SSL Sucks

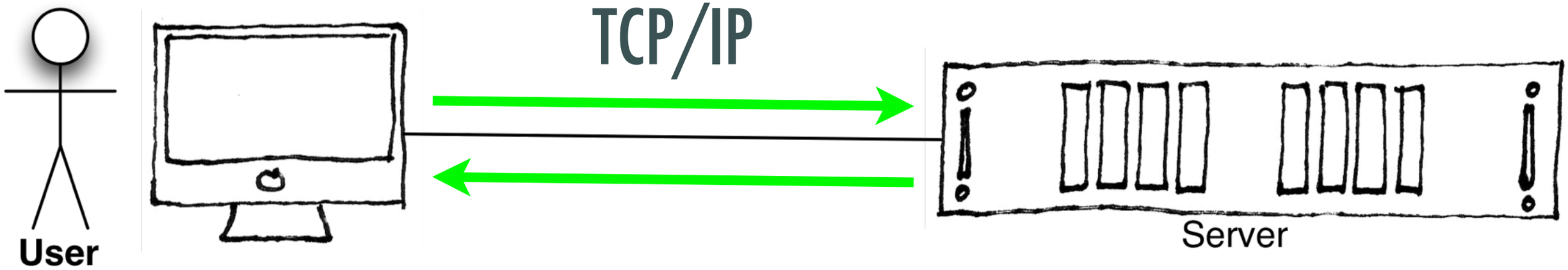
Man In The Middle Attacks

Scott Gustafson
@scottg0
scott@garlicsoftware.com

Background

- Networking
- Encryption
  - Symmetric Encryption
  - Public Key (Asymmetric) Encryption
- How does SSL work?

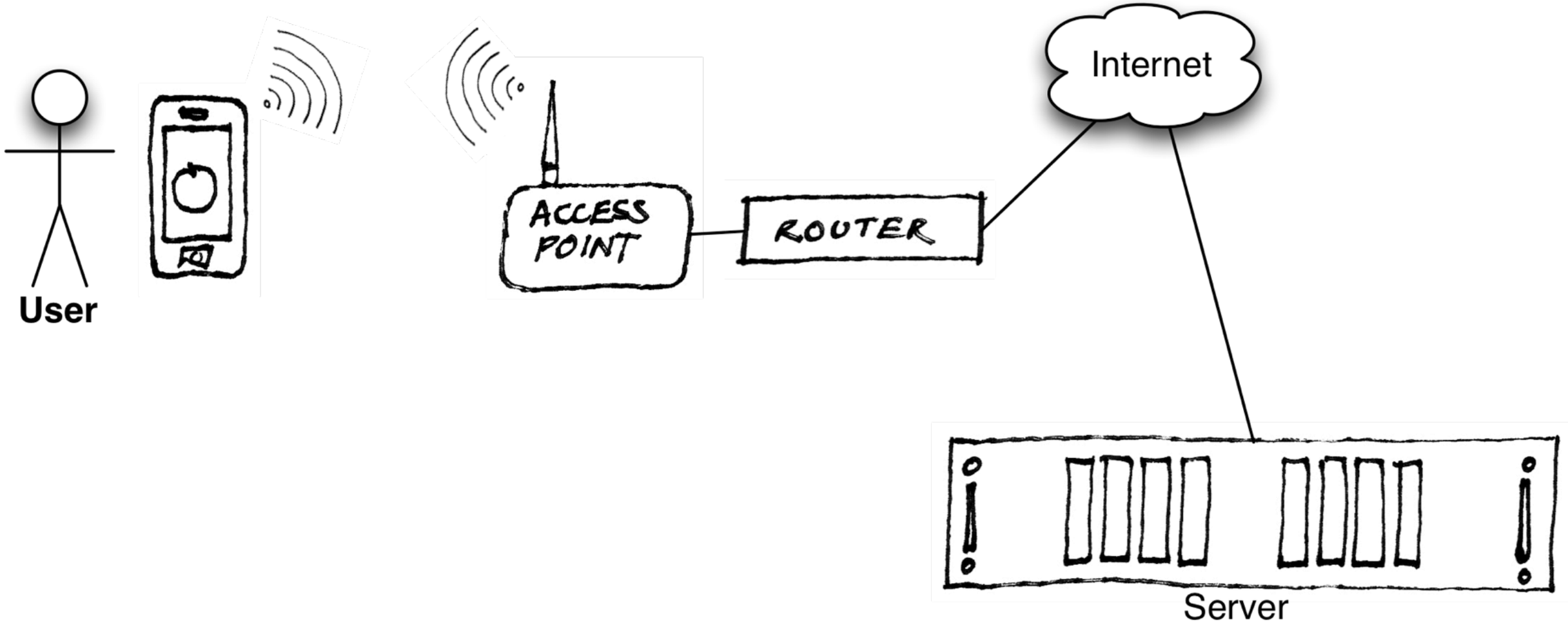
Networking



More Complicated

- Wired vs. Wireless networks
- Routers
- DNS resolvers
- Load Balancers
- Firewalls

