292 - Fall 2021
Quantitative Information Flow and Side Channels

Instructor: Tevfik Bultan

Lecture 1

Pandemic Prologue

UCSB is transitioning back to In Person Instruction

Chancellor Yang's Memo, August 27

EVC Marshall's Memo, September 8

Academic Senate Chair Scott's

Divisional Newsletter, September 10

Divisional Newsletter, August 31

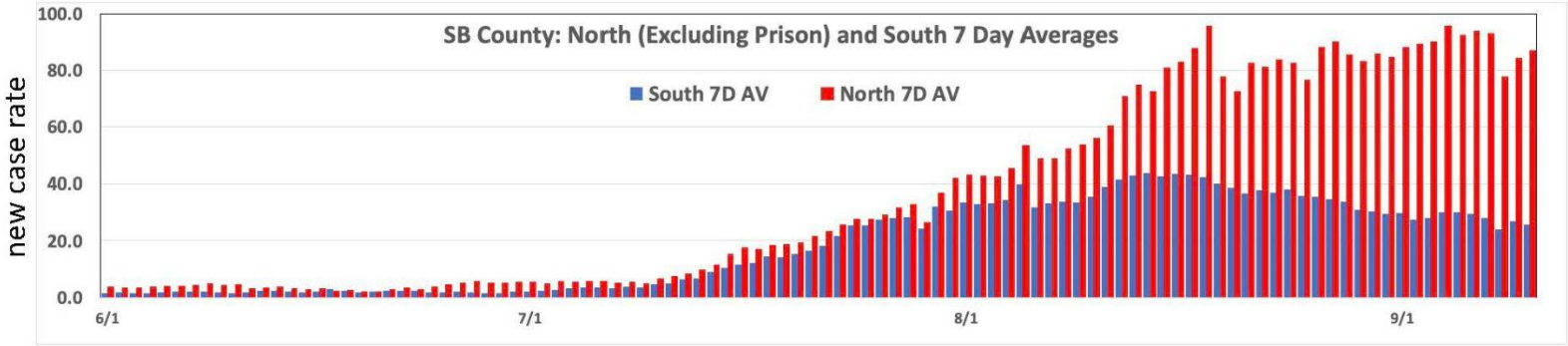
Instruction in Fall 2021

- In W21, President Drake announced that all UC campuses would return to "predominantly" in-person instruction by F21. Courses with prior approval to be offered online (designated "W" courses) may continue to be taught in this way.

- Since S21, the University has been planning how to bring students back to campus responsibly, including
  - widespread testing
  - vaccination
  - classroom preparation
  - face coverings

- The emergence of the Delta variant in late summer required a modification in our plans to allow limited exceptions to in-person teaching in Fall 2021:
  - instructors with verified medical accommodations
  - instructors living with immunocompromised family members or other household members
  - instructors temporarily unable to teach in-person due to their own quarantine/isolation, or a need to care for a child under the age of 12 who is required to quarantine/isolate

