MAFTIA WP2 Demonstration
Transaction Service and Middleware

University of Newcastle upon Tyne

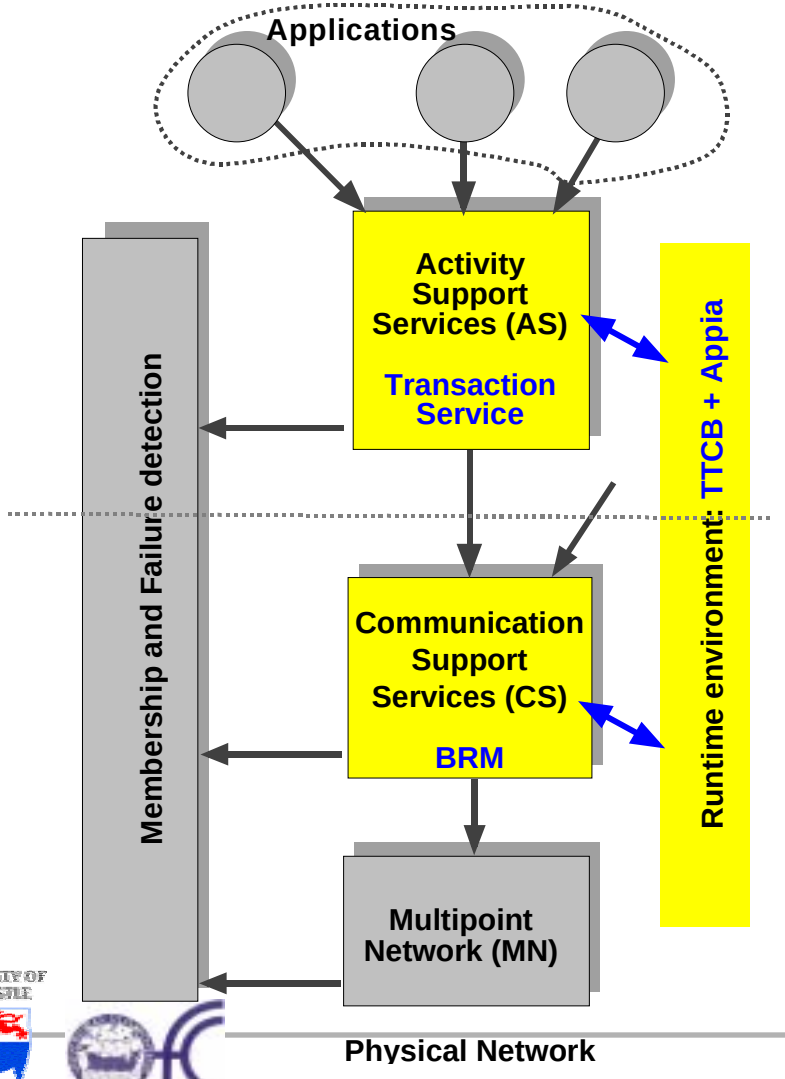
University of Lisboa

February 2003

Summary

- MAFTIA middleware
- TTCB and BRM
- Transaction Service
- Scenario: *an intrusion-tolerant transactional tic tac toe*
- Demonstration
  - ☞Normal and multiparty transactions
  - ☞Resilience to intrusions
  - ☞Limits of intrusion tolerance

