<FPSelect: Low-Cost Browser Fingerprints for Mitigating Dictionary Attacks against Web Authentication Mechanisms>

ACSAC 2020, December 11, 2020

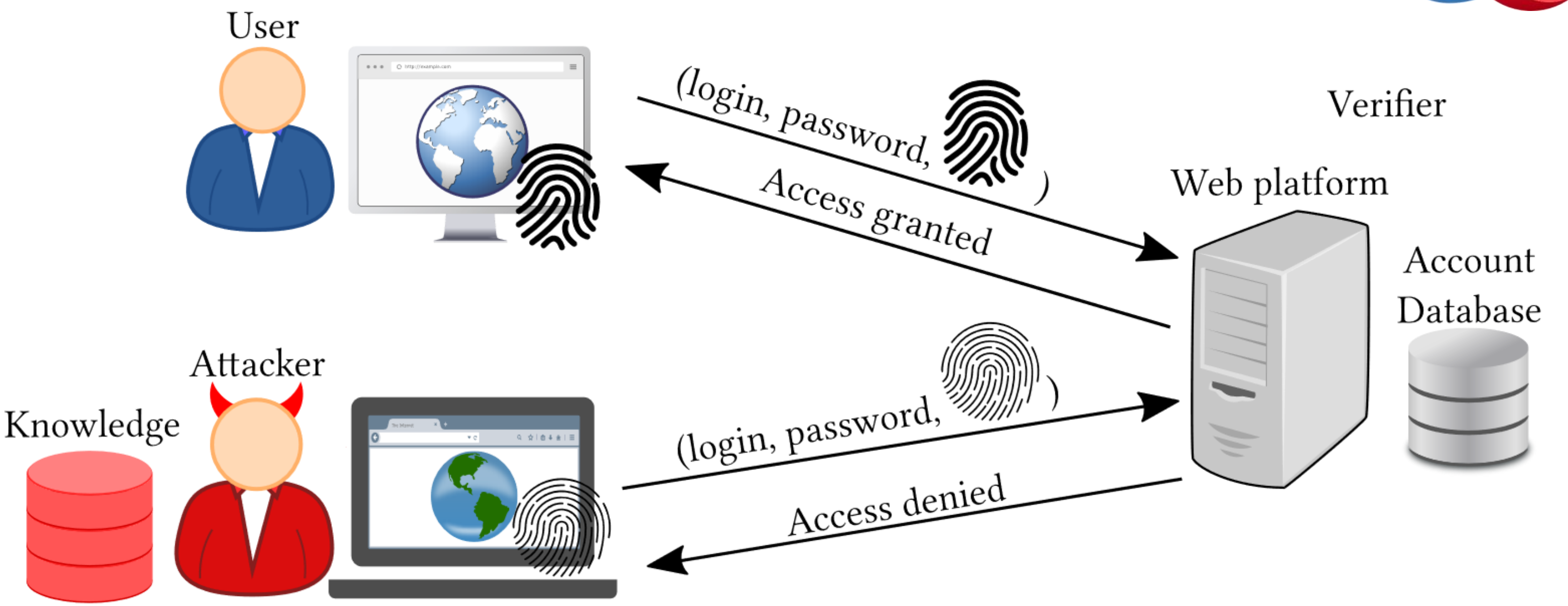
Nampoina Andriamilanto, Tristan Allard, Gaëtan Le Guelvouit

Context

- **Passwords suffer from flaws**
  - Dictionary attacks: common passwords [6] or reuse [16]
  - Phishing attacks: 12.4 million stolen credentials [12]

- **Other authentication factors reduces usability [3]**
  - User must remember, possess, or do something

- **Browser fingerprinting [2, 11]**
  - Collection of browser attributes
  - Depending on the web environment



