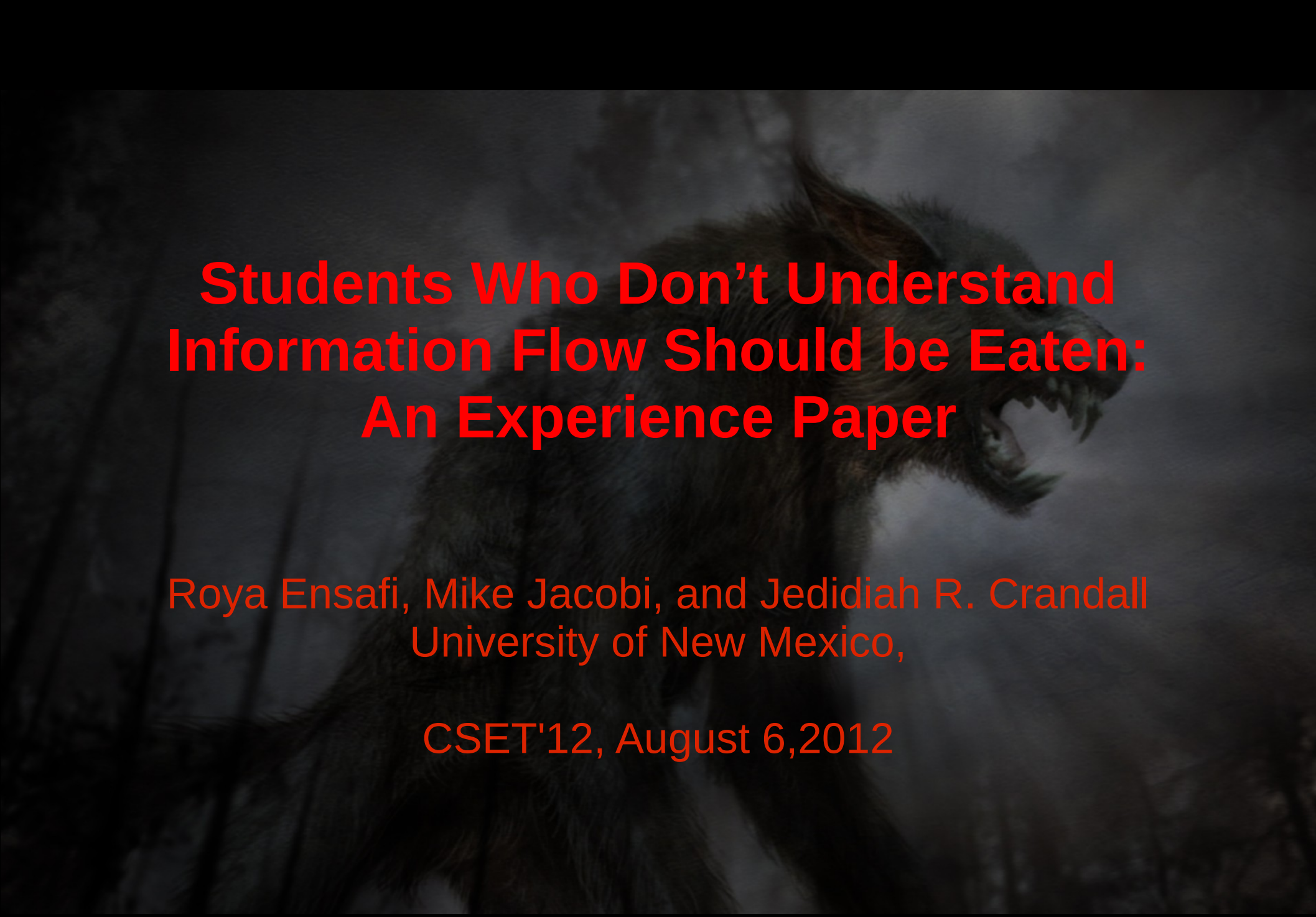


Students Who Don’t Understand Information Flow Should be Eaten: An Experience Paper

Roya Ensafi, Mike Jacobi, and Jedidiah R. Crandall
University of New Mexico,

CSET'12, August 6,2012

Students Act Like Wolves

Our Missions

Games are pedagogically effective learning environments.

