How to End Password Reuse On the Web

Ke Coby Wang ***Michael K. Reiter***

University of North Carolina at Chapel Hill

THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL

Password Reuse

same user,

same or similar password,

multiple websites.

Password Reuse

same user,

same or similar password,

multiple websites.

According to studies in past twenty years, most of users reuse same/similar passwords across multiple websites.

Leaked Passwords

Announced data breaches in the past **two months**:

GAMES WARNING: MASSIVE data breach leaks passwords for PS4, Xbox On

A MASS
here's w

Photography site 500px resets 14.8 million passwords after data breach

15 FEB 2019 3

Security

620 million accounts stolen from 16 hacked websites now for sale on dark web, seller boasts

Coinmama suffers a data breach of 450,000 emails and hashed passwords

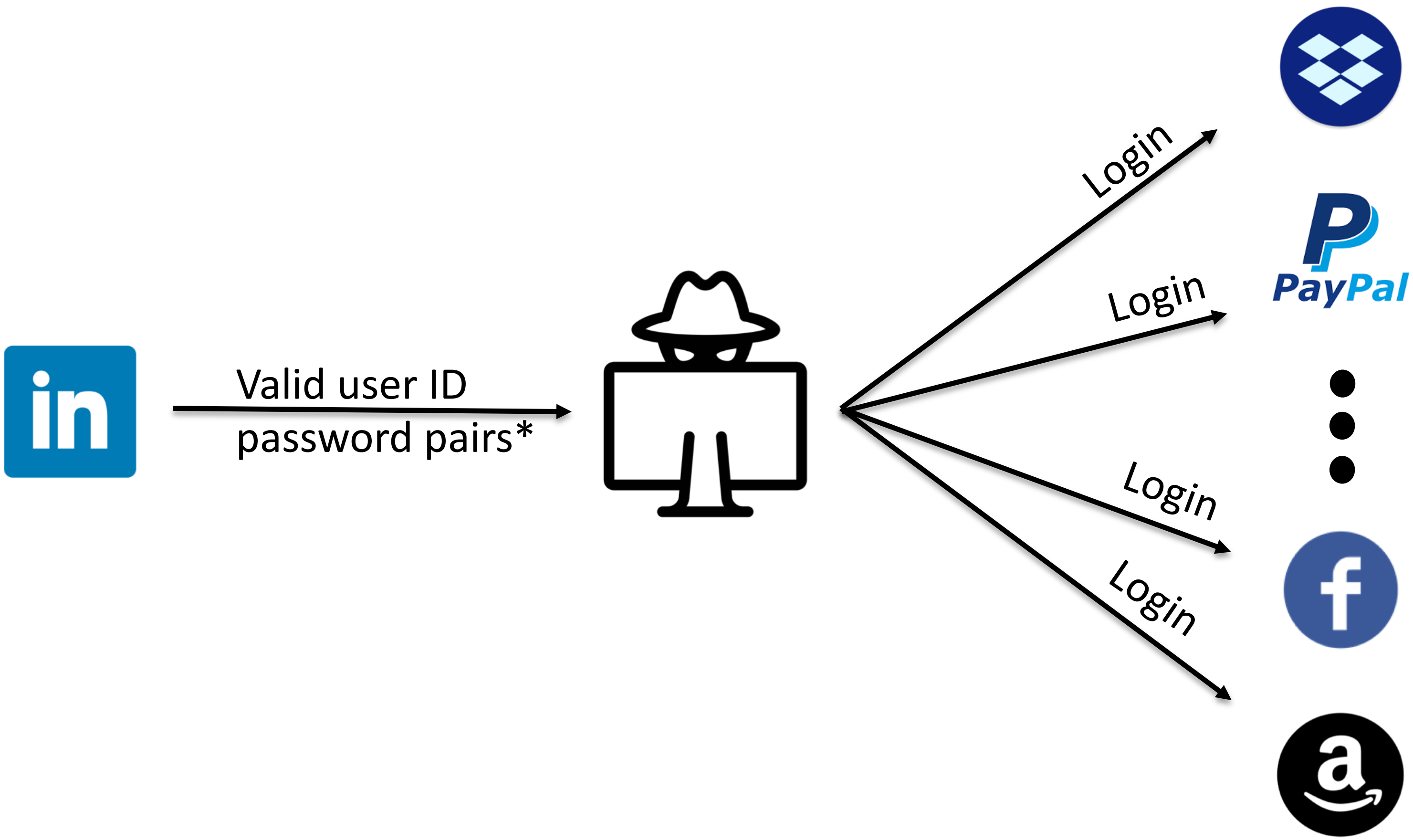
Coinmama, a crypto broker that specializes in letting users buy cryptocurrencies with credit cards, announced Friday that it suffered a a data breach of 450,000 emails and ... f a much ... s. Coinmama ... ssword.

The 773 Million Record "Collection #1" Data Breach

Houzz discloses data breach, asks some users to reset passwords

Citing an ongoing investigation, the company wouldn't say how or when the incident occurred

Credential Stuffing



* via database breaches, phishing, malware, social engineering, etc.

The reuse of passwords is the No. 1 cause of harm on the internet.

--- Alex Stamos (former CSO, Facebook)

99% of compromised user accounts come from password reuse.

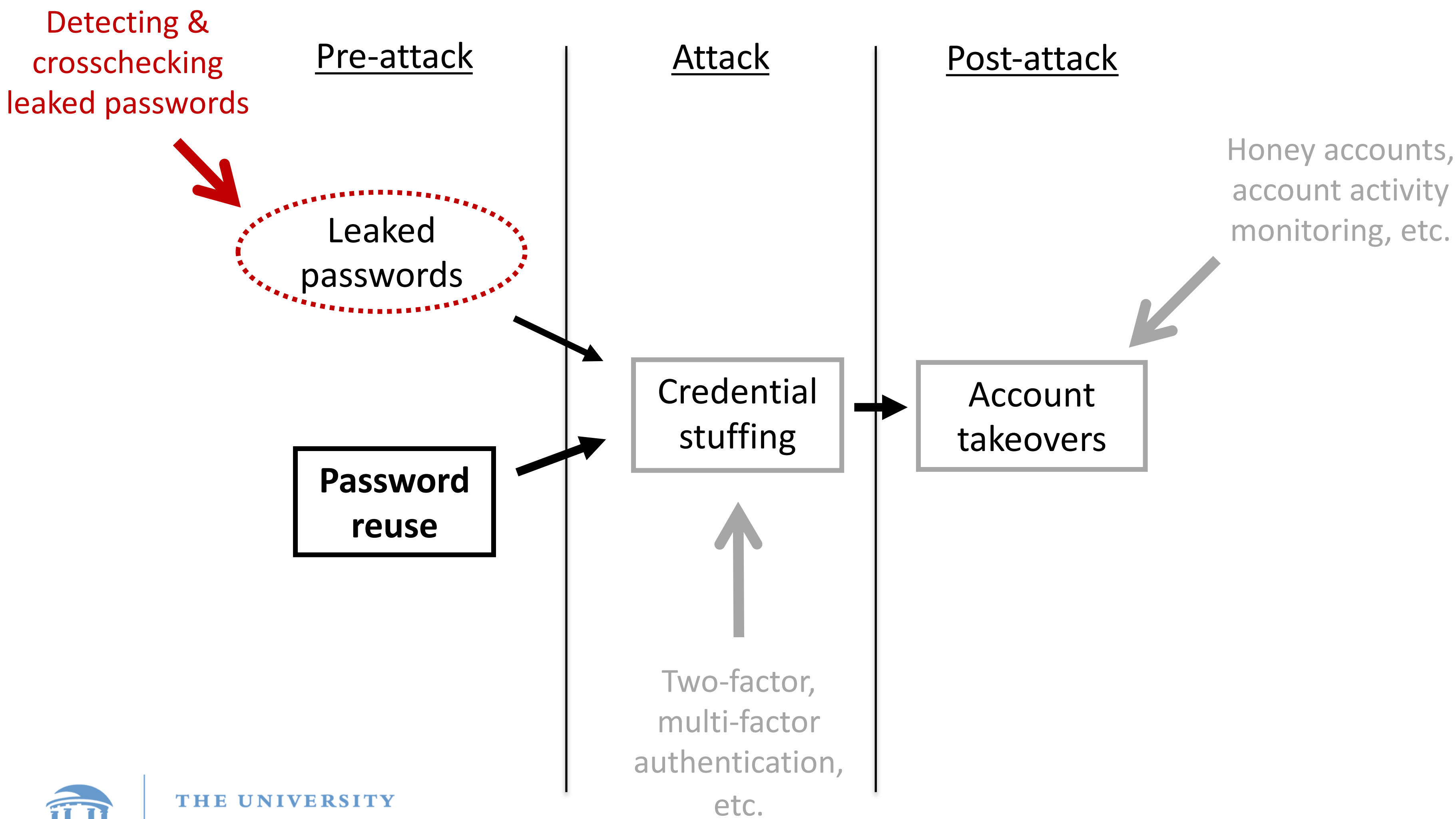
--- Patrick Heim (Head of Trust & Security, Dropbox)

Credential stuffing is enormously effective due to the password reuse problem.

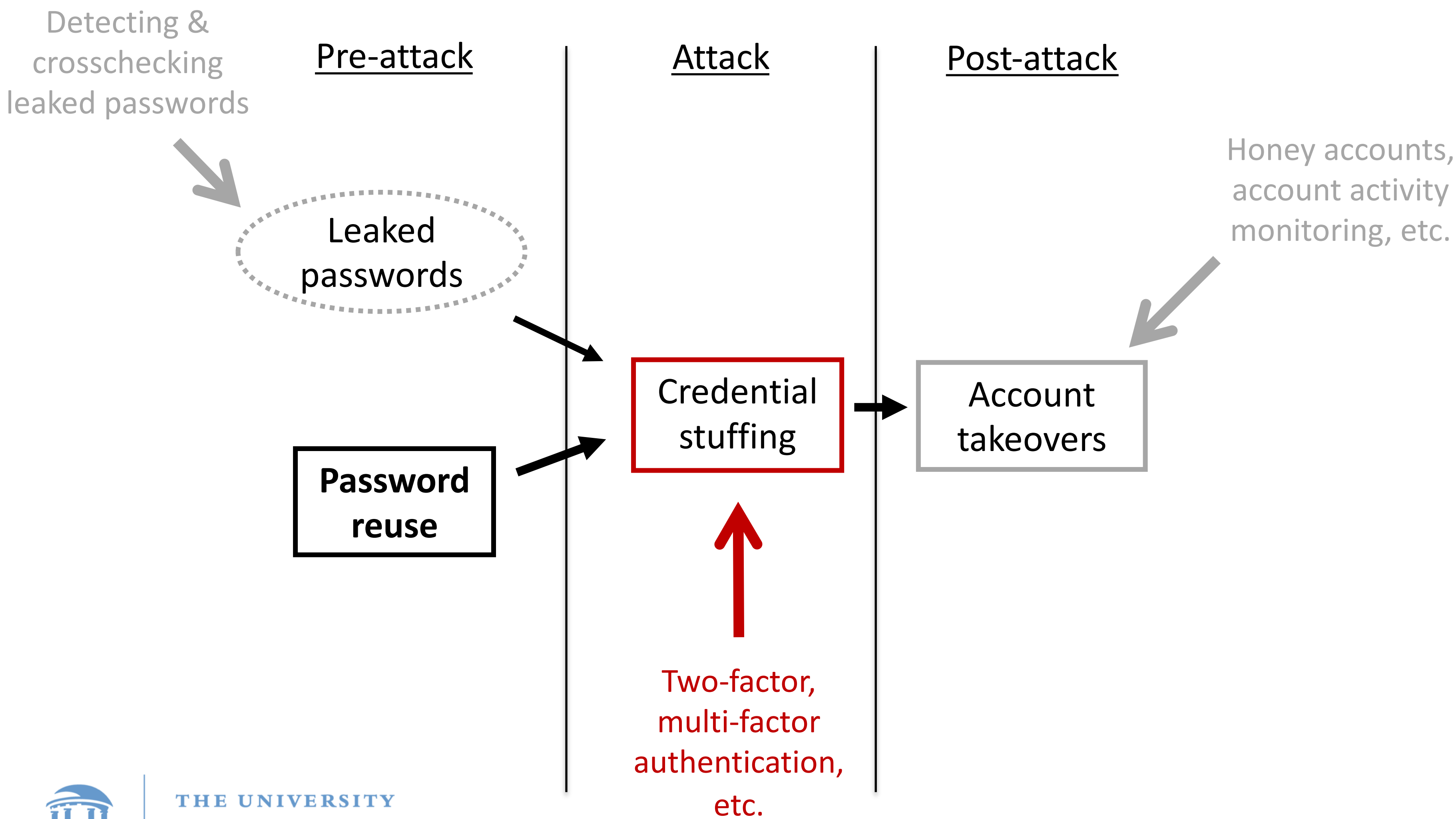
--- Troy Hunt (Regional Director, Microsoft)

* via database breaches, phishing, malware, social engineering, etc.