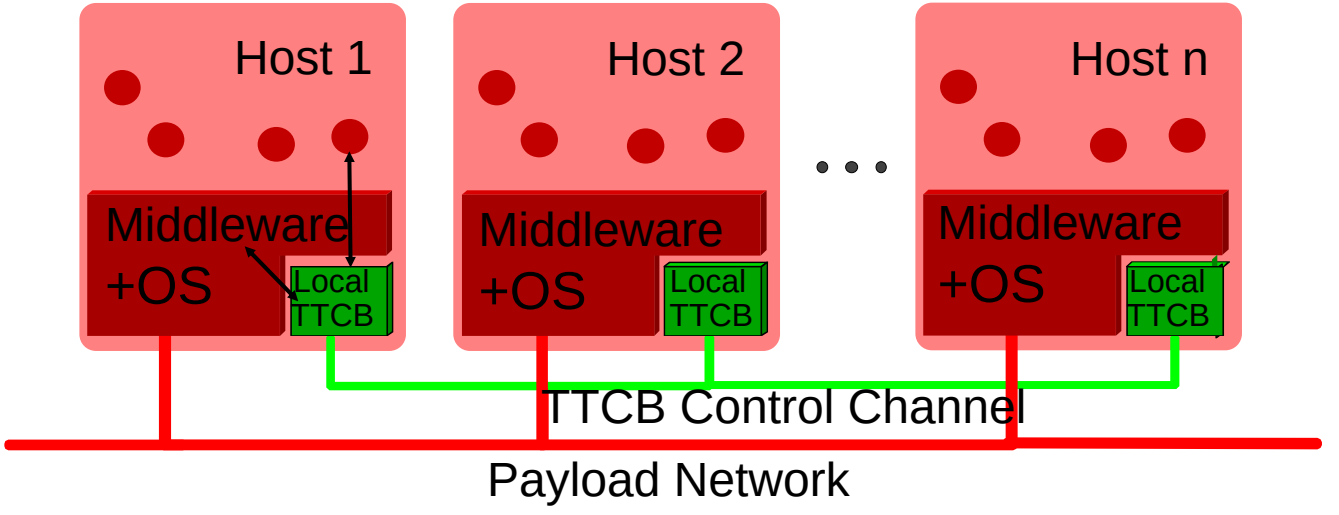
Maftia Middleware



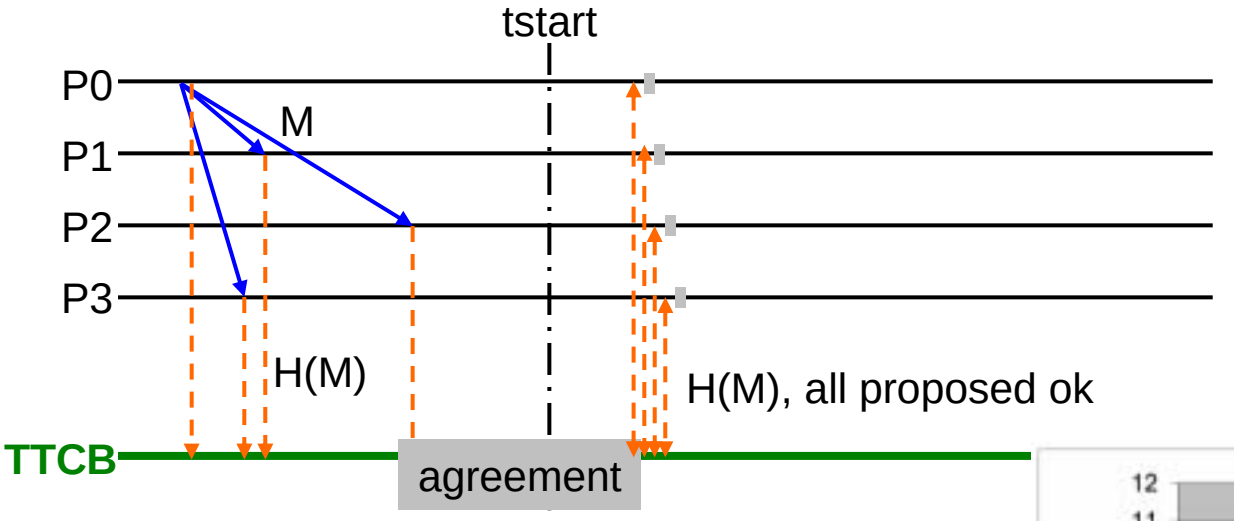
- Activity services
  - **Transaction Service**
    University of Newcastle upon Tyne (UK)
- Communication services
  - Partially synchronous protocols (**BRM**)
    University of Lisboa (P)
  - Asynchronous protocols:
    IBM, Zurich (CH)
- Runtime support
  - **TTCB** and **Appia**
    University of Lisboa (P)