Somewhat Modern



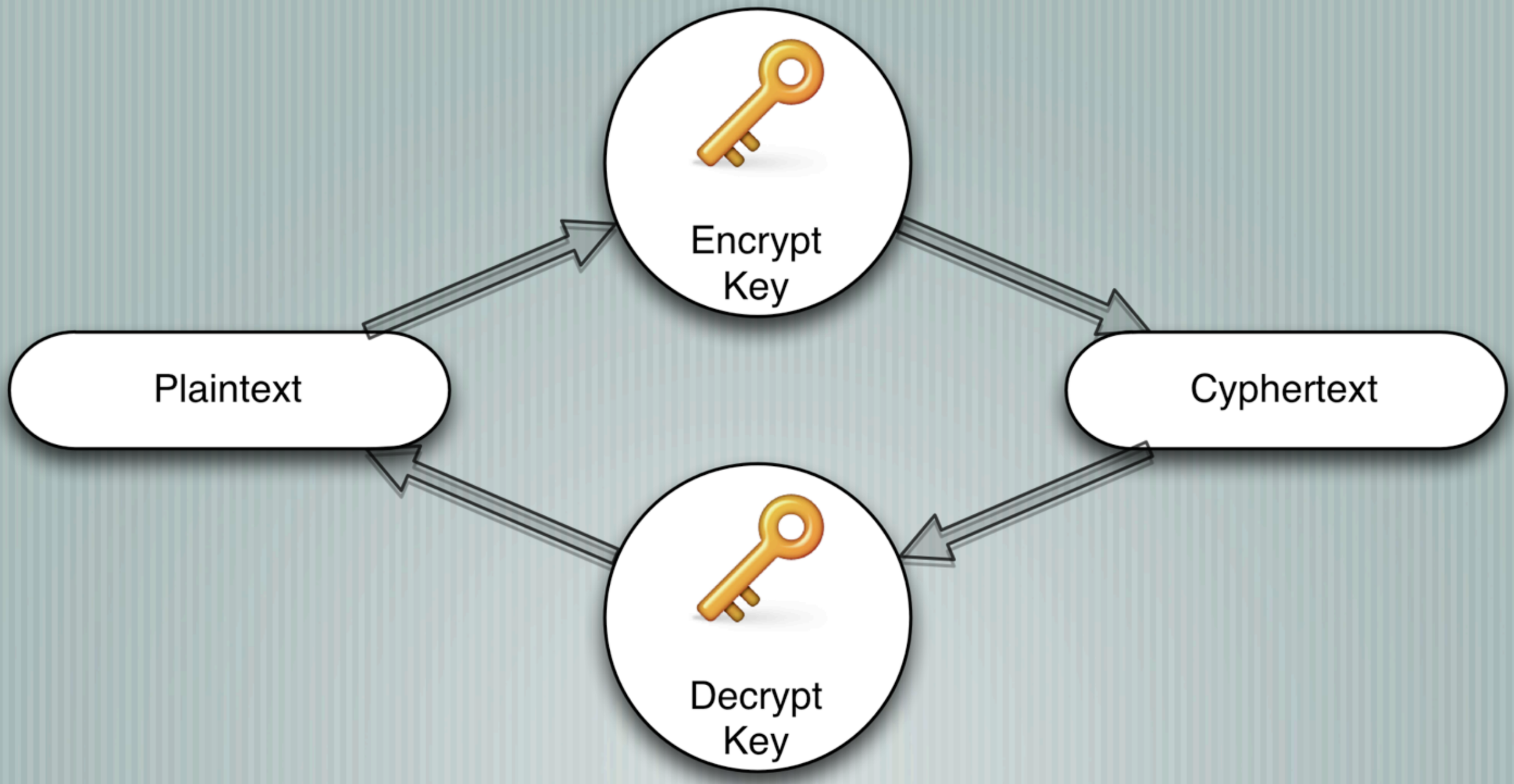
Encryption

- Converting plain text into cypher text using an algorithm
- Example: Substitution Cypher (A becomes Z)