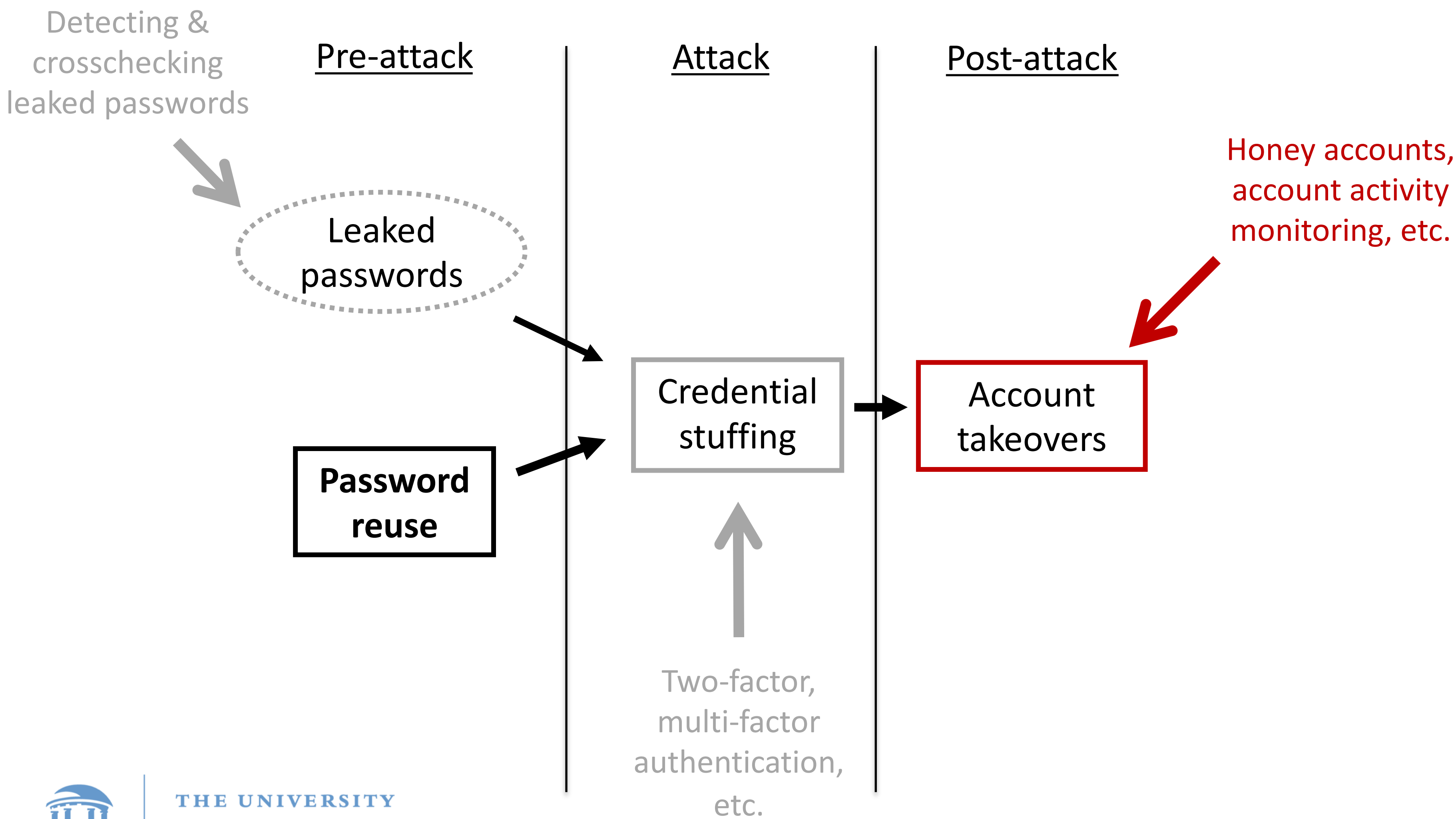
Existing Works



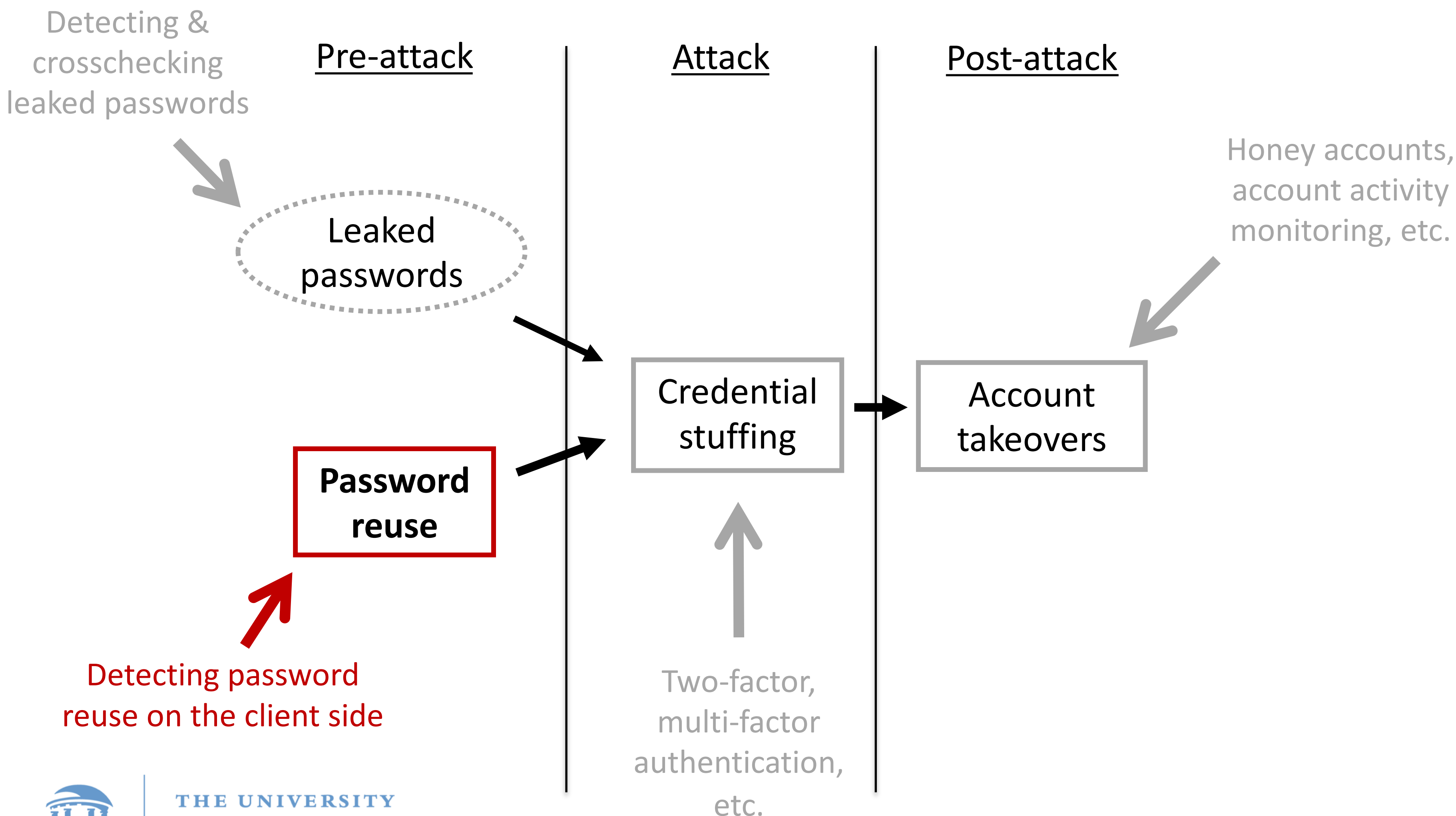
Existing Works



Existing Works

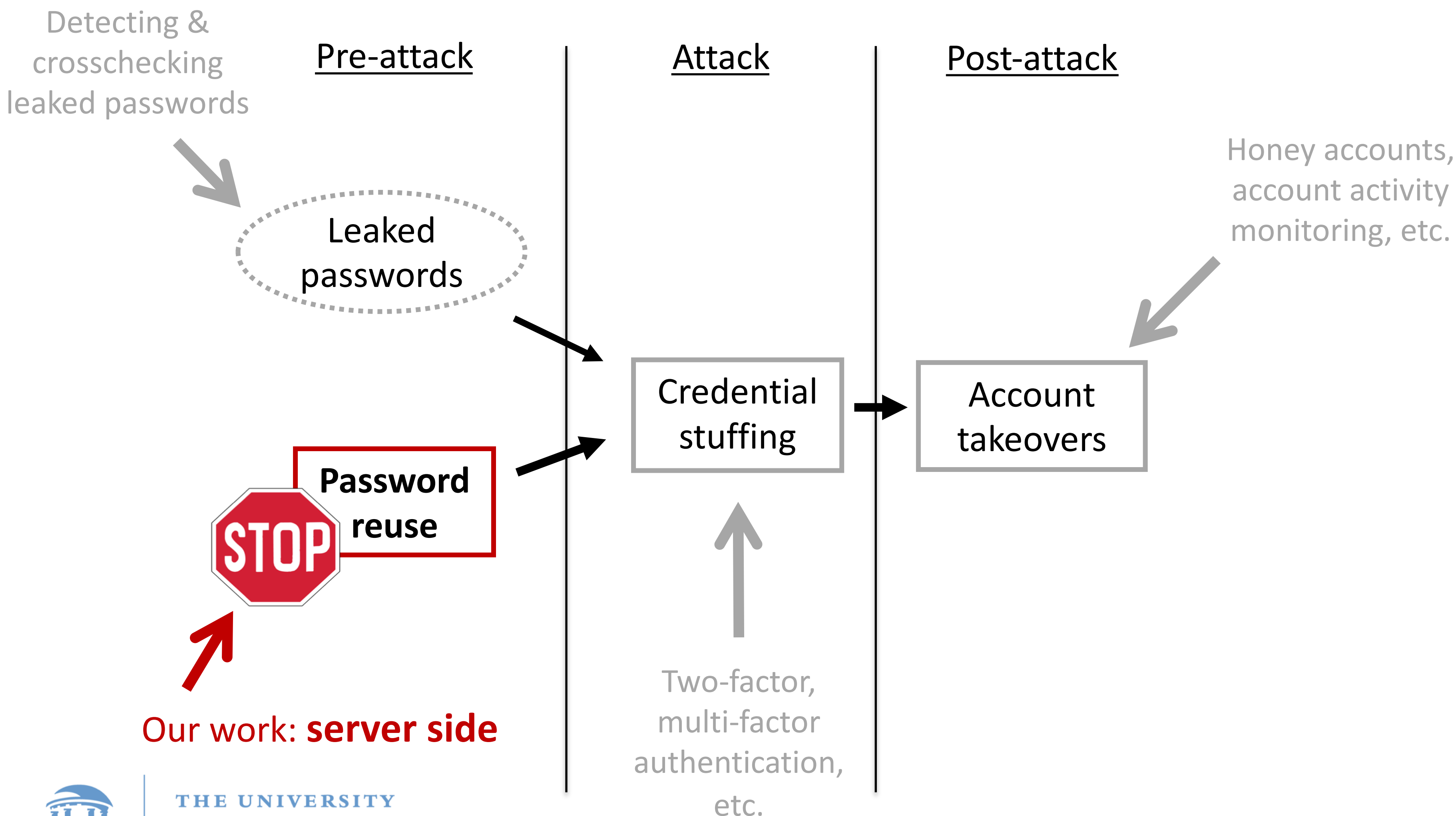


Existing Works



THE UNIVERSITY *of* NORTH CAROLINA *at* CHAPEL HILL

Our Work


Detecting & crosschecking leaked passwords
Pre-attack
Attack
Post-attack
Honey accounts, account activity monitoring, etc.
Leaked passwords
Credential stuffing
Account takeovers
Password reuse
STOP
Two-factor, multi-factor authentication, etc.
Our work: **server side**

Goals

Functionality

Functionality

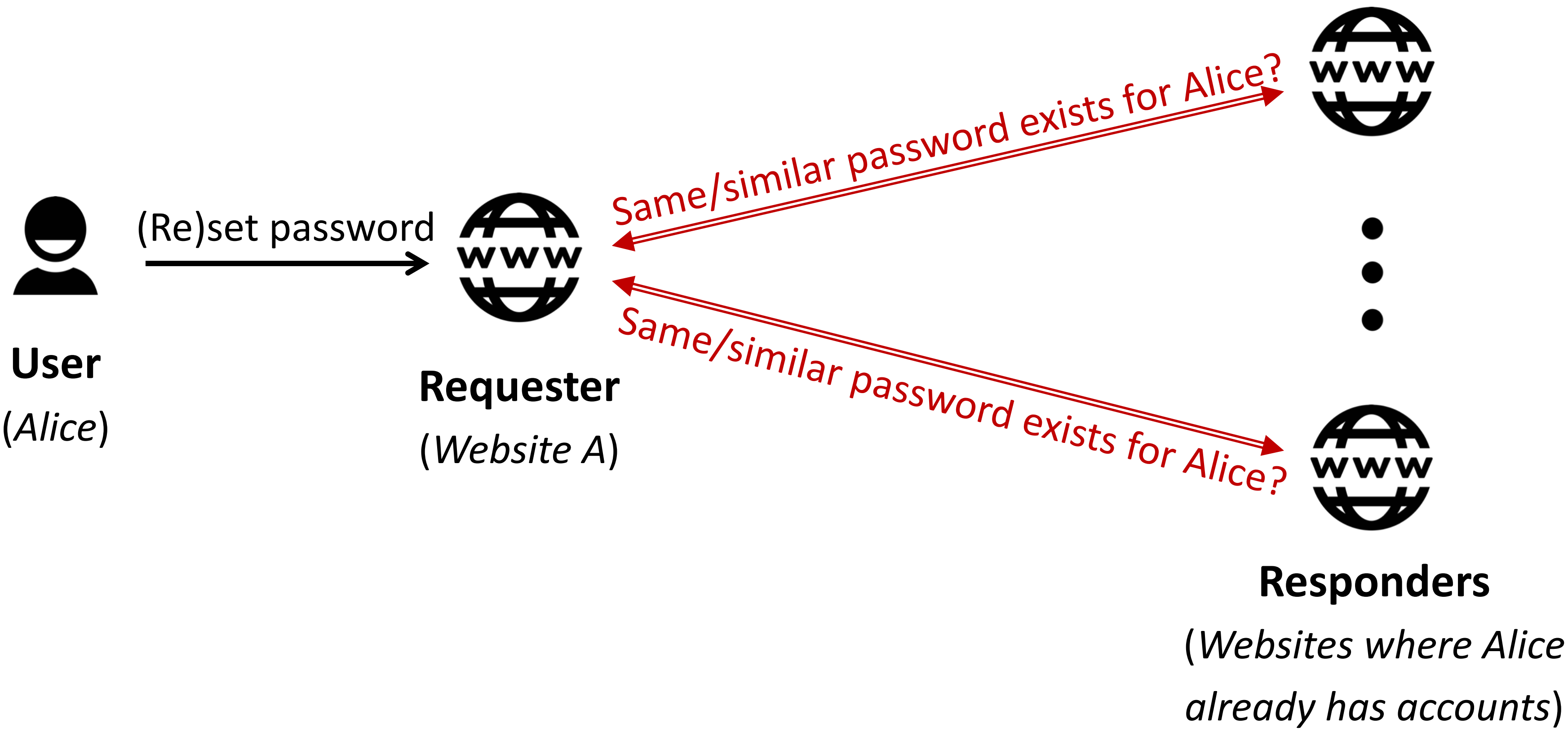
User

(*Alice*)

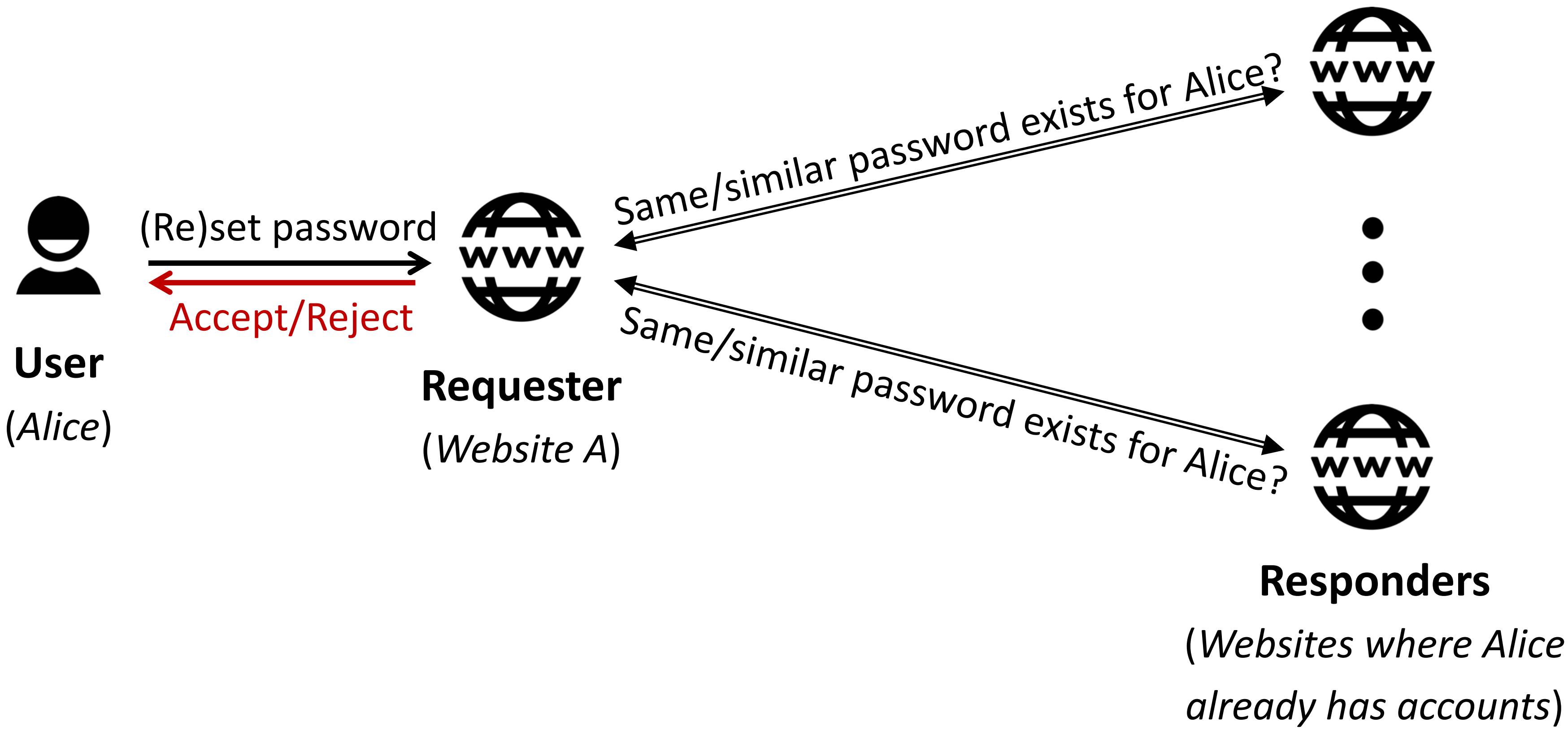
Requester

(*Website A*)

Functionality



Functionality



THE UNIVERSITY *of* NORTH CAROLINA *at* CHAPEL HILL

Security and Privacy Goals

Security and Privacy Goals

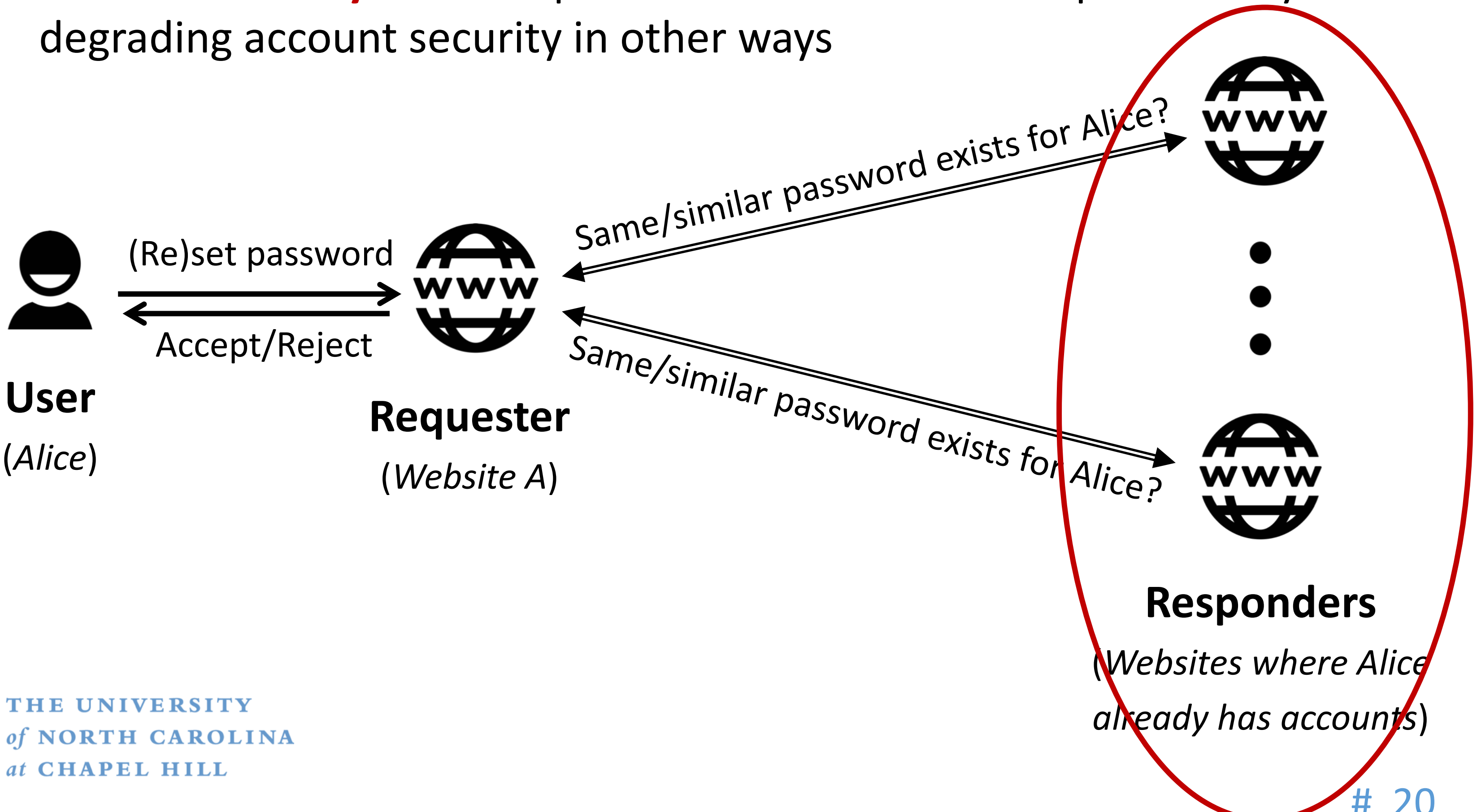
- **Account location privacy**: Participating websites are not disclosed to one another

Security and Privacy Goals

- **Account location privacy**: Participating websites are not disclosed to one another
- **Account security**: Prevent password reuse while not qualitatively degrading account security in other ways

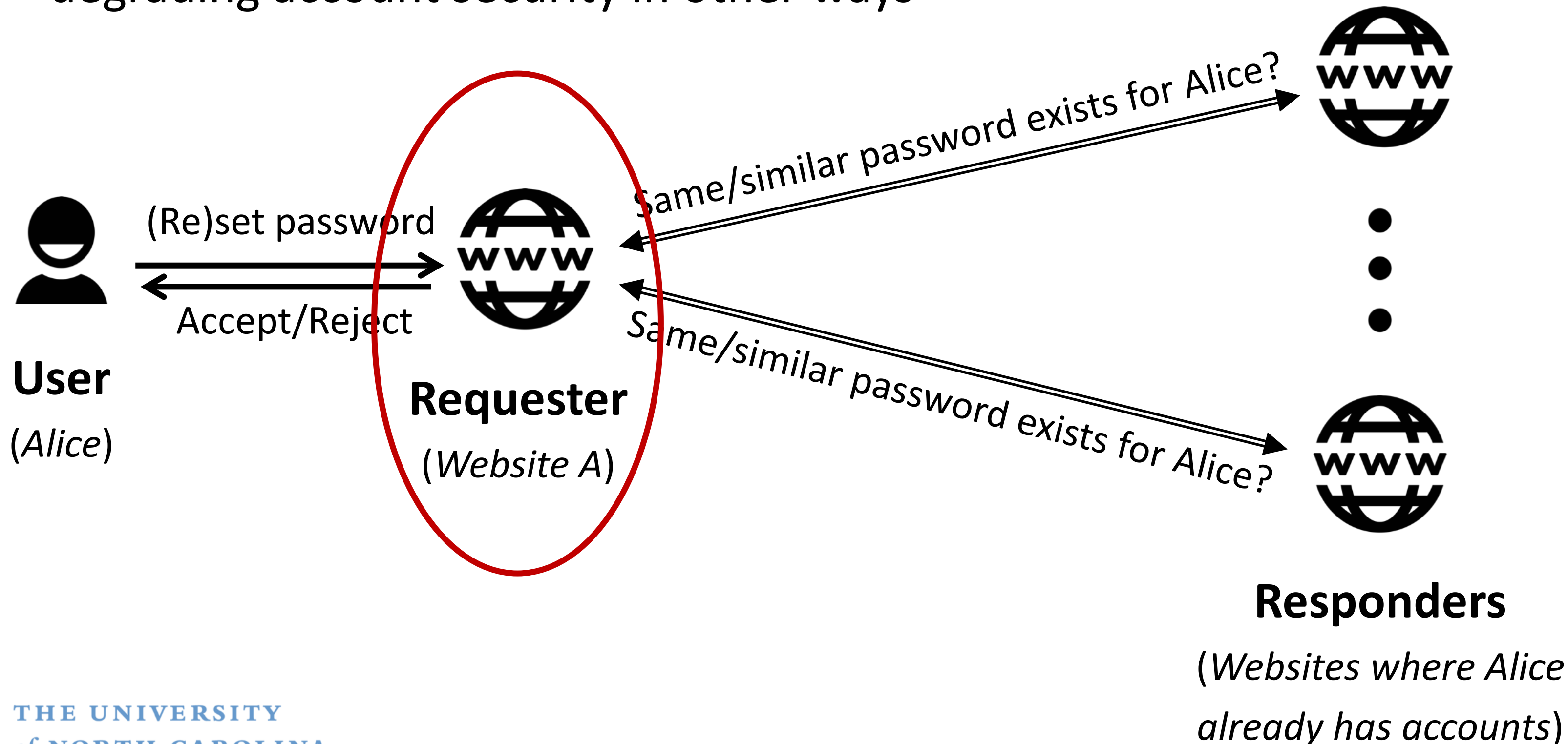
Security and Privacy Goals

- **Account location privacy**: Participating websites are not disclosed to one another
- **Account security**: Prevent password reuse while not qualitatively degrading account security in other ways



