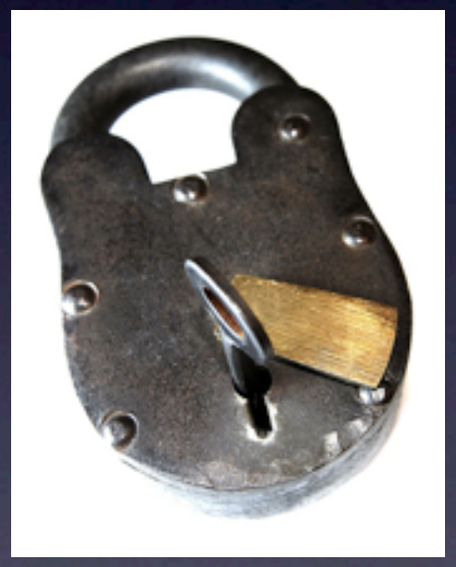
Cooking Security

Joshua Timberman
Senior Solutions Engineer
Opscode, Inc.

http://www.flickr.com/photos/26326001@N08/3530351328/

http://www.flickr.com/photos/williamhook/3201183945/



http://www.flickr.com/photos/amagill/235453953/

Who Am I?

- Network, System and Security Operations
- System Administration == Development
- Solving automation problems with code

Who is Opscode?

- Seattle based startup
- Former IT automation consultancy
- Infrastructure Automation for the Masses™

OPSCODE

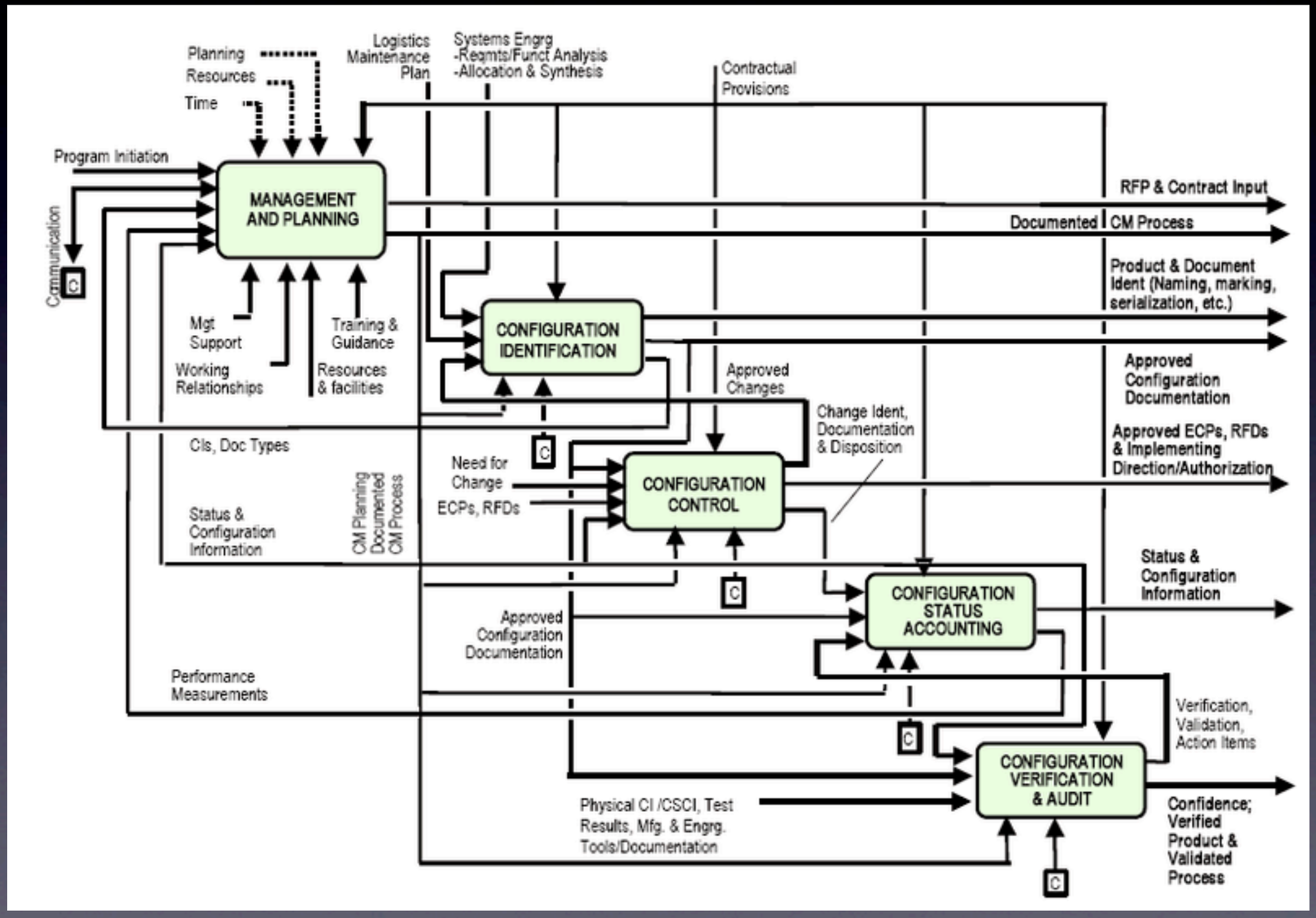
Is this a sales pitch?

http://www.flickr.com/photos/peterkaminski/11843486/

Configuration Management?

