

LookAhead: Augmenting Crowdsourced Website Reputation Systems with Predictive Modeling

Kalle Saari, Sourav Bhattacharya, Otto Huhta,
Mika Juuti, and N. Asokan

Aalto University, Finland

June 12, 2015

Crowdsourced Website Reputation Systems

VuuPC 

www.vuupc.com

Download VuuPC
download is not

VuuPC, You

www.shouldiremoveit.com

The software
legitimate app

WOT




[click to view details](#)

vuupc.com

Trustworthiness

Child safety



-  Malware or viruses
-  Scam
-  Suspicious

Download Size: 1mb. This
earn more.

Should I Remove It? 

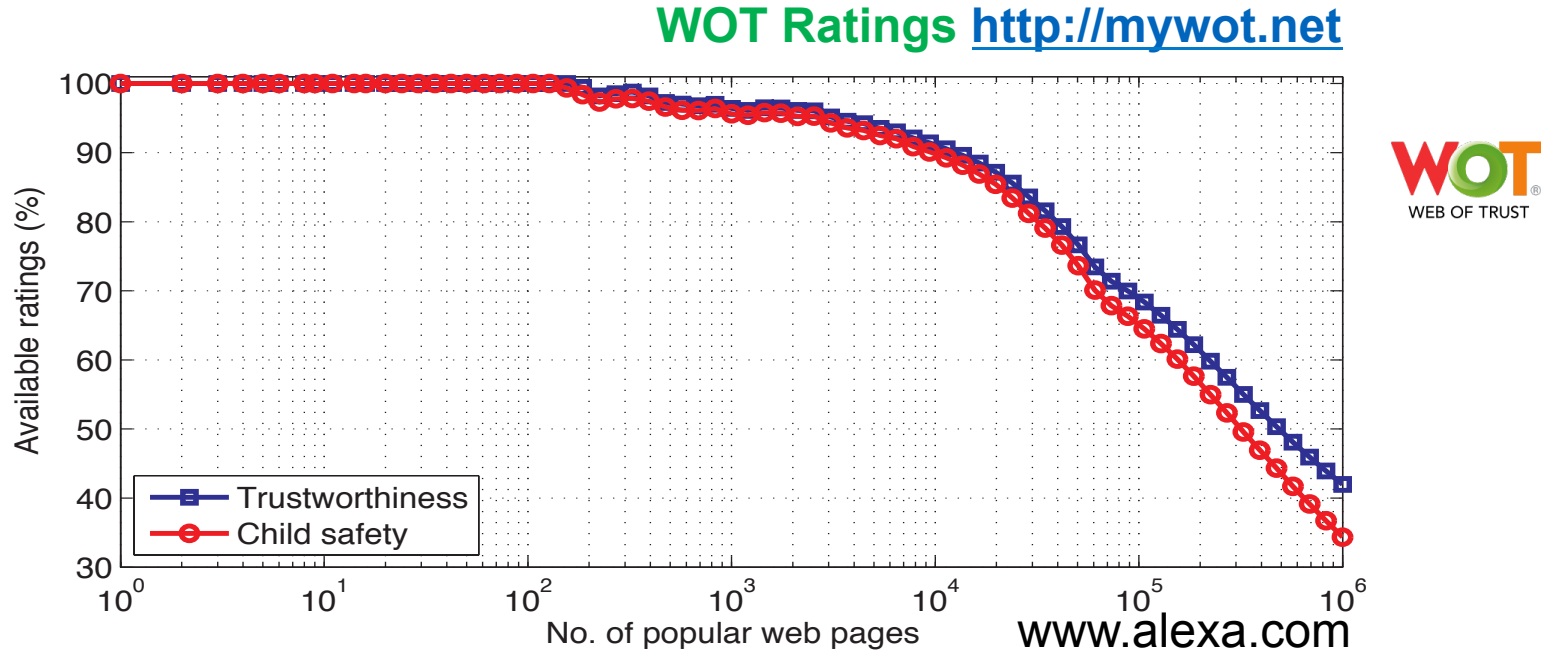
[Away-35025-...](#) ▼

an installer that bundles
ty ...

