Proxy in a Haystack

Uncovering and Classifying MFA Bypass Phishing Attacks in Large-Scale Authentication Data

Becca Lynch
Sr. Data Scientist, Duo / Cisco

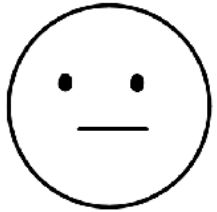
Lauren Saue-Fletcher
Stanford University

DUO | cisco SECURE

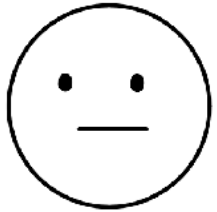
Agenda

+ Evolution of MFA Phishing
+ Why detection is hard
+ Enhancing auth data with DNS
+ We did some ML and it kind of worked

Phishing and its Even Eviler Twin

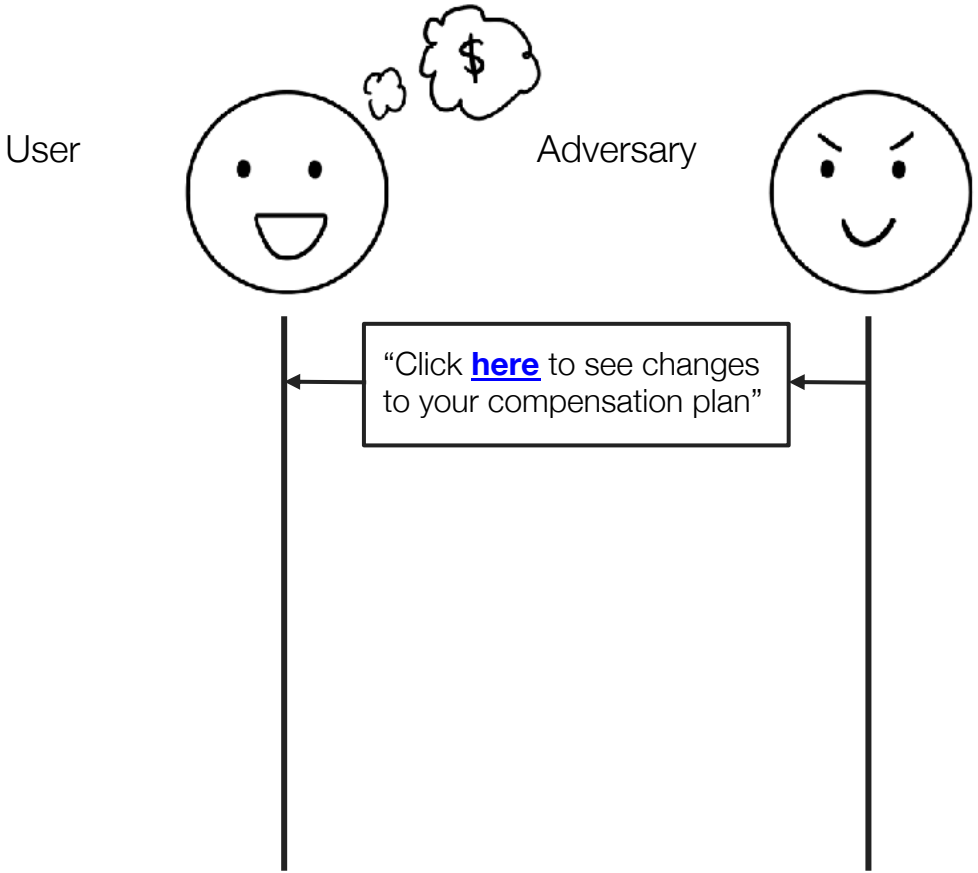


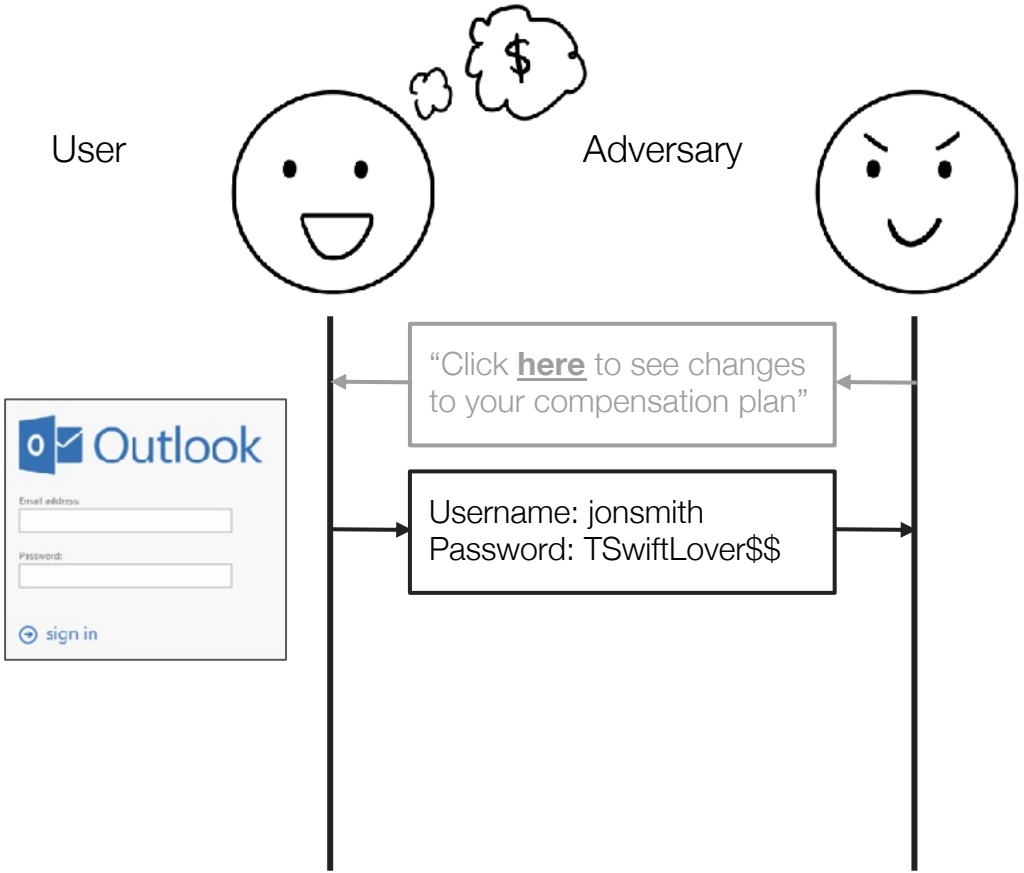
User

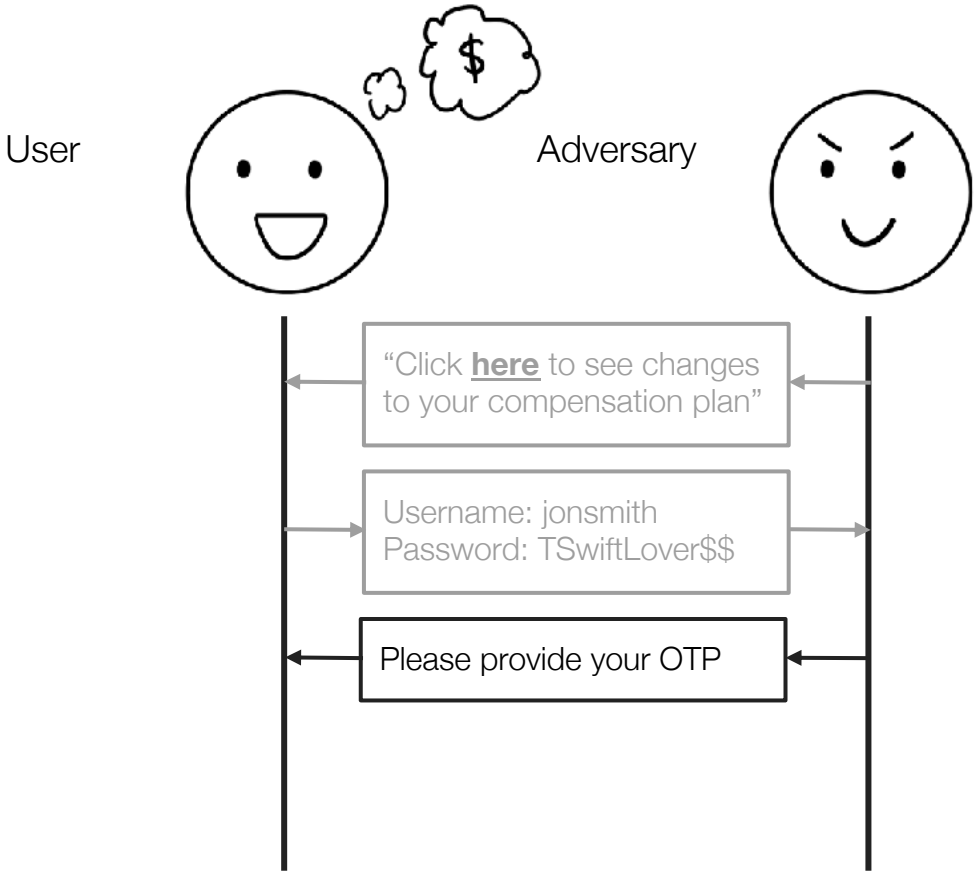


User

Adversary

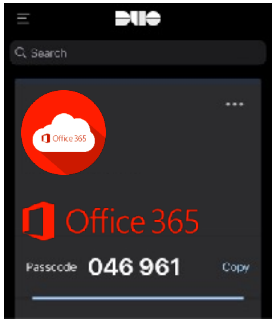






User

Adversary

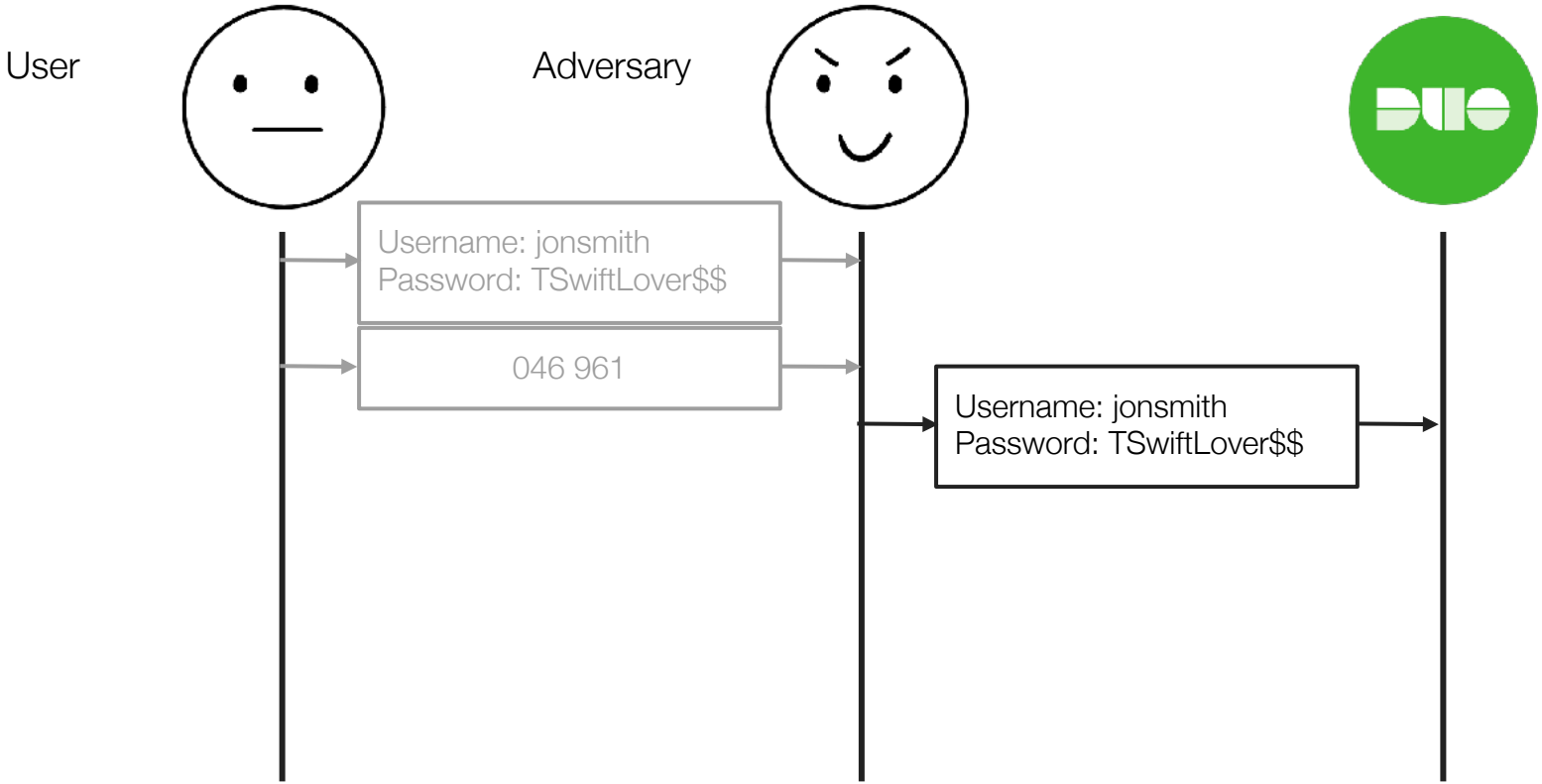


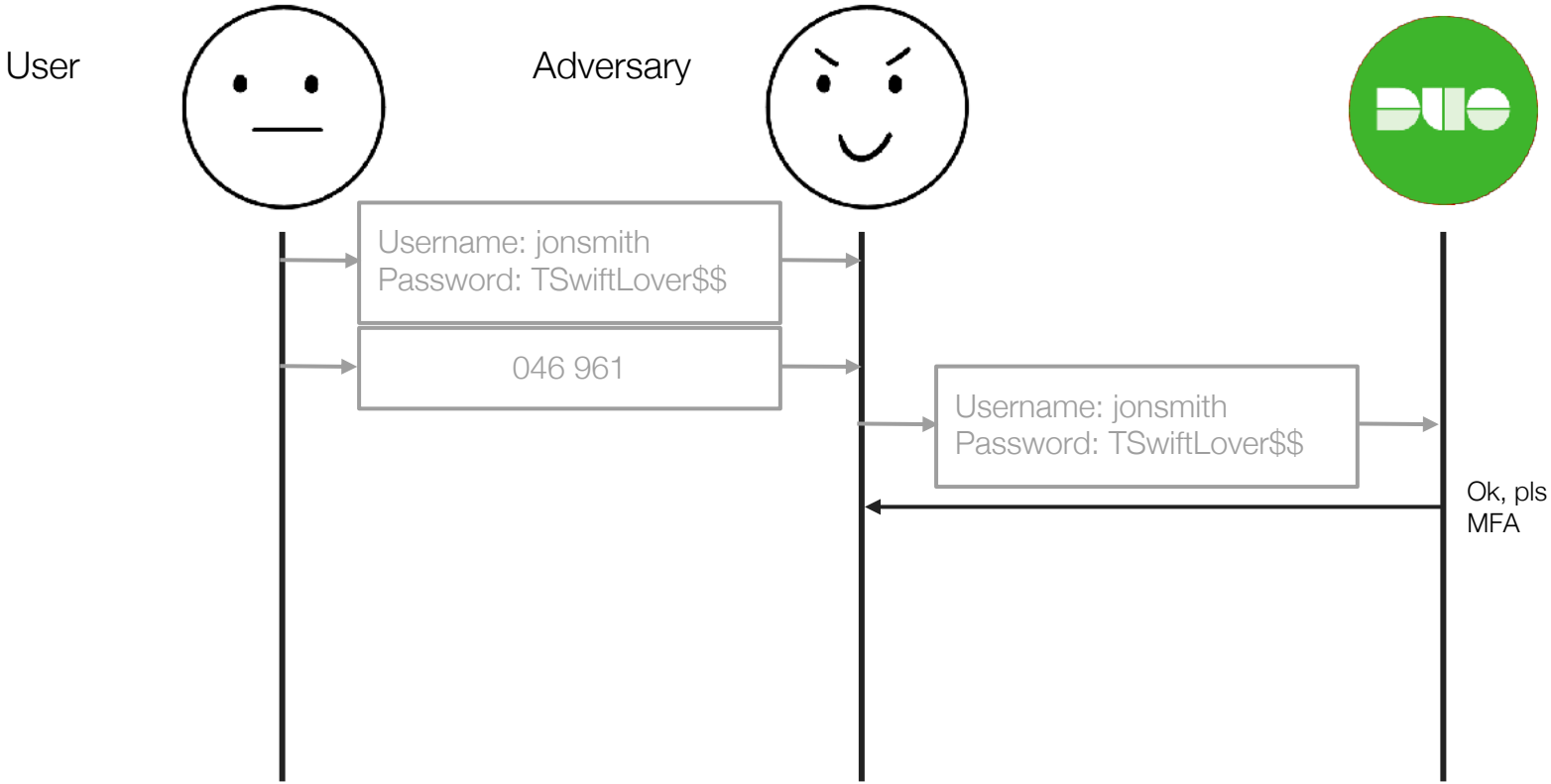
"Click **here** to see changes to your compensation plan"