Werewolves(Mafia) is a sustainable game.

Danger of trusting system isolation is not fully understood.

Our UNIX-based version can make a difference in your classes.

Our Missions

Games are pedagogically effective learning environments [1,2,3].

[1] *Batcheller et al.* Testing the technology: playing games with video conferencing.

[2] Ratus *et al.* What hackers learn that the rest of us don't: Notes on hacker curriculum.

[3] Blinger *et al.* The next generation of educational engagement.

Our Missions

Werewolves(Mafia) is a sustainable game [4,5].

[4] Raverman *et al.* Mafia: A theoretical study of players and coalitions in a partial information environment.

[5] Migda *et al.* mathematical model of the Mafia game.

Our Missions

Danger of trusting system isolation is not fully understood [6,7,8,9].

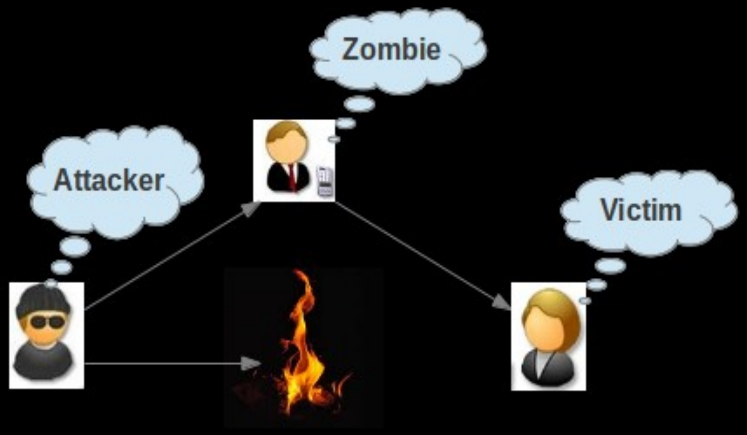
[6] Zhang *et al.* Peeping Tom in the neighborhood: keystroke eavesdropping on multi-user systems.

[7] Qian *et al.* Off-path TCP sequence number inference attack – how firewall middle-boxes reduce security.

[8] Jana *et al.* Memento: Learning secrets from process Footprints.

[9] Ensafi *et al.* Idle port scanning and non-interference analysis of network protocol stacks using model checking

Our Missions



Danger of trusting system isolation is not fully understood [8,9].

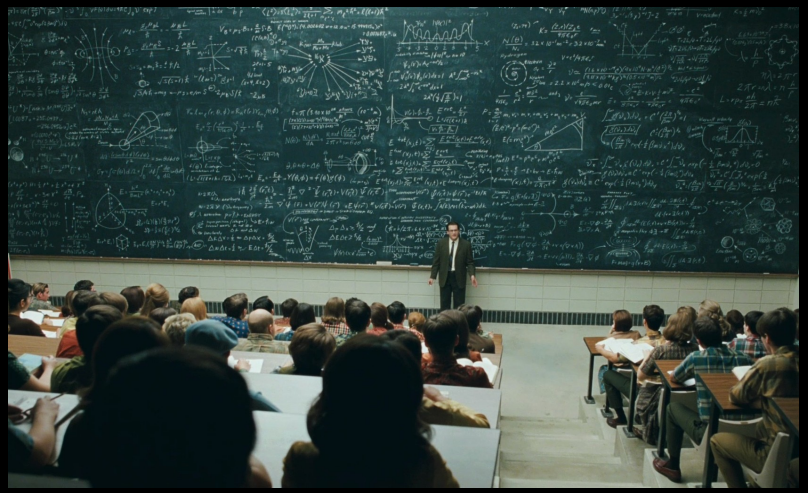
[8] Jana *et al.* Memento: Learning secrets from process footprints.
[9] Ensafi *et al.* Idle port scanning and non-interference analysis of network protocol stacks using model checking

Our Missions

Our UNIX-based version can make a difference in your classes.

