Cubicle vs. the Coffee Shop

Behavioral Modes in (Enterprise) End-Users

Frederic Giroire
Jaideep Chandrashekar
Gianluca Iannaccone
Dina Papagiannaki
Eve Schooler
Nina Taft

Intel Research/ INRIA

Motivation

- Previous studies of user profiles used traces collected "in-network"
- Corporate networks today have 50-60% mobile hosts
- When profile is constructed in one environment, how different in another?
- Do profiles computed from "averaging" hold true in any of the environments?
- Is there a canonical user profile?
- What (statistics) change when users move?
- Should user profiles care about location?

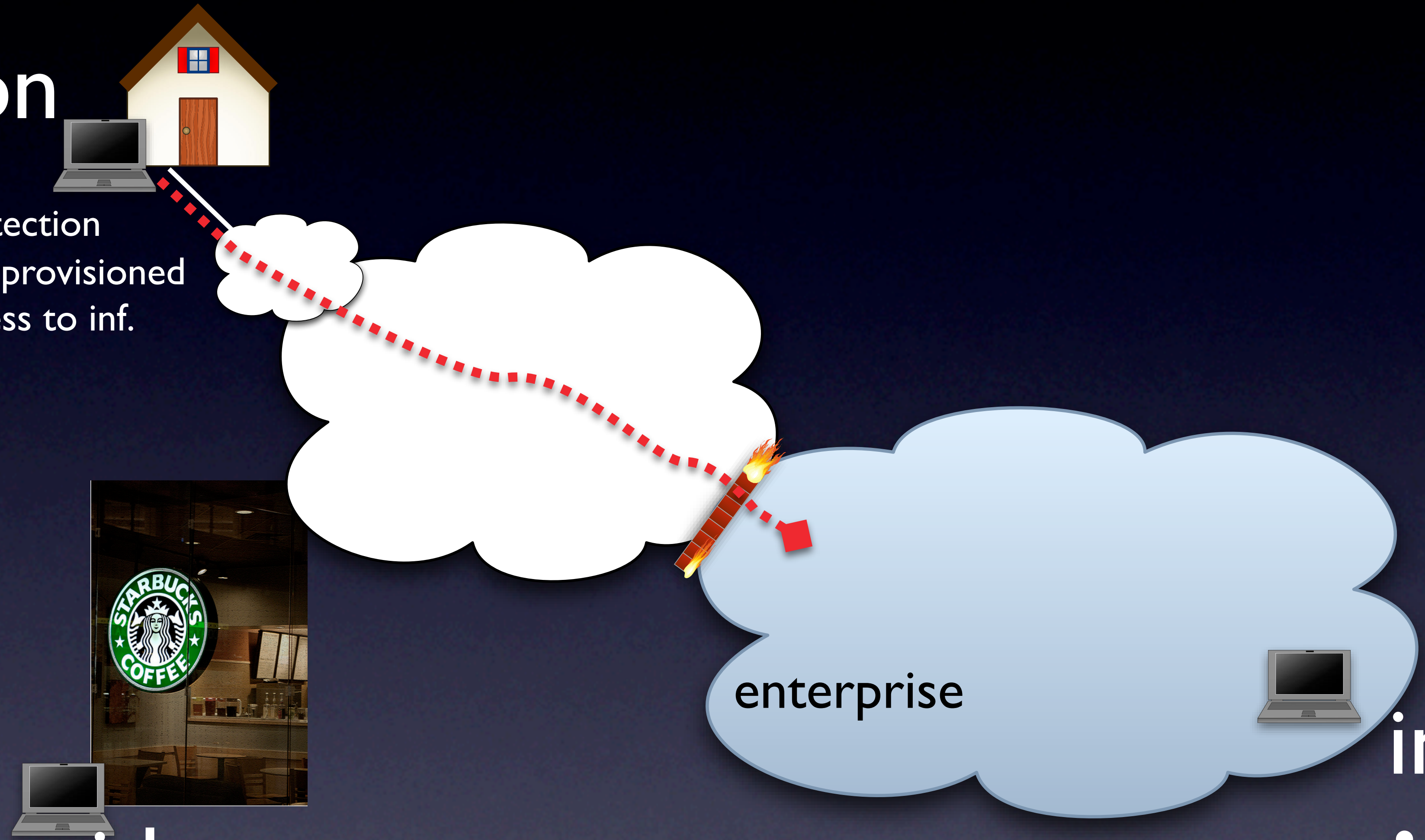
Data

- 350+ users, all running Windows XP SP2 custom build
- Collection software (windump+custom app) ran on laptops and (few) desktops
- Unique data-set (most traces collected in network)
- Traces collected for ~5 weeks; s/w automatically deactivated
- Traces periodically uploaded to central server

Recruiting users

- 1400+ people polled from across 3 business units
- Up front and clear statement about intended use
- Explicit consent-- software was installed by users
- Traces are uploaded anonymously; filenames do not identify individual users
- At central server: packets processed and payloads discarded
- Amazon gift certificates given out as enticement