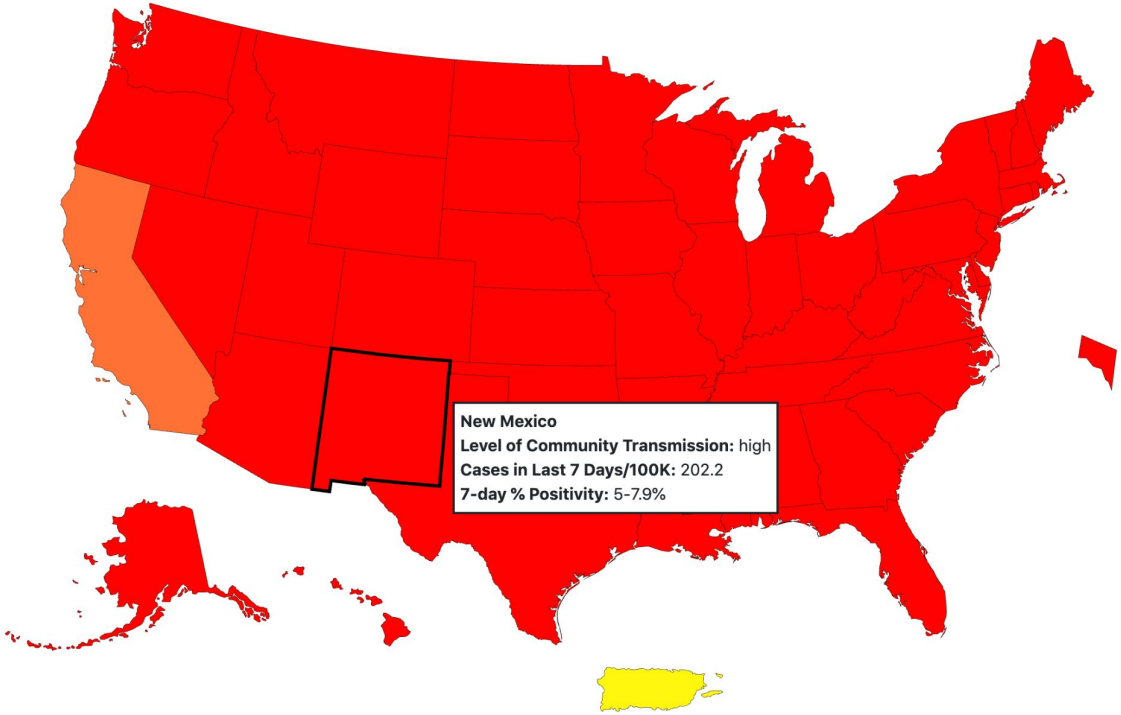
Current conditions and planning



The Academic Senate is

- monitoring local conditions (vaccination rate, case rate)
- consulting with medical advisors on the COVID-19 Working Group
- watching data and experiences from other California campuses
- communicating with instructors
- conducting contingency planning, including planning for a campus outbreak

Level of Community Transmission of COVID-19, by State/Territory



Territories

AS | FSM | GU | MP | PW | RMI | VI

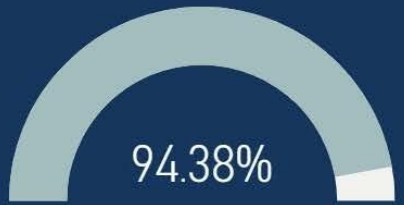
Level of Community Transmission

high | substantial | moderate | low | no data

CAMPUS OVERALL

Projected FALL 2021

Compliance Rate



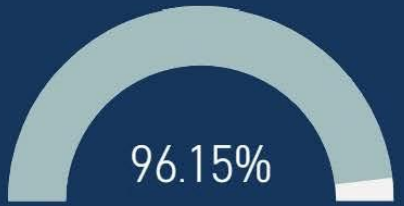
Vaccination Status

UC SANTA BARBARA

STUDENTS ONLY

Projected FALL 2021

Compliance Rate



Vaccination Status

UC SANTA BARBARA

Daily COVID-19 Screening Survey & Testing

- Clearance Badges incorporate COVID-19 vaccine compliance
- *Unvaccinated persons* must obtain weekly COVID-19 testing on campus
- All campus housing arrivals must obtain COVID-19 testing
  - Unvaccinated students must "sequester" for 7 days and obtain additional COVID-19 test on day 5 after arrival
- Non-Clearance Badges will show COVID-19 Isolation or Quarantine requirements

ACCESS TO **DAILY COVID-19 SCREENING SURVEY** and **CLEARANCE BADGES**

- Log in to UCSB Student Health Website "Patient Portal"

On Home Landing Page:
- Choose "Complete Survey" OR
- Choose "Show Badge"

- This is also where everyone can Schedule their COVID-19 testing appointments

- Dining Commons & RecCen will require Green Clearance Badges for entry
- Student Affairs Conduct Office will enforce non-compliance

UCSB COVID-19 Isolation & Quarantine

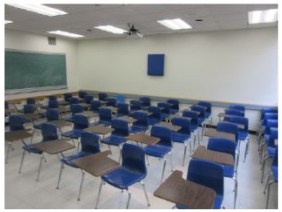
- **POSITIVE COVID-19 Test:** 10 days ISOLATION from date of symptoms or the positive test result
- **COVID-19 SYMPTOMS**
  - Fully Vaccinated: COVID-19 test and stay home until symptoms resolving and test negative
  - Unvaccinated: ISOLATE for 10 days, COVID-19 test useful
- **CLOSE CONTACT WITH CONFIRMED COVID-19 CASE**
  - Fully Vaccinated: COVID-19 test 3-5 days after exposure
  - Unvaccinated: QUARANTINE for 10 days, COVID-19 test useful
- **RECENT TRAVEL OUT-OF-COUNTRY**
  - Fully Vaccinated: COVID-19 test 3-5 days after ARRIVAL
  - Unvaccinated: QUARANTINE for 10 days, COVID-19 test 3-5 days

Exposure depends on many factors

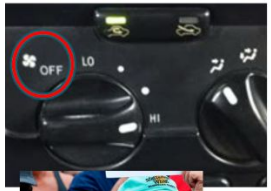
Exposure increases

Contagious Person:
Number and activity

Room volume



Ventilation



Masks
exhalation
inhalation

What has been done at UCSB?

