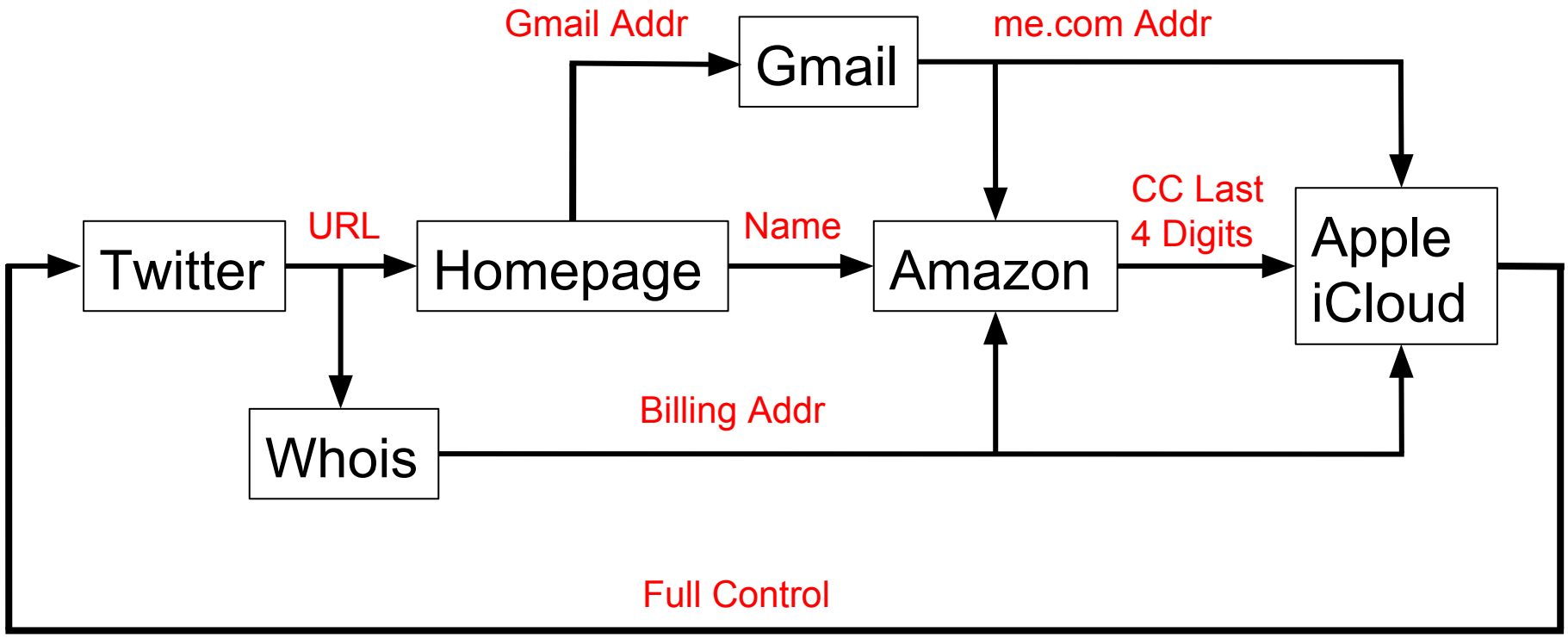
# Disinformation Techniques for Entity Resolution

Steven Whang[1,2], Hector Garcia-Molina[2]