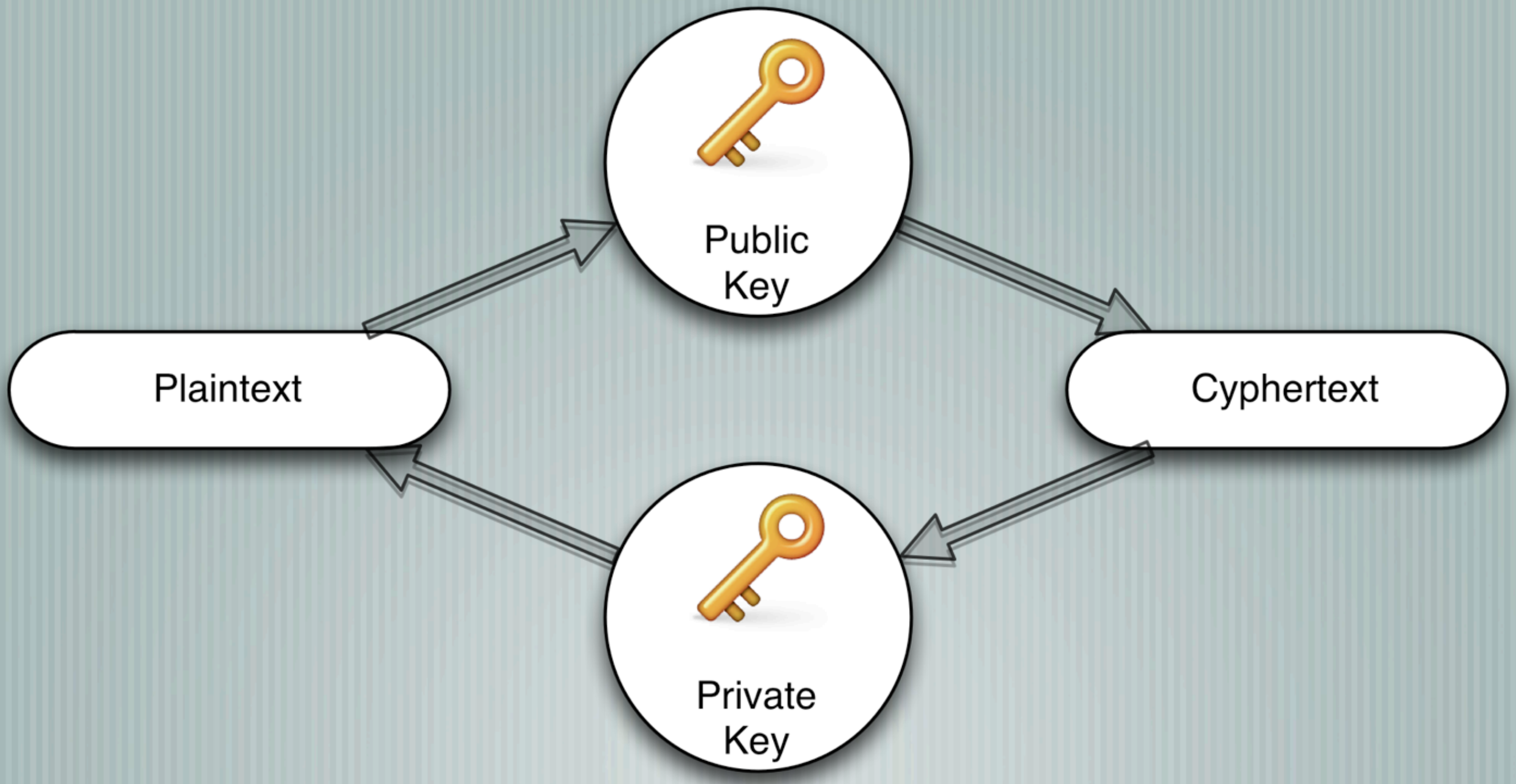
Symmetric Encryption

- Same key to encrypt and decrypt

Asymmetric Encryption



Public Key Encryption



SSL Encryption

- Uses both Public Key and Symmetric encryption
  - RSA (public/private keys)
  - Diffie-Hellman (Key Exchange)
  - AES (block cypher)
  - Lots of other algorithm options

SSL Intro

- Secure Sockets Layer (SSL) (version 2.0 1995)
  - Originally developed by Netscape
  - Last version 3.0 (1996)
- Transport Layer Security (TLS) (1999)
  - Latest version 1.2 (2008)
  - Version 1.3 is still in draft form (2014)

SSL Common Use

- Websites (HTTPS)
- Email (SMTP)
  - Just recently email providers are beginning to encrypt the transport of email between servers.

SSL Steps

- Client contacts Server
- Server responds with Certificate containing Public Key
- Client and Server exchange a Secret Key using the Servers Public and Private Keys
- Client and Server use Secret Key for rest of encryption

SSL Certificates

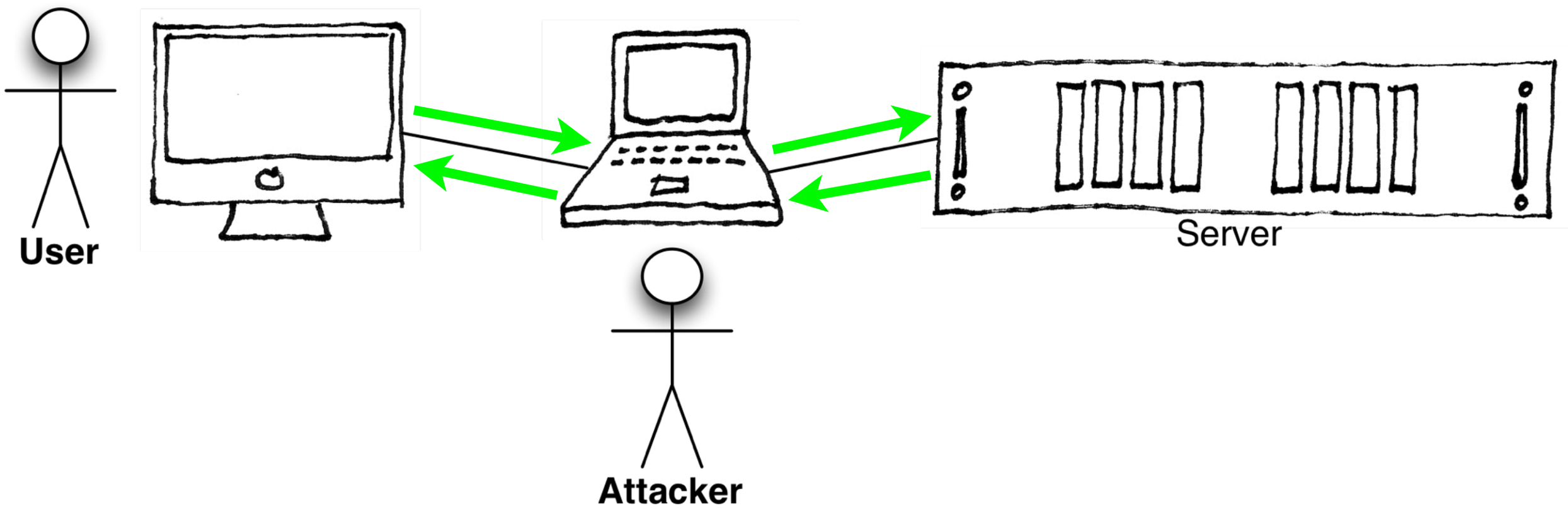
- This contains your servers Public Key for encryption
- Issued by a Certificate Authority

SSL Certificates

- Download a SSL certificate
  - echo -n | openssl s_client -connect www.garlicsoftware.com:443 | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > ./garlicsoftware.pem
- openssl x509 -in garlicsoftware.pem -text -noout

Attacks

Man In The Middle



Simple Sever App

- Responds with either Secure or Insecure Connection depending on connection type: http or https.
- Send POST headers with prefix X_CUSTOM and they are echoed back.
- **http**://www.garlicsoftware.com/scott/responder.cgi
- **https**://www.garlicsoftware.com/scott/responder.cgi

PAW Demo

```
<body>
<h1>Unsecure Connection</h1>
<h2>Data headers sent</h2>
<p>HTTP_X_CUSTOM_ME: Scott</p>
```

