

---

# **Public Key Protocols**

## **Epilogue**

Simon Foley

November 23, 2015

# Hacking the Secure Web

Semantic Attacks  
HCI Attacks  
MD5 Harmful  
MD5 Harmful  
Click Thru  
TOFU  
Perspectives

Early browsers (for US export) permitted only a 40-bit session key, making a brute force attack on the key possible.

An SSL-authenticated connection from your web-browser to a web-server does not secure the transaction, it only secures the connection/session;

It is typically the credit card that secures a web-purchase.

While the browser will authenticate an https connection to a website, the user must confirm by manual inspection that the website/certificate is indeed the business/etc that they expect.

- Earlier certificates/browsers did not necessarily include/validate the website address.
- It is a user's responsibility to confirm that the URL is as expected. An attacker (with website `www.amazon.com`) could obtain an X509 certificate for their public key. Any connection to this (malicious) website will be authentic and secure.

Who decides who should be the trustworthy CAs? Microsoft, Mozilla?

# What's this website?

▷ Semantic Attacks  
HCI Attacks  
MD5 Harmful  
MD5 Harmful  
Click Thru  
TOFU  
Perspectives

Semantic Attacks on URL by subtly changing its meaning without an (easily) apparent change in syntax.

Plain text attacks

`https://www.amazon.com`

`http://www.amazon.com@143.231.211.12/malicious`

`https://www.amazon.com@143.231.211.12/malicious`

Some browsers will warn you that you are attempting to login to a website.

Simple HTML attacks

`<A HREF=https://www.malicious.com> https://www.amazon.com </A>`

`<A HREF=http://www.amazon.com> https://www.amazon.com </A>`

It is the user's responsibility to know the website to which they are connecting.

It is the user's responsibility to know whether the connection they are making is secure or not.

# Yes, Yes, Yes, I accept!

Semantic Attacks

▷ HCI Attacks

MD5 Harmful

MD5 Harmful

Click Thru

TOFU

Perspectives



# MD5 Considered Harmful Today

Semantic Attacks  
HCI Attacks  
▷ MD5 Harmful  
MD5 Harmful  
Click Thru  
TOFU  
Perspectives

Recall that it is possible to find collisions in MD5, that is, it is possible to find values  $x$  and  $x'$  such that  $md5(x) = md5(x')$ .

This has a serious implication for public key certificates that use MD5 to implement their signatures. Recall that

$$\{K_A, Alice, \dots\}_{sK_B} \approx (K_A, Alice\dots), \{h(K_A, Alice, \dots)\}_{K_B^{-1}}$$

If MD5 is used to implement  $h()$  then it means that we could have two different certificates with the same signature.

