Proactive Discovery of Phishing Related Domain Names

Samuel Marchal, Jérôme François, Radu State and Thomas Engel

UNIVERSITÉ DU LUXEMBOURG

SnT

NETLAB

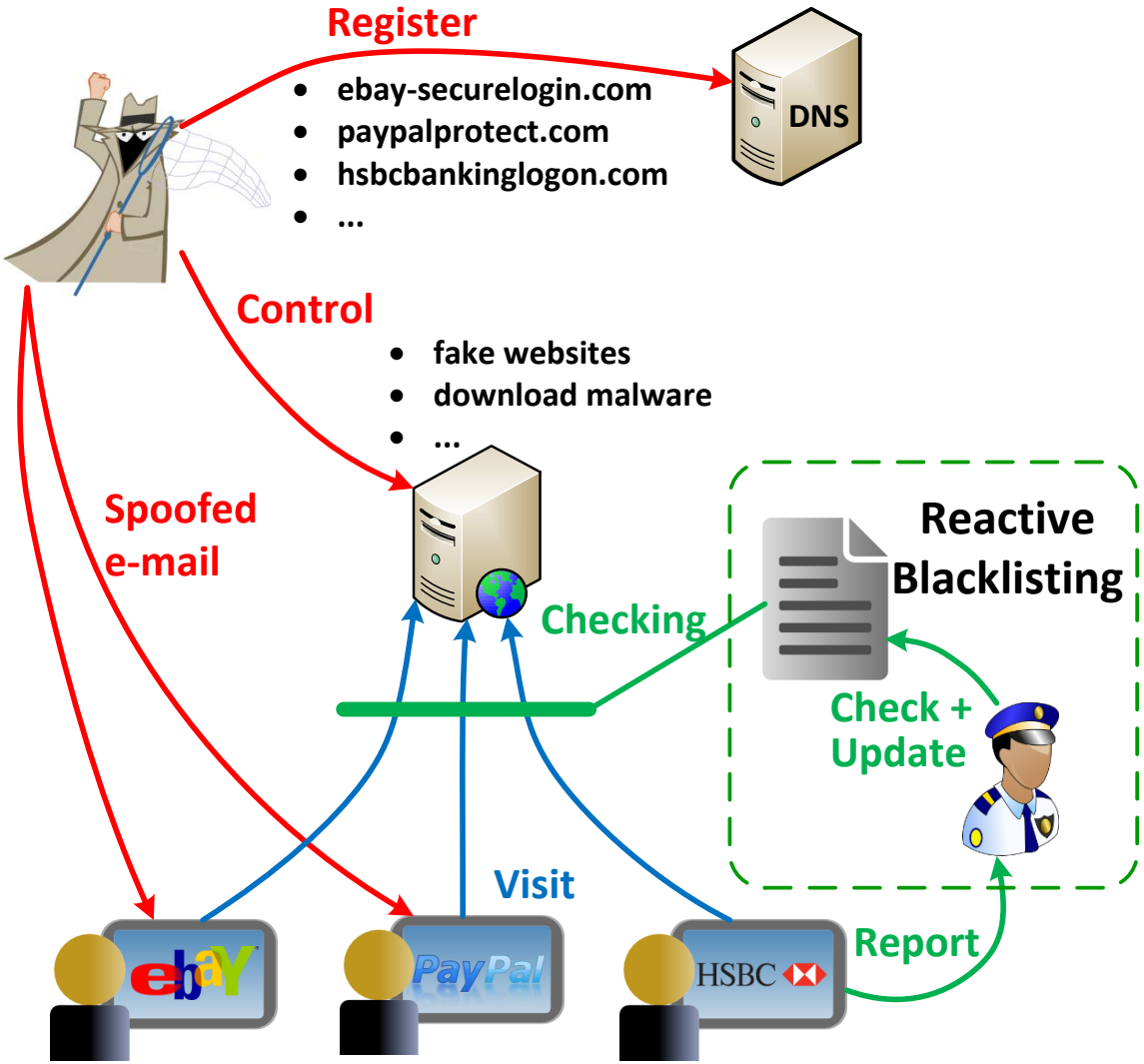
SNT

Outline

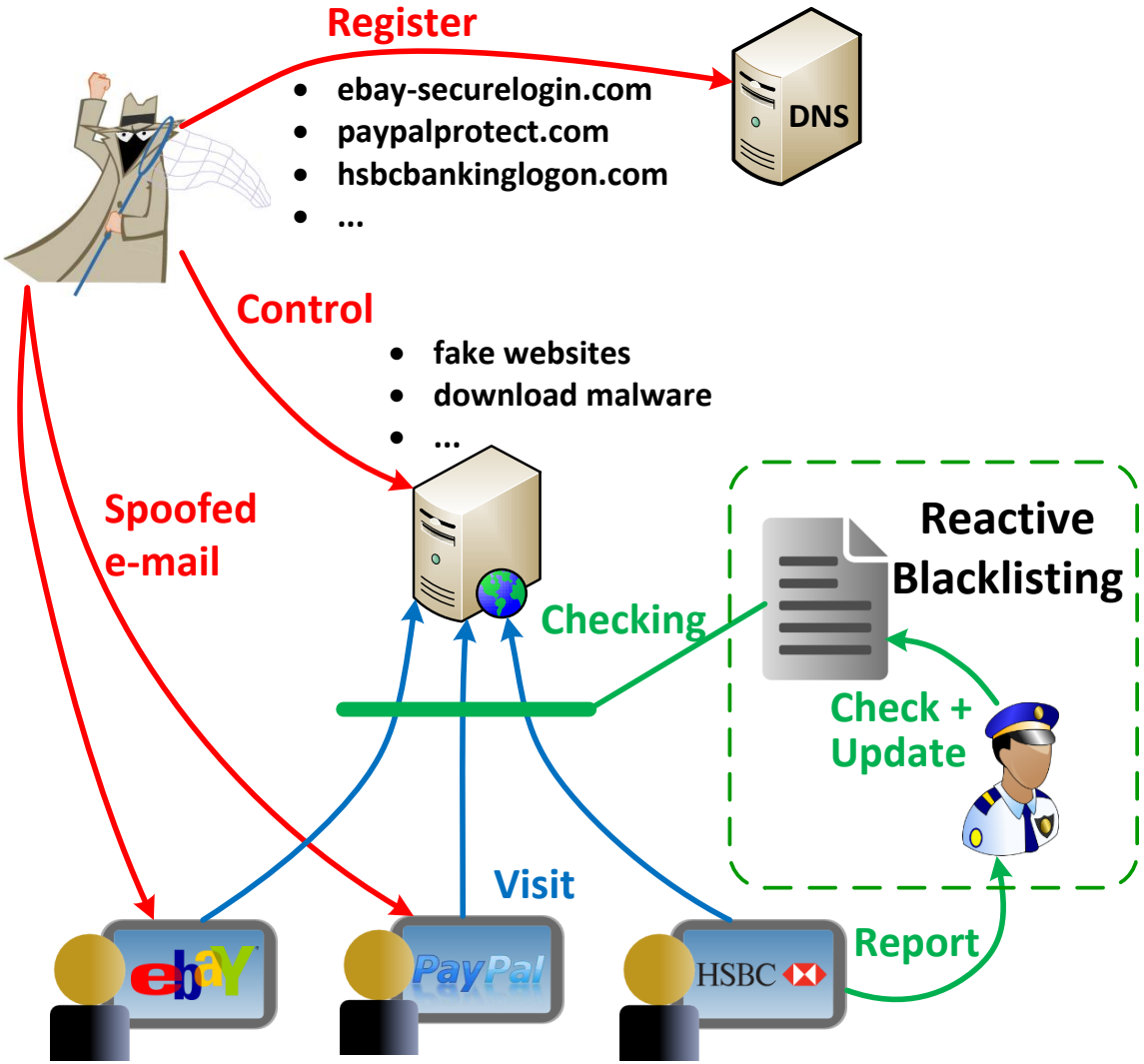
