

CLICKJACKING & PHISHING

CMSC 414

FEB 28 2019



Town Hall tonight

- CSIC 1115, 5pm-7pm
- There is insufficient space in Iribe
 - Virtually no student group space
 - No TA space
- Extra space is going to non-CS UMIACS
- [reddit.com/r/umd](https://www.reddit.com/r/umd) has a post about it
- Ask questions, find out what's going on, be a part of the future of computing at UMD

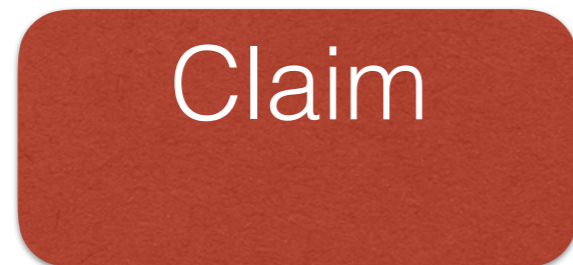
Misleading users

- Browser assumes that clicks and keystrokes = *clear indication* of what the user wants to do
 - Constitutes part of the user's *trusted path*
- Attacker can meddle with integrity of this relationship in all sorts of ways

Misleading users

- Browser assumes that clicks and keystrokes = *clear indication* of what the user wants to do
 - Constitutes part of the user's *trusted path*
- Attacker can meddle with integrity of this relationship in all sorts of ways
- Recall the power of Javascript
 - **Alter page contents (dynamically)**
 - **Track events (mouse clicks, motion, keystrokes)**
 - Read/set cookies
 - Issue web requests, read replies

Using JS to Steal Facebook *Likes*



Bait and switch

User tries to claim their free iPad, but you want them to click your Like button

(Many of these attacks are similar to TOCTTOU vulnerabilities)

Using JS to Steal Facebook *Likes*

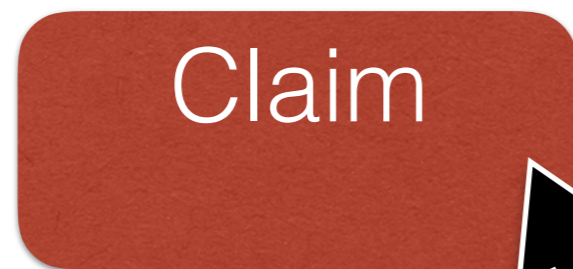


Bait and switch

User tries to claim their free iPad, but you want them to click your Like button

(Many of these attacks are similar to TOCTTOU vulnerabilities)

Using JS to Steal Facebook *Likes*



User intent



Actual outcome

Bait and switch

User tries to claim their free iPad, but you want them to click your Like button

(Many of these attacks are similar to TOCTTOU vulnerabilities)

Clickjacking

When one principal tricks the user into interacting with UI elements of another principal

An attack application (script) compromises the ***context integrity*** of another application's User Interface when the user acts on the UI

Clickjacking

When one principal tricks the user into interacting with UI elements of another principal

An attack application (script) compromises the ***context integrity*** of another application's User Interface when the user acts on the UI

Context
Integrity

1. **Visual context**: what a user should see right before the sensitive action. Ensuring this = the sensitive UI element and the cursor are both visible
2. **Temporal context**: the timing of a user action. Ensuring this = the user action at a particular time is what the user intended

Compromising visual integrity of the *target*

- Hide the target element
 - CSS lets you set the opacity of an element to zero (clear)



Compromising visual integrity of the *target*

- Hide the target element
 - CSS lets you set the opacity of an element to zero (clear)

- Partially overlay the target
 - Or *crop* the parts you don't want



To: Bad guy
From: Victim
Amount: \$1000

Pay

Compromising visual integrity of the *target*

- Hide the target element
 - CSS lets you set the opacity of an element to zero (clear)

- Partially overlay the target
 - Or *crop* the parts you don't want



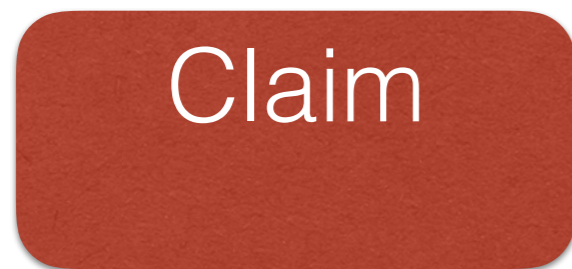
To: Charity

From: Nice person

Amount: \$10

Pay

Compromising visual integrity of the *pointer*



Actual cursor

- Manipulating cursor feedback

Compromising visual integrity of the *pointer*



- Manipulating cursor feedback

Compromising visual integrity of the *pointer*



- Manipulating cursor feedback

Clickjacking to access a user's webcam



Some clickjacking defenses

- Require confirmation for actions
 - Annoys users
- **Frame-busting:** Website ensures that its “vulnerable” pages can’t be included as a *frame* inside another browser frame
 - So user can’t be looking at it with something invisible overlaid on top...
 - ...nor have the site invisible above something else



The attacker implements this by placing Twitter's page in a "Frame" inside their own page, otherwise they wouldn't overlap

Some clickjacking defenses

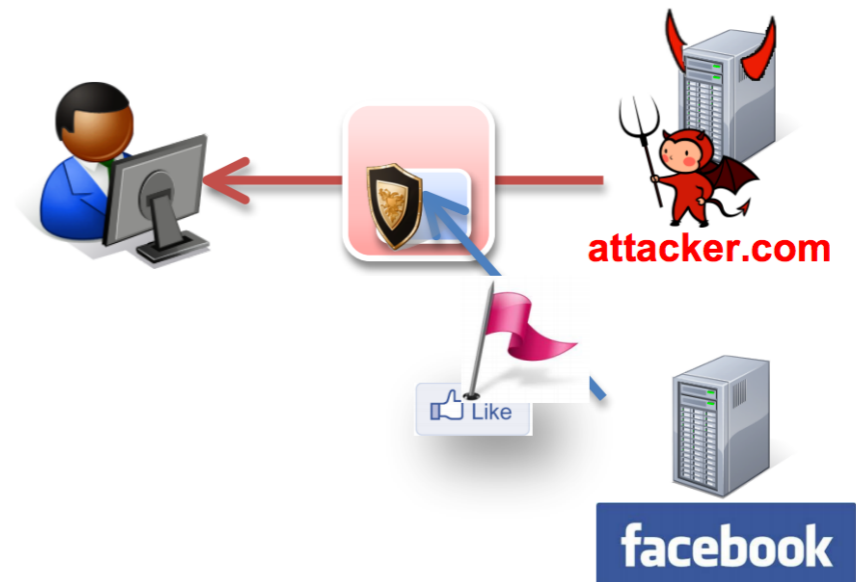
- Require confirmation for actions
 - Annoys users
- **Frame-busting:** Website ensures that its “vulnerable” pages can’t be included as a *frame* inside another browser frame
 - So user can’t be looking at it with something invisible overlaid on top...
 - ...nor have the site invisible above something else
- Conceptually implemented with Javascript like

```
if(top.location != self.location)
    top.location = self.location;
```

(actually, it’s quite tricky to get this right)
- Current research considers more general approaches

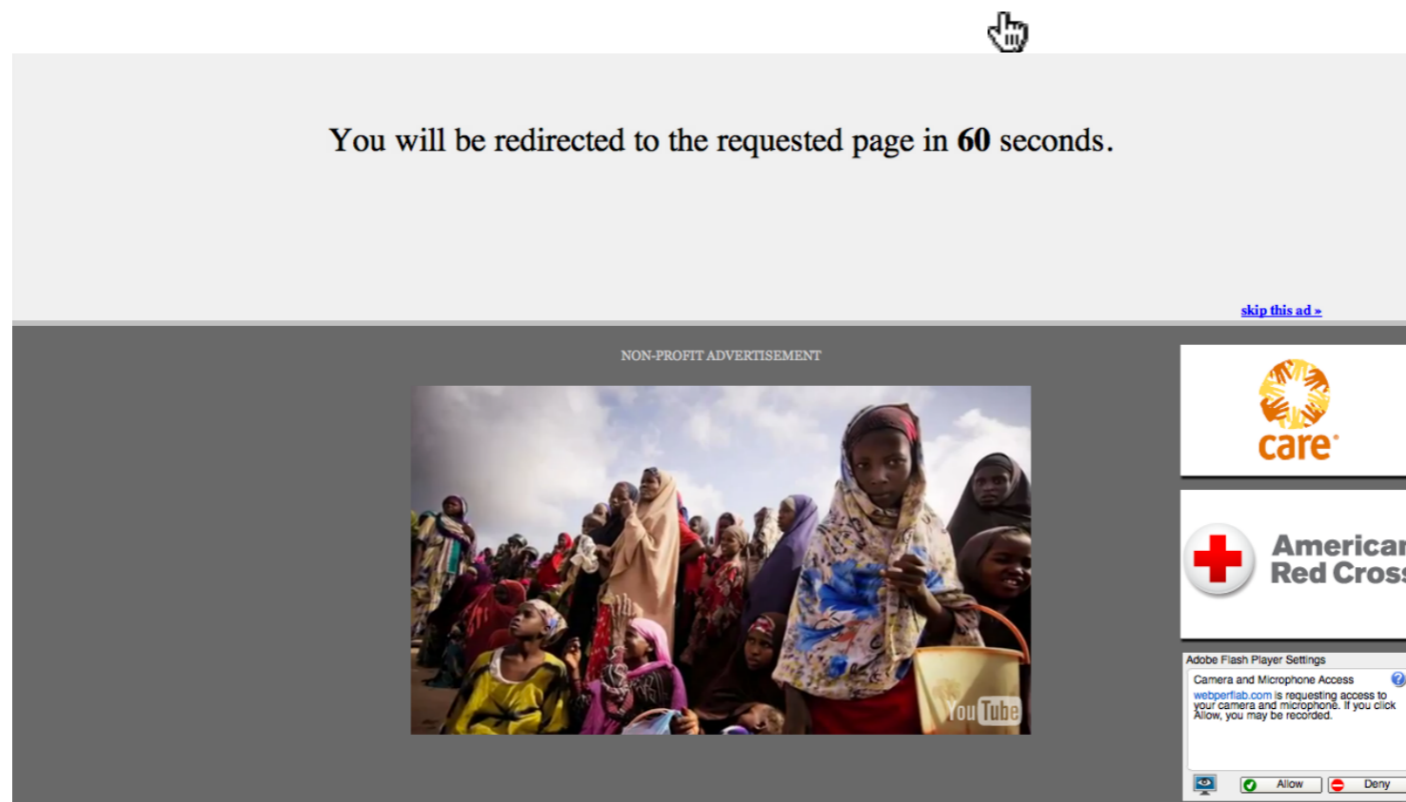
InContext Defense (recent research)

- A set of techniques to ensure context integrity for user actions
- Servers opt-in
 - Let the websites *indicate* their sensitive UIs
 - Let browsers *enforce* when users act on the



Ensuring visual integrity of pointer

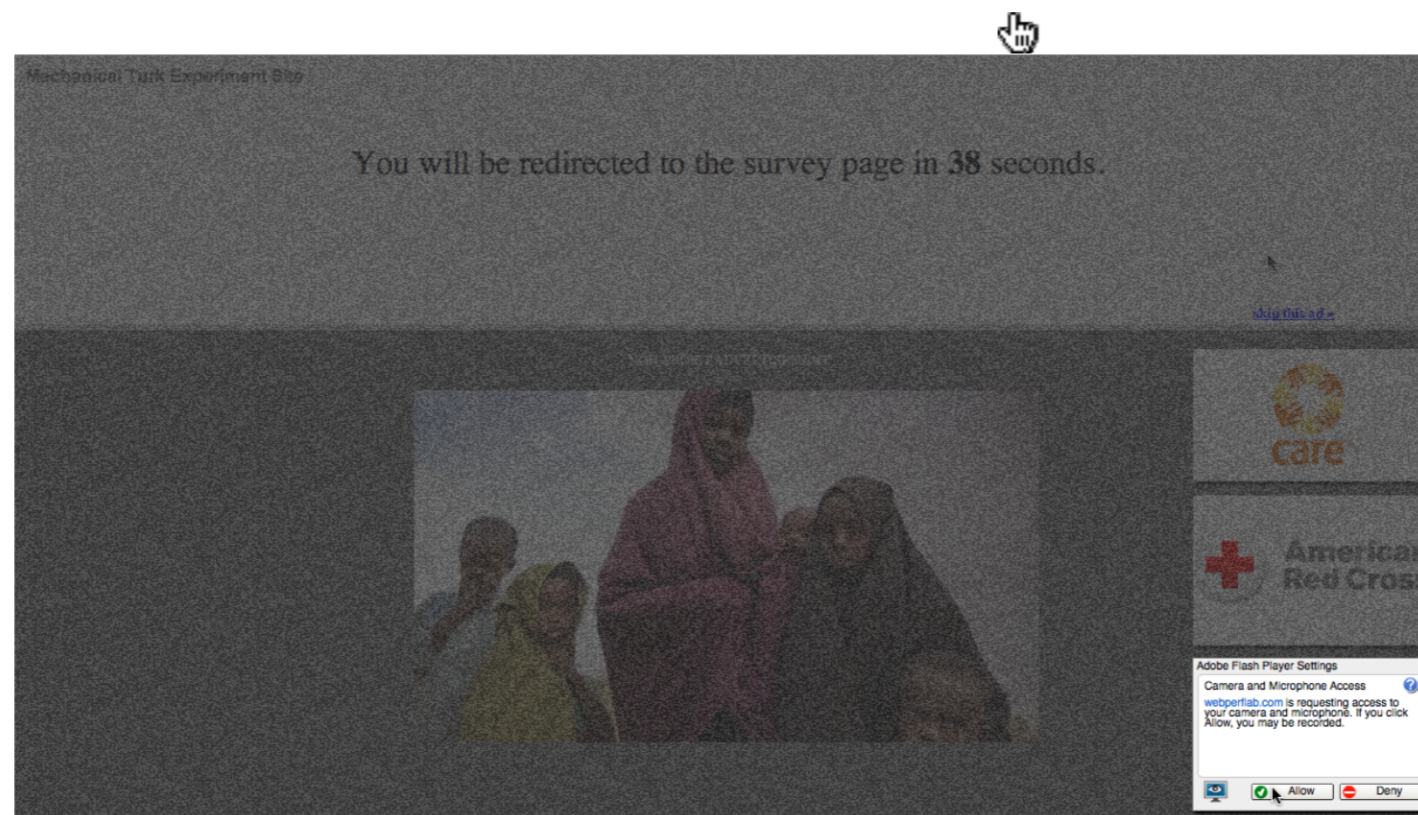
- Remove cursor customization
 - Attack success: 43% -> 16%

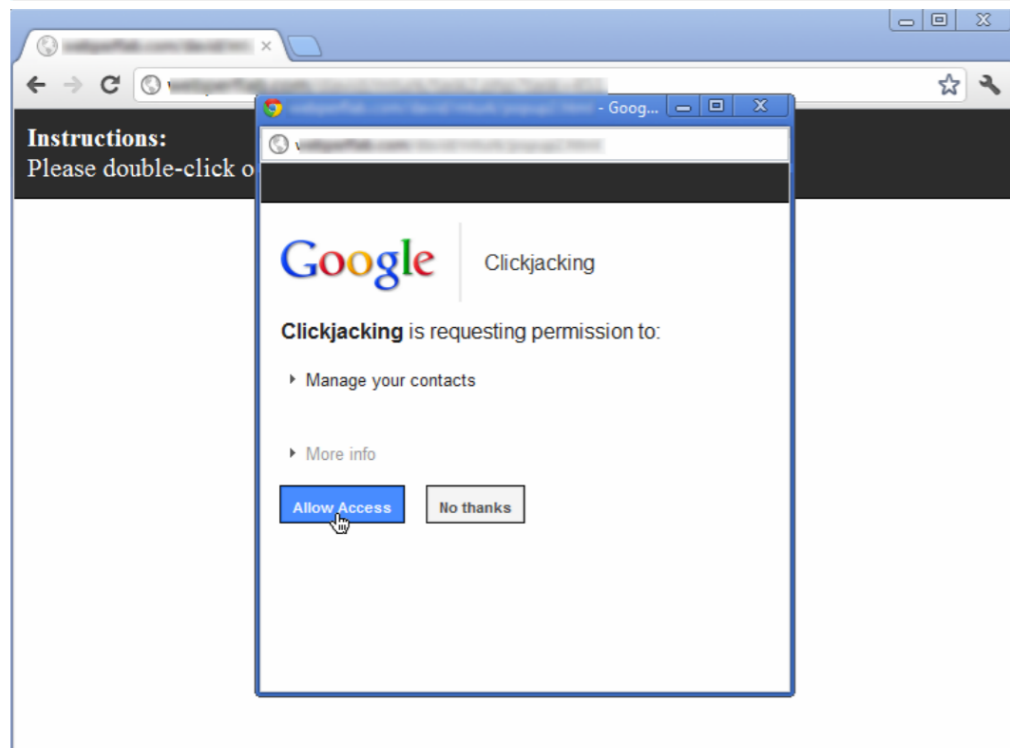
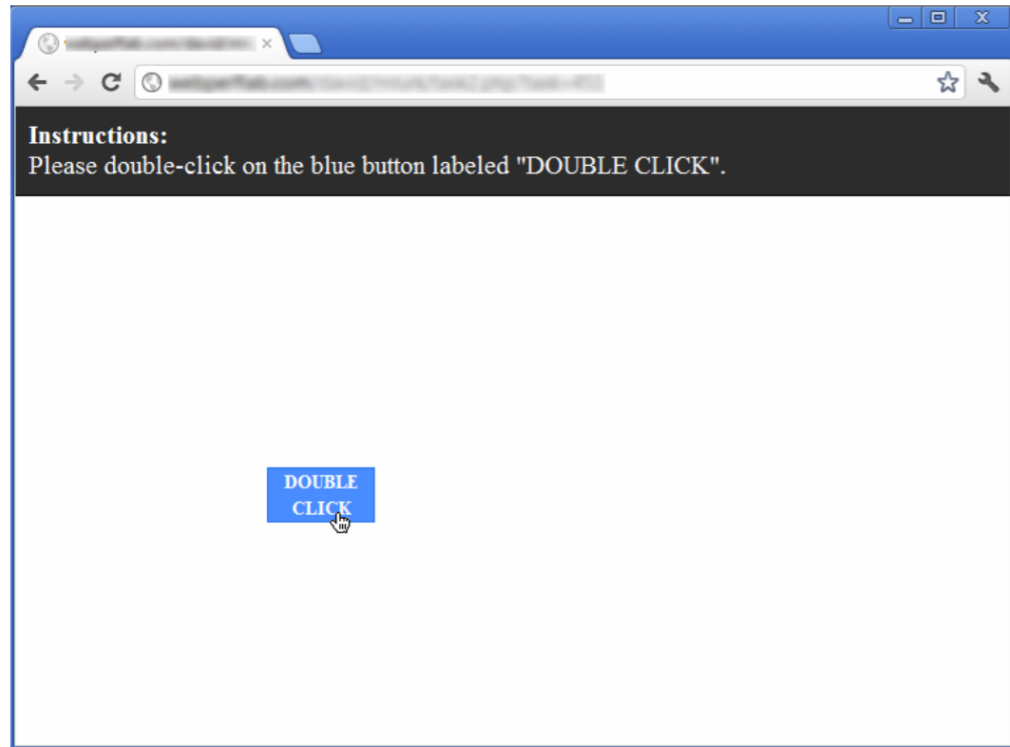


Ensuring visual integrity of pointer

- Lightbox effect around target on pointer entry

-





Enforcing temporal integrity

- UI delay: after visual changes on target or pointer, invalidate clicks for a few milliseconds
- Pointer re-entry: after visual changes on target, invalidate clicks until pointer re-enters target

Other forms of UI sneakiness

- Along with stealing events, attackers can use the power of Javascript customization and dynamic changes to mess with the user's mind
- For example, the user may not be paying attention, so you can swap tabs on them
- Or they may find themselves “eclipsed”

Browser in browser



WHAT IS UNTRUSTWORTHY HERE?