"... Is a field of management that focuses on establishing and maintaining consistency of a system's or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life. For information assurance, [it] can be defined as the management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an information system." - en.wikipedia.org

Maybe a Picture...?



Understand the Goals

- System, infrastructure automation
- Consistent, known state
- Self-documenting

http://www.flickr.com/photos/wwworks/2473052504/in/set-72157608035966422/

http://www.flickr.com/photos/loozrboy/3207812715/

Benefits

- Economics
- Efficiency
- Scalability
- Security

Security

- Security Policy Compliance
- Defense In Depth
- Auditing & Documentation

http://www.flickr.com/photos/anonymouscollective/2291896028/

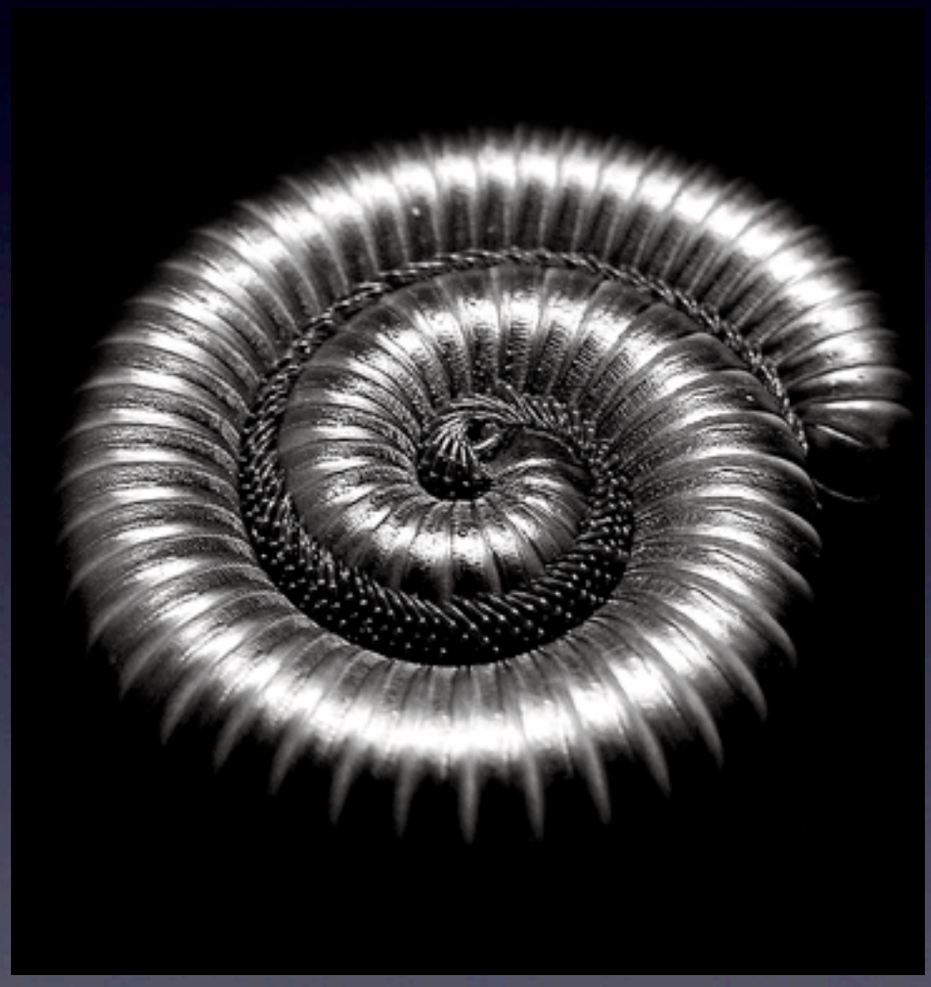
Policy Compliance

- Not a Silver Bullet
- System configuration
- Best practice(s) applied

http://www.flickr.com/photos/gi/168406150/

Defense In Depth

- Configuration layers
- Access control
- Incident handling



http://www.flickr.com/photos/furryscalyman/2081849769/

Auditing and Documentation

http://www.flickr.com/photos/hryckowian/2176673733/

- Declarative tools
- Version control
- Logging subsystems

Chef

- System tool
- Ruby library
- REST API

How Chef Helps

- Idempotent
- Flexible
- Scalable
- Community
- Clean configuration language

Idempotent

http://www.flickr.com/photos/redjar/360111326/

"Multiple applications of an operation do not change the result" - en.wikipedia.org

