Analysis of Anonymity Services from a Tunable Perspective

Reine Lundin, Stefan Lindskog, and Anna Brunstrom

Department of Computer Science

Karlstad University

Outline

- Tunable security (TS)
  - Definition and motivation
  - Conceptual Model
- Mix-Nets
- Crowds
- Future work

Tunable security (TS)

- A TS service is defined as a service that provides various security configurations that can be selected at run-time
- Tradeoff between computational cost and security
  - Hand-held Devices
  - Multimedia Applications

Conceptual Model of TS

- The purpose of the model is to provide a tool that can be used to describe and analyze TS services in a structured and consistent way
- Proposed in

  Stefan Lindskog, Anna Brunstrom, Reine Lundin, and Zoltán Faigl. "A Conceptual Model of Tunable Security Services". In Proceedings of the 3rd International Symposium on Wireless Communication Systems (ISWCS 2006), Valencia, Spain, September 5-8, 2006
- Used in

  Stefan Lindskog, Anna Brunstrom, and Zoltán Faigl. "Analyzing Tunable Security Services". In Proceedings of the Fourth Swedish National Computer Networking Workshop (SNCNW 2006), Luleå, Sweden, October 26-27, 2006

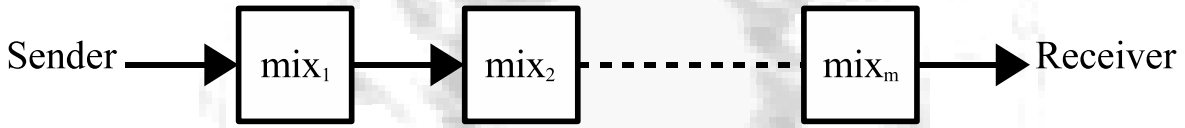
Conceptual Model of TS

- Core building blocks of a TS service
  - S = {Security configurations}
  - T = {Tuner preferences}
  - E = {Environmental descriptors}
- TS (mapping) function

$$TS : T \times E \rightarrow S$$

Mix-Nets

- Introduced by David Chaum in 1981
  - To achieve untraceable electronic mail
- Consist of a chain of mixes



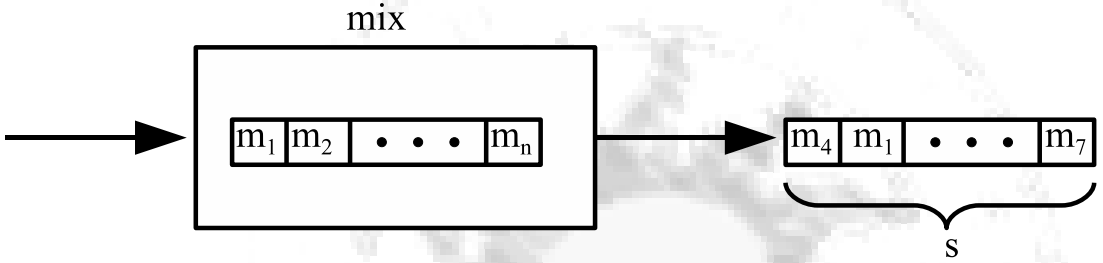
- Properties
  - Sender anonymity
  - Unlinkability of sender and recipient

Mix-Nets

- The work of a mix
  - Collect messages in a pool
  - Decide when to flush the pool
    - Threshold, Time, Combination
  - Decide which subset of the pool to flush
- The cycle of collecting and flushing is called one round