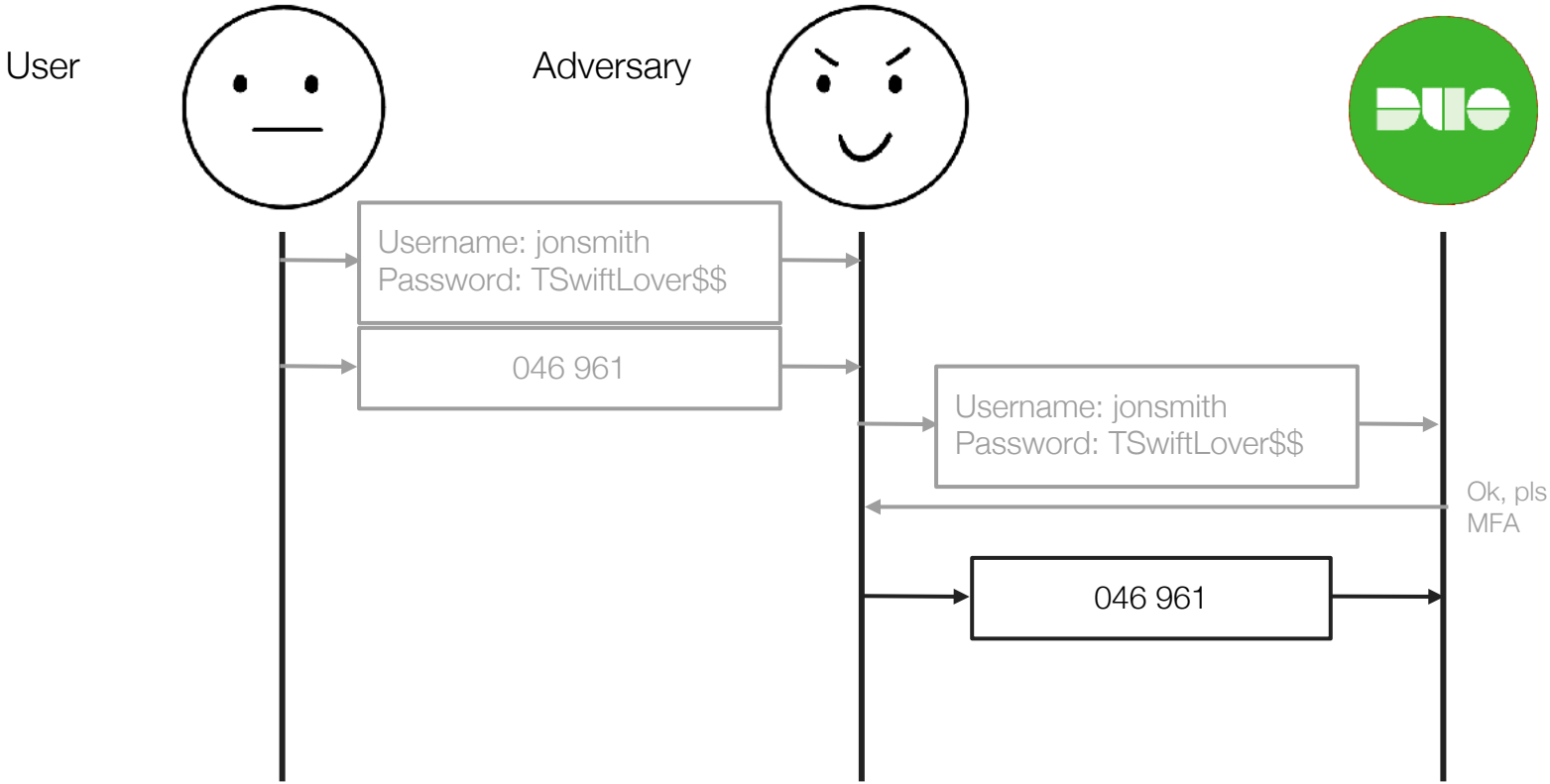
Username: jonsmith
Password: TSwiftLover$$

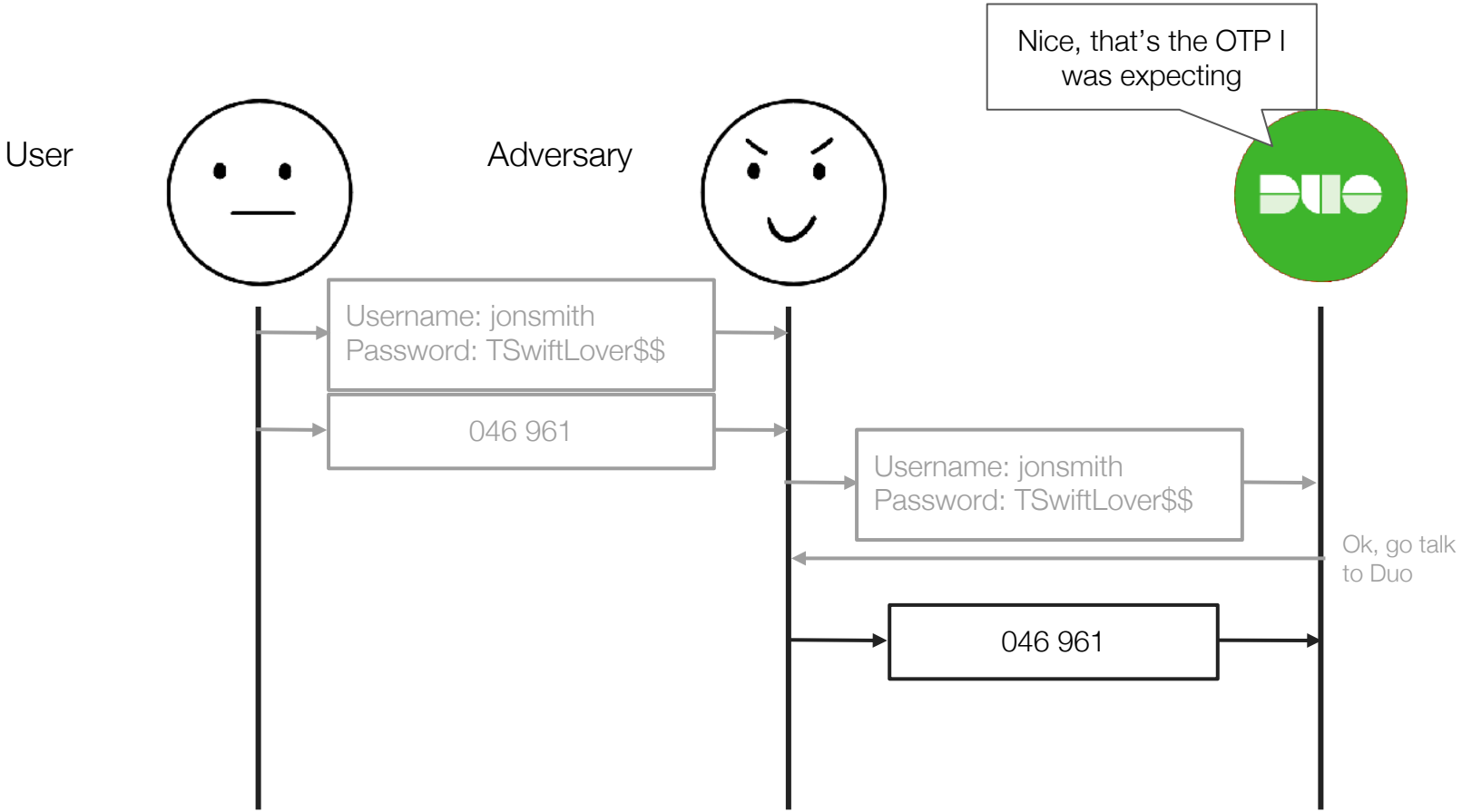
Please provide your OTP

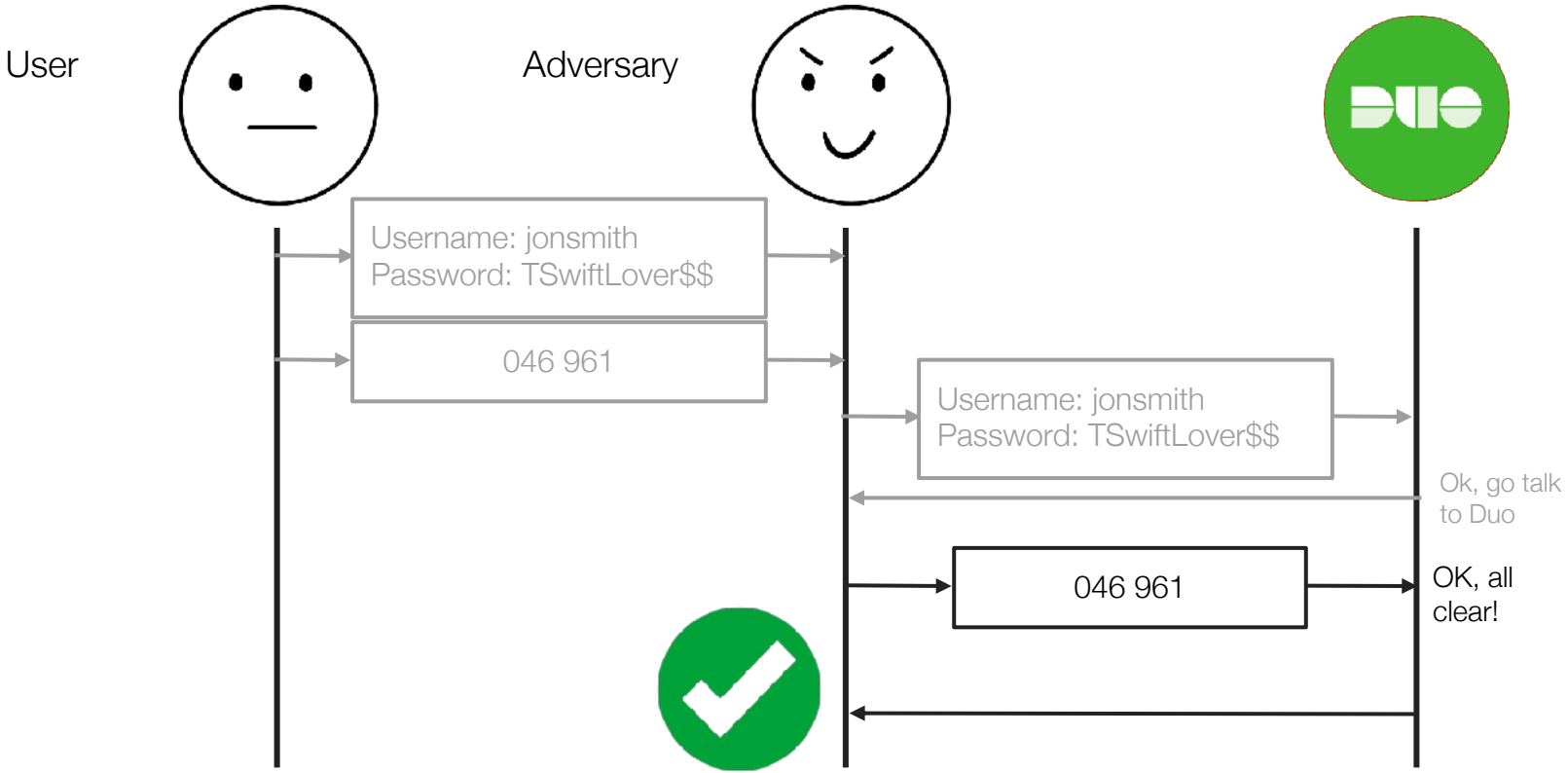
046 961

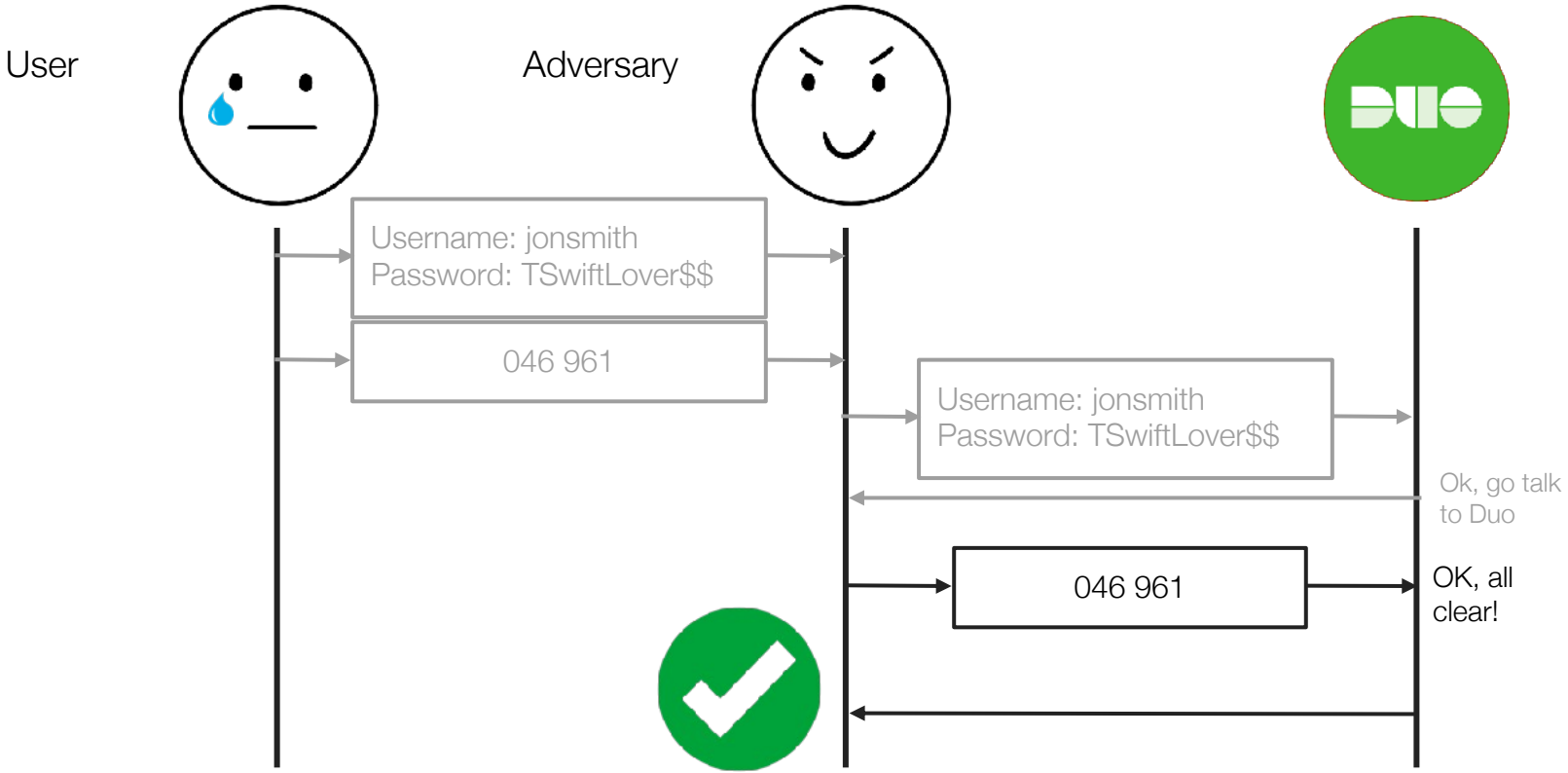

User
Adversary
Username: jonsmith
Password: TSwiftLover$$
046 961
Username: jonsmith
Password: TSwiftLover$$

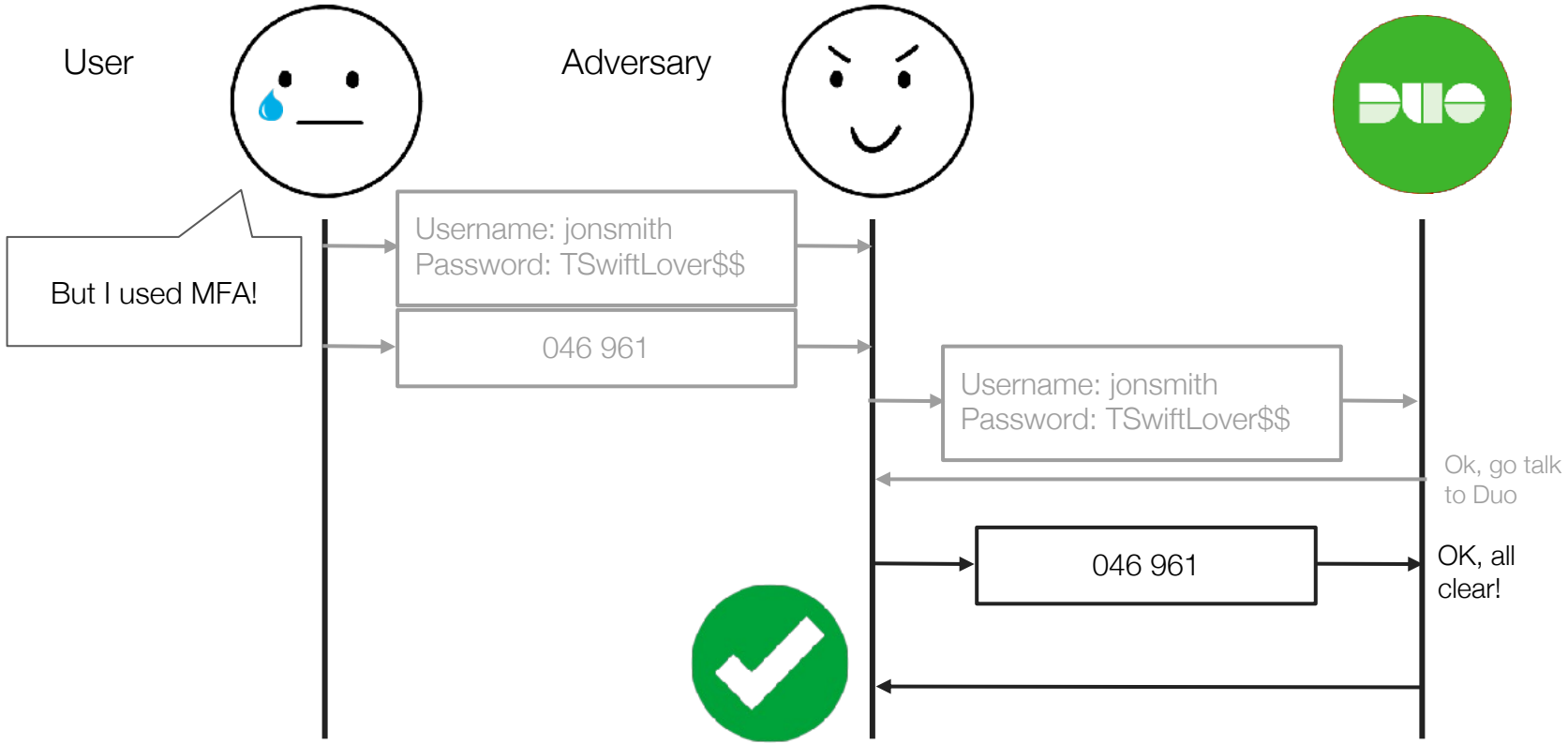

User
Adversary
Username: jonsmith
Password: TSwiftLover$$
046 961
Username: jonsmith
Password: TSwiftLover$$
Ok, pls
MFA

