UNIVERSITY OF Southampton
School of Electronics
and Computer Science

On the anonymity in the Crowds protocol

V. Sassone

14/12/2009

Joint work with C. Palamidessi, S. Hamadou and E. ElSalamouny

Outline

- Introduction
- Crowds protocol
- Anonymity
  - Probable innocence
  - Vulnerability
- Anonymity in presence of extra knowledge
  - Probable innocence
  - Vulnerability
- Recent results
- Conclusion

Motivations

- Anonymity protocol: Obfuscates the link between its private input (anonymous actions) and its public output.
  - Attacker tries to infer the hidden info from his observation of the protocol.

Motivations

Extra knowledge

Motivations

Extra knowledge

- Real world: attackers usually gather additional information correlated to the anonymous agents before attacking the protocol.

Motivations

Extra knowledge

- Real world: attackers usually gather additional information correlated to the anonymous agents before attacking the protocol.

- Example: two agents voting by “yes” or “no” and the result of the vote is {yes, no}

Motivations

Extra knowledge

- Real world: attackers usually gather additional information correlated to the anonymous agents before attacking the protocol.

- Example: two agents voting by "yes" or "no" and the result of the vote is {yes, no}

  - Agents used different colours but the adversary does not know the correlation between the colors and the agents:

Motivations

Extra knowledge

- Real world: attackers usually gather additional information correlated to the anonymous agents before attacking the protocol.

- Example: two agents voting by "yes" or "no" and the result of the vote is {yes, no}

  - Agents used different colours but the adversary does not know the correlation between the colors and the agents:

{yes, no} ≡ {yes, no}

Motivations

Extra knowledge

- Real world: attackers usually gather additional information correlated to the anonymous agents before attacking the protocol.

- Example: two agents voting by "yes" or "no" and the result of the vote is {yes, no}

  - Agents used different colours but the adversary does not know the correlation between the colors and the agents:

    {yes, no} ≡ {yes, no}

  - The adversary knows the correlation: {yes, no} ≠ {yes, no}

Motivations

NFC-Enabled Mobile Phones

Security system developed in IBM Zurich Research Laboratory to enhance authentication in eBanking with NFC-enabled mobile phones [Ortiz-Yepes 09]

Motivations

Attacking NFC-EMF

First two digits from the first line

Last two digits from the last column

Motivations

Attacking NFC-EMF

From the movement of the finger…

First two digits from the first line

Last two digits from the last column

Motivations

Attacking NFC-EMF

From the movement of the finger…

First two digits from the first line

Last two digits from the last column

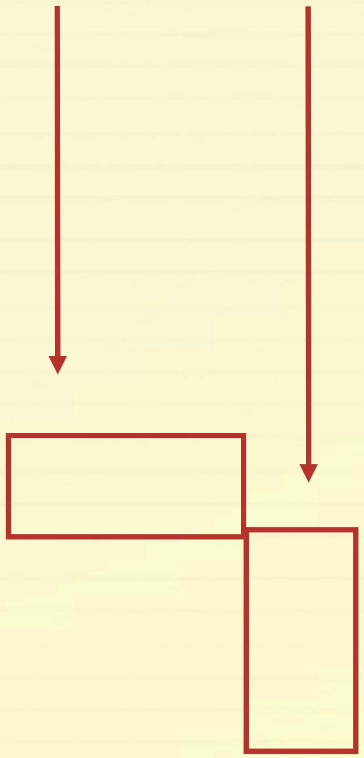
Motivations

Attacking NFC-EMF

[Social Networks:]() very easy to collect private and sensitive information about individuals.

Motivations

“Handless pick-pocket”



Motivations

"Handless pick-pocket"

User's mother born on 12/07/1969

Motivations

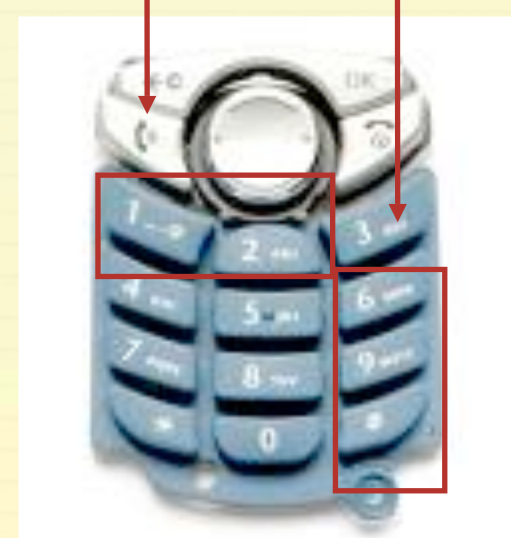
“Handless pick-pocket”

User’s mother born on 12/07/1969

Motivations

“Handless pick-pocket”

User’s mother born on 12/07/1969



Scan his pocket

Motivations

Extra knowledge

- **Our goal:** investigate the impact of the attacker's extra knowledge on the security of information hiding protocols.