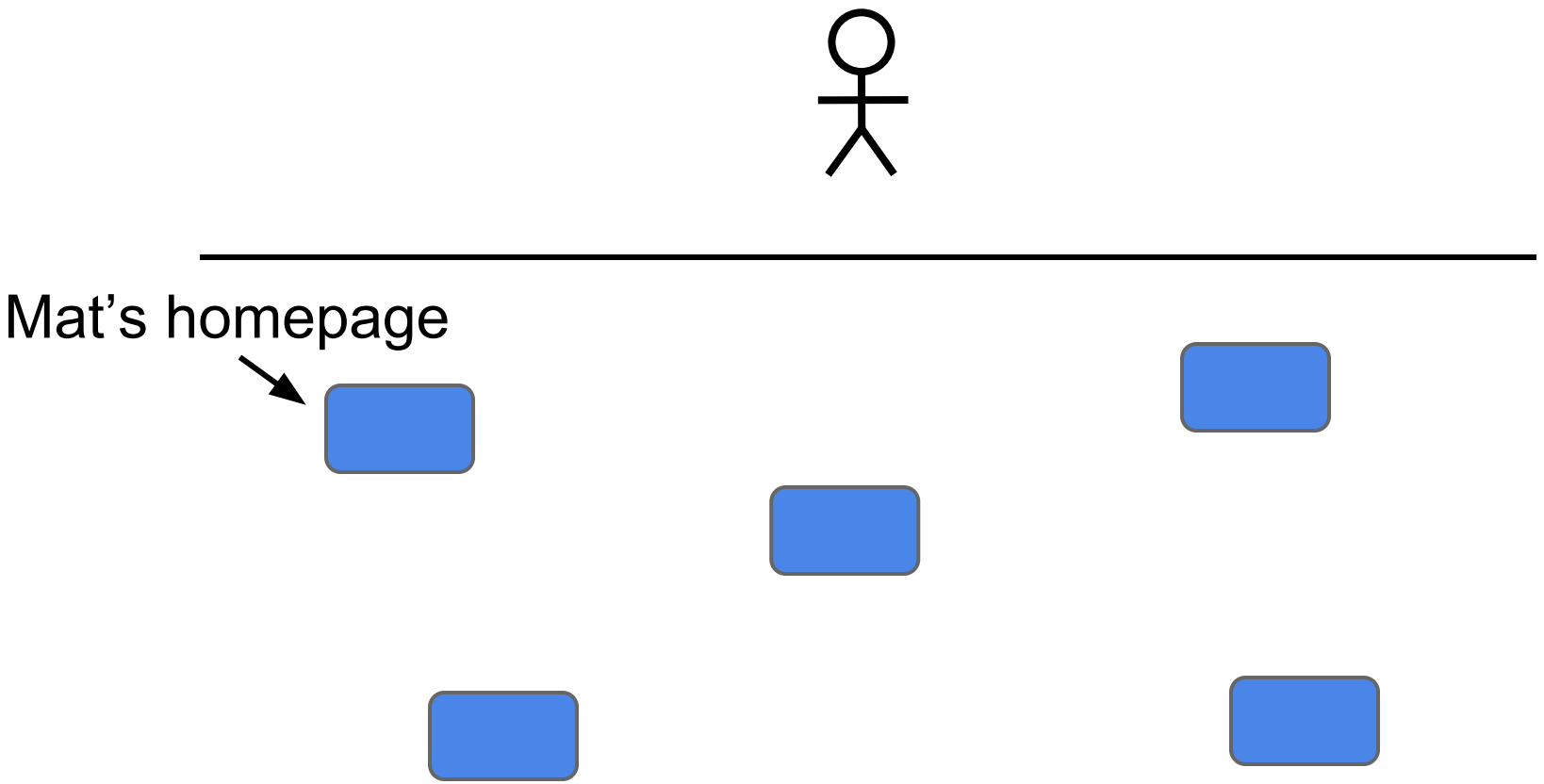
*Google Research[1], Stanford University[2]*

“How Apple and Amazon security flaws led to my epic hacking” *By Mat Honan - Wired.com*