Understanding Information Flow

- Information flow example:
  - If L <= H, flows from L to L, from H to H, and L to H would be allowed, while flows from H to L would not.
- Covert channel.
- Inference channel.
- Read [10,11,12].



[10] Lampson. A note on confinement problem.
[11] Kemmerer. Shared resource matrix methodology:
An approach to identifying storage and timing channels.
[12] Wray. An analysis of covert timing channels.

Understanding Information Flow

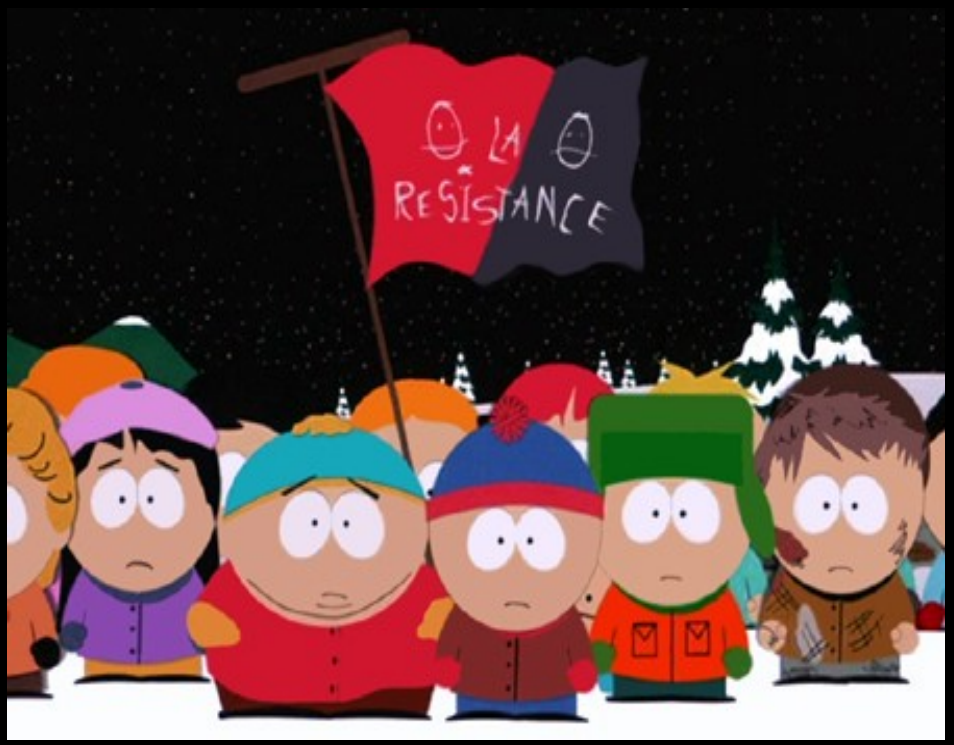
- Information flow example:
  - If L <= H, flows from L to L, from H to H, and L to H would be allowed, while flows from H
- Covert channel.
- Inference channel.
- Read [10,11,12].

[10] Lampson. A note on confinement problem.
[11] Kemmerer. Shared resource matrix methodology:
An approach to identifying storage and timing channels.
[12] Wray. An analysis of covert timing channels.

Werewolves of Miller's Hollow

Werewolves of Miller's Hollow

- Members:



Sample Round of Werewolves

Begin:
There are 2 wolves, and 8 townspeople.

Townspeople: [Alice, Bob, David, Joe, Mike, Jonas, Roya, Tooba]

Werewolves: [Mike, Jonas]

Witch: [David]

Sample Round of Werewolves

Sample Round of Werewolves

Werewolves, time to vote.

Mike: lets eat Roya
Jonas: no, I love her :)
lets vote for Bob

Jonas & Mike vote for Bob.
Werewolves, you selected to eat Bob, close your eyes.