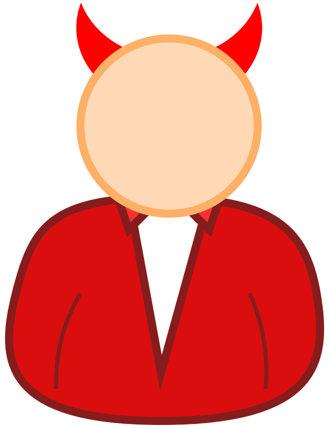
- **Adding an attribute**
  - Helps distinguish browsers
  - Reduces usability
- **Hundreds of attributes are available [2, 11, 13]**
  - Collecting them all is unpractical (e.g., taking too long to collect)
- **Previous works**
  - Use the well-known attributes [2, 11, 15]
  - Iteratively pick attributes [7, 8, 9, 17]
  - Evaluate every possible set [4]

Attribute Selection Framework

- The attacker knows a **fingerprint** distribution
  - Submits the **ß-most common** fingerprints

- Example
  - ß=2
  - f_1 and f_2 are submitted
  - The sensitivity is of 4/7

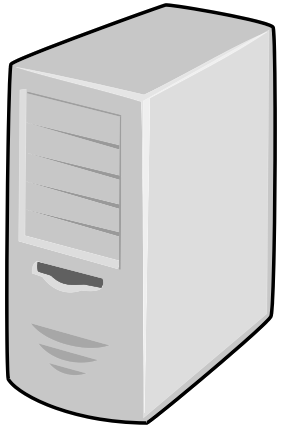
Attacker



F	PMF
f_1	0.40
f_2	0.20
f_3	0.10
f_4	0.10
f_5	0.10
f_6	0.05
f_7	0.05

U	F	Spoofed
u_1	f_2	●
u_2	f_1	●
u_3	f_4	○
u_4	f_2	●
u_5	f_3	○
u_6	f_5	○
u_7	f_1	●

Web platform



- **Verifier has a set *A* of candidate attributes**

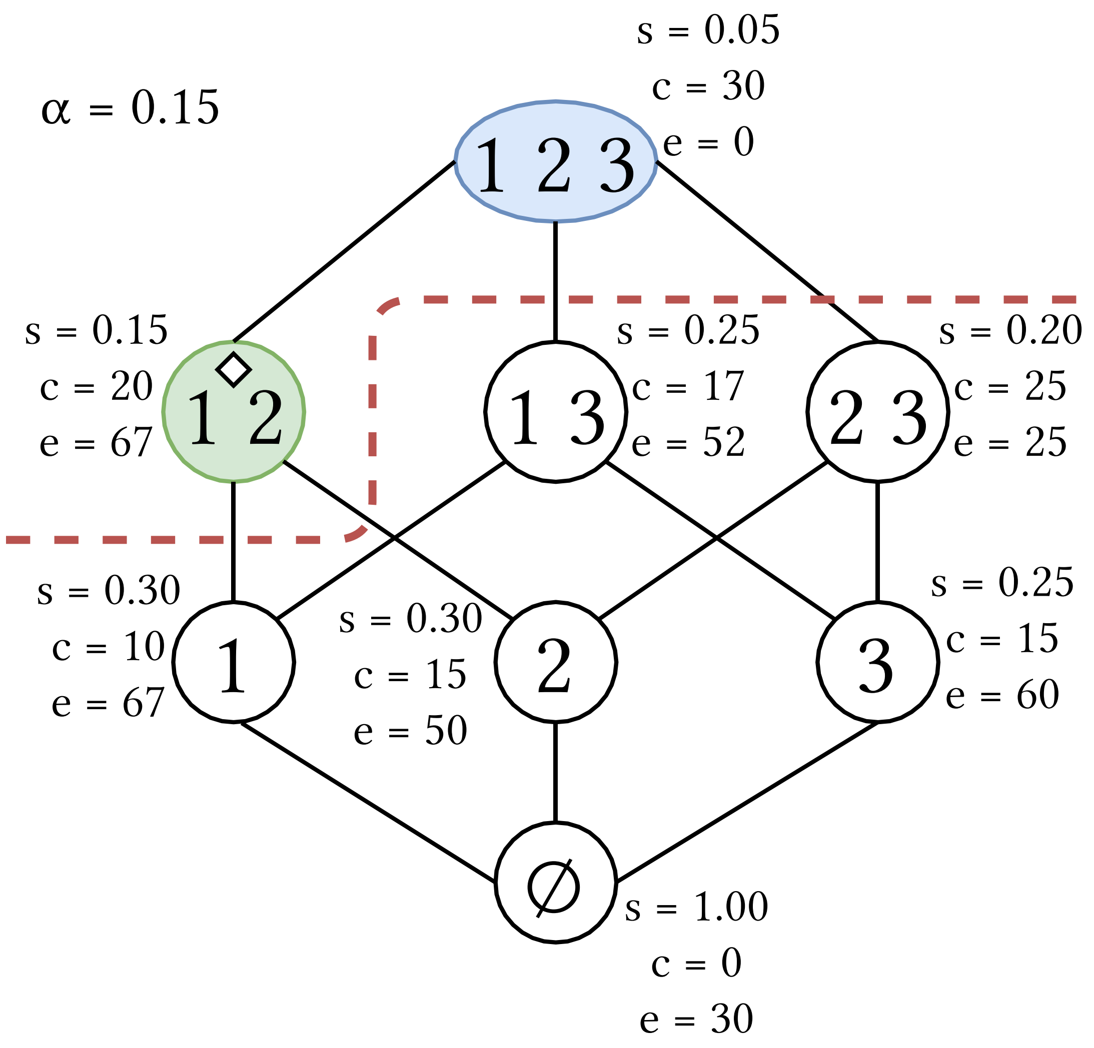
- **Verifier seeks the attribute set**
  - Satisfies a security level *α*
  - At the lowest cost