Server Output http

```
<body>
<h1>Secure Connection</h1>
<h2>Data headers sent</h2>
<p>HTTP_X_CUSTOM_ME: Scott</p>
```

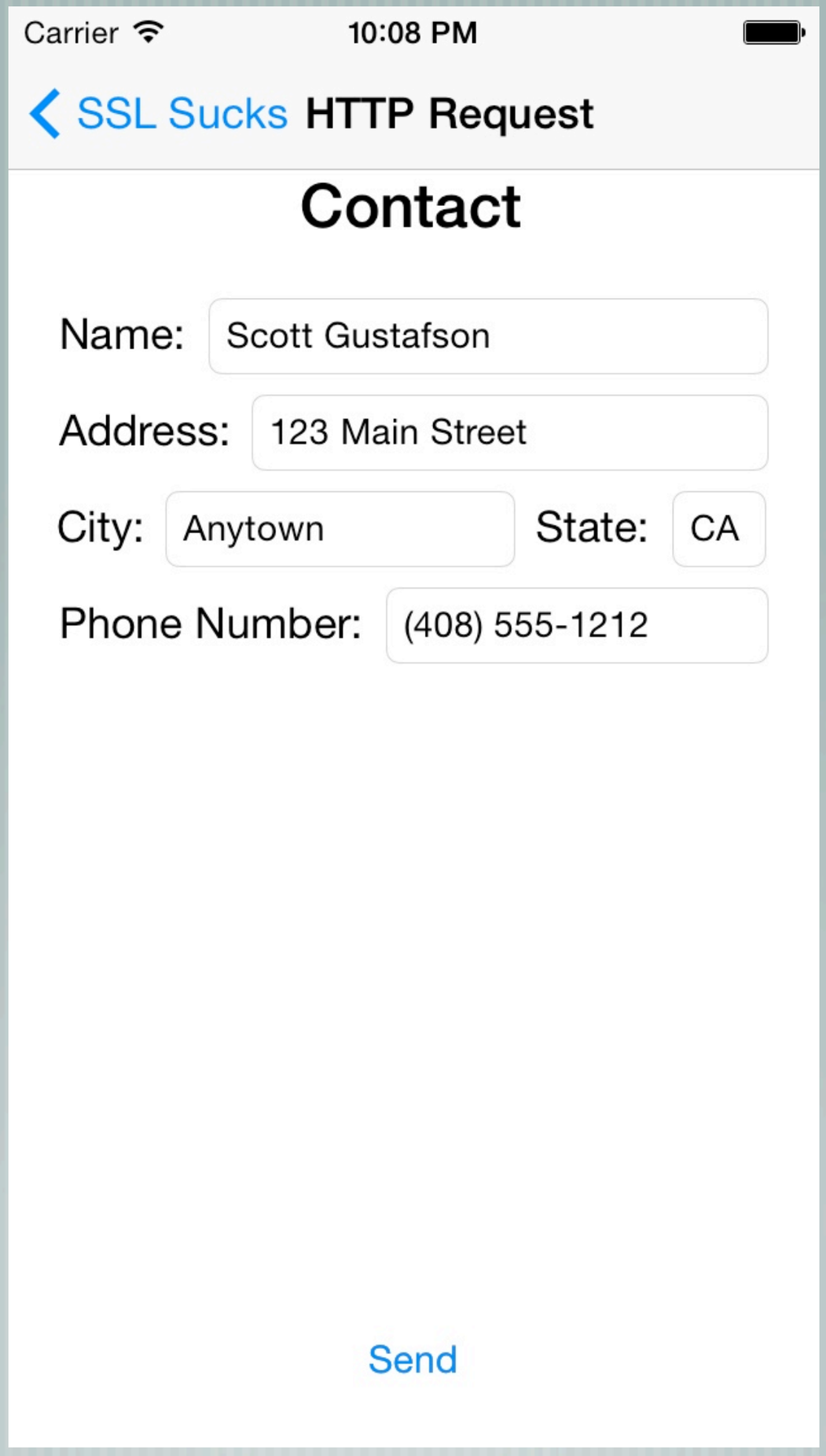
Server Output https

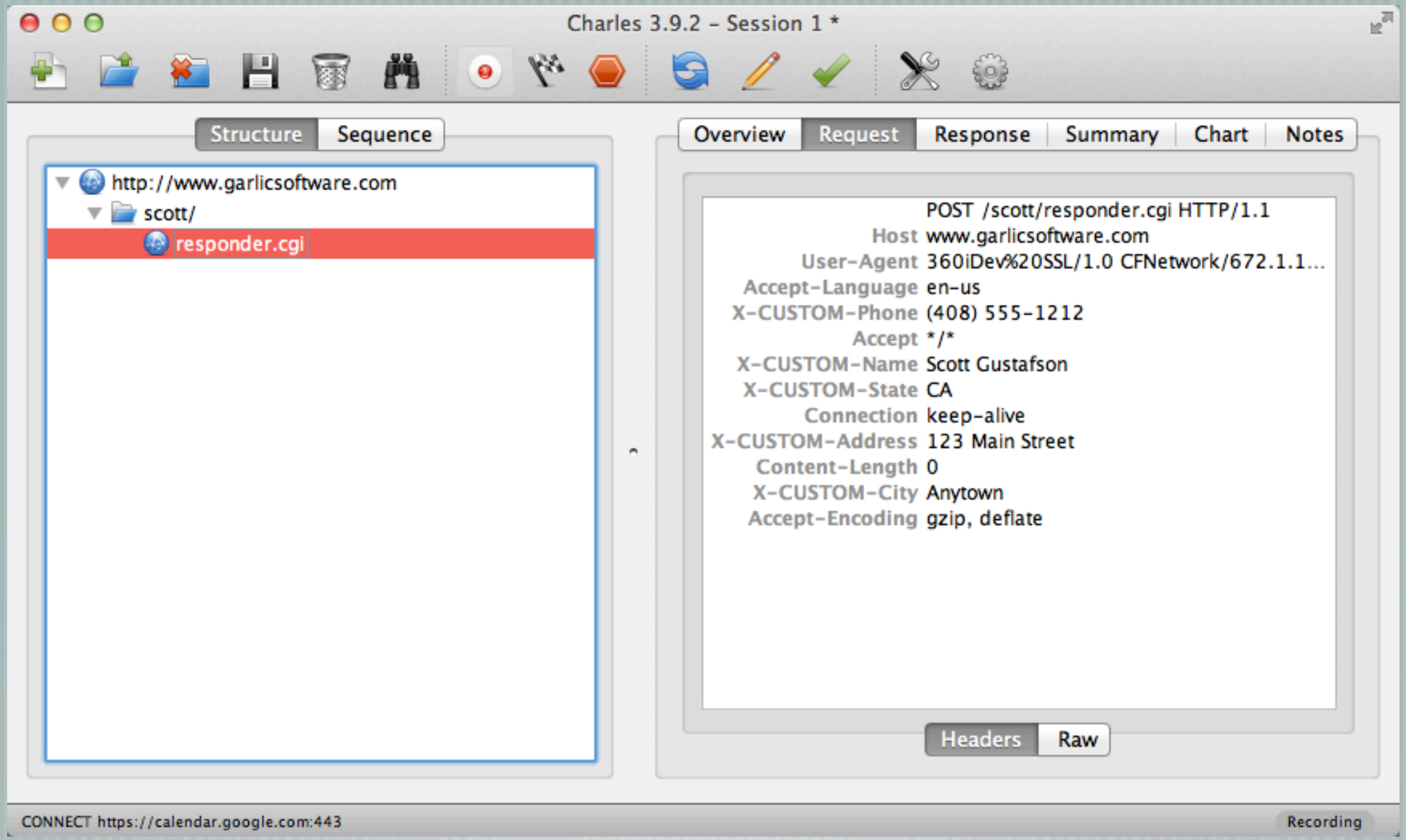
iOS Networking http

```
NSMutableURLRequest *request = [NSMutableURLRequest
requestWithURL:[NSURL URLWithString:@"http://
www.garlicsoftware.com/scott/responder.cgi"]];
```

```
NSData *data = [NSURLConnection
sendSynchronousRequest:request
returningResponse:&response error:&error];
```