Security and Privacy Goals

- **Account location privacy**: Participating websites are not disclosed to one another
- **Account security**: Prevent password reuse while not qualitatively degrading account security in other ways



THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Design

Key Elements in Framework Design

- **Private Membership Test (PMT) protocol**
  - A building block

Key Elements in Framework Design

- Private Membership Test (PMT) protocol
  - A building block
- **Directory**
  - A 3rd party

Key Elements in Framework Design

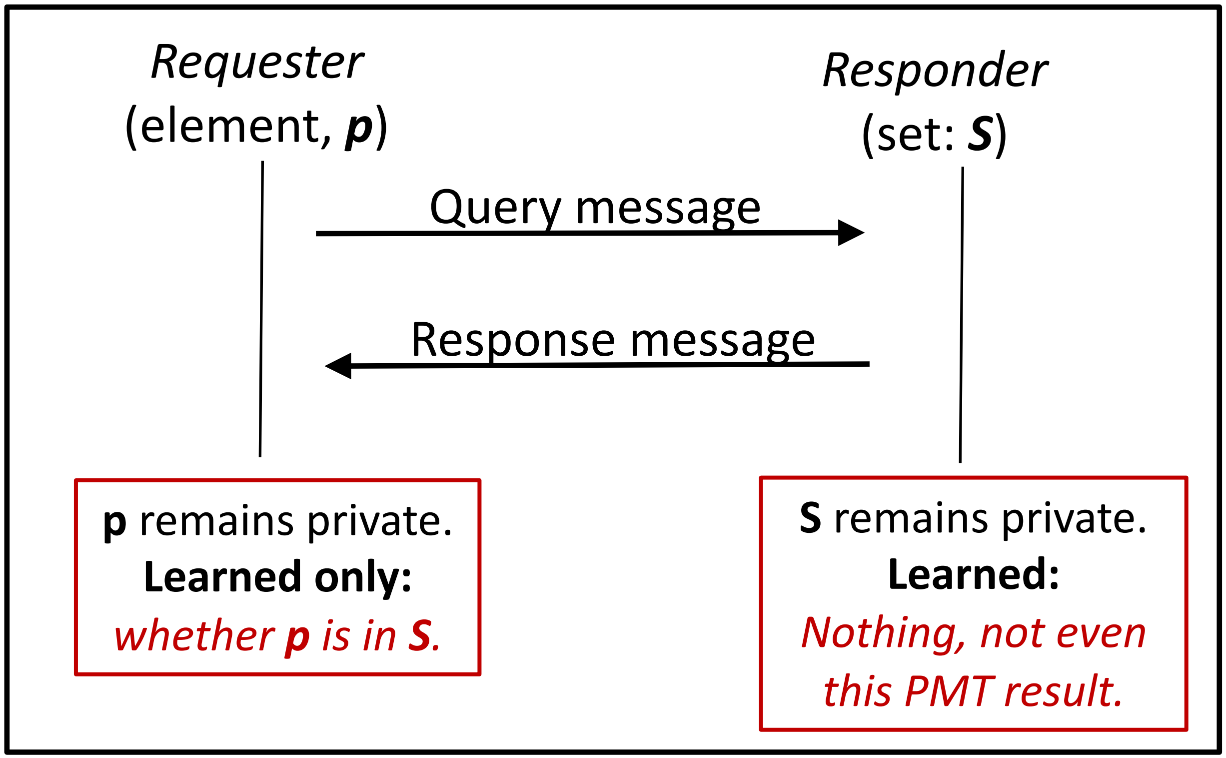
- Private Membership Test (PMT) protocol
  - A building block
- Directory
  - A 3rd party
- **Techniques for account location privacy**

Key Elements in Framework Design

- Private Membership Test (PMT) protocol
  - A building block
- Directory
  - A 3rd party
- Techniques for account location privacy
- **Countermeasures for information leakage**

Private Membership Test (PMT)

Membership Test: Is *p* in *S* ?



PMT Application

User

(*Alice*)

Requester

(*Website A*)

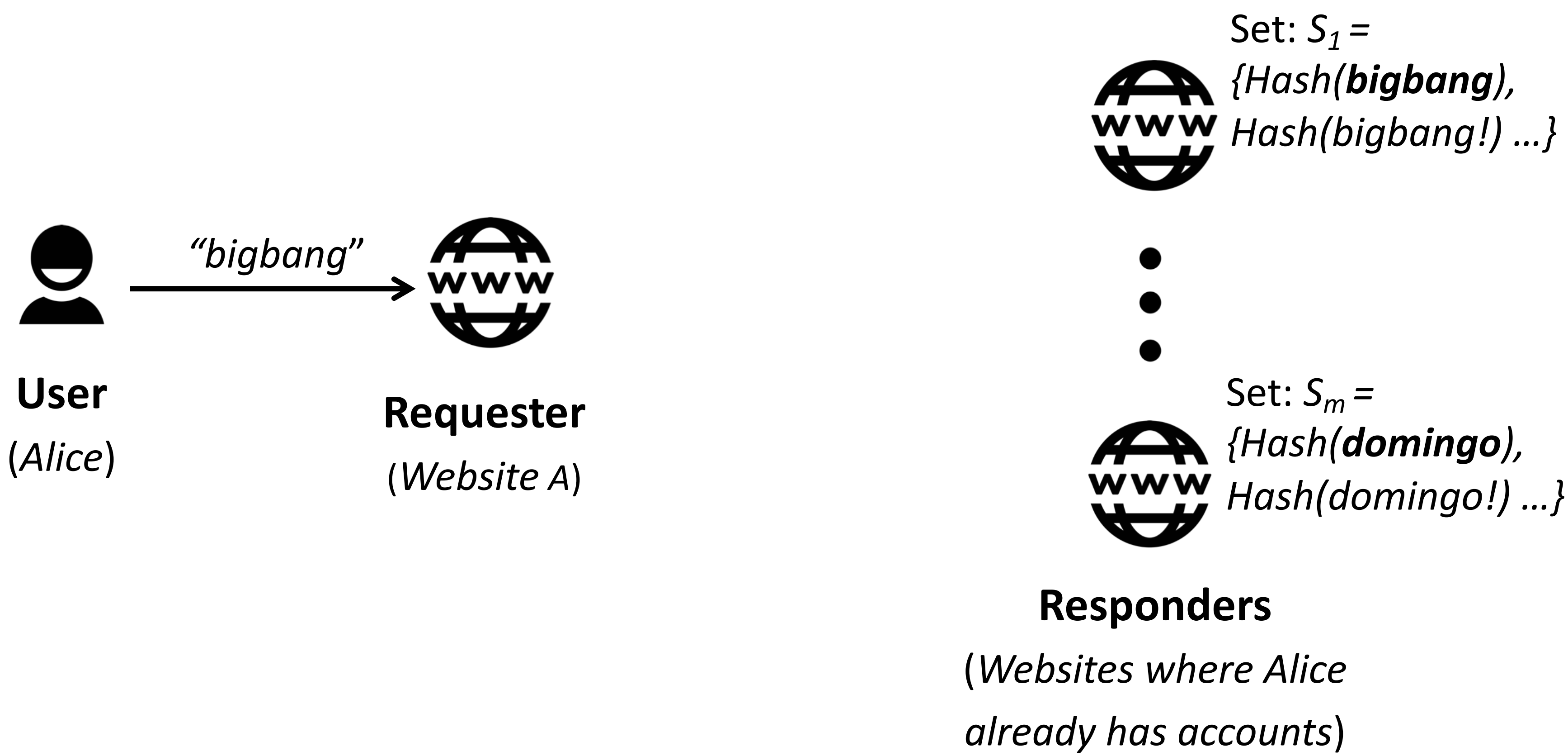
Set: S_1 =
*{Hash(**bigbang**),*
Hash(bigbang!) ...}

Set: S_m =
*{Hash(**domingo**),*
Hash(domingo!) ...}

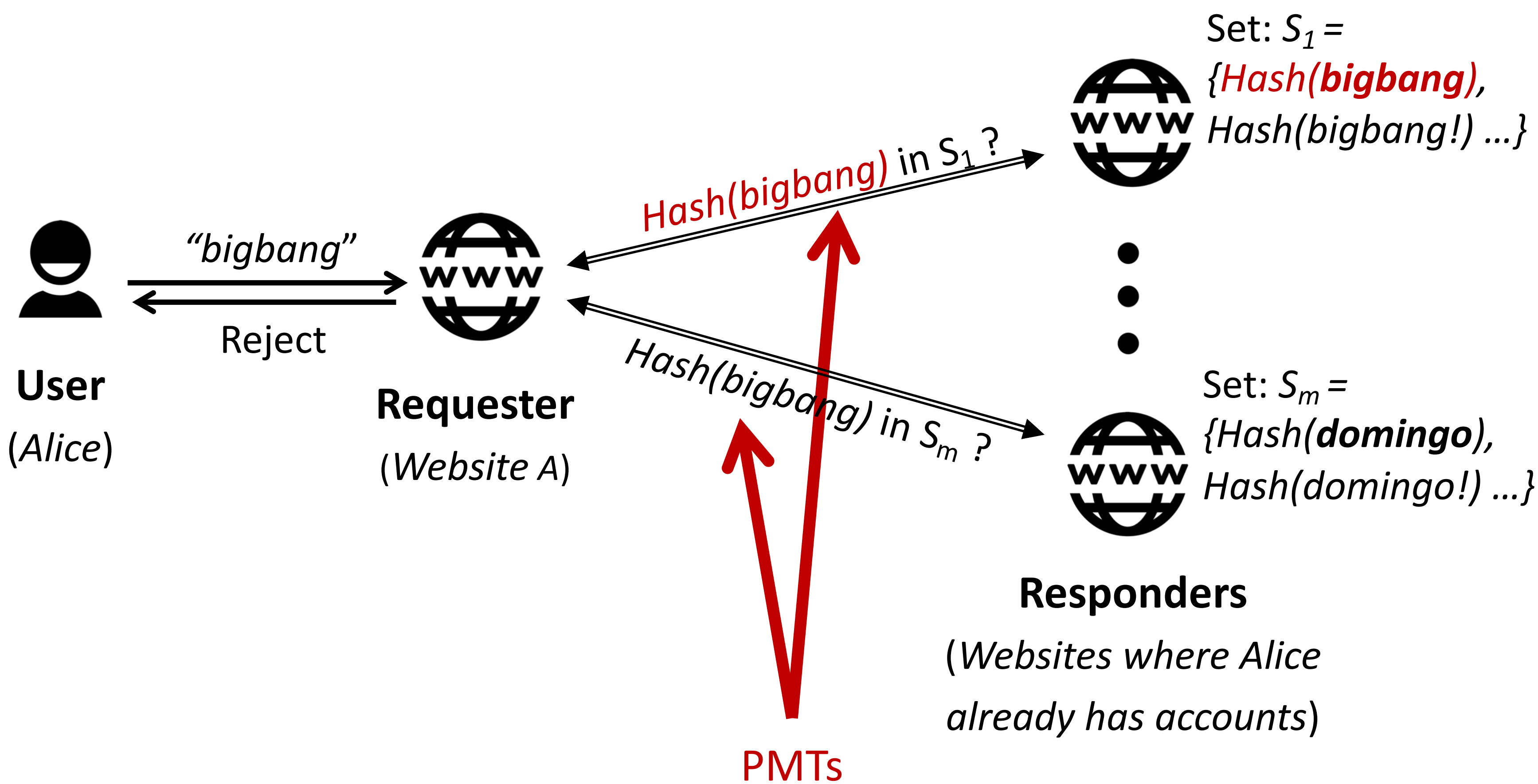
Responders

(*Websites where Alice already has accounts*)

PMT Application



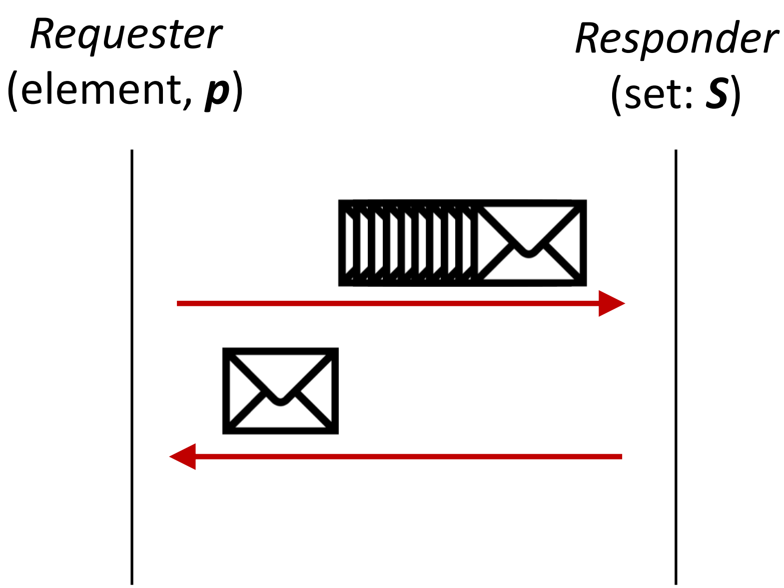
PMT Application



Our PMT Protocol

Our PMT Protocol

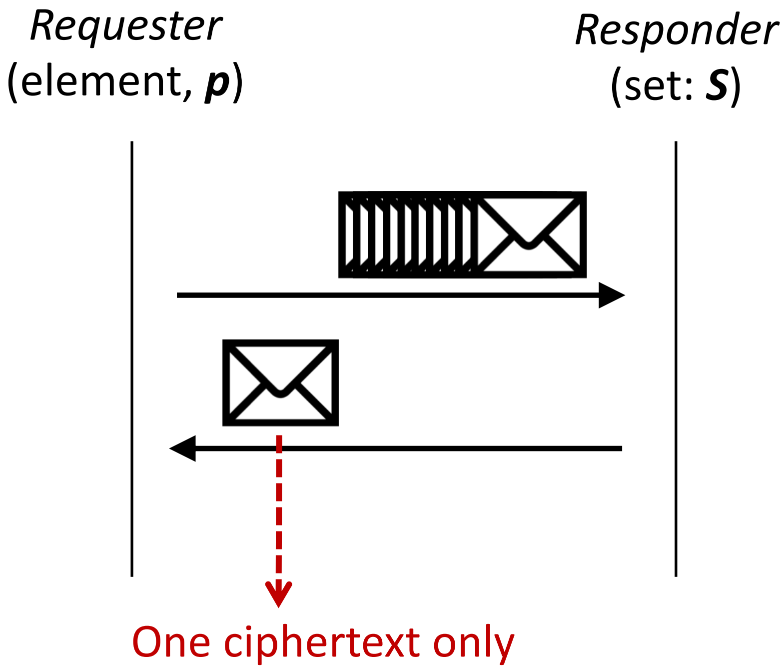
- **One round of interaction**



THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL

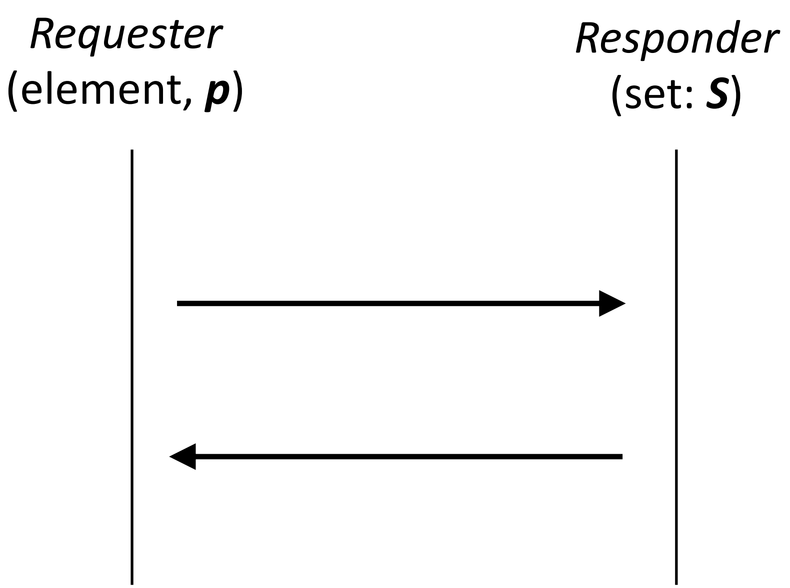
Our PMT Protocol

- One round of interaction
- **One ciphertext per response message**



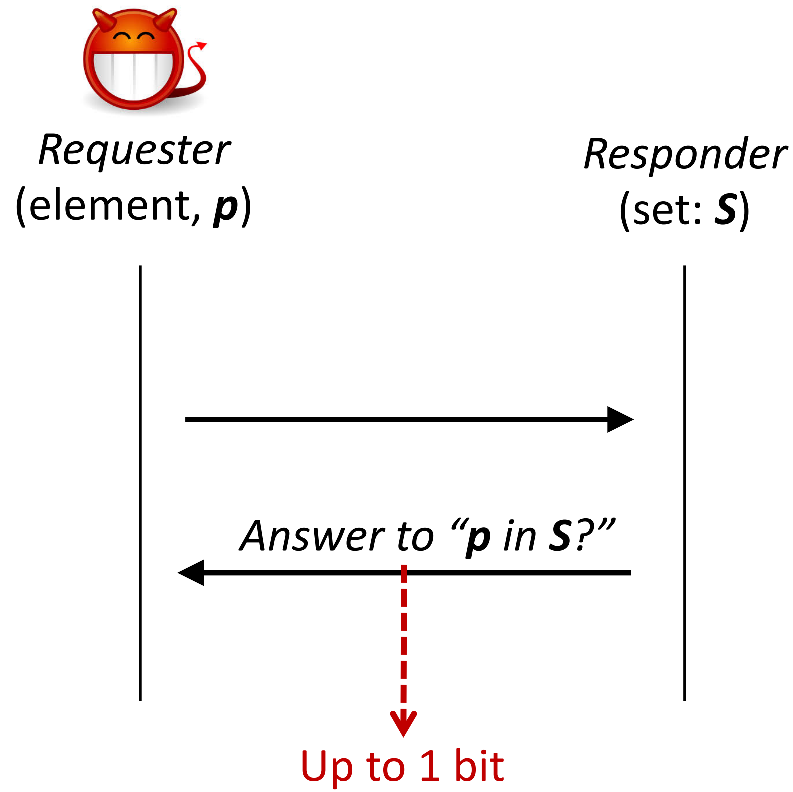
Our PMT Protocol

- One round of interaction
- One ciphertext per response message
- **Information leakage limited to one bit against malicious parties.**