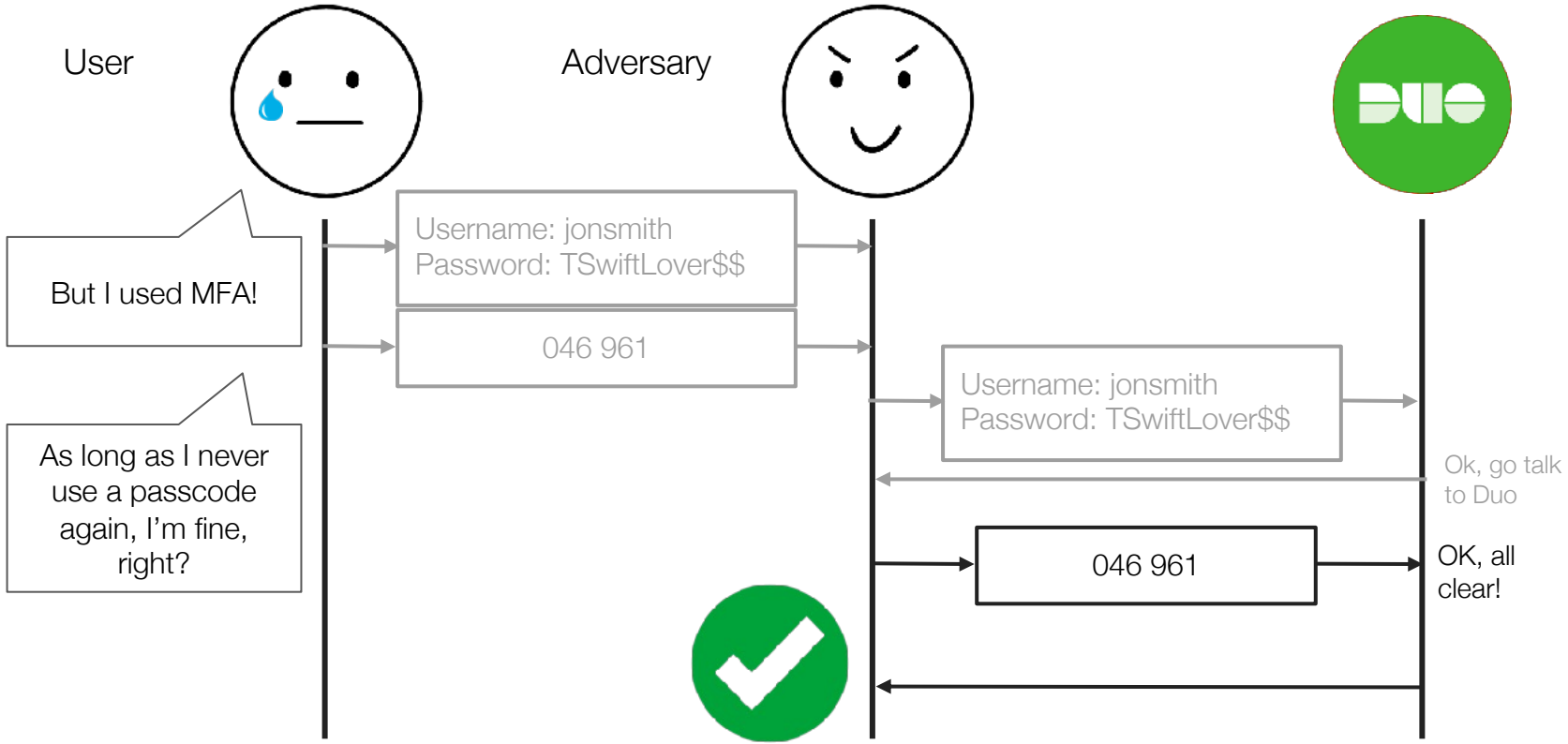

User
Adversary
Username: jonsmith
Password: TSwiftLover$$
046 961
Username: jonsmith
Password: TSwiftLover$$
Ok, pls
MFA
046 961


Nice, that's the OTP I was expecting
User
Adversary
Username: jonsmith
Password: TSwiftLover$$
046 961
Username: jonsmith
Password: TSwiftLover$$
Ok, go talk to Duo
046 961


User
Adversary
Username: jonsmith
Password: TSwiftLover$$
046 961
Username: jonsmith
Password: TSwiftLover$$
Ok, go talk to Duo
046 961
OK, all clear!

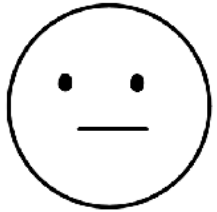

User
Adversary
Username: jonsmith
Password: TSwiftLover$$
046 961
Username: jonsmith
Password: TSwiftLover$$
Ok, go talk to Duo
046 961
OK, all clear!

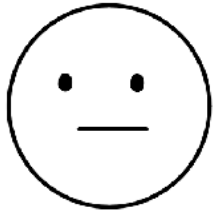

User
Adversary
But I used MFA!
Username: jonsmith
Password: TSwiftLover$$
046 961
Username: jonsmith
Password: TSwiftLover$$
Ok, go talk to Duo
046 961
OK, all clear!

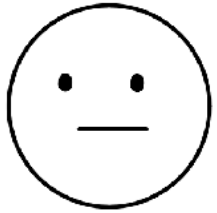

User
Adversary
But I used MFA!
As long as I never use a passcode again, I'm fine, right?
Username: jonsmith
Password: TSwiftLover$$
046 961
Username: jonsmith
Password: TSwiftLover$$
Ok, go talk to Duo
046 961
OK, all clear!

Enter…

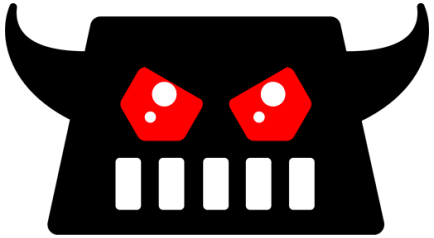
MFA Bypass Phishing

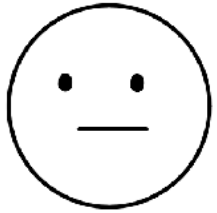




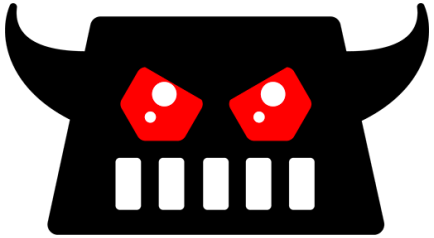


evilginx server
hosted on 1.2.3.4





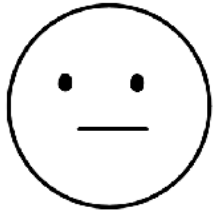
evilginx server
hosted on 1.2.3.4

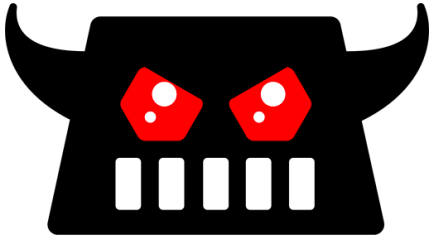


“Click **here** to see changes to your compensation plan”

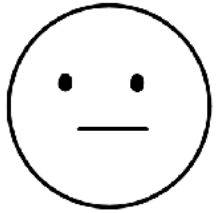
login.duo-secuurity.net

evilginx server
hosted on 1.2.3.4

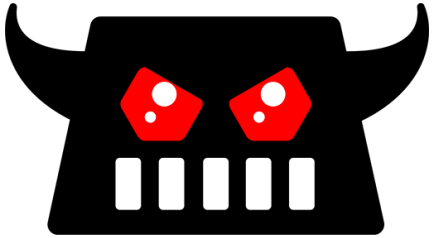


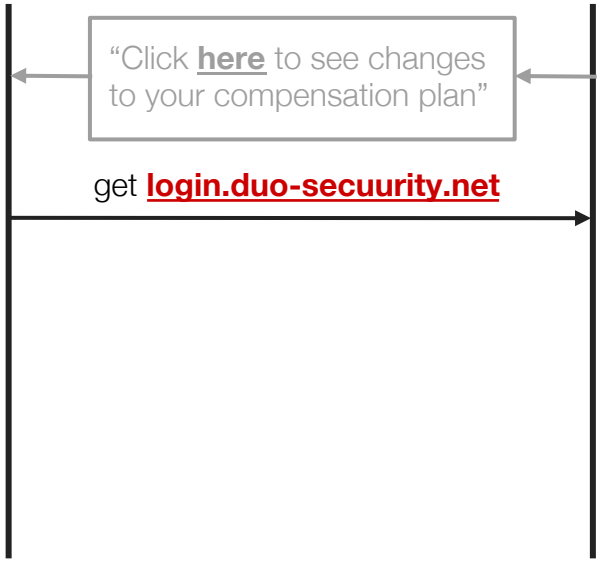


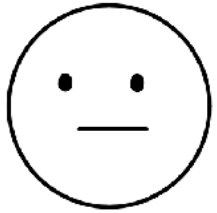
“Click here to see changes to your compensation plan”