SNT

Outline

Phishing principles & defenses



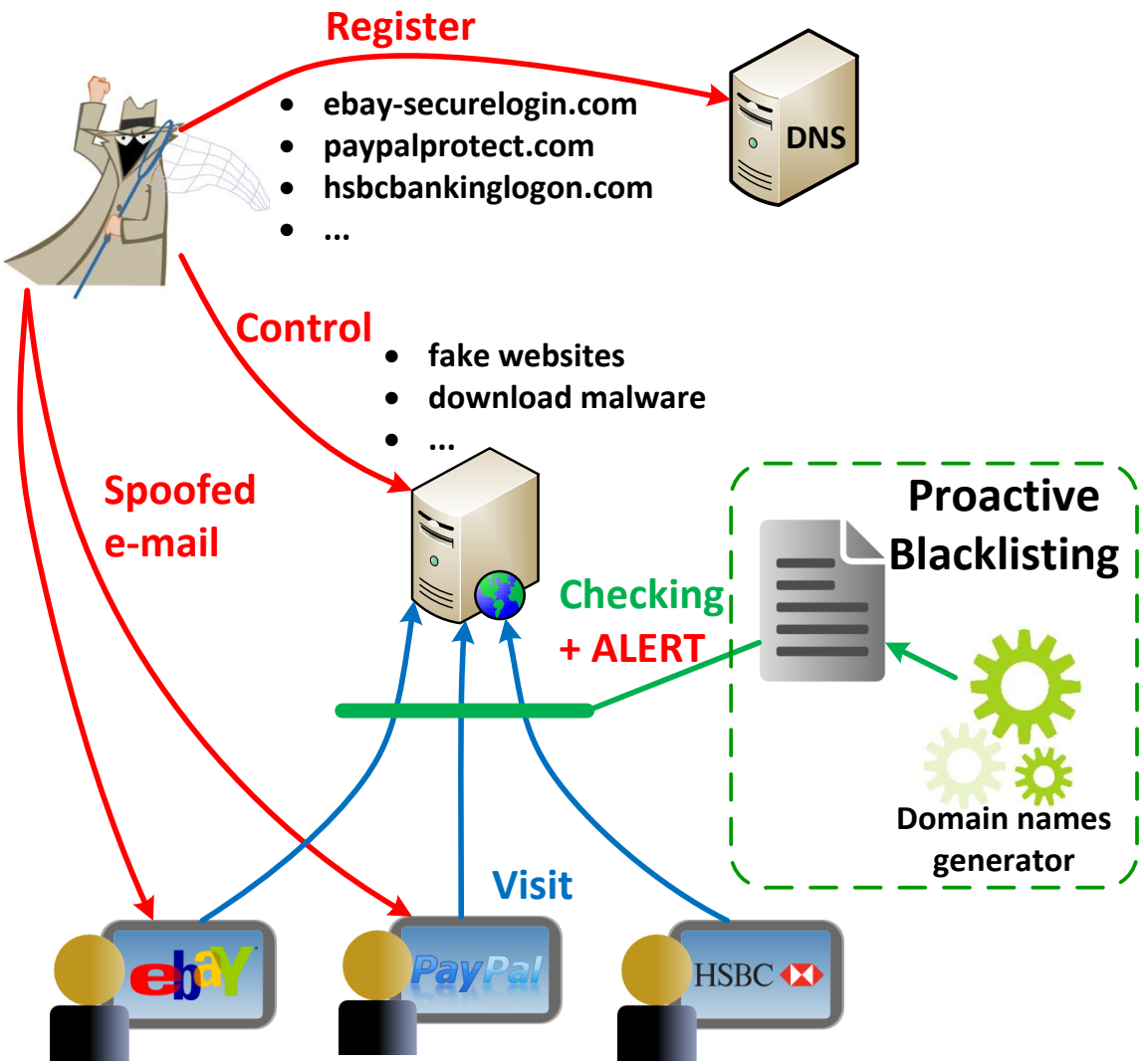
Phishing principles & defenses



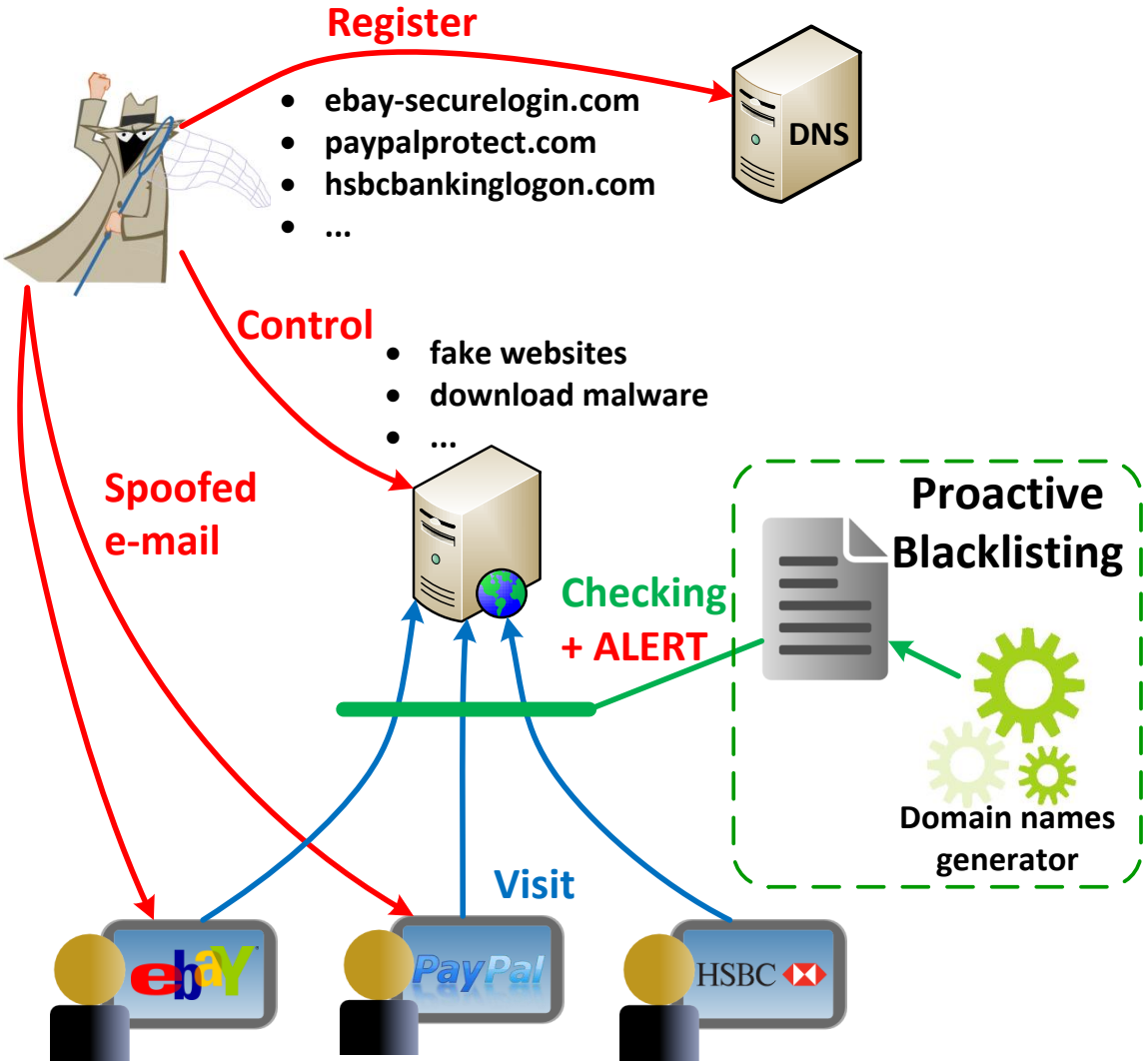
Limitations:

- median lifetime: 12 hours