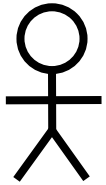
# Hacker Connecting the Dots

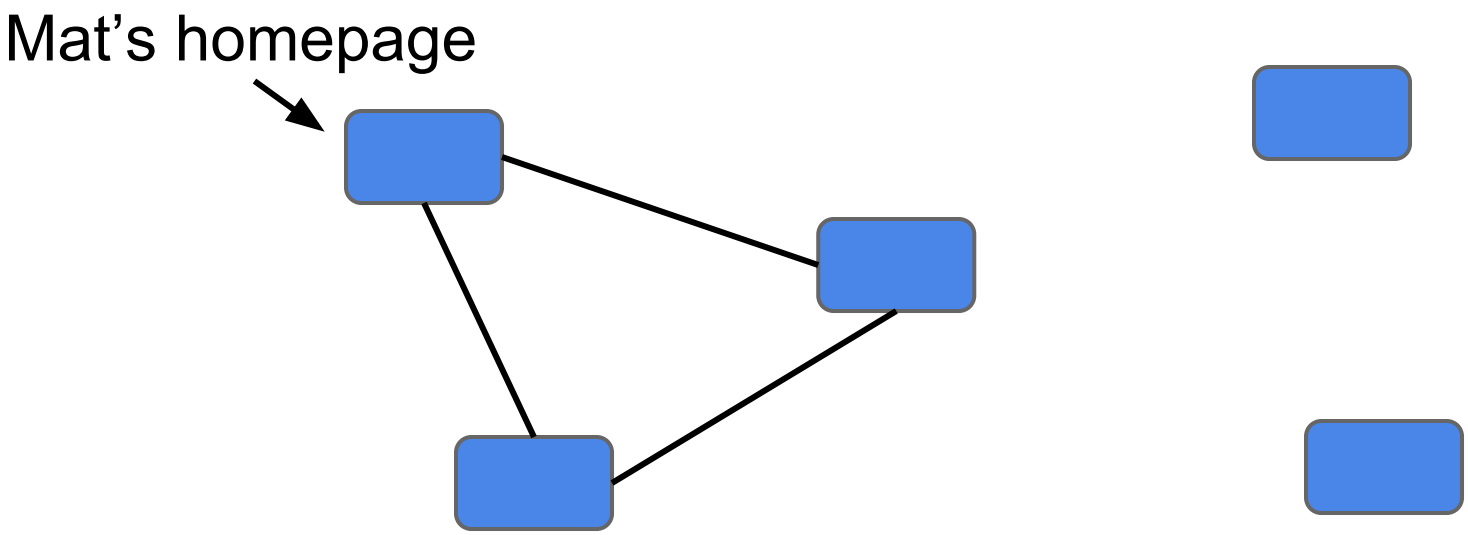


# Information Leakage



# Information Leakage





# Key Contributions

- Incorporate Entity Resolution

# Key Contributions

- Incorporate Entity Resolution
- Previous works assume that privacy is all or nothing

⇒ We assume privacy is within a continuum

# Key Contributions

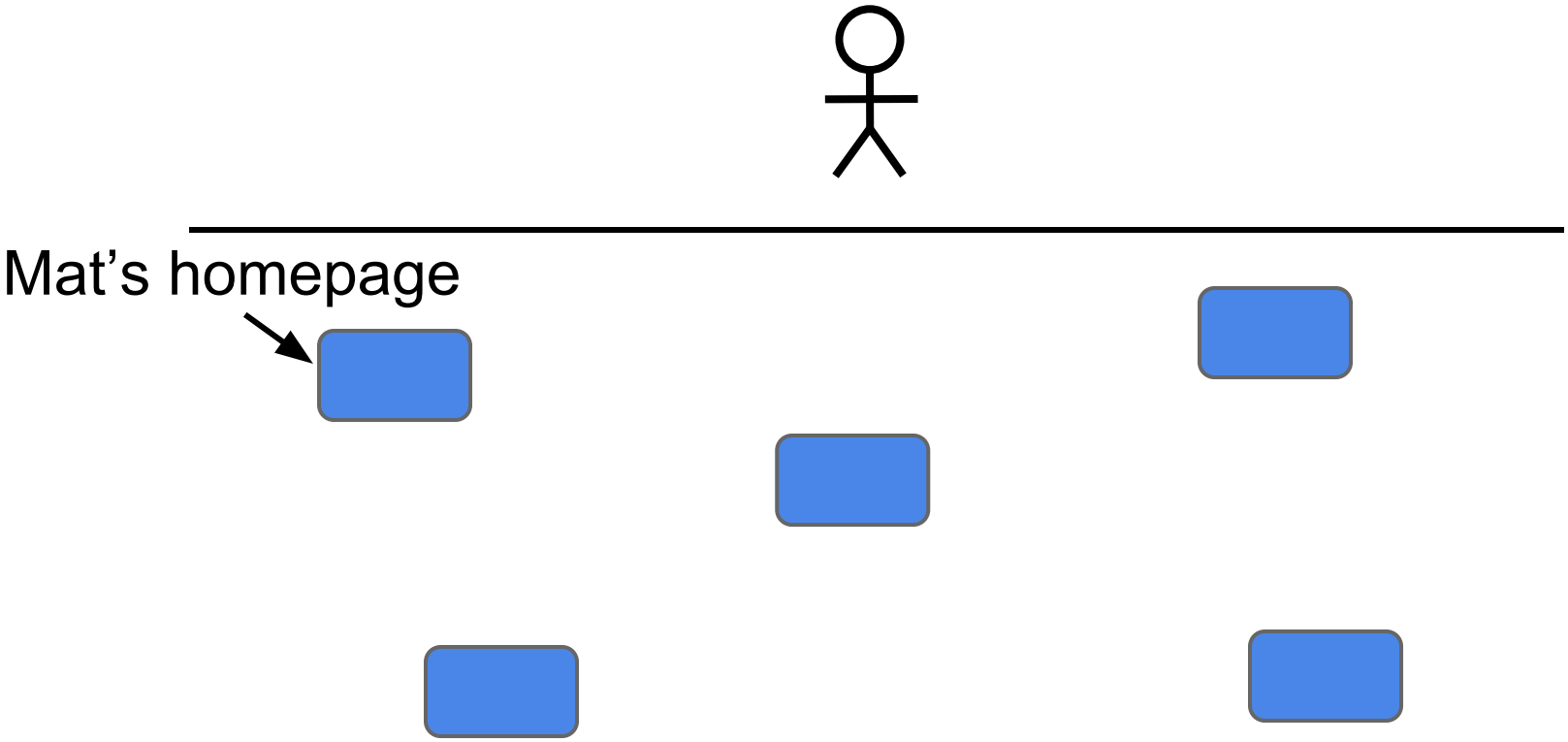
- Incorporate Entity Resolution
- Previous works assume that privacy is all or nothing

