Foundstone
Professional Services A DIVISION OF McAFEE

clipcaptcha

Gursev Singh Kalra

***black**hat* *2012 USA | July 26, 2012*

Who Am I?

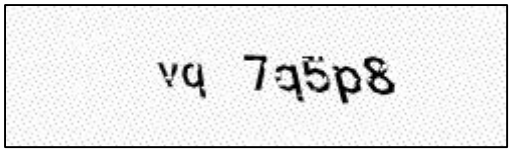
- Principal Consultant with McAfee Foundstone
- Security Research, Web Applications, Networks, Mobile Applications…. And more
- Tools (Oyedata, clipcaptcha, TesserCap, SSLSmart, and Internal)
- Ruby, C#, Rails

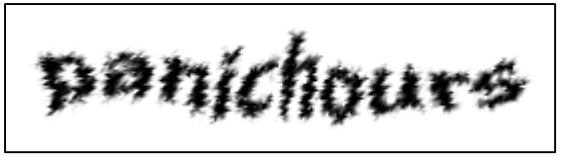
What is a CAPTCHA?

Completely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part

Attempt to ensure that a request is generated by a Human

Can be Audio/Visual/Combination





Foundstone
Professional Services A DIVISION OF McAFEE

Gursev Singh Kalra (@igursev)

What is a CAPTCHA Provider?