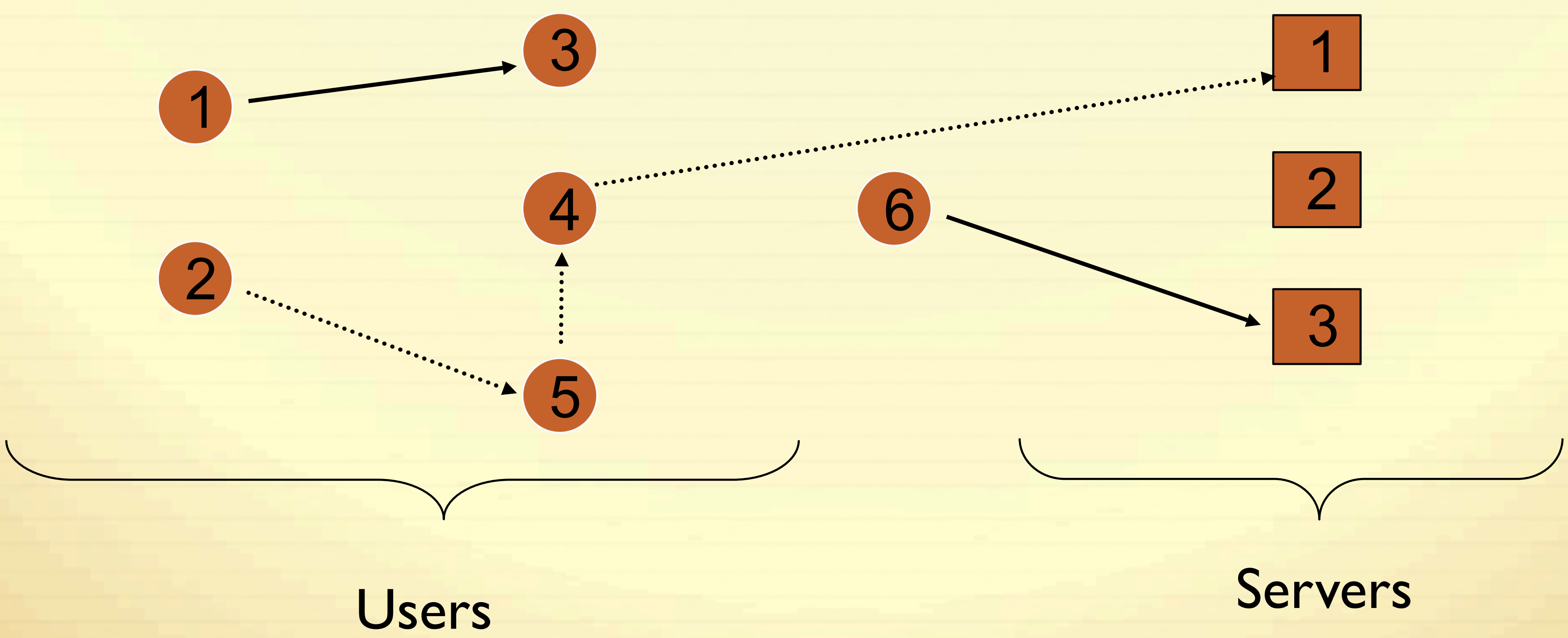
Outline

- Introduction
- Crowds protocol
- Anonymity
  - Probable innocence
  - Vulnerability
- Anonymity in presence of extra knowledge
  - Probable innocence
  - Vulnerability
- Recent results
- Conclusion

Crowds

The protocol

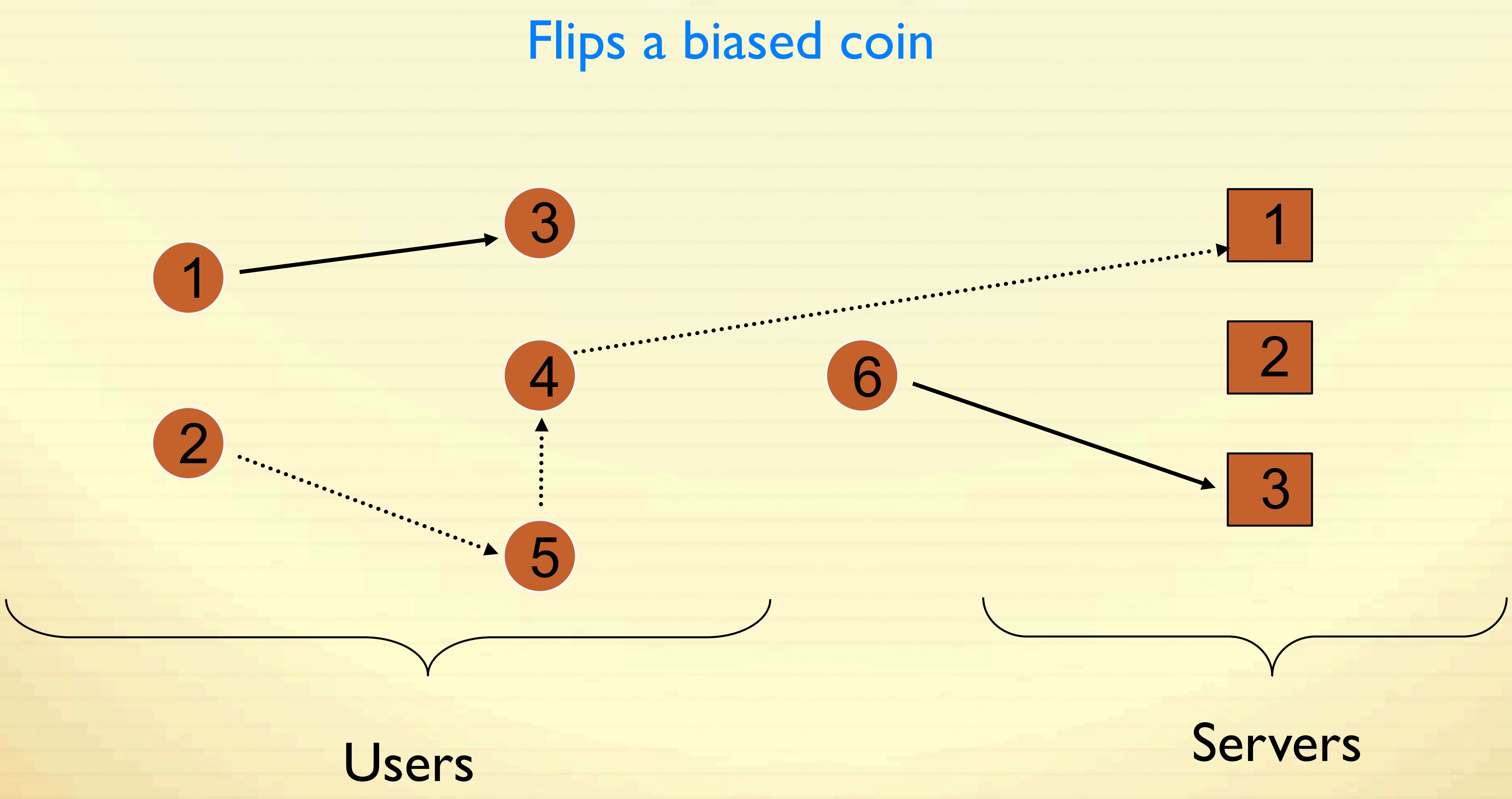
✧ Crowds [Reiter and Rubin 1998]: allows Internet users to perform anonymous web transactions.



