Do you trust that certificate?

@zundan

@zundan

heroku

@zundan

Important!

Introduction to modern cryptography

www.hyuki.com/cr/

Transport Layer Security

Secure Socket Layer

TLS/SSL

https://

A web application

Receives requests

Calls external resources

That handles secret information

How does app trust them?

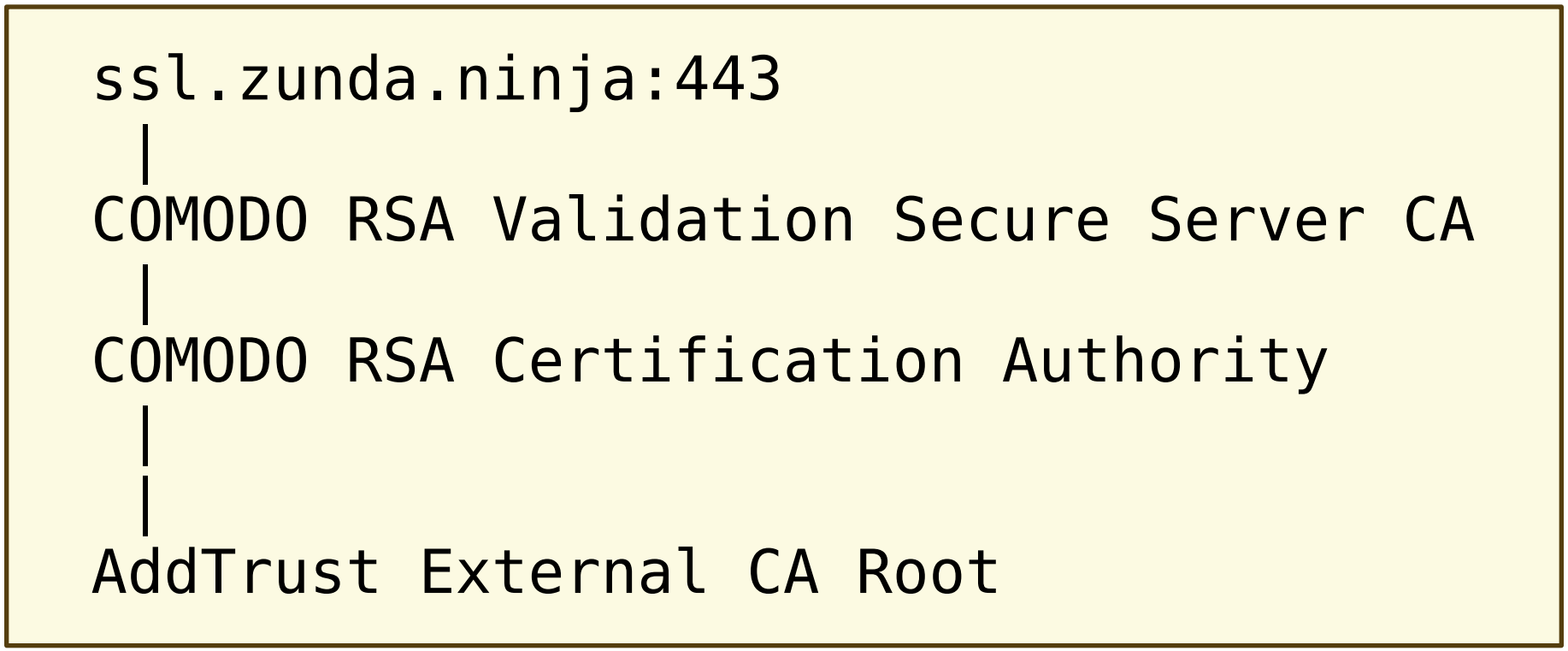
PKI

Public-key
nfrastructur

Server certificate

Signed by Certificate Authority

Certificate chain



One day

Error

Error

SSL_connect returned=1 errno=0 state=SSLv3 read server certificate B: certificate verify

I did not change anything!