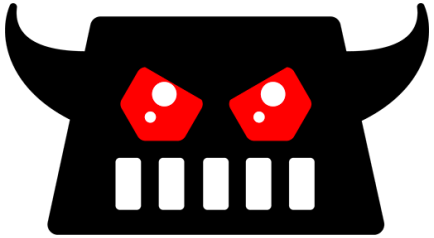
evilginx server

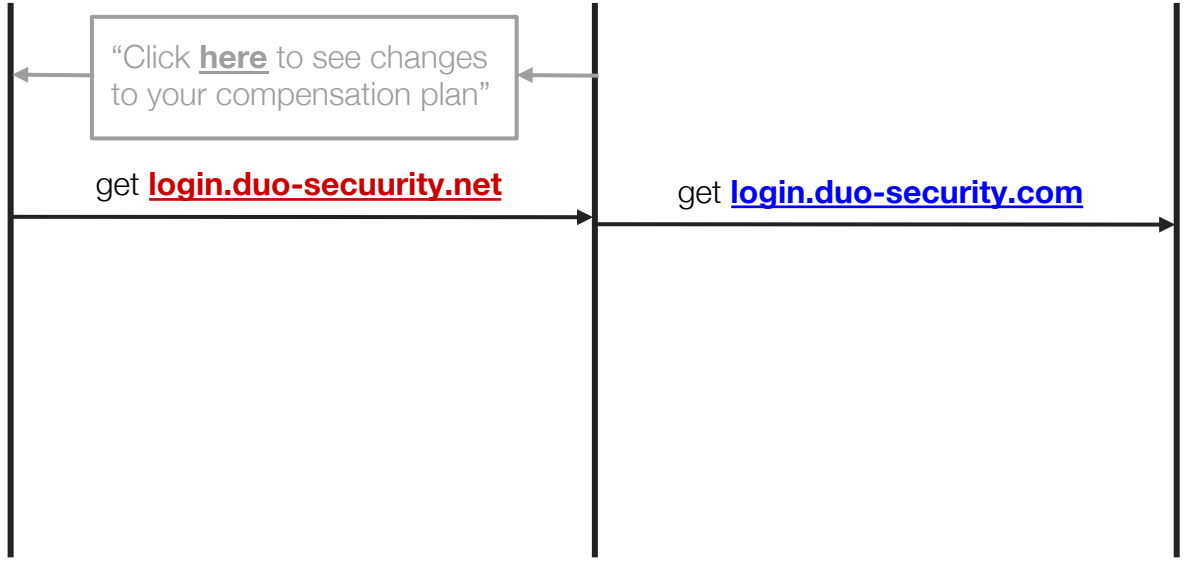


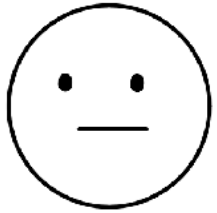




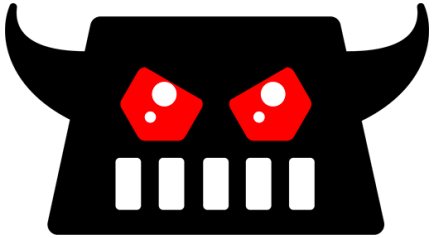
evilginx server

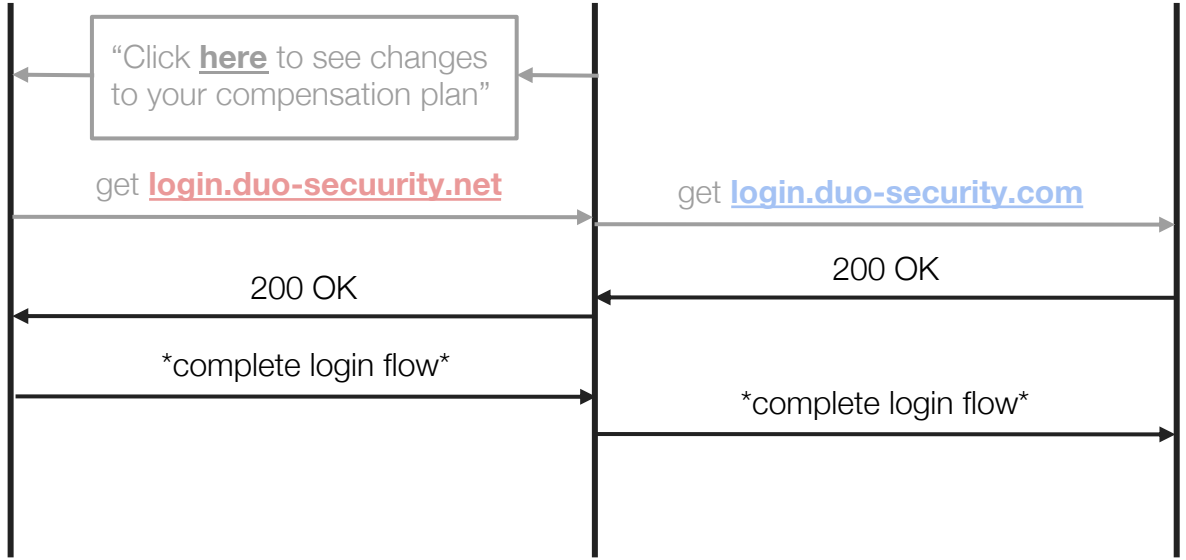


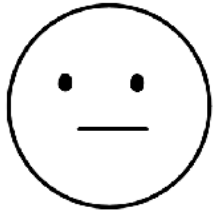




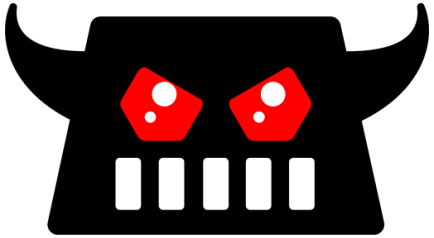
evilginx server

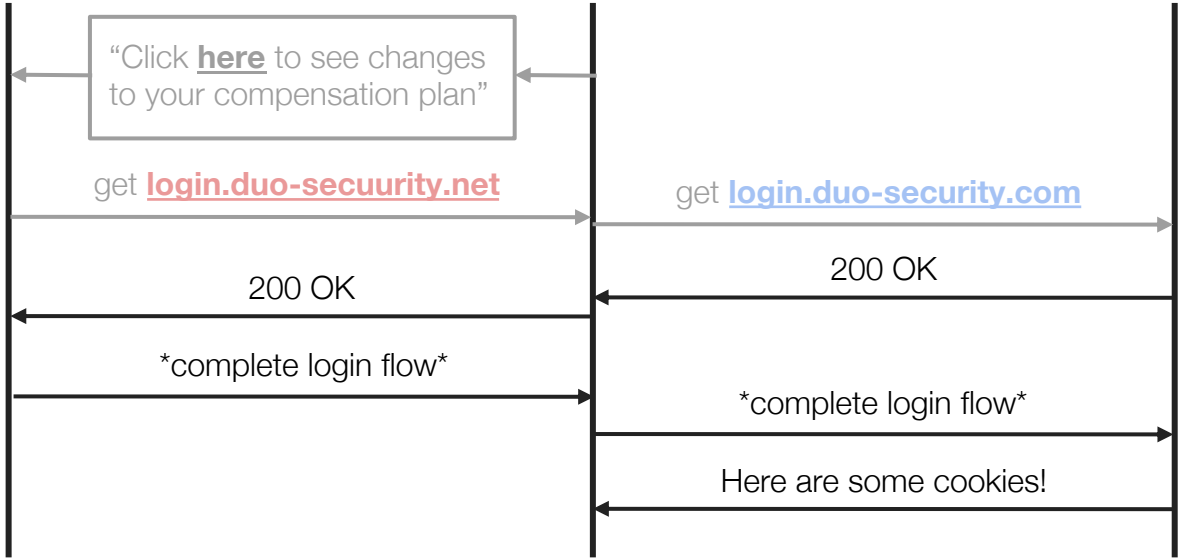


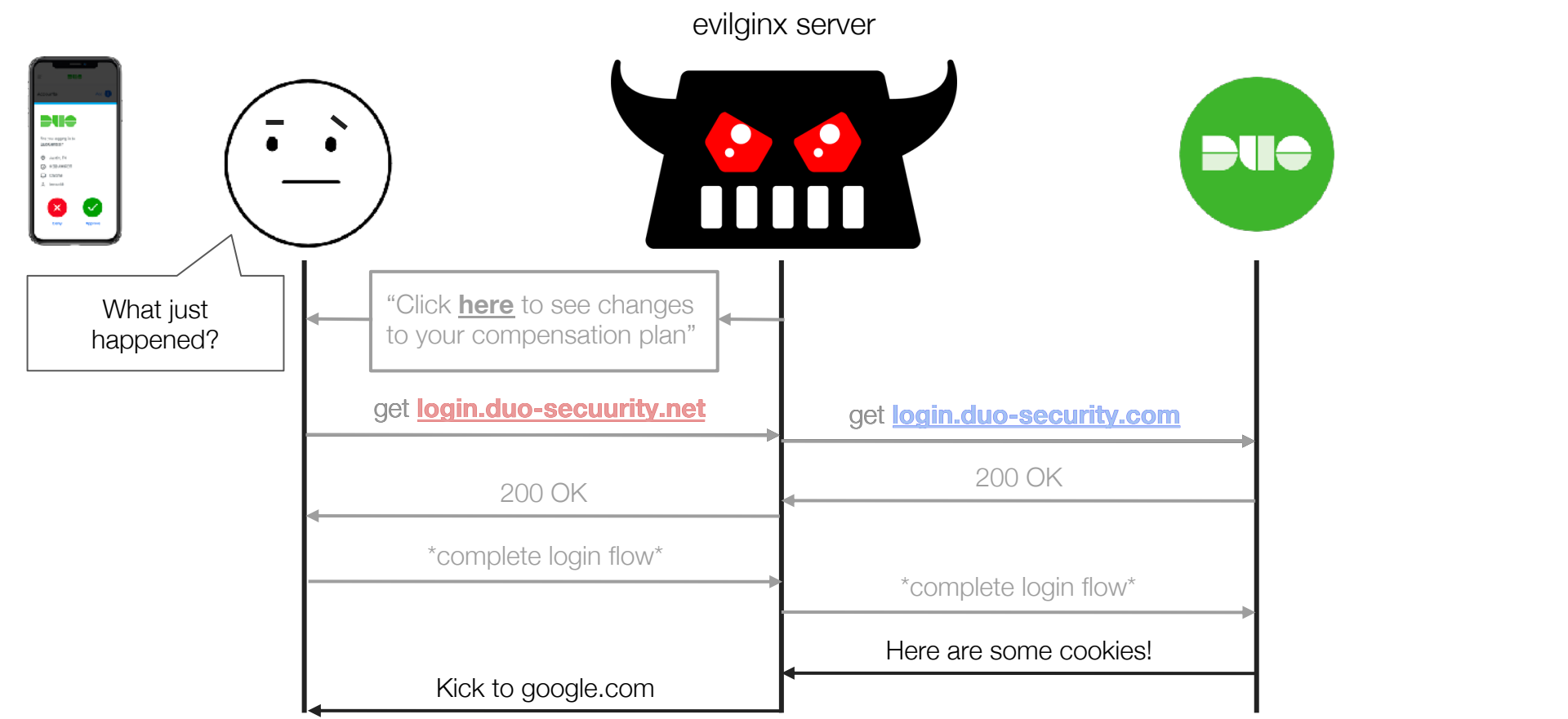




evilginx server



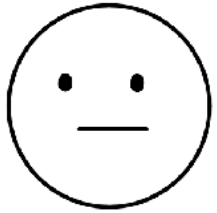



evilginx server
What just happened?
“Click here to see changes to your compensation plan”
get login.duo-secuurity.net
get login.duo-security.com
200 OK
200 OK
complete login flow
complete login flow
Here are some cookies!
Kick to google.com

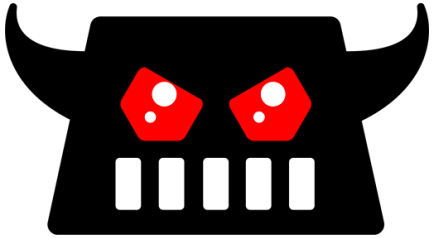
But you said we aren't using passcodes anymore!

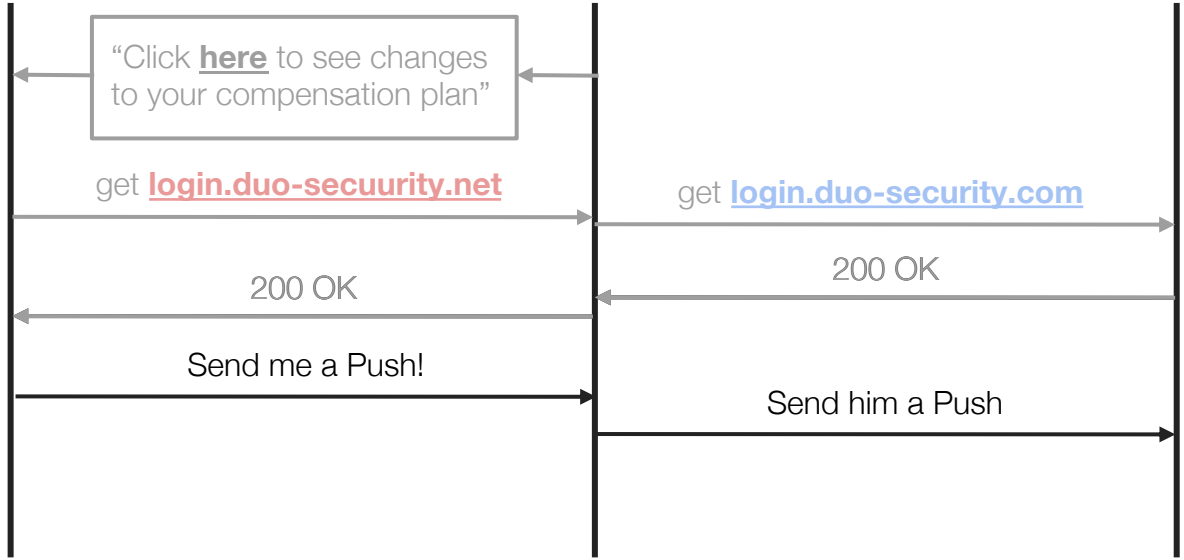
Spoiler, it won't help!