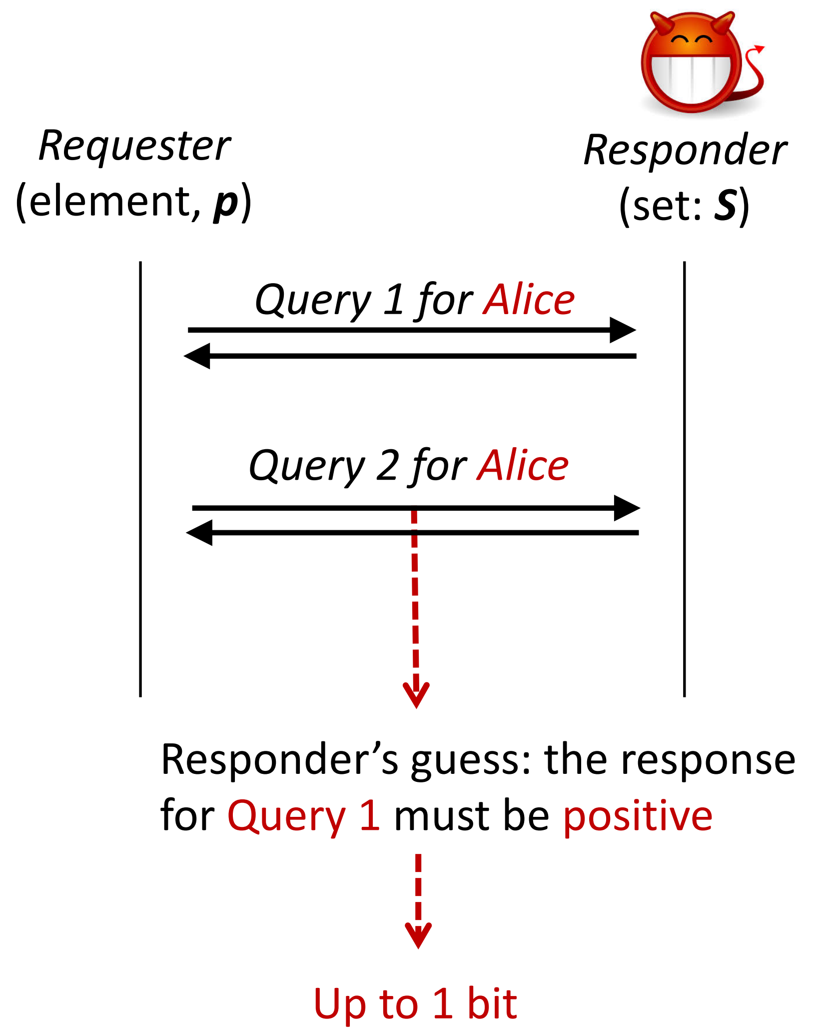
Our PMT Protocol

- One round of interaction
- One ciphertext per response message
- Information leakage limited to one bit against malicious parties.
    - **Requester obtains up to 1 bit**



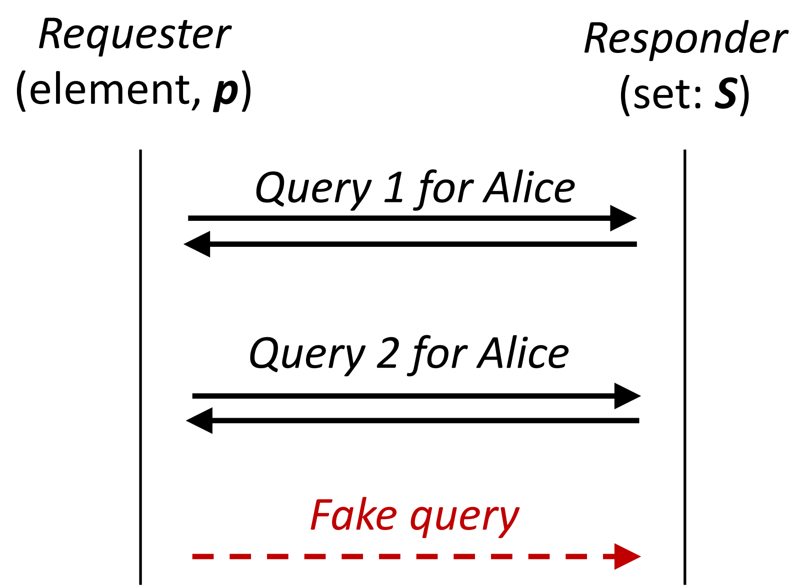
Our PMT Protocol

- One round of interaction
- One ciphertext per response message
- Information leakage limited to one bit against malicious parties.
  - Requester obtains up to 1 bit
  - **Responder obtains up to 1 bit**

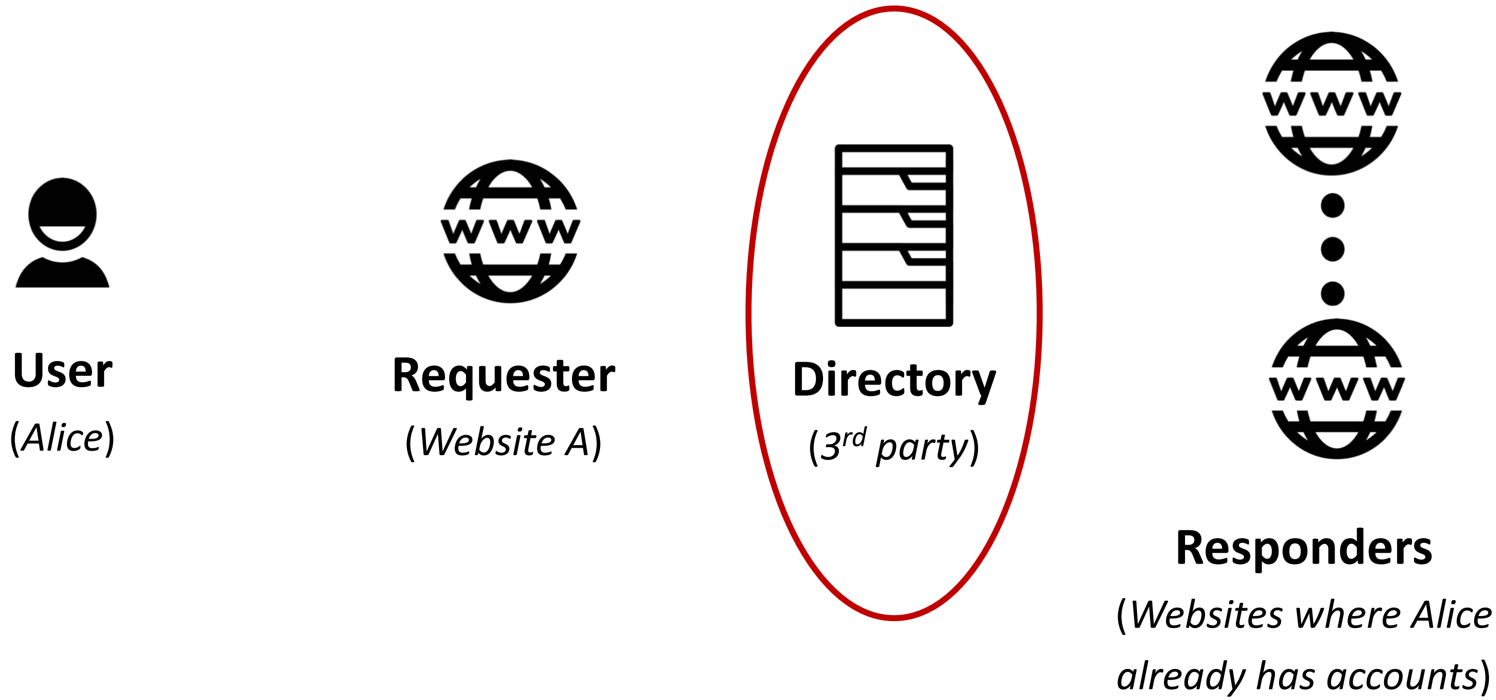


Our PMT Protocol

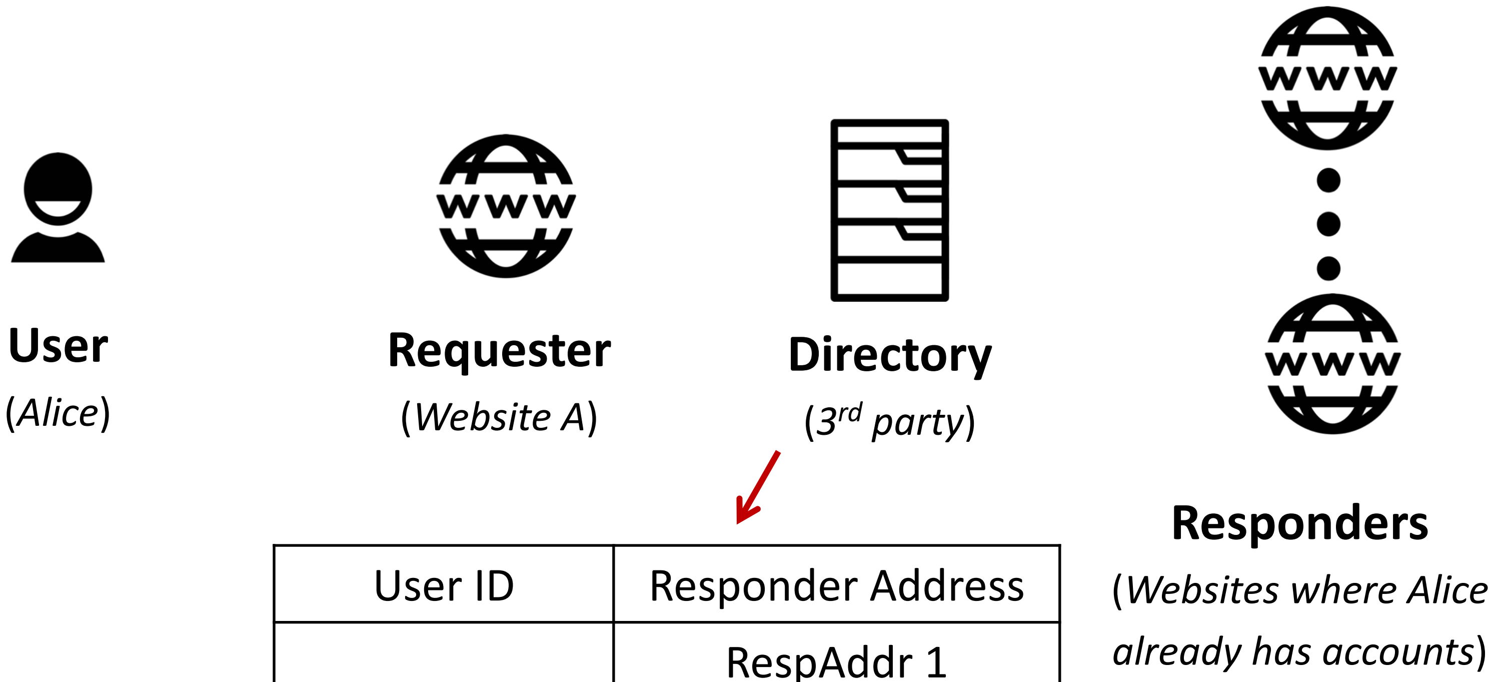
- One round of interaction
- One ciphertext per response message
- Information leakage limited to one bit against malicious parties.
  - Requester obtains up to 1 bit
  - Responder obtains up to 1 bit
    - **“probabilistic fake query”**



Directory

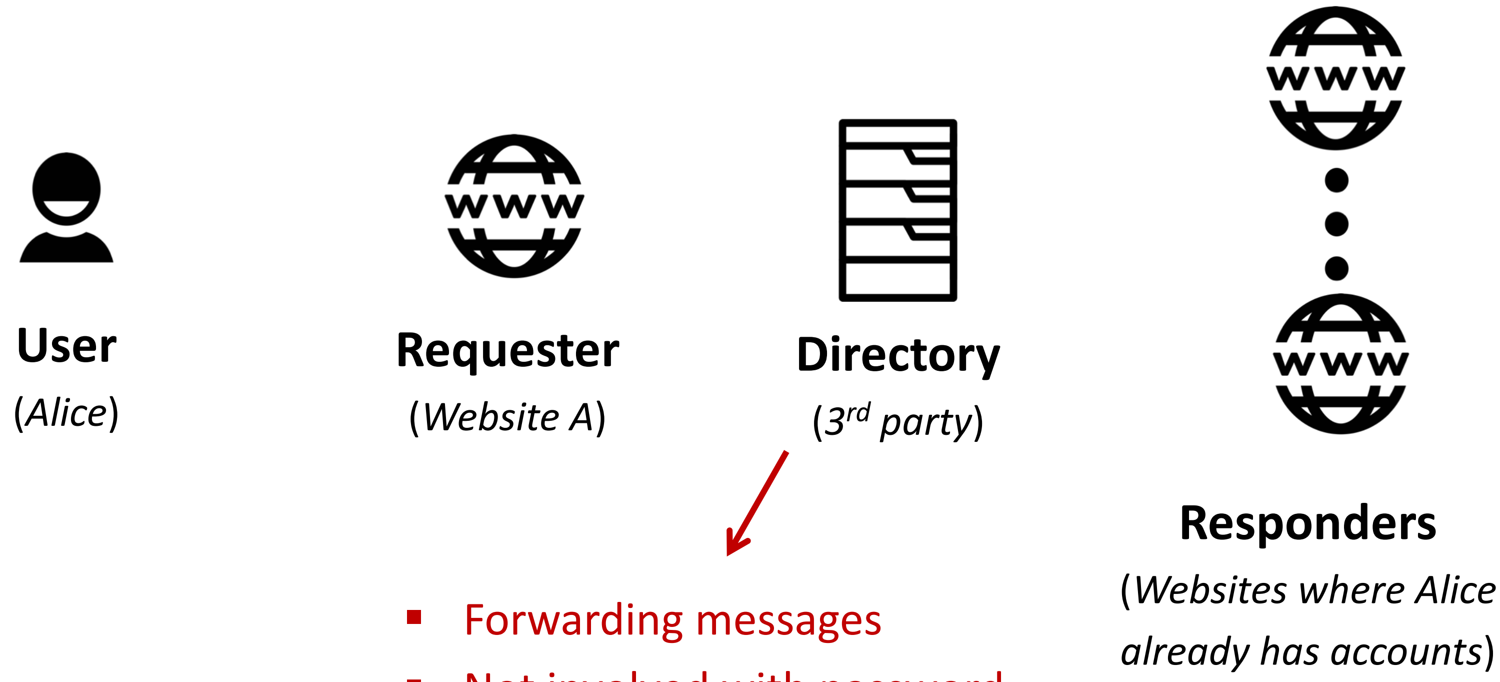

User
(*Alice*)
Requester
(*Website A*)
Directory
(*3rd party*)
Responders
(*Websites where Alice already has accounts*)

Directory



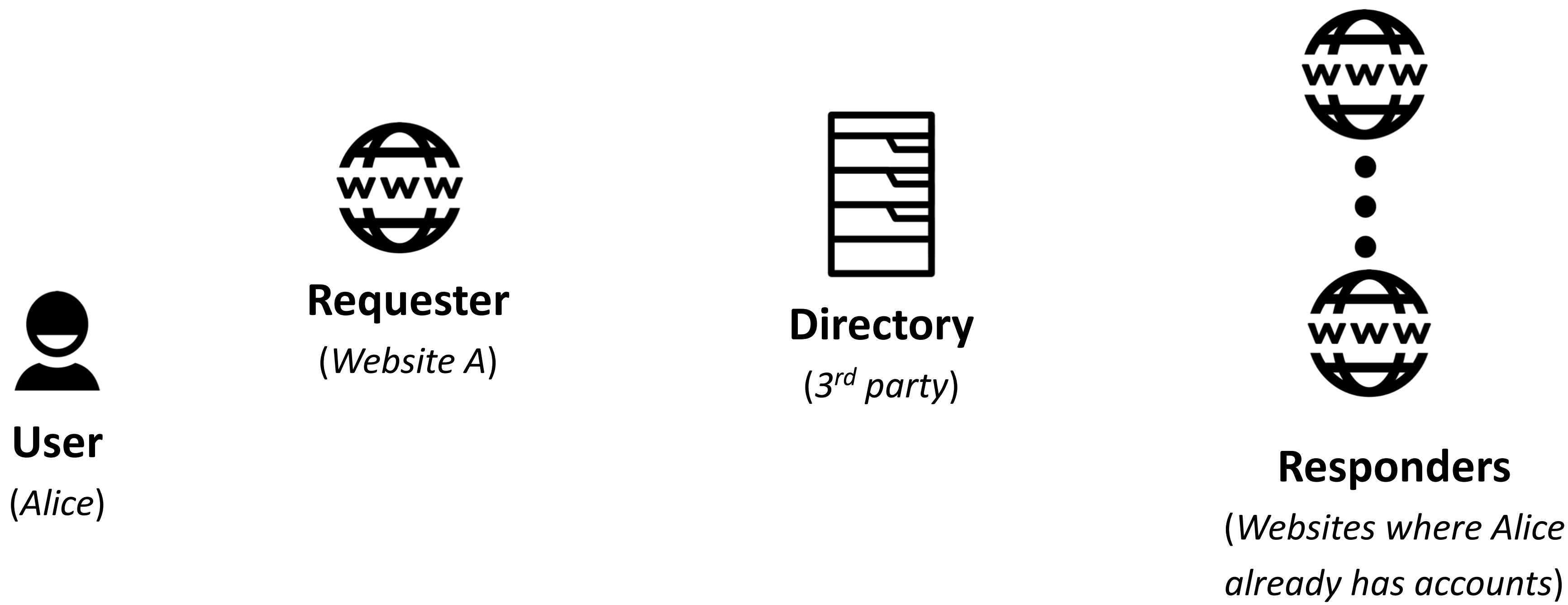
User ID	Responder Address
alice@xxx.com	RespAddr 1
	RespAddr 2
	RespAddr 3

