrics alias if exists
[[ -f ~/.config/fabric/alias.zsh ]] && source ~/.config/fabric/alias.zsh
# Function to create symlinks for all patterns
fabric-pattern-symlink() {
    echo "Creating symlinks for all fabric patterns in ~/bin/fabric-patterns..."
    pattern_count=$(ls ~/.config/fabric/patterns/ | wc -l)
    echo "Found $pattern_count patterns"
    # Execute the alias command to add it to the current session
    alias fabric-pattern-symlink
}
alias f='fabric'
alias yt='f -y "$(pbpaste)"'
alias fl='f --listpatterns'
alias fs='f --liststrategies'
alias fm='f --listmodels'
alias fv='f --listvendors'
alias fh='f -h'
alias fc='f --changeDefaultModel'
```

- Ctrl+X
- Y
- Enter

This also creates a `yt` alias that allows you to use `yt https://youtube.com/watch?v=dQw4w9WgXcQ` to get your transcripts.

Test 1: Analyze Paper

Input

```
pbpaste | fabric -p analyze_paper -m
```

Output

```
Based on the research paper, here's my analysis:

SUMMARY:
Small healthcare providers struggle with effective information security management due to resource and expertise constraints, due to lacking IT knowledge and expenditures on IT vendors for security.

AUTHORS:
David Kaiser

AFFIRM DESCRIPTION:
Sample State University

MAIN FINDINGS:
* 19% of participants self-identify as having limited IT and security knowledge.
* 14% have had no security or IT vendors for security support.
* 47% answer security in terms of IT vendor services.
* 14% have had security breaches or incidents.
* 42% are confident in their current security strategies.
* 19% outsource IT operations

STUDY METHODS:
Grounded theory study, interviews, surveys

STUDY FINDINGS:
* Lack of formal security procedures in small facilities interrupted
* Limited IT knowledge constrains security management decision processes
* Good internal organizational analysis and effectively analyze security

STUDY QUALITY:
Strong Methods: Qualitative grounded theory methodology with semi-structured interviews and theoretical sampling

SAMPLE SIZE: 7 participants, representing small healthcare providers in North Dakota

CONFIDENCE INTERVAL: Not applicable for qualitative study

EFFECT SIZE: Not applicable for qualitative study

CONSISTENCY OF RESULTS: Strong consistency in findings across participants

METHODOLOGY TRANSPARENCY: Clear documentation of methods, data collection and analysis approaches

STUDY REPRODUCIBILITY: Detailed protocol provided including interview guides and coding procedures

DATA ANALYSIS METHOD: Grounded theory systematic analysis with constant data collection and analysis

COMPLICATE OF INTEREST: NONE REPORTED

RESEARCHER'S BACKGROUND:
Lack of formal security procedures in small facilities interrupted information security management and access creates a security risk. Small healthcare providers have limited IT knowledge and expenditures on IT vendors for security.

PAPER QUALITY:
Rigorous Methods: Qualitative grounded theory methodology with semi-structured interviews and theoretical sampling

Sample Size: 7 participants, representing small healthcare providers in North Dakota

Consistency of Results: Strong consistency in findings across participants

Methodology Transparency: Clear documentation of methods, data collection and analysis approaches

Study Reproducibility: Detailed protocol provided including interview guides and coding procedures

Data Analysis Method: Grounded theory systematic analysis with constant data collection and analysis

Complicate of Interest: None reported

Overall Assessment: Well-executed qualitative study with clear methodological rigor and transparent reporting. The small sample size is appropriate for qualitative research and the findings are well-supported by the data.

RELEVANCE TO CYBERSECURITY:
Small healthcare providers have dangerous gaps in security due to limited knowledge and vendor dependency. Critical infrastructure protection and patient data security are at risk.

Can be used in your model time to be exposed on any part of this analysis.
```

Test 2: Extract Wisdom

Input

```
pbpaste | yt -p extract_wisdom -m
```

Output

```
# SUMMARY:
Detailed AWS infrastructure how to become a DNS Cybersecurity, Risk, Compliance, Fraud, Identity, Threat Intelligence, Threat Hunting, Vulnerability, and Incident Response.

