TURTLES ALL THE WAY DOWN

Storing Secrets in the Cloud and in the Data Center
Daniel Somerfield
daniel.somerfield@thoughtworks.com
TURTLES COMPANION SITE

http://danielsomerfield.github.io/turtles
We all have secrets

We want to know they're safe

And...
We need reliable, reproducible deployments
SETTING GOALS
Security Goals

• Secrets are secrets
• Auditing
• No reliance on heroes
• Standard practices
Operational Goals

• Automated
• Scales operationally
It haz 2B EZ 2 uze!!!!
SEARCHING FOR THE ELUSIVE LAST TURTLE
Does this sound familiar?

• Secrets in SCM
• Admins, admins everywhere
• Credential reuse
• Secrets are not really secrets
Goals

• Encrypted secrets
• Controlled distribution
• Secrets are automated
orchestrator decryption

- **encrypted secret**
- **plaintext secret**

- **target application**
  - plaintext secret

- **encrypted store**
  - encrypted secret

**Secure channel**
**Advantages**

– Key management
– Integration

**Disadvantages**

– Exploit severity
– Secrets at rest
– One more turtle…

**Diagram:**

- **Orchestrator Decryption**
- **Advantages:**
  - Key management
  - Integration
- **Disadvantages:**
  - Exploit severity
  - Secrets at rest
  - One more turtle…

- **Target Application** with plaintext secret
- **Orchestration Server** with plaintext secret
- **Encrypted Store** with encrypted secret

- **Secure Channel** connecting the target application to the orchestration server.
APPLICATION DECRYPTION

OWASP
The Open Web Application Security Project

application decryption

orchestration server

encrypted secret

encrypted secret

encrypted secret

encrypted store

plaintext secret

target application
Advantages
– Compartmentalization
– Integration

Disadvantages
– Key management
– Secrets at rest
– One more turtle...

Application Decryption
Operational Compartmentalization

Application deployment
- Artifact repo
- Orchestration server
- Target application

Secret deployment
- Encrypted store
- Orchestration server

Plaintext secret
Advantages

- Clear responsibilities
- Integration

Disadvantages

- Organizational silos
- Lack of transparency
SCM encryption

Orchestration tools

Secret service
Encryption of entire SCM repo or individual items within them.
Strengths

• Integration
• SCM-based audit
SCM ENCRYPTION

OWASP
The Open Web Application Security Project

Weaknesses

- Secret rotation support
- Data at rest
- Auditing of usage
- More turtles...
SCM Encryption Tools

- Blackbox
- GitCrypt
- Transcrypt
Strengths

• Automation
• Familiar workflow
Weaknesses

• Similar to SCM encryption, plus:
• Vendor lock-in
• Another turtle…
ORCHESTRATION ENCRYPTION TOOLS

- Chef
- Vault
- Ansible
- Vault
- Blackbox
- hiera-eyaml
SCM encryption

Orchestration tools

Secret service
Goals

- Key Rotation
- Limit secrets at rest
Application-pull

- Target application
  - Plaintext secret

- Secret server
  - Encrypted secret
  - Plaintext secret
  - Encrypted store

Secure channel
A separate endpoint providing secrets on demand over a secure channel.
Strengths

• Minimizes at rest
• Facilitates rotation
• Compartmentalization
• Ephemeral credentials
• Access policies
• Auditing
Weaknesses

• Adoption
• Single point of failure
• Few options
• One more turtle…
SECRETS AS A SERVICE

HashiCorp Vault

Square KeyWhiz
SCM encryption

Orchestration tools

Secret service
Goals

• Ephemeral credentials
• Instances without remote access
• Immutable infrastructure
• Credential-less architecture
Orchestration tools

Secret service

???
FINAL THOUGHTS
1. publishes artifact
2. push orchestration package
3. download app package
4. download secret
5. decrypt secret
6. start application
7. delete secret
So how do you find the last turtle?

- Tactical human intervention
- Audit
- Evolve
Daniel Somerfield
daniel.somerfield@thoughtworks.com
http://danielsomerfield.github.io/turtles