- **Campus-wide HVAC:**
  - Inspected, repaired, upgraded >100 air handling systems
  - Walked every room on campus to ensure proper HVAC function
  - Set ventilation to maximum outside air intake
- **Instructional Spaces**
  - Identified all 323 rooms where Fall 2021 instruction will occur
    - 98 General Assignment
    - 225 Department/College
  - Compiled ventilation specs for instructional spaces (80% complete)
  - Assessed transmission risk in mechanically-ventilated rooms
    - 80% complete, remainder are known to be well ventilated
  - Flagged ~40 rooms with non-standard or no mechanical ventilation
    - Inspected each one individually.
    - Developing individualized strategy for each
    - May involve portable HEPA filters, CO_2 monitors for rooms, special operating instructions
  - Will implement and communicate mitigation strategies

Vaccination + Masking + Daily Surveys

Health & Wellbeing

Student Affairs Resources for You and Your Students

All services here are listed at wellbeing.ucsb.edu – please consider listing on syllabus

- Financial Crisis Response Team – financialcrisis@sa.ucsb.edu
- Basic Needs (Food, Housing, Technology) – food.ucsb.edu/resources/basic-needs-advocates
- Distressed Student Protocol – http://www.sa.ucsb.edu/responding-to-distressed-students/protocol
- Student Mental Health Coordinator Office – 805-893-3030; www.sa.ucsb.edu/ReferaGaucho
- Counseling and Psychological Services (CAPS) – https://caps.sa.ucsb.edu; CAPS Service Request Form online; 805-893-4411 (24/7, press 2 for a counselor)
- Student Health Service and Behavioral Health, including Social Workers – 805-893-5361
- Undocumented Student Services – 805-893-5609
- Alcohol/Drug Program – 805-893-5013
- CARE – 805-893-4613 (24/7 advocacy line)
- Health & Wellness – 805-893-2630
- Bias or Hate Incident Response – https://studentlife.sa.ucsb.edu/bias

See also www.sa.ucsb.edu/departments for a complete directory of Student Affairs departments and services.

Course Introduction

What is a side channel?

What is a side channel?