TTCB Wormhole Model

- Most of the system is Byzantine-on-failure except…
- TTCB wormhole: secure, real-time, limited services

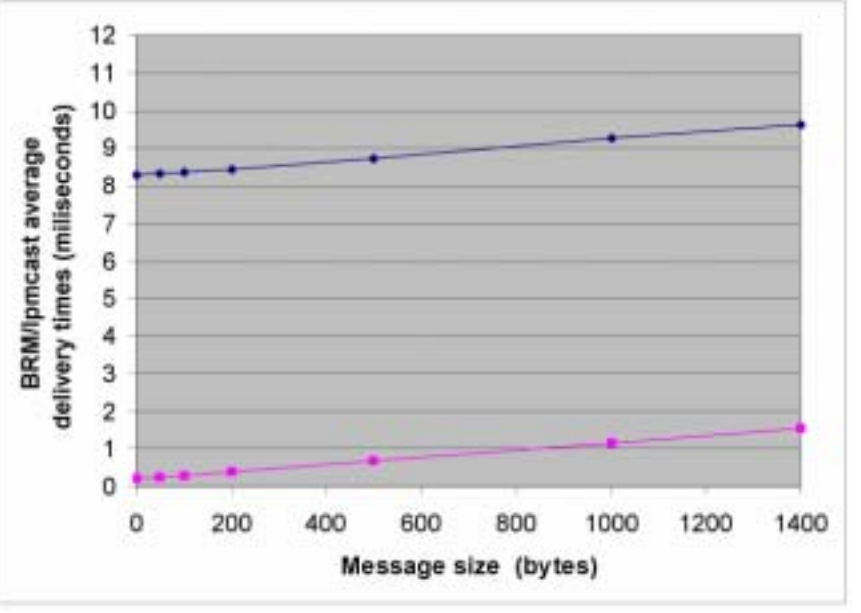


Byzantine Reliable Multicast BRM



1st phase

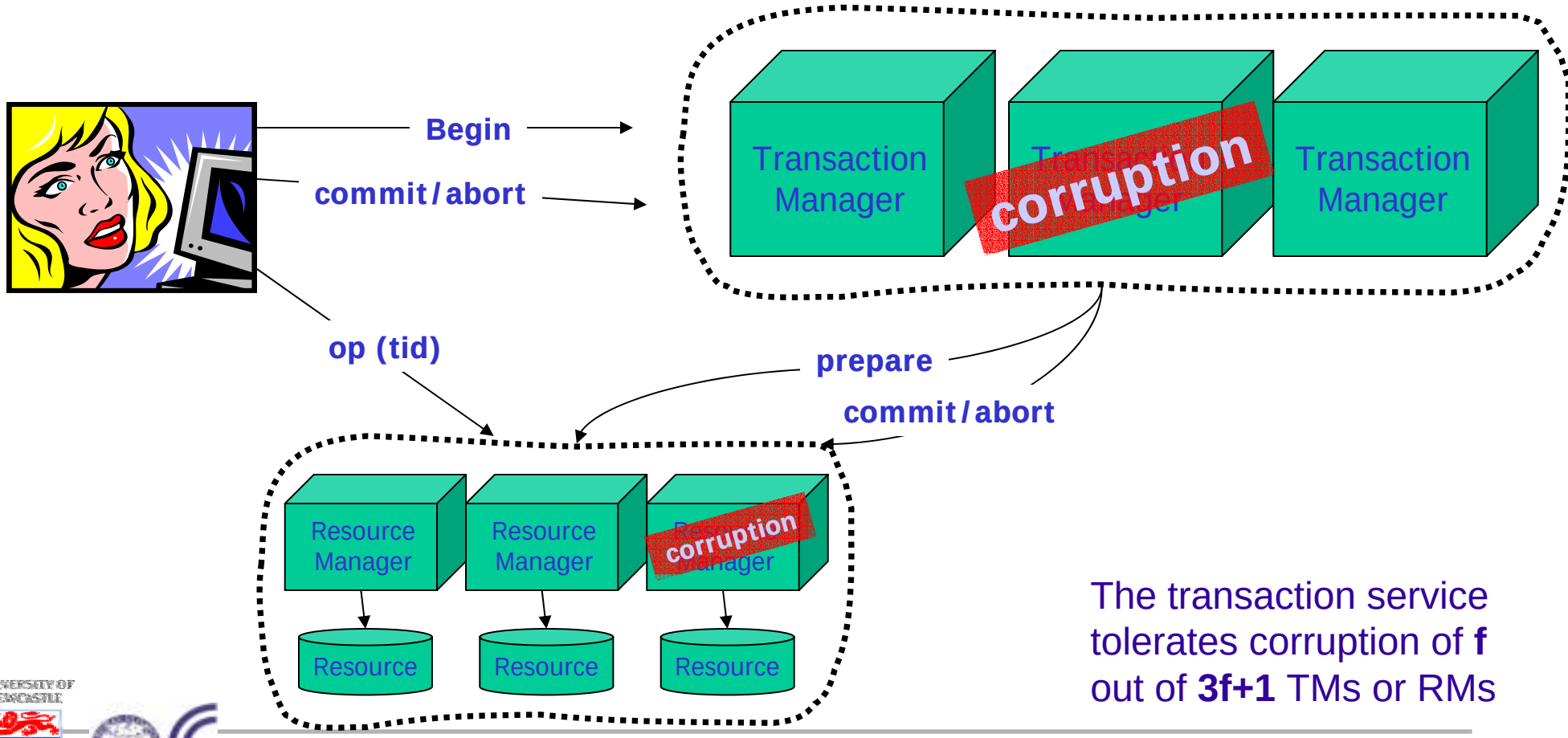
5-node delivery times



Transaction Service

- A CORBA-style transaction service
- Provide ACID properties: atomicity, consistency, isolation, durability
- Multiparty transactions
- Intrusion tolerant

Intrusion Masking – Replication



The transaction service tolerates corruption of **f** out of **3f+1** TMs or RMs

Multiparty Transactions

begin

commit/abort

Transaction Manager

Transaction Manager

Transaction Manager

join

commit/abort

op (tid)

prepare

commit/abort

op (tid)