iOS Demo http

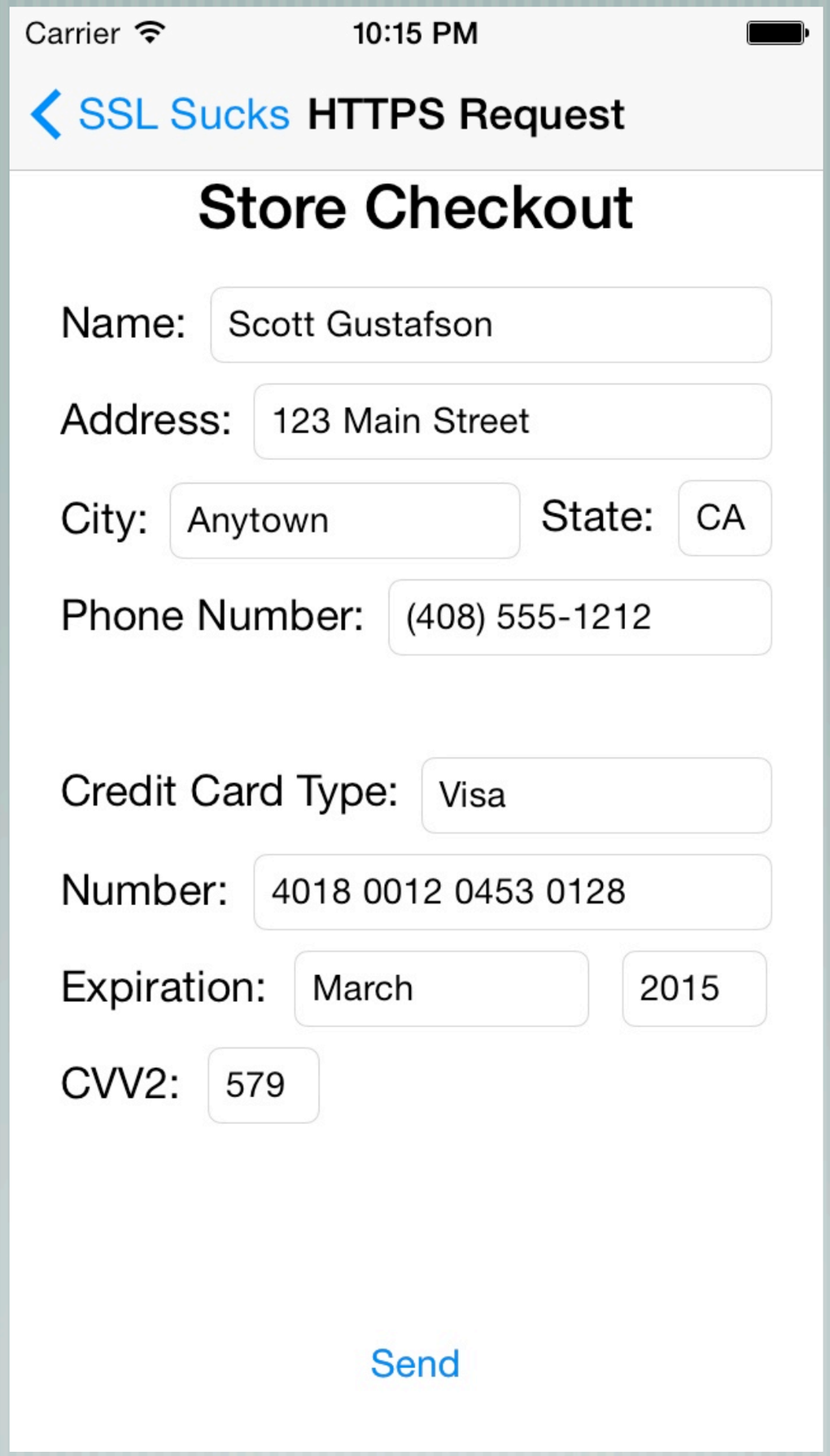

Carrier
10:08 PM
SSL Sucks
HTTP Request
Contact
Name:
Scott Gustafson
Address:
123 Main Street
City:
Anytown
State:
CA
Phone Number:
(408) 555-1212
Send

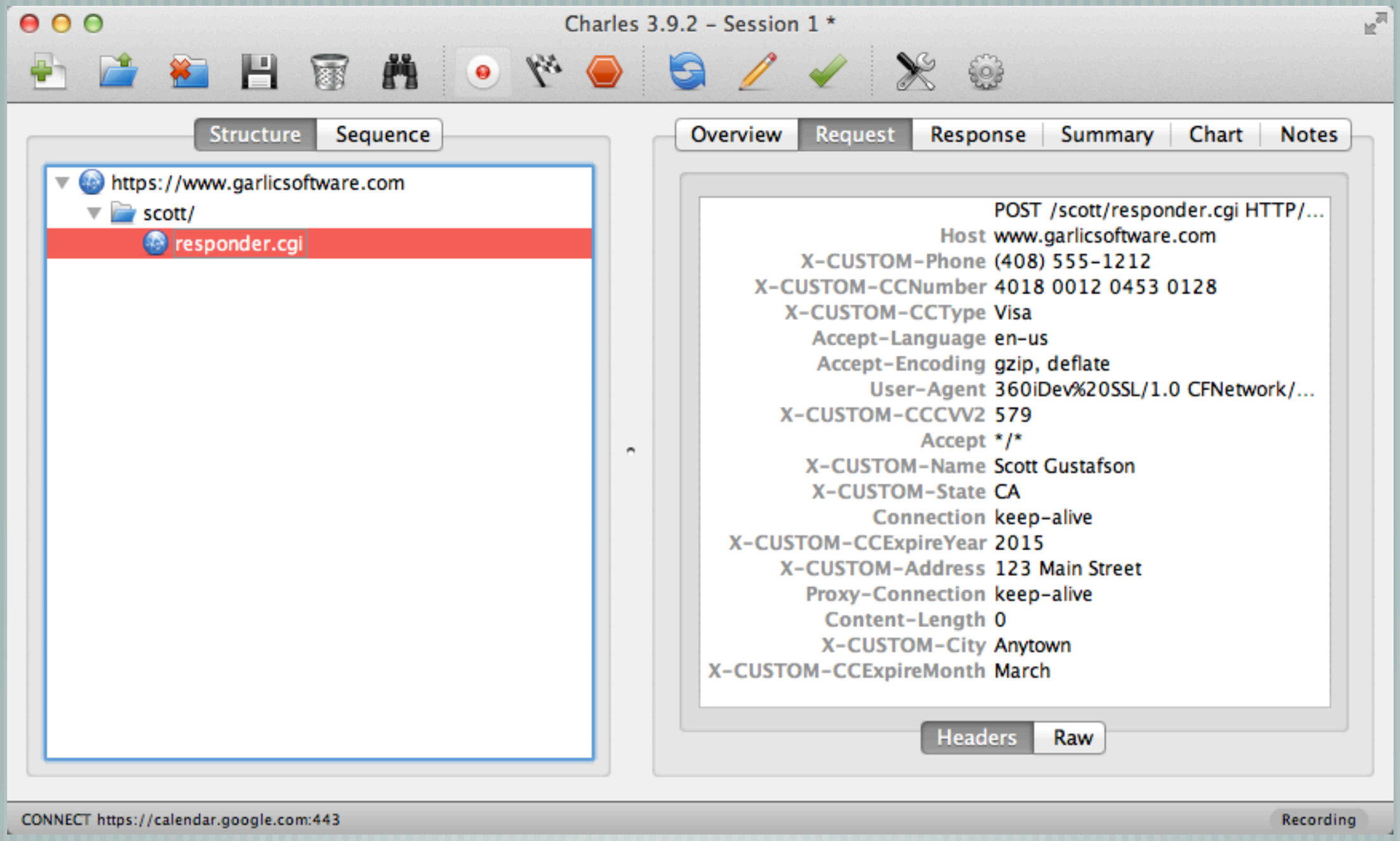

Charles 3.9.2 - Session 1 *
Structure
Sequence
http://www.garlicsoftware.com
scott/
responder.cgi
Overview
Request
Response
Summary
Chart
Notes
POST /scott/responder.cgi HTTP/1.1
Host www.garlicsoftware.com
User-Agent 360iDev%20SSL/1.0 CFNetwork/672.1.1...
Accept-Language en-us
X-CUSTOM-Phone (408) 555-1212
Accept */*
X-CUSTOM-Name Scott Gustafson
X-CUSTOM-State CA
Connection keep-alive
X-CUSTOM-Address 123 Main Street
Content-Length 0
X-CUSTOM-City Anytown
Accept-Encoding gzip, deflate
Headers
Raw
CONNECT https://calendar.google.com:443
Recording