- monetary damage: 90% in 24 hours
- new phishing websites: >50,000/month
- new maliciously registered domain names: >16,000/month

Early blacklisting solution



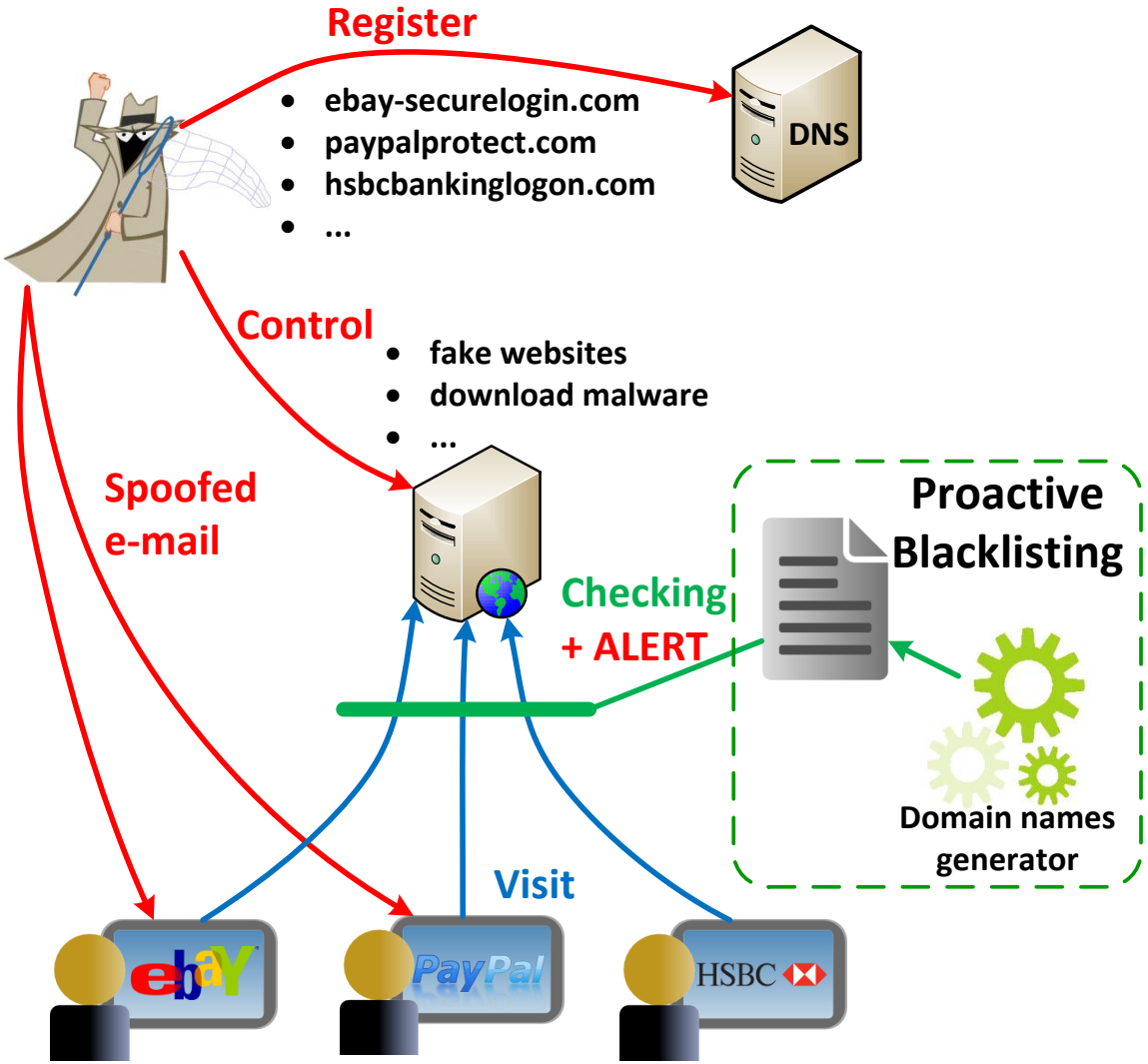
Early blacklisting solution



State of the Art:

- analyse early behaviour of domain names
- domains registered at the same time
- reg-exp based blacklisting

Early blacklisting solution



State of the Art:

- analyse early behaviour of domain names
- domains registered at the same time
- reg-exp based blacklisting

Limitations $\Longrightarrow$ needs users visit & phishing campaign specific

SNT

Outline

SnT

Natural language model

Key idea: generate domain names similar to those registered by phishers

SNT

Natural language model

Key idea: generate domain names similar to those registered by phishers $\Longrightarrow$ *relying on natural language*

SNT

Natural language model

Key idea: generate domain names similar to those registered by phishers $\Longrightarrow$ *relying on natural language*

- focus on *main domain* + *TLD*
  ex: www.login.**myphishingdomain.com**/index.php
- extract features from blacklisted phishing domain names
- deduce a generation model for domain names

SNT

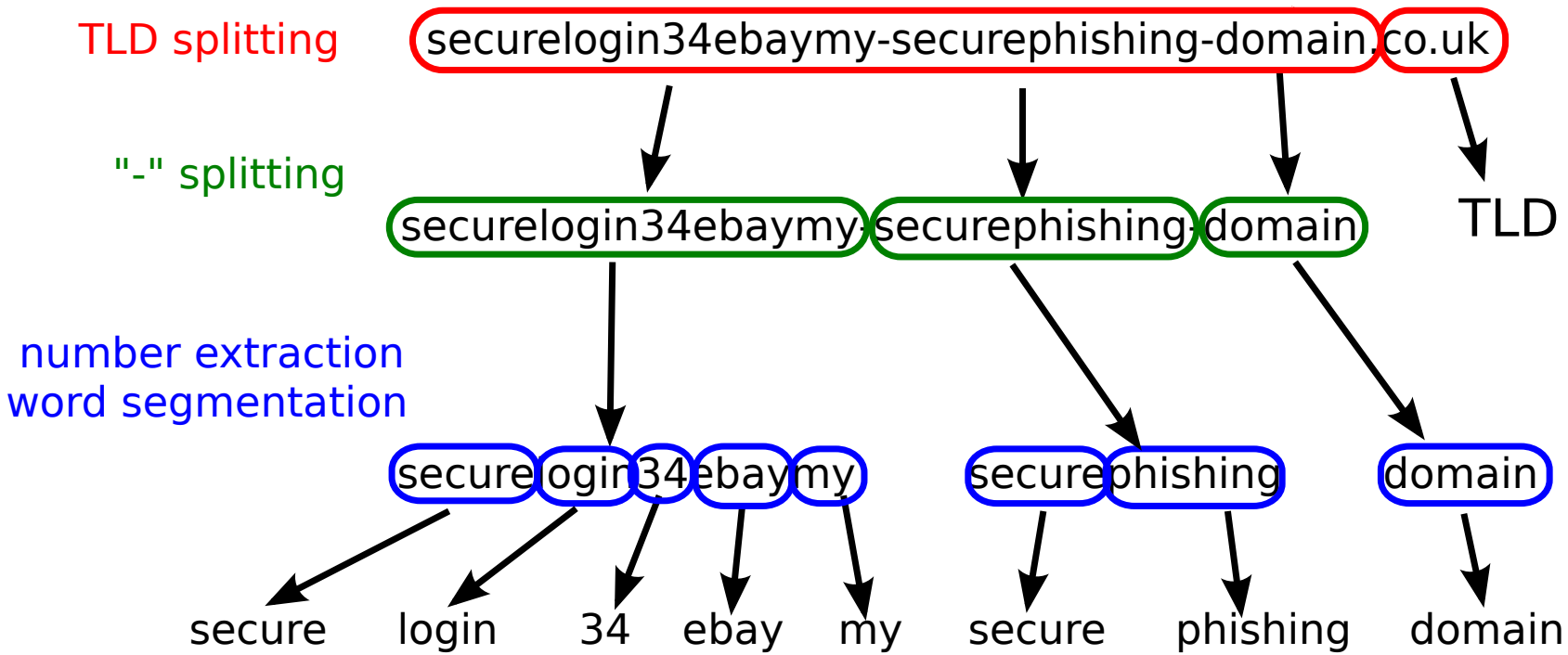
Natural language model

Key idea: generate domain names similar to those registered by phishers $\Longrightarrow$ *relying on natural language*

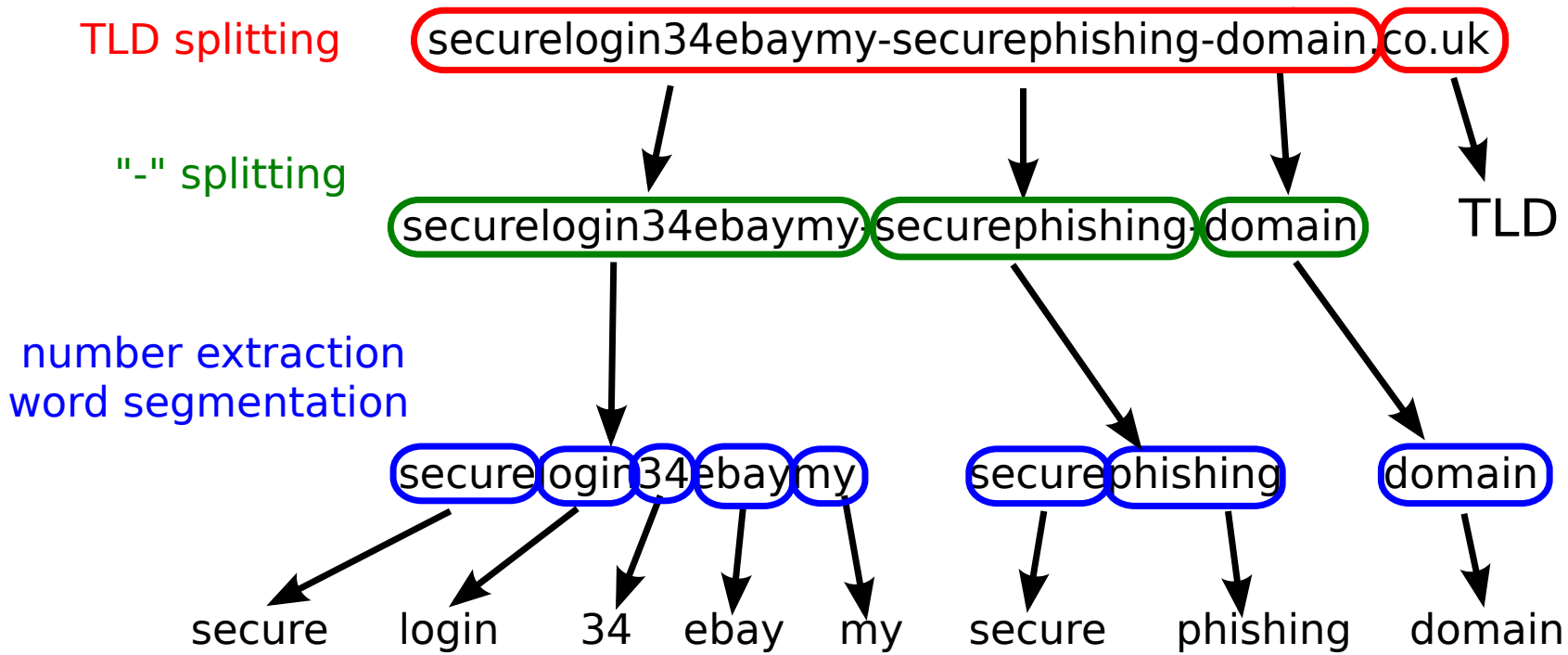
- focus on *main domain* + *TLD*
  ex: www.login.**myphishingdomain.com**/index.php
- extract features from blacklisted phishing domain names
- deduce a generation model for domain names