⇒ We assume privacy is within a continuum

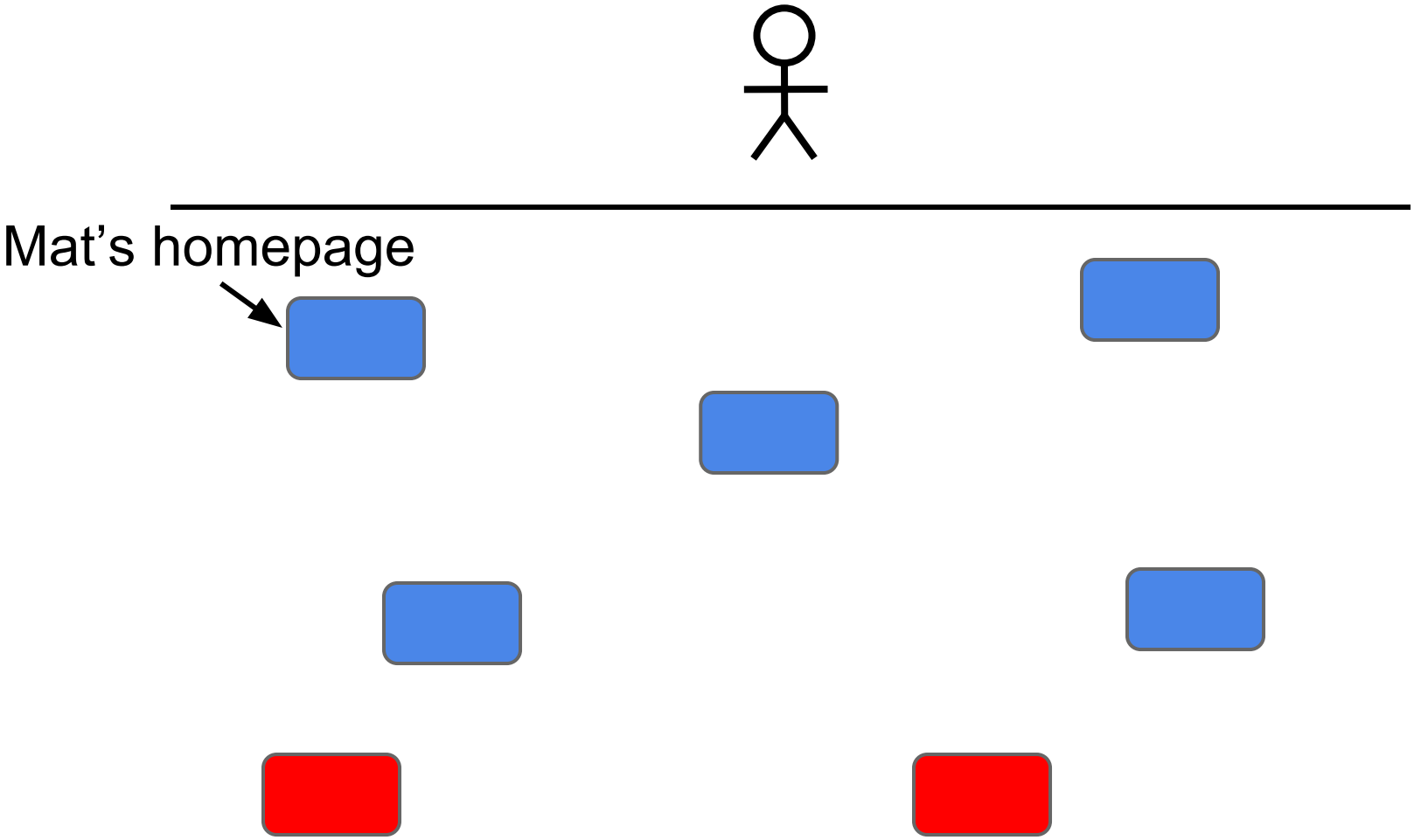

- Deleting information is very hard