# IDEAS:
- Cybersecurity spend eating percent of their risk setting. - Automation, detection, prevention, and patching remediation data matters.
- Cybersecurity the professional must be comfortable working in ambiguous situations and executing compelling business scenarios.
- Cybersecurity skill gaps are the primary driver of high compensation for experienced professionals.
- AWS Special Technician DNS skills provide immediate infrastructure visibility and business stakeholder impact.
- Cybersecurity professionals must be comfortable working in ambiguous situations and executing compelling business scenarios.
- Infrastructure security teams and business stakeholders.
- Cybersecurity professionals must be able to translate technical to effectively address business concerns and drive risk reduction.
- Compliance frameworks like CIS and NIST are a starting point but must be customized to actual business risk and threat landscapes.
- Technical knowledge alone is insufficient; success requires understanding threats and recommend appropriate security controls.
- Professional Services roles offer rapid exposure to diverse environments and accelerated skill development.
- Security awareness programs must engage employees to prevent social engineering and phishing attacks.
- Cybersecurity requires continuous learning and adaptation due to evolving threat landscapes.
- Cybersecurity management and networking solutions professional services roles provide high-impact, client-facing experience.
- Documentation and training are critical for maintaining consistent security posture in SMB environments.
- Cybersecurity professionals must balance security with business requirements, ensuring solutions enable rather than hinder business operations.
- Infrastructure security skills form the foundation for advanced cybersecurity roles and provide significant leverage when combined with business acumen.
- Cybersecurity is a critical function for protecting business assets and ensuring compliance.
- Cybersecurity is a rapidly growing field with high demand and lucrative compensation.
- AWS skills spend about 10% of their time writing documentation, which is a key aspect of their role.
- The best time to be a cybersecurity expert was yesterday.
- "Risk assessment is inherently the bread and butter of GRC."
- "Risk is the probability of an undesirable outcome multiplied by the impact."
- "Think of GRC as the interface between the technical cybersecurity world and the business."
- "The important technical knowledge is cybersecurity."
- "Risk is the probability of an undesired outcome multiplied by the impact."
- "Risk assessment is the bread and butter of GRC."

# ASK:
- Continuously stay current with evolving security threats and compliance requirements through regular study.
- Network logically with other GRC professionals through LinkedIn and professional communities.
- Document processes, findings, and recommendations clearly and thoroughly for stakeholder understanding.
- Develop strong communication skills to appropriate technical and business audiences.
- Leverage automation tools to improve efficiency and reduce human error in monitoring activities.
- Implement continuous security assessment rather than effectively conduct organizational risk.
- Build strong relationships with both technical teams and business stakeholders.
- Participate in professional conferences and industry meetups for learning.
- Develop incident response plans and cyber-attack response to stay current.
- Maintain technical knowledge while developing business acumen.

# TIPS:
- GRC A Cybersecurity will be required for all department of the future.
- GRC requires speed specialists; GRC of time is documentation and setting tasks.
- Cybersecurity is a critical function protecting business assets.
- Records are being held personally liable for cyber security breaches.
- The GRC field offers significant continuous learning and is exciting.
- Security awareness training is often ineffective due to boredom.
- Cybersecurity requires continuous learning and adaptation to stay current.
- Technical knowledge complemented by business acumen is crucial for success.
- The cyber security industry faces competencies GRC training shortages.

# REFERENCES:
- Cybersecurity Ventures
- NIST Special Publication 800-37 (Risk Management Framework)
- NIST Special Publication 800-53 (Security and Privacy Controls)
- NIST Special Publication 800-30 (Risk Assessment Guide)
- NIST Special Publication 800-61 (Incident Handling Guide)
- Gartner Research
- Study GRC analysts and cybersecurity
- Professional Blue Ops YouTube channel
- Cybersecurity Ventures Cybersecurity
- Study GRC analysts and cybersecurity
- SANS Institute
- OWASP (Open Project community)
- Jack Rudd's LinkedIn content
- Jack Rudd's YouTube channel
- ISC2 CBK Certification Training
- OTHER Organizations