Crowds

The protocol

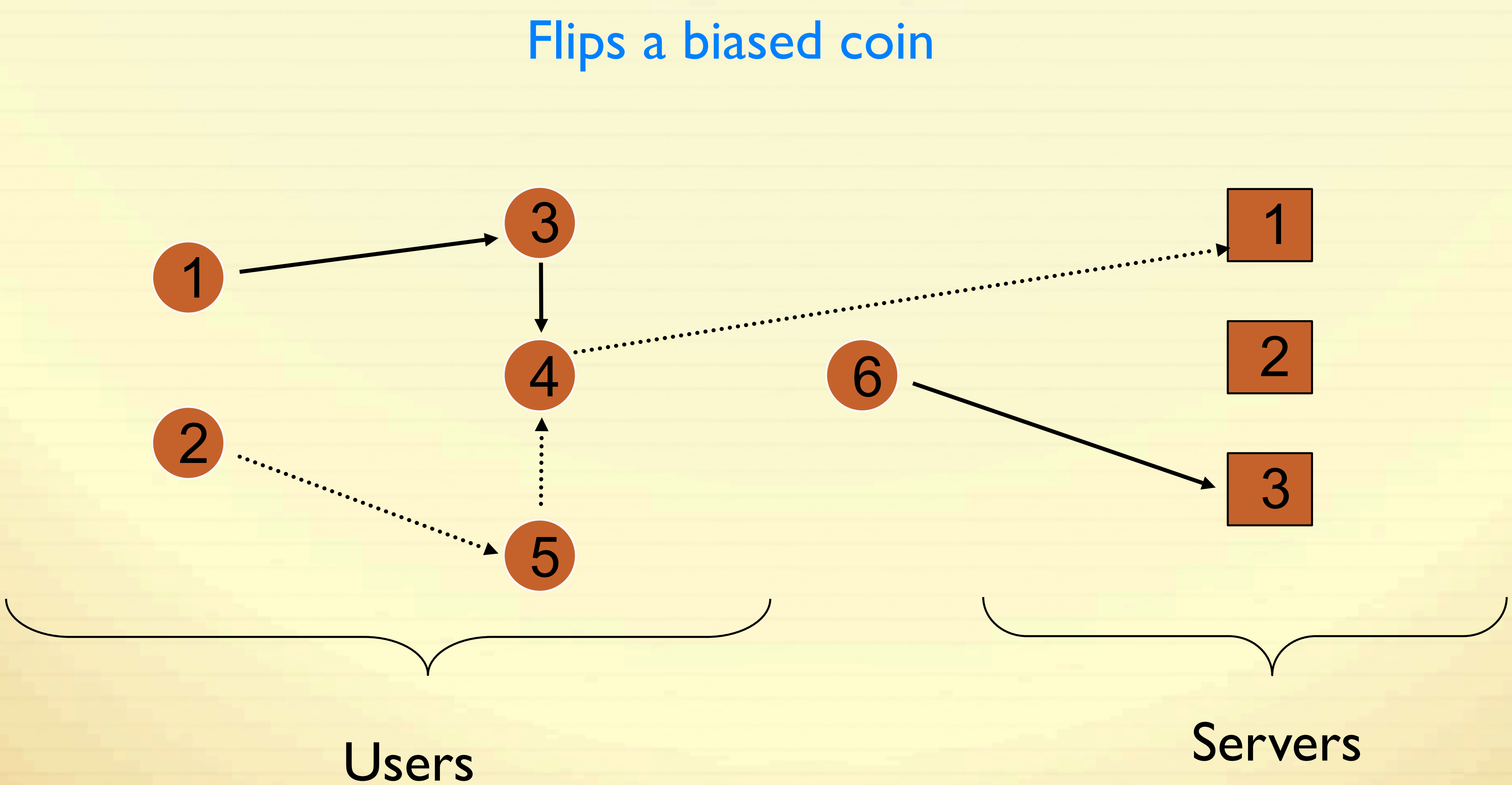
- Crowds [Reiter and Rubin 1998]: allows Internet users to perform anonymous web transactions.



Crowds

The protocol

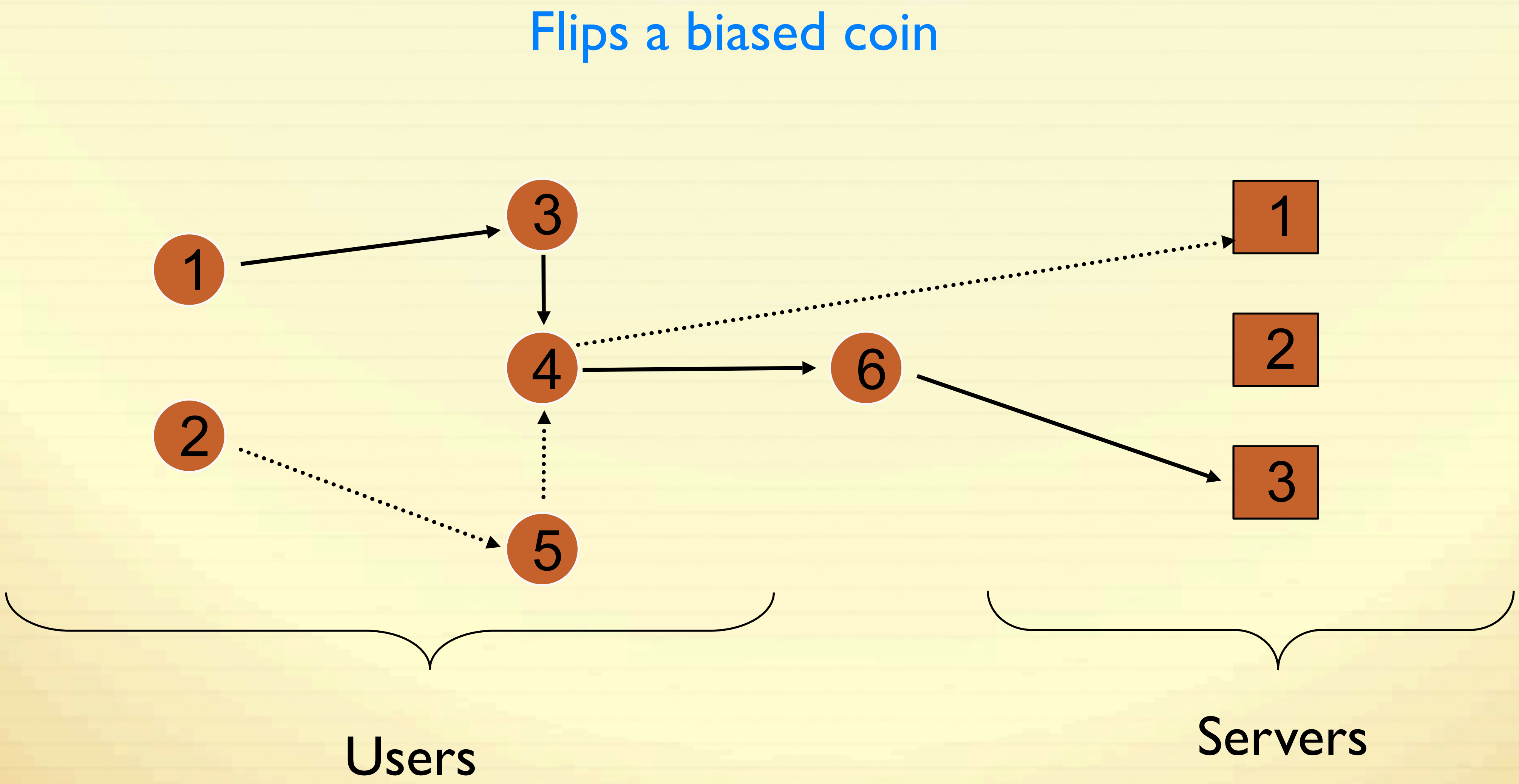
✧ Crowds [Reiter and Rubin 1998]: allows Internet users to perform anonymous web transactions.