TIME

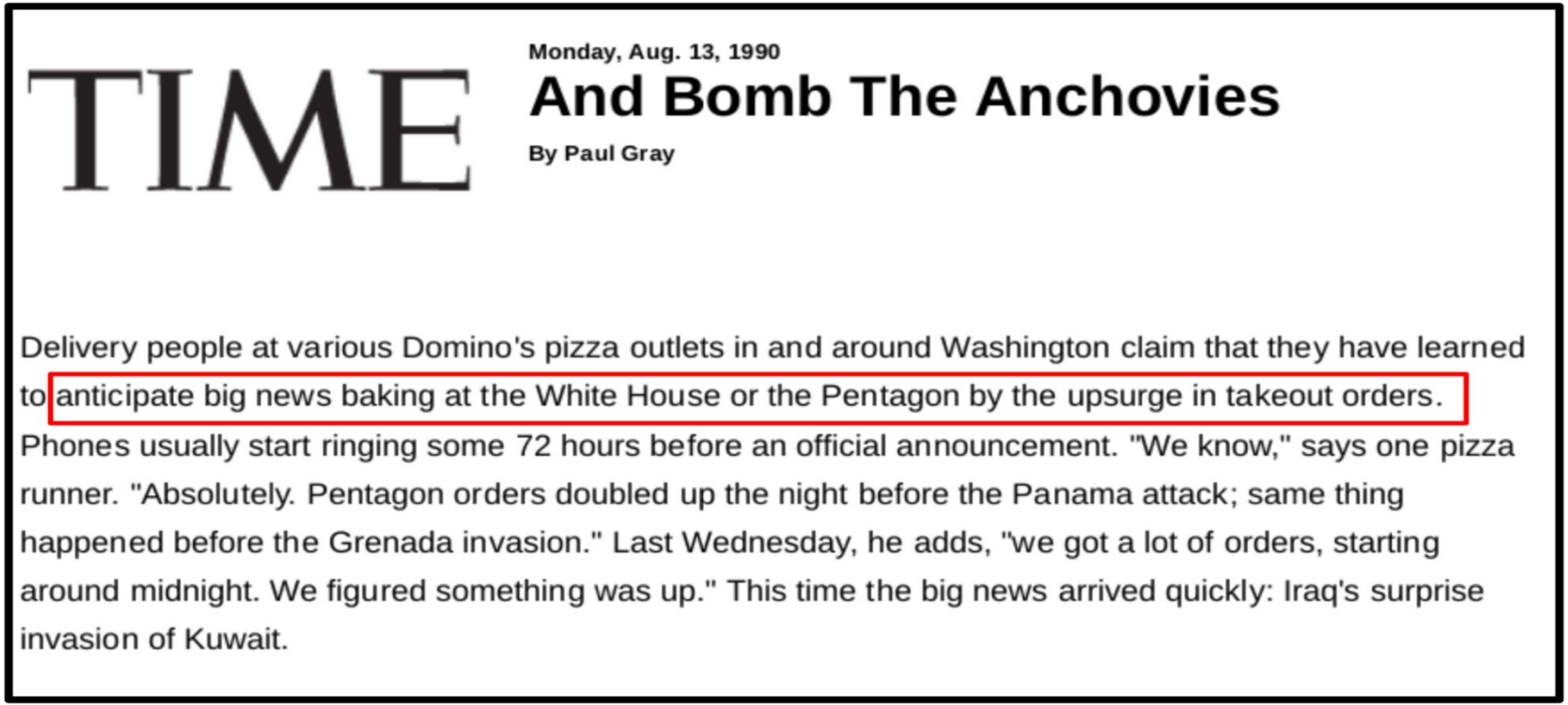
Monday, Aug. 13, 1990

And Bomb The Anchovies

By Paul Gray

Delivery people at various Domino's pizza outlets in and around Washington claim that they have learned to anticipate big news baking at the White House or the Pentagon by the upsurge in takeout orders. Phones usually start ringing some 72 hours before an official announcement. "We know," says one pizza runner. "Absolutely. Pentagon orders doubled up the night before the Panama attack; same thing happened before the Grenada invasion." Last Wednesday, he adds, "we got a lot of orders, starting around midnight. We figured something was up." This time the big news arrived quickly: Iraq's surprise invasion of Kuwait.

What is a side channel?