Environments



vpn

- limited protection
- moderately provisioned
- limited access to inf. services

outside

- no protection
- badly provisioned
- no access to inf. services

enterprise

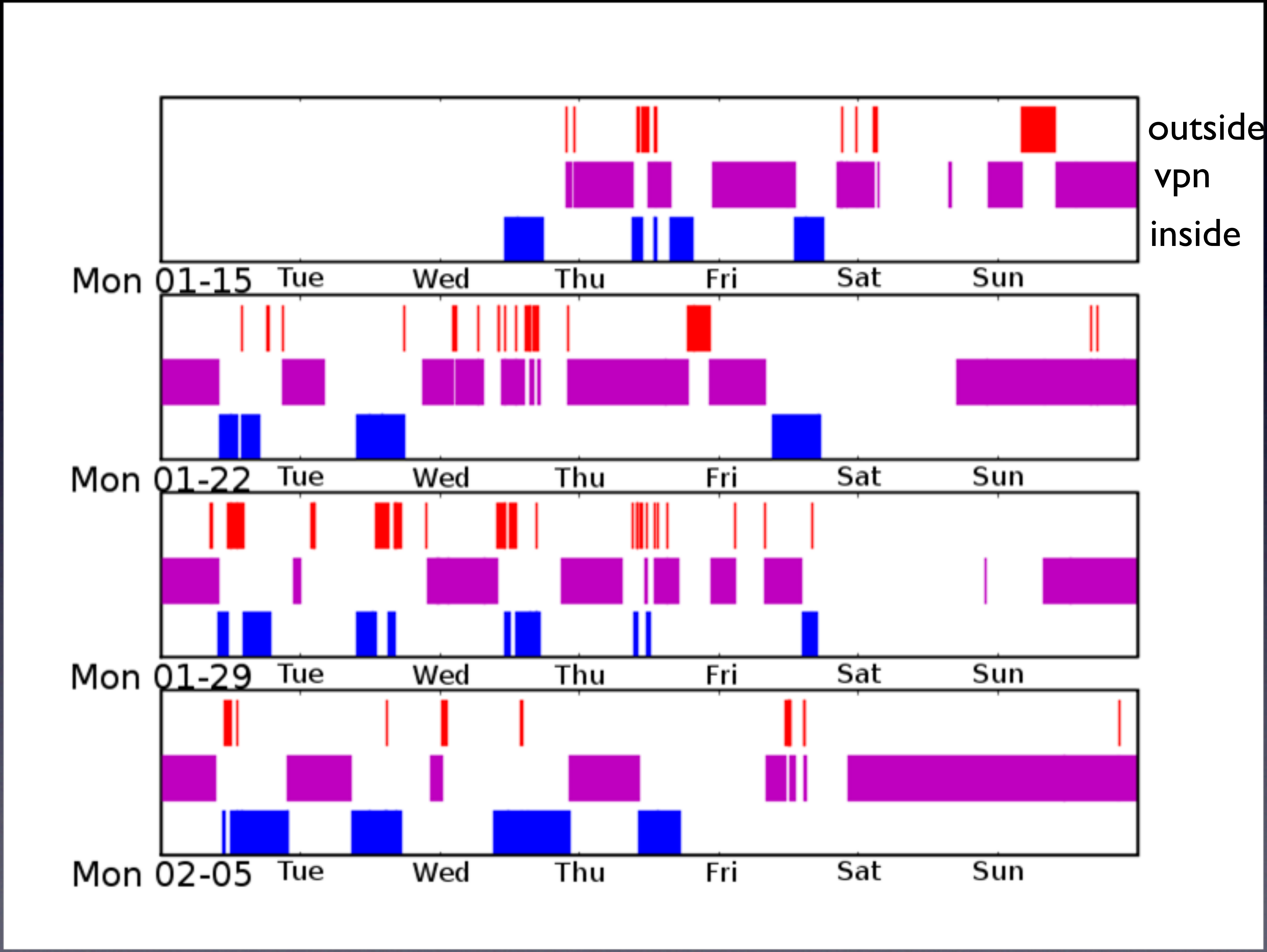
inside

- lots of protections
- well provisioned
- complete access to infrastructure services