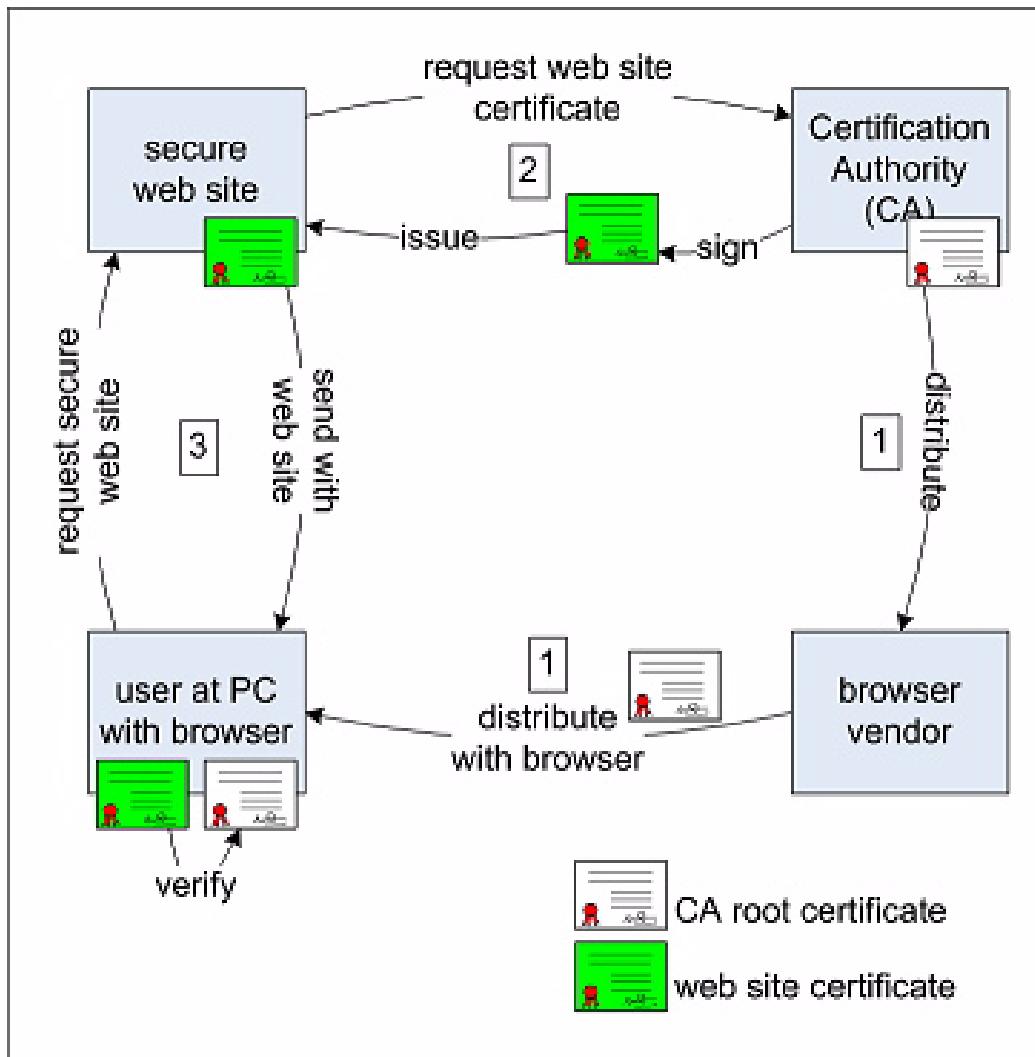
With MD5 it is possible, given  $\{K_A, Alice, \dots\}_{sK_B}$  for Malicious Mike (who owns  $K_M$ ) to forge another certificate  $\{K_M, Alice, \dots\}_{sK_B}$  that has the same signature value as the original certificate, that is,

$$\{h(K_A, Alice, \dots)\}_{K_B^{-1}} = \{h(K_M, Alice, \dots)\}_{K_B^{-1}}$$

MD5 certificates should never be accepted!

# MD5 Considered Harmful Today

Semantic Attacks  
HCI Attacks  
▷ MD5 Harmful  
MD5 Harmful  
Click Thru  
TOFU  
Perspectives