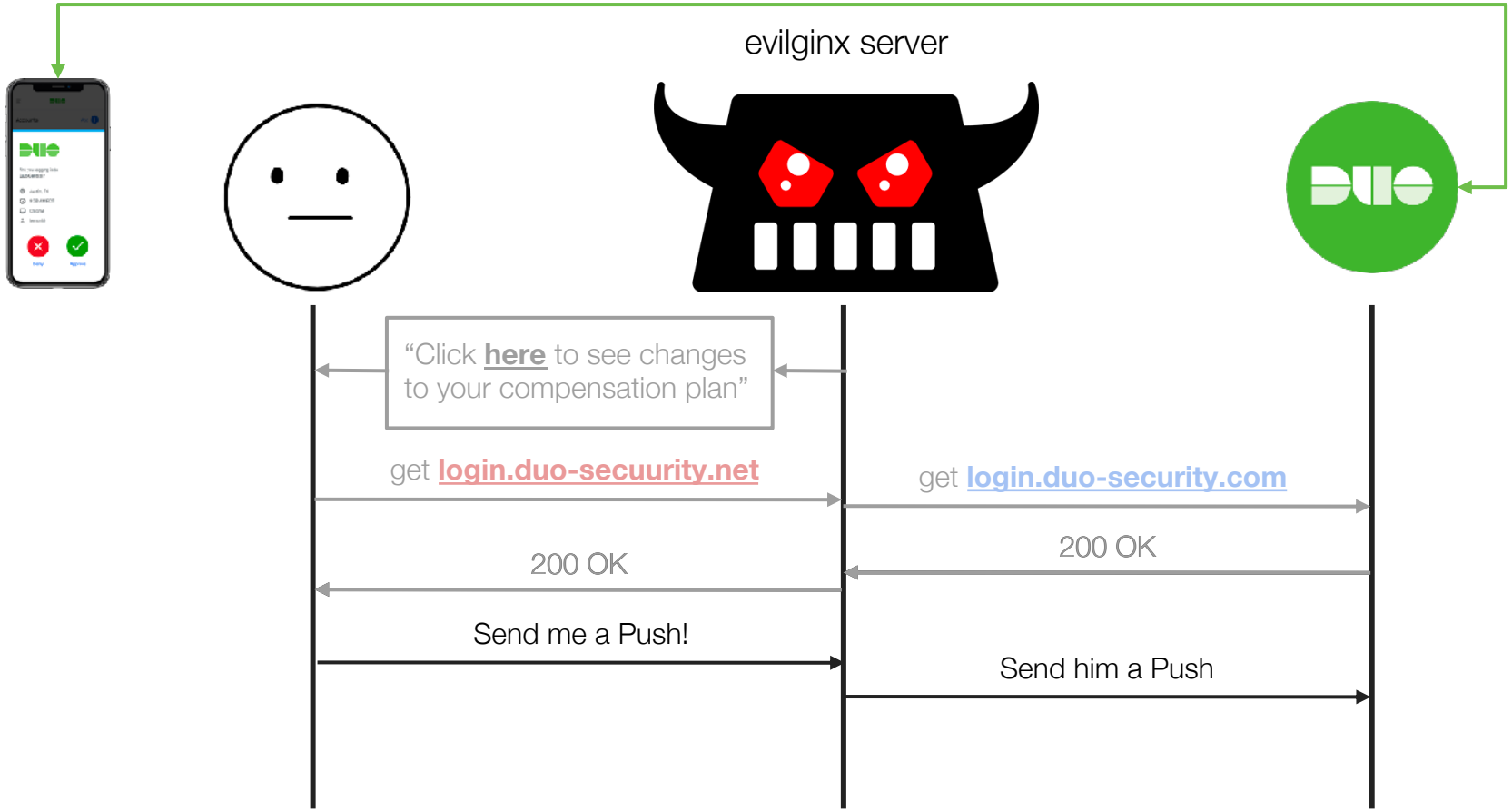
DUO | CISCO SECURE

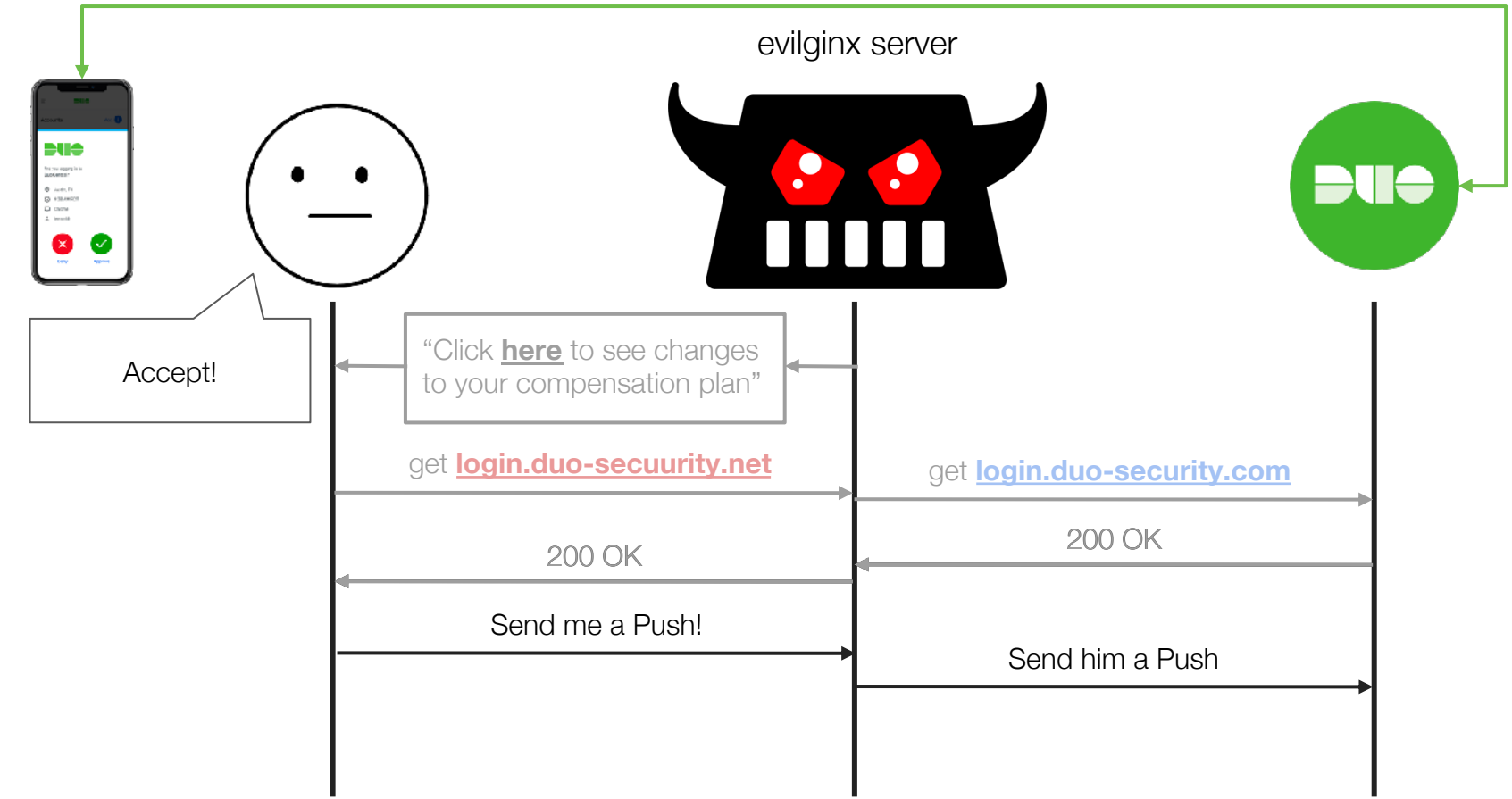


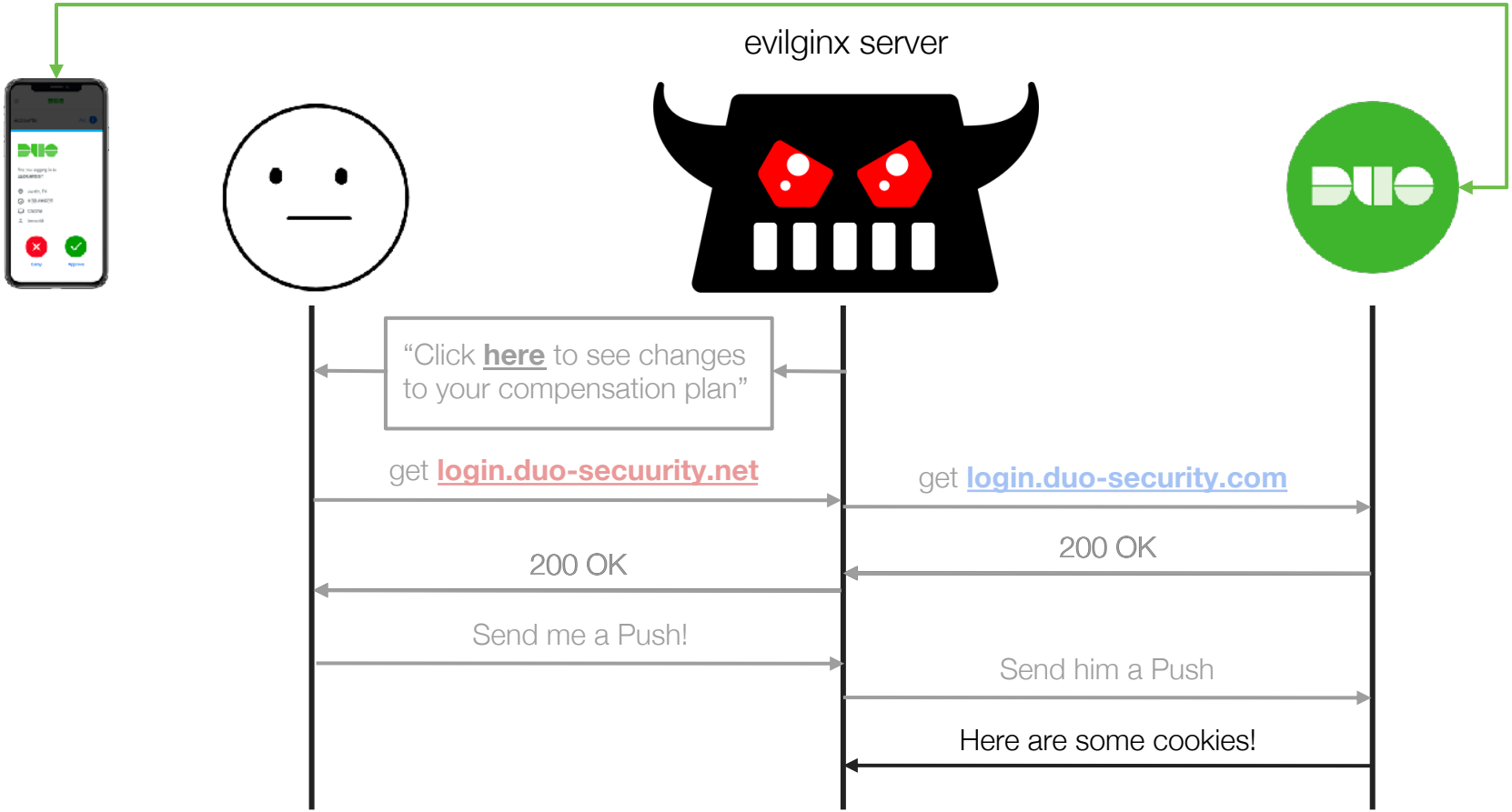
evilginx server

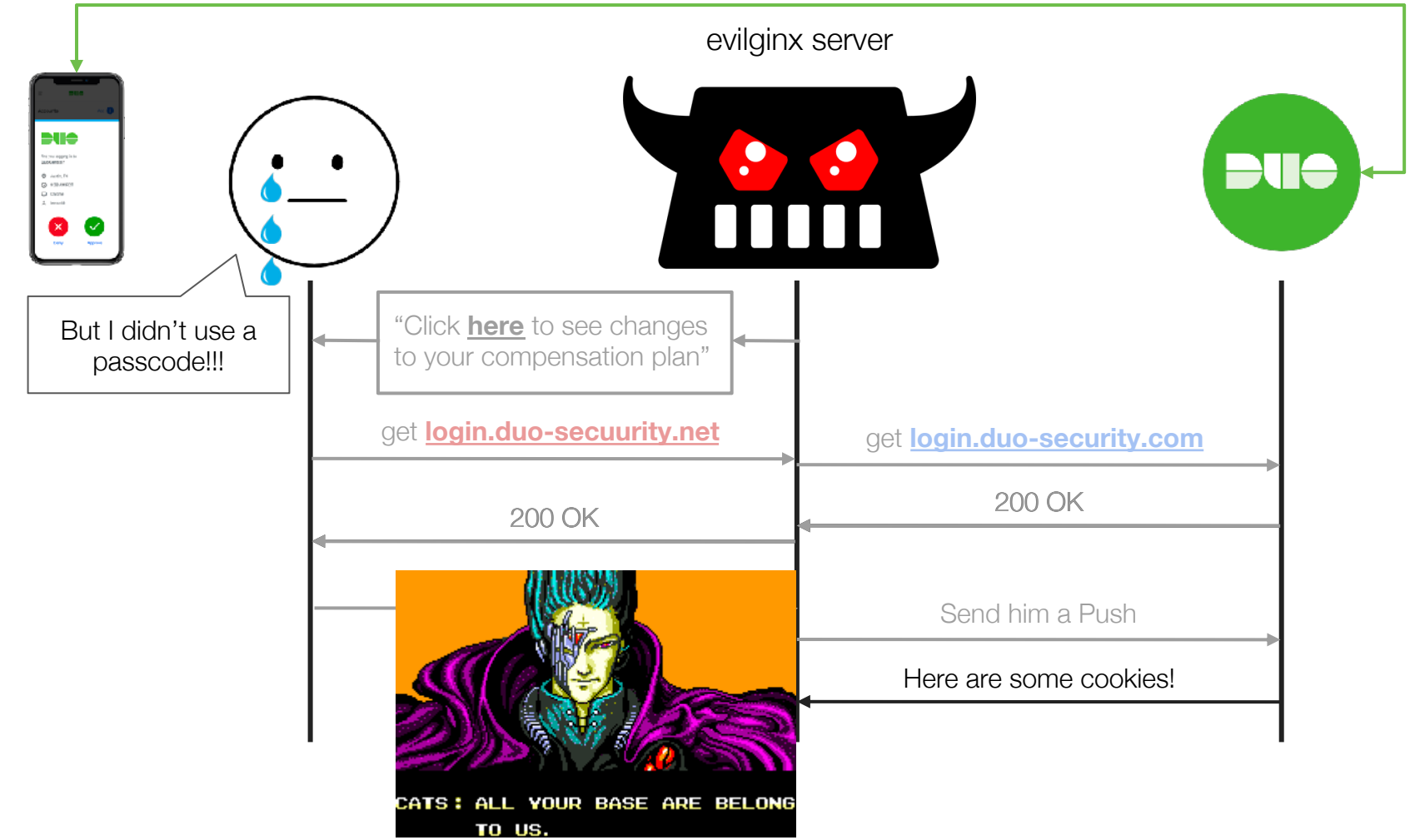





evilginx server
“Click here to see changes to your compensation plan”
get login.duo-secuurity.net
get login.duo-security.com
200 OK
200 OK
Send me a Push!
Send him a Push


evilginx server
Accept!
“Click here to see changes to your compensation plan”
get login.duo-secuurity.net
get login.duo-security.com
200 OK
200 OK
Send me a Push!
Send him a Push


evilginx server
“Click here to see changes to your compensation plan”
get login.duo-secuurity.net
get login.duo-security.com
200 OK
200 OK
Send me a Push!
Send him a Push
Here are some cookies!


evilginx server
But I didn't use a passcode!!!
"Click here to see changes to your compensation plan"
get login.duo-secuurity.net
get login.duo-security.com
200 OK
200 OK
Send him a Push
Here are some cookies!
CATS: ALL YOUR BASE ARE BELONG TO US.

Wait, this is bad

The evilginx setup proxies *everything* between the user and end server, meaning detection is even harder…

Wait, this is bad

The evilginx setup proxies *everything* between the user and end server, meaning detection is even harder…

	“Classic” Phishing	**MFA Bypass Proxy**
OS	Server sees **attacker’s OS**	Server sees **user’s OS** proxied through attack server

Wait, this is bad

The evilginx setup proxies *everything* between the user and end server, meaning detection is even harder…

	“Classic” Phishing	**MFA Bypass Proxy**
OS	Server sees **attacker’s OS**	Server sees **user’s OS** proxied through attack server
Browser	Server sees **attacker’s user agent**	Server sees **user’s user agent** proxied through attack server

Wait, this is bad

The evilginx setup proxies *everything* between the user and end server, meaning detection is even harder…

	“Classic” Phishing	**MFA Bypass Proxy**
OS	Server sees **attacker’s OS**	Server sees **user’s OS** proxied through attack server
Browser	Server sees **attacker’s user agent**	Server sees **user’s user agent** proxied through attack server
User Experience	User sees potentially **different login** UX than normal	User sees the **exact same login** they are used to

Wait, this is bad

The evilginx setup proxies *everything* between the user and end server, meaning detection is even harder…

	“Classic” Phishing	**MFA Bypass Proxy**
OS	Server sees **attacker’s OS**	Server sees **user’s OS** proxied through attack server
Browser	Server sees **attacker’s user agent**	Server sees **user’s user agent** proxied through attack server
User Experience	User sees potentially **different login** UX than normal	User sees the **exact same login** they are used to
Attacker Setup	Attacker has to **setup full website** to capture credentials	Attacker can spin up one of many **OSS** tools and run in minutes

Wait, this is bad

The evilginx setup proxies *everything* between the user and end server, meaning detection is even harder…

	“Classic” Phishing	**MFA Bypass Proxy**
OS	Server sees **attacker’s OS**	Server sees **user’s OS** proxied through attack server
Browser	Server sees **attacker’s user agent**	Server sees **user’s user agent** proxied through attack server
User Experience	User sees potentially **different login** UX than normal	User sees the **exact same login** they are used to
Attacker Setup	Attacker has to **setup full website** to capture credentials	Attacker can spin up one of many **OSS** tools and run in minutes
Different IP	Server sees attacker’s IP	Server sees attacker’s IP

Is a new IP actually meaningful?

In 2 weeks, the
average user uses…

Is a new IP actually meaningful?

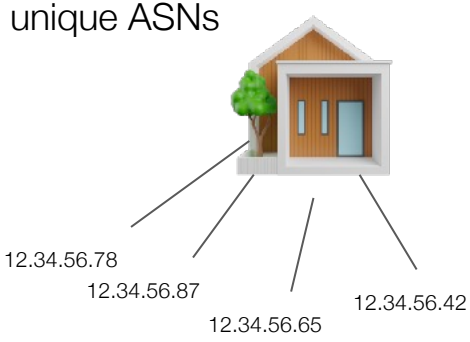
In 2 weeks, the
average user uses…

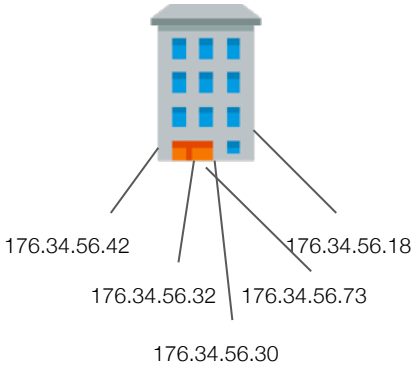
4.5 unique ASNs

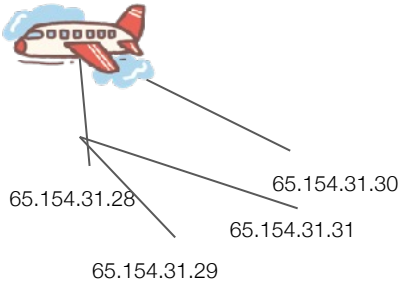
Is a new IP actually meaningful?

In 2 weeks, the
average user uses…

4.5 unique ASNs



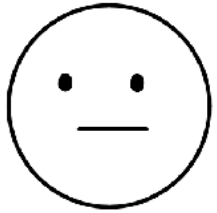


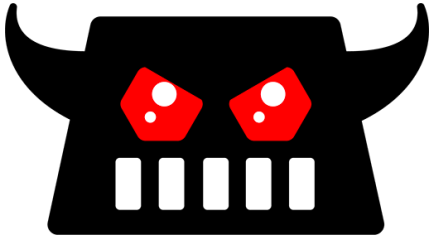


18 unique IPs

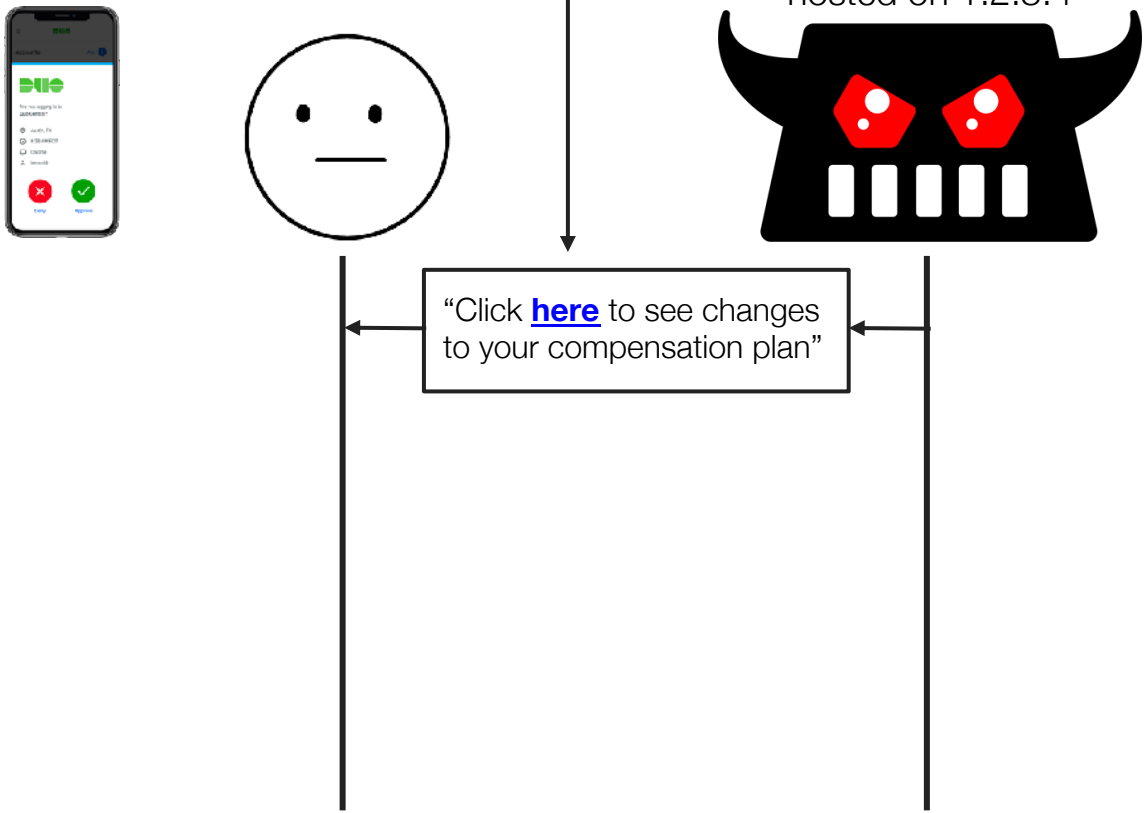
login.duo-secuurity.net

evilginx server
hosted on 1.2.3.4



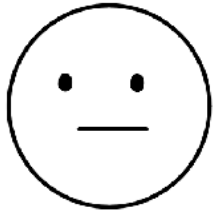


“Click here to see changes to your compensation plan”

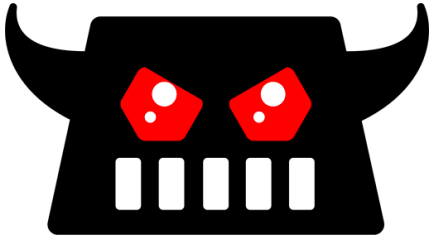


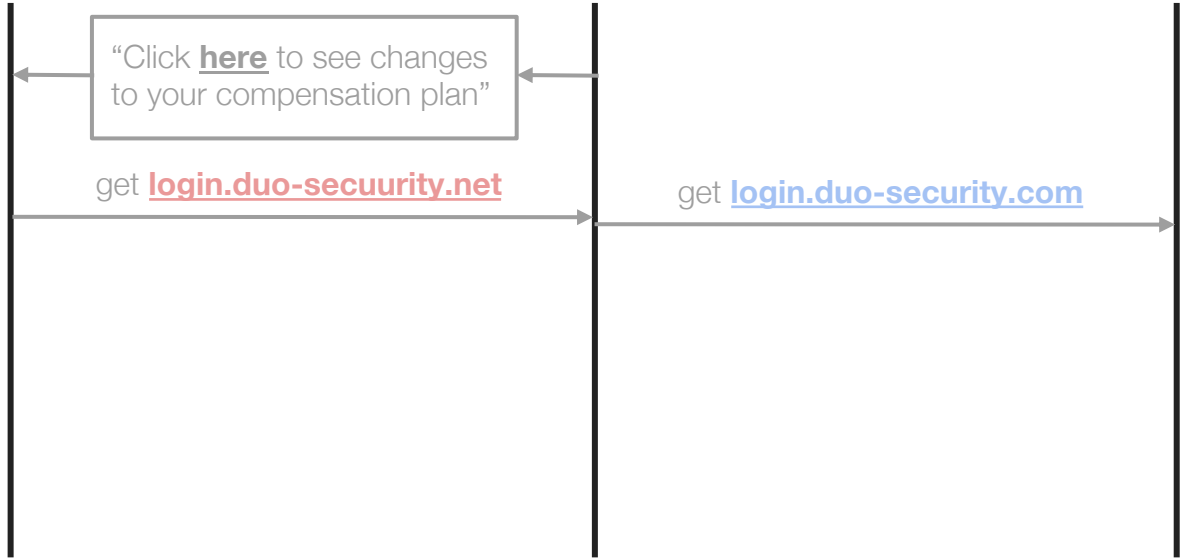
1.2.3.4 is the IP the server sees, and somewhere in DNS, there is a record.

login.duo-secuurity.net -> 1.2.3.4

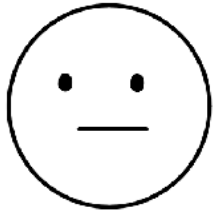


evilginx server
hosted on 1.2.3.4

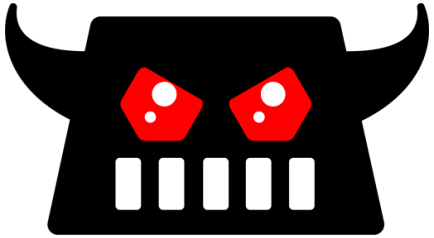


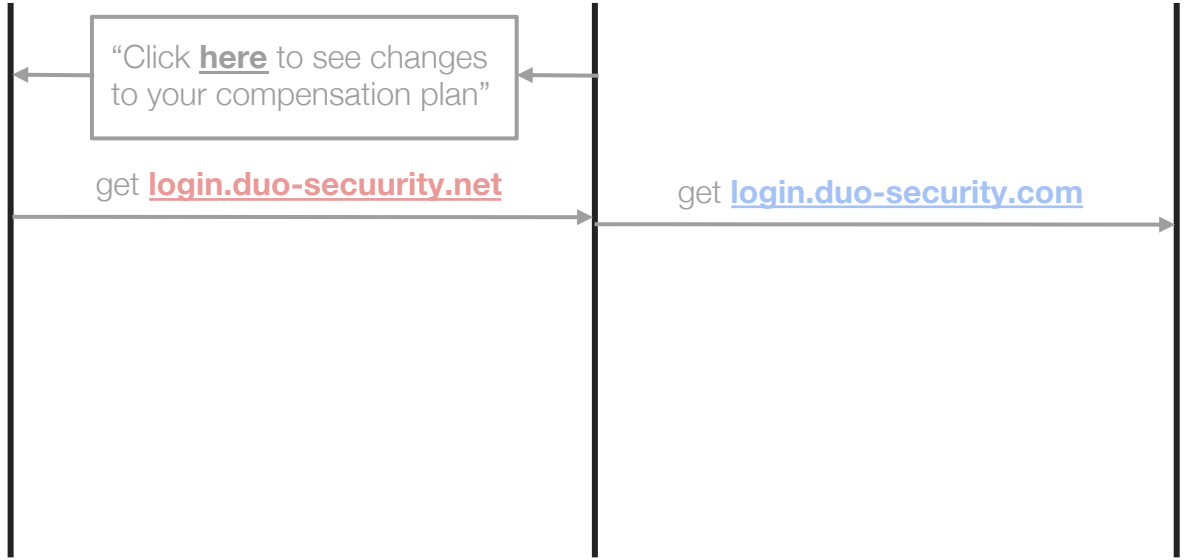


Source IP = 1.2.3.4



evilginx server
hosted on 1.2.3.4





Source IP = 1.2.3.4
… 1.2.3.4 maps to
login.duo-secuurity.net!

DNS Query Data

Enhance!