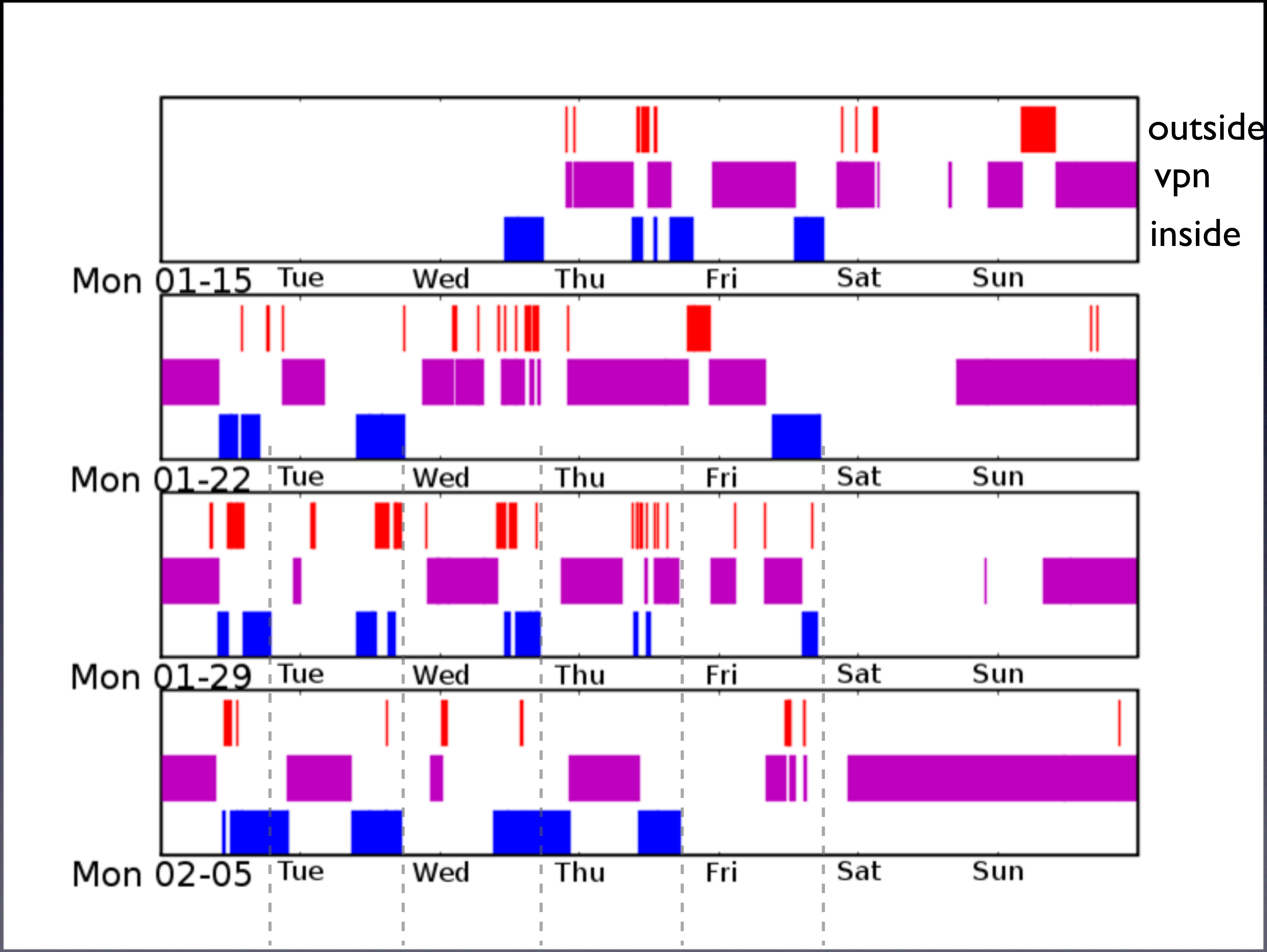
Questions

- How do users spend their time across environments
- Are there very big differences in protocol activity across the environments
- What are the differences in how various network services are used