iOS Networking https

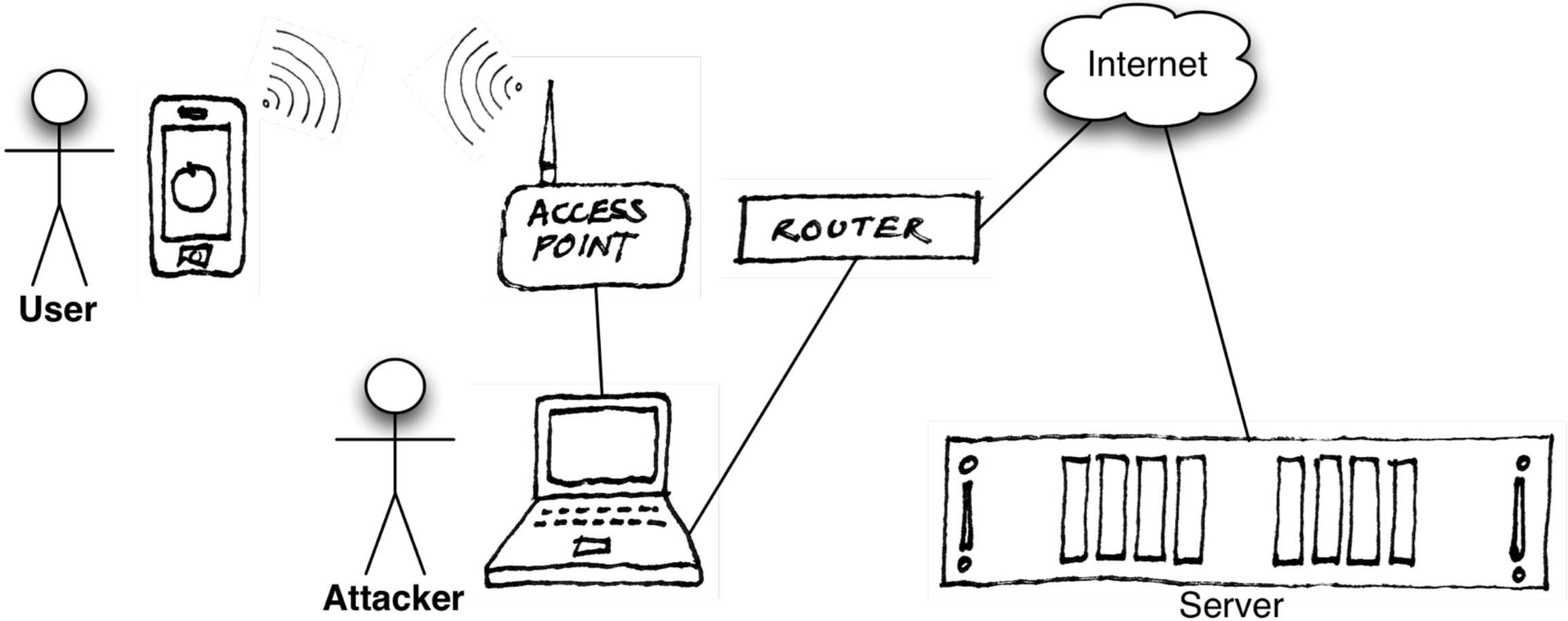
- NSMutableURLRequest *request = [NSMutableURLRequest requestWithURL:[NSURL URLWithString:@"**https**://www.garlicsoftware.com/scott/responder.cgi"]];
- [NSURLConnection connectionWithRequest:request delegate:self];

iOS Demo https


Carrier
10:15 PM
SSL Sucks
HTTPS Request
Store Checkout
Name:
Scott Gustafson
Address:
123 Main Street
City:
Anytown
State:
CA
Phone Number:
(408) 555-1212
Credit Card Type:
Visa
Number:
4018 0012 0453 0128
Expiration:
March
2015
CVV2:
579
Send


Charles 3.9.2 - Session 1 *
Structure
Sequence
https://www.garlicsoftware.com
scott/
responder.cgi
Overview
Request
Response
Summary
Chart
Notes
POST /scott/responder.cgi HTTP/...
Host www.garlicsoftware.com
X-CUSTOM-Phone (408) 555-1212
X-CUSTOM-CCNumber 4018 0012 0453 0128
X-CUSTOM-CCType Visa
Accept-Language en-us
Accept-Encoding gzip, deflate
User-Agent 360iDev%20SSL/1.0 CFNetwork/...
X-CUSTOM-CCCVV2 579
Accept */*
X-CUSTOM-Name Scott Gustafson
X-CUSTOM-State CA
Connection keep-alive
X-CUSTOM-CCExpireYear 2015
X-CUSTOM-Address 123 Main Street
Proxy-Connection keep-alive
Content-Length 0
X-CUSTOM-City Anytown
X-CUSTOM-CCExpireMonth March
Headers
Raw
CONNECT https://calendar.google.com:443
Recording

Modern Network Attack



Defenses

- Certificate Pinning
  - Components (i.e. public key or hash)
  - Full certificate (what we will use)
- DNSSEC