⇒ We add *disinformation* to reduce leakage

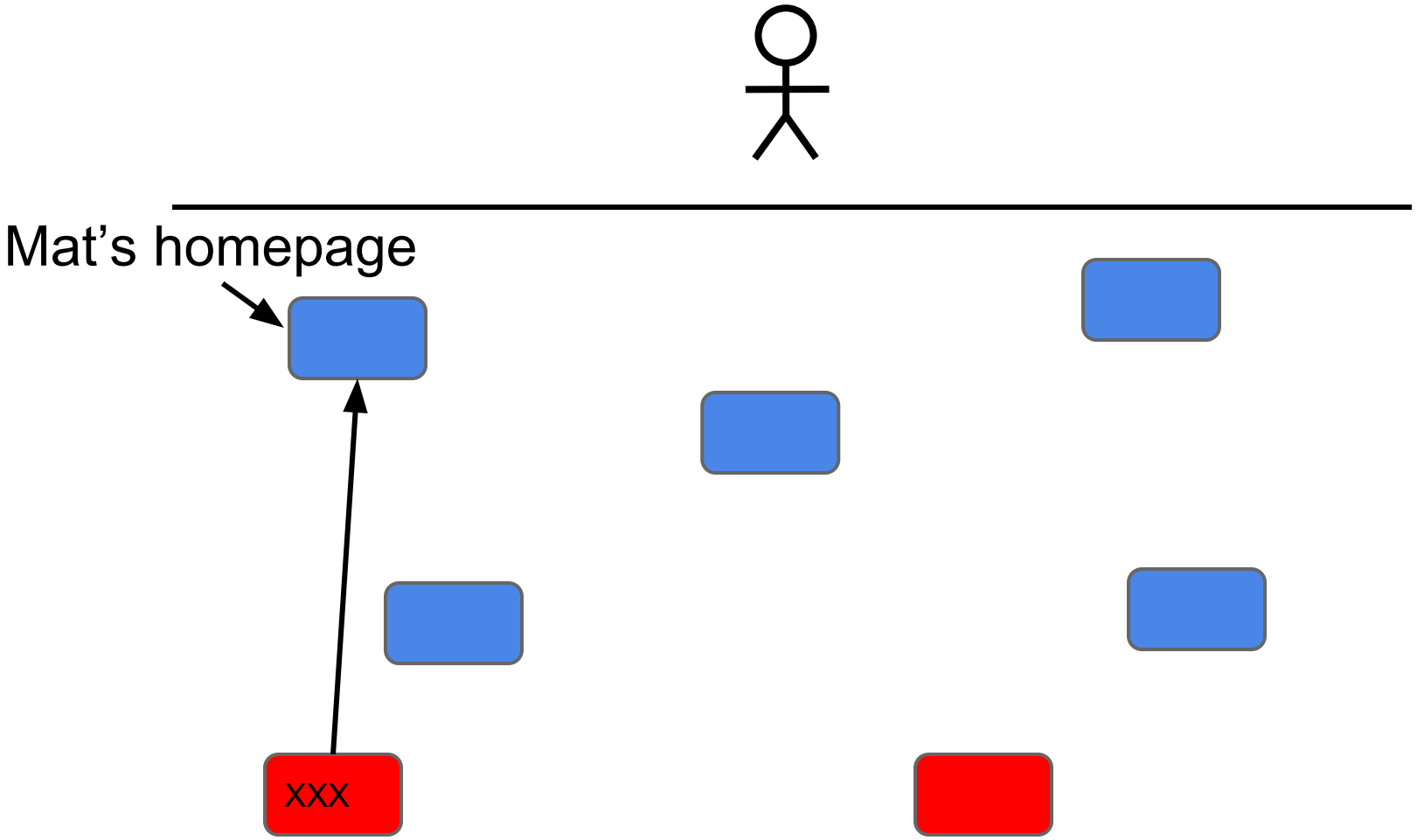
# Releasing Disinformation



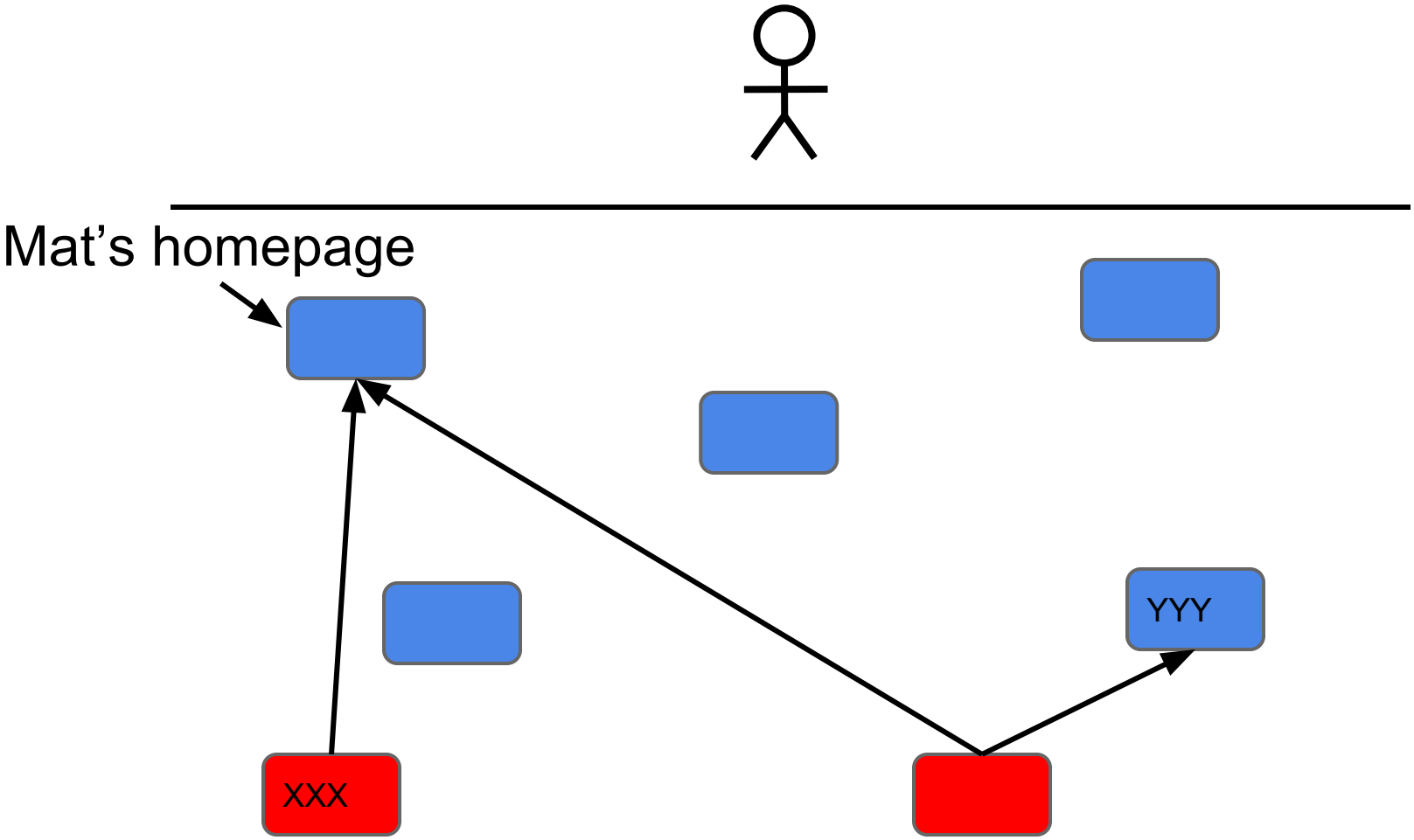