WHAT IS UNTRUSTWORTHY HERE?







widalec.org



CLICKJACKING: EXPERIMENTS

- Mechanical Turks
 - \$0.25 per participant to “follow the on-screen instructions and complete an interactive task.”
 - Simulated attacks, simulated defenses
 - 3251 participants
 - Note: You must control for sloppy participation
 - Excluded 370 repeat-participants

CLICKJACKING: EXPERIMENTS

- Control group 1
 - “Skip ad” button
 - No attack to trick the user
 - Purpose: To determine the click rate we would hope a defense could achieve in countering an attack
 - 38% didn’t skip the ad
- Control group 2
 - “Allow” button to skip ad
 - Purpose: An attempt to persuade users to grant access without tricking them
 - 8% allowed (statistically indistinguishable from group 1)

CLICKJACKING: EXPERIMENTS

7.5 Ethics

The ethical elements of our study were reviewed as per our research institution's requirements. No participants were actually attacked in the course of our experiments; the images they were tricked to click appeared identical to sensitive third-party embedded content elements, but were actually harmless replicas. However, participants may have realized that they had been tricked and this discovery could potentially lead to anxiety. Thus, after the simulated attack we not only disclosed the attack but explained that it was simulated.

CLICKJACKING: EXPERIMENTS

Treatment Group	Total	Timeout	Skip	Quit	Attack Success
1. Base control	68	26	35	3	4 (5%)
2. Persuasion control	73	65	0	2	6 (8%)
3. Attack	72	38	0	3	31 (43%)
4. No cursor styles	72	34	23	3	12 (16%)
5a. Freezing ($M=0\text{px}$)	70	52	0	7	11 (15%)
5b. Freezing ($M=10\text{px}$)	72	60	0	3	9 (12%)
5c. Freezing ($M=20\text{px}$)	72	63	0	6	3 (4%)
6. Muting + 5c	70	66	0	2	2 (2%)
7. Lightbox + 5c	71	66	0	3	2 (2%)
8. Lightbox + 6	71	60	0	8	3 (4%)

Table 2: Results of the cursor-spoofing attack. *Our attack tricked 43% of participants to click on a button that would grant webcam access. Several of our proposed defenses reduced the rate of clicking to the level expected if no attack had occurred.*

Treatment Group	Total	Timeout	Quit	Attack Success
1. Attack	90	46	1	43 (47%)
2a. UI Delay ($T_A=250\text{ms}$)	91	89	0	2 (2%)
2b. UI Delay ($T_A=500\text{ms}$)	89	86	2	1 (1%)
3. Pointer re-entry	88	88	0	0 (0%)

Table 3: Results of double-click attack. *43 of 90 participants fell for the attack that would grant access to their personal Google data. Two of our defenses stopped the attack completely.*

CLICKJACKING: EXPERIMENTS

Instructions:
Please click on blue buttons *as fast as possible*. The faster you complete this game, the greater your chances to win a \$100 prize! If you don't click on a button, the game will skip it in 10 seconds.

Buttons clicked: 16/20
Time elapsed: 24.6 sec

CLICK ME

Instructions:
Please click on blue buttons *as fast as possible*. The faster you complete this game, the greater your chances to win a \$100 prize! If you don't click on a button, the game will skip it in 10 seconds.

Buttons clicked: 17/20
Time elapsed: 27.6 sec

CLICK ME

f Like 1

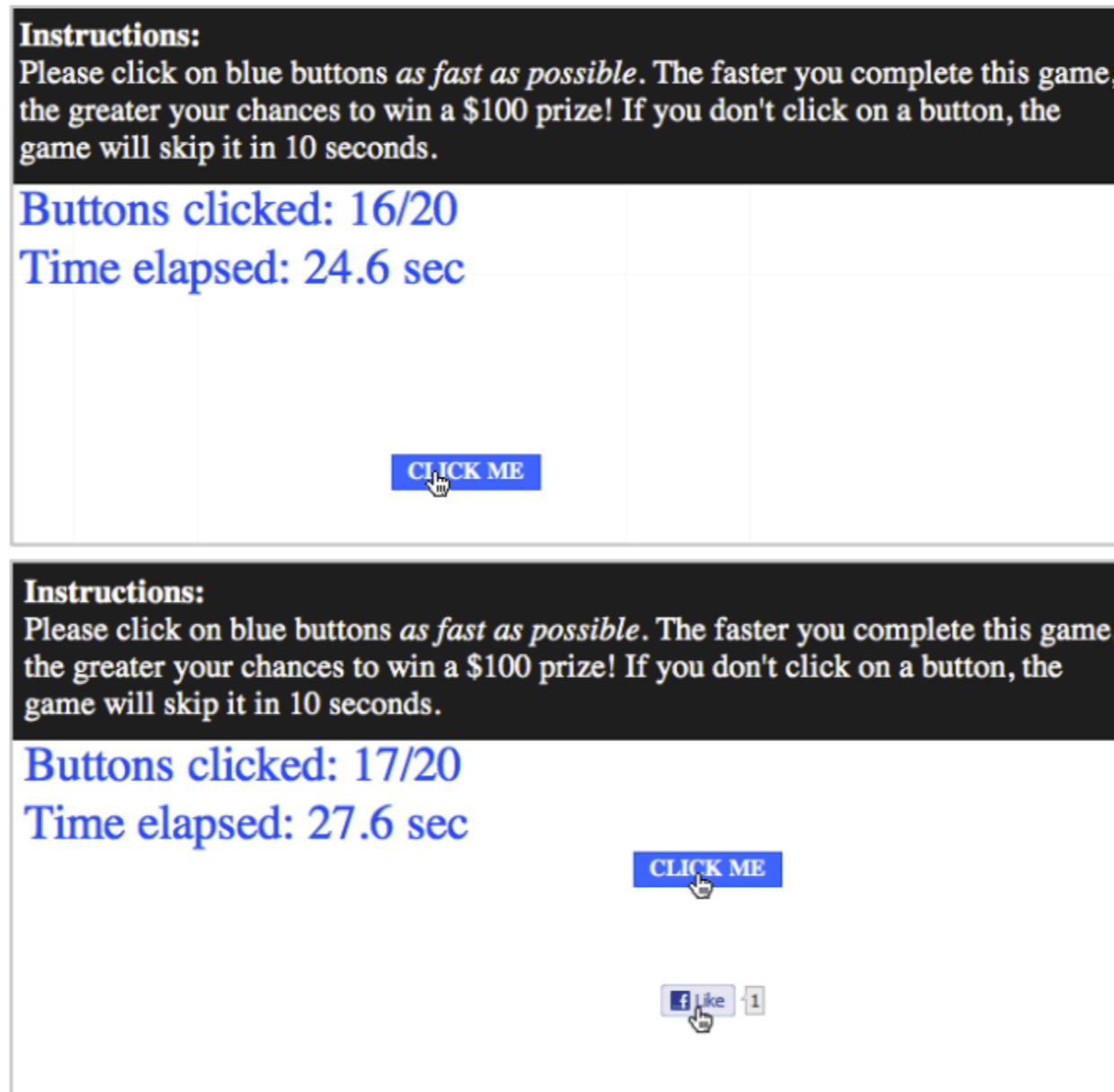


Figure 3: **Whack-a-mole attack page.** *This is a cursor spoofing variant of the whack-a-mole attack. On the 18th trial, the attacker displays the target Like button underneath the actual pointer.*

CLICKJACKING: EXPERIMENTS

Treatment Group	Total	Timeout	Quit	Attack Success	Attack Success (On 1st Mouseover)	Attack Success (Filter by Survey)
1a. Attack without clickjacking	84	1	0	83 (98%)	N/A	42/43 (97%)
1b. Attack without clickjacking (webcam)	71	1	1	69 (97%)	N/A	13/13 (100%)
2. Attack with timing	84	3	1	80 (95%)	80 (95%)	49/50 (98%)
3. Attack with cursor-spoofing	84	0	1	83 (98%)	78 (92%)	52/52 (100%)
4a. Combined defense ($M=0\text{px}$)	77	0	1	76 (98%)	42 (54%)	54/54 (100%)
4b. Combined defense ($M=10\text{px}$)	78	10	1	67 (85%)	27 (34%)	45/53 (84%)
4c. Combined defense ($M=20\text{px}$)	73	18	4	51 (69%)	12 (16%)	31/45 (68%)
5. Lightbox + 4c	73	21	0	52 (71%)	10 (13%)	24/35 (68%)
6a. Entry delay ($T_E=250\text{ms}$) + 4c	77	27	4	46 (59%)	6 (7%)	27/44 (61%)
6b. Entry delay ($T_E=500\text{ms}$) + 4c	73	25	3	45 (61%)	3 (4%)	31/45 (68%)
6c. Entry delay ($T_E=1000\text{ms}$) + 4c	71	25	1	45 (63%)	1 (1%)	25/38 (65%)
6d. Entry delay ($T_E=500\text{ms}$) + 4a	77	6	0	71 (92%)	16 (20%)	46/49 (93%)
7. Lightbox + 6b	73	19	0	54 (73%)	6 (8%)	34/46 (73%)

Table 4: Results of the whack-a-mole attack.

98% of participants were vulnerable to Likejacking de-anonymization under the attack that combined whack-a-mole with cursor-spoofing. Several defenses showed a dramatic drop in attack success rates, reducing them to as low as 1% when filtered by first mouseover events.

PHISHING

PHISHING

- The attacker pretends to be someone (or something) they are not....
 - Email addresses that look like someone else
 - Domain names that look like real ones
- ...In an attempt to gain information/access
 - "Email your password"
 - "Enter your credit card number"

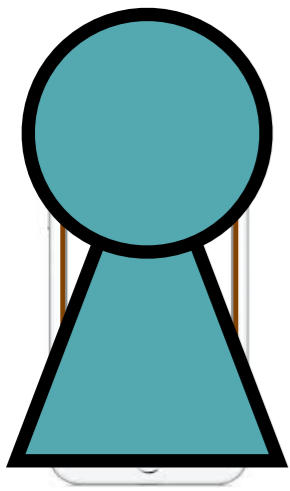
TYPES OF PHISHING

- “Phishing” generally casts a wide net
 - Generally has little to no domain-specific information
 - E.g., emails that appear to come from Apple, asking for appleid passwords
 - Broader audience, less likely to fall for it
- “Spearphishing” is more targeted
 - Exploits domain knowledge
 - E.g., “I’m your TA; we need the keys for your project”
 - Narrower audience, more likely to fall for it

DEFENDING AGAINST PHISHING

- **Training**
 - Try to educate users to identify and avoid
 - Many companies internally phish; if you fall for it once, you get a warning — if you fall for it twice, you go to mandatory training
- **Automated detection**
 - Can we identify phishing and filter it?
 - Can we make it **harder for the attacker to do?**

AN EXAMPLE RESEARCH PROBLEM, END-TO-END



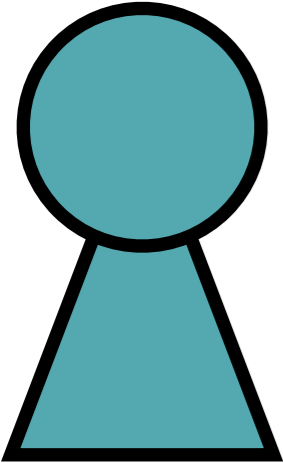
My wife



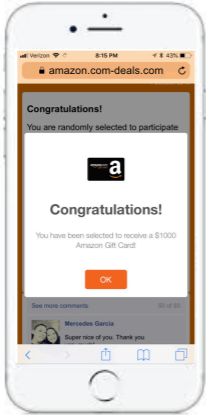
Me

AN EXAMPLE RESEARCH PROBLEM, END-TO-END

Is this actually Amazon?



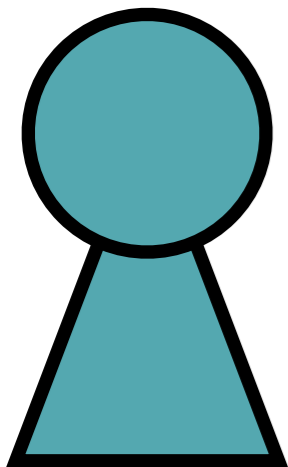
My wife



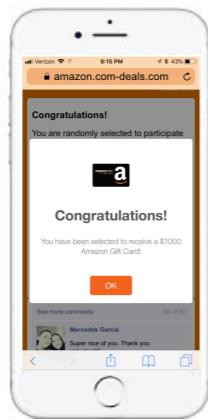
Me

AN EXAMPLE RESEARCH PROBLEM, END-TO-END

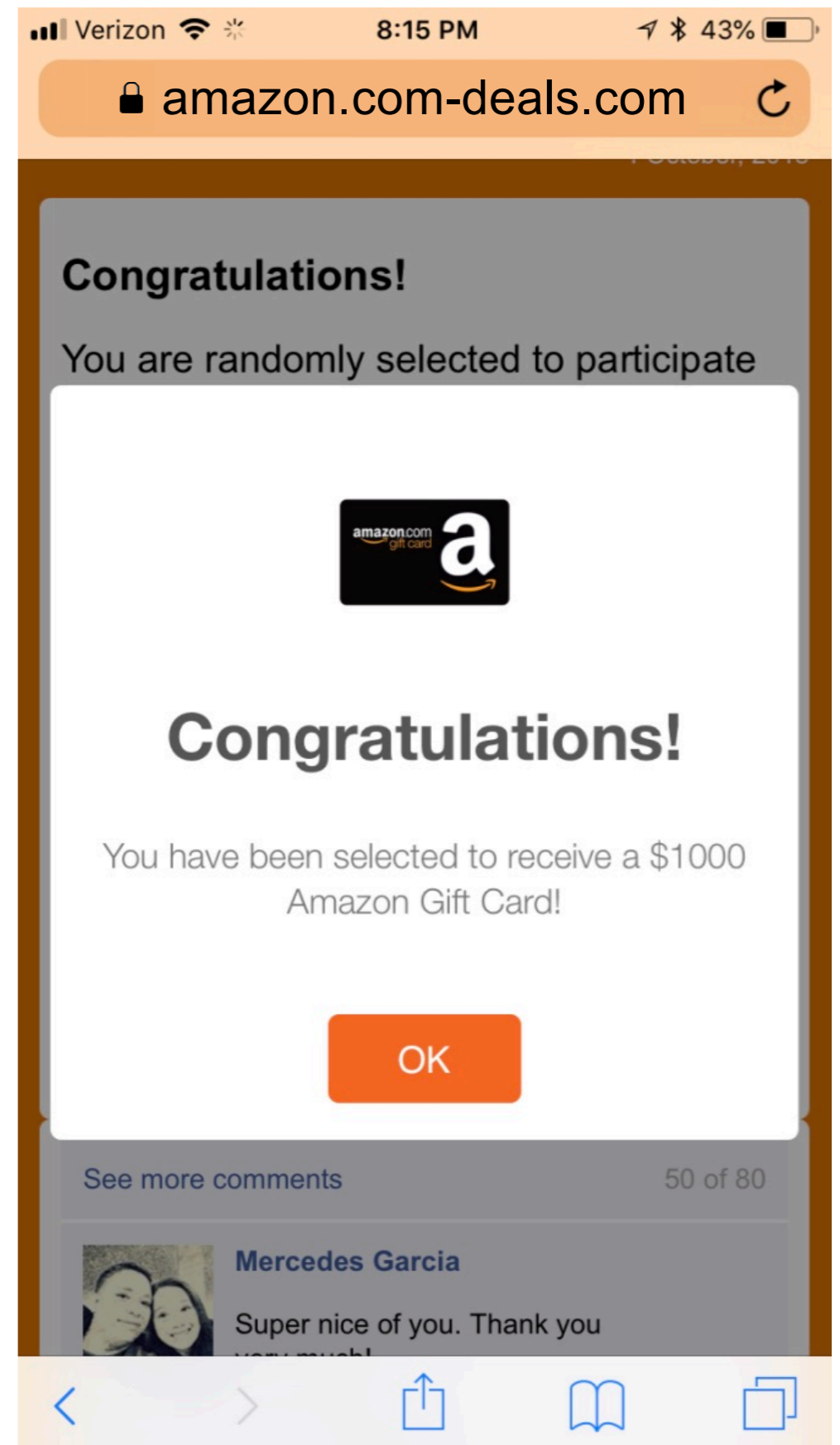
Is this
actually
Amazon?