- **Attribute set *C* ⊆ *A***
  - c(*C*): its usability cost (strictly increasing)
  - s(*C*): its sensitivity (decreasing)

$$\arg\min_{C \subseteq A} \{\mathrm{c}(C) : \mathrm{s}(C) \leq \alpha\}$$

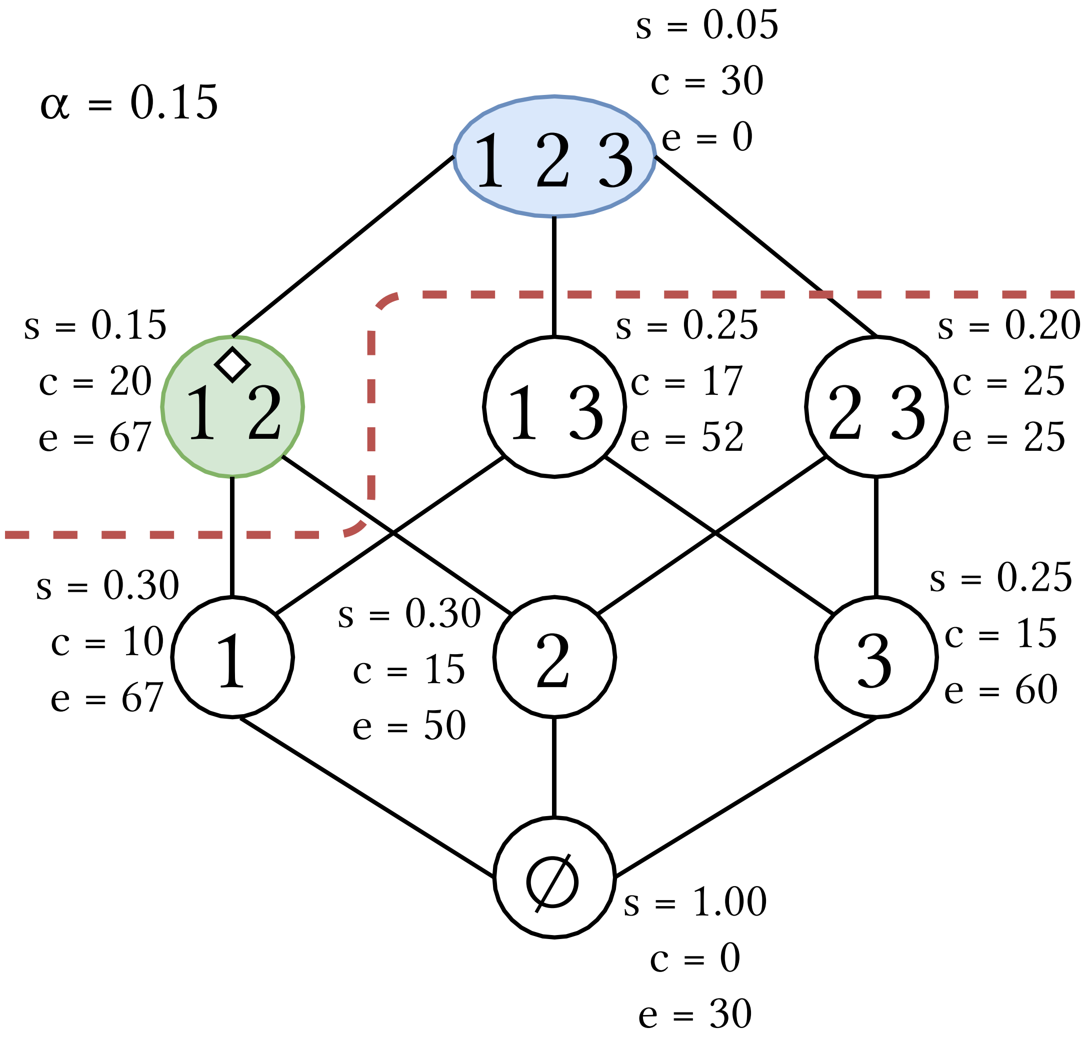
- **Greedy exploration algorithm**
  - Expands by adding one attribute
  - Holds *k*-nodes to expand
  - Partial solutions ordered by the usability gain/sensitivity ratio