Resource Manager

Resource Manager

Resource Manager

Resource

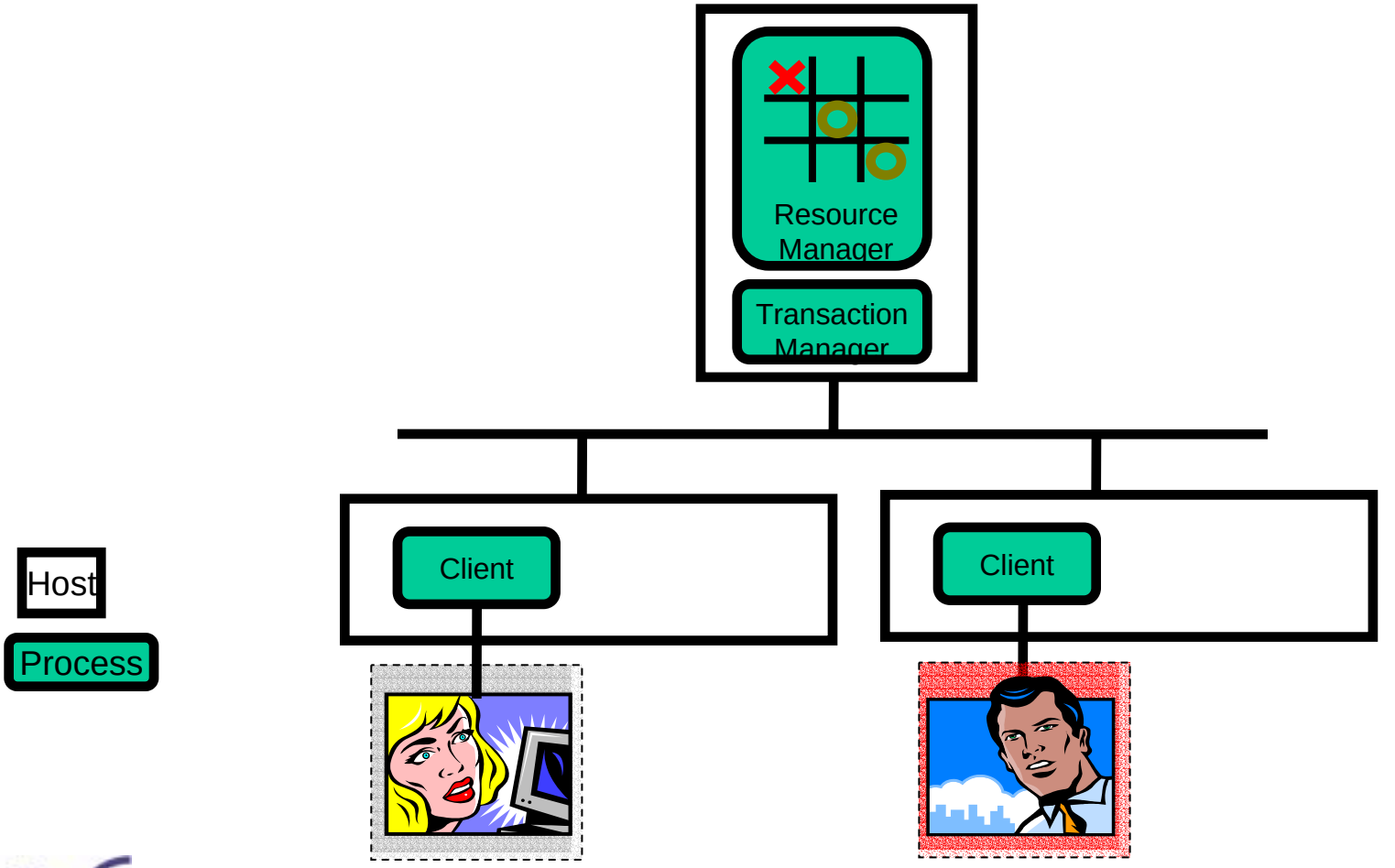
Resource

Resource

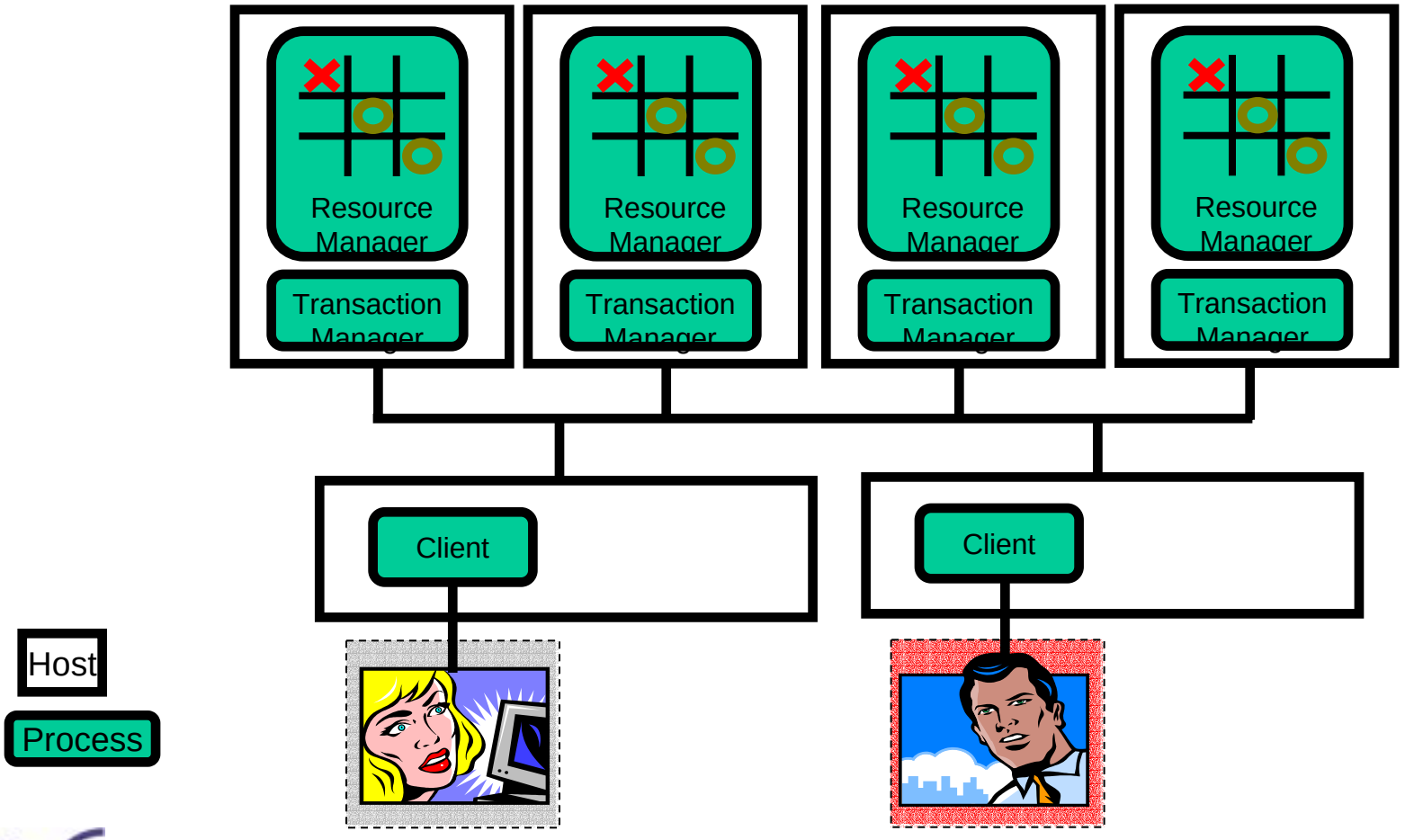
Demonstration Scenario

- A simple *tic tac toe* game
- There are two players who interact the game (transactional resource)
- We show that an intrusion tolerant transaction service can provide a correct service despite intrusions