My wife



Me



MAKING AN OBSERVATION

🔒 amazon.com-deals.com



Me

MAKING AN OBSERVATION

🔒 amazon.com-deals.com



The apparent website



Me

MAKING AN OBSERVATION

The *actual* website

🔒 amazon.com-deals.com

The *apparent* website



Me

MAKING AN OBSERVATION

🔒 amazon.com-deals.com



Me

MAKING AN OBSERVATION

 amazon.com-deals.com



Me

What does this mean to you?

MAKING AN OBSERVATION

 amazon.com-deals.com



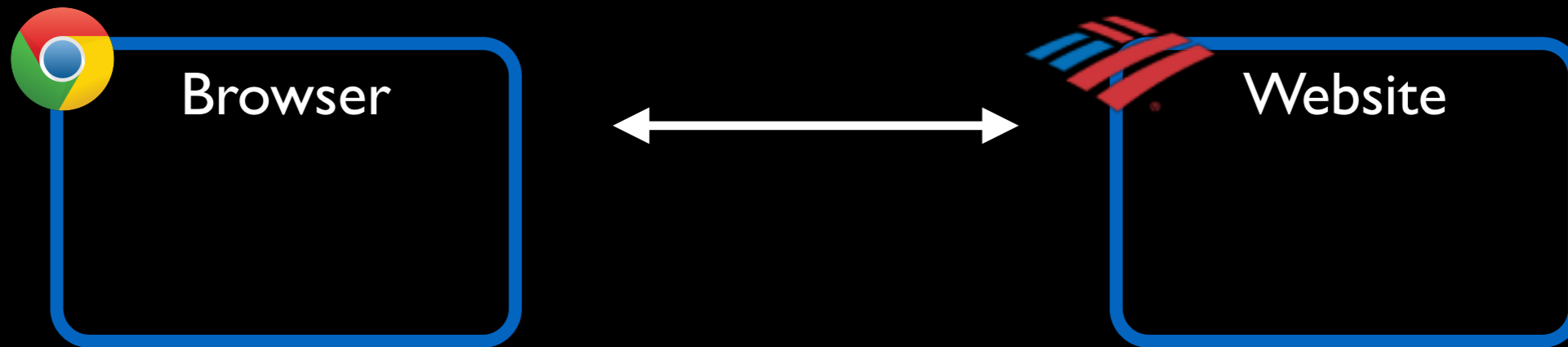
Me

What does this mean to you?

0. Learn from other people's work

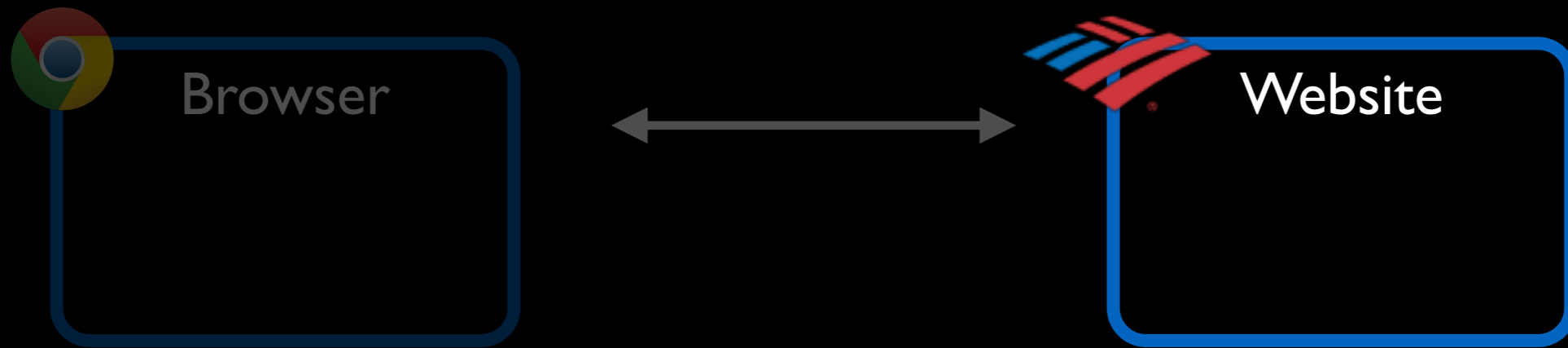
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



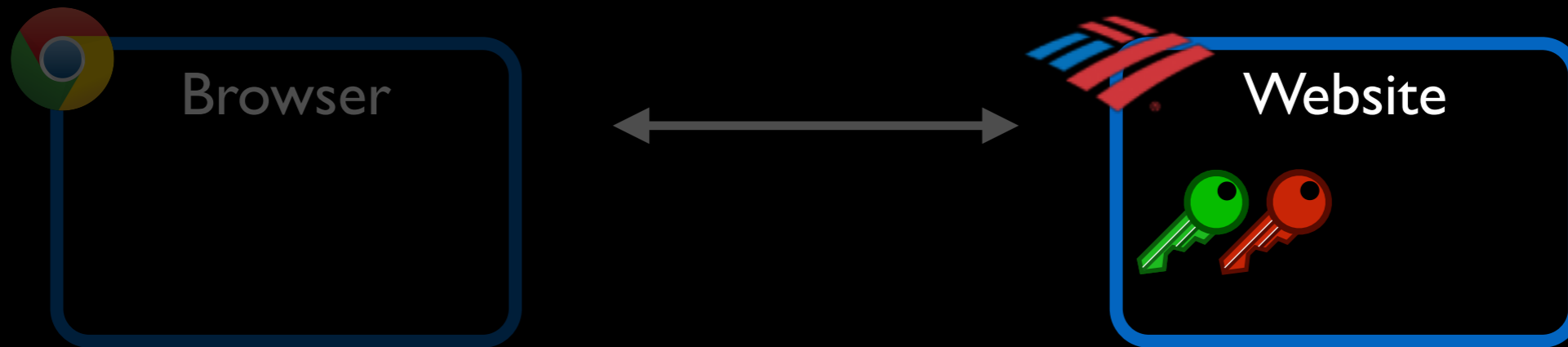
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



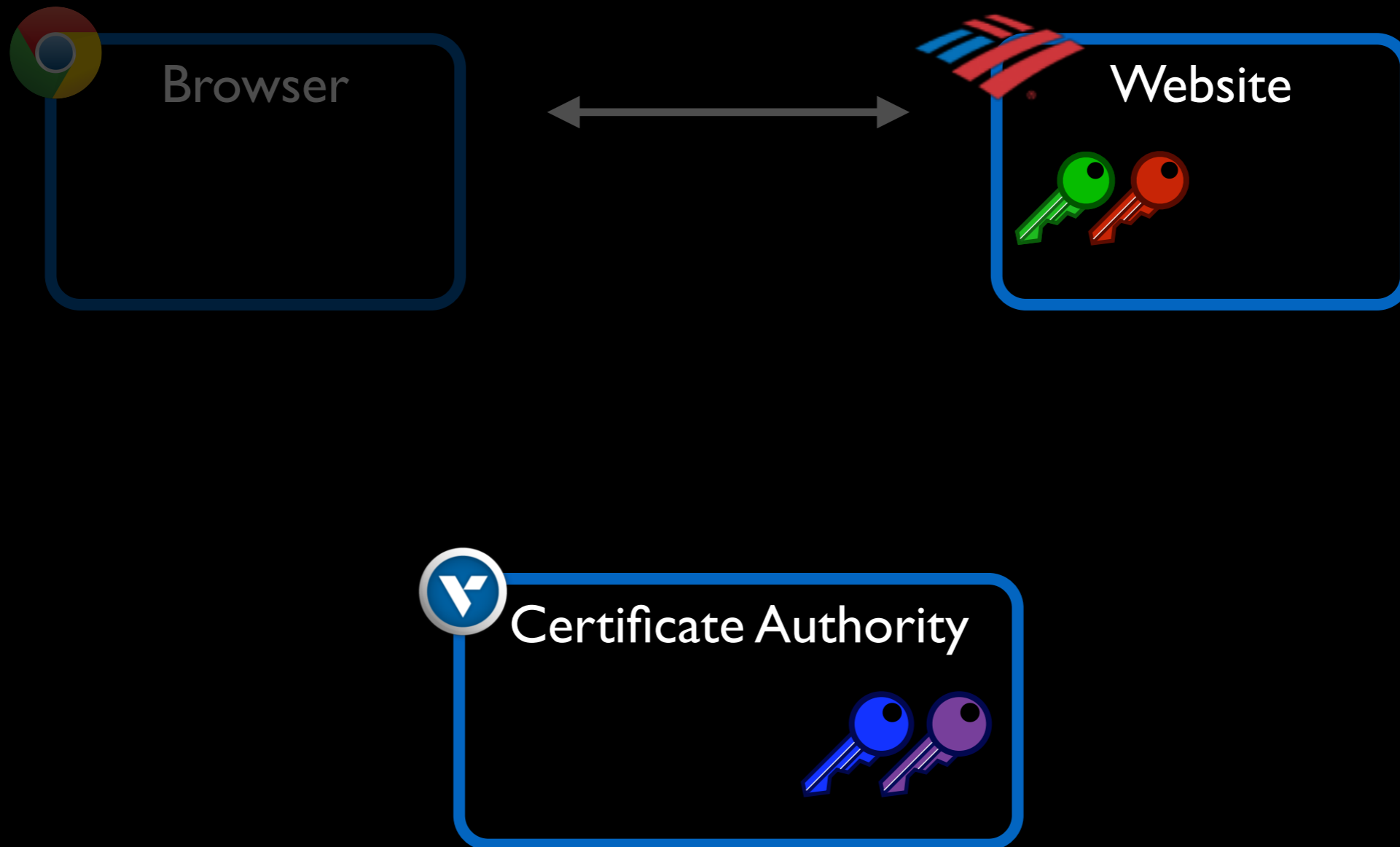
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



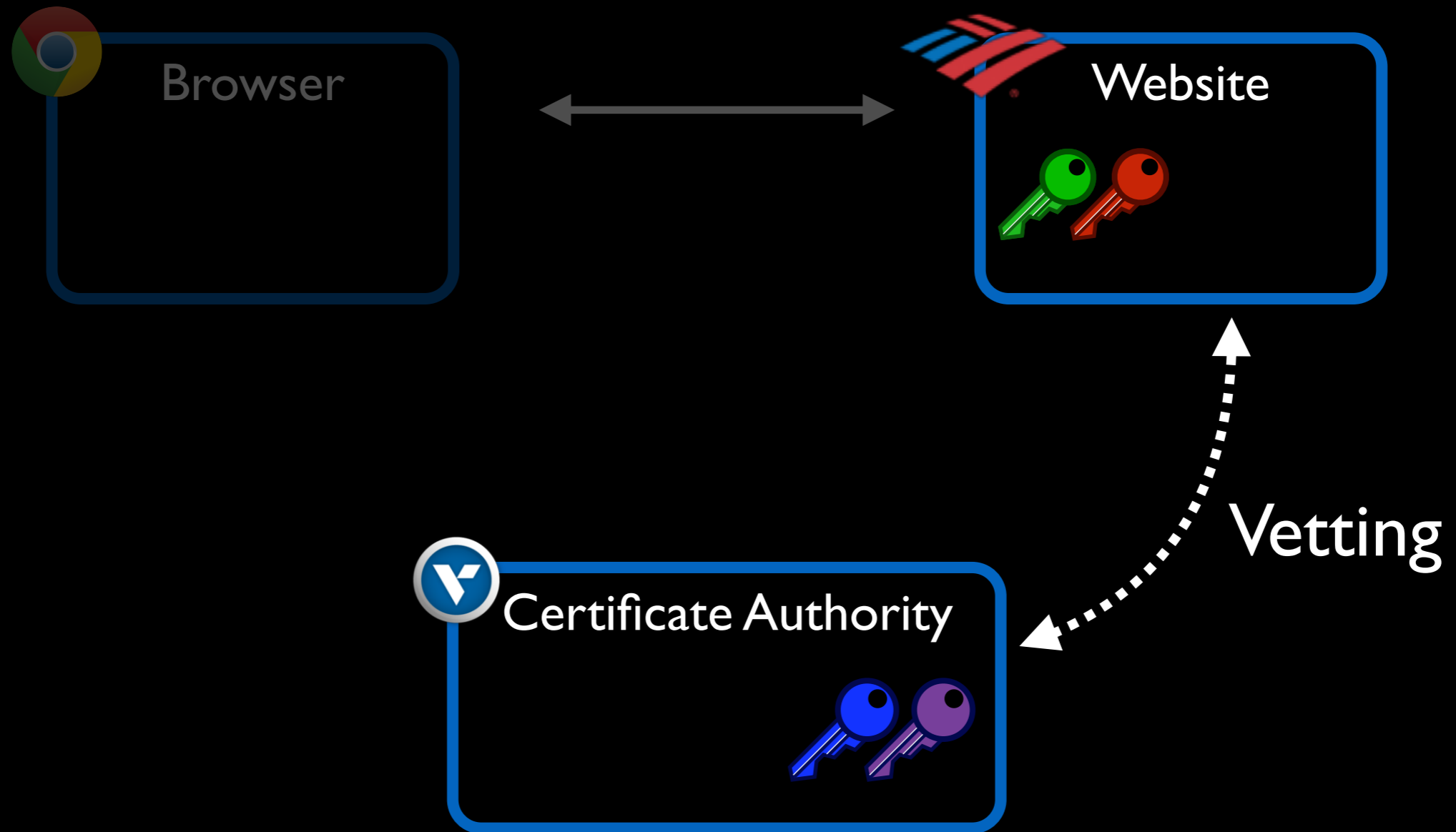
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



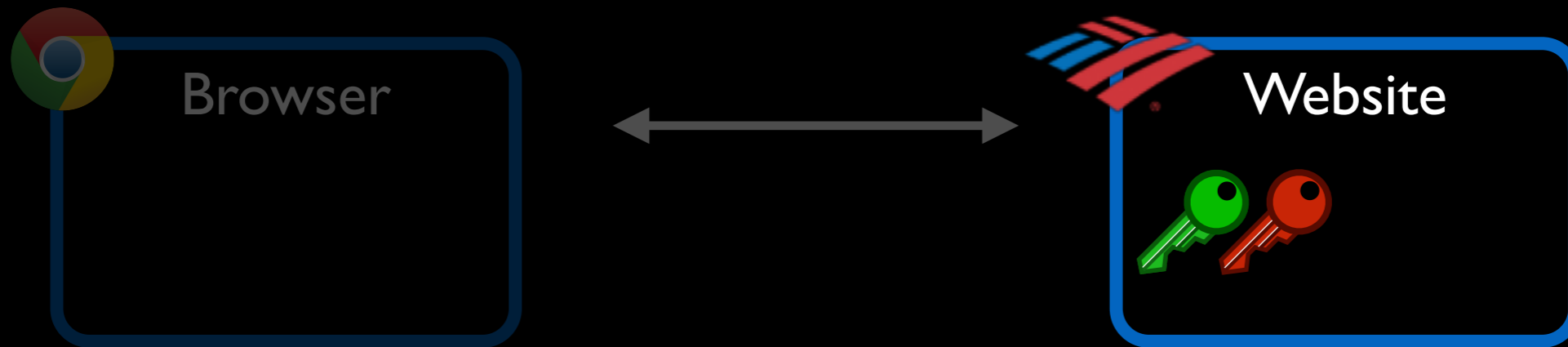
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



Public Key Infrastructures (PKIs)

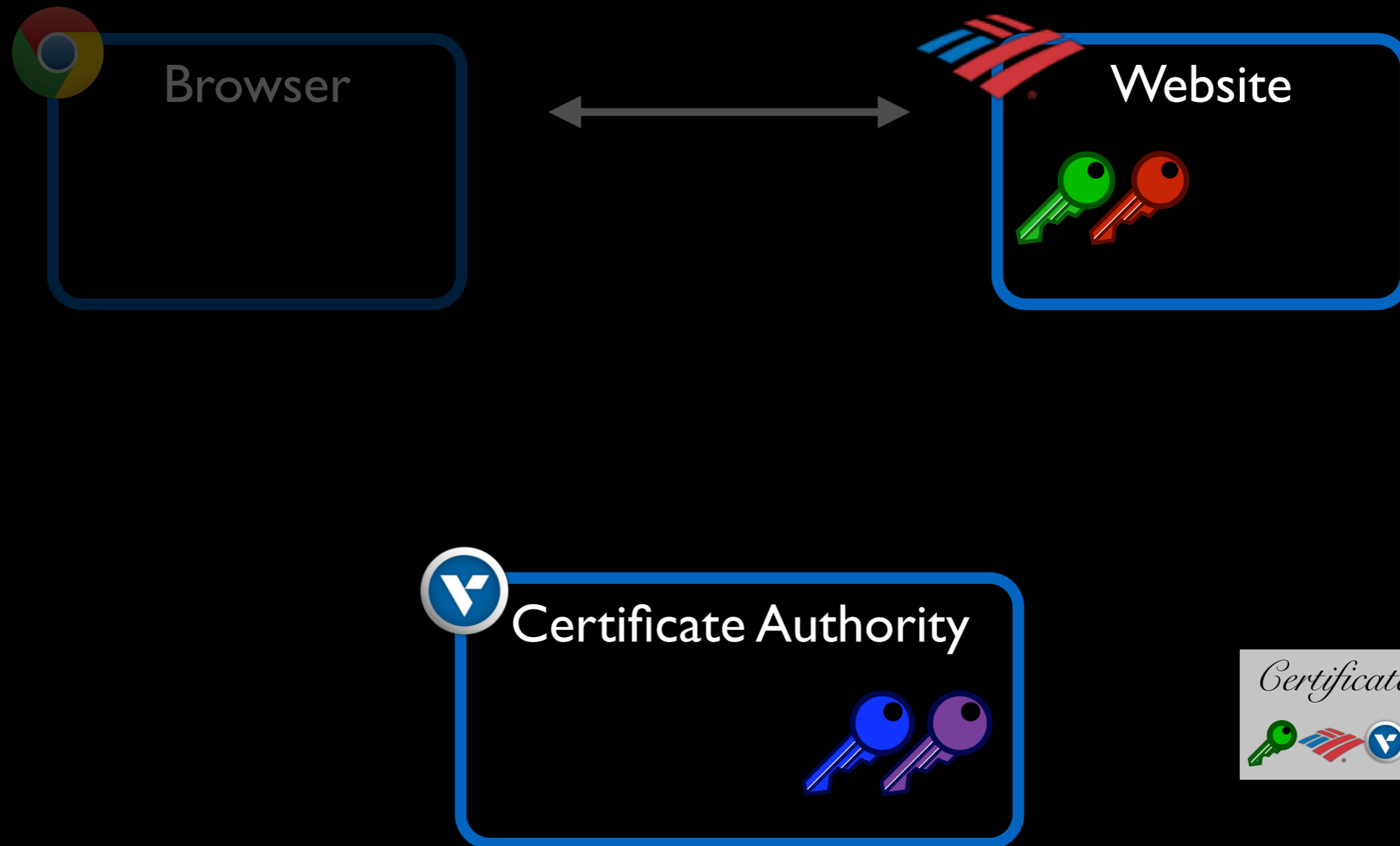
How can users truly know with whom they are communicating?