- **Pruning methods**
  - Cost higher than the current minimum c_{min} (1)
  - Superset of a node satisfying the threshold or (1)



- **Execution with k=2 and α=0.15**
  - S starts with k-empty sets
  - c_{min} = 20 at stage 2
    - {2, 3} is not expanded
  - {1, 2, 3} is not added to E as it is a superset of {1, 2}

Stage	E	T	S
1	$\{\{1\},\{2\},\{3\}\}$	$\{\}$	$\{\{1\},\{3\}\}$
2	$\{\{1,2\},\{1,3\},\{2,3\}\}$	$\{\{1,2\}\}$	$\{\{1,3\}\}$
3	$\{\}$	$\{\{1,2\}\}$	$\{\}$



- **Usability cost in points**
  - Memory size (10 kilobytes = 10K points)
  - Collection time (1 second = 10K points)
  - Number of changing attributes (1 changing attribute = 10K points)

$$\mathrm{cost}(C, D) = \gamma \cdot [\mathrm{mem}(C, D), \mathrm{time}(C, D), \mathrm{ins}(C, D)]^\intercal$$

C : attribute set
D : fingerprint dataset
γ : cost weights

- **Sensitivity**
  - Measured by the verifier
  - Attacker knows the fingerprint distribution of the protected users
  - Matching function between a submitted and a stored fingerprint

Results

Experimental setup

- **Sample of 30 thousand fingerprints [20, 21]**

- **Verifier and attacker instantiation**
  - Sensitivity thresholds: 0.001, 0.005, 0.015, 0.025 [1, 3, 14]
  - Number of submissions: 1, 4, 16 [5, 18]
  - Explored paths: 1 and 3