TIME

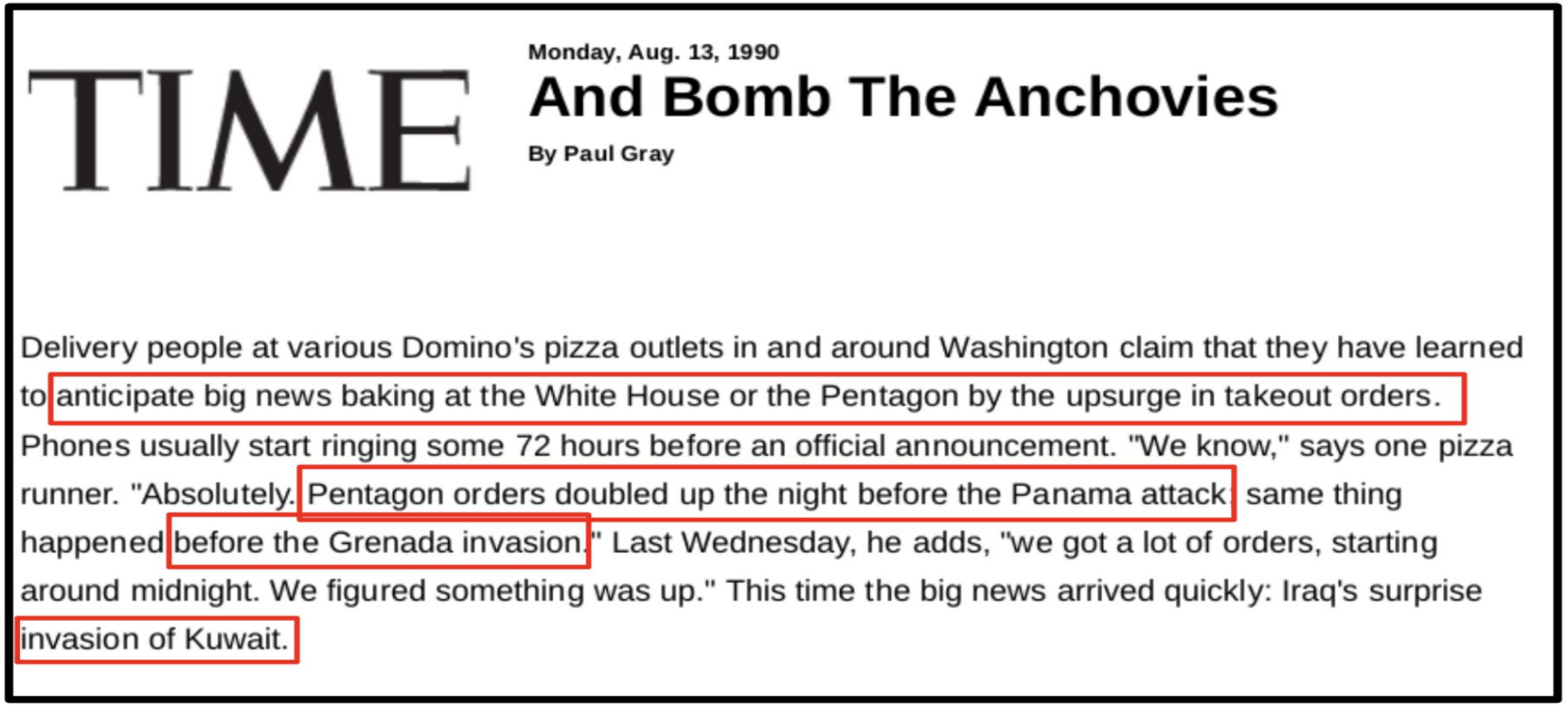
Monday, Aug. 13, 1990

And Bomb The Anchovies

By Paul Gray

Delivery people at various Domino's pizza outlets in and around Washington claim that they have learned to anticipate big news baking at the White House or the Pentagon by the upsurge in takeout orders. Phones usually start ringing some 72 hours before an official announcement. "We know," says one pizza runner. "Absolutely. Pentagon orders doubled up the night before the Panama attack; same thing happened before the Grenada invasion." Last Wednesday, he adds, "we got a lot of orders, starting around midnight. We figured something was up." This time the big news arrived quickly: Iraq's surprise invasion of Kuwait.

What is a side channel?