Mix-Nets

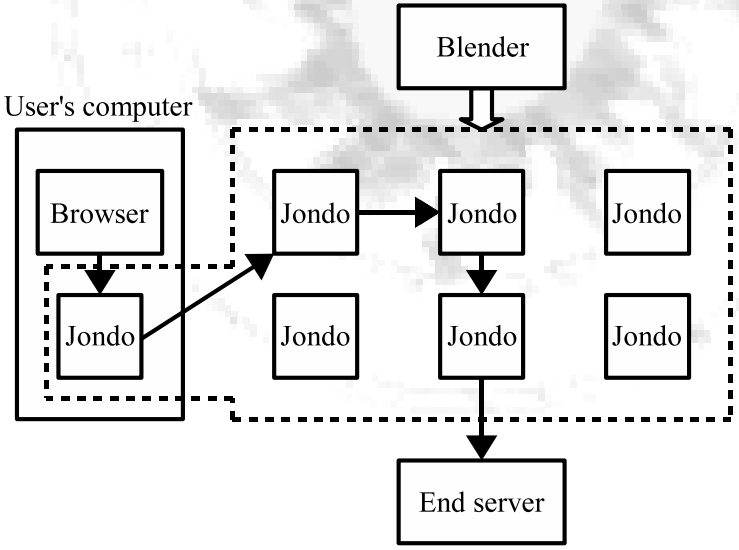
- Deterministic mixes $s = nP$



- $S = \prod_{j=1}^{m}(s_{ij} \times n_{ij})$
- $T = S$
- $E = \varnothing$
- $TS(t, \varnothing) = t$

Crowds

- Invented by Reiter and Rubin in 1997
- The system consists of
  - A Blender (central database)
  - Jondos (user applications)

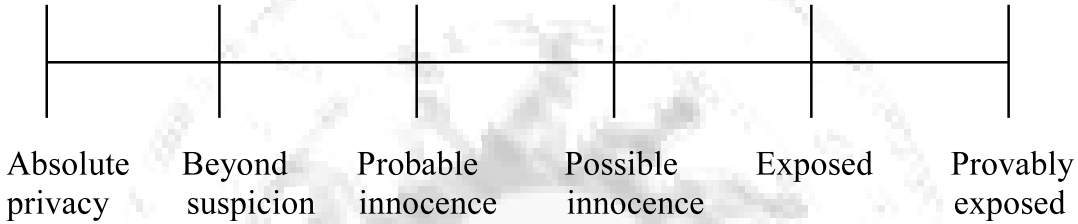


Crowds

- The Crowds system can be described by the three parameters p_f, n and A
- p_f is the probability of forwarding during path creation
- n is the number of Jondos
- A is the attacker
  - Local eavesdropper (LE)
  - Collaborating members (CM)
  - End server (ES)

Crowds

- Anonymity levels (the tuner preference)



Attacker	Sender anonymity	Receiver anonymity
LE	Ex	Ex/BS
CM	AP/BS/PrI/PoI/Ex	Ex/AP
ES	BS	N/A

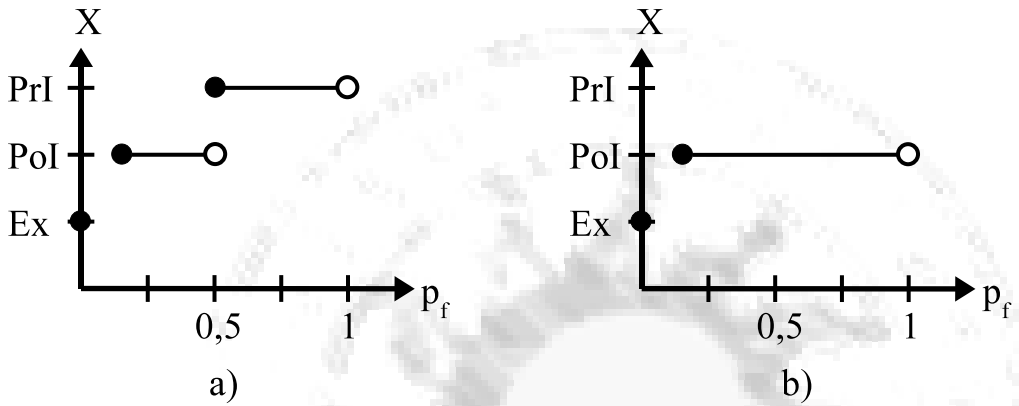
Crowds

- $T = PrI \mid PoI \mid Ex$
- $E = n \times A = n \times CM$
- $S = p_f$
- $TS(PrI, n, c) = \frac{1}{2} \frac{n}{(n - c - 1)}$

$$TS(PoI, n, c) = \delta \frac{n}{n - c - 1}$$

$$TS(Ex, n, c) = 0$$

Crowds



a) $\frac{n-c-1}{n} = 1 \ (\delta = \frac{1}{6})$

b) $\frac{n-c-1}{n} = \frac{1}{2} \ (\delta = \frac{1}{6})$

Future Work

- To further investigate the dynamic features of Mix-nets and Crowds
- Examine if additional tunability can be added to Mix-Nets and Crowd
- Investigate the tradeoff between performance and security.