Crowds

The protocol

- Crowds [Reiter and Rubin 1998]: allows Internet users to perform anonymous web transactions.



Probable Innocence

Informal definition

Absolute privacy | Beyond suspicion | Probable innocence | Possible innocence | Exposed | Provably exposed

> *"A sender is <u>probably innocent</u> if, from the attacker's point of view, the sender appears no more likely to be the originator than to not be the originator"*

Probable Innocence

Formal definition

- **Members:** a total of m members participating in the protocol
  - n honest members
  - $c=(m-n)$ corrupted members or collaborating attackers
- **Anonymous events:** a random variable A distributed over $\{a_1, a_2 \ldots, a_n\}$, where a_i indicates that the honest user i is the initiator of the message.
- **Observable events:** a random variable O distributed over $\{o_1, o_2 \ldots, o_n\}$, where o_i indicates that user i is honest and forwards the message to a corrupted user. In this case we say that user i is detected.

Probable Innocence

Formal definition

Definition [Reiter and Ruben, 98]: a protocol satisfies probable innocence if

$$\forall i \; p(o_i \mid a_i) \leq 1/2$$

$$\forall i \; p(a_i \mid o_i) \leq 1/2$$

Probable Innocence

Formal definition

Definition [Reiter and Ruben, 98]: a protocol satisfies probable innocence if

$$\forall i \; p(o_i \mid a_i) \leq 1/2$$

Definition [Halpern and O'Neill, 05]

$$\forall i \; p(a_i \mid o_i) \leq 1/2$$

Probable Innocence

Formal definition

Proposition: if the a priori distribution is uniform then

$$\forall i \; p(o_i \mid a_i) = p(a_i \mid o_i)$$

$$p(o_j \mid a_i)\, p(a_i) = p(a_i \mid o_j) p(o_j)$$

Probable Innocence

Formal definition

Proposition: if the a priori distribution is uniform then

$$\forall i \; p(o_i \mid a_i) = p(a_i \mid o_i)$$

Proof: by Bayes theorem we have

$$p(o_j \mid a_i)\, p(a_i) = p(a_i \mid o_j) p(o_j)$$

If A is uniformly distributed then (in Crowds) O is uniformly distributed too.
Hence $p(a_i) = p(o_j) = 1/n$

Probable Innocence

extended

Definition: a protocol satisfies α-probable innocence ($0 \leq \alpha \leq 1$) if

$$\forall i \; p(a_i \mid o_i) \leq \alpha$$

Vulnerability

[Smith 09]

[In Crowds]

$$\forall\, i \neq j\;\; p(a_i \mid o_i) > p(a_j \mid o_i)$$

$$V(A) = \max_i p(a_i)$$

$$V(A \mid O) = \Sigma_j\, p(o_j) \max_i(p(a_i \mid o_j))$$

Vulnerability

[Smith 09]

[In Crowds]

$$\forall\, i \neq j \;\; p(a_i \mid o_i) > p(a_j \mid o_i)$$

The a priori vulnerability of a random variable A is

$$V(A) = \max_i p(a_i)$$

$$V(A \mid O) = \Sigma_j\, p(o_j) \max_i(p(a_i \mid o_j))$$

Vulnerability

[Smith 09]

[In Crowds]

$$\forall\, i \neq j\;\; p(a_i \mid o_i) > p(a_j \mid o_i)$$

The a priori vulnerability of a random variable A is

$$V(A) = \max_i p(a_i)$$

The a posteriori vulnerability of a random variable A is

$$V(A \mid O) = \Sigma_j\, p(o_j)\, \max_i(p(a_i \mid o_j))$$

Vulnerability

Definition: a protocol satisfies α-vulnerability if

$$V(A \mid O) \leq \alpha$$

Vulnerability

Definition: a protocol satisfies α-vulnerability if

$$V(A \mid O) \leq \alpha$$

Proposition:

1. α-probable innocence implies α-vulnerability.
2. If the a priori distribution is uniform then the two notions coincide.