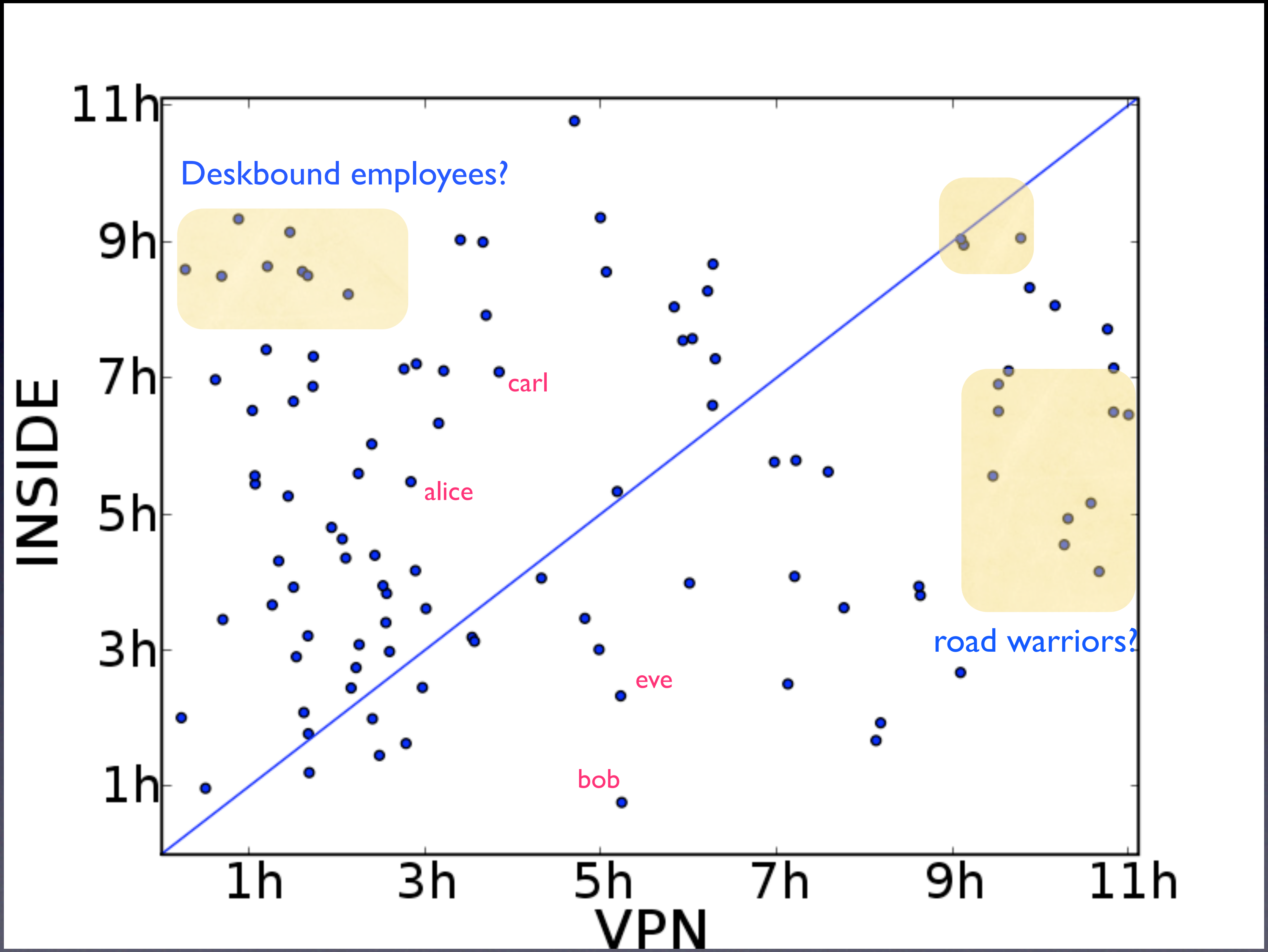
A month in the life of a laptop



A month in the life of a laptop



Environment Lifetimes

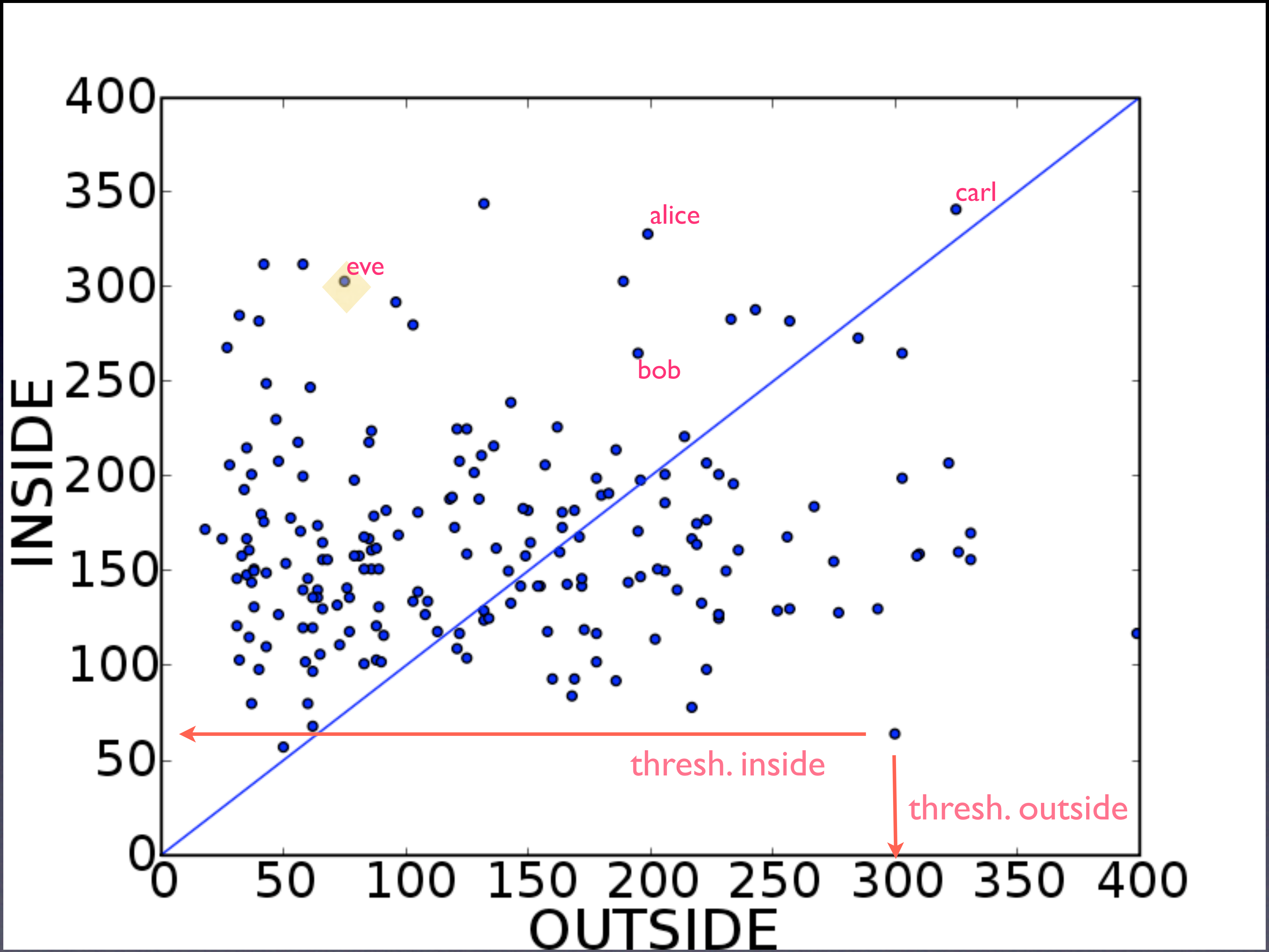


median time of “session”   (avg. diff =85%)