- **Matching function** $\sum_{a \in A} f[a] \approx^{a} g[a] > \theta$

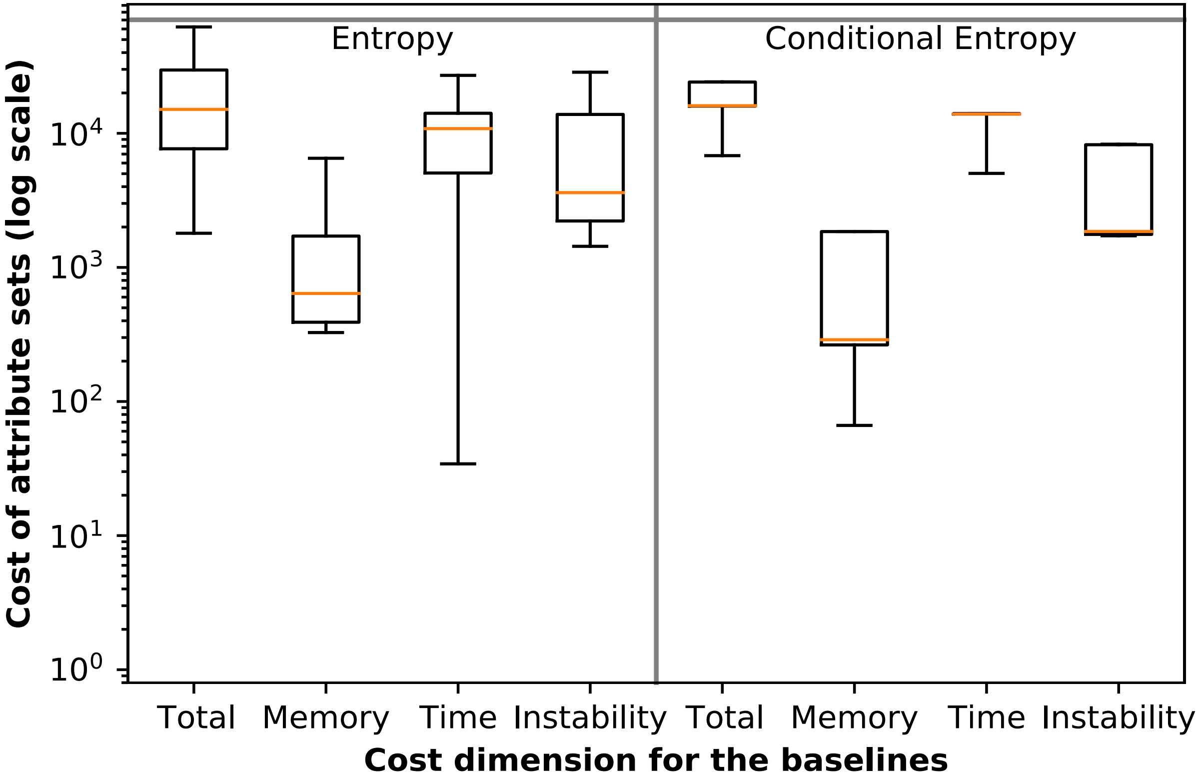
f, g : submitted and stored fingerprint

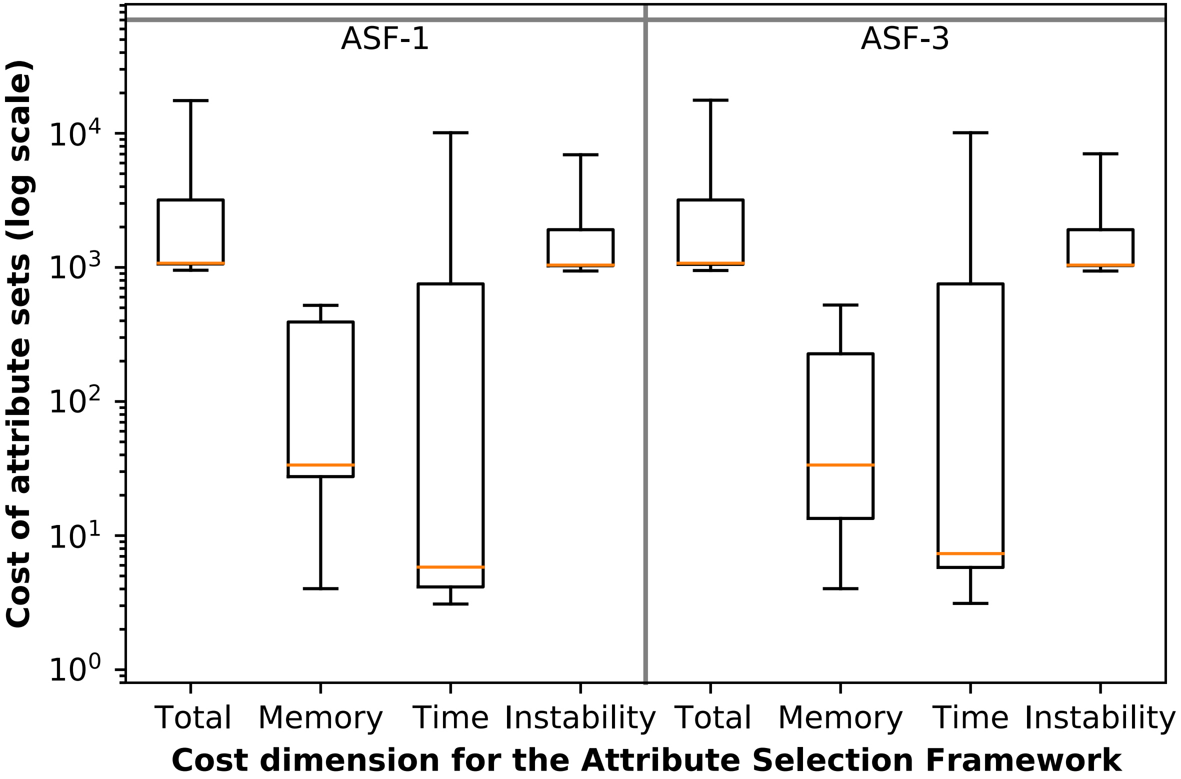
$\approx^{a}$: 1 if a is sufficiently similar between f and g, else 0