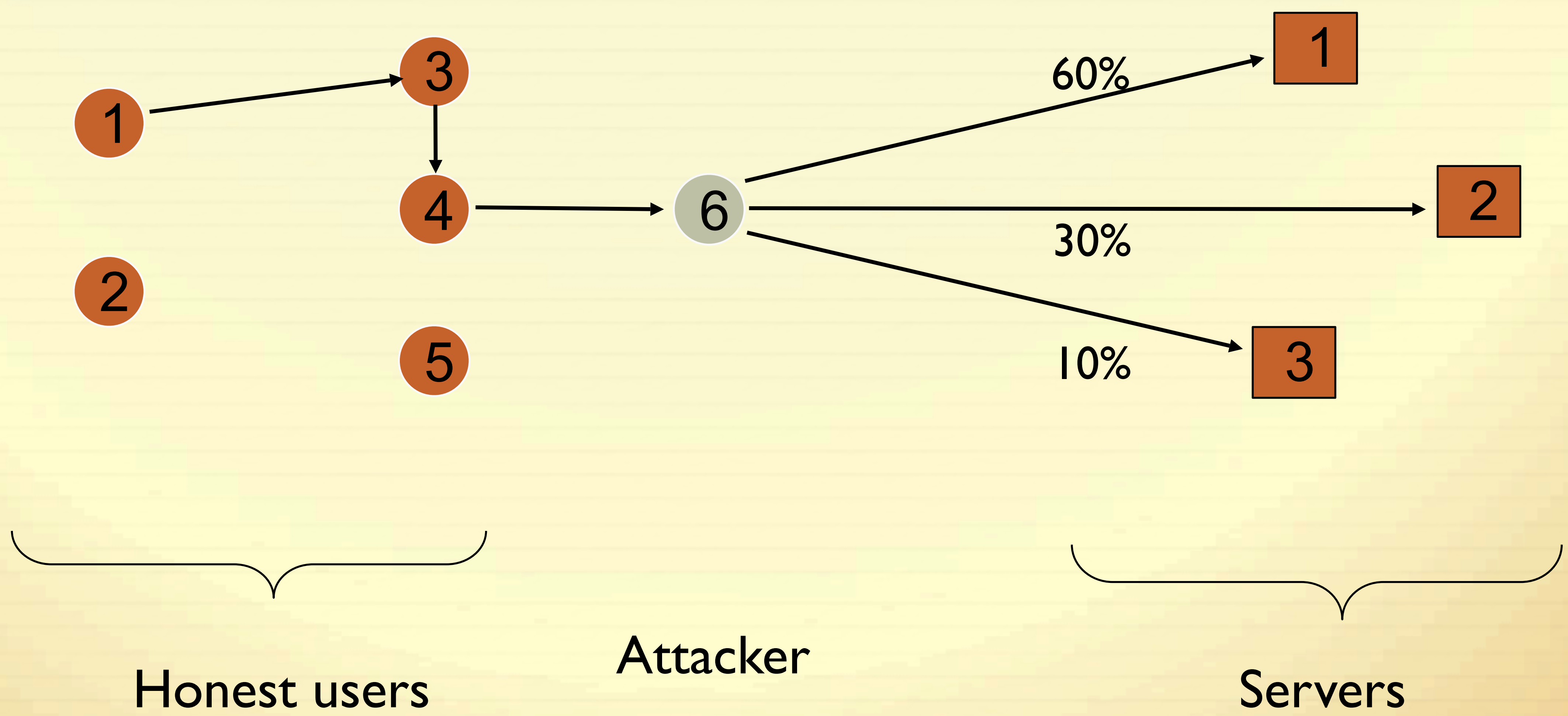
Outline

- Introduction
- Crowds protocol
- Anonymity
  - Probable innocence
  - Vulnerability
- Anonymity in presence of extra knowledge
  - Probable innocence
  - Vulnerability
- Recent results
- Conclusion

Extra knowledge

(in Crowds)

- Fixed paths: allows attackers to identify the users' preference level of the servers.



Extra knowledge

Probable innocence

$$\forall i,k \; p(a_i \mid o_i, s_k) \leq \alpha$$

Extra knowledge

Probable innocence

- Modeling the extra knowledge
  - Extra observables: a random variable S distributed over the set $\{s_1, s_2, \ldots, s_r\}$.
  - Correlation between S and A: the conditional probabilities matrix $p(s_k \mid a_i)$.

$$\forall i,k \; p(a_i \mid o_i, s_k) \leq \alpha$$

Extra knowledge

Probable innocence

- Modeling the extra knowledge
  - Extra observables: a random variable S distributed over the set $\{s_1, s_2, \ldots, s_r\}$.
  - Correlation between S and A: the conditional probabilities matrix $p(s_k \mid a_i)$.

- Definition [Fist attempt]: a protocol satisfies α–probable innocence in presence of extra knowledge if

$$\forall i,k \; p(a_i \mid o_i, s_k) \leq \alpha$$

Extra knowledge

Probable innocence

- **Example 1:** an instance of Crowds with 6 members and 2 servers
  - 5 honest members {1,2,3,4,5}
  - One attacker {6}
  - Probability of forwarding (of the biased coin) $p_f = 3/4$
  - Members {1,2} prefer the first server:

    $\forall\, i \in \{1,2\}\ p(s_1 \mid a_i) = 3/4$
  - Members {3,4,5} prefer the second server:

    $\forall\, i \in \{3,4,5\}\ p(s_2 \mid a_i) = 3/4$

Extra knowledge

Probable innocence

- Extra knowledge does not alter the relevance of the detection

$p(a \mid o, s)$	o_1, s_1	o_2, s_1	o_3, s_1	o_4, s_1	o_5, s_1	o_1, s_2	o_2, s_2	o_3, s_2	o_4, s_2	o_5, s_2
a_1	$\frac{2}{3}$	$\frac{1}{6}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{2}{7}$	$\frac{1}{14}$	$\frac{1}{20}$	$\frac{1}{20}$	$\frac{1}{20}$
a_2	$\frac{1}{6}$	$\frac{2}{3}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{14}$	$\frac{2}{7}$	$\frac{1}{20}$	$\frac{1}{20}$	$\frac{1}{20}$
a_3	$\frac{1}{18}$	$\frac{1}{18}$	$\frac{1}{3}$	$\frac{1}{12}$	$\frac{1}{12}$	$\frac{3}{14}$	$\frac{3}{14}$	$\frac{3}{5}$	$\frac{3}{20}$	$\frac{3}{20}$
a_4	$\frac{1}{18}$	$\frac{1}{18}$	$\frac{1}{12}$	$\frac{1}{3}$	$\frac{1}{12}$	$\frac{3}{14}$	$\frac{3}{14}$	$\frac{3}{20}$	$\frac{3}{5}$	$\frac{3}{20}$
a_5	$\frac{1}{18}$	$\frac{1}{18}$	$\frac{1}{12}$	$\frac{1}{12}$	$\frac{1}{3}$	$\frac{3}{14}$	$\frac{3}{14}$	$\frac{3}{20}$	$\frac{3}{20}$	$\frac{3}{5}$