Questions

- How do users spend their time across environments
- Are there very big differences in protocol activity across the environments
- Differences in how various network services are used

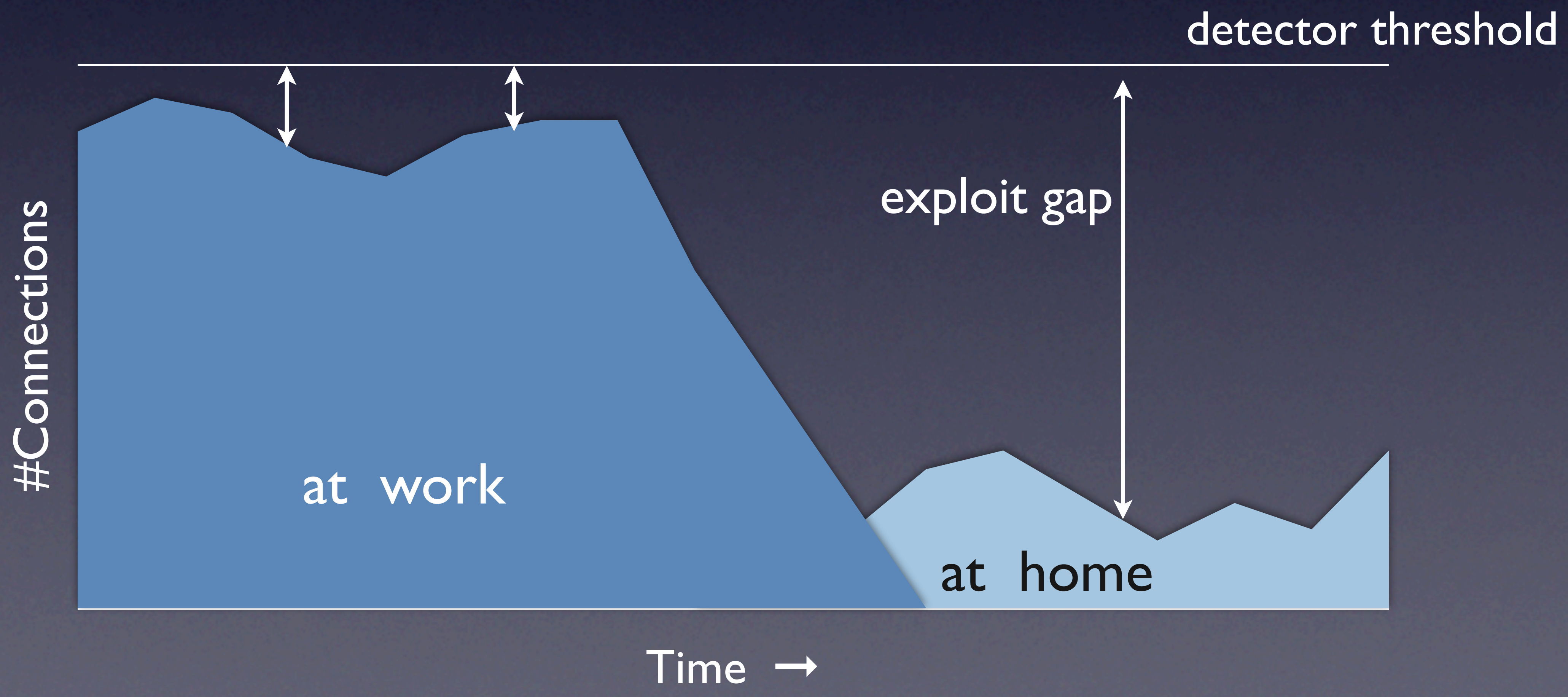
TCP usage (connections)