θ : matching threshold A : the attributes used

- **Compare FPSelect results with the baselines**
  - Entropy [8, 9]
  - Conditional entropy [7]

Usability Cost Results





A solution for **9** among the **12** cases, due to unreachable sensitivity threshold.

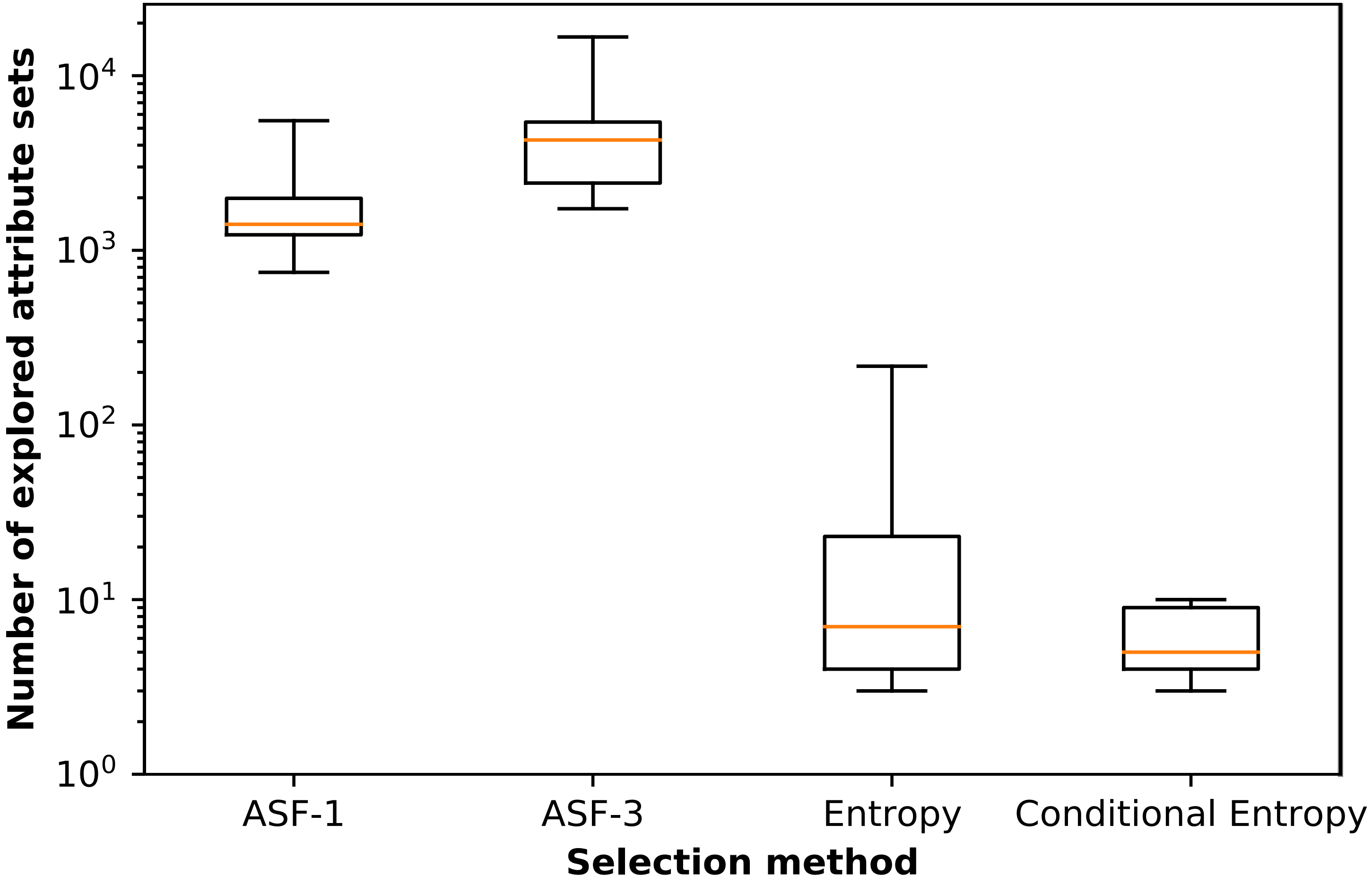
The fingerprints are, on average, up to

- **97 times smaller**
- **3,361 times faster** to collect
- with **7.2 times fewer changing** attributes

Computation Cost

- ASF-1: **three orders of magnitude** more attribute sets than the **baselines**

- ASF3: **three times** more attribute sets than **ASF-1**



Conclusion

- **FPSelect: attribute selection framework**
  - Possibility space as a lattice
  - Greedy exploration algorithm
  - Fingerprints of lower cost than the baselines
  - Higher computation cost
- **Future works**
  - Attackers with targeted knowledge
  - Other experimental settings (browser population, measures)

Thank You

Any question ?

tompoariniaina.andriamilanto@irisa.fr

References

References I

1. **Eiji Hayashi, Rachna Dhamija, Nicolas Christin, and Adrian Perrig. « Use your Illusion: Secure Authentication Usable Anywhere ». In *Symposium on Usable Privacy and Security (SOUPS)*, 35–45, 2008. https://doi.org/10.1145/1408664.1408670.**
2. **Peter Eckersley. « How Unique Is Your Web Browser? » In *International Conference on Privacy Enhancing Technologies (PETS)*, 1–18, 2010. https://doi.org/10.1007/978-3-642-14527-8_1.**