Directory

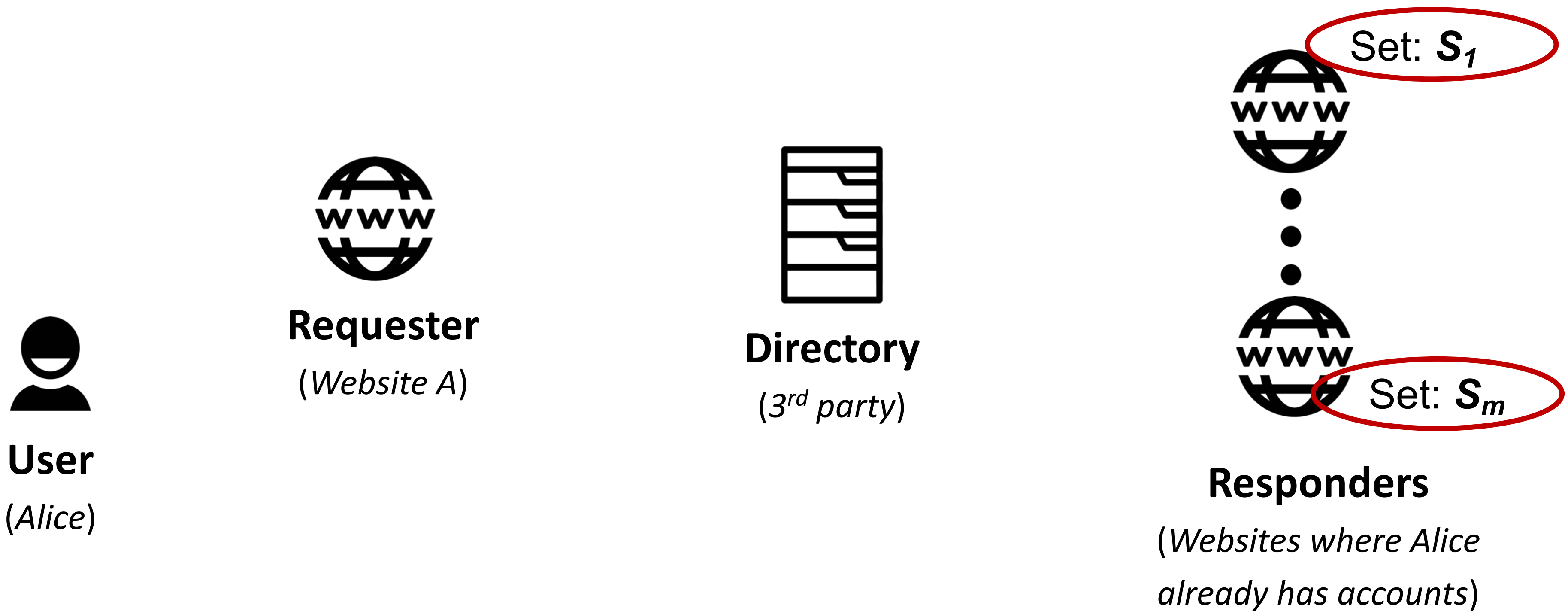


- Forwarding messages
- Not involved with password storage or any cryptographic operations for PMTs

Framework Design

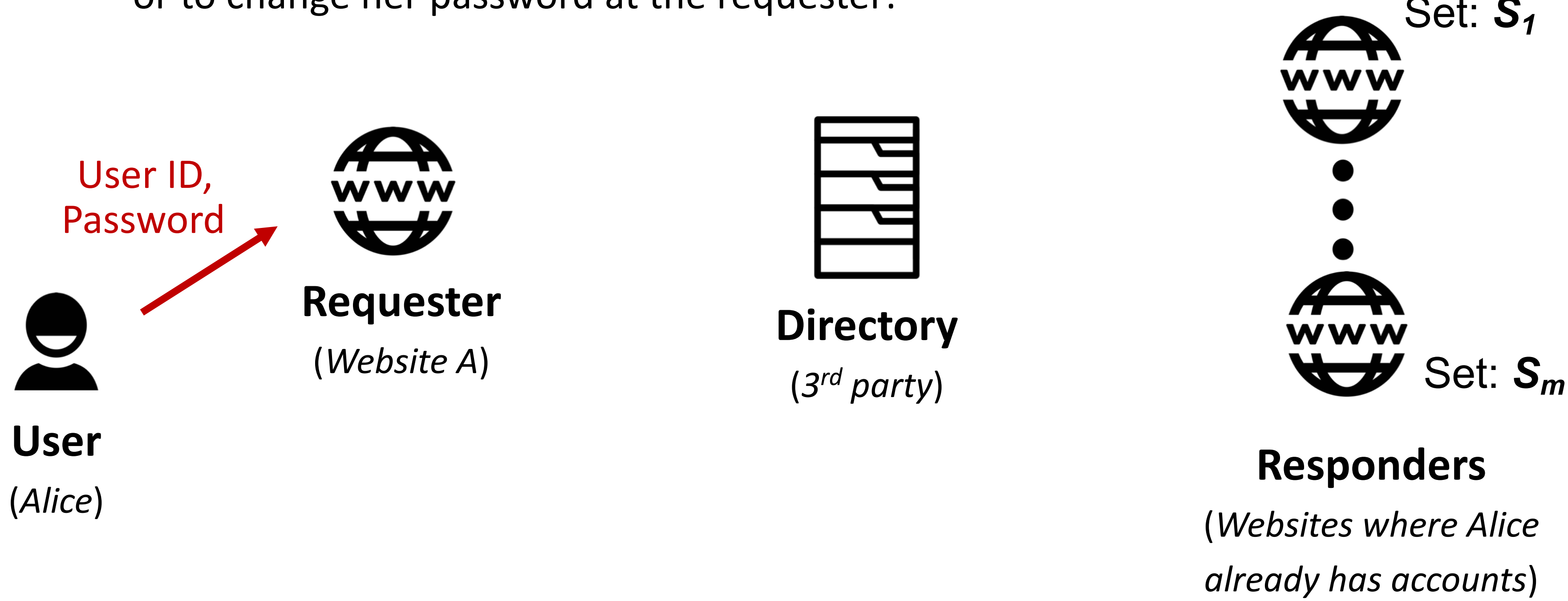


Framework Design



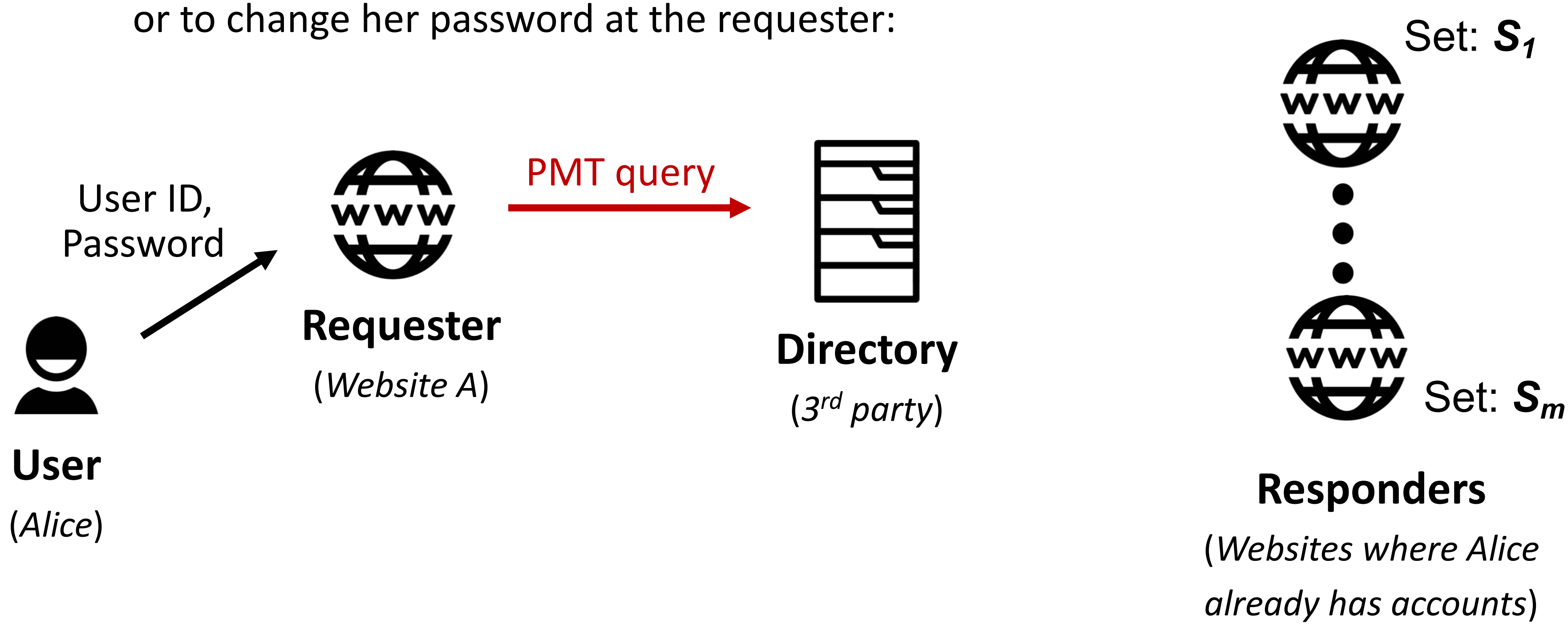
Framework Design

When Alice tries to register a new account
or to change her password at the requester:



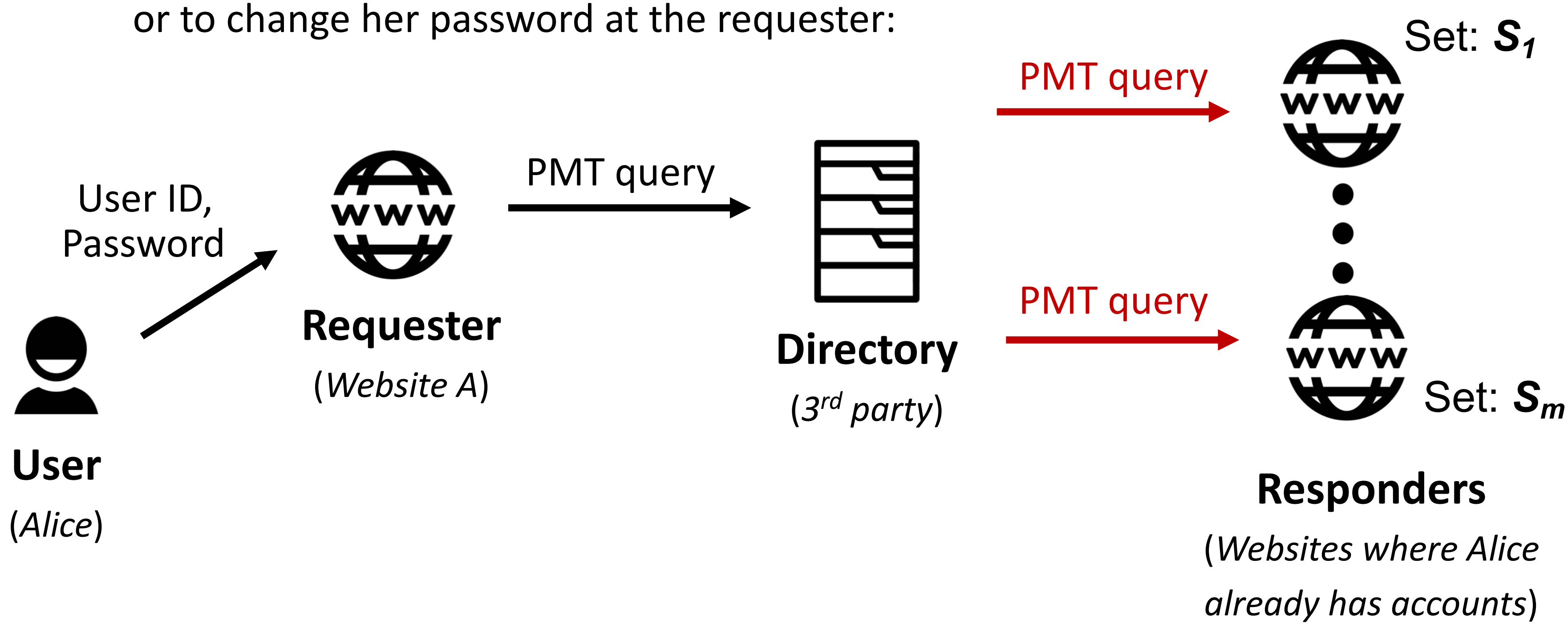
Framework Design

When Alice tries to register a new account
or to change her password at the requester:



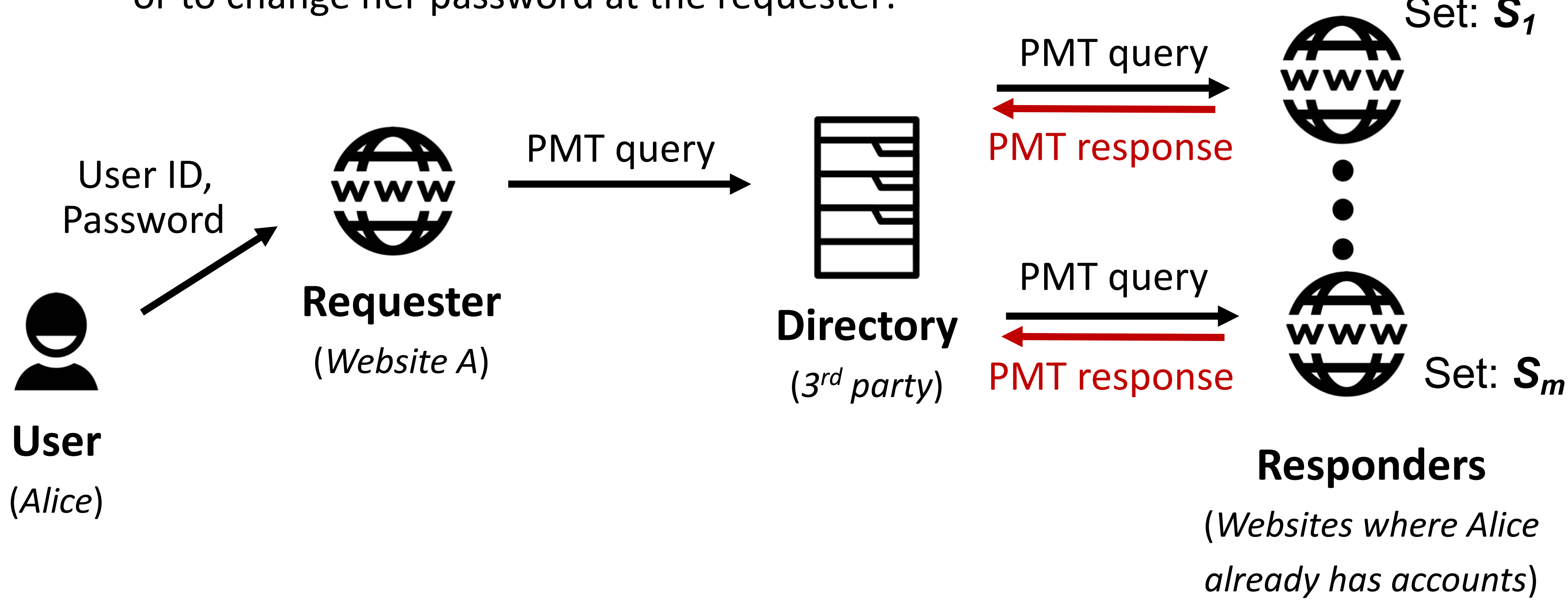
Framework Design

When Alice tries to register a new account
or to change her password at the requester:



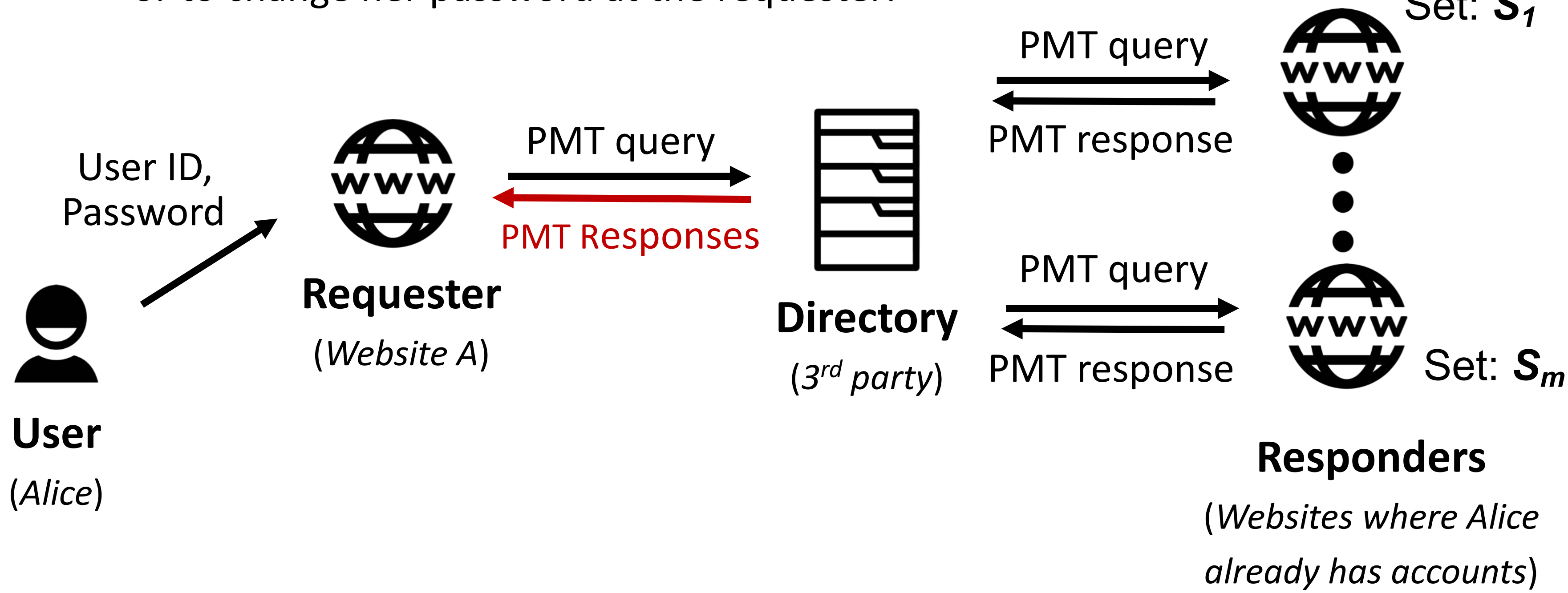
Framework Design

When Alice tries to register a new account or to change her password at the requester:



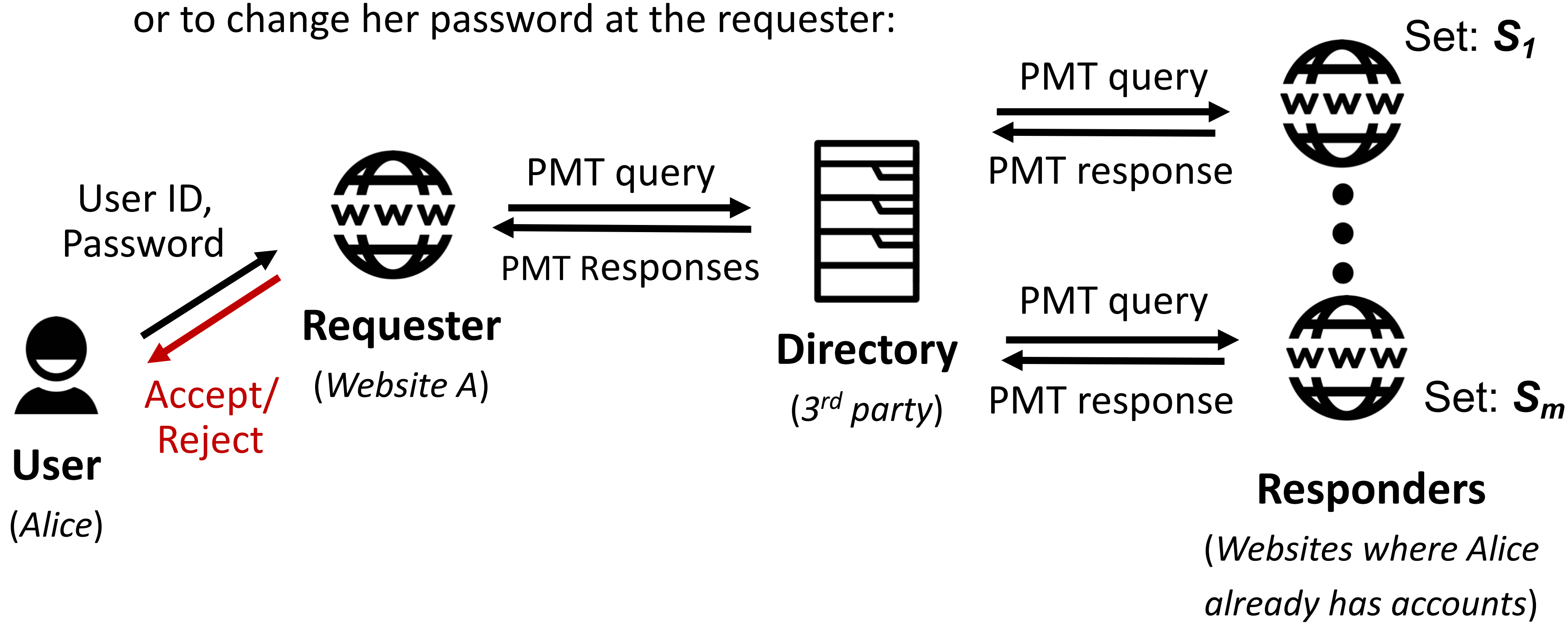
Framework Design

When Alice tries to register a new account
or to change her password at the requester:

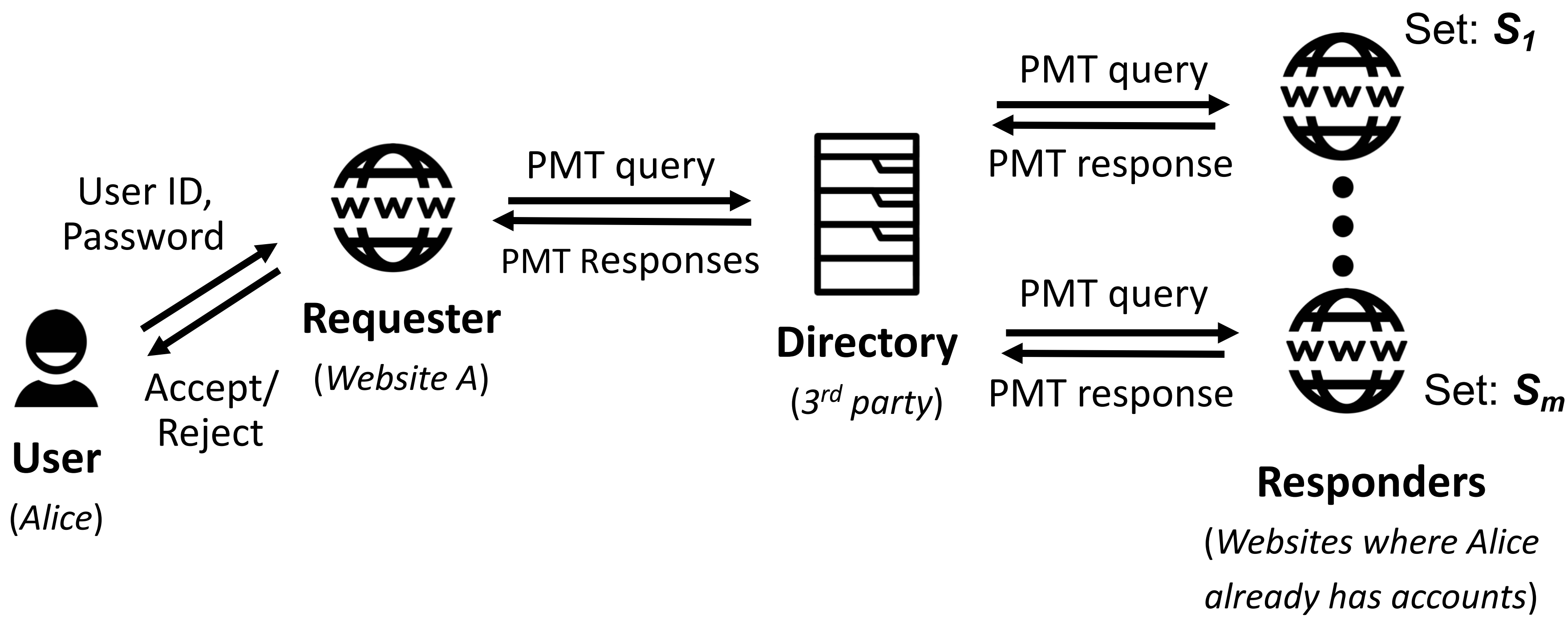


Framework Design

When Alice tries to register a new account
or to change her password at the requester:

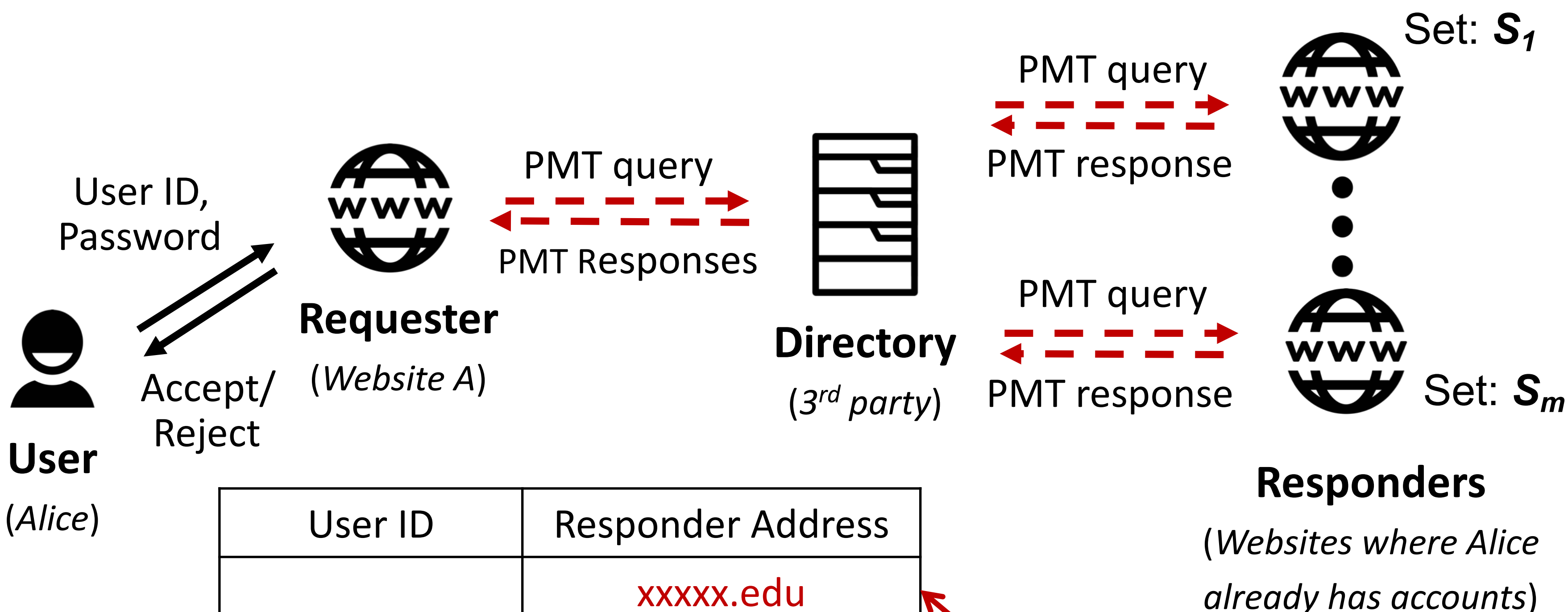


Framework Design



Account Location Privacy

Framework Design

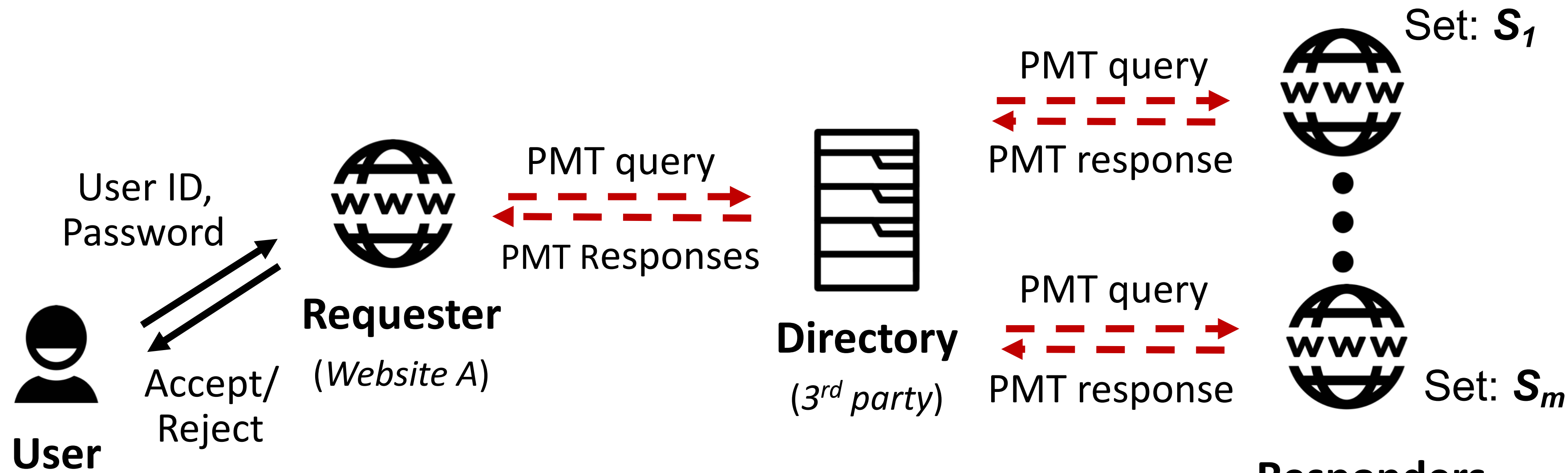


User ID	Responder Address
alice@xxx.com	xxxxx.edu
	pseudo address 1
	pseudo address 2

When Directory is trusted
for account location privacy

THE UNIVERSITY *of* NORTH CAROLINA *at* CHAPEL HILL

Framework Design

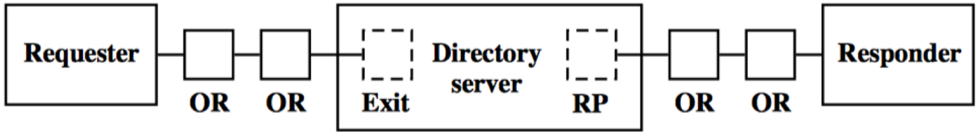


User ID	Responder Address
alice@xxx.com	xxxxx.edu
	pseudo address 1
	pseudo address 2

When Directory is untrusted for account location privacy

Anonymous Communication

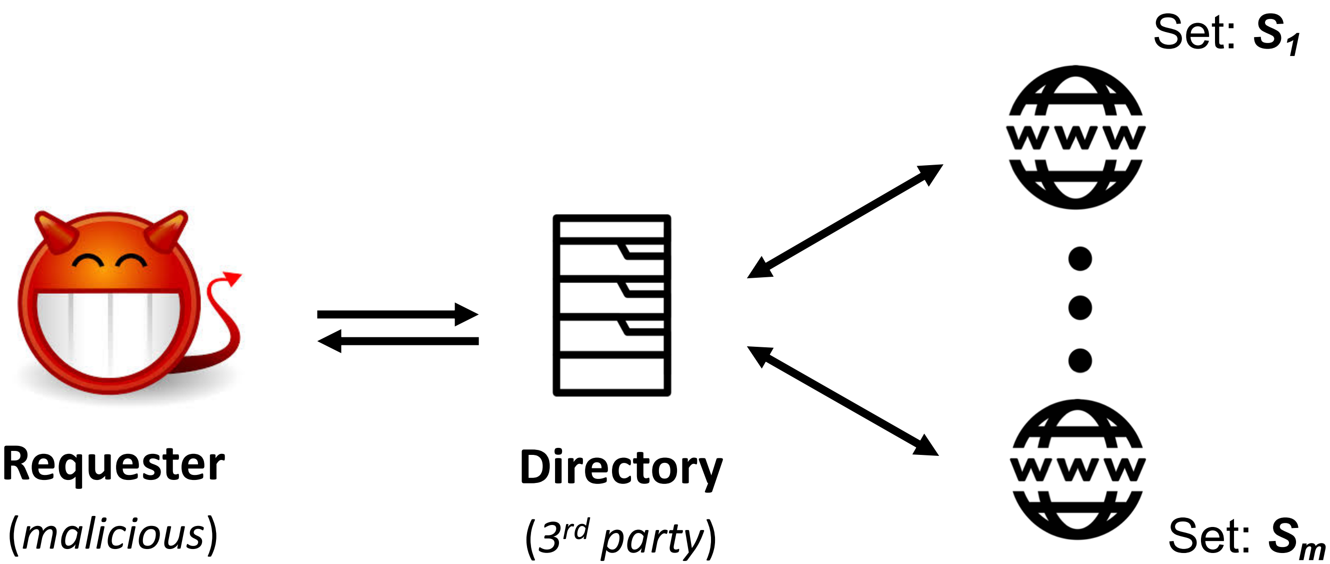
Tor (The Onion Router) network enables anonymous communication, which can hide the identities of the **requester** and **responders** when the directory is **untrusted** for **account location privacy**.



A customized Tor network for our prototype system, across 8 different datacenters in Europe and North America.

Security

Against Malicious Requester

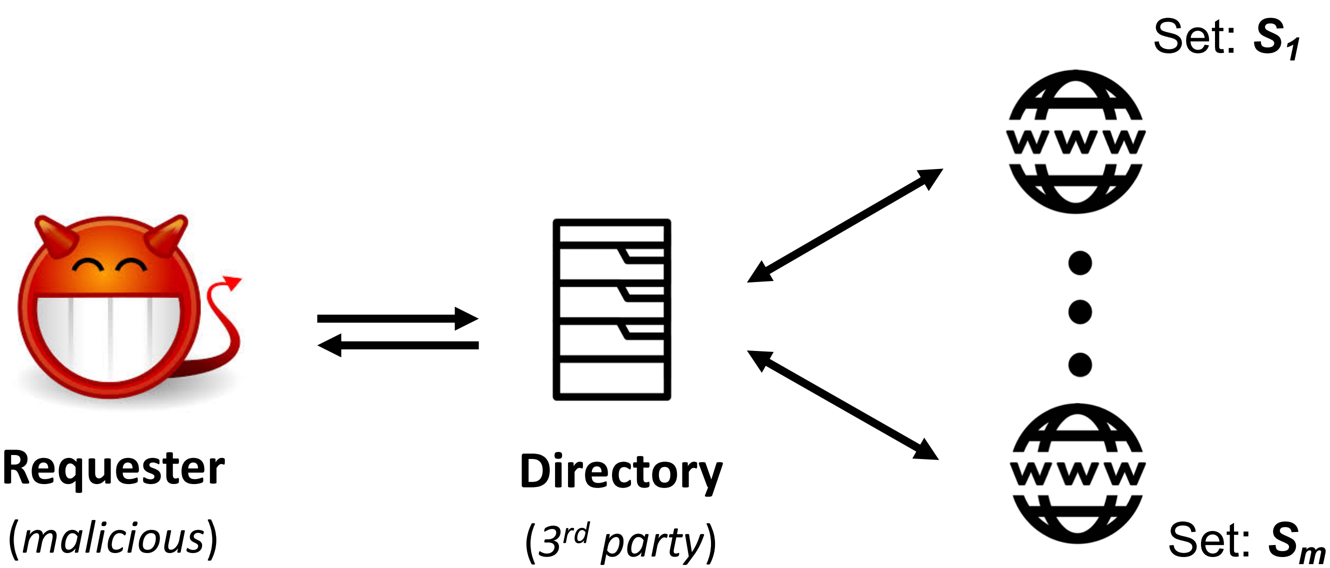


Requester
(*malicious*)

Directory
(*3rd party*)

Responders
(*Websites where the user already has accounts*)

Against Malicious Requester

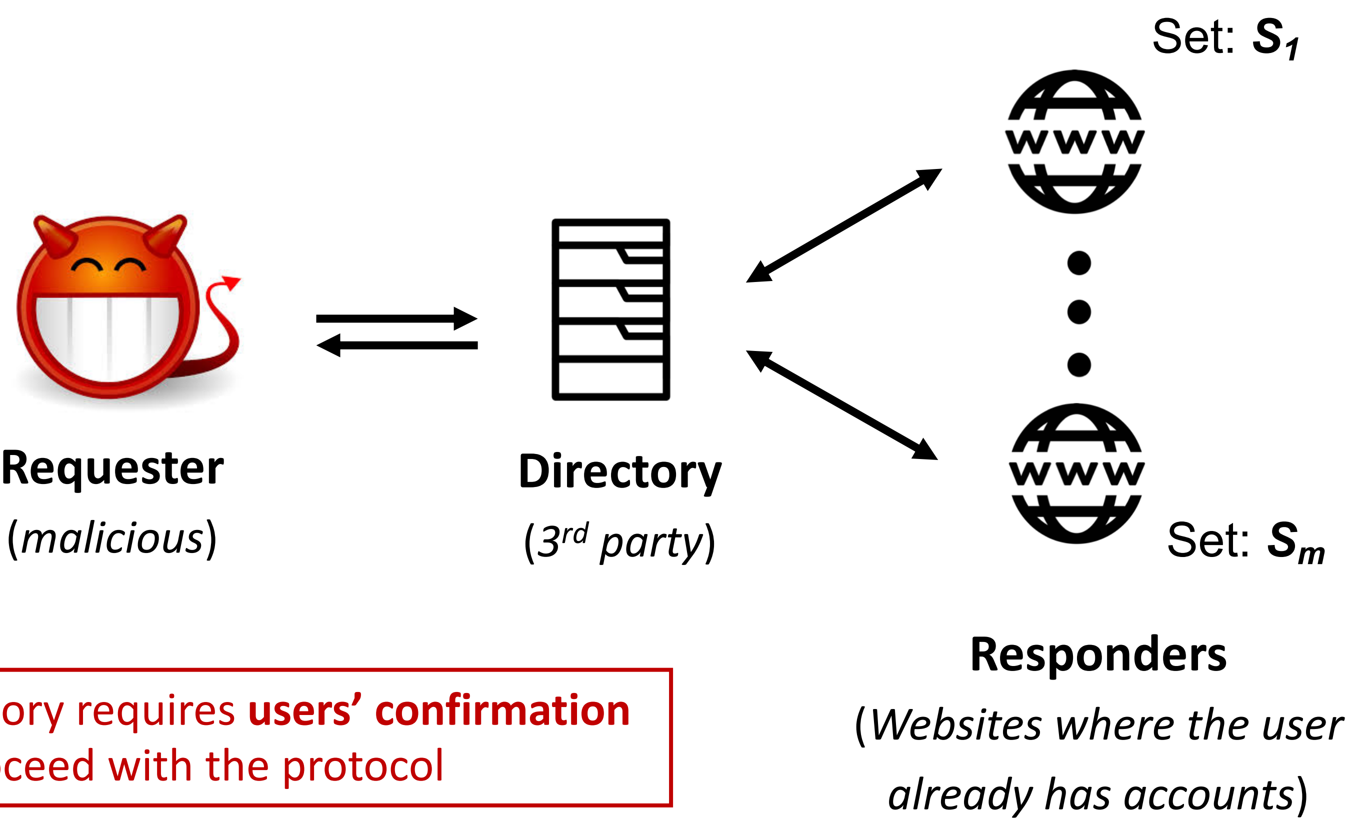


Responders

(*Websites where the user already has accounts*)