Sample Round of Werewolves

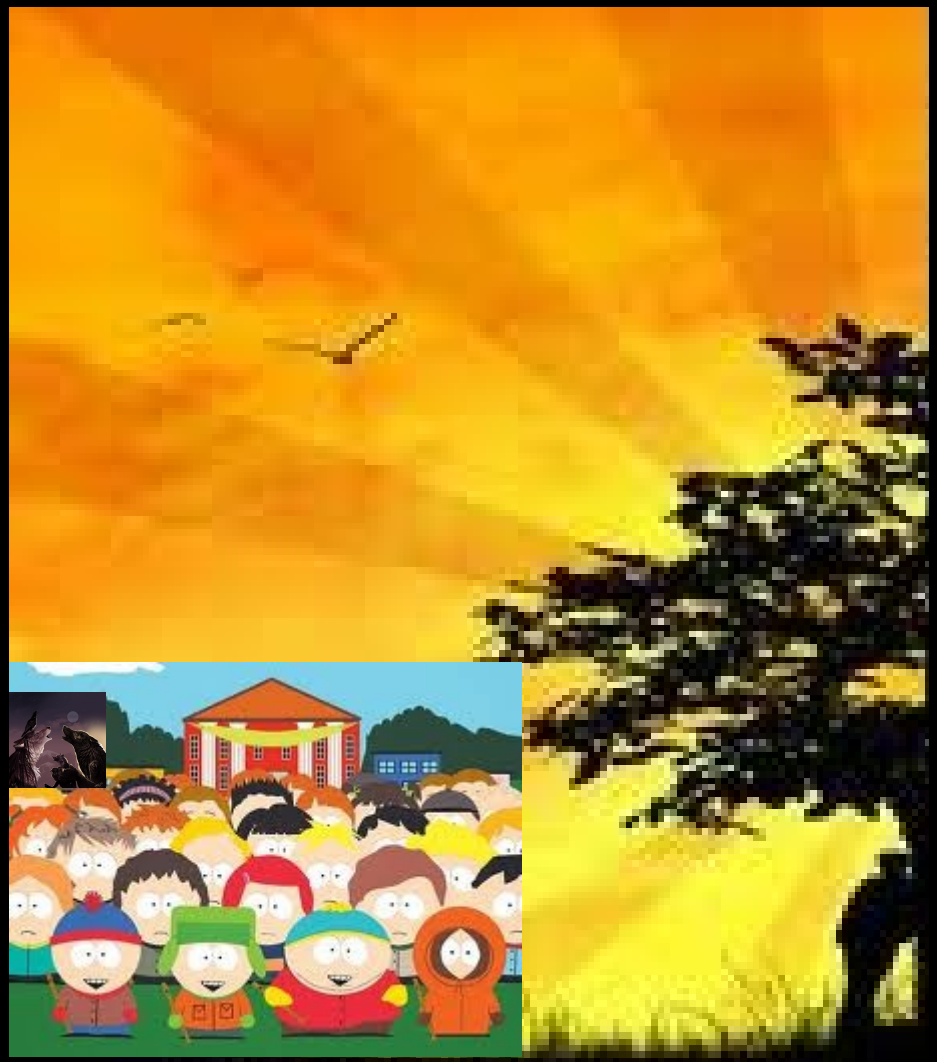
Sample Round of Werewolves

Witch,
open your eyes &
Vote: [pass, poison, save]