- Consistency
- Known state
- Easy to build

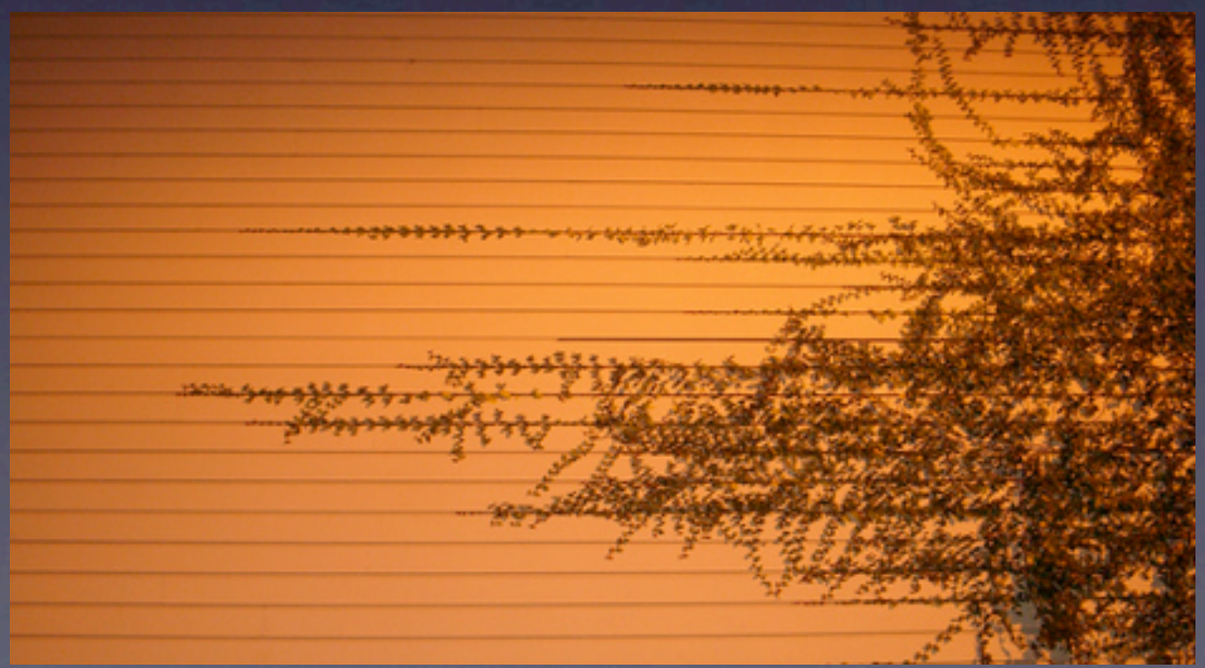
Flexible

- TIMTOWTDI
- Standalone or client / server
- Few assumptions

http://www.flickr.com/photos/66164549@N00/1920513385/

Scalable

- Horizontal scaling
- Lightweight server
- Clients do the work



Community

- Chef is open source
- Operations experts
- Best practices

Clean Language

- Configuration language is Ruby
- Ruby is easy to understand
- Chef is easier to understand!

Example Recipe

```
1  package "apache2" do
2    action :install
3  end
4
5  service "apache2" do
6    action [:enable, :start]
7  end
8
9  template "/etc/apache2/apache2.conf" do
10   source "apache2.conf.erb"
11   owner "root"
12   group "root"
13   mode 0644
14   notifies :restart, resources(:service => "apache2")
15 end
```

Moving Parts

- Clients
- Resources
- Providers
- Cookbooks
- Search indexes

How Does Chef Work?

- Authenticate
- Build node
- Synchronize cookbooks
- Converge

Configuring Systems

```
package "tar" do
  version "1.16.1-1"
  action :install
end
```

```
service "some_service" do
  supports :status => true, :restart => true, :reload => true
  action [ :enable, :start ]
end
```

```
file "/etc/specific_perms" do
  owner "root"
  group "root"
  mode
  actic
end
```

```
bash "install_something" do
user "root"
  cwd "/tmp"
                                    .gz
                                    ake install)
  EOH
end
```

Over 20 resource types

```
file "/etc/unwanted_file" do
  action :delete
end
```

```
template "/etc/some_service.conf" do
  source "some_service.conf.erb"
end
```

```
execute "slapadd" do
  command "slapadd < /tmp/this_org.ldif"
  creates "/var/lib/slapd/uid.bdb"
  action :run
end
```

```
remote_file "/tmp/testfile" do
  source "http://www.example.com/testfile"
  mode "0644"
end
```

```
route "10.0.0.0" do
  gateway "10.0.0.1"
  netmask "255.255.255.0"
end
```

Workflow

- Define policy
- Install Chef
- Get a local configuration started
- Deploy the configuration for testing
- Deploy the configuration to production

Questions?

joshua@opscode.com

Twitter: @jtimberman, #opschef

IRC: irc.freenode.net #chef

http://www.flickr.com/photos/38299630@N05/3635356091/

http://wiki.opscode.com/display/chef/Home