95th %-ile of connections/15 mins

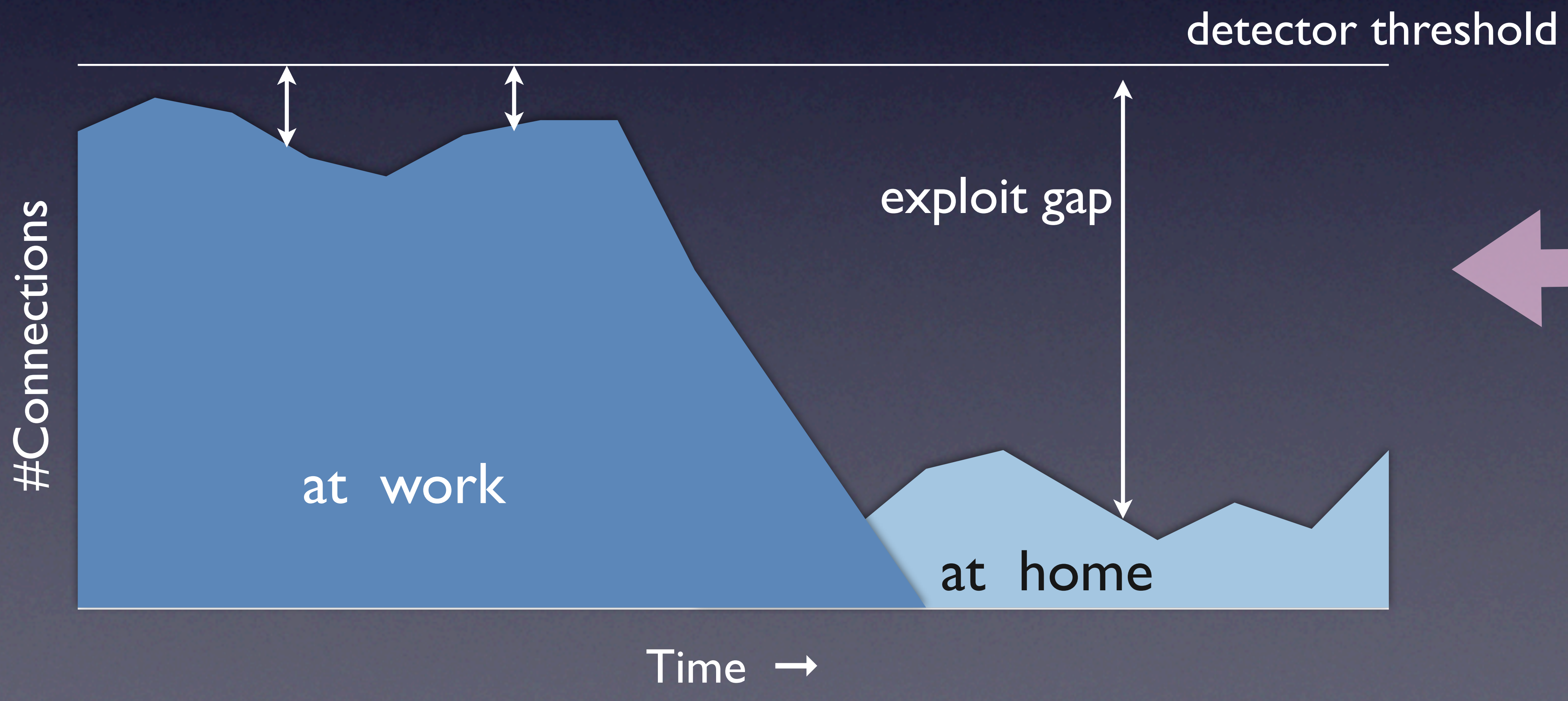
Variation creates “exploit gap”

Current security mechanisms ➡ static thresholds ignore location context ➡ allow a larger operating region for malicious traffic to go undetected



Variation creates "exploit gap"

Current security mechanisms → static thresholds ignore location context → allow a larger operating region for malicious traffic to go undetected



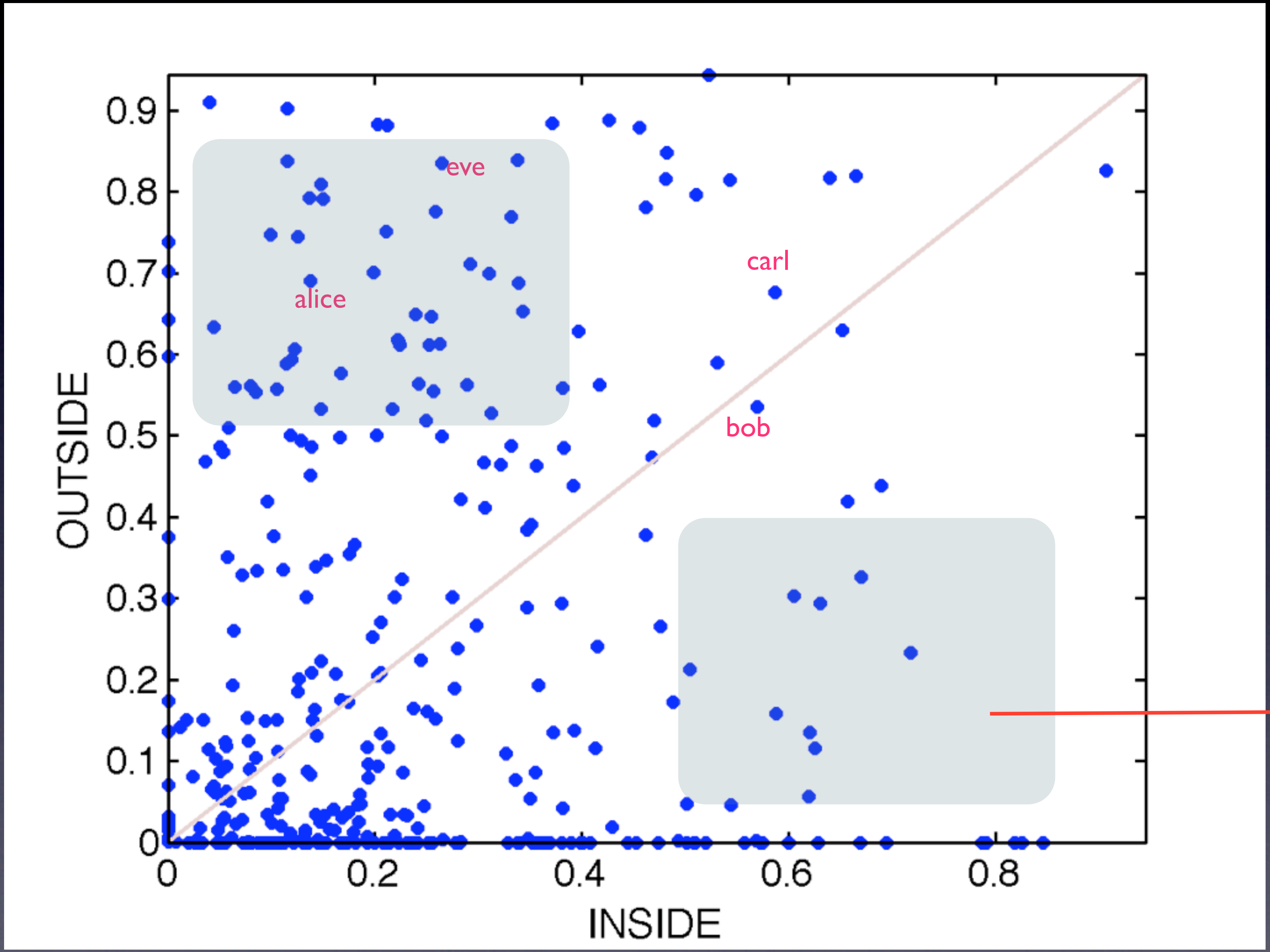
examples (conns/min)