$\Longrightarrow$ Build a blacklist of potential phishing domains even before they are registered

Features extraction

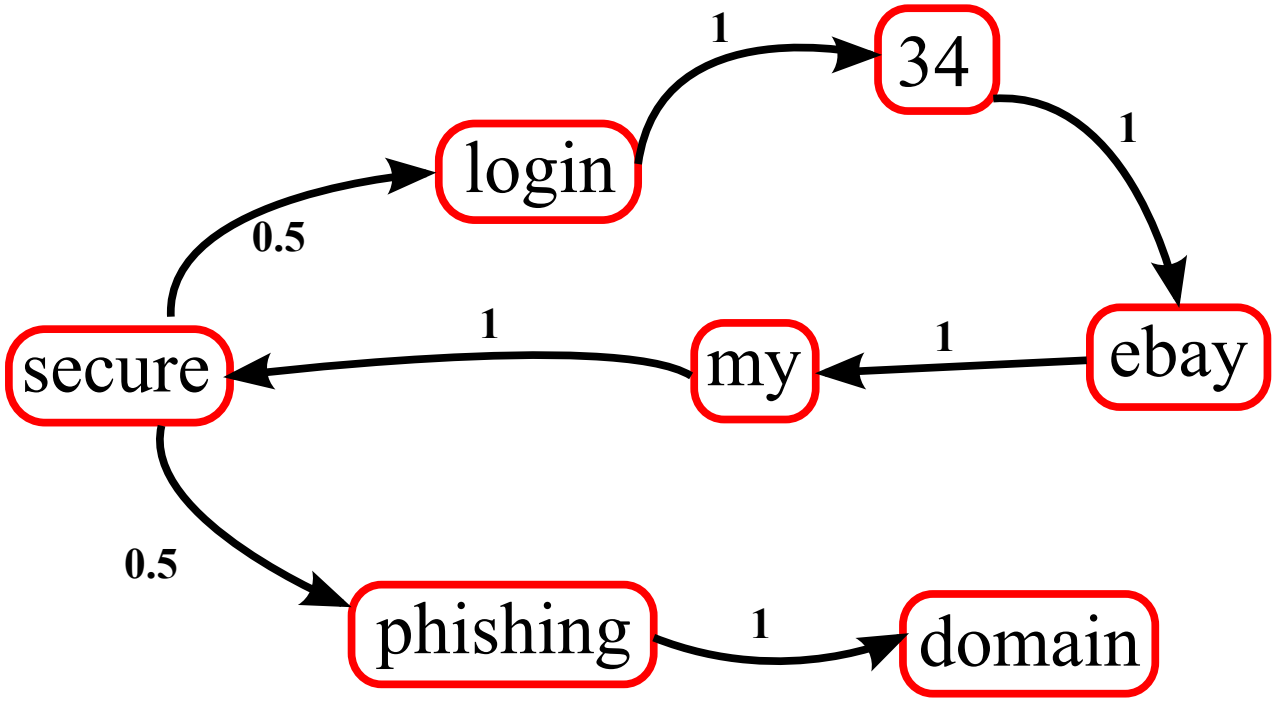


Features extraction



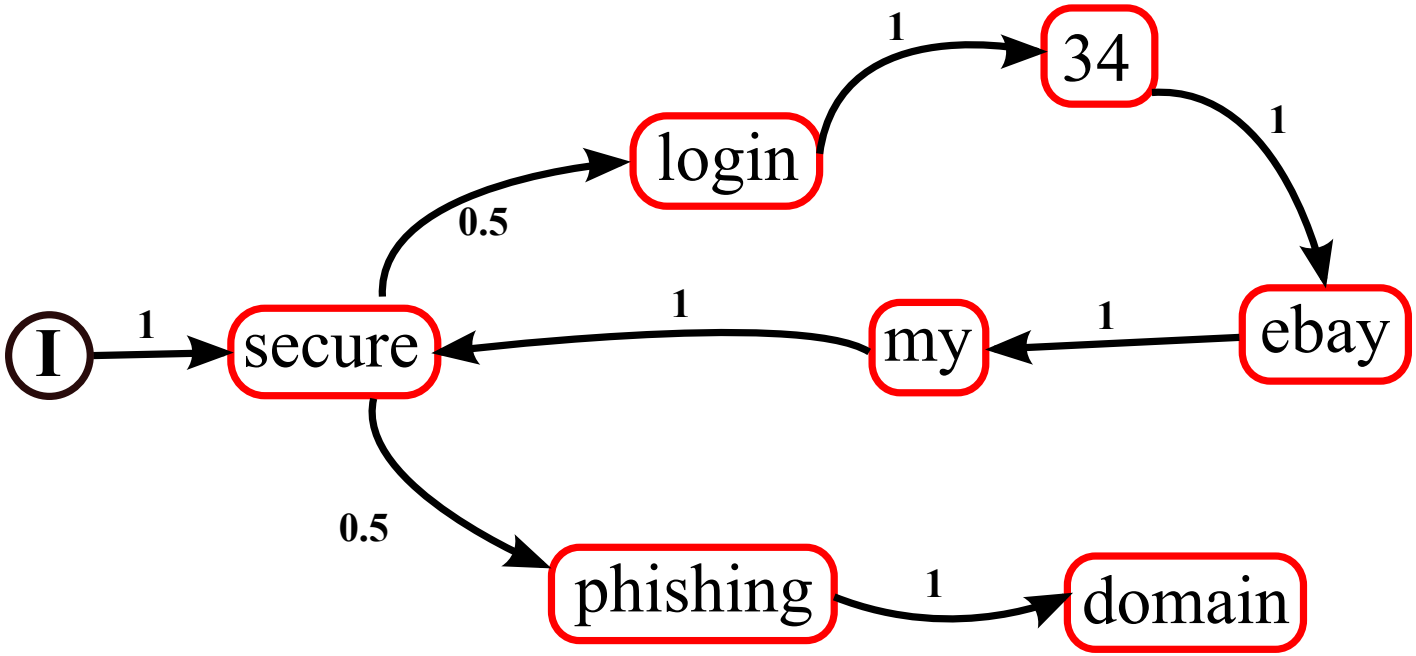
- $distlen = \{(8, 1)\}$
- $distword = \{(secure, 0.25), (login, 0.125), (34, 0.125), (ebay, 0.125), ...\}$
- $distfirstword = \{(secure, 1)\}$
- $distbiwords = \{(secure, \{(login, 0.5), (phishing, 0.5)\}), (login, \{(34, 1)\}), ...\}$