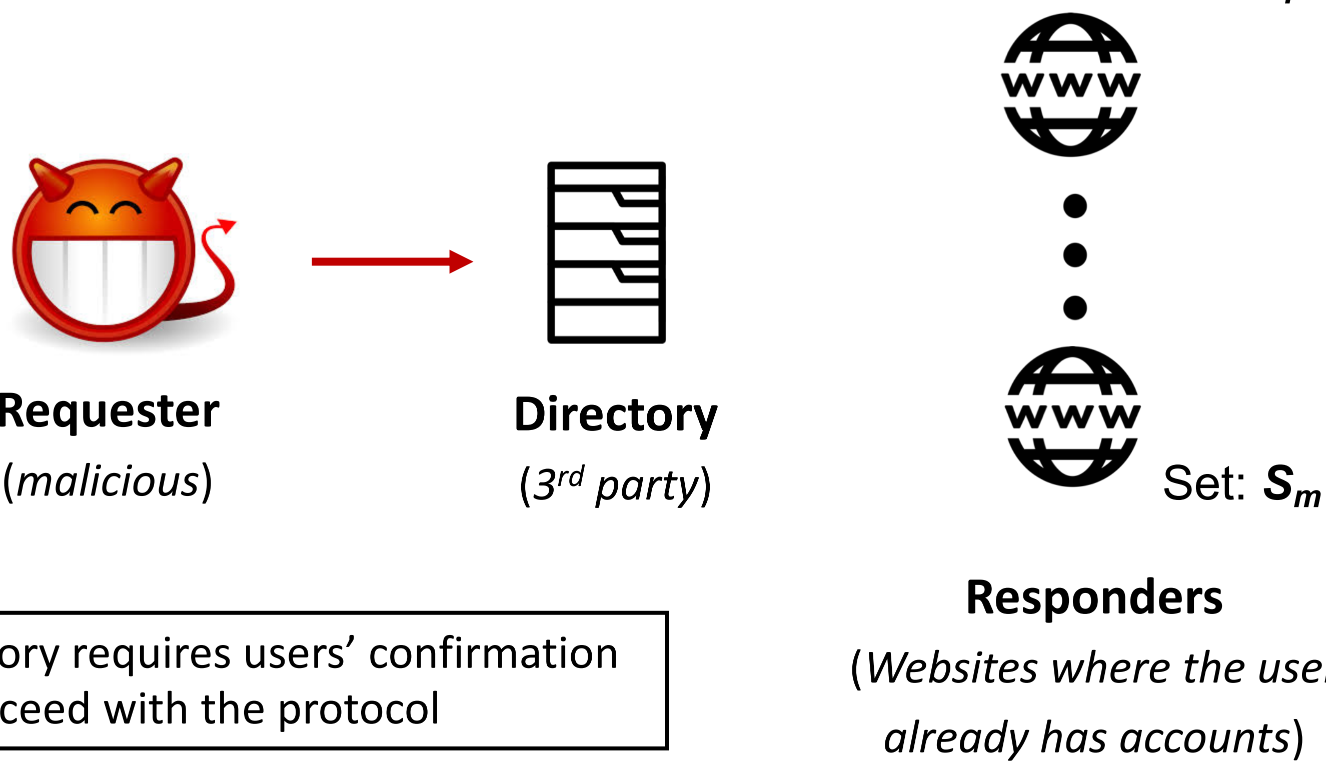
Account location privacy makes it more difficult to determine the identities of responders

Against Malicious Requester



Directory requires **users' confirmation** to proceed with the protocol

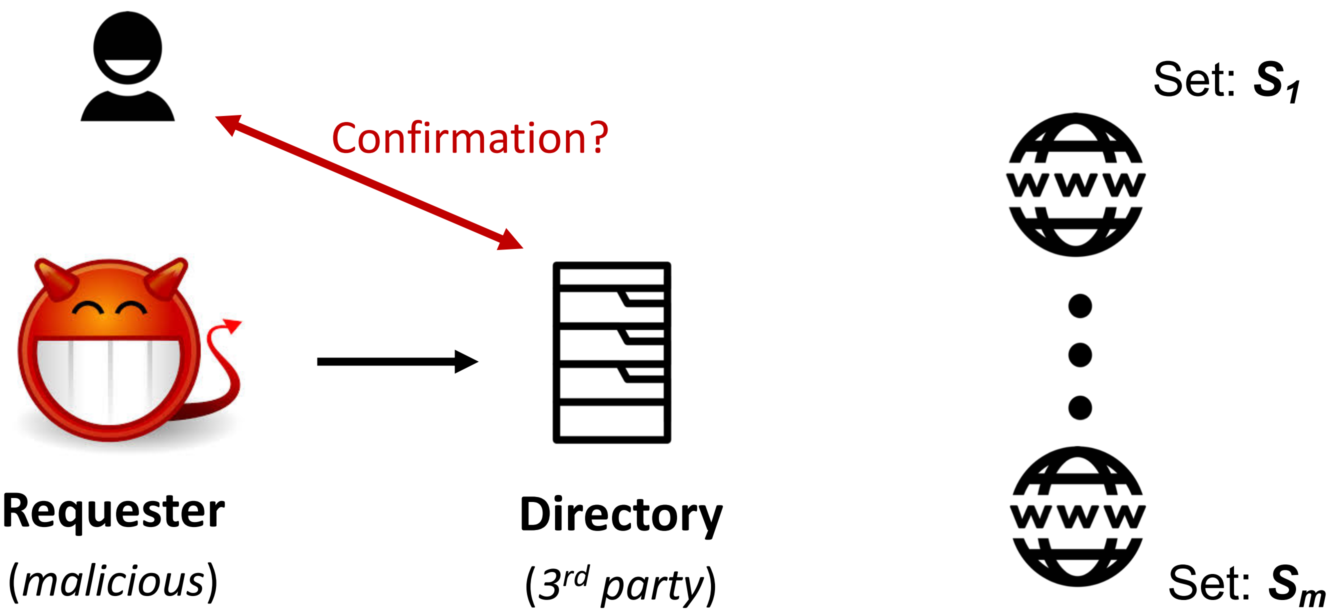
User Confirmation :: Example



Directory requires users' confirmation to proceed with the protocol

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

User Confirmation :: Example

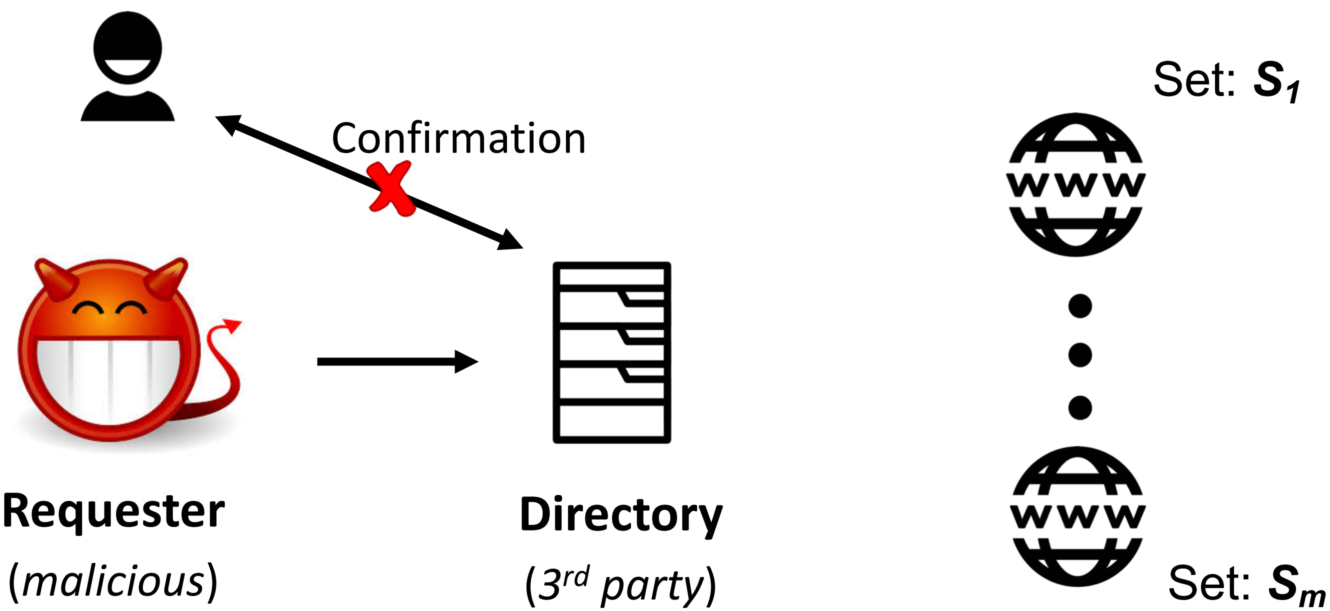


Directory requires users' confirmation to proceed with the protocol

Responders

(*Websites where the user already has accounts*)

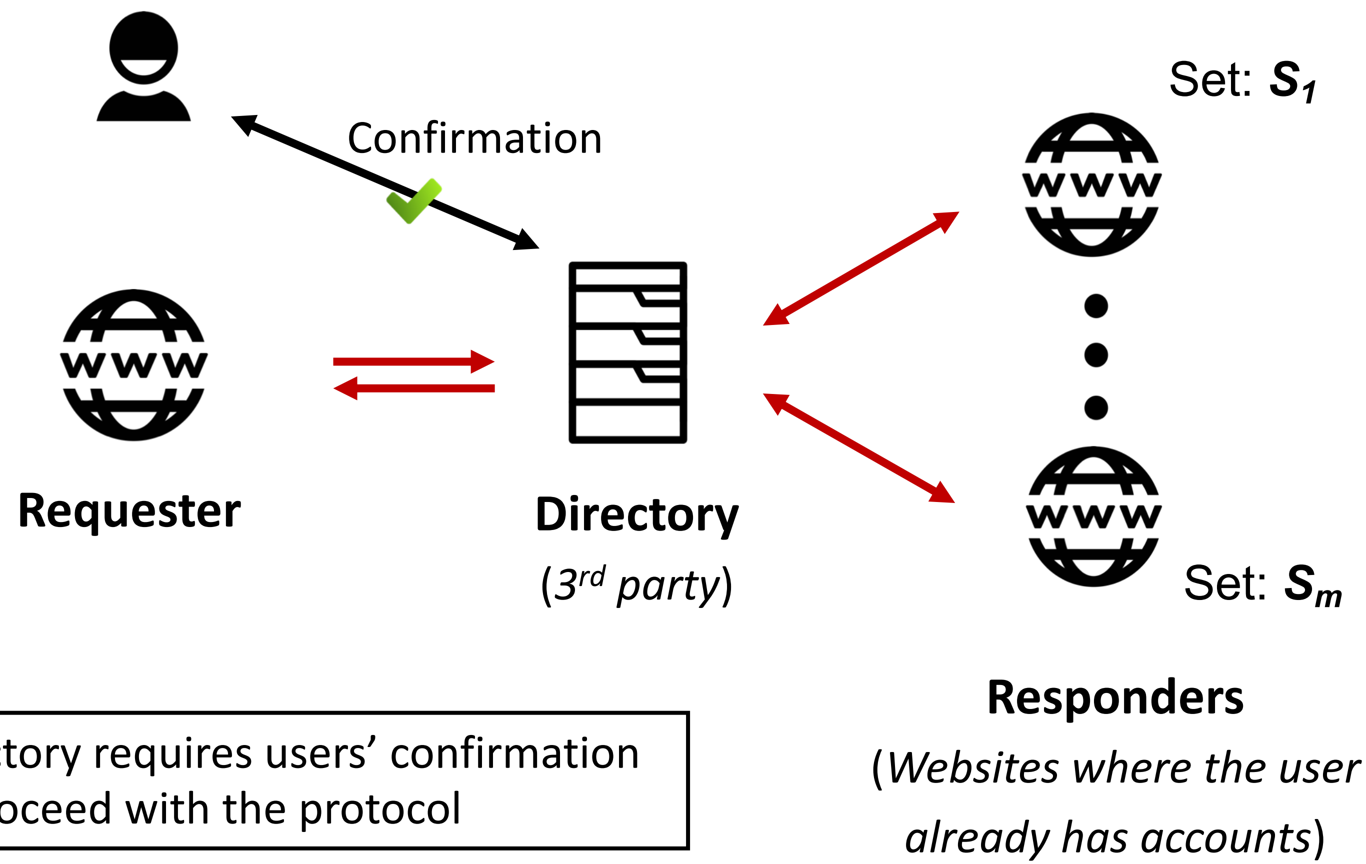
User Confirmation :: Example



Directory requires users' confirmation to proceed with the protocol

Responders
(*Websites where the user already has accounts*)

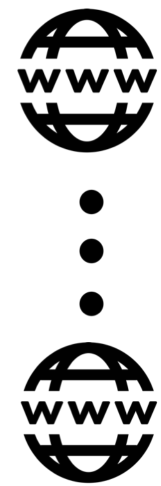
User Confirmation :: Example



Directory requires users' confirmation to proceed with the protocol

Probabilistic Model Checking

Adversary



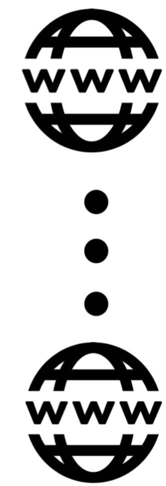
Responders

(*Websites where Alice already has accounts*)

Probabilistic Model Checking

Adversary

(Markov Decision Process)



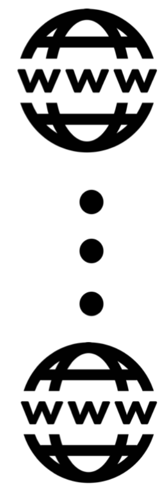
Responders

(*Websites where Alice already has accounts*)

Probabilistic Model Checking

Prior knowledge about
Alice’s passwords

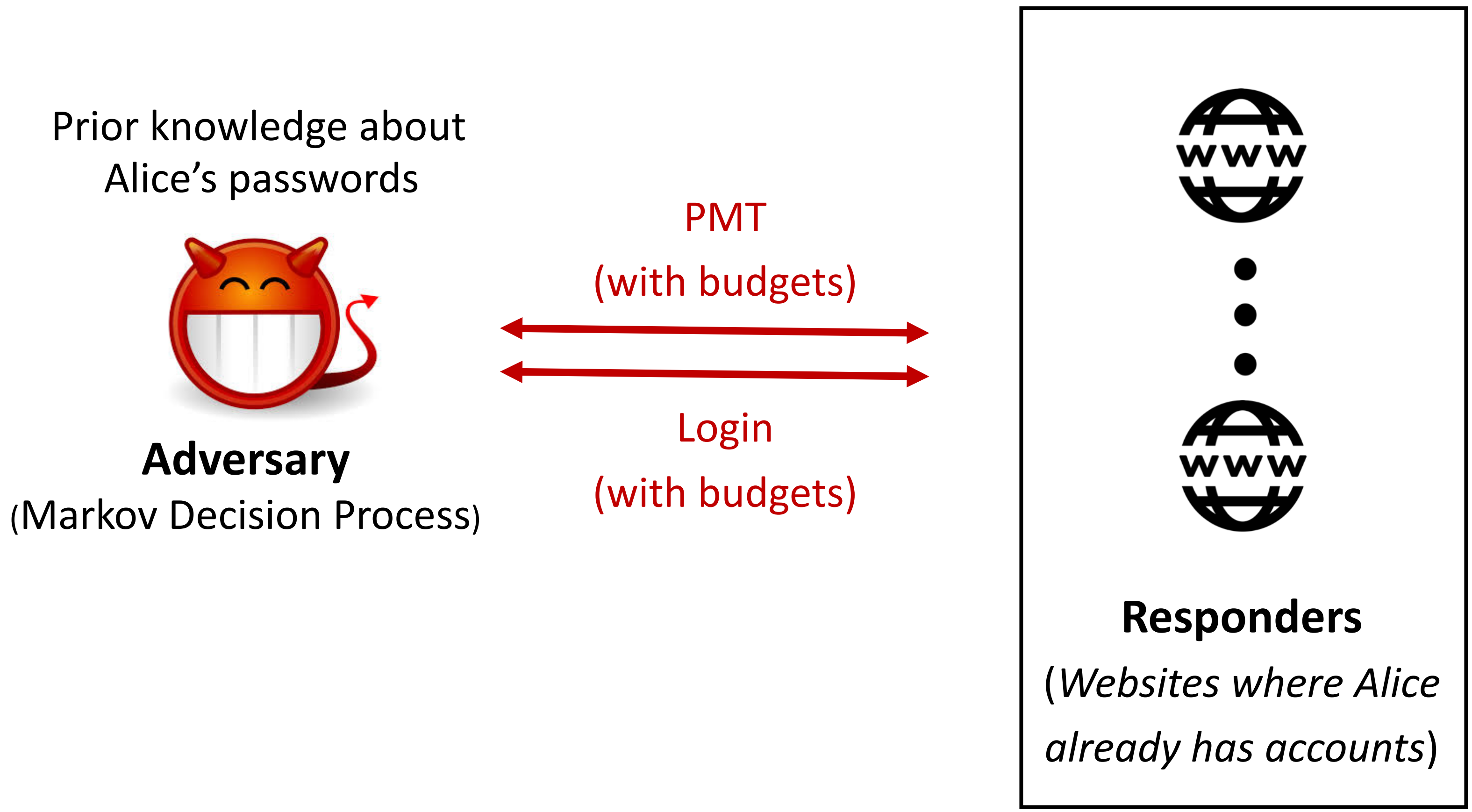
Adversary
(Markov Decision Process)



Responders
(*Websites where Alice already has accounts*)

THE UNIVERSITY *of* NORTH CAROLINA *at* CHAPEL HILL

Probabilistic Model Checking



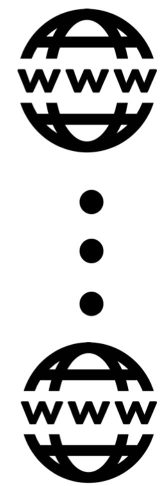
Probabilistic Model Checking

Prior knowledge about
Alice's passwords

Adversary
(Markov Decision Process)

PMT
(with budgets)

Login
(with budgets)