Certificate

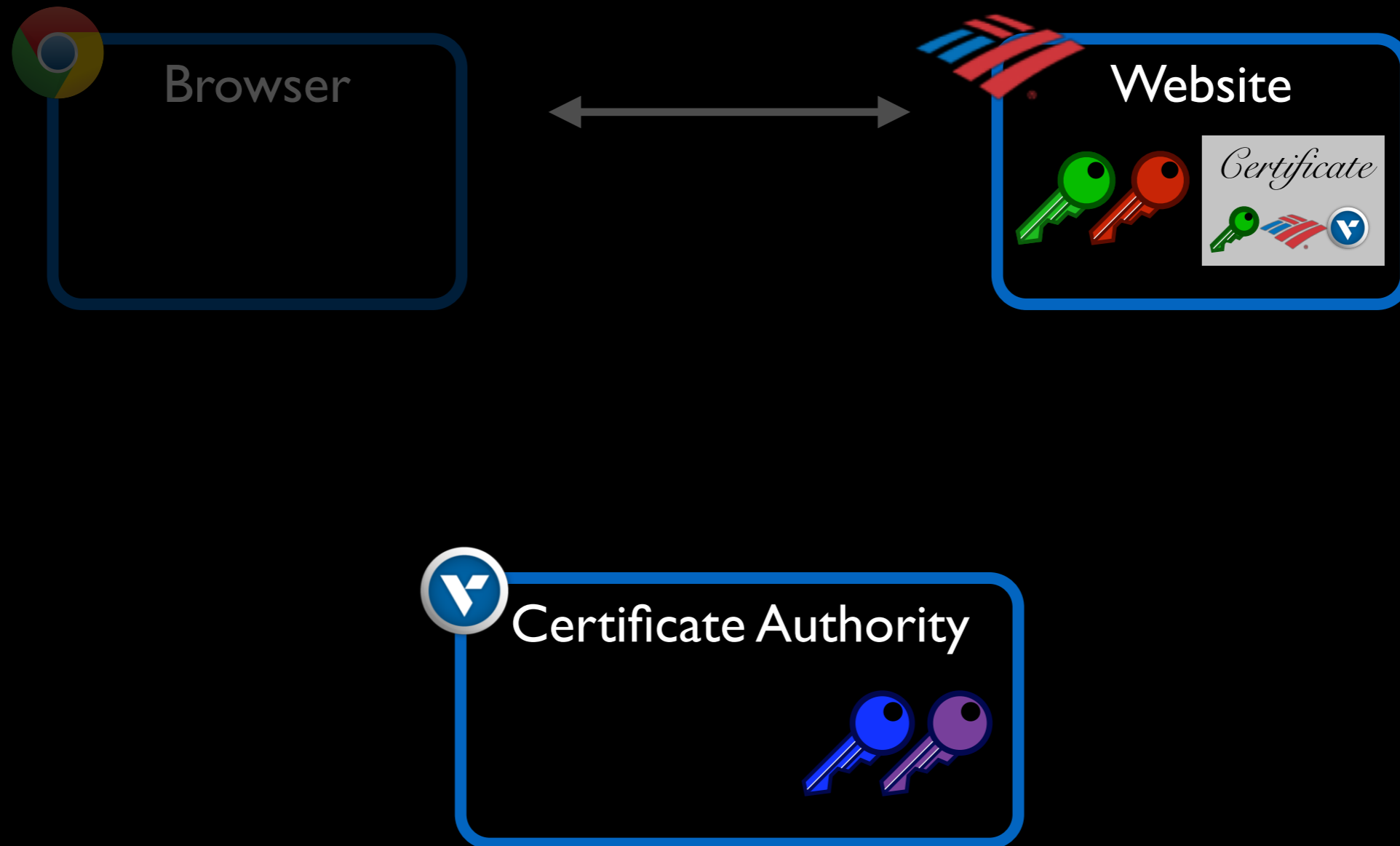
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



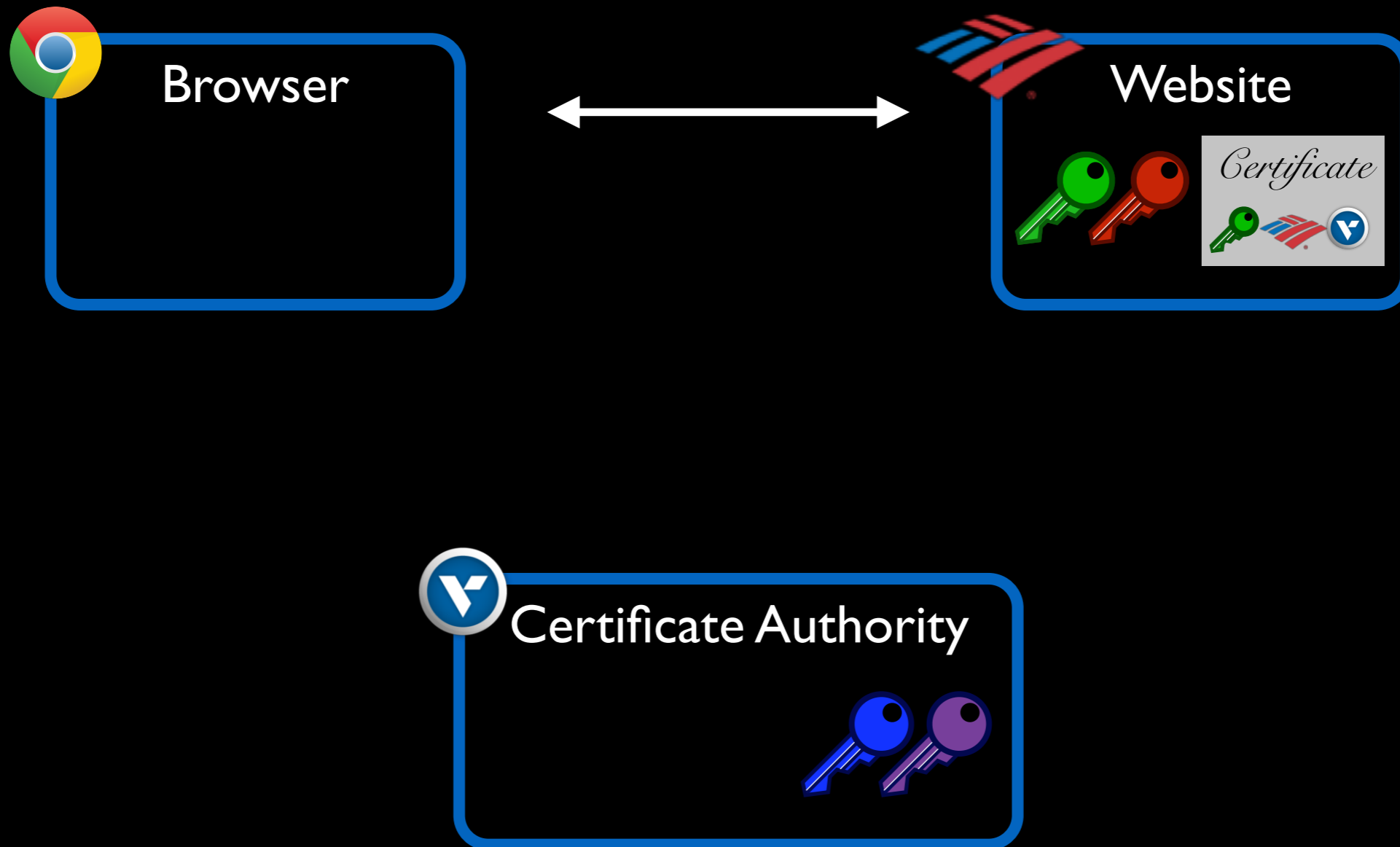
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



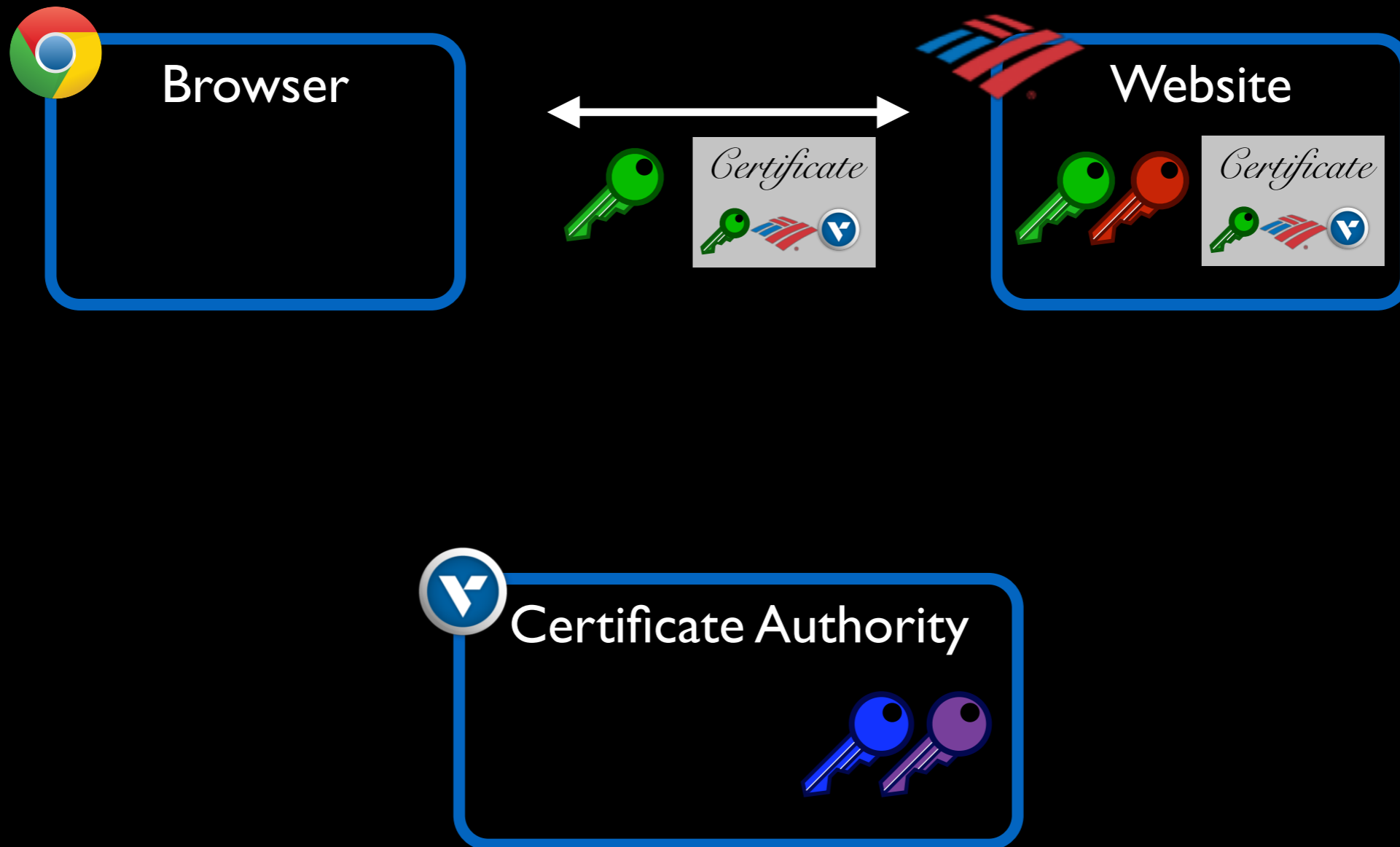
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



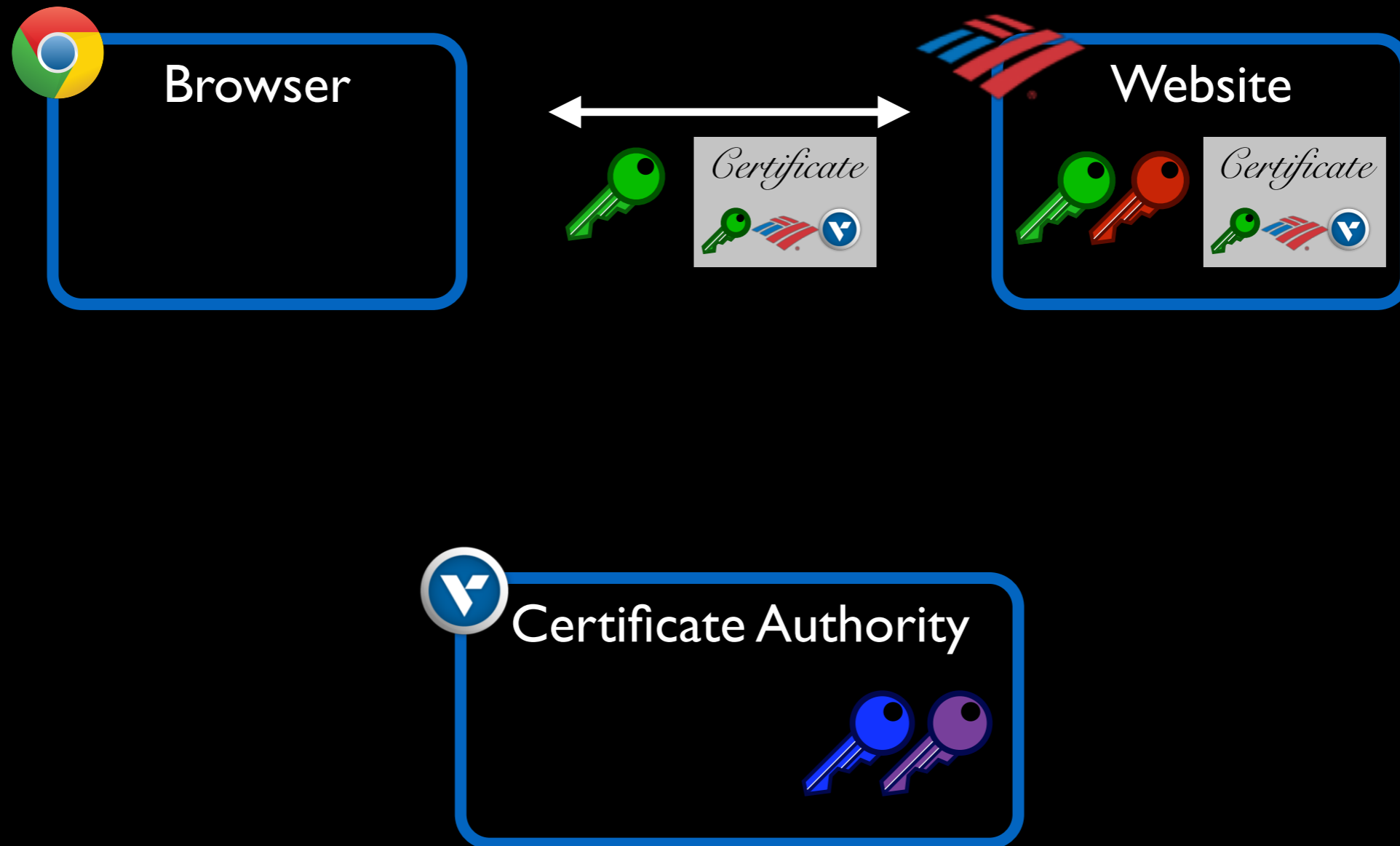
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



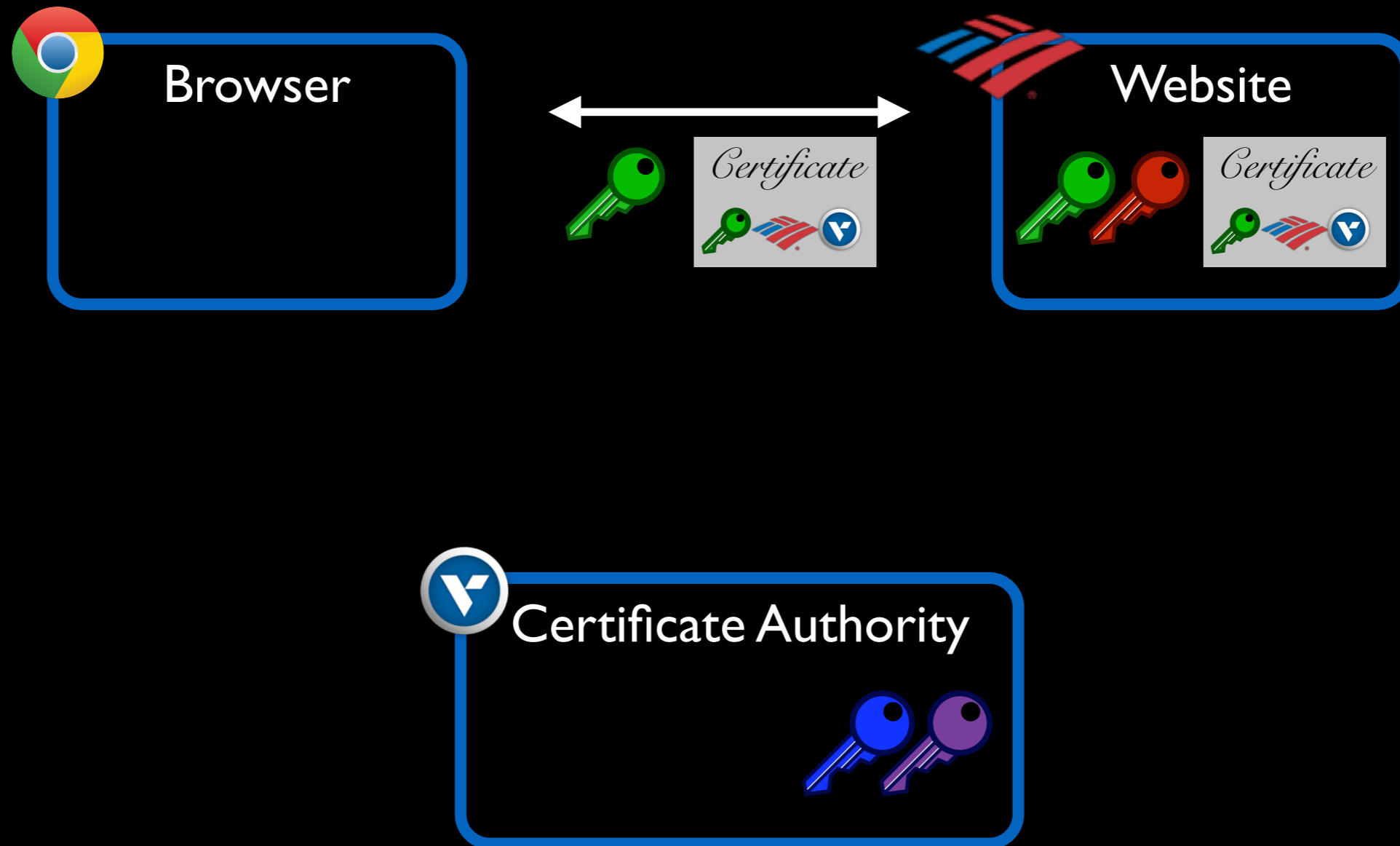
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