Farsight DNS Query Data

Record Type	Key	Value	First seen	Last seen
A	duo-secuurity.net	1.2.3.4	1683712810	1684404010
CNAME	login.duo-secuurity.net	duo-secuurity.net	1683712810	1684404010

Farsight DNS Query Data

Record Type	Key	Value	First seen	Last seen
A	duo-secuurity.net	1.2.3.4	1683712810	1684404010
CNAME	login.duo-secuurity.net	duo-secuurity.net	1683712810	1684404010

- Okay great but we need to unfurl all of those recursions

Farsight DNS Query Data

Record Type	Key	Value	First seen	Last seen
A	duo-secuurity.net	1.2.3.4	1683712810	1684404010
CNAME	login.duo-secuurity.net	duo-secuurity.net	1683712810	1684404010

- Okay great but we need to unfurl all of those recursions
- Okay great except this DB is the size of the entire internet (Big™)

Farsight DNS Query Data

Record Type	Key	Value	First seen	Last seen
A	duo-secuurity.net	1.2.3.4	1683712810	1684404010
CNAME	login.duo-secuurity.net	duo-secuurity.net	1683712810	1684404010

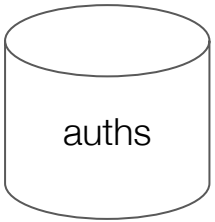
- Okay great but we need to unfurl all of those recursions
- Okay great except this DB is the size of the entire Internet (Big™)

Farsight DNS Query Data

Record Type	Key	Value	First seen	Last seen
A	duo-secuurity.net	1.2.3.4	1683712810	1684404010
CNAME	login.duo-secuurity.net	duo-secuurity.net	1683712810	1684404010

Farsight DNS Query Data

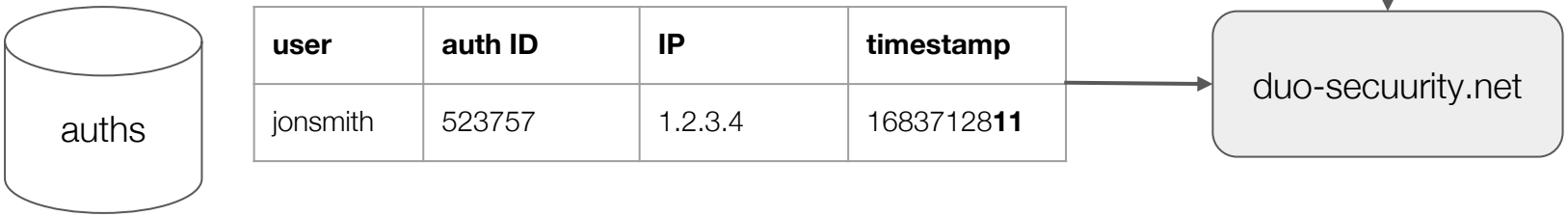
Record Type	Key	Value	First seen	Last seen
A	duo-secuurity.net	1.2.3.4	1683712**10**	1684404010
CNAME	login.duo-secuurity.net	duo-secuurity.net	1683712810	1684404010

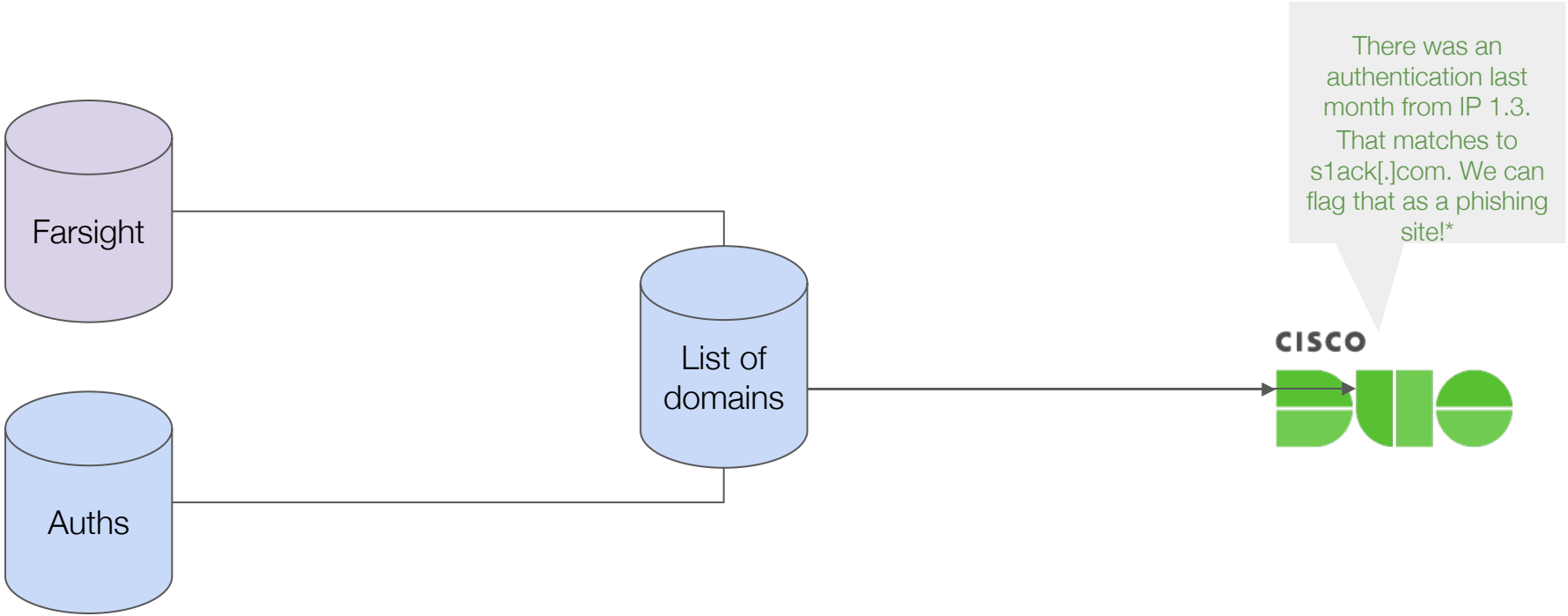


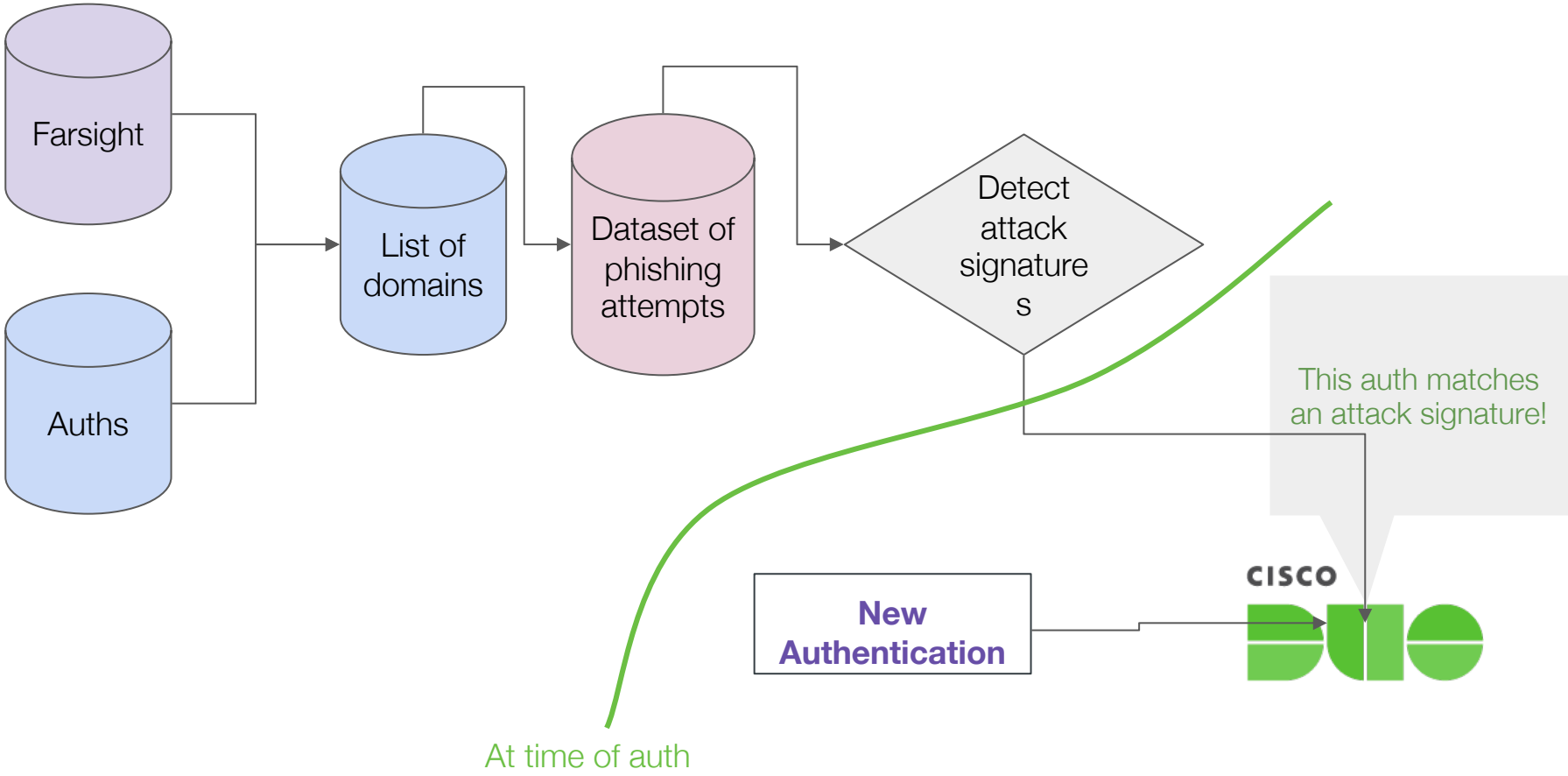
user	auth ID	IP	timestamp
jonsmith	523757	1.2.3.4	1683712**11**

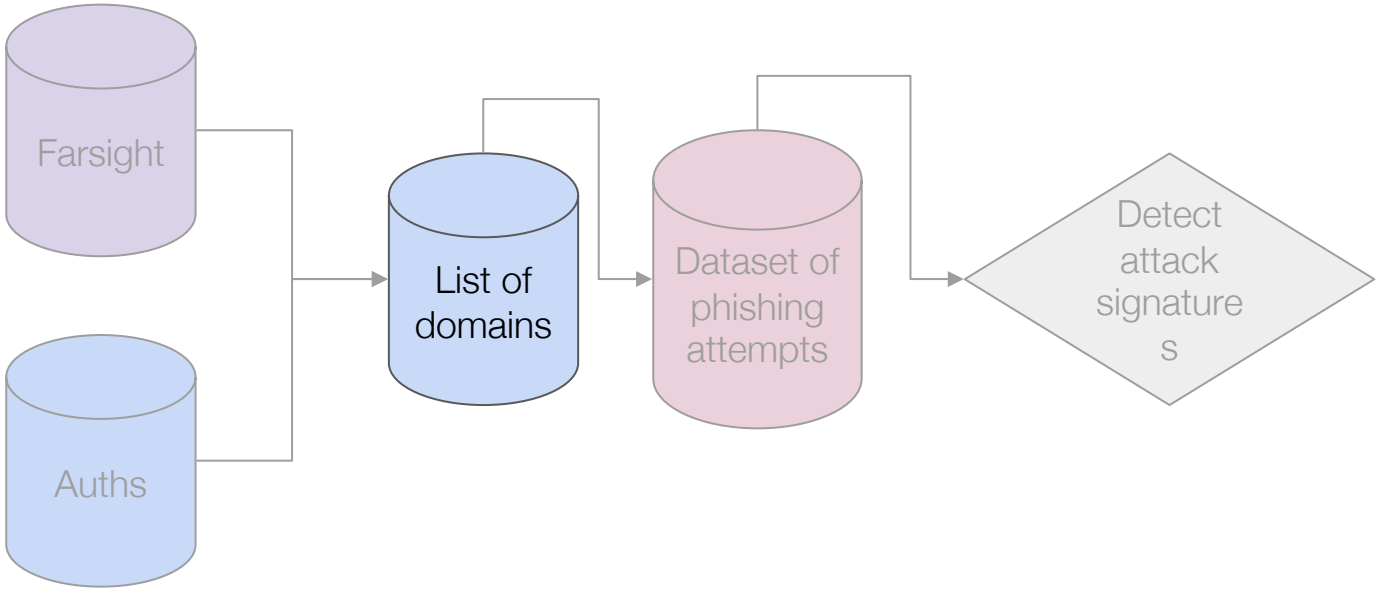
Farsight DNS Query Data

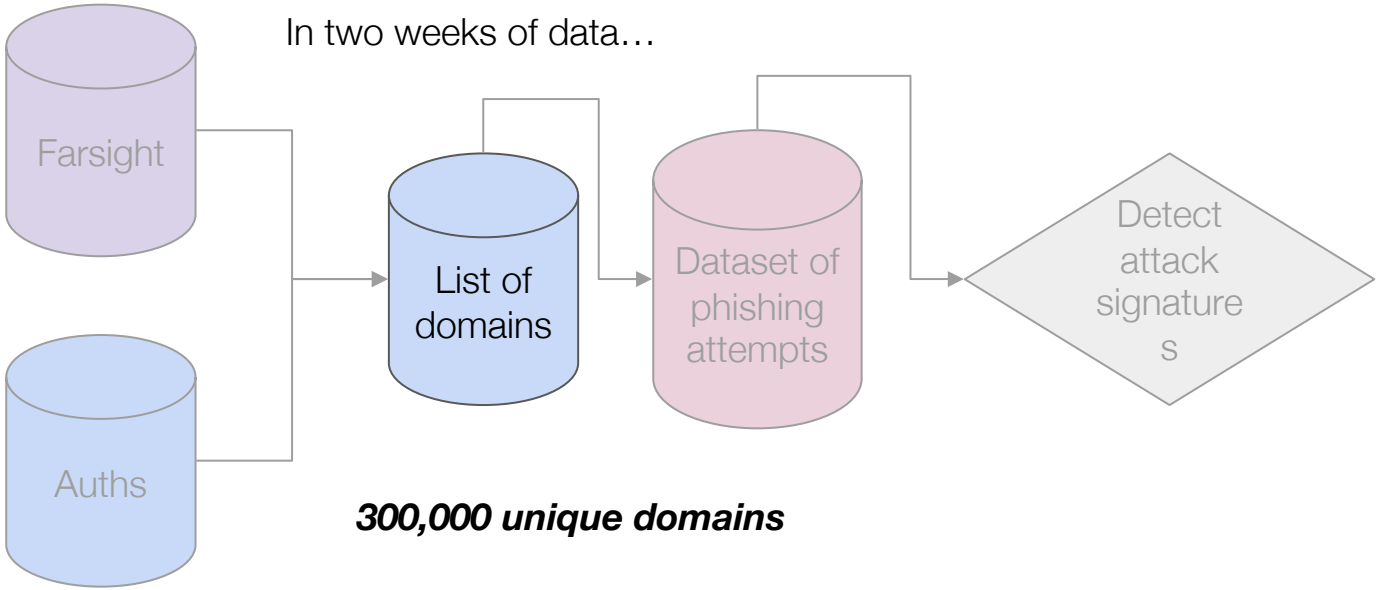
Record Type	Key	Value	First seen	Last seen
A	duo-secuurity.net	1.2.3.4	1683712**10**	1684404010
CNAME	login.duo-secuurity.net	duo-secuurity.net	1683712810	1684404010





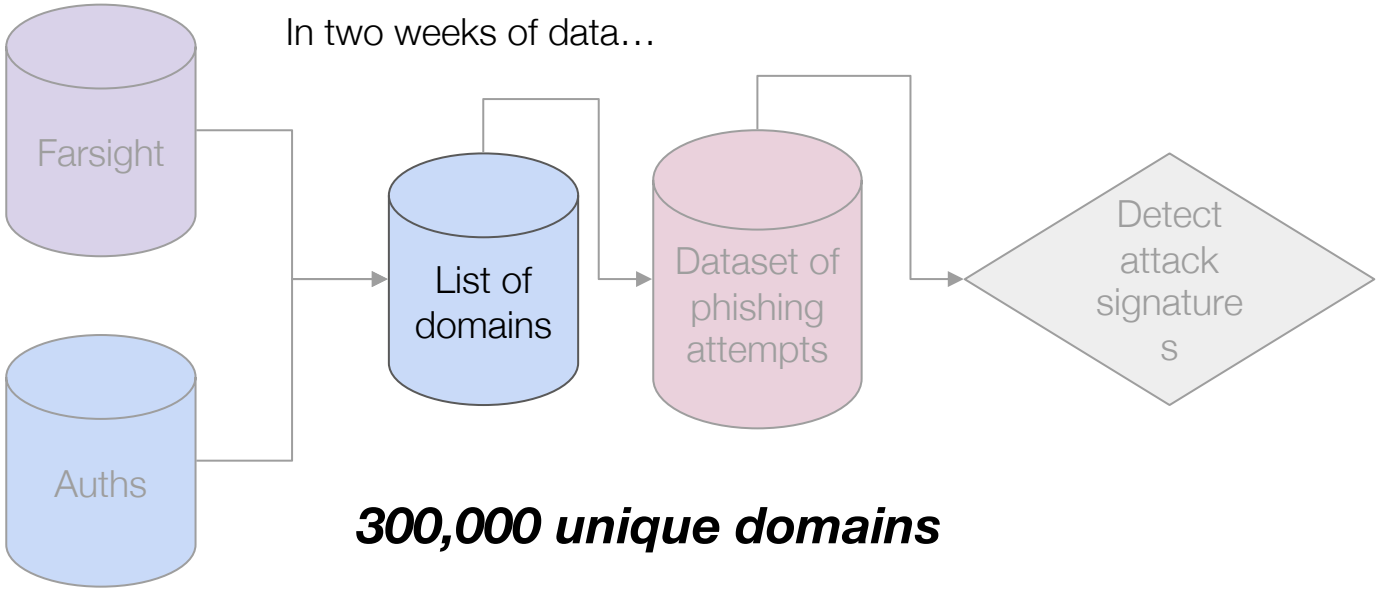






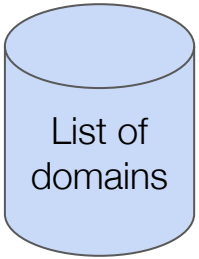
21 million unique IPs

In two weeks of data…

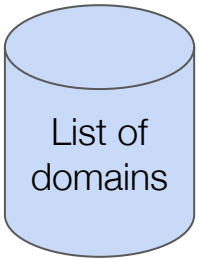


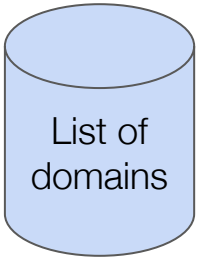
300,000 unique domains

22 million unique IPs



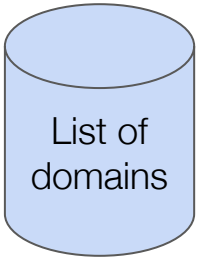
Filter domains ending in **.edu** or **.gov**





Filter domains ending in **.edu** or **.gov**

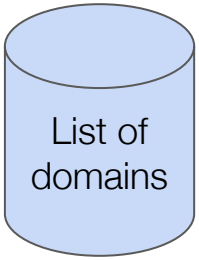
Filter domains older than **one year**



Filter domains ending in **.edu** or **.gov**

Filter domains older than **one year**

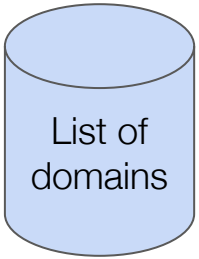
Filter IPs with regular activity from a single user



Filter domains ending in **.edu** or **.gov**

Filter domains older than **one year**

Filter IPs with regular activity from a single user

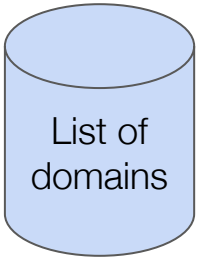


Filter domains ending in **.edu** or **.gov**

Filter domains older than **one year**

Filter IPs with regular activity from a single user

Select domains with phish hints *login, cash, quick, auth*



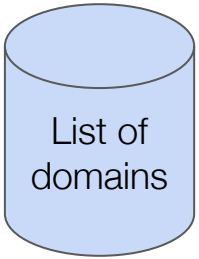
Filter domains ending in **.edu** or **.gov**

Filter domains older than **one year**

Filter IPs with regular activity from a single user

Select domains with phish hints *login, cash, quick, auth*

Select domains that have misspelled brand names



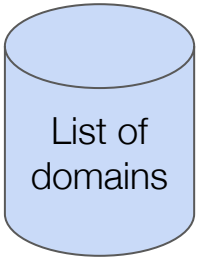
Filter domains ending in **.edu** or **.gov**

Filter domains older than **one year**

Filter IPs with regular activity from a single user

Select domains with phish hints *login, cash, quick, auth*

Select domains that have misspelled brand names



Filter domains ending in **.edu** or **.gov**

Filter domains older than **one year**

Filter IPs with regular activity from a single user

Select domains with phish hints *login, cash, quick, auth*

Select domains that have misspelled brand names

14 domains!