Extra knowledge

Probable innocence

- Extra knowledge does not alter the relevance of the detection

$p(a \mid o, s)$	o_1, s_1	o_2, s_1	o_3, s_1	o_4, s_1	o_5, s_1	o_1, s_2	o_2, s_2	o_3, s_2	o_4, s_2	o_5, s_2
a_1	$\frac{2}{3}$	$\frac{1}{6}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{2}{7}$	$\frac{1}{14}$	$\frac{1}{20}$	$\frac{1}{20}$	$\frac{1}{20}$
a_2	$\frac{1}{6}$	$\frac{2}{3}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{14}$	$\frac{2}{7}$	$\frac{1}{20}$	$\frac{1}{20}$	$\frac{1}{20}$
a_3	$\frac{1}{18}$	$\frac{1}{18}$	$\frac{1}{3}$	$\frac{1}{12}$	$\frac{1}{12}$	$\frac{3}{14}$	$\frac{3}{14}$	$\frac{3}{5}$	$\frac{3}{20}$	$\frac{3}{20}$
a_4	$\frac{1}{18}$	$\frac{1}{18}$	$\frac{1}{12}$	$\frac{1}{3}$	$\frac{1}{12}$	$\frac{3}{14}$	$\frac{3}{14}$	$\frac{3}{20}$	$\frac{3}{5}$	$\frac{3}{20}$
a_5	$\frac{1}{18}$	$\frac{1}{18}$	$\frac{1}{12}$	$\frac{1}{12}$	$\frac{1}{3}$	$\frac{3}{14}$	$\frac{3}{14}$	$\frac{3}{20}$	$\frac{3}{20}$	$\frac{3}{5}$

Extra knowledge

Probable innocence

- Extra knowledge does not alter the relevance of the detection

$p(a \mid o, s)$	o_1, s_1	o_2, s_1	o_3, s_1	o_4, s_1	o_5, s_1	o_1, s_2	o_2, s_2	o_3, s_2	o_4, s_2	o_5, s_2
a_1	$\frac{2}{3}$	$\frac{1}{6}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{2}{7}$	$\frac{1}{14}$	$\frac{1}{20}$	$\frac{1}{20}$	$\frac{1}{20}$
a_2	$\frac{1}{6}$	$\frac{2}{3}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{14}$	$\frac{2}{7}$	$\frac{1}{20}$	$\frac{1}{20}$	$\frac{1}{20}$
a_3	$\frac{1}{18}$	$\frac{1}{18}$	$\frac{1}{3}$	$\frac{1}{12}$	$\frac{1}{12}$	$\frac{3}{14}$	$\frac{3}{14}$	$\frac{3}{5}$	$\frac{3}{20}$	$\frac{3}{20}$
a_4	$\frac{1}{18}$	$\frac{1}{18}$	$\frac{1}{12}$	$\frac{1}{3}$	$\frac{1}{12}$	$\frac{3}{14}$	$\frac{3}{14}$	$\frac{3}{20}$	$\frac{3}{5}$	$\frac{3}{20}$
a_5	$\frac{1}{18}$	$\frac{1}{18}$	$\frac{1}{12}$	$\frac{1}{12}$	$\frac{1}{3}$	$\frac{3}{14}$	$\frac{3}{14}$	$\frac{3}{20}$	$\frac{3}{20}$	$\frac{3}{5}$

Extra knowledge

Probable innocence

Extra knowledge

Probable innocence

- **<u>Example 2:</u>** an instance of Crowds with 6 members and 2 servers
  - 5 honest members {1,2,3,4,5}

Extra knowledge

Probable innocence

- **Example 2:** an instance of Crowds with 6 members and 2 servers
  - 5 honest members {1,2,3,4,5}
  - One attacker {6}

Extra knowledge

Probable innocence

- **Example 2:** an instance of Crowds with 6 members and 2 servers
  - 5 honest members {1,2,3,4,5}
  - One attacker {6}
  - Probability of forwarding (of the biased coin) $p_f = 3/4$

Extra knowledge

Probable innocence

- **Example 2:** an instance of Crowds with 6 members and 2 servers
  - 5 honest members {1,2,3,4,5}
  - One attacker {6}
  - Probability of forwarding (of the biased coin) $p_f = 3/4$
  - Members {1,2} prefer the first server:

Extra knowledge

Probable innocence

- **Example 2:** an instance of Crowds with 6 members and 2 servers
  - 5 honest members {1,2,3,4,5}
  - One attacker {6}
  - Probability of forwarding (of the biased coin) $p_f = 3/4$
  - Members {1,2} prefer the first server:

$$\forall\, i \in \{1,2\}\; p(s_1 \mid a_i) = 9/10$$

Extra knowledge

Probable innocence

- **Example 2:** an instance of Crowds with 6 members and 2 servers
  - 5 honest members {1,2,3,4,5}
  - One attacker {6}
  - Probability of forwarding (of the biased coin) $p_f = 3/4$
  - Members {1,2} prefer the first server:

    $\forall\ i \in \{1,2\}\ p(s_1 \mid a_i) = 9/10$
  - Members {3,4,5} prefer the second server:

Extra knowledge

Probable innocence

- **Example 2:** an instance of Crowds with 6 members and 2 servers
  - 5 honest members {1,2,3,4,5}
  - One attacker {6}
  - Probability of forwarding (of the biased coin) $p_f = 3/4$
  - Members {1,2} prefer the first server:

    $\forall\, i \in \{1,2\}\; p(s_1 \mid a_i) = 9/10$
  - Members {3,4,5} prefer the second server:

    $\forall\, i \in \{3,4,5\}\; p(s_2 \mid a_i) = 9/10$

Extra knowledge

Probable innocence

- Extra knowledge alters the relevance of the detection

$p(a \mid o, s)$	o_1, s_1	o_2, s_1	o_3, s_1	o_4, s_1	o_5, s_1	o_1, s_2	o_2, s_2	o_3, s_2	o_4, s_2	o_5, s_2
a_1	$\frac{3}{4}$	$\frac{3}{16}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{1}{8}$	$\frac{1}{32}$	$\frac{1}{56}$	$\frac{1}{56}$	$\frac{1}{56}$
a_2	$\frac{3}{16}$	$\frac{3}{4}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{1}{32}$	$\frac{1}{8}$	$\frac{1}{56}$	$\frac{1}{56}$	$\frac{1}{56}$
a_3	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{6}$	$\frac{1}{24}$	$\frac{1}{24}$	$\frac{9}{32}$	$\frac{9}{32}$	$\frac{9}{14}$	$\frac{9}{56}$	$\frac{9}{56}$
a_4	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{24}$	$\frac{1}{6}$	$\frac{1}{24}$	$\frac{9}{32}$	$\frac{9}{32}$	$\frac{9}{56}$	$\frac{9}{14}$	$\frac{9}{56}$
a_5	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{24}$	$\frac{1}{24}$	$\frac{1}{6}$	$\frac{9}{32}$	$\frac{9}{32}$	$\frac{9}{56}$	$\frac{9}{56}$	$\frac{9}{14}$

Extra knowledge

Probable innocence

- Extra knowledge alters the relevance of the detection

$p(a \mid o, s)$	o_1, s_1	o_2, s_1	o_3, s_1	o_4, s_1	o_5, s_1	o_1, s_2	o_2, s_2	o_3, s_2	o_4, s_2	o_5, s_2
a_1	$\frac{3}{4}$	$\frac{3}{16}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{1}{8}$	$\frac{1}{32}$	$\frac{1}{56}$	$\frac{1}{56}$	$\frac{1}{56}$
a_2	$\frac{3}{16}$	$\frac{3}{4}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{1}{32}$	$\frac{1}{8}$	$\frac{1}{56}$	$\frac{1}{56}$	$\frac{1}{56}$
a_3	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{6}$	$\frac{1}{24}$	$\frac{1}{24}$	$\frac{9}{32}$	$\frac{9}{32}$	$\frac{9}{14}$	$\frac{9}{56}$	$\frac{9}{56}$
a_4	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{24}$	$\frac{1}{6}$	$\frac{1}{24}$	$\frac{9}{32}$	$\frac{9}{32}$	$\frac{9}{56}$	$\frac{9}{14}$	$\frac{9}{56}$
a_5	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{24}$	$\frac{1}{24}$	$\frac{1}{6}$	$\frac{9}{32}$	$\frac{9}{32}$	$\frac{9}{56}$	$\frac{9}{56}$	$\frac{9}{14}$

Extra knowledge

Probable innocence

- Extra knowledge alters the relevance of the detection

$p(a \mid o, s)$	o_1, s_1	o_2, s_1	o_3, s_1	o_4, s_1	o_5, s_1	o_1, s_2	o_2, s_2	o_3, s_2	o_4, s_2	o_5, s_2
a_1	$\frac{3}{4}$	$\frac{3}{16}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{1}{8}$	$\frac{1}{32}$	$\frac{1}{56}$	$\frac{1}{56}$	$\frac{1}{56}$
a_2	$\frac{3}{16}$	$\frac{3}{4}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{1}{32}$	$\frac{1}{8}$	$\frac{1}{56}$	$\frac{1}{56}$	$\frac{1}{56}$
a_3	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{6}$	$\frac{1}{24}$	$\frac{1}{24}$	$\frac{9}{32}$	$\frac{9}{32}$	$\frac{9}{14}$	$\frac{9}{56}$	$\frac{9}{56}$
a_4	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{24}$	$\frac{1}{6}$	$\frac{1}{24}$	$\frac{9}{32}$	$\frac{9}{32}$	$\frac{9}{56}$	$\frac{9}{14}$	$\frac{9}{56}$
a_5	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{24}$	$\frac{1}{24}$	$\frac{1}{6}$	$\frac{9}{32}$	$\frac{9}{32}$	$\frac{9}{56}$	$\frac{9}{56}$	$\frac{9}{14}$

Extra knowledge

Probable innocence

✧ Extra knowledge alters the relevance of the detection

$p(a \mid o, s)$	o_1, s_1	o_2, s_1	o_3, s_1	o_4, s_1	o_5, s_1	o_1, s_2	o_2, s_2	o_3, s_2	o_4, s_2	o_5, s_2
a_1	$\frac{3}{4}$	$\frac{3}{16}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{1}{8}$	$\frac{1}{32}$	$\frac{1}{56}$	$\frac{1}{56}$	$\frac{1}{56}$
a_2	$\frac{3}{16}$	$\frac{3}{4}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{1}{32}$	$\frac{1}{8}$	$\frac{1}{56}$	$\frac{1}{56}$	$\frac{1}{56}$
a_3	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{6}$	$\frac{1}{24}$	$\frac{1}{24}$	$\frac{9}{32}$	$\frac{9}{32}$	$\frac{9}{14}$	$\frac{9}{56}$	$\frac{9}{56}$
a_4	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{24}$	$\frac{1}{6}$	$\frac{1}{24}$	$\frac{9}{32}$	$\frac{9}{32}$	$\frac{9}{56}$	$\frac{9}{14}$	$\frac{9}{56}$
a_5	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{24}$	$\frac{1}{24}$	$\frac{1}{6}$	$\frac{9}{32}$	$\frac{9}{32}$	$\frac{9}{56}$	$\frac{9}{56}$	$\frac{9}{14}$