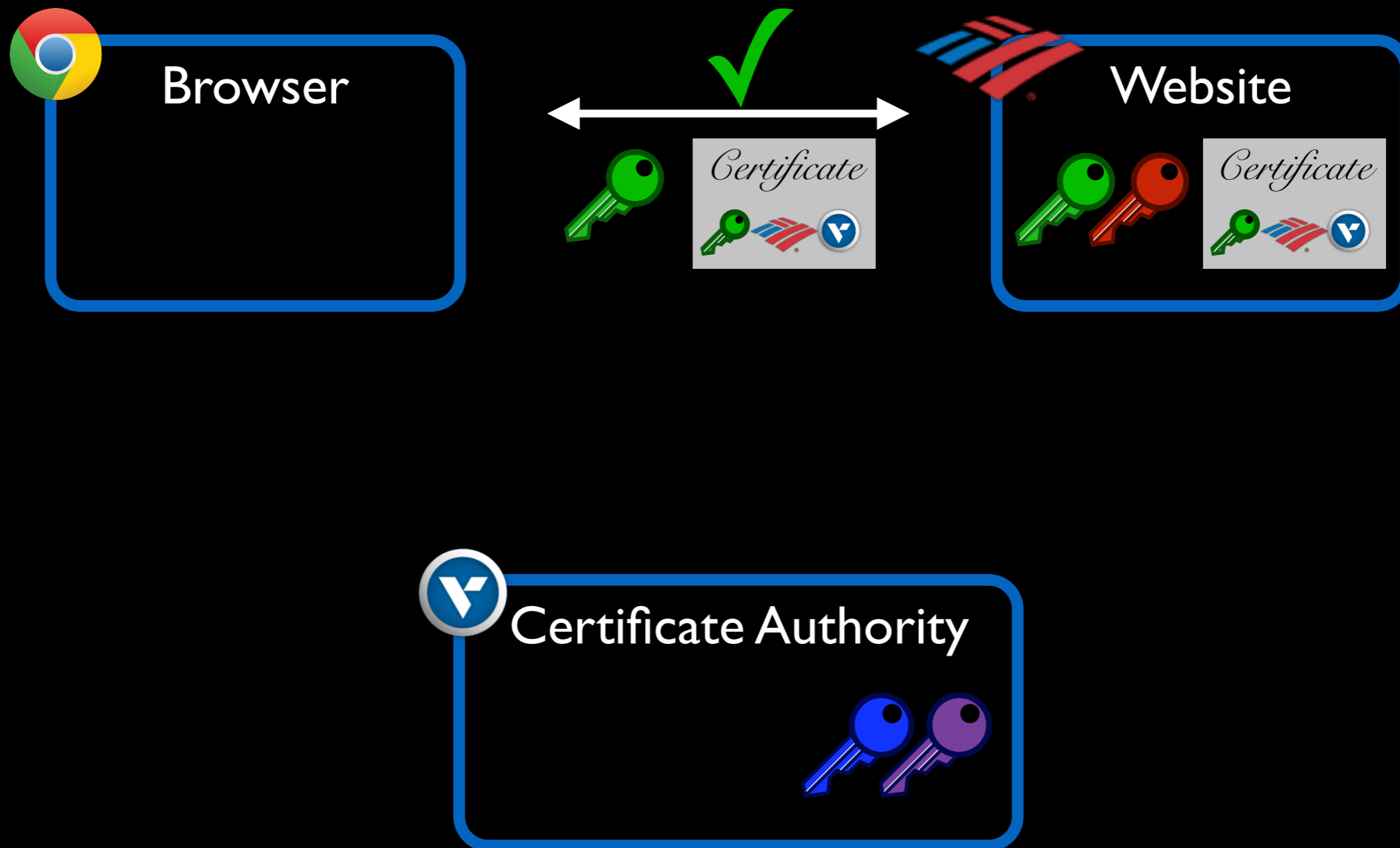
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



MAKING AN OBSERVATION

🔒 amazon.com-deals.com



Me

MAKING AN OBSERVATION



Me

 amazon.com-deals.com

What does this mean to you?

MAKING AN OBSERVATION

Somehow, com-deals.com got a certificate that looks like amazon.com

 amazon.com-deals.com



Me

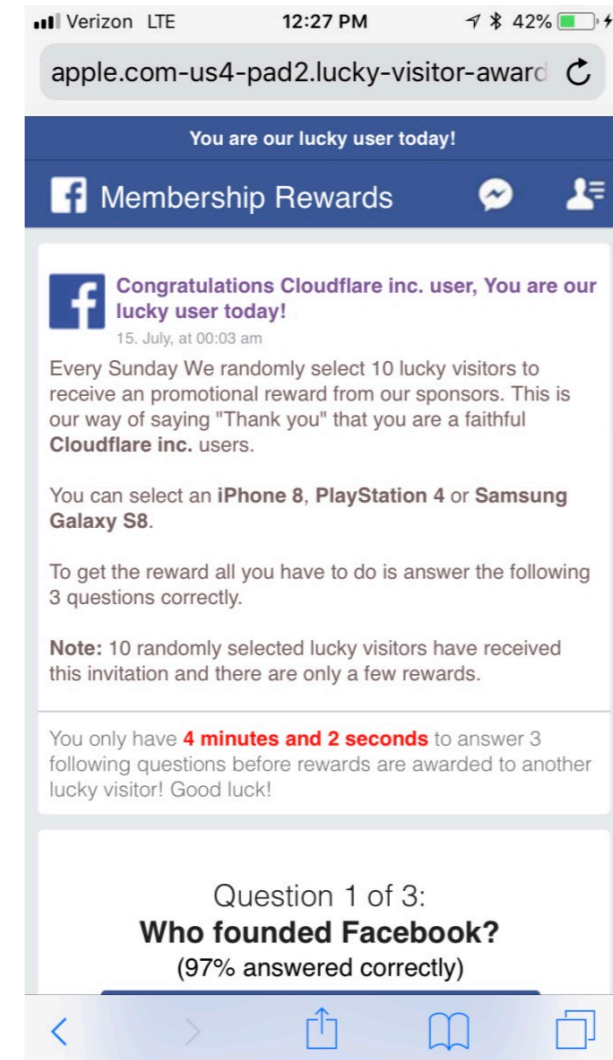
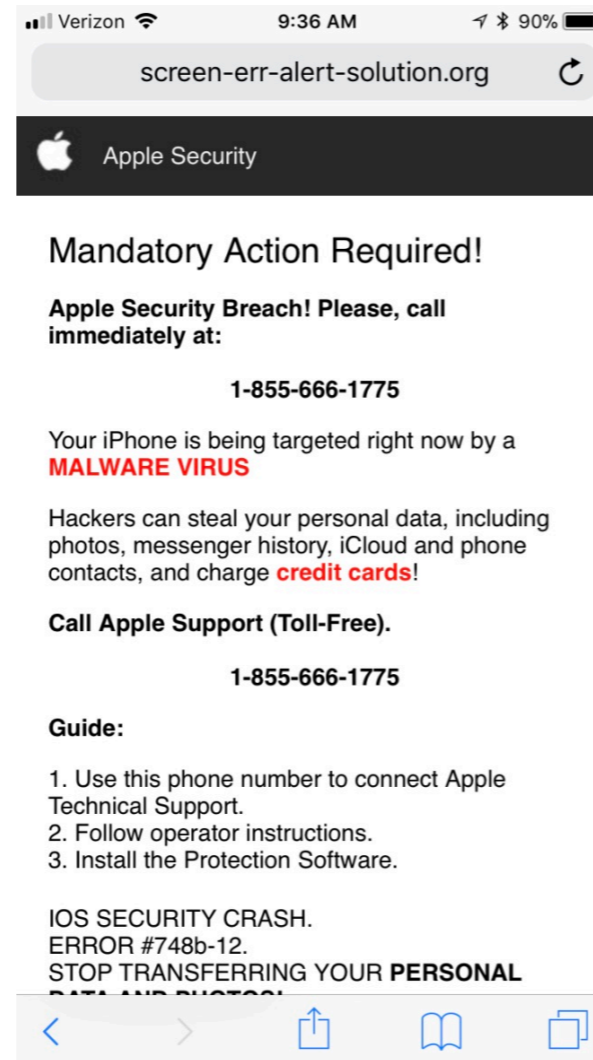
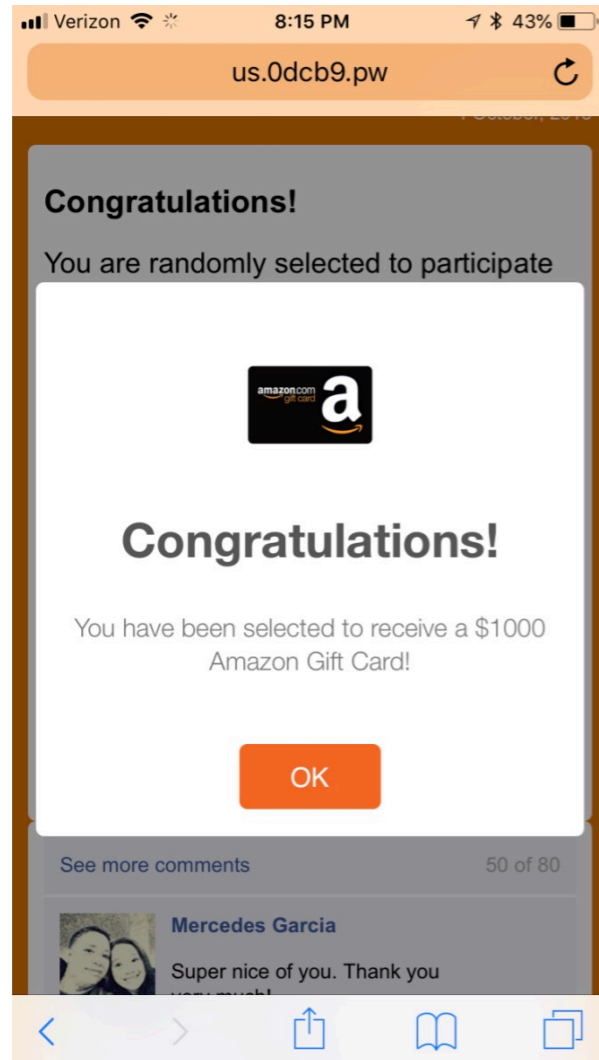
What does this mean to you?

MAKING AN OBSERVATION

This appears to be prevalent

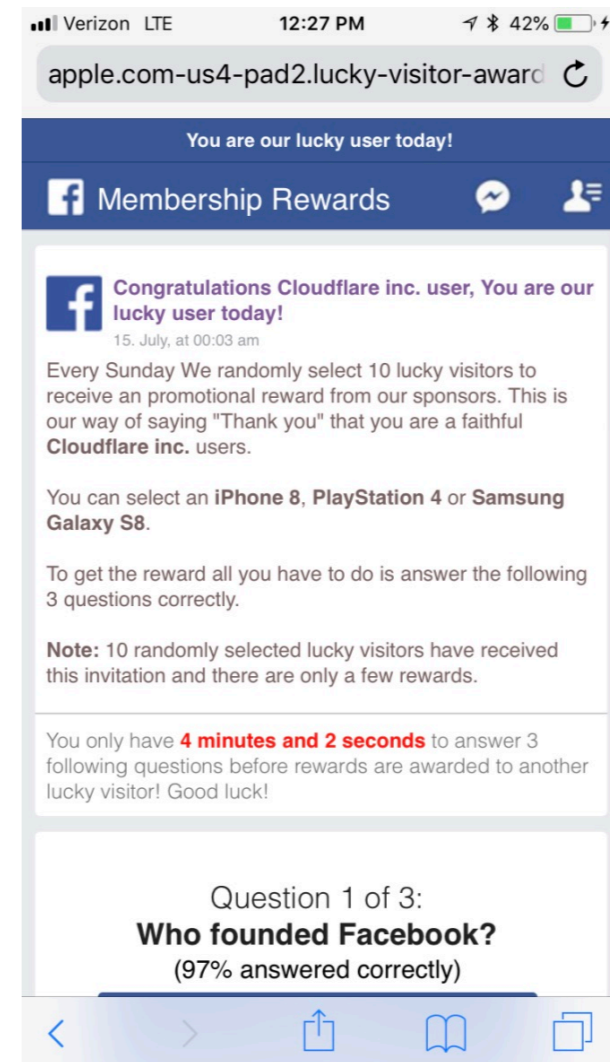
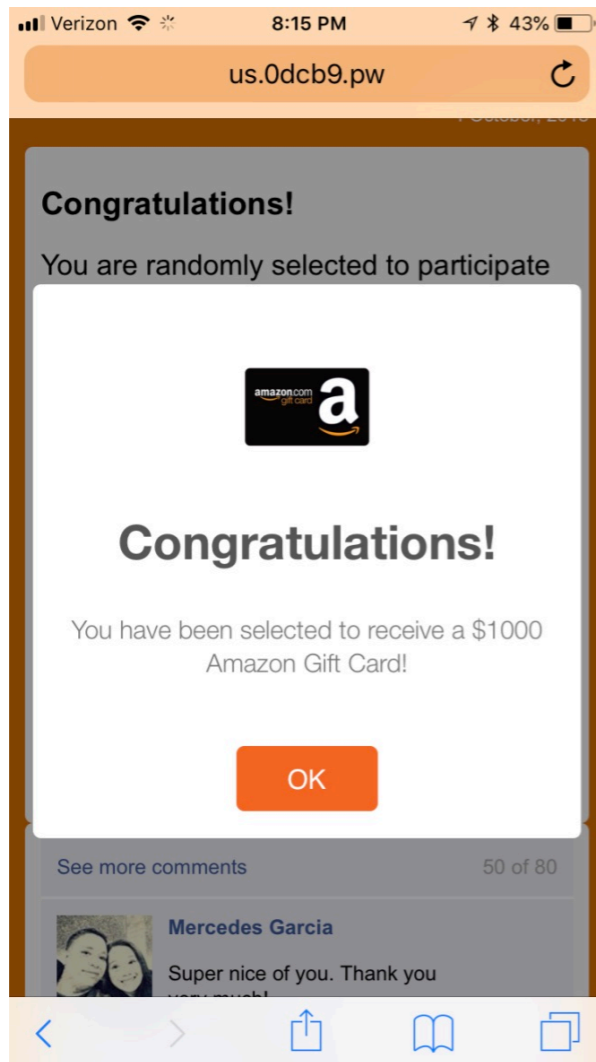
MAKING AN OBSERVATION