Zapchast	(0–20)
SDbot C&C	(0–50)

Questions

- How do users spend their time across environments
- Are there differences in protocol activity across the environments
- Differences in how various network services are used

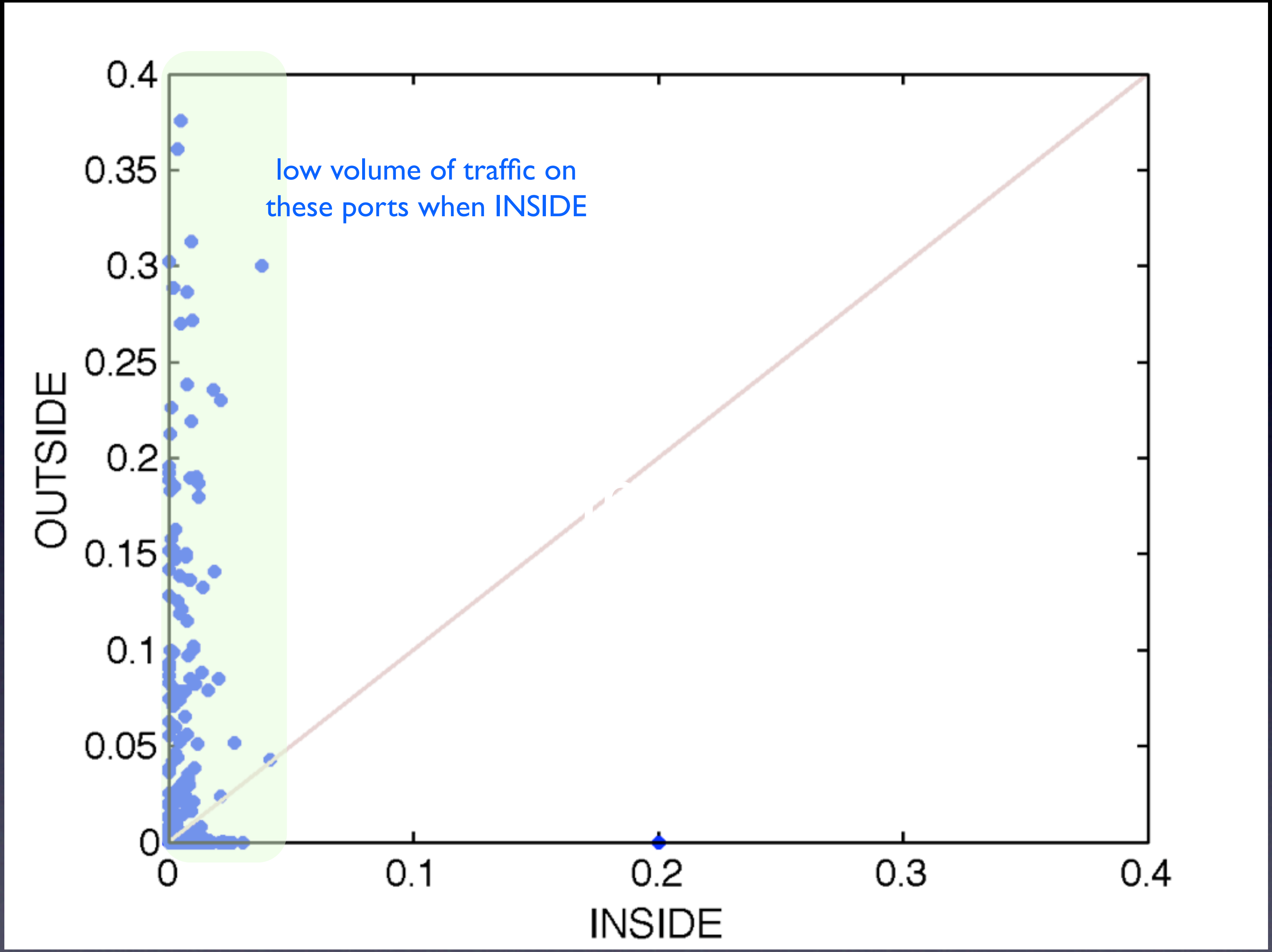
Network Services (ports)