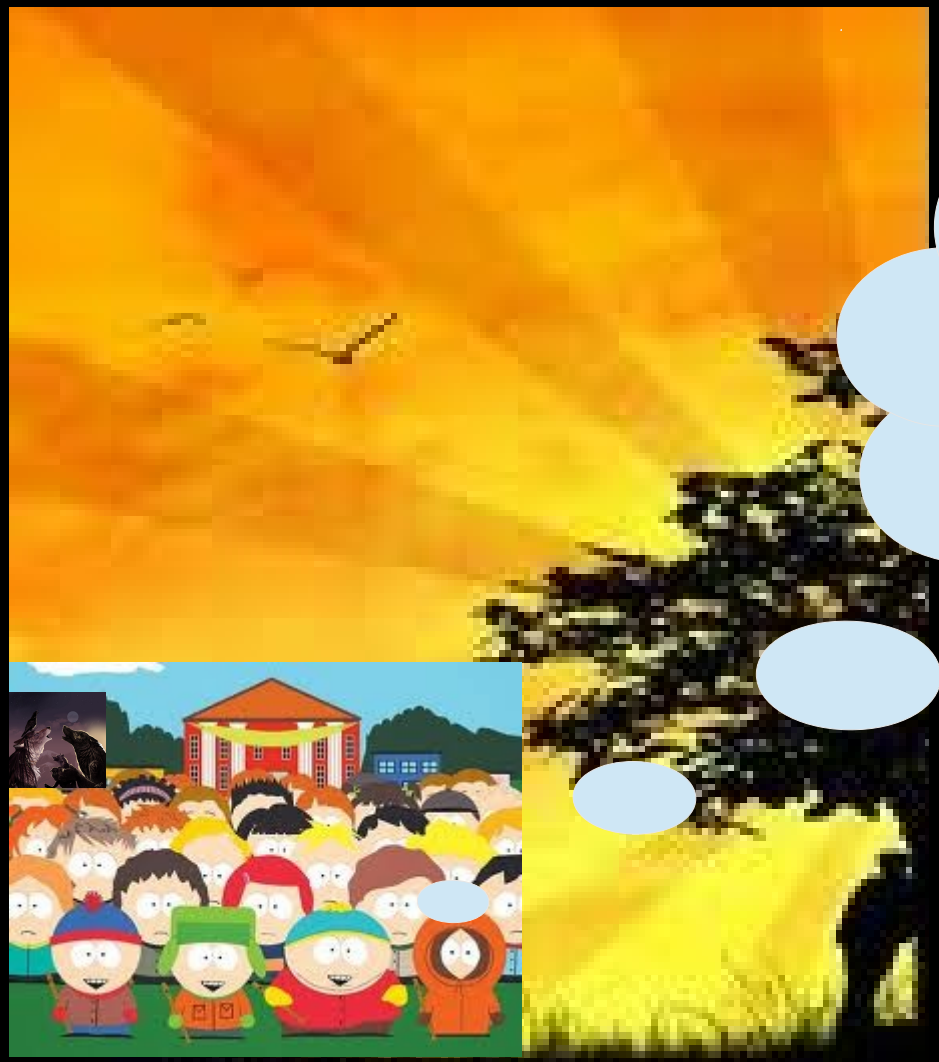
Witch: I pass.

Witch, close your eyes.

Sample Round of Werewolves



Sample Round of Werewolves



The werewolves ate Bob.

Bob:
I was townspeople,
I think Mike is werewolves.
Goodbye, cruel world.