List of domains

Filter domains ending in **.edu** or **.gov**

Filter domains older than **one year**

Filter IPs with regular activity from a single user

Select domains with phish hints *login, cash, quick, auth*

Select domains that have misspelled brand names

14 domains!

Domain	Carrier
package-usps[.]us	Microsoft (Azure)
*[.]zetlandcapitals[.]com	DigitalOcean
criteriacorp[.]microsoftonline[.]app-account-127[.]cloud	DigitalOcean
volvo[.]microsoftonline[.]app-account-140[.]cloud	DigitalOcean
cbeyondata[.]microsoftonline[.]app-account-126[.]cloud	DigitalOcean
b9746927-a325-5d2d-7f91-ca0105ac5f52[.]cnnic[.]rip	Microsoft (Azure)
t3[.]freegradely[.]xyz	RIPE Network Coordination Centre
starburkx[.]com	Clouvider Limited
goodduugfdhqf[.]click	DigitalOcean
clientedesco004[.]descobrresgate[.]com	DigitalOcean
dvfffpyvl[.]mom	DigitalOcean
lswj35[.]suporteswr[.]com	DigitalOcean
uiuvjfkkge[.]buzz	DigitalOcean
wwwofc[.]getgoingmove[.]com	Akamai

Microsoft

Domain	Carrier
package-usps[.]us	Microsoft (Azure)
*[.]zetlandcapitals[.]com	DigitalOcean
criteriacorp[.]microsoftonline[.]app-account-127[.]cloud	DigitalOcean
volvo[.]microsoftonline[.]app-account-140[.]cloud	DigitalOcean
cbeyondata[.]microsoftonline[.]app-account-126[.]cloud	DigitalOcean
b9746927-a325-5d2d-7f91-ca0105ac5f52[.]cnnic[.]rip	Microsoft (Azure)
t3[.]freegradely[.]xyz	RIPE Network Coordination Centre
starburkx[.]com	Clouvider Limited
goodduqfdhqf[.]click	DigitalOcean
clientedesco004[.]descobrresgate[.]com	DigitalOcean
dvfffpyvl[.]mom	DigitalOcean
lswj35[.]suporteswr[.]com	DigitalOcean
uiuvjfkkge[.]buzz	DigitalOcean
wwwofc[.]getgoingmove[.]com	Akamai

USPS

Domain	Carrier
package-usps[.]us	Microsoft (Azure)
*[.]zetlandcapitals[.]com	DigitalOcean
criteriacorp[.]microsoftonline[.]app-account-127[.]cloud	DigitalOcean
volvo[.]microsoftonline[.]app-account-140[.]cloud	DigitalOcean
cbeyondata[.]microsoftonline[.]app-account-126[.]cloud	DigitalOcean
b9746927-a325-5d2d-7f91-ca0105ac5f52[.]cnnic[.]rip	Microsoft (Azure)
t3[.]freegradely[.]xyz	RIPE Network Coordination Centre
starburkx[.]com	Clouvider Limited
goodduqfdhqf[.]click	DigitalOcean
clientedesco004[.]descobrresgate[.]com	DigitalOcean
dvfffpyvl[.]mom	DigitalOcean
lswj35[.]suporteswr[.]com	DigitalOcean
uiuvjfkkge[.]buzz	DigitalOcean
wwwofc[.]getgoingmove[.]com	Akamai

Uni Tools

Domain	Carrier
package-usps[.]us	Microsoft (Azure)
*[.]zetlandcapitals[.]com	DigitalOcean
criteriacorp[.]microsoftonline[.]app-account-127[.]cloud	DigitalOcean
volvo[.]microsoftonline[.]app-account-140[.]cloud	DigitalOcean
cbeyondata[.]microsoftonline[.]app-account-126[.]cloud	DigitalOcean
b9746927-a325-5d2d-7f91-ca0105ac5f52[.]cnnic[.]rip	Microsoft (Azure)
t3[.]freegradely[.]xyz	RIPE Network Coordination Centre
starburkx[.]com	Clouvider Limited
goodduugfdhqf[.]click	DigitalOcean
clientedesco004[.]descobrresgate[.]com	DigitalOcean
dvfffpyvl[.]mom	DigitalOcean
lswj35[.]suporteswr[.]com	DigitalOcean
uiuvjfkkge[.]buzz	DigitalOcean
wwwofc[.]getgoingmove[.]com	Akamai

STARBURKX

Domain	Carrier
package-usps[.]us	Microsoft (Azure)
*[.]zetlandcapitals[.]com	DigitalOcean
criteriacorp[.]microsoftonline[.]app-account-127[.]cloud	DigitalOcean
volvo[.]microsoftonline[.]app-account-140[.]cloud	DigitalOcean
cbeyondata[.]microsoftonline[.]app-account-126[.]cloud	DigitalOcean
b9746927-a325-5d2d-7f91-ca0105ac5f52[.]cnnic[.]rip	Microsoft (Azure)
t3[.]freegradely[.]xyz	RIPE Network Coordination Centre
starburkx[.]com	Clouvider Limited
goodduugfdhqf[.]click	DigitalOcean
clientedesco004[.]descobrresgate[.]com	DigitalOcean
dvfffpyvl[.]mom	DigitalOcean
lswj35[.]suporteswr[.]com	DigitalOcean
uiuvjfkkge[.]buzz	DigitalOcean
wwwofc[.]getgoingmove[.]com	Akamai

All auth data in 2023 was pulled

+

Auths through phish domain IPs were labeled **malicious**

+

For impacted users…

All auth data in 2023 was pulled

+

Auths through phish domain IPs were labeled **malicious**

+

77 malicious

12,561 benign

For impacted users…

Rolling Per-User Features

Probabilities generated by observing the 90 days of auths prior to current auth being evaluated

+ p(access IP country)
+ p(access IP state)
+ p(ASN + application)
+ p(MFA factor + application)
+ p(OS + application)

Rolling Per-User Features

+ p(access IP country)
+ p(access IP state)
+ p(ASN + application)
+ p(MFA factor + application)
+ p(OS + application)
+ ASN had changed since prior auth

DUO | cisco SECURE

Rolling Per-User Features

+ p(access IP country)
+ p(access IP state)
+ p(ASN + application)
+ p(MFA factor + application)
+ p(OS + application)
+ ASN had changed since prior auth
+ Whether ASN and IP are novel within org's authentications

Rolling Per-User Features

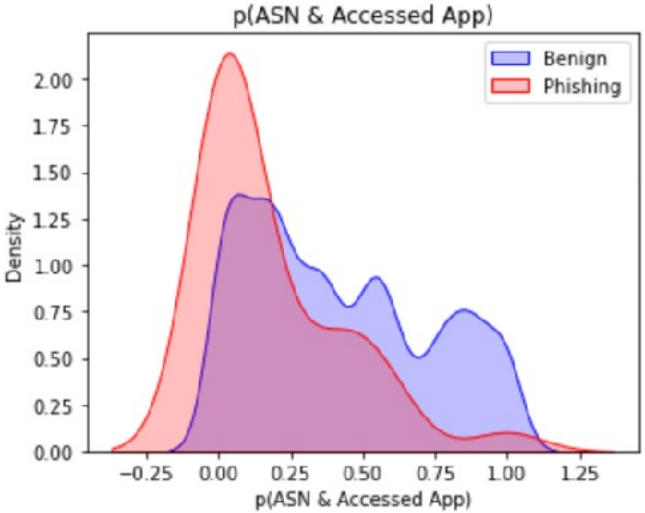
+ p(access IP country)
+ p(access IP state)
+ p(ASN + application)
+ p(MFA factor + application)
+ p(OS + application)
+ ASN had changed since prior auth
+ Whether ASN and IP are novel within org's authentications
+ Whether IP has been seen in a *different* org's authentications in 24 hrs prior

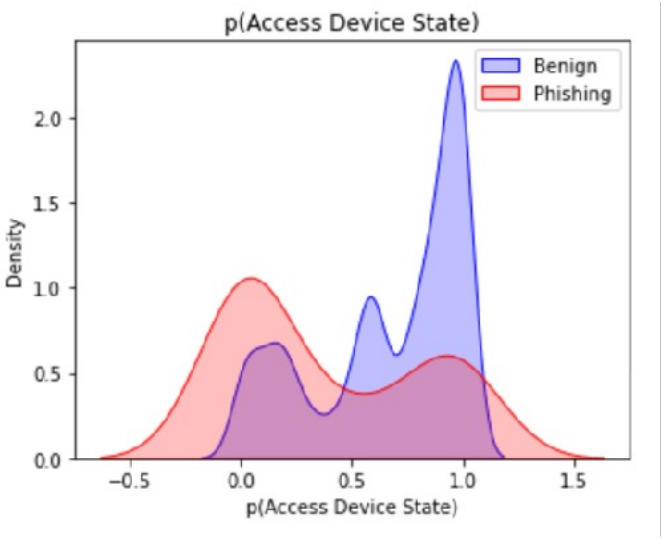
DUO | cisco SECURE

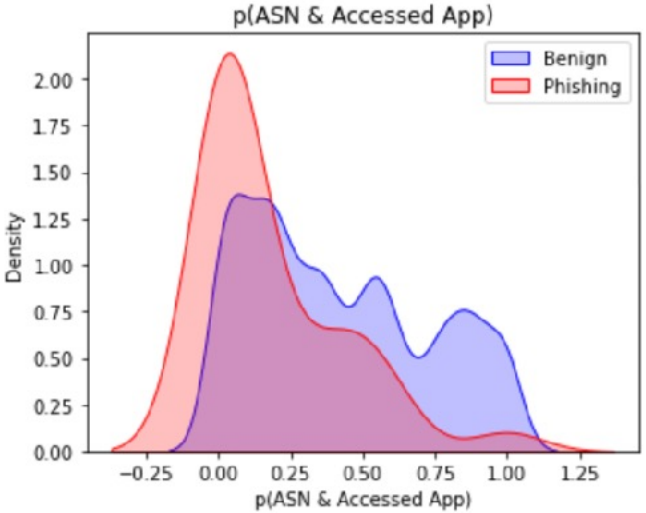
Rolling Per-User Features

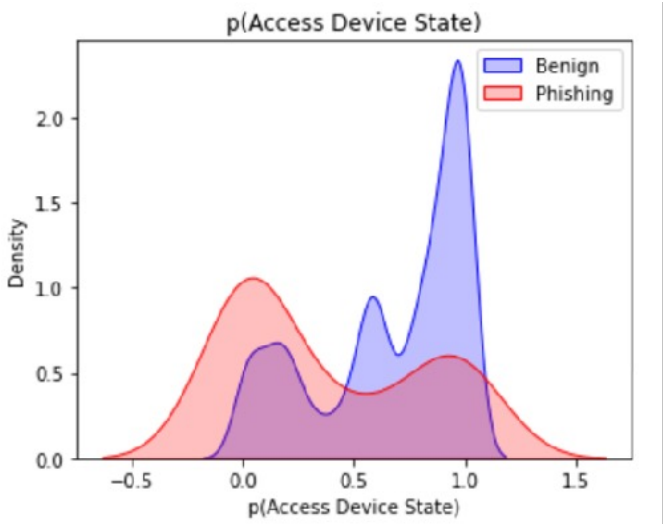
- p(access IP country)
- p(access IP state)
- p(ASN + application)
- p(MFA factor + application)
- p(OS + application)
- ASN had changed since prior auth
- Whether ASN and IP are novel within org's authentications
- Whether IP has been seen in a *different* org's authentications in 24 hrs prior
- Distance between auth and prior auth
- Mean distance between auth and prior 10

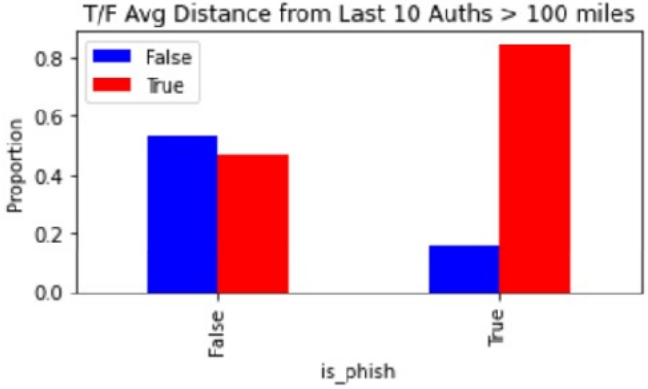
DUO | cisco SECURE

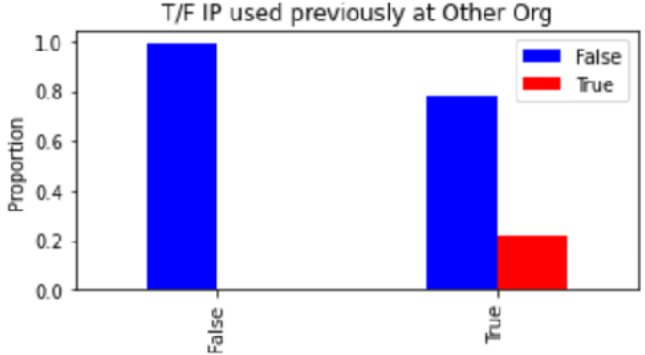












Because this is an ML conference…

We threw some classifiers at it

XGBoost

Recall: 0.63

Precision: 0.02**

LightGBM

Recall: 0.61

Precision: 0.05**

We threw some classifiers at it

XGBoost

Recall: 0.63

Precision: 0.02**

LightGBM

Recall: 0.61

Precision: 0.05**

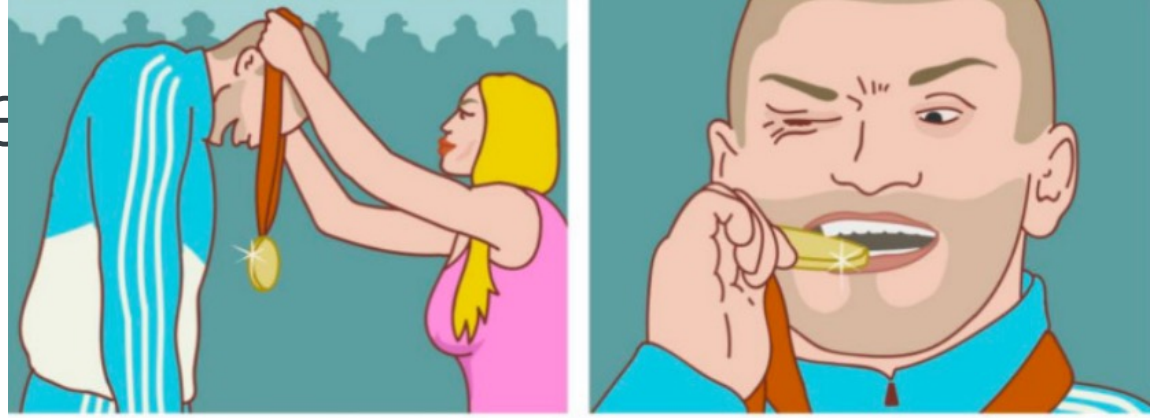
** this was classified purely on the features outlined, with none of the real time metrics that would prevent false positives:
remembered devices, wifi fingerprinting, trusted network policies, etc