relatively more http traffic when INSIDE

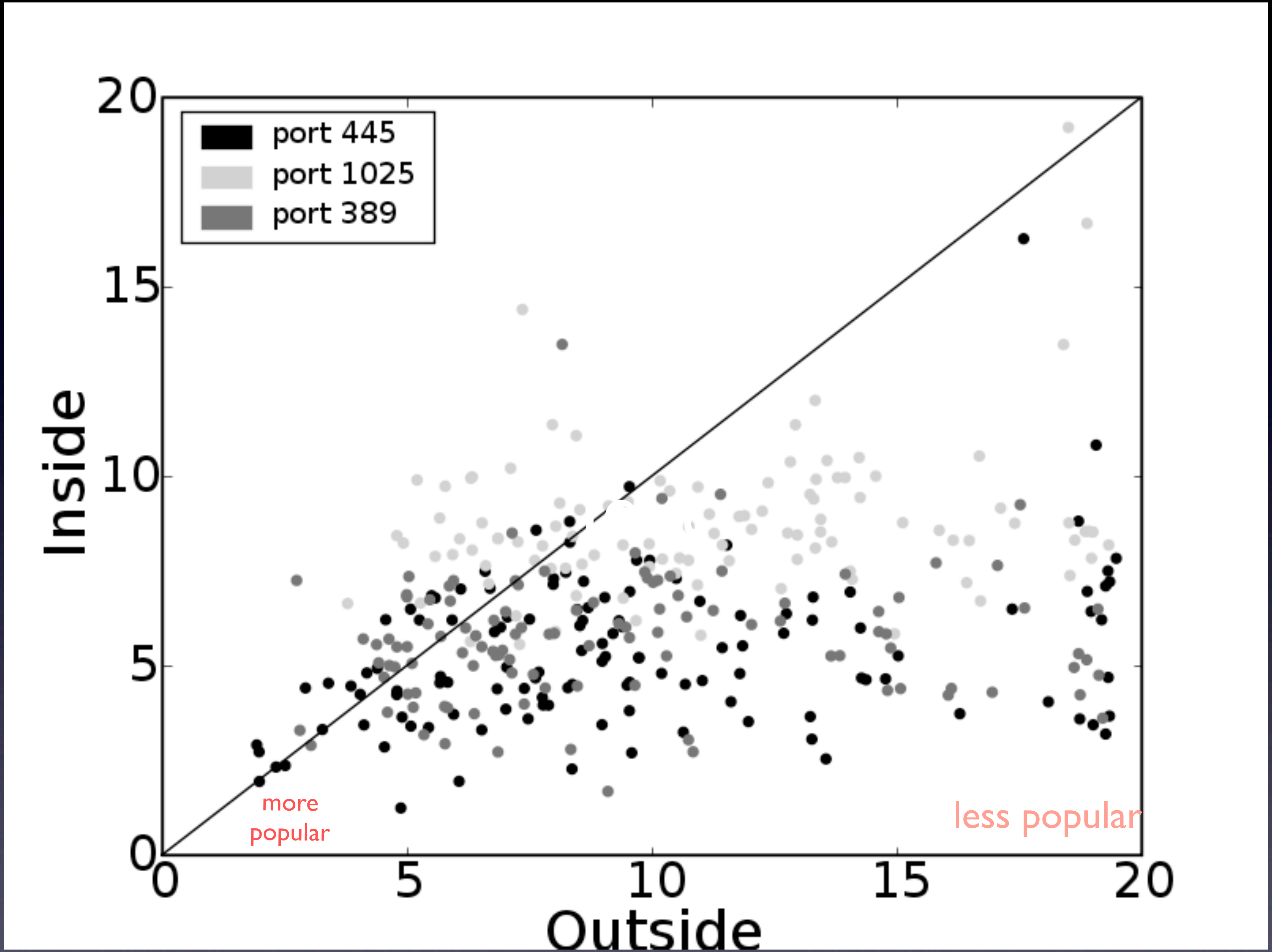
fraction of connections for web traffic (80,8080,8888)

Network Services (ports)



fraction of connections for Microsoft traffic

Network Services (ports)



a different view-- “popularity” of the protocols

Conclusions

- Behavior is drastically different across all the dimensions studied
- Profile constructed from averaged behavior not reflective of any particular environment
- No canonical user profile: users vary greatly from each other
- Security mechanisms need to be location aware to close “gaps” that can be exploited

Questions

Jaideep Chandrashekar

jaideep.chandrashekar@intel.com