This appears to be prevalent



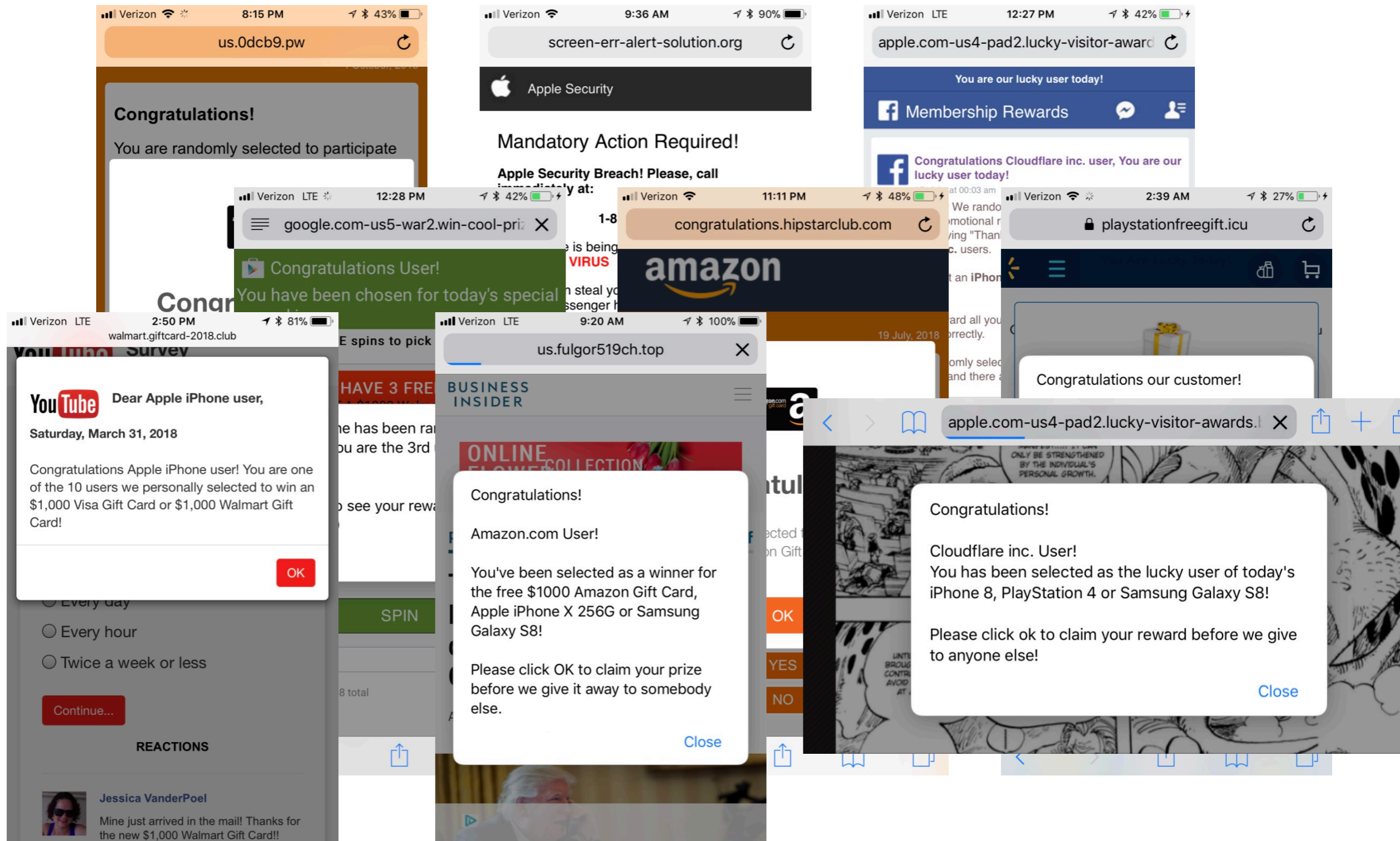
MAKING AN OBSERVATION

This appears to be prevalent...like *really* prevalent



MAKING AN OBSERVATION

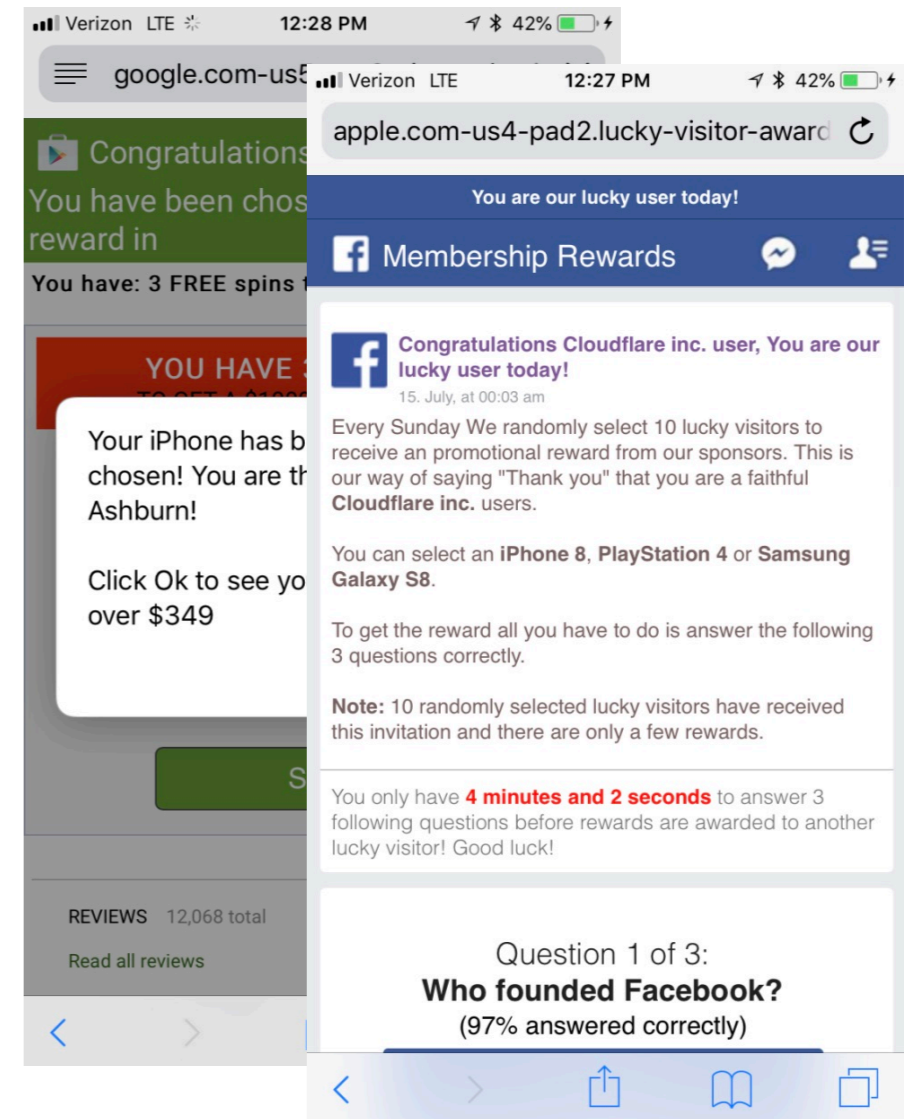
This appears to be prevalent...like *really* prevalent



The *actual* website

 amazon.com-deals.com

The *apparent* website

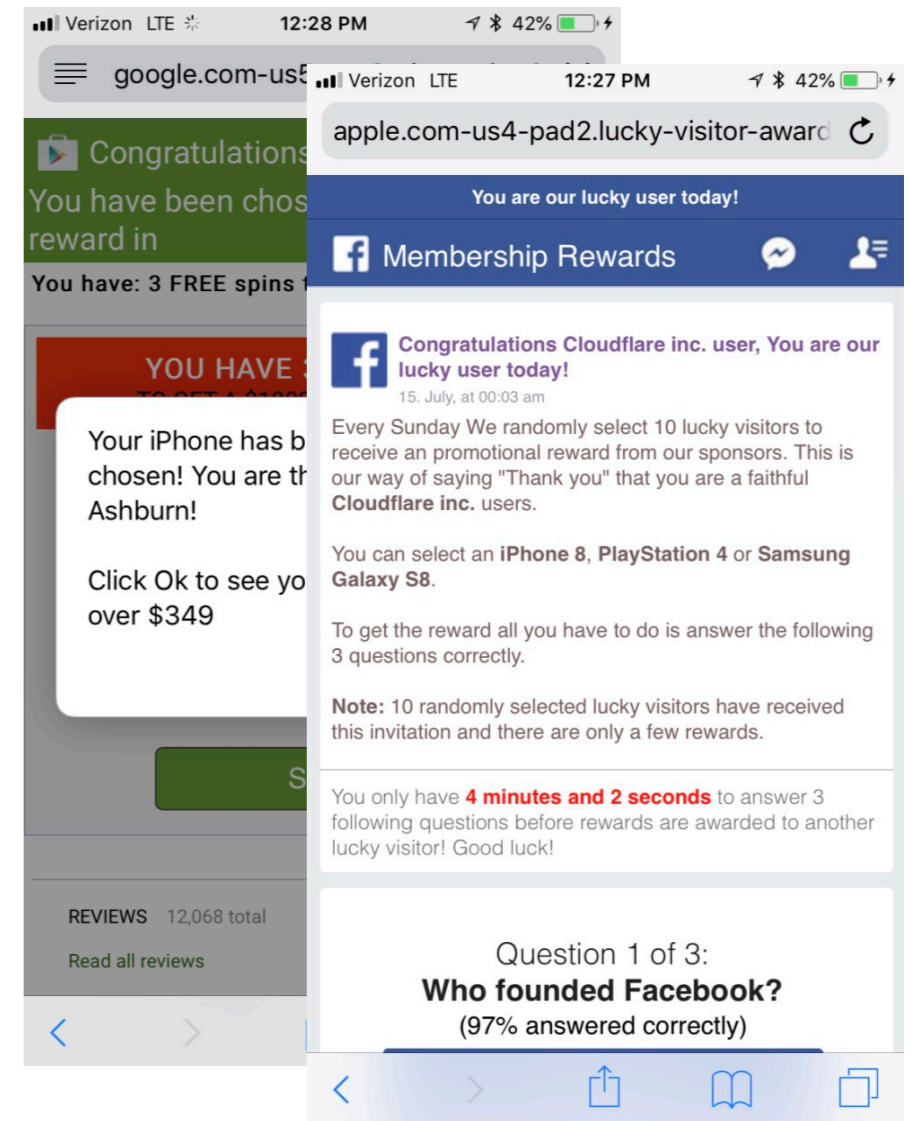


The *actual* website

 amazon.com-deals.com

The *apparent* website

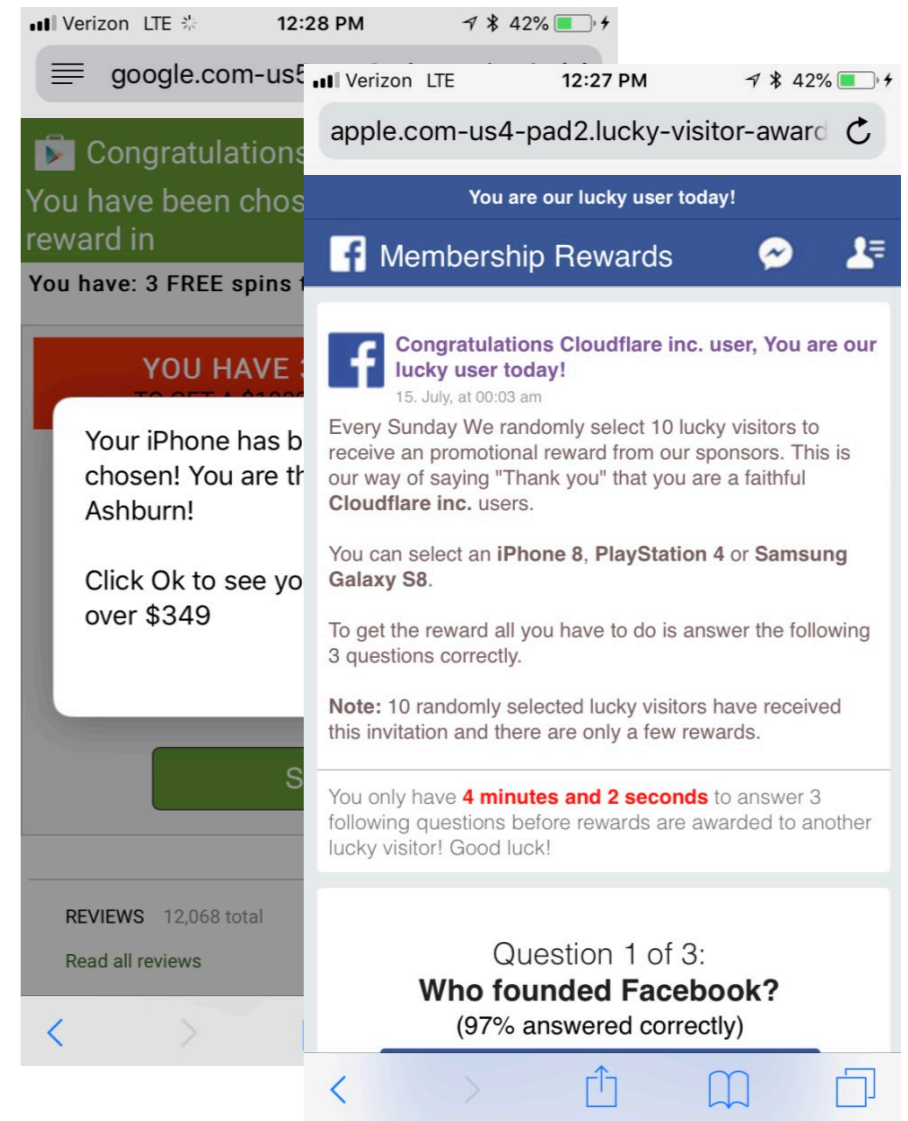
ASKING A QUESTION



The *actual* website

amazon.com-deals.com

The *apparent* website



ASKING A QUESTION

WHAT DO YOU THINK ARE SOME GOOD QUESTIONS WE COULD ASK?

ASKING SOME QUESTIONS

ASKING SOME QUESTIONS

How often does this happen?

ASKING SOME QUESTIONS

How often does this happen?

Who is giving these attackers certificates?

ASKING SOME QUESTIONS

How often does this happen?

When it happens, does it tend to be malicious?

Who is giving these attackers certificates?

ASKING SOME QUESTIONS

How often does this happen?

When it happens, does it tend to be malicious?

Who is giving these attackers certificates?

What can we do to stop this kind of attack?

HOW DO WE ANSWER THESE QUESTIONS?

How often does this happen?

When it happens, does it tend to be malicious?

Who is giving these attackers certificates?

What can we do to stop this kind of attack?

HOW DO WE ANSWER THESE QUESTIONS?

How often does this happen?

When it happens, does it tend to be malicious?

Who is giving these attackers certificates?

What can we do to stop this kind of attack?

WE NEED A DATASET

HOW DO WE ANSWER THESE QUESTIONS?

How often does this happen?

When it happens, does it tend to be malicious?

Who is giving these attackers certificates?

What can we do to stop this kind of attack?

WE NEED A DATASET

GET *ALL* OF THE CERTIFICATES!

RESEARCH DATASETS

If it doesn't exist, collect it

If it does exist, download it

If you do something new with the data, share it

RESEARCH DATASETS

If it doesn't exist, collect it

If it does exist, download it

If you do something new with the data, share it

**PART OF BEING A GOOD RESEARCHER IS KNOWING
WHAT DATA IS OUT THERE (EXPERIENCE WITH TIME)**

RESEARCH DATASETS

If it doesn't exist, collect it

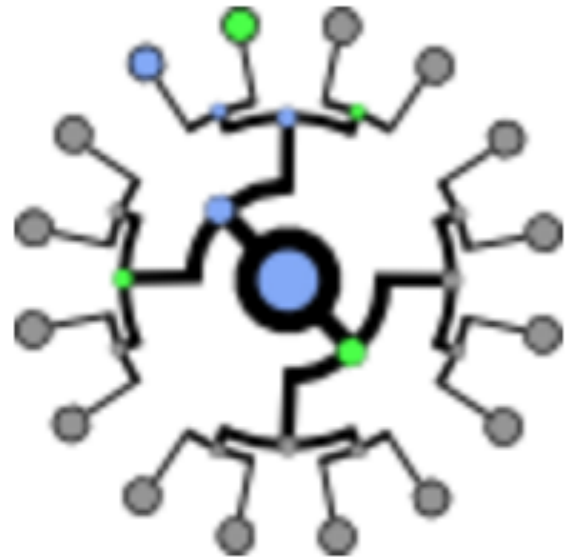
If it does exist, download it

If you do something new with the data, share it

**PART OF BEING A GOOD RESEARCHER IS KNOWING
WHAT DATA IS OUT THERE (EXPERIENCE WITH TIME)**

YOUR ADVISOR WILL HELP WITH THIS

CERTIFICATE DATASETS



Certificate Transparency

RAPID7



censys

**IT IS NOW POSSIBLE TO DOWNLOAD
ALL KNOWN CERTIFICATES ON THE WEB!**

DEVisING A SOLUTION

DEVISING A SOLUTION

Certificate dataset **C**

Each certificate has ≥ 1 domain name

315,284,603 total domain names

amazon.com-deals.com

DEVISING A SOLUTION

Certificate dataset **C**

Each certificate has ≥ 1 domain name

315,284,603 total domain names

Website popularity dataset **P**

Alexa top-10,000 most popular websites

amazon.com-deals.com

google.com
youtube.com
amazon.com

DEVisING A SOLUTION

Certificate dataset **C**

Each certificate has ≥ 1 domain name

315,284,603 total domain names

Website popularity dataset **P**

Alexa top-**10,000** most popular websites

We need an algorithm

Search in each certificate in **C** for a popular website from **P**

amazon.com-deals.com

google.com

youtube.com

amazon.com

DEVisING A SOLUTION

Certificate dataset **C**

Each certificate has ≥ 1 domain name

315,284,603 total domain names

Website popularity dataset **P**

Alexa top-**10,000** most popular websites

We need an algorithm

Search in each certificate in **C** for a popular website from **P**

amazon.com-deals.com

× google.com

× youtube.com

✓ amazon.com

DEVisING A SOLUTIOn

Certificate dataset **C**

Each certificate has ≥ 1 domain name

315,284,603 total domain names

Naive algorithm

Website popularity dataset **P**

3.15 Trillion checks!

Alexa top-10,000 most popular websites

We need an algorithm

Search in each certificate in **C** for a popular website from **P**

amazon.com-deals.com

× google.com

× youtube.com

✓ amazon.com

ANALYZING A DATASET

How often does this happen?

When it happens, does it tend to be malicious?

Who is giving these attackers certificates?

What can we do to stop this kind of attack?

As you analyze a dataset, it is important to really understand the results and the outliers

WHO IS BEING IMPERSONATED?