# Releasing Disinformation



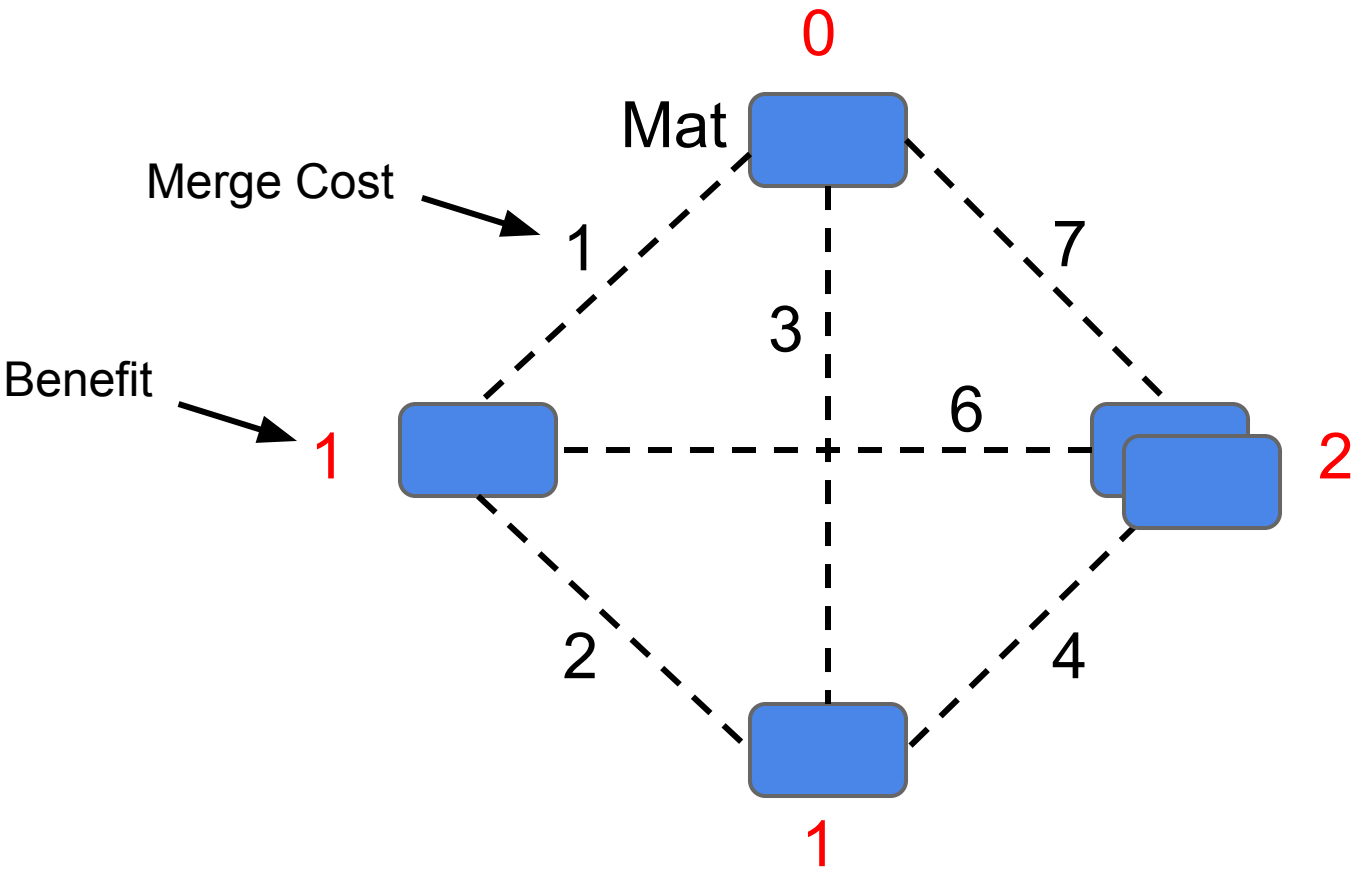
# Releasing Disinformation



# Releasing Disinformation



