Fast Forward

Reflecting on a Life of Watching Movies and a Career in Security

Jason Chan
VP, Information Security @ Netflix
@chanjbs
Netflix Subscribers Streamed Record-Breaking 350 Million Hours of Video on Jan. 7
So ... what does this have to do with security?
TRADITIONAL APPLICATION SECURITY
WE HARDLY KNEW YOU...
Back to the movies . . .
square
/skwər/  
noun

1. a plane figure with four equal straight sides and four right angles.
Simplifying the Security Interface for Developers
Are you trying to make your engineers security experts? Or do you just want them to build and operate secure systems?
What security functions can we abstract to simplify the developer experience?
Netflix Studio Engineering
Bojack Horseman
Netflix Studio Engineering

Optimize production from “pitch to play”
Lots of innovation and iteration
Netflix Studio Apps

Netflix Studio User

Studio LOB App A

Studio LOB App N
Simplify and Improve Security through Functionality Abstraction
Leverage Netflix OSS - Zuul

“built to enable dynamic routing, monitoring, resiliency and security”

https://github.com/Netflix/zuul/wiki
Netflix Studio Apps with Zuul and Wall-E

Pre-Filters
- Rate Limit
- IP Blacklist
- Authentication
- Authorization
- SigSci WAF
- Schema Check

Post-Filters
- Schema Check
- Sec Headers
- DLP

Wall-E

Netflix Studio User

Studio LOB App A

Studio LOB App N
Results

Lower cognitive load for onboarding security
Centralized and managed functionality

Frees developers to build the Netflix Studio!
Blurring Lines: App and Infra

Monolith to microservices: network
Immutable infra: OS, custom app, middleware
Infra as code: Everything!
Tackling App and Infra Integration: Seamless Least Privilege
The Magic of IaaS
Ex: Cloud Based Word Processor
Ex: Cloud Based Word Processor

```json
{
  "Effect": "Allow",
  "Action": ["*:*:*"],
  "Resource": "*
}
```
Ex: Cloud Based Word Processor

{
    "Effect": "Allow",
    "Action": ["s3:*"],
    "Resource": "*
}

Ex: Cloud Based Word Processor

{
  "Effect": "Allow",
  "Action": ["s3:GetObject", "s3:PutObject"],
  "Resource": "*"
}
Ex: Cloud Based Word Processor

{
  "Effect": "Allow",
  "Action": ["s3:GetObject", "s3:PutObject"]
  "Resource": "arn:aws:s3:::wp_bucket"
}

AWS provides data about API use

This data acts as a basis for action
When a new application is created, we provide a base set of permissions:

- s3:GetObject
- s3:PutObject
- ...
- ...
- ...
- ...
- sqs:ReceiveMessage
We observe the application to see which permissions are actually used
We then remove unused permissions

s3:GetObject
s3:PutObject
...
...
...
...
sqs:ReceiveMessage
We then remove unused permissions

s3:GetObject
s3:PutObject
sqs:ReceiveMessage
Available as OSS - Repokid

https://github.com/Netflix/repokid
Results

Low-risk access reduction
Transparent and versioned ops ops
Innovation and high-velocity development without friction
Potential for “Controlled” Anarchy

Microservices
YBIYRI
Polyglot and multiple tech stacks
Independent deployments

Intentionally decentralized governance leads to increased attack surface
Managing the Anarchy
The Security Paved Road

- Well-supported solutions from central teams
- Clarifies and evangelizes successful patterns and practices
- Automated observation and evaluation of adoption
- Provides a standard way of interfacing with engineering teams about security
- **Uncover risk and reward operational excellence**
Security Paved Road (ex.)

Example Solutions & Measures

Per-app IAM role
Per-app Security Group
No secrets in code
Instance identity
Updated machine image
Security Paved Road

**Quarterly Change Cycle**

Commit to update once per quarter to pull in upgrades, library changes, and modifications to paved road components.
Deprecations and Blacklists

* Deprecation:
  - `gandalf-agent <=0.16.0`
  - Started on April 10, 2018
  - By Platform Security
  - Contact: platformsecurity@netflix.com

* Chart:
  - Title: Server Group Usage History
  - Description: Apr 13 at 6:00 pm: 67 server groups
Security Paved Road

Security Brain

Make our expectations, asks, and recommendations explicit and easy to navigate
Most security backlog is standard; explicitly limit bespoke/custom backlog
In closing . . .
Overall Takeaways

Stay attuned to trends
Simplify and standardize
Favor transparent decisions
Measure adoption and uptake
Get comfortable with tradeoffs
Thank you!
@chanjbs