From <http://www.win.tue.nl/hashclash/rogue-ca/>

# MD5 Considered Harmful Today (2008)

Semantic Attacks

HCI Attacks

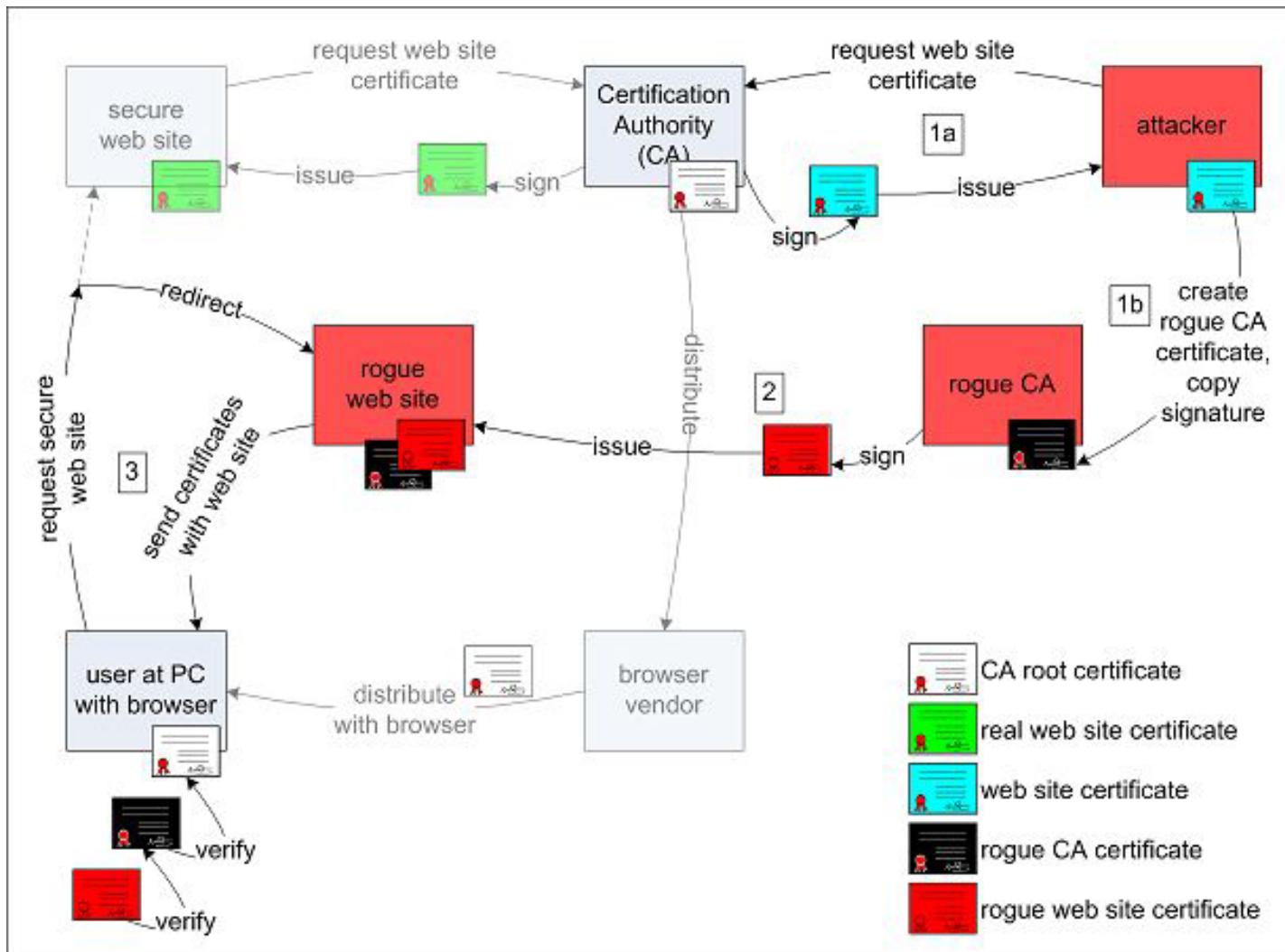
MD5 Harmful

▷ MD5 Harmful

Click Thru

TOFU

Perspectives



From <http://www.win.tue.nl/hashclash/rogue-ca/>

# MD5 Considered Harmful Today

Semantic Attacks  
HCI Attacks  
MD5 Harmful  
▷ MD5 Harmful  
Click Thru  
TOFU  
Perspectives

- 1a A legitimate website certificate is obtained from a commercial CA.
- 1b A rogue CA certificate is constructed. It bears exactly the same signature as the website certificate. Thus it appears as being issued by the CA, whereas in fact the CA has never even seen it.
- 2 Then a website certificate bearing the genuine website's identity but another public key is created and signed by the rogue CA. A copy of the genuine website is built, put on another web server, and equipped with the rogue website certificate.
- 3 When a user wants to visit the secure website, the web browser will look on the Internet for the genuine web server. There exist "redirection attacks", by which the communication from the browser can be redirected to the rogue website. This rogue website presents its certificate to the user, together with the rogue CA certificate. The signature in the rogue website certificate can be verified with the rogue CA certificate, and this rogue CA certificate in turn will be accepted by the browser, as its signature can be verified with the CA root certificate in the trust list. The user will not notice anything.