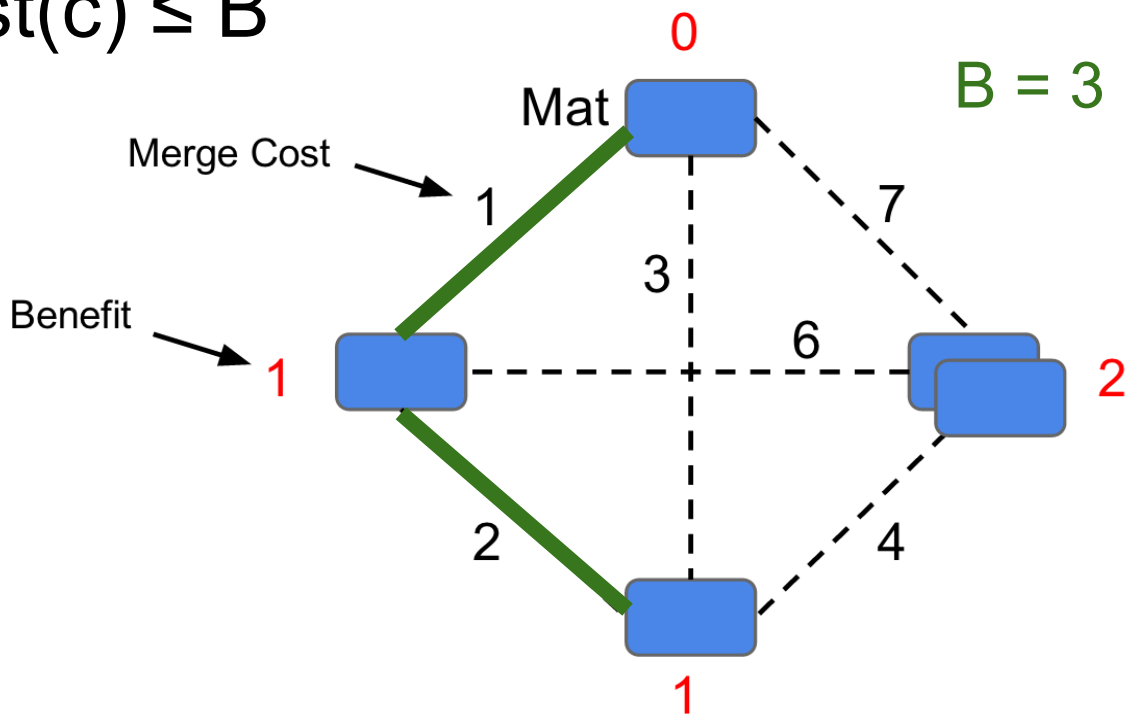
# Linkage Disinformation Model



# Disinformation Plan

- Maximize $\sum_{c \in Plan}$ Benefit(c)