Extra knowledge

Probable innocence

- Extra knowledge alters the relevance of the detection

$p(a \mid o, s)$	o_1, s_1	o_2, s_1	o_3, s_1	o_4, s_1	o_5, s_1	o_1, s_2	o_2, s_2	o_3, s_2	o_4, s_2	o_5, s_2
a_1	$\frac{3}{4}$	$\frac{3}{16}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{1}{8}$	$\frac{1}{32}$	$\frac{1}{56}$	$\frac{1}{56}$	$\frac{1}{56}$
a_2	$\frac{3}{16}$	$\frac{3}{4}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{1}{32}$	$\frac{1}{8}$	$\frac{1}{56}$	$\frac{1}{56}$	$\frac{1}{56}$
a_3	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{6}$	$\frac{1}{24}$	$\frac{1}{24}$	$\frac{9}{32}$	$\frac{9}{32}$	$\frac{9}{14}$	$\frac{9}{56}$	$\frac{9}{56}$
a_4	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{24}$	$\frac{1}{6}$	$\frac{1}{24}$	$\frac{9}{32}$	$\frac{9}{32}$	$\frac{9}{56}$	$\frac{9}{14}$	$\frac{9}{56}$
a_5	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{24}$	$\frac{1}{24}$	$\frac{1}{6}$	$\frac{9}{32}$	$\frac{9}{32}$	$\frac{9}{56}$	$\frac{9}{56}$	$\frac{9}{14}$

Extra knowledge

Probable innocence

- Extra knowledge alters the relevance of the detection

$p(a \mid o, s)$	o_1, s_1	o_2, s_1	o_3, s_1	o_4, s_1	o_5, s_1	o_1, s_2	o_2, s_2	o_3, s_2	o_4, s_2	o_5, s_2
a_1	$\frac{3}{4}$	$\frac{3}{16}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{1}{8}$	$\frac{1}{32}$	$\frac{1}{56}$	$\frac{1}{56}$	$\frac{1}{56}$
a_2	$\frac{3}{16}$	$\frac{3}{4}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{1}{32}$	$\frac{1}{8}$	$\frac{1}{56}$	$\frac{1}{56}$	$\frac{1}{56}$
a_3	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{6}$	$\frac{1}{24}$	$\frac{1}{24}$	$\frac{9}{32}$	$\frac{9}{32}$	$\frac{9}{14}$	$\frac{9}{56}$	$\frac{9}{56}$
a_4	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{24}$	$\frac{1}{6}$	$\frac{1}{24}$	$\frac{9}{32}$	$\frac{9}{32}$	$\frac{9}{56}$	$\frac{9}{14}$	$\frac{9}{56}$
a_5	$\frac{1}{48}$	$\frac{1}{48}$	$\frac{1}{24}$	$\frac{1}{24}$	$\frac{1}{6}$	$\frac{9}{32}$	$\frac{9}{32}$	$\frac{9}{56}$	$\frac{9}{56}$	$\frac{9}{14}$

Extra knowledge

Probable innocence

Definition [Safe version]: a protocol satisfies α-probable innocence in presence of extra knowledge if

$$\forall i,j,k \; p(a_i \mid o_j, s_k) \leq \alpha$$

Extra knowledge

Probable innocence

Proposition [Impact of the extra info]

1. $\forall i,j,k\ p(a_i \mid o_j, s_k) \leq \alpha$ if $p(a_i \mid o_j) \leq q\alpha$

2. If $\forall i,j,\ p(a_i \mid o_i) = p(a_j \mid o_j)$ then
   $\forall i,j,k\ p(a_i \mid o_j, s_k) \leq \alpha$ iff $p(a_i \mid o_j) \leq q\alpha$

where

$$q = \min_{i,j,k} \left(p(s_k \mid o_j) / p(s_k \mid a_i) \right)$$

Extra knowledge

Vulnerability

Definition: a protocol satisfies α-vulnerability in presence of extra knowledge if

$$V(A \mid O,S) \leq \alpha$$

where

$$V(A \mid O,S) = \Sigma_{j,k}\, p(o_j,s_k)\, \max_i(p(a_i \mid o_j,s_k))$$

Extra knowledge

Vulnerability

Proposition [Impact of the extra info] Assume that $\forall i\ p(o_i \mid a_i) = p = \max_{i,j} p(o_j \mid a_i)$ then

1. $V(A \mid O,S) \leq \alpha$ if $V(A \mid O) \leq \alpha/(qr)$

2. If the a priori distribution is uniform and $\frac{(1-p)}{n-1} q \leq \frac{(1-q)}{r-1} p$ then
   $V(A \mid O,S) \leq \alpha$ iff $V(A \mid O) \leq \alpha$

where

- $r = card(\{s_1, s_2, \ldots, s_r\})$
- $q = \max_{i,k} p(s_k \mid a_i)$

Outline

- Introduction
- Crowds protocol
- Anonymity
  - Probable innocence
  - Vulnerability
- Anonymity in presence of extra knowledge
  - Probable innocence
  - Vulnerability
- **Recent results**
- Conclusion

Recent results

Trust in Crowds

- Extend Crowds protocol with trust:
  - Associate to each principal a trust level $t \in [0,1]$.
  - The forwarding process is governed by a policy where the probability of choosing a member depends on her trust level.
- Results:
  - Study the impact of such probabilistic behaviour of principals.
  - Establish necessary and sufficient criteria for choosing an appropriate policy of forwarding between members in order to achieve a desired level of privacy.

Recent results

Beliefs

- Open problem: measure and account for the accuracy of the adversary extra knowledge.
- Integrate the notion of adversary's beliefs:
  - Assume that both the actual a priori distribution of the hidden input and its correlation to the extra information are unknown to the adversary.
  - Generalise the approach to information flow systems.
- Results:
  - New metric for quantitative information flow based on the concept of vulnerability that takes into account the adversary's beliefs.
  - Our model allows to identify the levels of accuracy for the adversary's beliefs which are compatible with the security of a given program or protocol.

Future work

- In many cases the confidentiality scenarios are interactive:
  - Part of the secrets come after observable events and may depend on them.
- Extend the metric so to capture the dynamic nature of interactive protocols.

Conclusion

- Extra knowledge
  - Highly likely in the new era of ubiquitous computing world
  - May have a serious impact on the security.
  - Makes both probable innocence and vulnerability more difficult to achieve.
  - Fundamental issues remain however wide open.