Certificate Pinning

- Compare the SSL certificate received from the server in the connection attempt to the one stored in the application.
- openssl x509 -in garlicsoftware.pem -C -noout
- -connection:canAuthenticateAgainstProtectionSpace:
- -connection:didReceiveAuthenticationChallenge:

iOS Demo Secure

Carrier 8:19 PM

SSL Sucks **Secure Request**

New Brokerage Account

Name: Scott Gustafson

Address: 123 Main Street

City: Anytown State: CA

Phone Number: (408) 555-1212

SSN: 987-65-4321

Birth Date: 01/23/1945

Mother's Maiden Name: Jones

Send

Carrier 8:19 PM

SSL Sucks **Secure Request**

New Brokerage Account

Name: Scott Gustafson

Address: 123 Main Street

City: Anytown State: CA

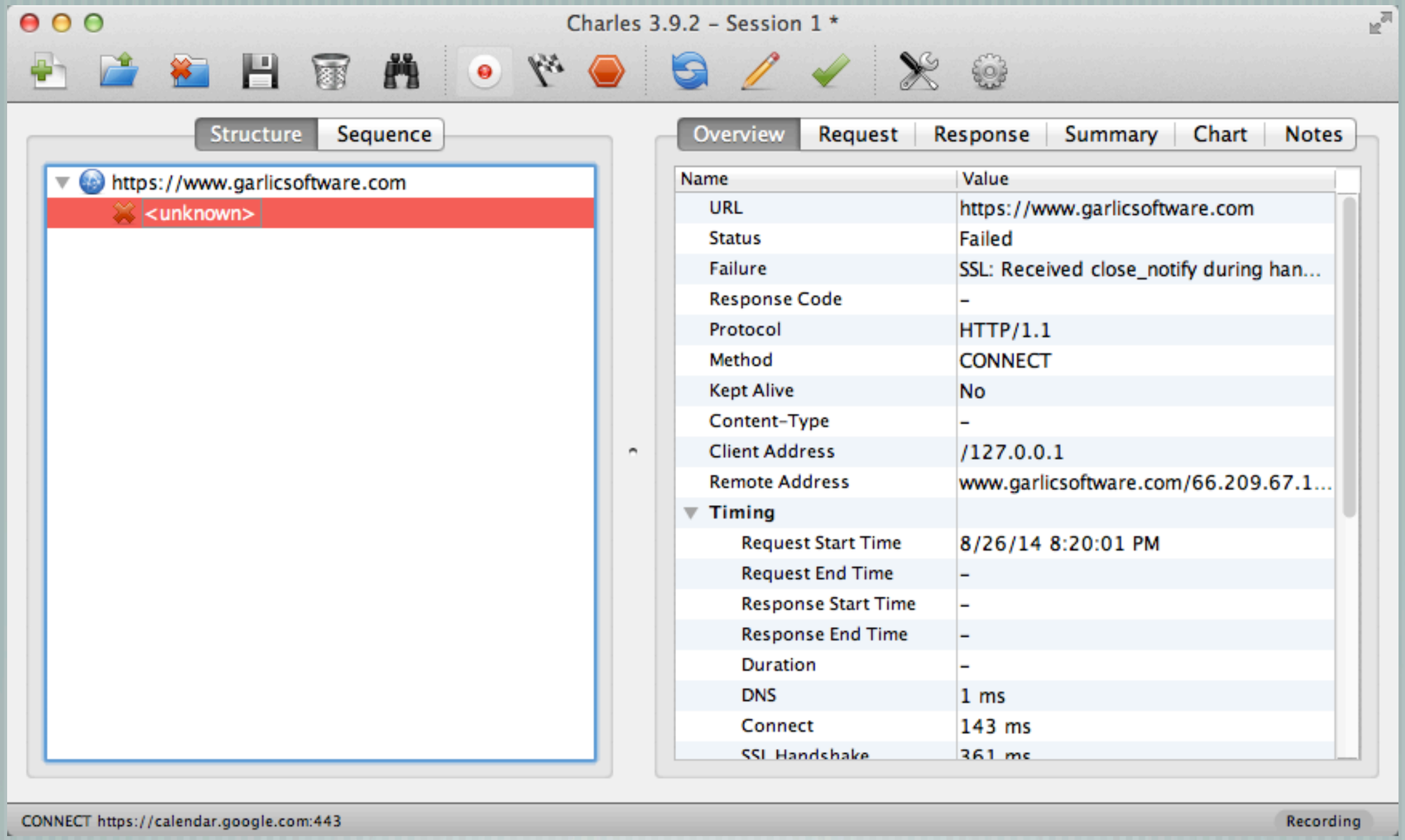
Attack Detected

A man in the middle attack has been detected. Data not sent.

OK

Mother's Maiden Name: Jones

Send


Charles 3.9.2 – Session 1 *
Structure
Sequence
https://www.garlicsoftware.com
<unknown>
Overview
Request
Response
Summary
Chart
Notes
Name
Value
URL
https://www.garlicsoftware.com
Status
Failed
Failure
SSL: Received close_notify during han...
Response Code
-
Protocol
HTTP/1.1
Method
CONNECT
Kept Alive
No
Content-Type
-
Client Address
/127.0.0.1
Remote Address
www.garlicsoftware.com/66.209.67.1...
Timing
Request Start Time
8/26/14 8:20:01 PM
Request End Time
-
Response Start Time
-
Response End Time
-
Duration
-
DNS
1 ms
Connect
143 ms
CONNECT https://calendar.google.com:443
Recording

Secure Your App

- Implement Certificate Pinning
- Define a strategy for rotating certificates as they expire

Secure Your Device

- Don't accept random certificates from wireless access points
- Can also be a problem with Enterprise environments (Provisioning Profiles)
- iOS 7 trusts 211 CAs

Secure Your Server

- Enable Forward Secrecy on key exchange
  - Ephemeral Elliptic Curve Diffie-Hellman
  - Ephemeral Diffie-Hellman
- Use a minimum of a 2048 bit public key
- Disable SSL 2.0 and TLS 1.0 support
  - Prefer TLS 1.2 or later

Testing Tools

- Charles (HTTP Proxy)
  http://www.charlesproxy.com
- PAW (HTTP REST Client)
  http://luckymarmot.com/paw
- mitmproxy (Man in the Middle Proxy)
  http://mitmproxy.org/

Contact Info

- Email: scott@garlicsoftware.com
  - PGP key ID: B0CC AC31 B097 C6C5
- Twitter: @scottg0
- Web: https://www.garlicsoftware.com
- GitHub: https://github.com/scott-42/SSLSucks