3. **J. Bonneau, C. Herley, P. C. v Oorschot, and F. Stajano. « The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes ». In *IEEE Symposium on Security and Privacy (S&P)*, 553-67, 2012. https://doi.org/10.1109/SP.2012.44.**
4. **Erik Flood and Joel Karlsson. « Browser Fingerprinting ». Master Thesis, *University of Gothenburg*, 2012. https://hdl.handle.net/20.500.12380/163728.**
5. **Joseph Bonneau. « The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords ». In *IEEE Symposium on Security and Privacy (S&P)*, 538-52, 2012. https://doi.org/10.1109/SP.2012.49.**

References II

6. Joseph Bonneau. « The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. » In *IEEE Symposium on Security and Privacy (S&P)*, 538–52, 2012. https://doi.org/10.1109/SP.2012.49.
7. David Fifield and Serge Egelman. « Fingerprinting Web Users Through Font Metrics ». In *Financial Cryptography and Data Security (FC)*, edited by Rainer Böhme and Tatsuaki Okamoto, 107-24, 2015. https://doi.org/10.1007/978-3-662-47854-7_7.
8. Amin Faiz Khademi, Mohammad Zulkernine, and Komminist Weldemariam. « An Empirical Evaluation of Web-Based Fingerprinting ». *IEEE Software* 32 nº 4, 2015. https://doi.org/10.1109/MS.2015.77.
9. C. Blakemore, J. Redol, and M. Correia. « Fingerprinting for Web Applications: From Devices to Related Groups ». In *IEEE Trustcom/BigDataSE/ISPA*, 144-51, 2016. https://doi.org/10.1109/TrustCom.2016.0057.