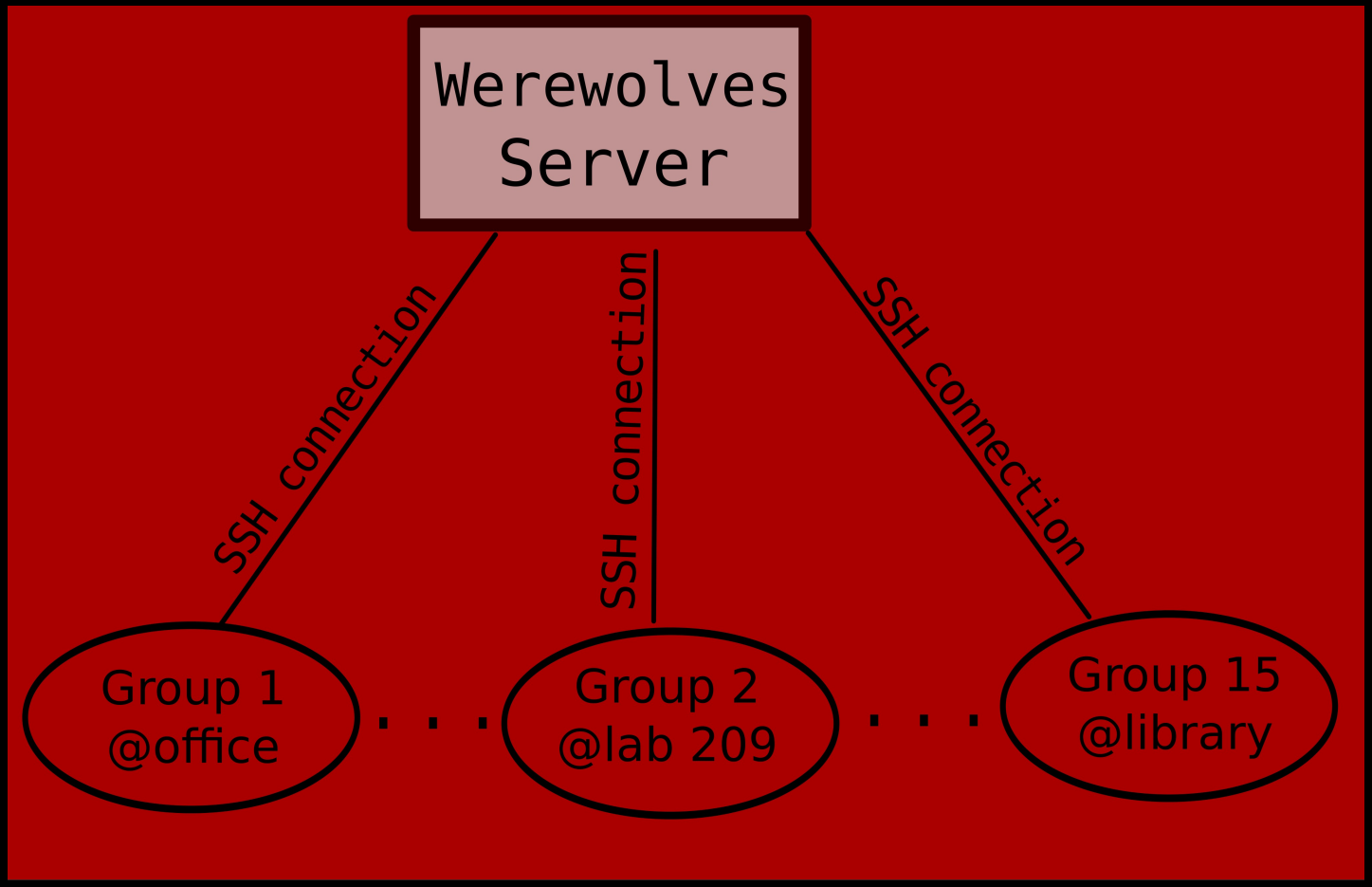
Mike: Lets kill Alice.
Alice & Bob always talked.

Everyone open your eyes.
You have 240" to discuss who the werewolves are, and 60" to vote....

Werewolves of Miller's Hollow

"Detective" is removed for the sake of pushing our students to use inference channels.

UNIX-based Version of Werewolves



Werewolves to Teach Covert Channels

Acknowledgements

THANK TO:

Sean Peisert,

Nick Aase, Xu Zhang
students of CS/UNM 444/544, 2012

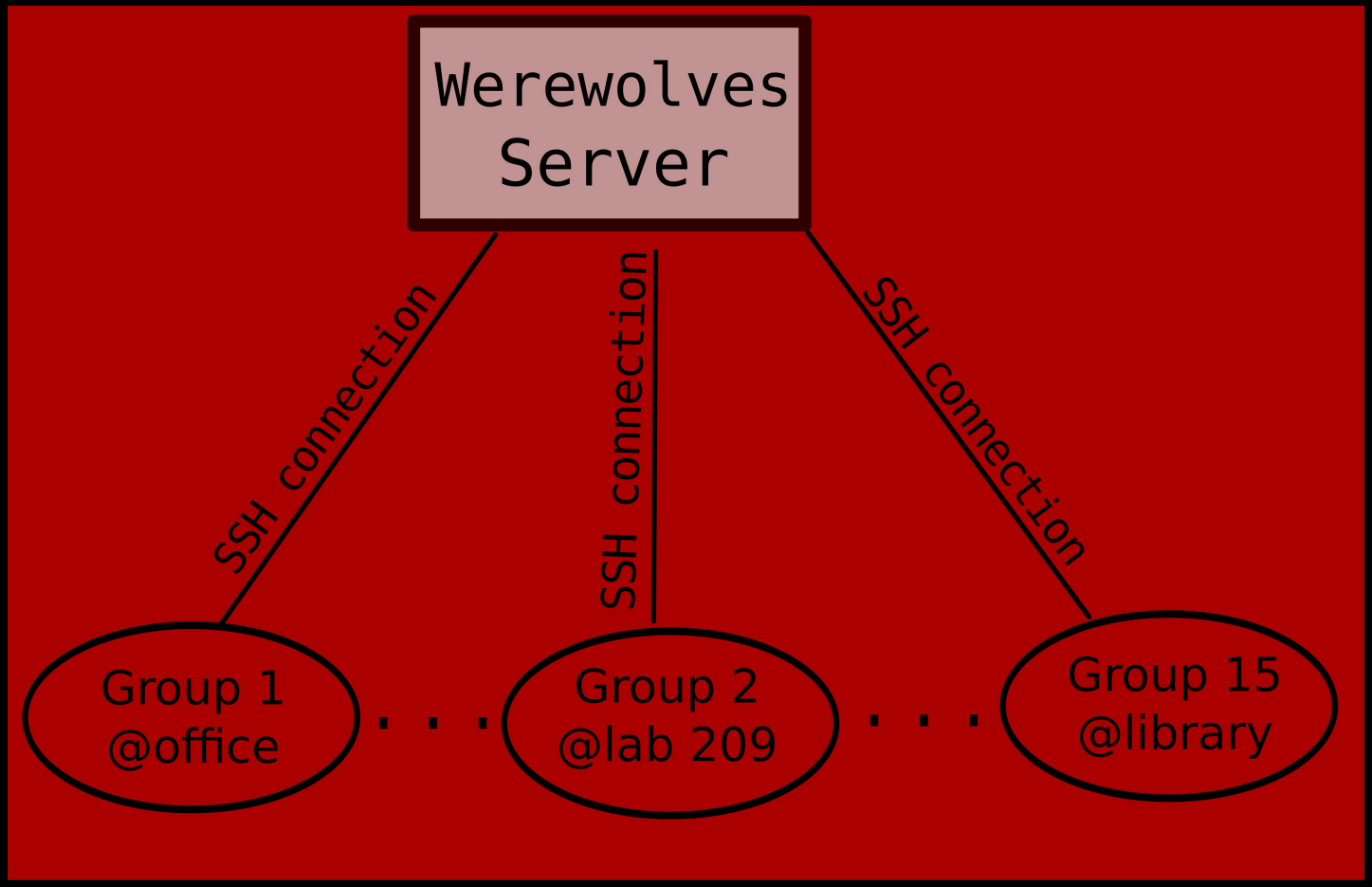
National Science Foundation under Grant Nos. #0844880, #0905177, and #1017602.

تقدیم به
مادر و پدرم
که همیشه پناهم بودند

UNIX-based Version of Werewolves

- Introduction to Cybersecurity (CS 444/544)
  - Spring 2012 at UNM/CS
- 45 students
- 3 credits course, every Mon/Wed/Friday
- Link to class website:
  - http://www.cs.unm.edu/~royaen/teaching.html

UNIX-based Version of Werewolves



Our Werewolves Program Architecture

- **server.py** (Automated moderator)
- **client.py** (Run by players)
  - Can be written in any language
- **communication.py** (Consists of helper methods)

Talk to Mike Jacobi for details.

Strategies Students Discovered

- Silent werewolves
  - Successful Werewolves strategy
  - Solution: Shift the balance of powers using knob
- Create many system calls
  - Unsuccessful Werewolves strategy to hide their identities
- Find shadow file
  - “If you are not cheating, you are not trying”.
- Chang identity
  - During chat phase, make a town person look like a werewolf.

Lessons Learned

- Server design
- Great student enthusiasm
  - All students were challenged, but still able to contribute.
- Continuously engaging students
  - Feedback loop
  - Interesting discussions about info. flow, and game theory

Examples of Information Leaks

Live demo …

WILL you use our UNIX-based werewolves in your class?

why or why not?

Links and Email

- Link to class materials:
  - (www.cs.unm.edu/~royaen/teaching/)
- Email:
  - werewolves@cs.unm.edu
    - Don't hesitate to ask us for help