s.t. $\sum_{c \in Plan}$ Cost(c) ≤ B



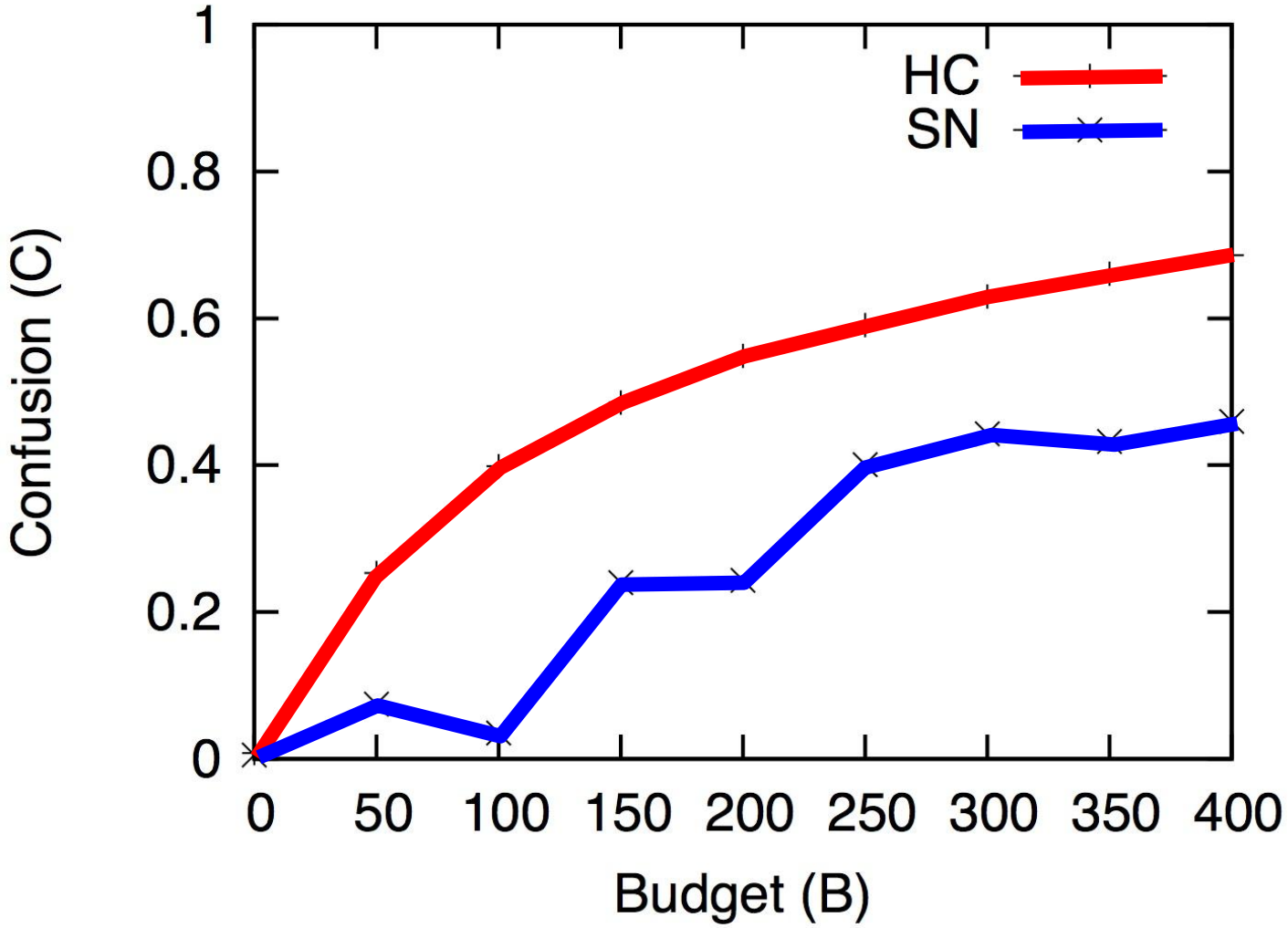
# Complexity

- Height of Plan > 1
  - Strongly NP-hard
  - Heuristics
- Height of Plan = 1
  - Weakly NP-hard
  - Exact Pseudo-Polynomial Algorithm: O(|V| B)
  - 2-Approximate Algorithm: O(|V| log(|V|))

# Creating Disinformation

- Euclidean Space
- Non-Euclidean Space

# Sample Result



# Conclusion

- Privacy model
  - Adversary “connects the dots” using Entity Resolution
  - Privacy is NOT all or nothing, but continuous
  - Hard to delete information
- Disinformation reduces information leakage
  - Proposed exact and approximate algorithms
  - Can also evaluate robustness of ER algorithms

# Thanks!