References III

10. Tom Goethem, Wout Scheepers, Davy Preuveneers, and Wouter Joosen. “Accelerometer-Based Device Fingerprinting for Multi-Factor Mobile Authentication.” In *International Symposium on Engineering Secure Software and Systems (ESSoS)*, 106–121, 2016. https://doi.org/10.1007/978-3-319-30806-7_7.
11. Pierre Laperdrix, Walter Rudametkin, and Benoit Baudry. « Beauty and the Beast: Diverting Modern Web Browsers to Build Unique Browser Fingerprints. » In *IEEE Symposium on Security and Privacy (S&P)*, 878–94, 2016. https://doi.org/10.1109/SP.2016.57.
12. Kurt Thomas, Frank Li, Ali Zand, Jacob Barrett, Juri Ranieri, Luca Invernizzi, Yarik Markov, et al. « Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials. » In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 1421–1434, 2017. https://doi.org/10.1145/3133956.3134067.
13. Furkan Alaca and P. C. van Oorschot. « Device Fingerprinting for Augmenting Web Authentication: Classification and Analysis of Methods ». In *Annual Conference on Computer Security Applications (ACSAC)*, 289–301, 2016. https://doi.org/10.1145/2991079.2991091.

References IV

14. **Ding Wang, Zijian Zhang, Ping Wang, Jeff Yan, and Xinyi Huang. « Targeted Online Password Guessing: An Underestimated Threat ». In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 1242–1254, 2016. https://doi.org/10.1145/2976749.2978339.**
15. **Alejandro Gómez-Boix, Pierre Laperdrix, and Benoit Baudry. « Hiding in the Crowd: An Analysis of the Effectiveness of Browser Fingerprinting at Large Scale. » In *The Web Conference (TheWebConf)*, 2018. https://doi.org/10.1145/3178876.3186097.**
16. **Chun Wang, Steve T.K. Jan, Hang Hu, Douglas Bossart, and Gang Wang. « The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services. » In *ACM Conference on Data and Application Security and Privacy (CODASPY)*, 196–203, 2018. https://doi.org/10.1145/3176258.3176332.**
17. **Kazuhisa Tanabe, Ryohei Hosoya, and Takamichi Saito. « Combining Features in Browser Fingerprinting ». In *Advances on Broadband and Wireless Computing, Communication and Applications (BWCCA)*, edited by Leonard Barolli, Fang-Yie Leu, Tomoya Enokido, and Hsing-Chung Chen, 671-81, 2018. https://doi.org/10.1007/978-3-030-02613-4_60.**

References V

18. Maximilian Golla, Theodor Schnitzler, and Markus Dürmuth. « "Will Any Password Do?" Exploring Rate-Limiting on the Web ». In *USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2018. https://wayworkshop.org/2018/papers/way2018-golla.pdf.
19. Gaston Pugliese, Christian Riess, Freya Gassmann, and Zinaida Benenson. « Long-Term Observation on Browser Fingerprinting: Users' Trackability and Perspective. » *Proceedings on Privacy Enhancing Technologies* 2020 no. 2, 2020. https://doi.org/10.2478/popets-2020-0041.
20. Nampoina Andriamilanto, Tristan Allard, and Gaëtan Le Guelvouit. « "Guess Who?" Large-Scale Data-Centric Study of the Adequacy of Browser Fingerprints for Web Authentication ». In *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, edited by Leonard Barolli, Aneta Poniszewska-Maranda, and Hyunhee Park, 161-72, 2021. https://doi.org/10.1007/978-3-030-50399-4_16.
21. Nampoina Andriamilanto, Tristan Allard, Gaëtan Le Guelvouit, and Alexandre Garel. « A Large-scale Empirical Analysis of Browser Fingerprints Properties for Web Authentication ». *arXiv:2006.09511 [cs]*, 2020. https://arxiv.org/abs/2006.09511.