# Numbers of MD5 based certificates

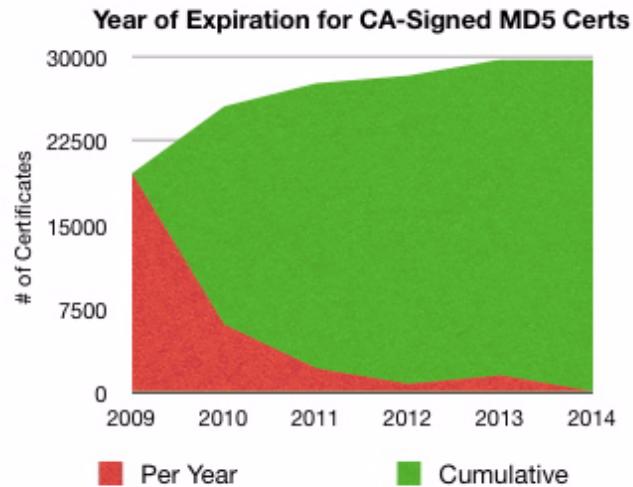
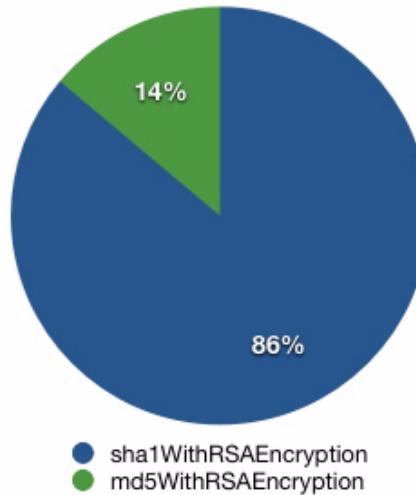
Semantic Attacks  
HCI Attacks  
MD5 Harmful  
▷ MD5 Harmful  
Click Thru  
TOFU  
Perspectives

From

<http://blog.johnath.com/2009/01/21/ssl-information-wants-to-be-free/>

Crawled the top 1 million HTTPS sites [Jan 2009]

Signature Algorithms on Valid CA-Signed Certs (n=214035)



# iOS 5/6 phone comes with US DoD root CA certificate pre-installed

Semantic Attacks  
HCI Attacks  
MD5 Harmful  
▷ MD5 Harmful  
Click Thru  
TOFU  
Perspectives

The screenshot shows a web page from support.apple.com with the URL support.apple.com/ht5012. The page title is "iOS 5 and iOS 6: List of available trusted root certificates". It features a sidebar with navigation links like Apple, Store, Mac, iPod, iPhone, iPad, and iTunes. Below the title, there's a summary section and a products affected section. A large button labeled "Click here to reveal the certificates for iOS 5 and iOS 6." is present. When clicked, it reveals a detailed view of the certificate data, including fields for Certificate, Data, and Validity.

**Summary**  
These trusted root certificates are preinstalled with iOS 5 and iOS 6. When IT administrators create Configuration Profiles for iPhone, iPad, or iPod touch using the iPhone Configuration Utility, these certificates do not need to be included.

**Products Affected**  
iPad, iPhone, iPod touch

▼ Click here to reveal the certificates for iOS 5 and iOS 6.

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 4 (0x4)
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, O=U.S. Government, OU=DoD, OU=PKI, CN=DoD CLASS 3 Root CA
Validity
Not Before: May 19 13:13:00 2000 GMT
Not After : May 14 13:13:00 2020 GMT
Subject: C=US, O=U.S. Government, OU=DoD, OU=PKI, CN=DoD CLASS 3 Root CA

<https://twitter.com/mikko/status/327170802673917952/photo/1/large>

[as does latest iOS7] What are the threats?