# ON CONTINUED TRAINING:
- Continuous learning is critical for continuing training, staying accelerated skills, and effective communication between security and business.
- Continuous learning is critical.
- Join Security Blue Ops community by looking with other GRC professionals through LinkedIn and Slack.
- Study NIST Special Publications 800-37 (Risk Management Framework), 800-53 (Security and Privacy Controls), 800-30 (Risk Assessment Guide), 800-61 (Incident Handling Guide).
- Develop strong technical fundamentals while focusing on business acumen for maximum impact.
- Join Security Blue Ops community by looking with other GRC professionals through LinkedIn and Slack.
```

```
real-world scenarios.
- Create engaging security awareness content that effectively
reduces organizational risk.
- Build relationships with both technical teams and business
stakeholders.
- Stay current with evolving regulations through continuous
learning and community involvement.
- Focus on practical experience through hands-on labs and
projects.
- Document processes and findings clearly for different
audience types.
- Network regularly through local meetups and online
communities.
```

Test 3: Get Wow Per Minute

fabric/patterns/get_wow_per_minute/system.md at main · danielmiessler/fabric

You are an expert at determining the wow-factor of content as measured per minute of content, as determined by the steps below.

github.com/danielmiessler/fabric/blob/main/patterns/get_wow_per_minute/system.md

Input

```
yt https://youtu.be/jYwNI5IB__K | fabric -p
get_wow_per_minute -s
```

Output

```
{
  "Summary": "Comprehensive overview of cybersecurity
careers, focusing on entry-level opportunities, salary
ranges, job types, and networking strategies, with emphasis
on addressing the experience catch-22.",
  "Surprise_per_minute": 7,
  "Surprise_per_minute_explanation": "Frequent revelations
about salary ranges, job accessibility, and alternative paths
into cybersecurity provide consistent surprising insights
throughout the presentation.",
  "Novelty_per_minute": 8,
  "Novelty_per_minute_explanation": "Fresh perspectives on
entering cybersecurity, including unconventional paths and
practical strategies for gaining experience, delivered
consistently throughout.",
  "Insight_per_minute": 9,
  "Insight_per_minute_explanation": "Rich with insider
knowledge about industry dynamics, job roles, and practical
advice for breaking into cybersecurity from various
backgrounds.",
  "Value_per_minute": 9,
  "Value_per_minute_explanation": "Extremely high practical
value with actionable advice, salary information, job search
strategies, and specific steps for entering cybersecurity.",
  "Wisdom_per_minute": 8,
  "Wisdom_per_minute_explanation": "Deep industry knowledge
shared through personal experiences and strategic career
advice, particularly valuable for career transitions and
networking.",
  "WPM_score": 8.2,
  "WPM_score_explanation": "Consistently high-value content
combining practical advice, industry insights, and actionable
strategies, making it extremely valuable for cybersecurity
career seekers."
}
```

More Fabric Pattern Demos

Fabric Pattern Demo: create_visualization

Order 2 Cash Control Narrative for an Audit

www.cpatocybersecurity.com/p/data-visualization

Discrete AI Components to Break Down and Solve Challenges

Customize Patterns/Prompts in the Fabric Ecosystem + 5 More Demos

www.cpatocybersecurity.com/p/discrete-ai-components

Why Cybersecurity GRC Professionals Should Get Hands on with AI

6 More Fabric Demos

www.cpatocybersecurity.com/p/learn-ai

Game of Thrones Career Lessons in a Post-AI World

5 More Fabric Demos

www.cpatocybersecurity.com/p/nights-watch-ai

Keep reading

Daily "Go Use It" AI Practice
5 More 1 Minute Fabric Pattern Demos

"Are You Future-Ready?" Analysis of an AI Parody
Analyze_claims Pattern/Prompt Demo

AI Productivity Lab: Five 1 Minute Demos
Concrete Examples to Pour Gasoline on the Flames of Your Curiosity

View more ›

© 2024 CPA to Cybersecurity.