CAPTCHA Providers offer CAPTCHA Generation and Verification Services

Writing Secure CAPTCHAs is Hard

Websites Consume CAPTCHA Provider Services

CAPTCHA Retrieval

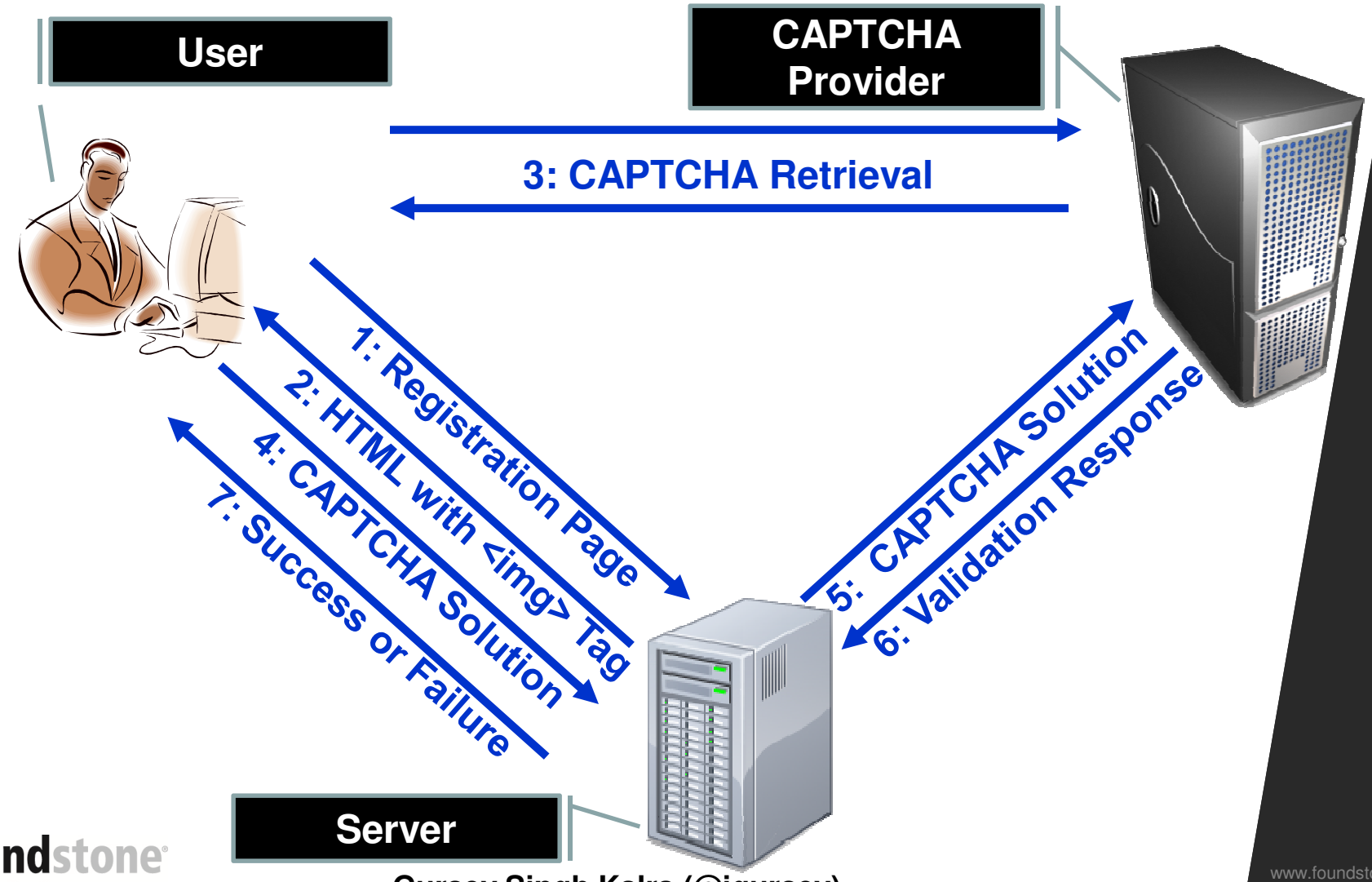
```
20
21 <h1>New OpenCAPTCHA Secret</h1>
22
23 <form accept-charset="UTF-8" action="/opsecrets/" method="post"><div
   style="margin:0;padding:0;display:inline"><input name="utf8" type="hidden" value="&#x2713;" /><input
   name="authenticity_token" type="hidden" value="Y+fPfwFI317SJbO8Dmn570pwM6vc570NpqZRPmM1lYM=" /></div>
24 Secr
25 <br/
26 <br/
27 <img
28 <br/
29 CAPT
30 <inp
31 <br/
32 <inp
33 </fo
34 <a h
35
```

```
20
21 <h1>New resecret</h1>
22
23 <form accept-charset="UTF-8" action="/resecrets/" method="post"><div
   style="margin:0;padding:0;display:inline"><input name="utf8" type="hidden" value="&#x2713;" /><input
   name="authenticity_token" type="hidden" value="Y+fPfwFI317SJbO8Dmn570pwM6vc570NpqZRPmM1lYM=" /></div>
24 <input id="resecret_secret" name="resecret[secret]" type="text" />
25 <script type="text/javascript" src="http://www.google.com/recaptcha/api/challenge?
   k=6LfQ5tMSAAAAAOfZy9j4VjYJJw24ZesEIT88LnQj&amp;error=expression"></script>
26 <noscript>
27   <iframe src="http://www.google.com/recaptcha/api/noscript?k=6LfQ5tMSAAAAAOfZy9j4VjYJJw24ZesEIT88LnQj"
   height="300" width="500" style="border:none;"></iframe><br/>
28   <textarea name="recaptcha_challenge_field" rows="3" cols="40"></textarea>
29   <input type="hidden" name="recaptcha_response_field" value="manual_challenge"/></noscript>
30
31 <input name="commit" type="submit" value="commit" />
32 </form>
33 <a href="/resecrets">Back</a>
34
```

Foundstone
Professional Services A DIVISION OF McAFEE

Gursev Singh Kalra (@igursev)

CAPTCHA Provider Integration



Foundstone Professional Services A DIVISION OF McAFEE

Gursev Singh Kalra (@igursev)

So What Went Wrong?

- Insecure Integration Libraries
- CAPTCHA Verification Performed over Plain Text HTTP
- Requests can be intercepted
- Responses can be altered

Insecure CAPTCHA Verification Libraries

```
require 'recaptcha/configuration'
require 'recaptcha/client_helper'
require 'recaptcha/verify'

module Recaptcha
  RECAPTCHA_API_SERVER_URL        = 'http://www.google.com/recaptcha/api'
  RECAPTCHA_API_SECURE_SERVER_URL = 'https://www.google.com/recaptcha/api'
  RECAPTCHA_VERIFY_URL            = 'http://www.google.com/recaptcha/api/verify'

  SKIP_VERI

  # Gives a
  def self.
    @config
  end
```