Problems with Crowdsourced Systems 1

- **Coverage**

- Majority of top-1M of websites do not have WOT ratings



Problems with Crowdsourced Systems 2

- **Time lag**
 - Time needed to accumulate enough ratings
- **Susceptibility to Sybil attacks**
 - Attacker generates false ratings to influence final ratings
- **Lack of incentives**
 - Lack of motivation for user to participate in rating
- **Subjectivity**
 - *Trustworthiness* is highly **subjective** notion

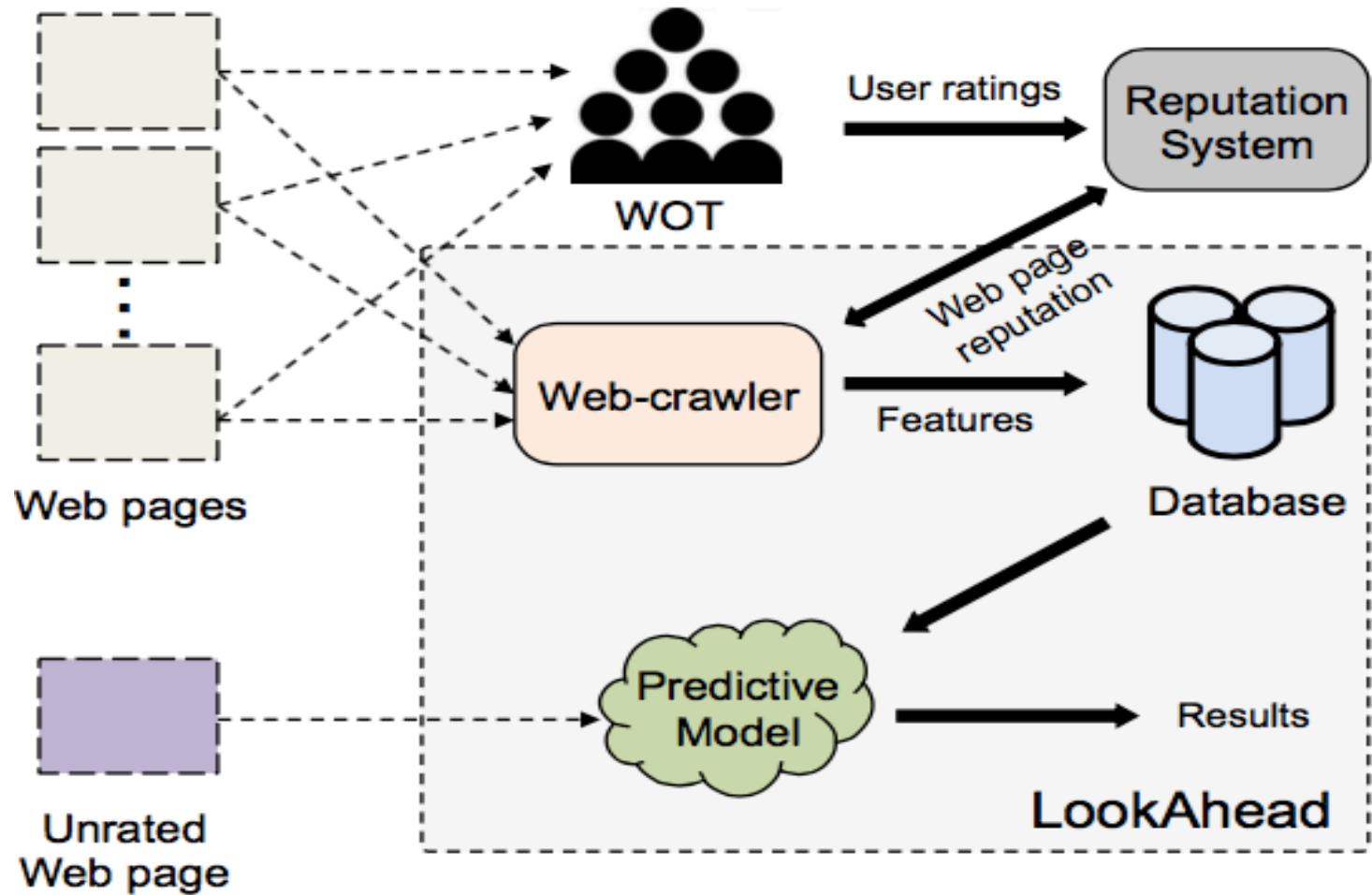
Idea: Predict Reputation Ratings

Use available data to generate **automatic** predictions for **eventual** ratings

Potential applications

1. **Immediate** user feedback: give estimates of ratings for unrated websites
2. **Fast-track** publication of ratings: fewer ratings needed