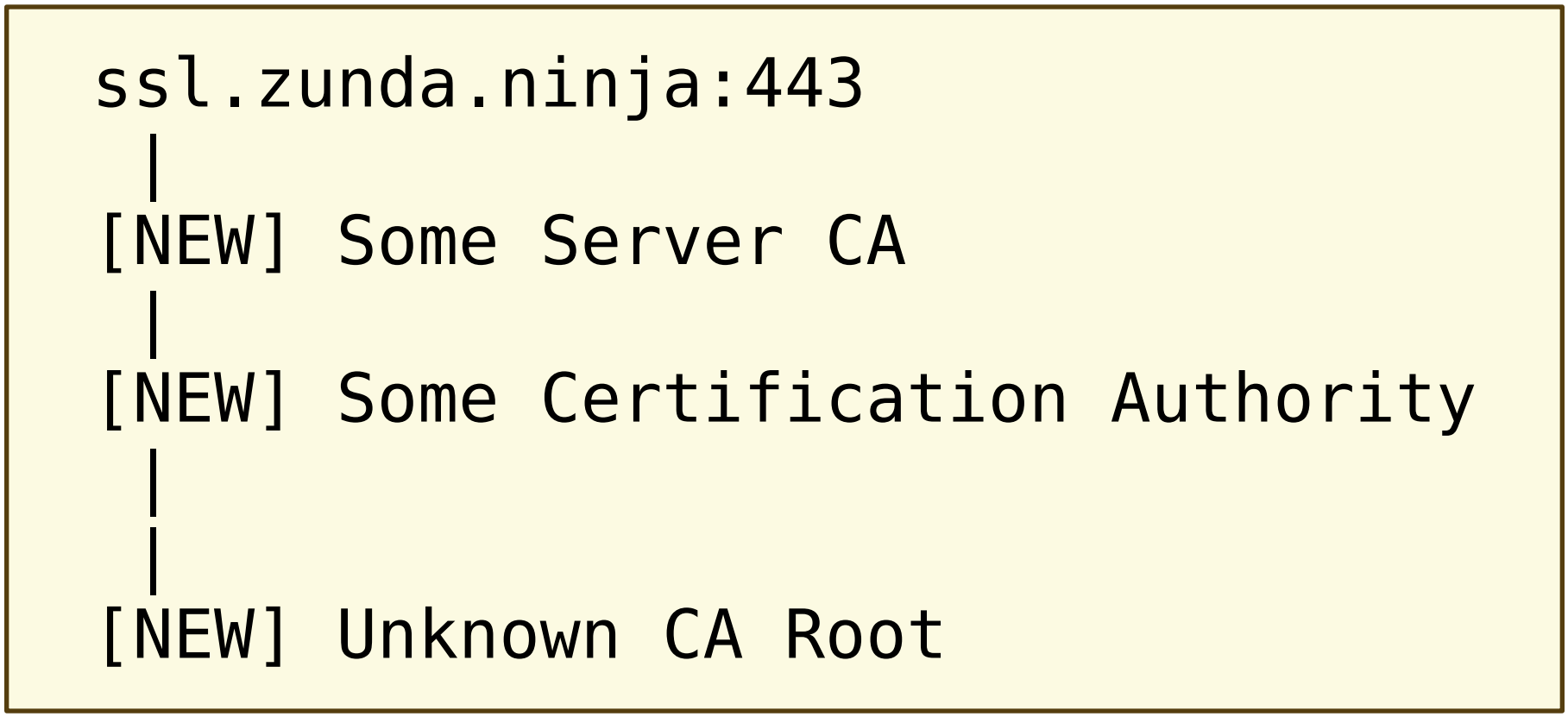
but

Something outside has changed

Error

SSL_connect returned=1 errno=0 state=SSLv3 read server certificate B: certificate verify

Certificate chain



2014-09 1024 bit hash

2015-09
SHA-1

Replace with new certs

On new CA certs

That app does not know

Certificate chain

Error

SSL_connect returned=1 errno=0 state=SSLv3 read server certificate B: certificate verify

So ...

$ bundle update

well ...

Include new CA cert in app

Monkey patch to use it

Net::HTTP

```
module Net
  class HTTP
    alias_method :original_use_ssl=, :use_ssl=

    def use_ssl=(flag)
      self.ca_file     = File.dirname(__FILE__) + \
        '/../../certs/cacert.pem'
      self.verify_mode = OpenSSL::SSL::VERIFY_PEER
      self.original_use_ssl = flag
    end
  end
end
```

ActiveMerchant

```
module ActiveMerchant
  class Connection
    def configure_ssl(http)
      return unless endpoint.scheme == "https"
      http.use_ssl = true
      if verify_peer
        http.verify_mode = OpenSSL::SSL::VERIFY_PEER
        http.ca_file     = File.dirname(__FILE__) + \
          '/../../certs/cacert.pem'
      else
        http.verify_mode = OpenSSL::SSL::VERIFY_NONE
      end
    end
  end
end
```

System's CA certs

Where are they?

System's certs

```
$ openssl version -d
OPENSSLDIR: "/usr/lib/ssl"

$ ls /usr/lib/ssl
certs@  misc/  openssl.cnf@  private@

$ ls -l /usr/lib/ssl/certs
... /usr/lib/ssl/certs -> /etc/ssl/certs/
```

openssl/ssl.rb

If the verify_mode is not VERIFY_NONE and ca_file, ca_path and cert_store are not set then the system default certificate store is used.

openssl/ssl.rb

```ruby
module OpenSSL
  module SSL
    class SSLContext
      def set_params(params={})
        # snip
        if self.verify_mode != OpenSSL::SSL::VERIFY_NONE
          unless self.ca_file or self.ca_path or self.cert_store
            self.cert_store = OpenSSL::X509::Store.new
          end
        end
        return params
      end
    end
  end
end
```

System's certs

```
module ActiveMerchant
  class Connection
    def configure_ssl(http)
      return unless endpoint.scheme == "https"
      http.use_ssl = true
      if verify_peer
        http.verify_mode = OpenSSL::SSL::VERIFY_PEER
        http.ca_path = nil
        http.ca_file = nil
      else
        http.verify_mode = OpenSSL::SSL::VERIFY_NONE
      end
    end
  end
end
```

Anyway

Remember what we trust

What are coming?

2016-06-01

Symantec certs on Google products?

Will there be updates?

On Ubuntu

:

2013-01-19

2013-06-10

2013-09-06

2014-03-25

2014-10-19

2015-04-26

launchpad - ca-certificates

On ActiveMerchant

2007-03-03

2011-09-15

2015-01-16

activemerchant - active_merchant

Remember and be prepared!

Once more

www.hyuki.com/cr/

CRL

Certificate Revocation List

How are we updating this?

SSL and TLS1.0 will be disabled

PCI Compliance

Payment Card Industry

Remember what we trust

URLs

暗号技術入門

Phasing out Certificates with 1024-bit RSA Keys

SHA-1

AWS to Switch to SHA256 Hash Algorithm for SSL Certificates

Sustaining Digital Certificate

CC BY-ND 4.0

Presented as a lightning talk in RubyKaigi 2015 on 2015-12-12