RecaptchaValidator.cs | RecaptchaControl.cs

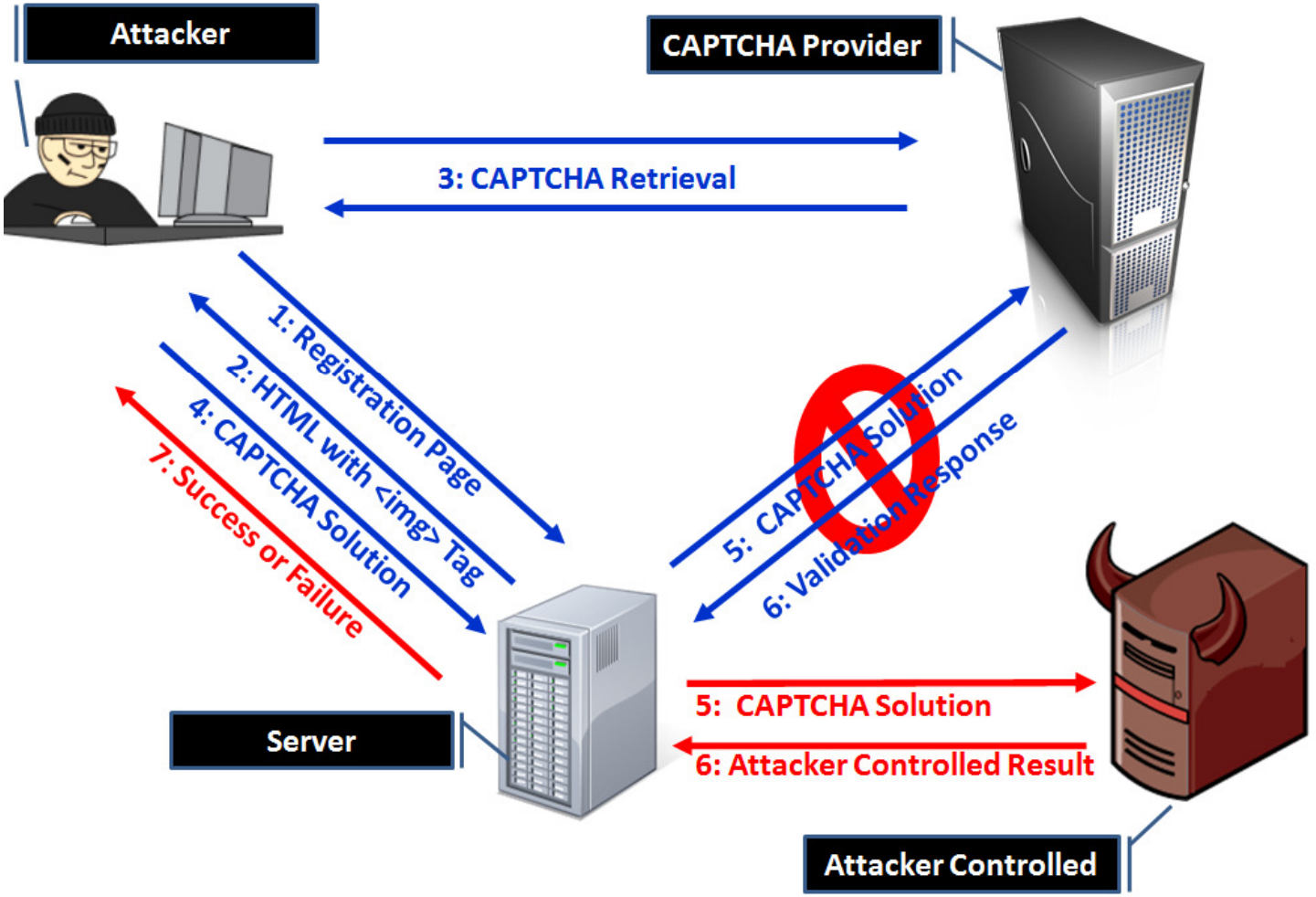
Recaptcha.RecaptchaValidator | PrivateKey

```
1  using System;
2  using System.Diagnostics;
3  using System.IO;
4  using System.Net;
5  using System.Net.Sockets;
6  using System.Text;
7  using System.Web;
8  namespace Recaptcha
9  {
10     public class RecaptchaValidator
11     {
12         private const string VerifyUrl = "http://www.google.com/recaptcha/api/verify";
13         private string privateKey;
14         private string remoteIp;
15         private string challenge;
16         private string response;
17         private IWebProxy proxy;
18         public string PrivateKey
```