# Ignoring Security Warnings

Semantic Attacks

HCI Attacks

MD5 Harmful

MD5 Harmful

▷ Click Thru

TOFU

Perspectives

Browser Understood	Expired Certificate			Unknown CA		Domain Mismatch		
			Ignored		Ignored		Ignored	
<b>FF2</b>	Y	48	50%	71%	37	39%	43%	57 19% $\chi^2 = 9.40$
	N	48	50%	56%	59	61%	49%	39 49% $p < 0.009$
<b>FF3</b>	Y	55	47%	64% $\chi^2 = 21.05$	35	30%	31%	46 15% $\chi^2 = 8.65$
	N	62	53%	34% $p < 0.0005$	82	70%	34%	71 41% $p < 0.013$
<b>IE7</b>	Y	45	23%	53% $\chi^2 = 11.81$	44	22%	27%	62 16% $\chi^2 = 7.50$
	N	151	77%	32% $p < 0.003$	152	78%	32%	134 35% $p < 0.024$

Table 1: Participants from each condition who could correctly identify each warning, and of those, how many said they would continue to the website. Differences in comprehension within each browser condition were statistically significant (FF2:  $Q_2 = 10.945$ ,  $p < 0.004$ ; FF3:  $Q_2 = 11.358$ ,  $p < 0.003$ ; IE7:  $Q_2 = 9.903$ ,  $p < 0.007$ ). For each browser condition, the first line depicts the respondents who could correctly define the warnings, while the second depicts those who could not. There were no statistically significant differences between correctly understanding the unknown CA warning and whether they chose to ignore it.

[From J. Sunshine et al, *Crying Wolf: An Empirical Study of SSL Warning Effectiveness*, 18th USENIX Security Symposium, 2008]

# Trust on First Use (TOFU)

Semantic Attacks  
HCI Attacks  
MD5 Harmful  
MD5 Harmful  
Click Thru  
▷ TOFU  
Perspectives

It's not unusual for a website to have a self-signed certificate, rather than having to pay a CA to sign their public key.

The user-strategy is that the first they visit the site they decide how likely is there to be a man-in-the-middle attacker between the website and their browser. If they decide the likelihood is low then they accept the certificate and trust on its first use that it comes from the legitimate website (and not a man in the middle). All subsequent use is as secure as the first use, regardless of the presence of an man-in-the-middle.

For example, for a wired connection on the UCC backbone there is a low-chance of a man in the middle attacker and the user accepts (and stores) the <https://www.cs.ucc.ie> certificate. This (stored) certificate is used when the user visits <https://www.cs.ucc.ie> from outside the ucc domain, where the chance of an attacker is higher.

ssh can rely on a similar TOFU strategy.

# Example: ssh TOFU

Semantic Attacks

HCI Attacks

MD5 Harmful

MD5 Harmful

Click Thru

▷ TOFU

Perspectives

**machine:~/.ssh simon\$ ssh cosmos.ucc.ie**

The authenticity of host 'cosmos.ucc.ie' (143.239.159.63) can't be established.

RSA key fingerprint is 10:2c:a2:1f:5d:9e:c4:b1:1d:12:e1:66:dc:ac:49:e1.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added 'cosmos.ucc.ie,143.239.159.63' (RSA) to the list of known hosts.

Password:

Last login : Mon Dec 1 14:21:10 2008 from machine.ucc.ie

#####
#####

#### Welcome to cosmos ####

Note: sftp is available NOT ftp

#####
#####

Directory : /home/simon

Mon Dec 1 14:22:49 GMT 2008

cosmos:/home/simon>

# Example: ssh TOFU, saved public key

Semantic Attacks

HCI Attacks

MD5 Harmful

MD5 Harmful

Click Thru

▷ TOFU

Perspectives

```
machine:~ simon$ more .ssh/known_hosts"  
cosmos.ucc.ie,143.239.159.63 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAsZ1  
PWZELHoW2qEX6WraLPxzZVrN/iHlfz/zKkvRdoFy+UYXsI0OccbMvOevcAbFm  
aDFWufU1OtrtvC81E8IQIHsQEjQ/5lvY08rnvQ7Vt/kwbfPym00DlikhsfP6LIRa2Qn
```

# Example: ssh TOFU, next login

Semantic Attacks

HCI Attacks

MD5 Harmful

MD5 Harmful

Click Thru

▷ TOFU

Perspectives

machine:~ simon\$ ssh cosmos.ucc.ie

Password:

Last login: Mon Dec 1 14:22:49 2008 from machine.ucc.ie

#####

### Welcome to cosmos #####

Note: sftp is available NOT ftp

-----

#####

Directory : /home/simon

Wed Dec 3 12:39:40 GMT 2008

cosmos /home/simon>

# Example: ssh TOFU, change cosmos PK

Semantic Attacks

HCI Attacks

MD5 Harmful

MD5 Harmful

Click Thru

▷ TOFU

Perspectives

machine:~ simon\$ emacs .ssh/known\_hosts

...

machine:~ simon\$ ssh cosmos.ucc.ie

@@@@@@@  
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @

@@@@@@@  
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!

Someone could be eavesdropping on you right now (man-in-the-middle attack)!

It is also possible that the RSA host key has just been changed.

The fingerprint **for** the RSA key sent by the remote host is

10:2c:a2:1f:5d:9e:c4:b1:1d:12:e1:66:dc:ac:49:e1.

Please contact your system administrator .

Add correct host key in /Users/simon/.ssh/known\_hosts to get rid of **this** message.

Offending key in /Users/simon/.ssh/known\_hosts:1

RSA host key **for** cosmos.ucc.ie has changed and you have requested strict checking

Host key verification failed .

machine:~ simon\$

# Example: ssh TOFU, strong client authentication

Semantic Attacks

HCI Attacks

MD5 Harmful

MD5 Harmful

Click Thru

▷ TOFU

Perspectives

```
machine:~ simon$ ssh-keygen
Generating public/private rsa key pair .
Enter file in which to save the key (/Users/simon/.ssh/id_rsa ):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/simon/.ssh/id_rsa .
Your public key has been saved in /Users/simon/.ssh/id_rsa.pub.
The key fingerprint is :
79:c6:49:24:9b:6a:d7:b6:ef:67:0e:e2:bc:c7:b9 simon@machine.ucc.ie
machine:~ simon$
..... then copy d_rsa.pub to .ssh/authorized_keys on cosmos ....
machine:~ ssh cosmos.ucc.ie
Last login: Wed Jan 14 12:32:17 2009 from machine.ucc.ie
### Welcome to cosmos #####
Note: sftp is available NOT ftp
-----
######
Directory : /home/simon
```

# Perspectives: Strengthening TOFU

Semantic Attacks  
HCI Attacks  
MD5 Harmful  
MD5 Harmful  
Click Thru  
TOFU  
▷ Perspectives

A plug-in for Firefox that strengthens TOFU of self-signed certificates.

Network Notary servers maintain databases of self-signed keys that have been accepted by users in the past.

On presentation of a self-signed certificate, the plug-in consults with the network servers in order to confirm the certificate and whether the public key has appeared to have changed recently.

See <http://perspectives-project.org/> for overview and plugin.

Semantic Attacks  
HCI Attacks  
MD5 Harmful  
MD5 Harmful  
Click Thru  
TOFU  
▷ Perspectives

how secure is my ssl client

<https://www.howsmyssl.com/>

<https://news.ycombinator.com/item?id=7027255>

# The complexity of it all

Semantic Attacks  
HCI Attacks  
MD5 Harmful  
MD5 Harmful  
Click Thru  
TOFU  
▷ Perspectives