Model generation



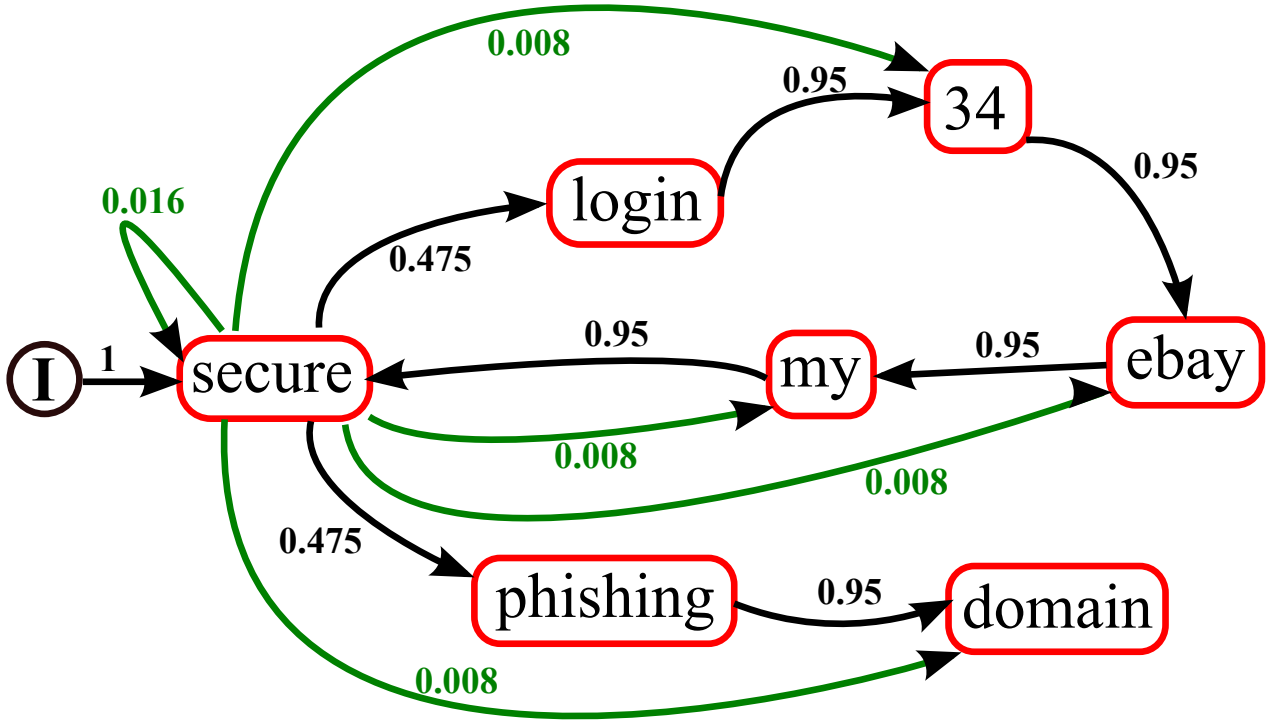
- $distlen = \{(8, 1)\}$
- $distword = \{(secure, 0.25), (login, 0.125), (34, 0.125), (ebay, 0.125), ...\}$
- $distfirstword = \{(secure, 1)\}$
- $distbiwords = \{(secure, \{(login, 0.5), (phishing, 0.5)\}), (login, \{(34, 1)\}), ...\}$

Model generation



- $distlen = \{(8, 1)\}$
- $distword = \{(secure, 0.25), (login, 0.125), (34, 0.125), (ebay, 0.125), ...\}$
- $distfirstword = \{(secure, 1)\}$
- $distbiwords = \{(secure, \{(login, 0.5), (phishing, 0.5)\}), (login, \{(34, 1)\}), ...\}$

Model generation



- $distlen = \{(8, 1)\}$
- $distword = \{(secure, 0.25), (login, 0.125), (34, 0.125), (ebay, 0.125), ...\}$
- $distfirstword = \{(secure, 1)\}$
- $distbiwords = \{(secure, \{(login, 0.5), (phishing, 0.5)\}), (login, \{(34, 1)\}), ...\}$

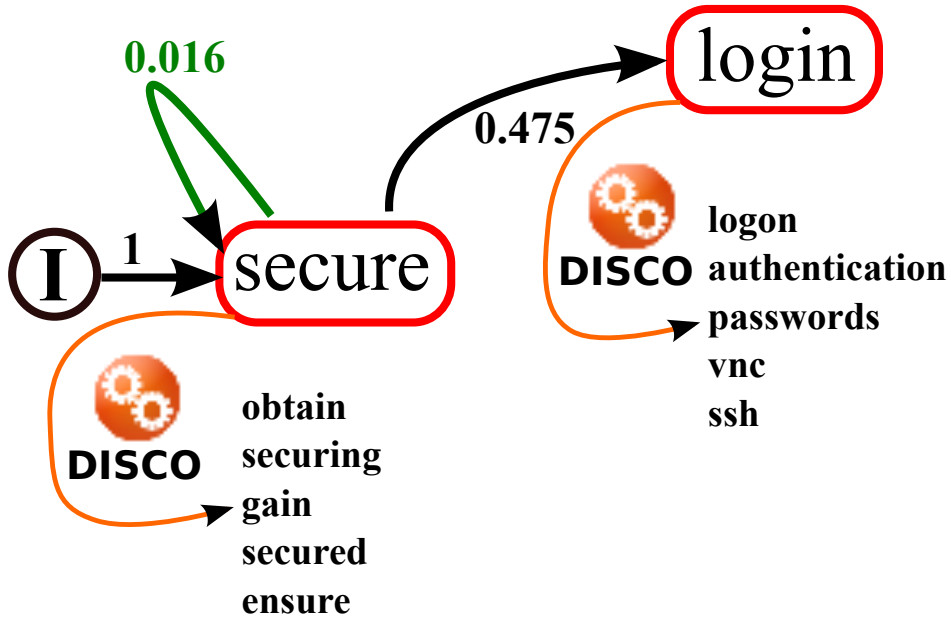
Semantic extension

Disco:

- calculate a similarity score (semantic relatedness) between 2 words
- give the *n* most related words to *w*
- based on dictionary (Wikipedia, BNC, PubMed, etc.)
- applied to each state of the Markov Chain

$\Rightarrow$ expand the discovery

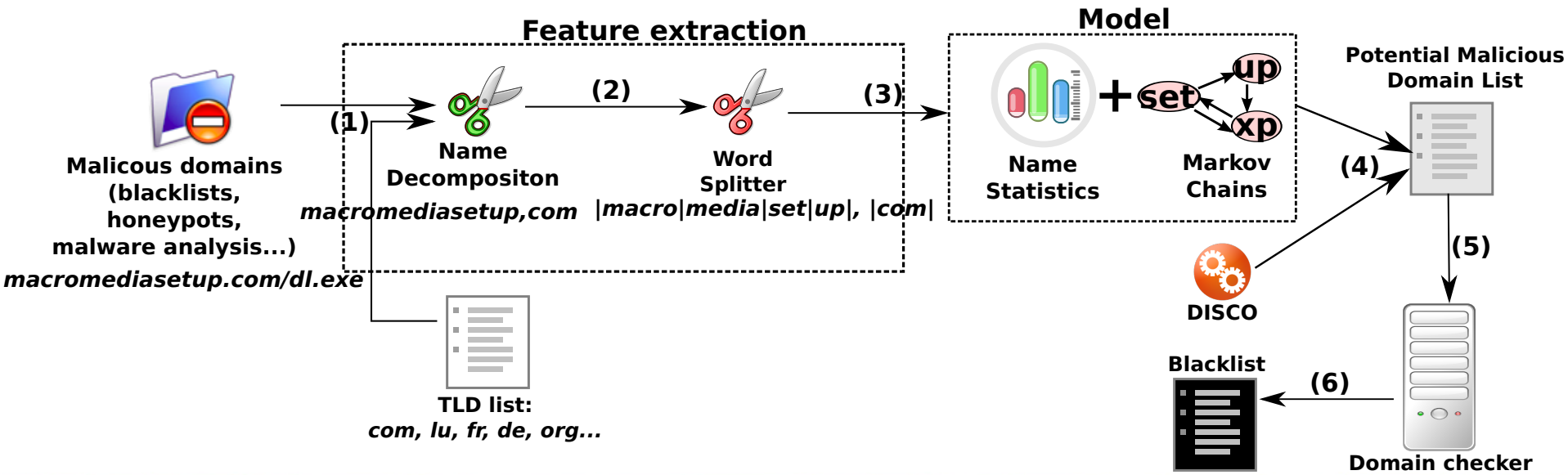
`http://www.linguatools.de/disco`



Generator global overview

- extract features from known phishing domains
- generate domain names ⇒ potentially phishing
- domain names automatically checked further

$\Longrightarrow$ **Blacklist**



SNT

Outline

SNT

Offline testing

Phishing domain set from blacklists (∼ 50,000):

- Malware Domain List (01/2009 → 03/2012)
- DNS-Black-Hole (01/2009 → 03/2012)
- PhishTank (07/2007 → 03/2012)

SNT

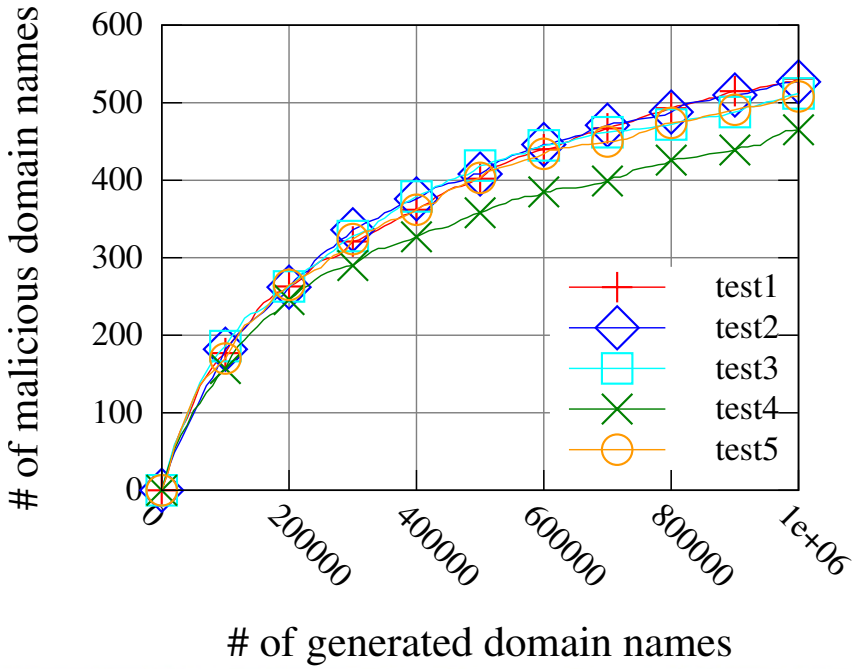
Offline testing

Phishing domain set from blacklists (∼ 50,000):

- Malware Domain List (01/2009 → 03/2012)
- DNS-Black-Hole (01/2009 → 03/2012)
- PhishTank (07/2007 → 03/2012)

5 tests of 1 million domain generations

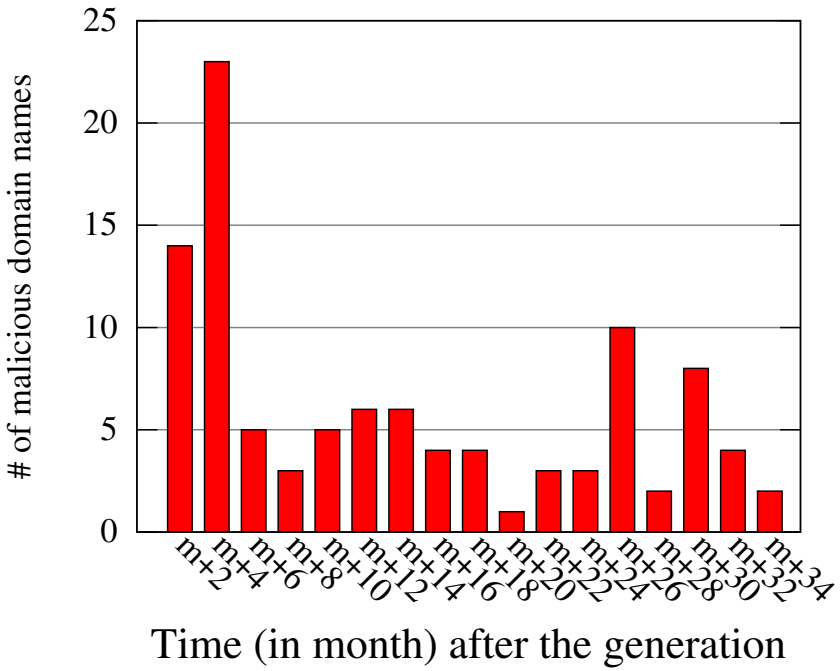
- learning set 30% (15,000 domains)
- testing set 70% (35,000 domains)