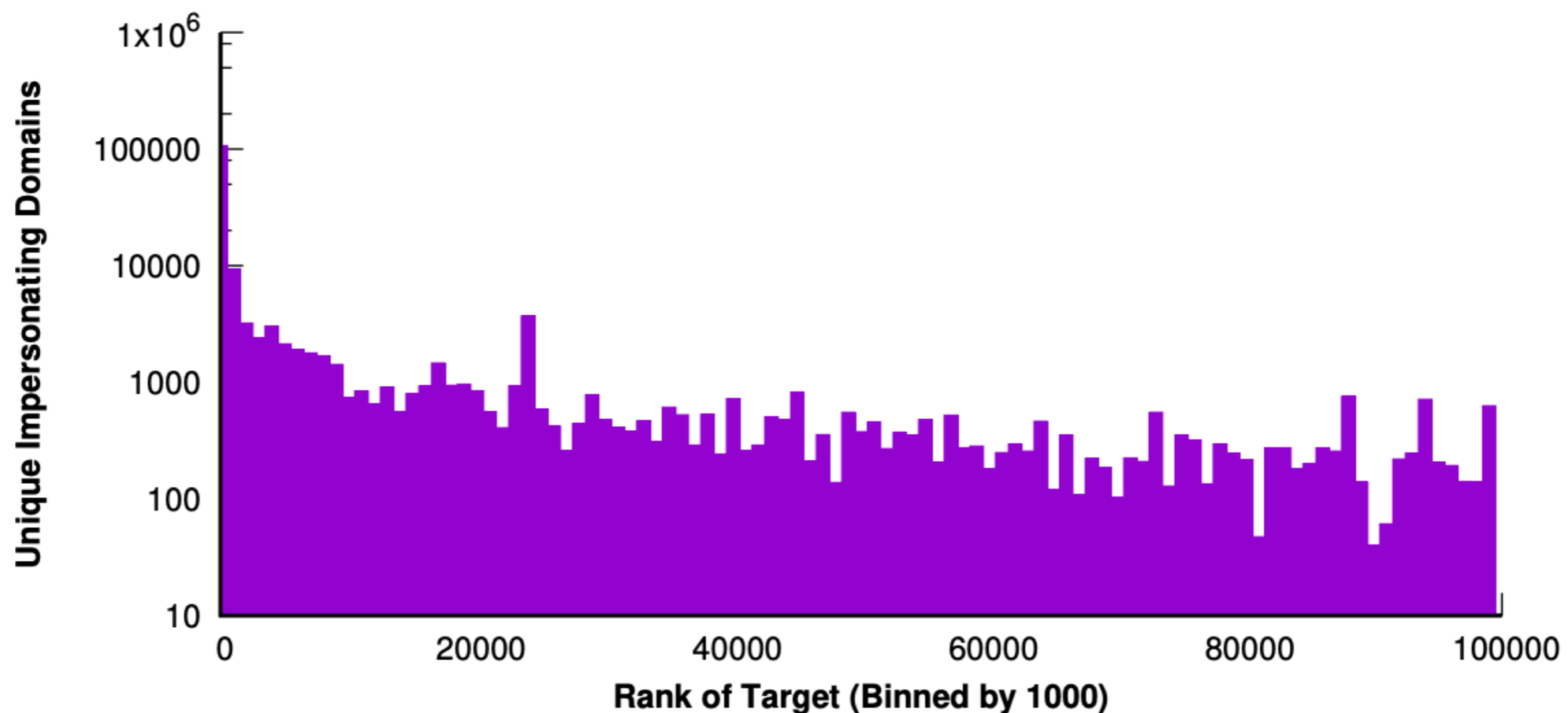


Fig. 2: Number of unique impersonating domains as a function of Alexa rank (binned by 1,000). The long tail indicates that many domains were targeted a small number of times.

WHO IS BEING IMPERSONATED?

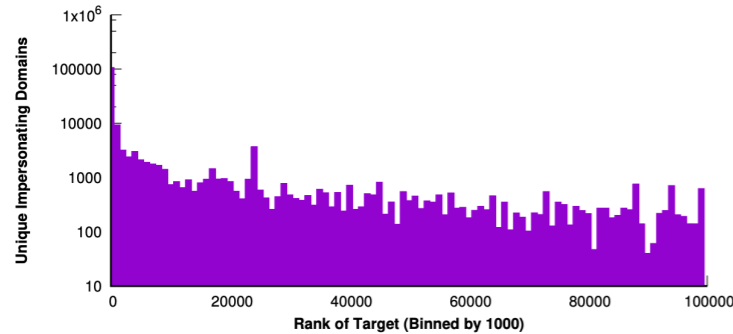


Fig. 2: Number of unique impersonating domains as a function of Alexa rank (binned by 1,000). The long tail indicates that many domains were targeted a small number of times.

Domain	Unique Domains	Alexa Rank
apple.com	43,291	77
paypal.com	26,269	78
icloud.com	7,368	408
runescape.com	4,522	1,822
facebook.com	3,276	3
starwars.com	3,073	24,867
google.com	2,506	1
amazon.com	1,655	12
ebay.co.uk	1,145	149
ebay.com	983	36
chase.com	823	183
bankofamerica.com	788	305
mail.ru	703	44
live.com	700	19
banorte.com	690	17,467
mail.com	652	1,804
login.com	645	94,994
dropbox.com	640	120
vk.com	624	16
yandex.ru	571	22
Other	72,397	

TABLE IV: Most commonly impersonated domains, by count of unique complete domains impersonating the target domain.

WHAT TLD'S ARE ATTACKERS USING?

TLD	Unique Domains	Alexa Rank	Censys Rank
.com	48,458	1	1
.info	11,527	11	17
.ga	8,557	146	9
.ml	7,979	133	14
.tk	7,500	83	4
.cf	6,864	157	7
.net	6,047	4	2
.gq	5,654	275	16
.ru	5,421	3	8
.org	3,463	2	5
.online	2,985	63	44
.xyz	2,936	50	13
.top	2,623	72	22
.site	2,449	87	47
.us	2,396	43	27
.cc	2,393	58	78
.bid	2,034	167	65
.me	1,859	29	33
.in	1,546	17	32
.pw	1,483	91	51
Others	39,147		

TABLE V: Most common actual TLDs used by impersonating domains. “Alexa Rank” ranks the TLD by how many of the Alexa top-1M websites use that TLD; similarly, “Censys Rank” ranks by how many unique root domains from the entire Censys dataset use that TLD.

WHO GIVES OUT THESE CERTIFICATES?

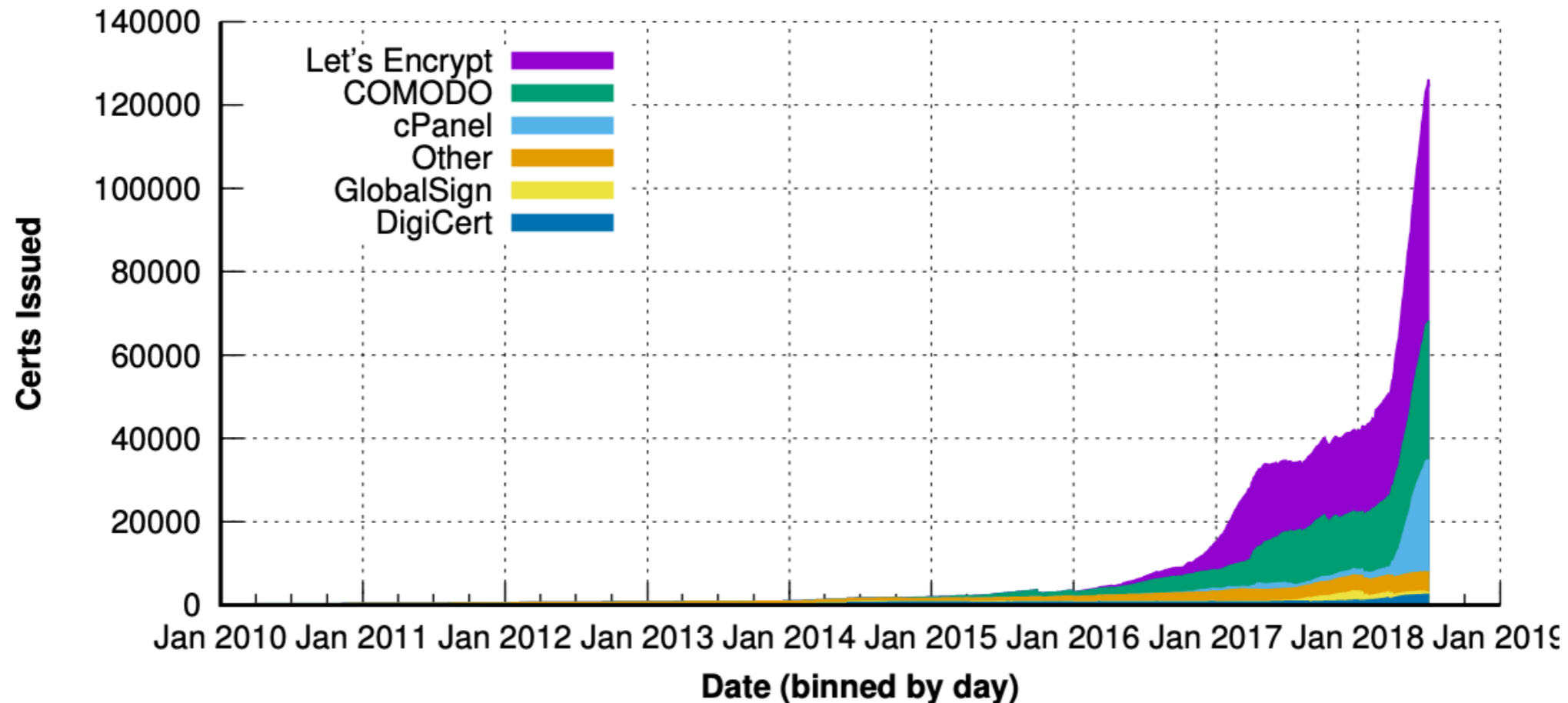


Fig. 5: Stacked-plot graph representing the number of certificates valid on a given day that included a target embedding domain, broken down by the CA that issued each certificate.

Largely free domains

WHERE ARE THEY HOSTING THESE DOMAINS?

Hosting Provider	Unique Domains
verotel.com	1,725
cloudflare.com	903
websitewelcome.com	750
unifiedlayer.com	671
amazonaws.com	452
ovh.net	417
hetzner.de	339
digitalocean.com	252
namecheaphosting.com	244
godaddy.com	190
Others	7,715

TABLE VI: Top 10 most popular hosting providers for target embedding domains.

Largely free hosting providers

QUESTIONS YIELD NEW QUESTIONS...

informationen.support.cgi.log.ssl.cembra.ch.aktualisieren.amerbay.com

(Swiss bank)

Why is this domain name so long?!?

QUESTIONS YIELD NEW QUESTIONS...

informationen.support.cgi.log.ssl.cembra.ch.aktualisieren.amerbay.com

(Swiss bank)

Why is this domain name so long?!?

Safari on iPhones left-justify in Safari

informationen.support.cgi.log.ssl.cem



QUESTIONS YIELD NEW QUESTIONS...

informationen.support.cgi.log.ssl.cembra.ch.aktualisieren.amerbay.com

(Swiss bank)

Why is this domain name so long?!?

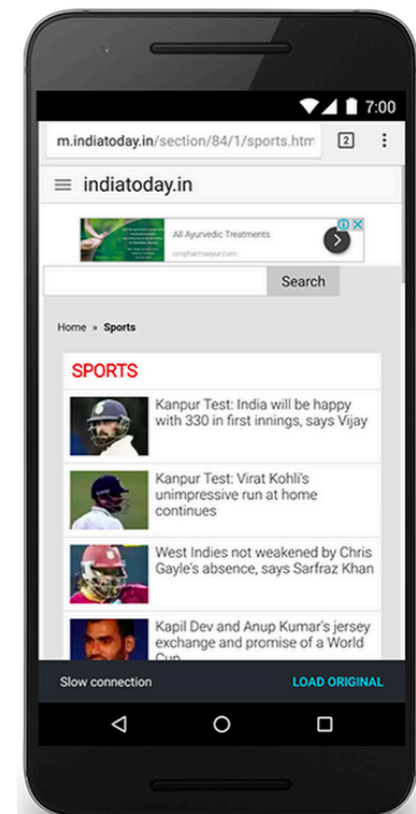
Safari on iPhones left-justify in Safari

informationen.support.cgi.log.ssl.cem

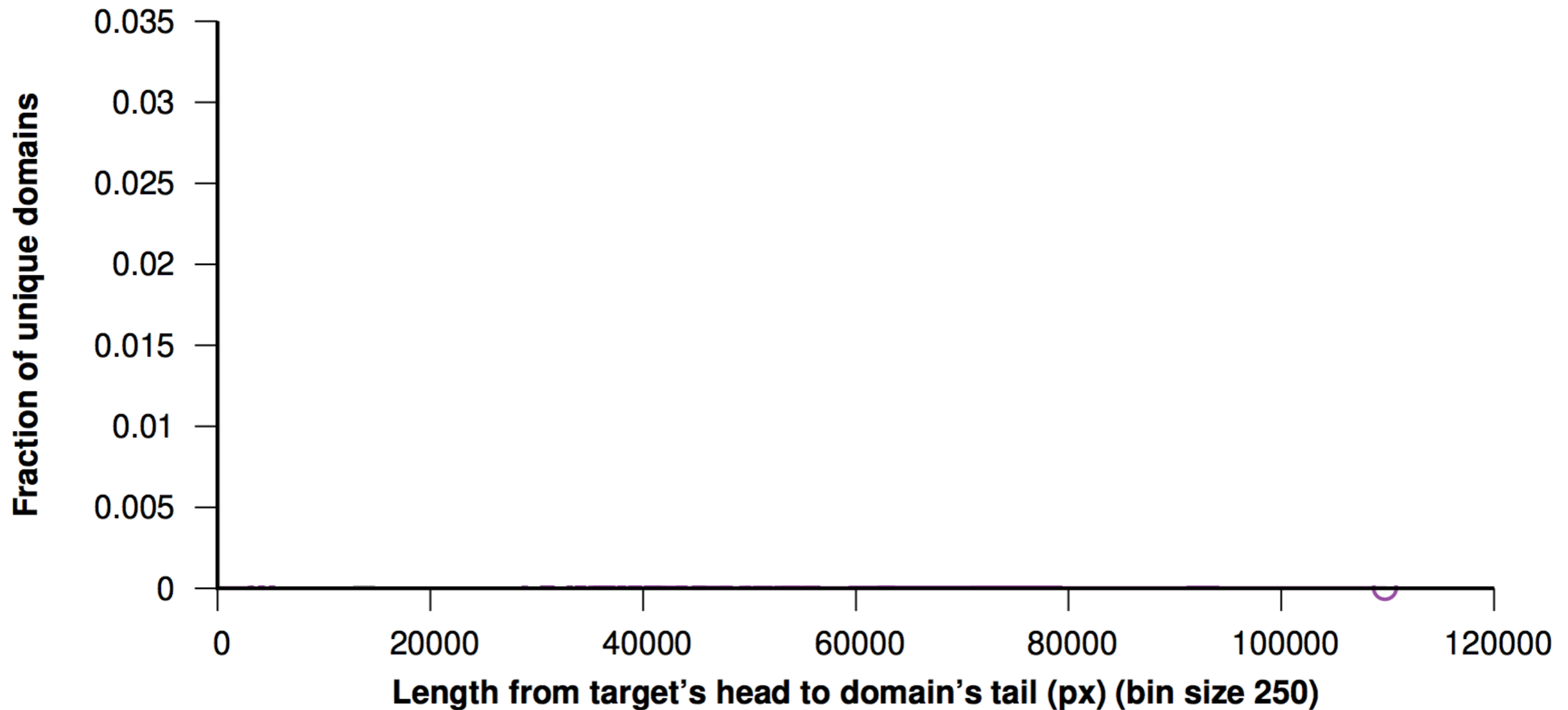


Chrome on Android *right-justifies*

cembra.ch.aktualisieren.amerbay.com

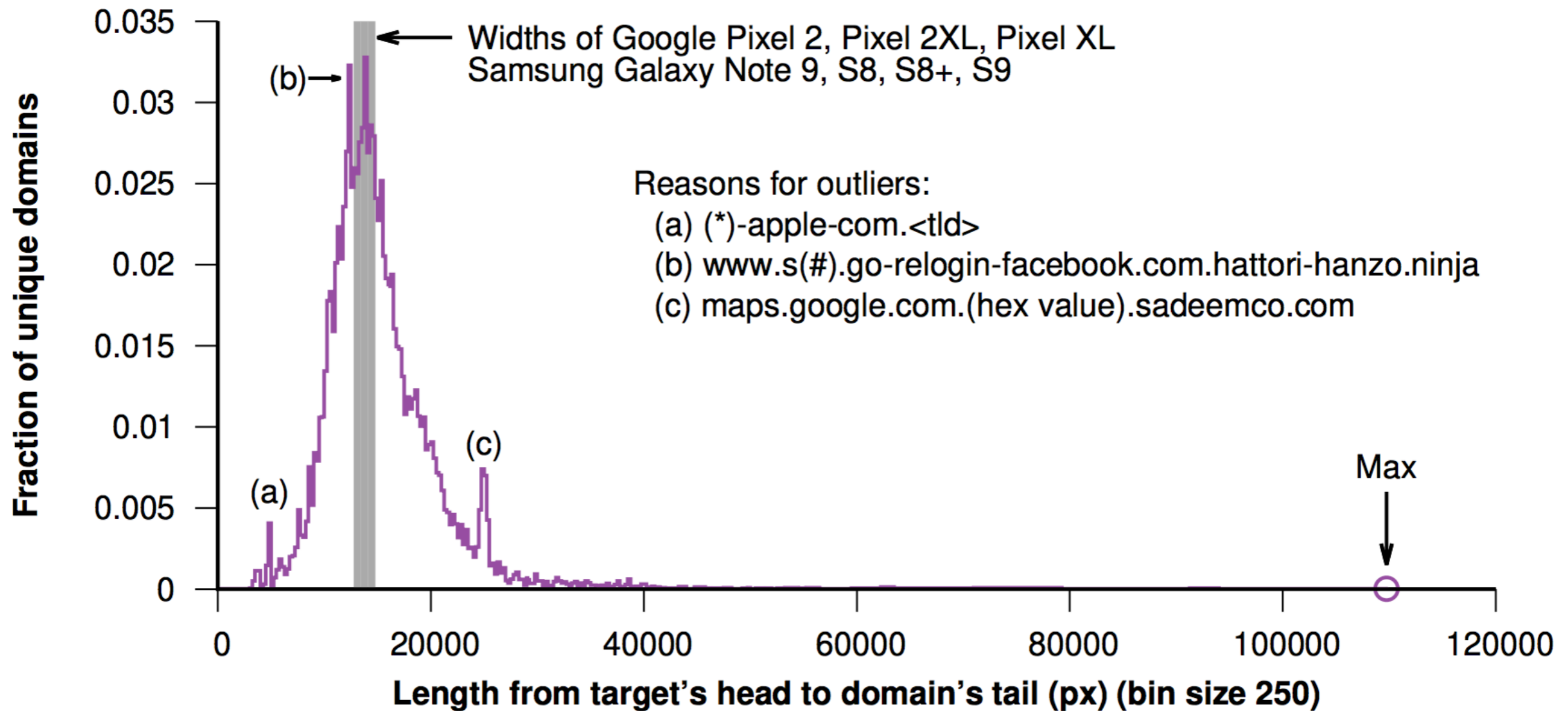


SOPHISTICATED IMPERSONATION ATTACKS



informationen.support.cgi.log.ssl.cembra.ch.aktualisieren.amerbay.com

SOPHISTICATED IMPERSONATION ATTACKS



informationen.support.cgi.log.ssl.cembra.ch.aktualisieren.amerbay.com

WHY DO ATTACKERS DO THIS?