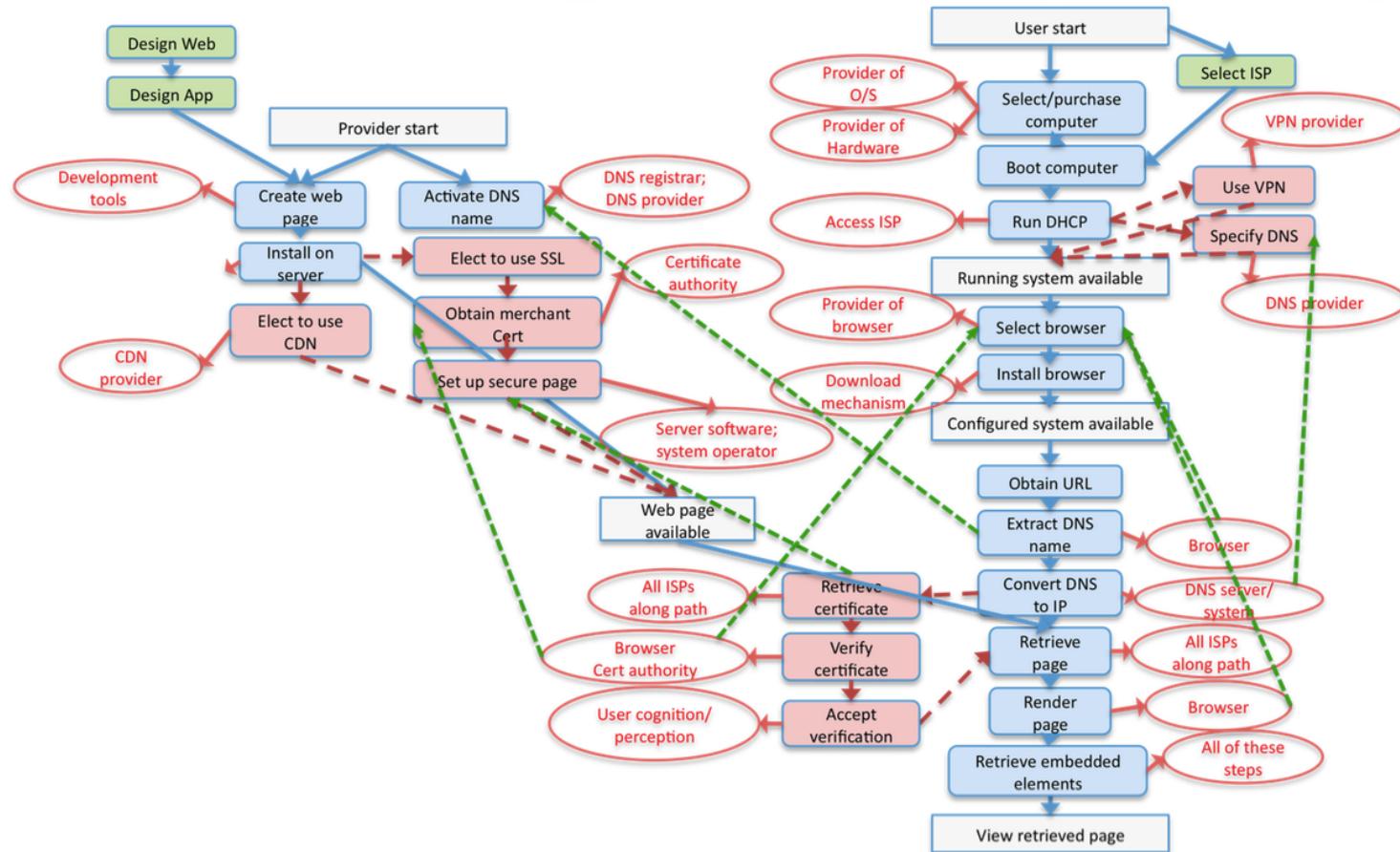


Figure 1: Steps in the retrieval and viewing of a web page. Blue arrows indicate the normal sequence of steps. Green arrows capture dependencies on prior steps. Red ovals catalog the actor(s) that have control of the outcome of each step. Green boxes are parts of the diagram that are not elaborated in this paper.

[D. Clark, Control Point Analysis, MIT CSAIL, TPRC submission version 2.2 of September 10, 2012]  
<http://ecir.mit.edu/images/stories/Control%20point%20analysis%20TPRC%202-2.pdf>

# The complexity of it all

Semantic Attacks  
HCI Attacks  
MD5 Harmful  
MD5 Harmful  
Click Thru  
TOFU  
▷ Perspectives