Solution Overview: LookAhead Architecture



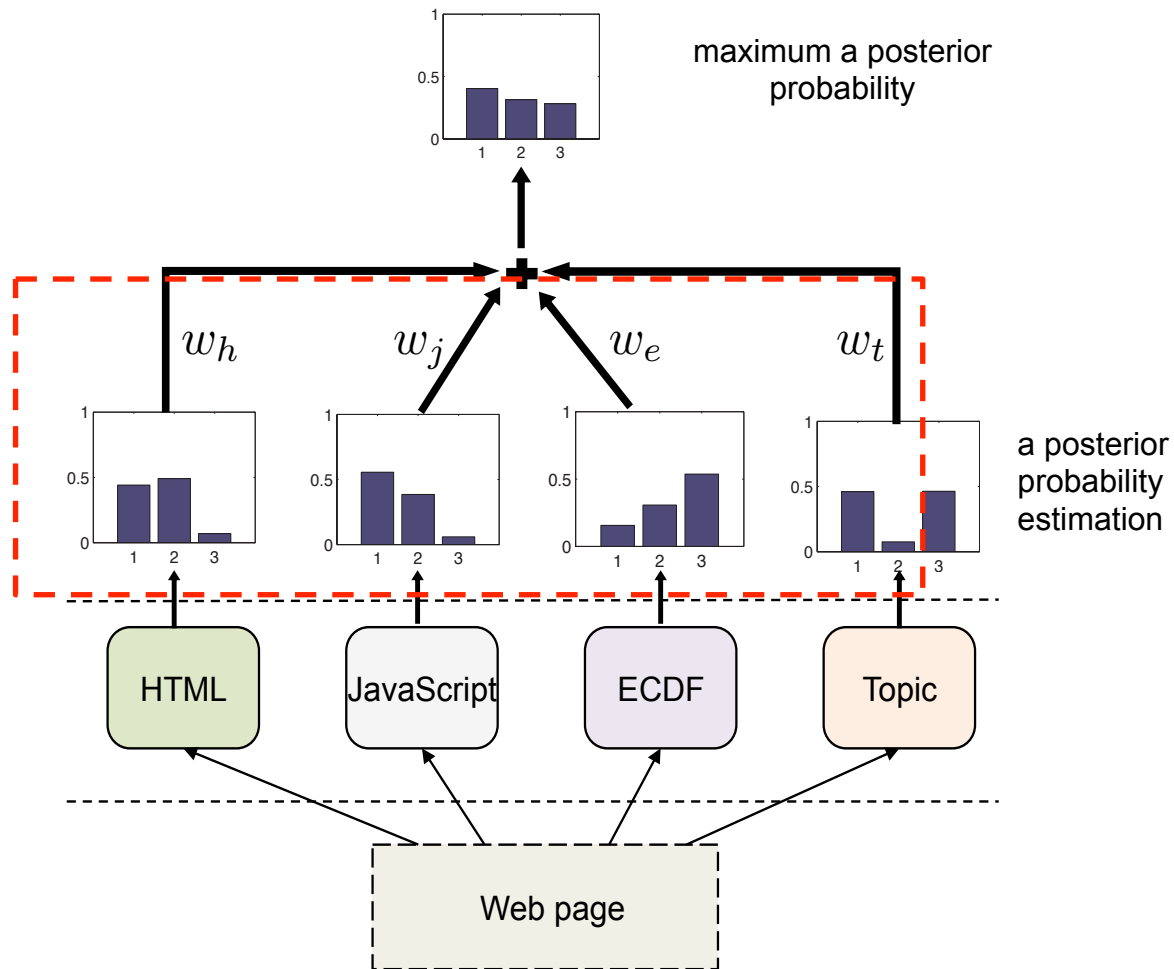
Solution Overview: Features

We use four different **feature classes** based on:

- HTML *
- JavaScript *
- Ratings of **embedded links**
- **Topic model** from text contents of websites

** Prophiler: a fast filter for the large-scale detection of malicious web pages. (WWW '11) by Canali et al.*

Solution Overview



Fundamental Problem: Feature Availability

- Not all features always present
 - HTML always there
 - But JavaScript, ratings of links, or topics might be missing
- How to deal with missing features?

Fixing the Problem: Modify Features

- **Observation:** Missing values are **not missing at random**, they provide information!
- Add indicator variable for each feature class that lights up if that feature class is missing

Performance

Reputation	F1-score (%)	FNR (%)	FPR (%)
Trustworthiness	81.4	14.7	23.3
Child-safety	83.4	15.9	17.5

Future Work

- Working with McAfee URL categorization team
- Survey **state of the art** for identifying phishing sites
 - Scope for applying LookAhead techniques?
 - Extend to spam sites?
- Predicting
 - **Categories** of websites?
 - **Susceptibility** for phishing?
- Fortifying features against **adversarial behavior**?
- Use of **additional features** (e.g., URL)?

Conclusion

- **LookAhead**: novel classifier to **support** crowdsourced website reputation systems such as Web of Trust
- Uses four feature classes: HTML, JS, LINKS, TOPICS
- Performance: FPR and FNR in the range of 14-24%
- Satisfying because of **subjective** ratings and **static** features