Standard Transactional TicTacToe



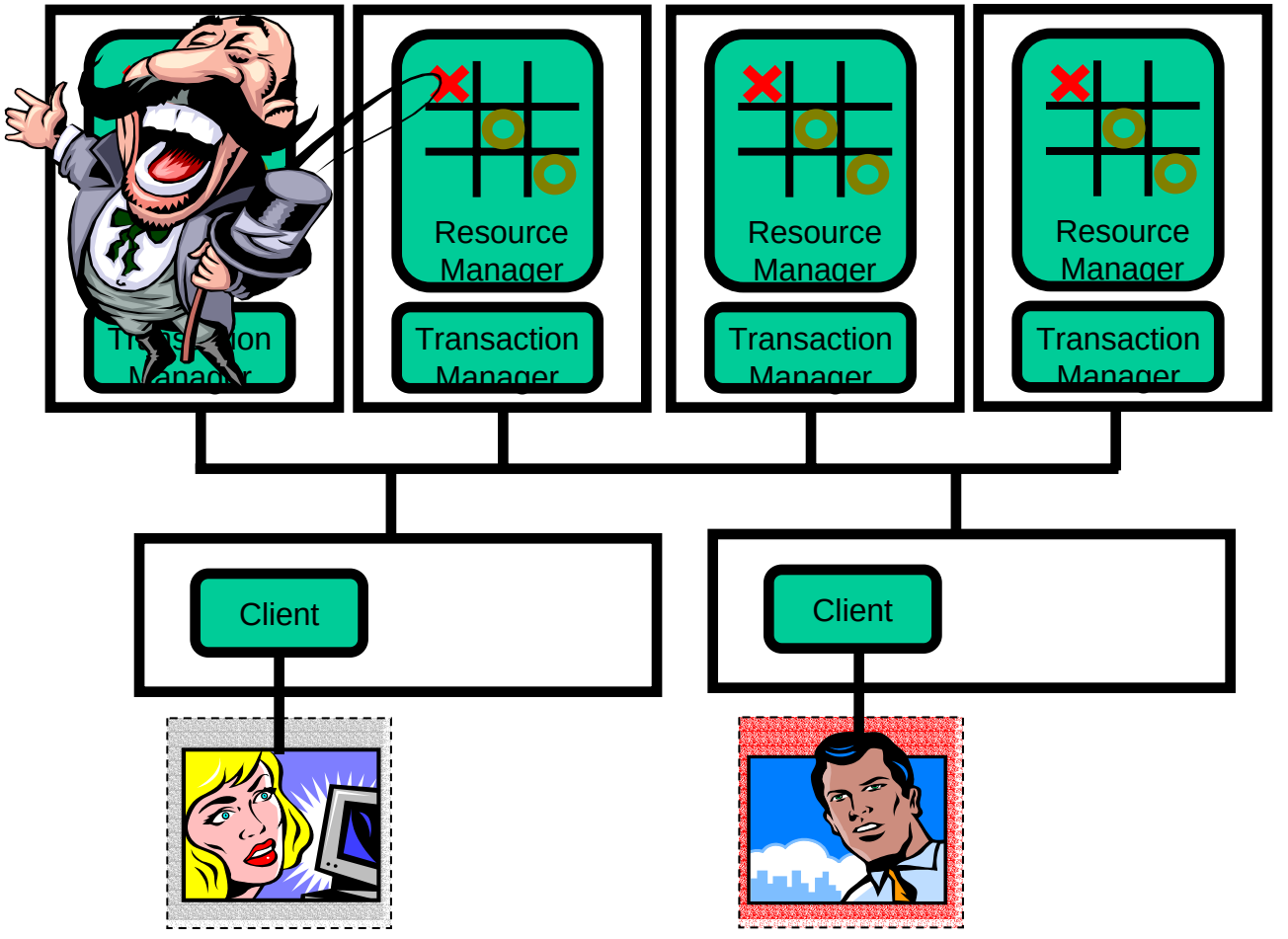
IT Transactional Tic Tac Toe



Hacker Behaviour

- A hacker may be able to install trapdoors in the TMs and RMs that allow him to bring them under his control
- Hacker wishes to influence the outcomes of games

Hacked Tic Tac Toe



Demonstration

- 1 resource manager (tic tac toe board) per machine (4 total)
- 1 transaction manager per machine (4 total)
- 2 clients
- TTCB: one local TTCB per machine and control network
- Appia and protocol stack (BRM)

Demonstration 1: Normal Case

- Making a move : Player begins a transaction, places a piece, and either aborts or commits the change making it visible to other players
- Benign Environment:
  - ☞ Player 1 makes move, player 2 makes a move
  - ☞ Player 1 makes move but aborts
  - ☞ Multiparty transaction: player 1 begins a transaction, player 2 joins, both make a move and commit

Demonstration 2: Intrusion Tolerance (RM)

- Hack one RM
  - Player 1 makes move
  - Hacked RM flips piece
  - Player 2 starts move and refreshes board
  - **The hacker is not able to change the moves**

Demonstration 3: Intrusion Tolerance (TM)

- Hack one TM
  - Player 1 makes move and commits
  - Hacked TM requests resource managers to abort
  - Move is committed despite intrusion
  - **The hacker is not able to change the decision**

Demonstration 4: Limits of Intrusion Tolerance

- Hack two more RMs (3 total)
  - Hackers now control the majority of the RMs…
  - Player 1 makes move and commits
  - Three out of four RMs flip piece
  - Player 2 begins move and refreshes board state from resource managers
  - Board displays as intended by the hacker rather than Player 1
  - **To tolerate more intrusions we require more replicas (10 for 3 intrusions)**

Summary

- Demonstrated IT transaction service
  - ☞ Distributed CORBA style transaction service with support for multiparty transactions
  - ☞ Intrusion tolerance service composed of intrusion tolerant protocols
  - ☞ Can tolerate intrusions, the number is related to the degree of replication
- Demonstrated
  - ☞ Application of MAFTIA design principles (WP1) to Middleware activity service (WP2)
  - ☞ Integration between middleware layers and TTCB