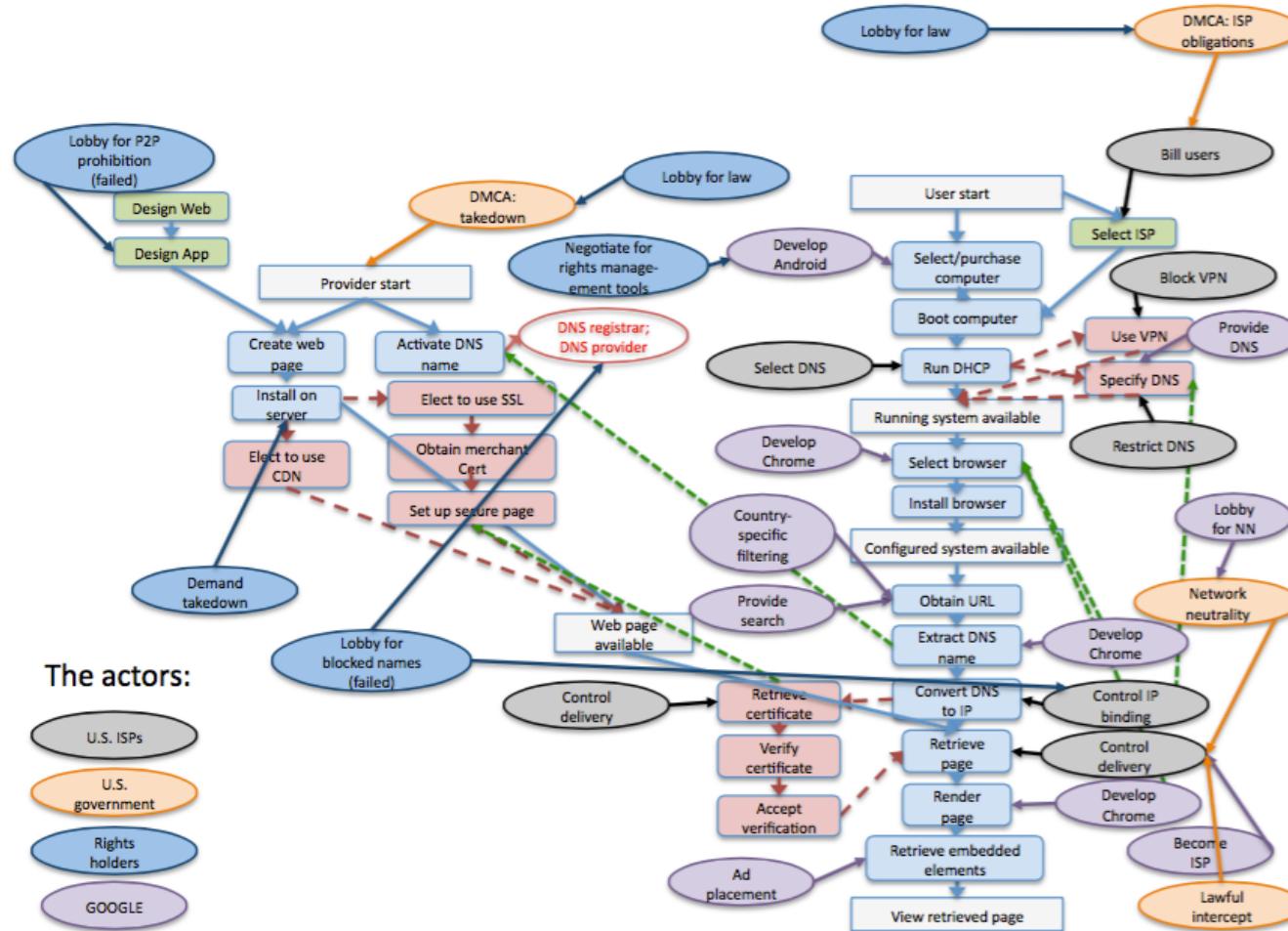


Figure 8: Points of control for Google. Google is a distinctively powerful private sector actor, with many direct means to control the experience of using the Internet.

[D. Clark, Control Point Analysis, MIT CSAIL, TPRC submission version 2.2 of September 10, 2012]  
<http://ecir.mit.edu/images/stories/Control%20point%20analysis%20TPRC%202-2.pdf>