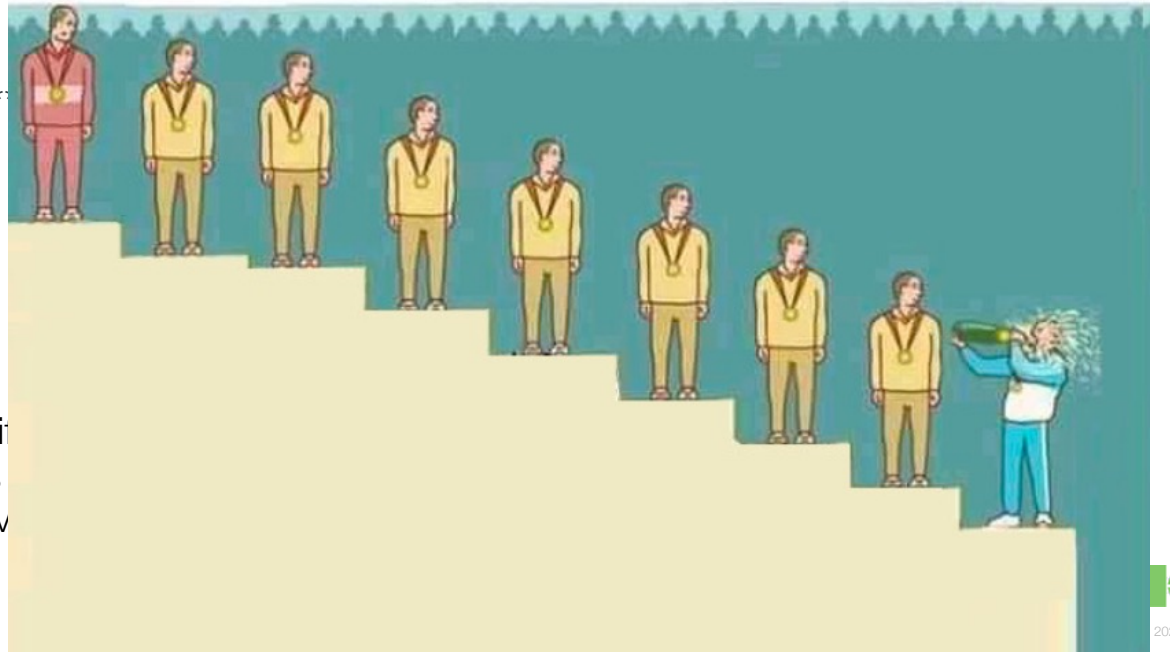
We thre

XGBoost

Recall: 0.63

Precision: 0.02**

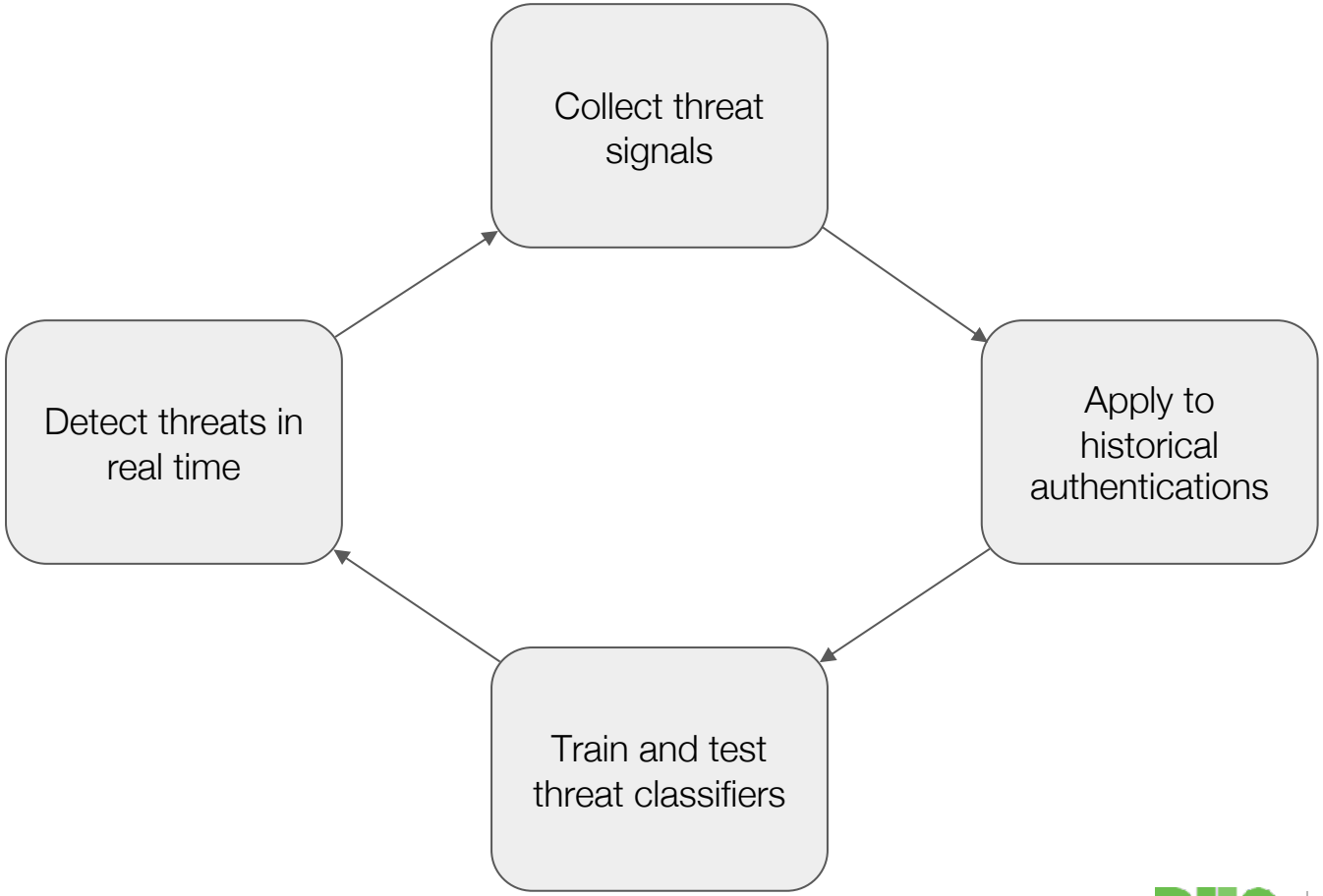


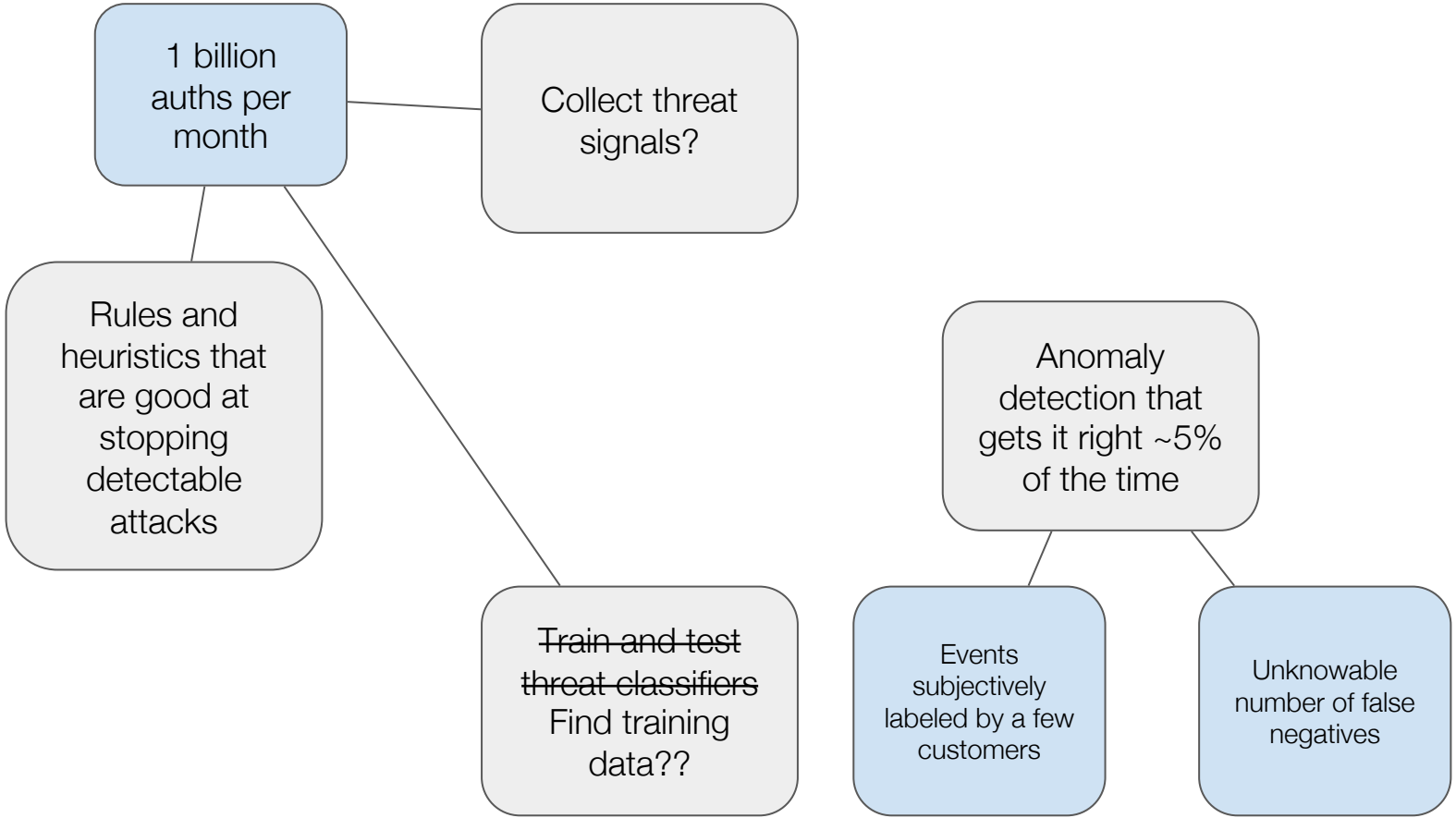


** this was classi
real time metrics
remembered dev

Good news, a perfect classifier isn’t the goal

…Yet!





1 billion auths per month

Collect threat signals?

Rules and heuristics that are good at stopping detectable attacks

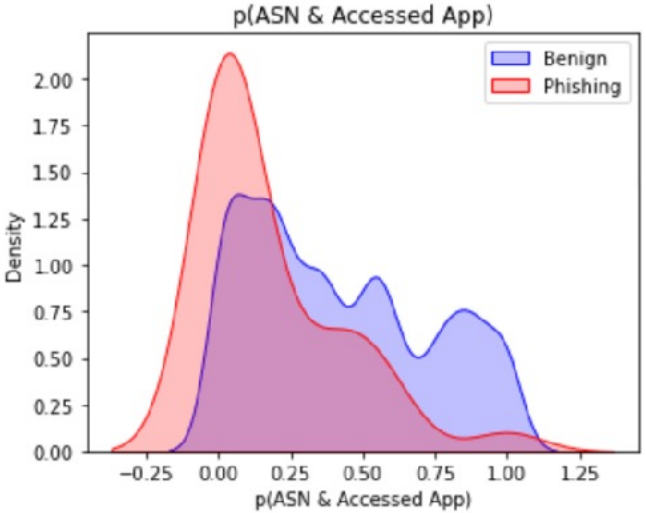
~~Train and test threat classifiers~~ Find training data??

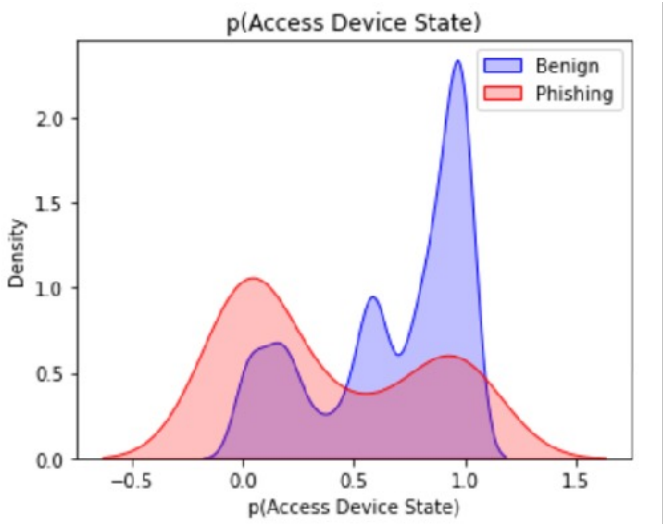
Anomaly detection that gets it right ~5% of the time

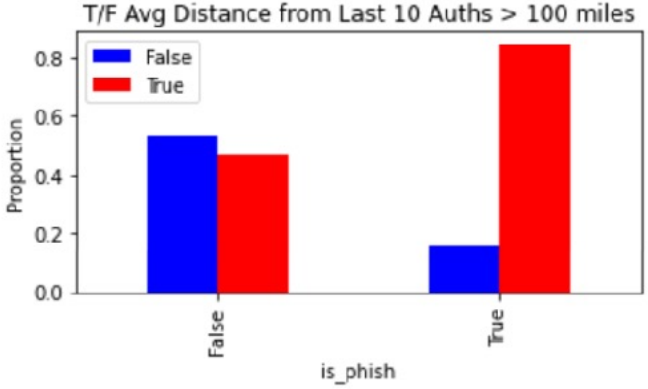
Events subjectively labeled by a few customers

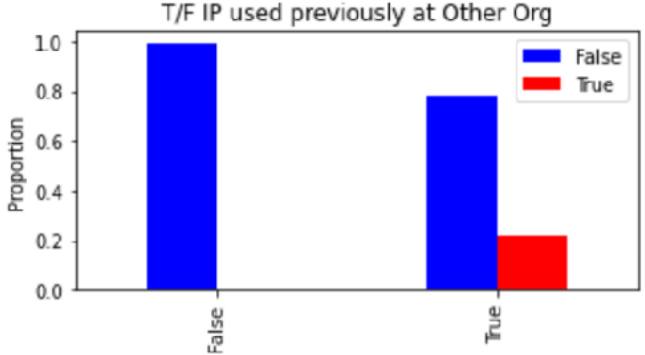
Unknowable number of false negatives

We didn’t fail at classification, we found a repeatable way to find more threat signals!

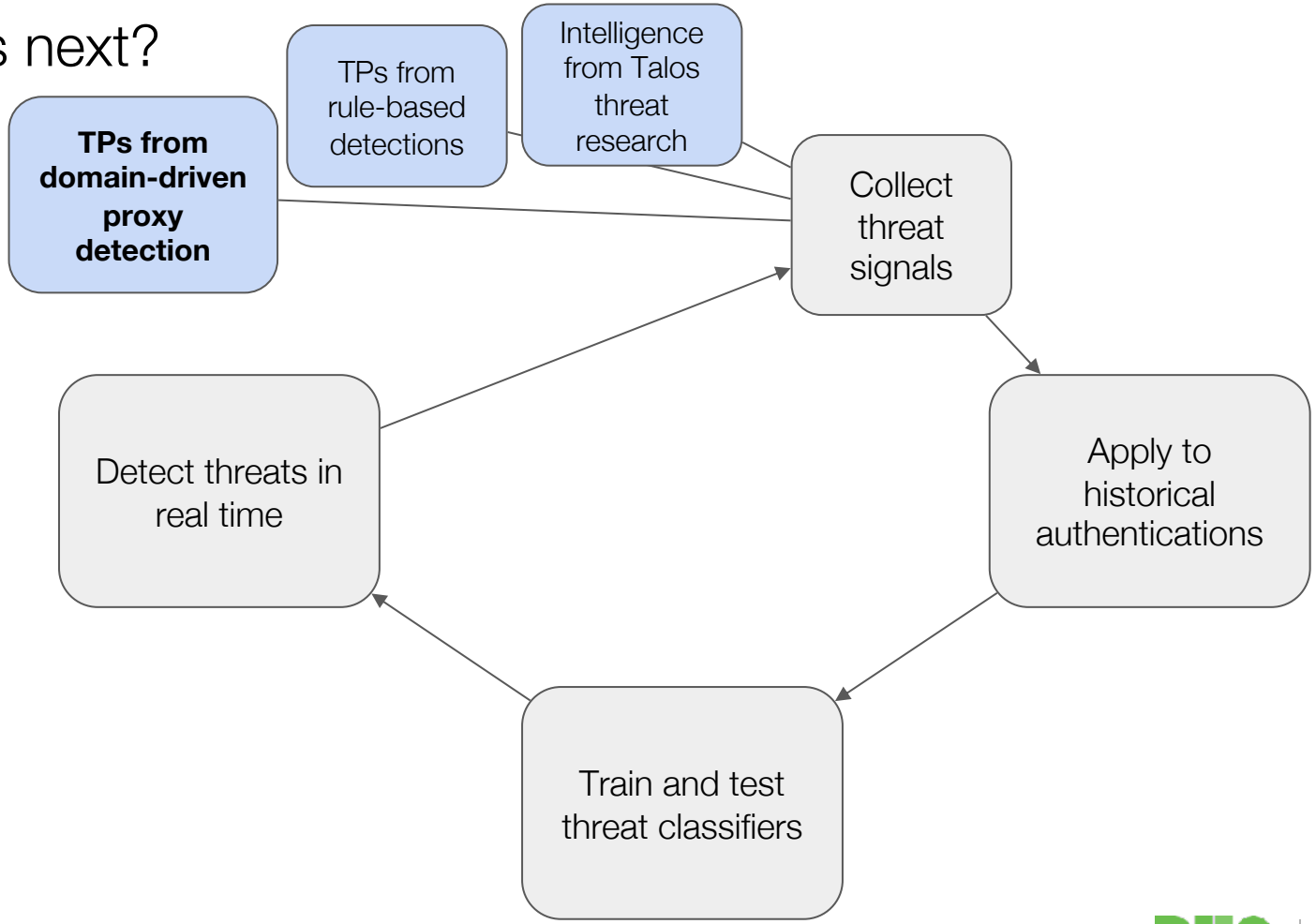








What's next?



Questions?