Foundstone Professional Services A DIVISION OF McAFEE

Gursev Singh Kalra (@igursev)

CAPTCHA Provider Impersonation



clipcaptcha

Foundstone
Professional Services A DIVISION OF McAFEE

Gursev Singh Kalra (@igursev)

clipcaptcha Overview

- Based on sslstrip codebase
- Written in Python
- Impersonates CAPTCHA Providers
- Administers CAPTCHA Verification Requests
- Logs Verification Requests (Private Keys)

CAPTCHA Verification Requests

CAPTCHA Provider =>	reCAPTCHA	OpenCAPTCHA
Validating Host	www.google.com	www.opencaptcha.com
CAPTCHA Validation Request		
Validation Path	/recaptcha/api/verify	/validate.php
Query String	None	ans=<CAPTCHA Solution>&img=<CAPTCHA Identifier>
Request Headers	None mandated	None mandated
POST Contents	privatekey=<privateKey>&remoteip=<remoteIP>&challenge=<CAPTCHA Identifier>&response=<CAPTCHA Solution>	None

CAPTCHA Provider Responses

CAPTCHA Provider =>	reCAPTCHA	OpenCAPTCHA
Validating Host	www.google.com	www.opencaptcha.com
CAPTCHA Validation Response		
Success Status Line	HTTP/1.0 200 OK	HTTP/1.0 200 OK
Success Response Headers	None mandated	None mandated
Success Body	true	pass
Failure Status Line	HTTP/1.0 200 OK	HTTP/1.0 200 OK
Failure Response Headers	None mandated	None mandated
Failure Body	false <ErrorCode>	fail

CAPTCHA Verification Request and Response Characteristics

Requests and Responses

- Dedicated server
- Abide by HTTP specifications

Responses are Boolean

- True or False
- Pass or Fail
- “1” or “0”

clipcaptcha Help Screen

```
gk> python clipcaptcha.py -h
=>> clipcaptcha 0.1 by Gursev Singh Kalra
Usage: clipcaptcha <mode> <options>
Modes(choose one):
        -m , --monitor                          Listen and log. No changes made (default)
        -a , --avalanche                        Return success for all CAPTCHA validations
        -s <secret> , --stealth <secret>        Stealth mode with secret string to approve our own submissions
        -d , --dos                              Return failure for all CAPTCHA validations
        -r , --random                           Return random success or failures for CAPTCHA validations
Options:
        -c <filename> , --config=<filename>     clipcaptcha Config file with CAPTCHA provider signatures (optional)
        -p <port> , --port=<port>               Port to listen on (default 7777).
        -f <filename> , --file=<filename>       Specify file to log to (default clipcaptcha.log).
        -l , --list                             List CAPTCHA providers available
        -h , --help                             Print this help message.

gk>
```

clipcapcha Operational Modes

- Monitor
- Avalanche
- Denial of Service
- Stealth
- Random

clipcaptcha Configuration File

CAPTCHA Provider Request and Response Information

XML Based and Extensible

```
        <provider>
                <name>OpenCAPTCHA</name>
                <hostname>www.opencaptcha.com</hostname>
                <path>/validate.php</path>
                <success>
                        <rcode>200</rcode>
                        <rcodestr>OK</rcodestr>
                        <rbody>pass</rbody>
                </success>
                <failure>
                        <rcode>200</rcode>
                        <rcodestr>OK</rcodestr>
                        <rbody>fail</rbody>
                </failure>
        </provider>
</clipcaptcha>
```

clipcaptcha Demonstrations

Foundstone Professional Services A DIVISION OF McAFEE

Gursev Singh Kalra (@igursev)

Special Thanks!

Moxie Marlinspike for sslstrip and saving me tons of time

Thank You!

https://github.com/OpenSecurityResearch/clipcaptcha

gursev.kalra@foundstone.com
http://gursevkalra.blogspot.com
http://blog.opensecurityresearch.com

Foundstone
Professional Services A DIVISION OF McAFEE

Gursev Singh Kalra (@igursev)