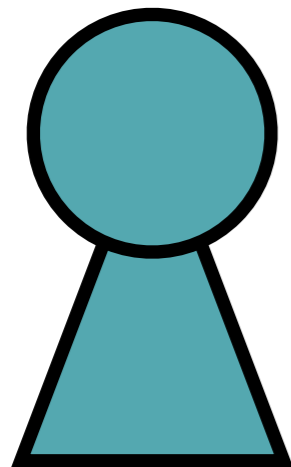
*Largely **free** domain registration*

*Largely **free** CAs*

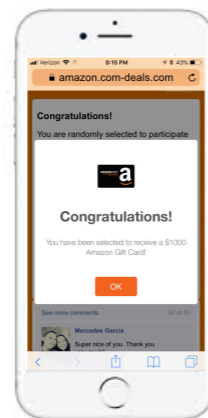
*Largely **free** hosting providers*

It's effective!

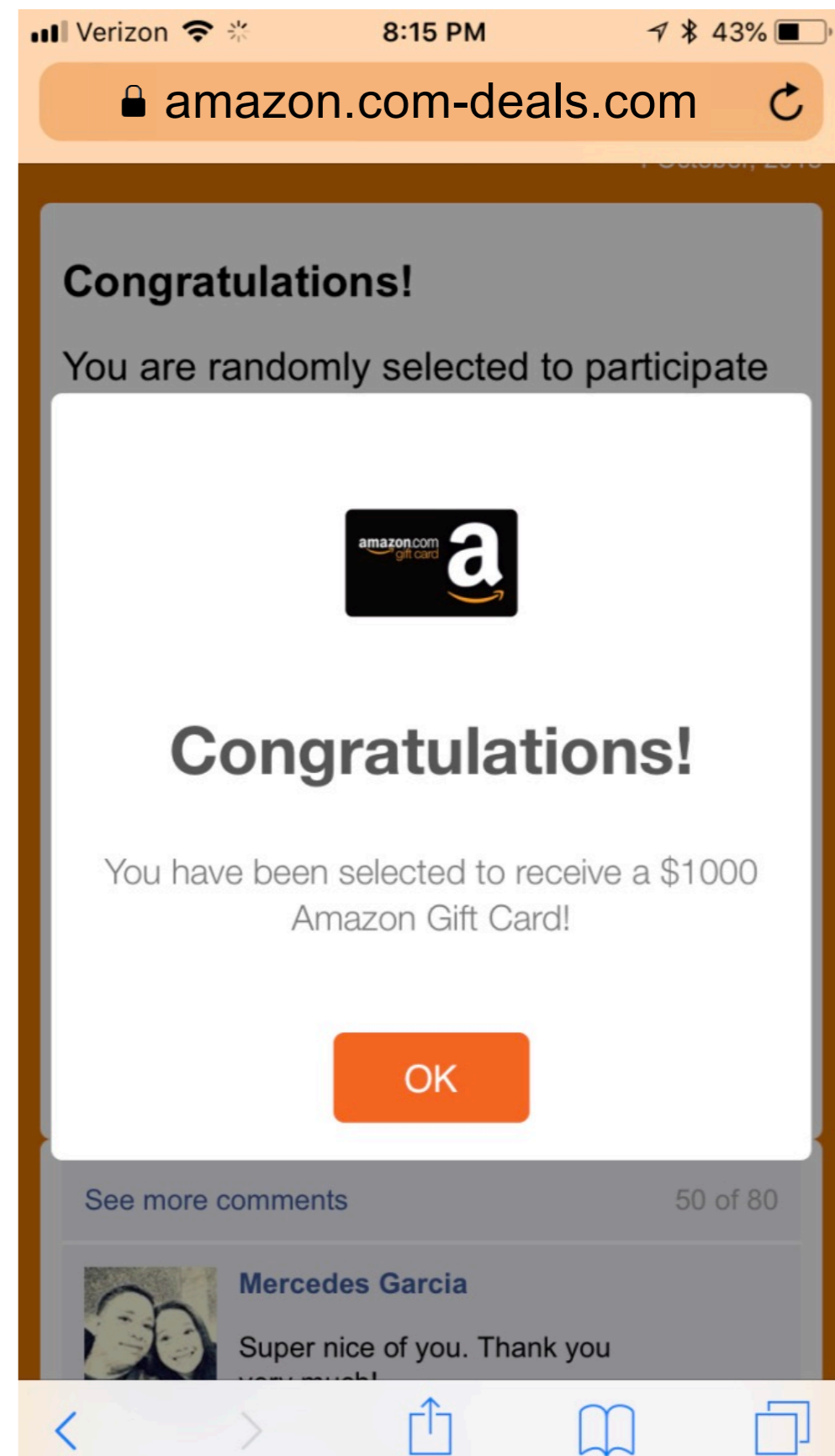
COMMUNICATING YOUR RESULTS



My wife

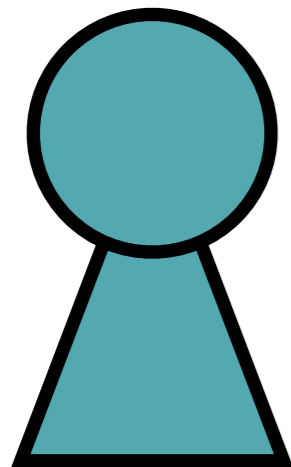


Me

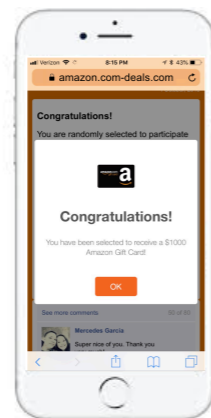


COMMUNICATING YOUR RESULTS

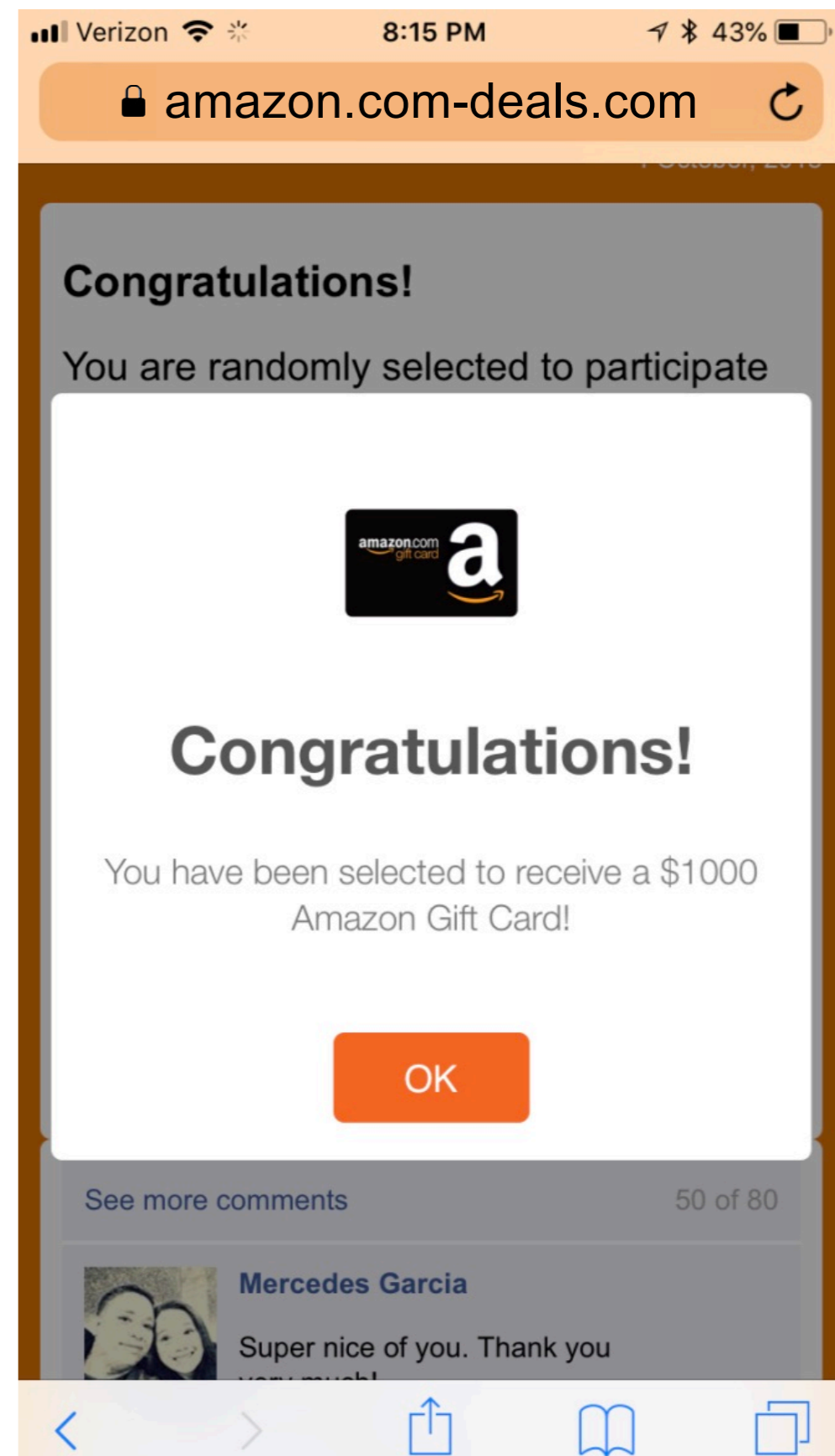
Nope, it isn't Amazon, and I know why!



My wife

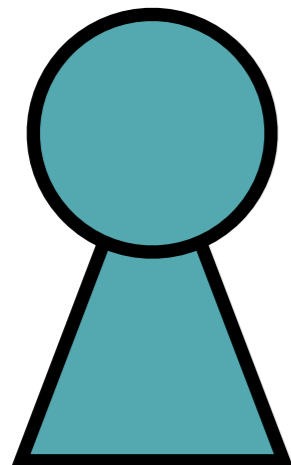


Me

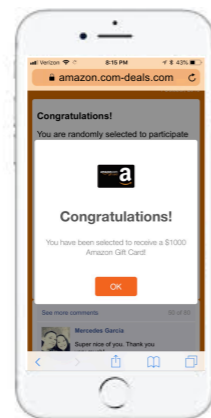


COMMUNICATING YOUR RESULTS

Nope, it isn't Amazon, and I know why!

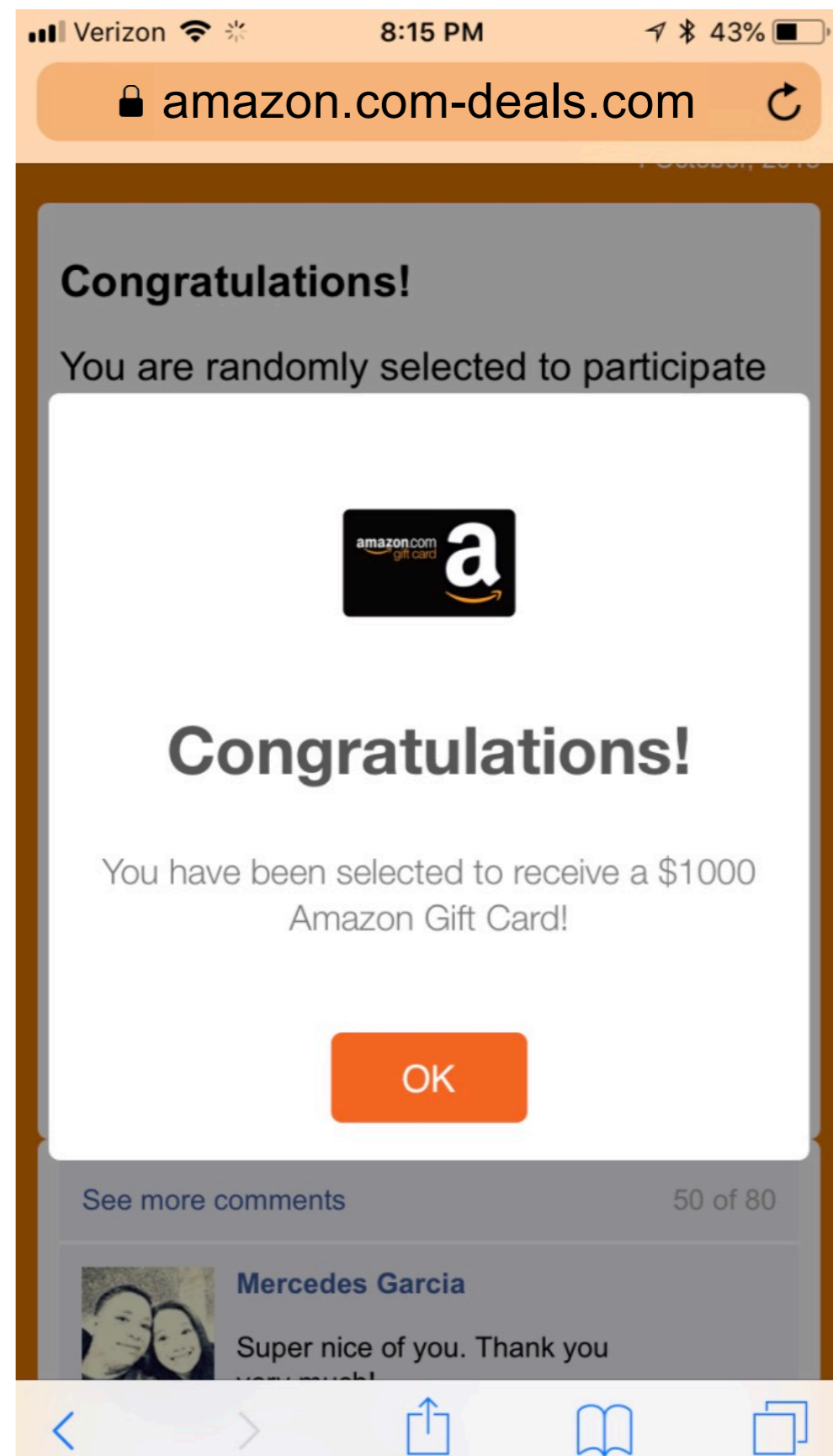


My wife



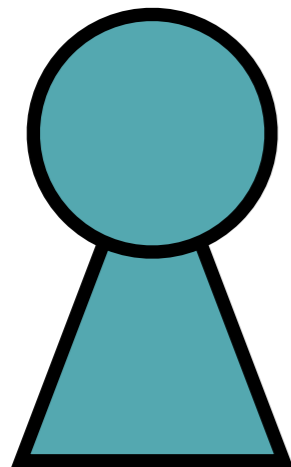
Me

I asked you that like 4 months ago

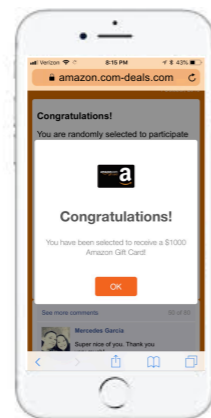


COMMUNICATING YOUR RESULTS

Nope, it isn't Amazon, and I know why!



My wife



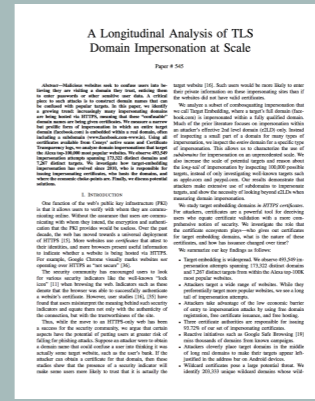
Me

I asked you that like 4 months ago

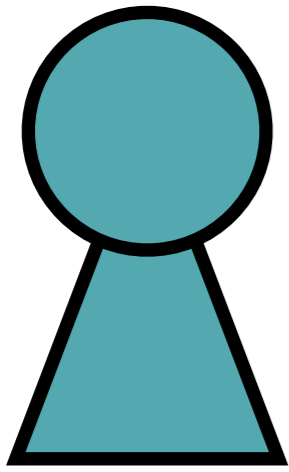


COMMUNICATING YOUR RESULTS

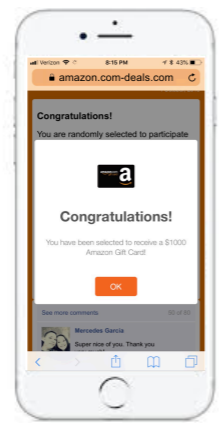
Nope, it isn't Amazon, and I know why!



Me



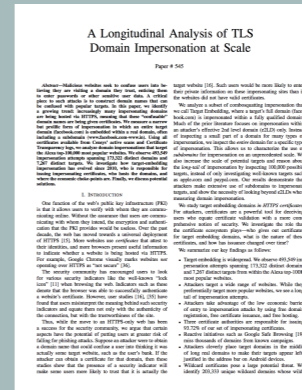
My wife



I asked you that like 4 months ago

COMMUNICATING YOUR RESULTS

Nope, it isn't Amazon, and I know why!

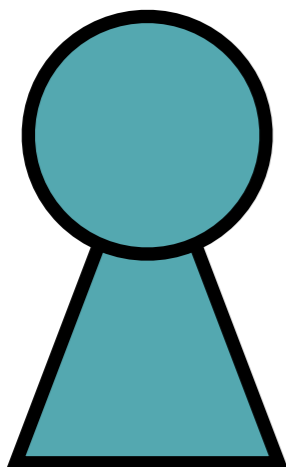


Me

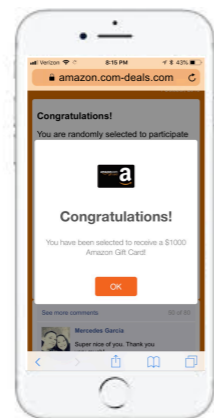


Can we help?

I asked you that like 4 months ago



My wife



OTHER FORMS OF DOMAIN IMPERSONATION

Typosquatting: gogole.com

gooogle.com

googl.com

Homographs: g00gle.com

google.com