Offline testing

Predictability

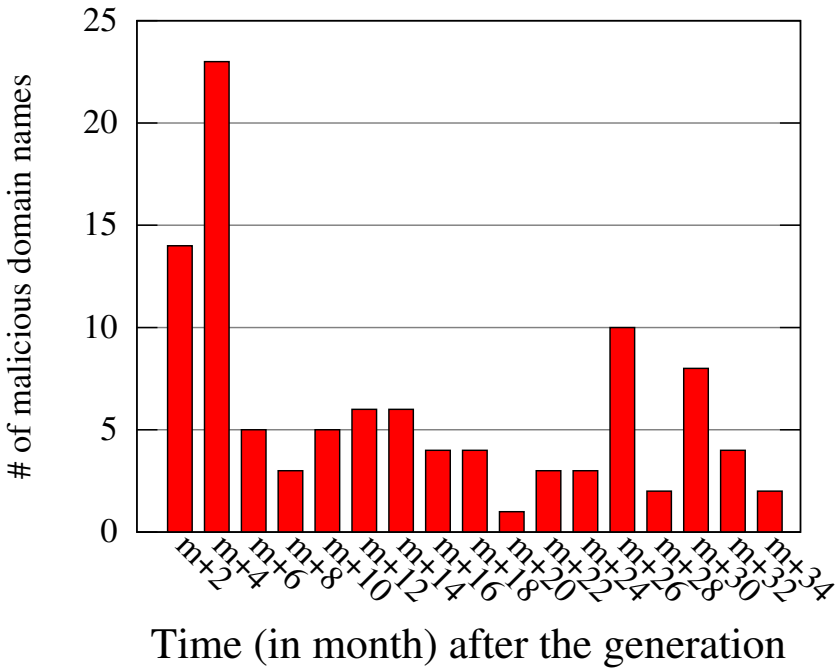
- learning: the 10% oldest
- testing: 90% remaining



Offline testing

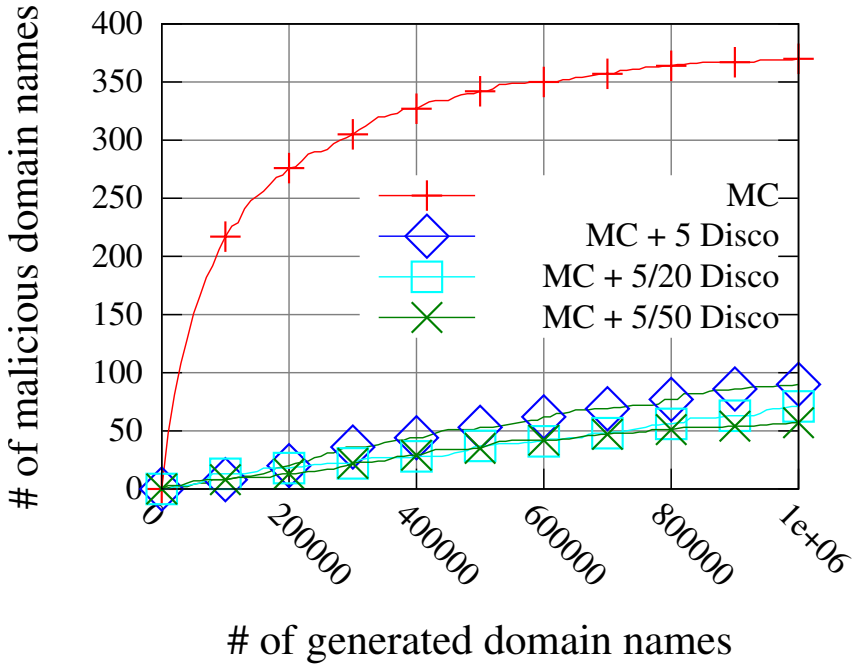
Predictability

- learning: the 10% oldest
- testing: 90% remaining



Strategy

- learning set 30%
- testing set 70%



SNT

Online testing

DNS request for 1 million domains generated

$\sim$ 100,000 domains match an @IP:

- $\sim$ 80,000 wildcardings domains
- $\sim$ 5,000 domains for sale
- $\sim$ 15,000 remaining domains:
  - $\sim$ 500 actually malicious and blacklisted
  - $\sim$ 200 legitimate domains

SNT

Online testing

DNS request for 1 million domains generated

$\sim$ 100,000 domains match an @IP:

- $\sim$ 80,000 wildcardings domains
- $\sim$ 5,000 domains for sale
- $\sim$ 15,000 remaining domains:
  - $\sim$ 500 actually malicious and blacklisted
  - $\sim$ 200 legitimate domains

Discriminate phishing from legitimate generated domains:

MCscore

$\Longrightarrow$ Eliminate 93 % of legitimate domains...

SNT

Online testing

DNS request for 1 million domains generated

$\sim$ 100,000 domains match an @IP:

- $\sim$ 80,000 wildcardings domains
- $\sim$ 5,000 domains for sale
- $\sim$ 15,000 remaining domains:
  - $\sim$ 500 actually malicious and blacklisted
  - $\sim$ 200 legitimate domains

Discriminate phishing from legitimate generated domains:

MCscore

$\Longrightarrow$ Eliminate 93 % of legitimate domains...

...while keeping 57 % of phishing domains (285)

SNT

Outline

SNT

Conclusion

Generation of domain names likely to be malicious

- features extracted from existing domain names
- Markov chain model
- semantic relatedness techniques

$\Longrightarrow$ Proactively build a phishing blacklist

Results:

- able to generate phishing domains...
- ... still with false positives

$\Longrightarrow$ Domain scoring based on Markov chain model

Future works:

- remaining part of architecture: domain checker
- reinforcement learning

Proactive Discovery of Phishing Related Domain Names

Samuel Marchal, Jérôme François, Radu State and Thomas Engel

UNIVERSITÉ DU LUXEMBOURG

SnT

NETLAB