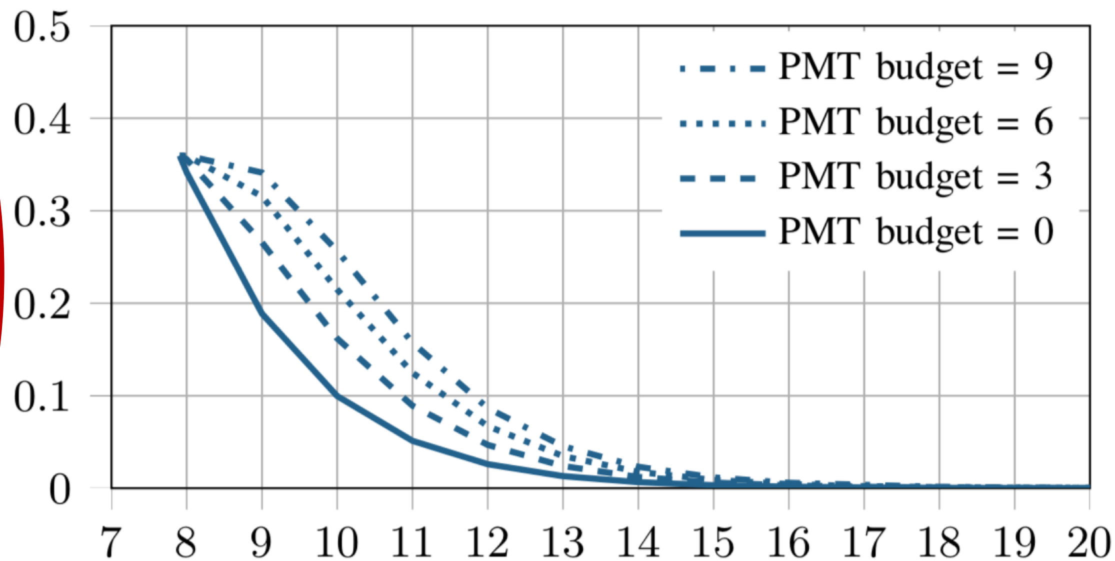
Responders
(*Websites where Alice already has accounts*)

<u>Adversary's goal: wins if she is able to compromise **at least one** account on those responders.</u>

THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL

Probabilistic Model Checking

Max. Prob. of the adversary's success (at least one account takeover)



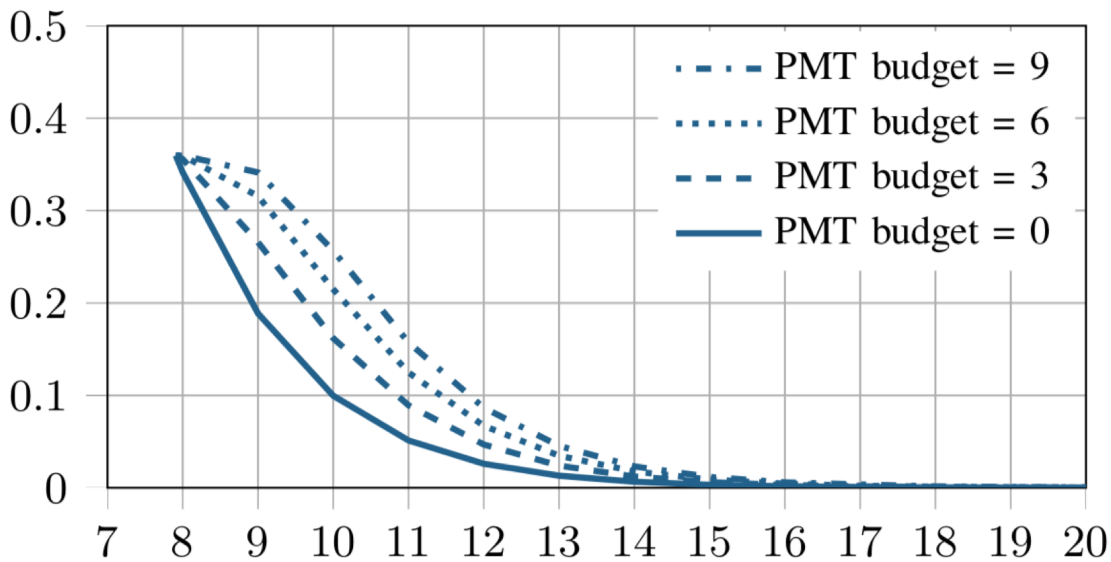
Dictionary size (bits)

\# of websites: 12

Login budgets: 9

Probabilistic Model Checking

Max. Prob. of the adversary's success (at least one account takeover)



Dictionary size (bits)

# of websites: 12

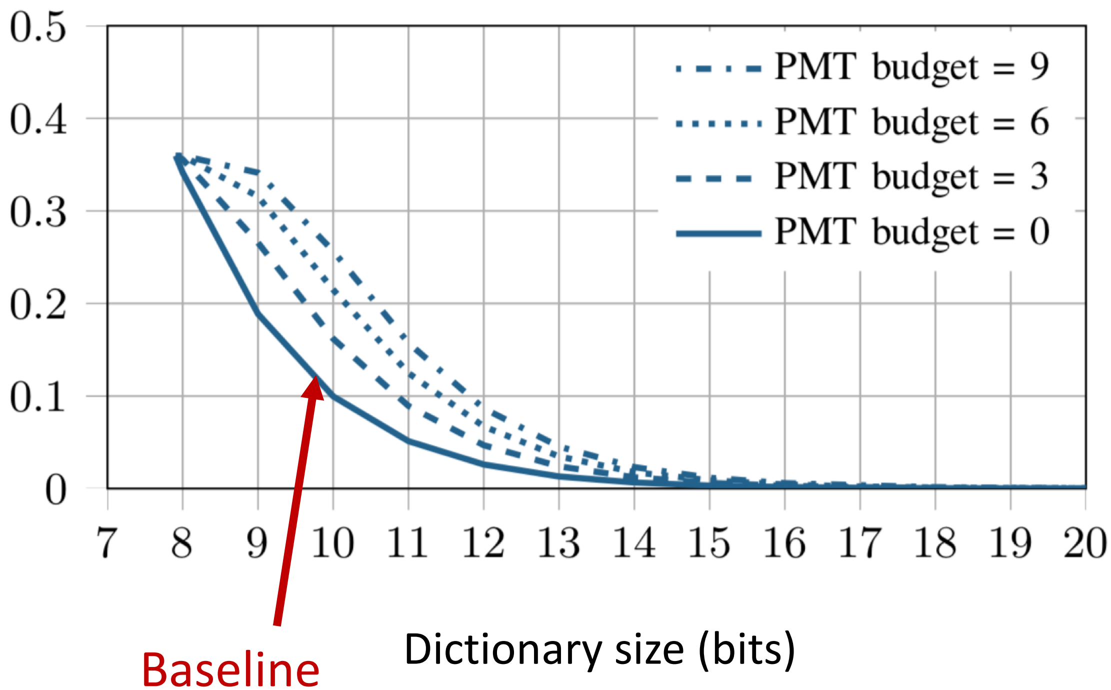
Login budgets: 9

Difficulty of guessing a user's passwords, given different levels of prior knowledge

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Probabilistic Model Checking

Max. Prob. of the adversary's success (at least one account takeover)



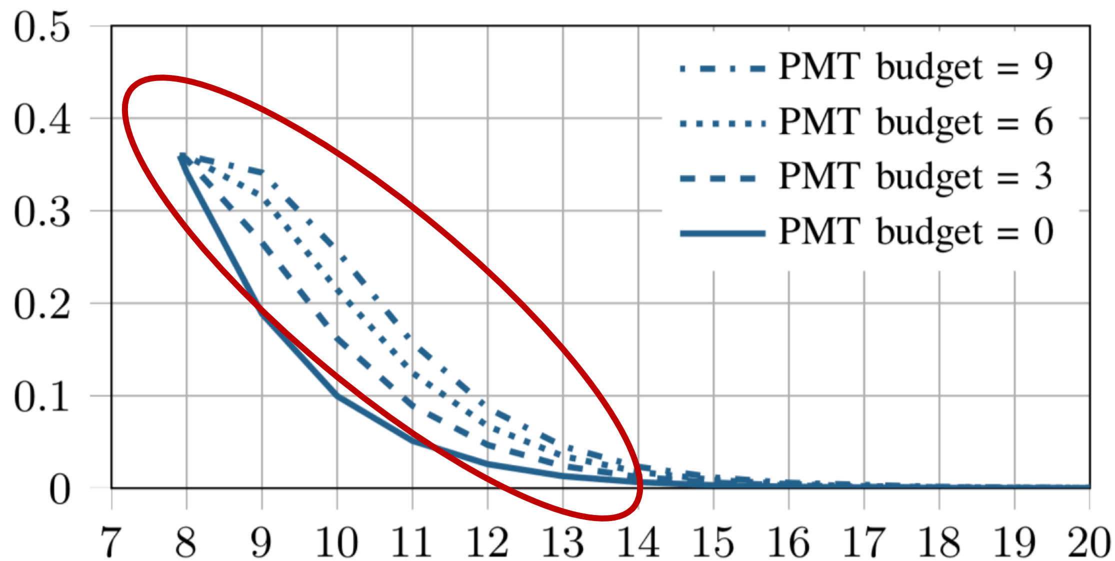
Dictionary size (bits)

# of websites: 12

Login budgets: 9

Probabilistic Model Checking

Max. Prob. of the adversary's success (at least one account takeover)



Dictionary size (bits)

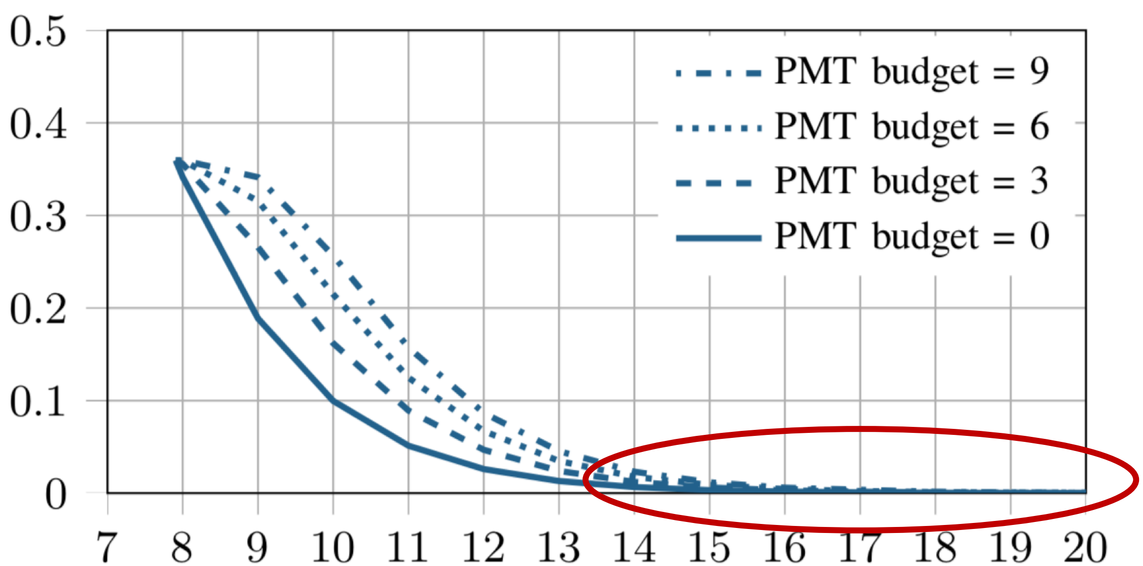
# of websites: 12

Login budgets: 9

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Probabilistic Model Checking

Max. Prob. of the adversary's success (at least one account takeover)



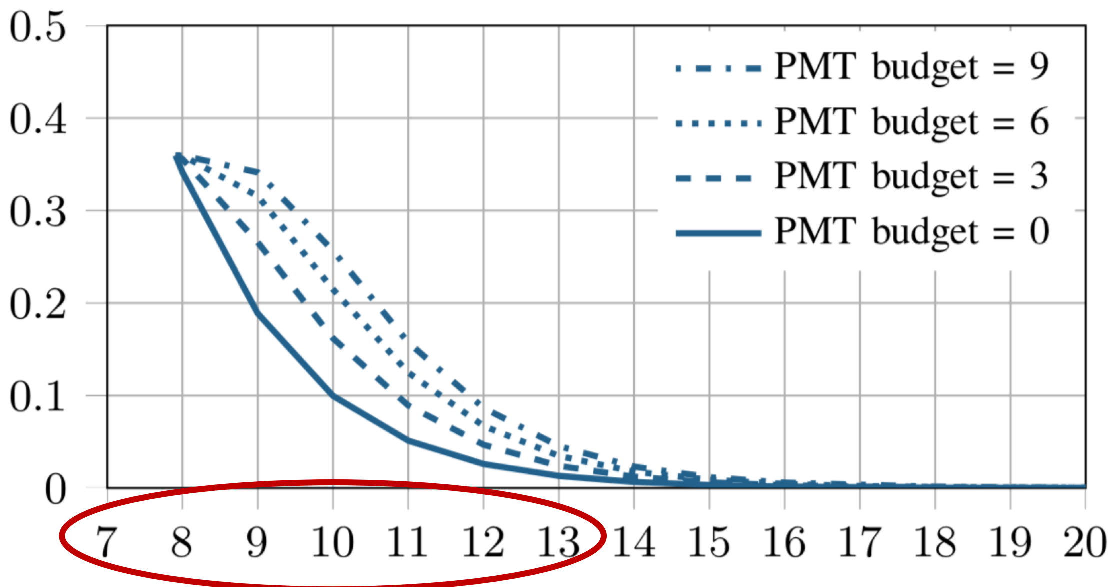
Dictionary size (bits)

# of websites: 12

Login budgets: 9

Probabilistic Model Checking

Max. Prob. of the adversary's success (at least one account takeover)



Dictionary size (bits)

Decent amount of prior knowledge

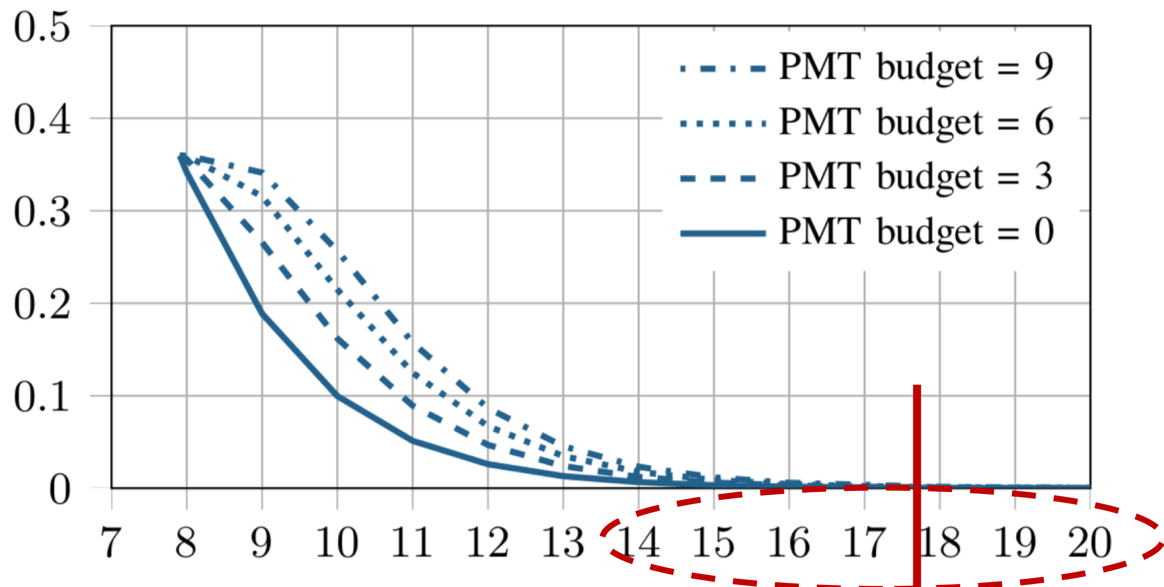
\# of websites: 12

Login budgets: 9

THE UNIVERSITY *of* NORTH CAROLINA *at* CHAPEL HILL

Probabilistic Model Checking

Max. Prob. of the adversary's success (at least one account takeover)



Dictionary size (bits)

# of websites: 12

Login budgets: 9

Not too guessable

a password with only **3** randomly generated characters (a-z, A-Z, 0-9).

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Scalability

Scalability Evaluation

Max qualifying responses per sec.

number of responders / set size at responders

	1	6	11	16	21	26
1	4304	1013	492	325	237	174
10	2415	549	277	188	155	122
20	1478	336	182	129	98	78
30	1076	243	124	86	63	53
40	788	187	94	67	49	40
50	683	159	76	52	39	33
60	611	132	63	43	32	25

Trusted directory
(Qualifying response: <= 5s)

number of responders / set size at responders

	1	6	11	16	21	26
1	95	61	42	33	27	22
10	87	59	40	31	25	20
20	78	54	37	28	23	19
30	71	51	35	27	20	16
40	62	44	32	24	18	14
50	53	39	26	20	15	11
60	42	31	20	16	10	10

Untrusted directory
(Qualifying response: <= 8s)

"Roundtrip" time measured
at the requester

Scalability Evaluation

<u>Max qualifying responses per sec.</u>

number of responders \ set size at responders	1	6	11	16	21	26
1	4304	1013	492	325	237	174
10	2415	549	277	188	155	122
20	1478	336	182	129	98	78
30	1076	243	124	86	63	53
40	788	187	94	67	49	40
50	683	159	76	52	39	33
60	611	132	63	43	32	25

Trusted directory
(Qualifying response: <= 5s)

number of responders \ set size at responders	1	6	11	16	21	26
1	95	61	42	33	27	22
10	87	59	40	31	25	20
20	78	54	37	28	23	19
30	71	51	35	27	20	16
40	62	44	32	24	18	14
50	53	39	26	20	15	11
60	42	31	20	16	10	10

Untrusted directory
(Qualifying response: <= 8s)

Scalability Evaluation

Max qualifying responses per sec.

number of responders \ set size at responders	1	6	11	16	21	26
1	4304	1013	492	325	237	174
10	2415	549	277	188	155	122
20	1478	336	182	129	98	78
30	1076	243	124	86	63	53
40	788	187	94	67	49	40
50	683	159	76	52	39	33
60	611	132	63	43	32	25

Trusted directory
(Qualifying response: <= 5s)

number of responders \ set size at responders	1	6	11	16	21	26
1	95	61	42	33	27	22
10	87	59	40	31	25	20
20	78	54	37	28	23	19
30	71	51	35	27	20	16
40	62	44	32	24	18	14
50	53	39	26	20	15	11
60	42	31	20	16	10	10

Untrusted directory
(Qualifying response: <= 8s)

Scalability Evaluation

Max qualifying responses per sec.

set size at responders

	1	6	11	16	21	26

Trusted directory
(Qualifying response: <= 5s)

set size at responders

	1	6	11	16	21	26

Untrusted directory
(Qualifying response: <= 8s)

A conservative estimate:

A throughput of 50 qualifying responses per second is enough to enable each of the about $3x10^8$ Internet users in the U.S to set up or change passwords on more than 5 accounts per year.

Summary

Summary

- **A framework to detect password reuse:**
  - **Account security**
  - **Account location privacy**

Summary

- A framework to detect password reuse:
  - Account security
  - Account location privacy
- **A novel PMT protocol**

Summary

- A framework to detect password reuse:
    - Account security
    - Account location privacy
- A novel PMT protocol
- **First to actively interfere with password reuse on the server side**

Summary

- A framework to detect password reuse:
  - Account security
  - Account location privacy
- A novel PMT protocol
- First to actively interfere with password reuse on the server side
- **We believe even modest adoption of our framework would break the culture of password reuse and improve users' account security on the web**