TIME

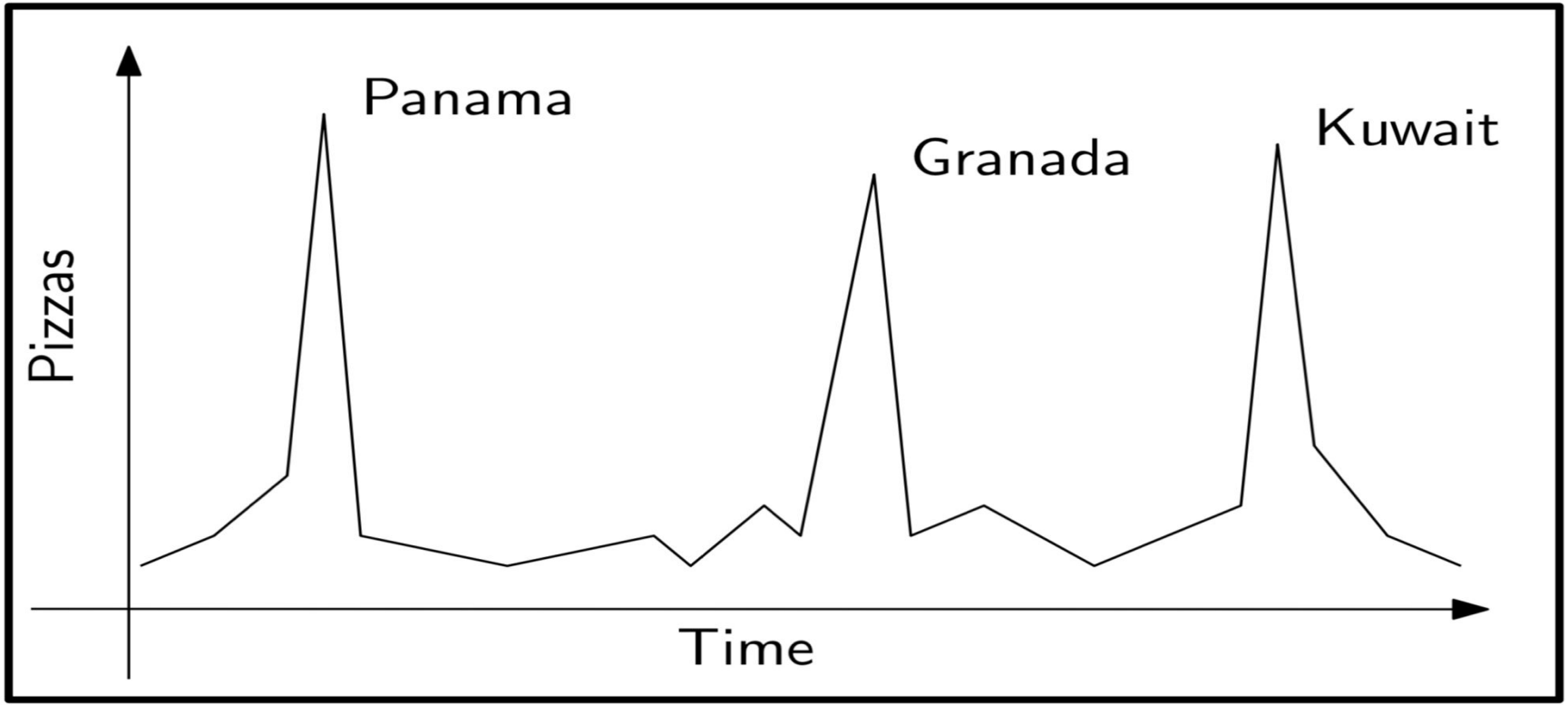
Monday, Aug. 13, 1990

And Bomb The Anchovies

By Paul Gray

Delivery people at various Domino's pizza outlets in and around Washington claim that they have learned to anticipate big news baking at the White House or the Pentagon by the upsurge in takeout orders. Phones usually start ringing some 72 hours before an official announcement. "We know," says one pizza runner. "Absolutely. Pentagon orders doubled up the night before the Panama attack, same thing happened before the Grenada invasion." Last Wednesday, he adds, "we got a lot of orders, starting around midnight. We figured something was up." This time the big news arrived quickly: Iraq's surprise invasion of Kuwait.

What is a side channel?



What is a side channel?

- Confidentiality: A program that manipulates secret information should not reveal that information
- Confidentiality can be hard to achieve
  - Especially if an attacker is able to observe different aspects of program behavior such as execution time and memory usage
- Side-channel attacks recover secret information from programs
  - by observing non-functional characteristics of program executions
    - such as execution time, memory usage, memory accesses, or packets transmitted over a network.

UCSB

Information leakage

```
if (password==guess) grant_access(); else print_error();
```

- This code leaks information about the secret password
- It leaks the information through the main channel (the output) of the program

Information leakage

In many cases some leakage it unavoidable:

- Any password checker leaks some information about the password
- Consider an electronic voting application, the result of the vote is public and it does leak information about the votes, but still individual votes should be private.

Information leakage

- One common way to model information leakage in programs is to separate the inputs and outputs of the program to different security levels

High: highly classified (secret)

Low: not highly classified (public)

- Then confidentiality means that information about High values should not be leaked to Low values

Non-interference

- Having no information leakage is characterized as non-interference, which means that:

  High values have no influence on Low values

Non-interference

- Let us assume that:
  - a program is a function from High and Low input values to High and Low output values where
  - f_L denotes the function that maps High and Low input values to the Low output value
  - H and L denote the domains of High and Low values

Then, we can state non-interference property (for deterministic programs) as:

$$\forall h_1 \in H, h_2 \in H, l \in L : f_L(h_1, l) = f_L(h_2, l)$$

Information leakage

- Non-interference for main channel can be checked using dependency analysis techniques:
  - Determine data and control dependencies among High and Low values and make sure that Low values do not depend on High values)
  - Determining non-interference for side-channels could be more difficult to figure out

Information leakage

- As we discussed, for many practical cases (such as password checking or electronic voting) non-interference is simply not possible and some information leakage from High values to Low values is unavoidable

Information leakage

- If leakage is unavoidable, then the question becomes:
  - “How much information is leaked?”
- For example, how much information about password can be obtained by the attacker who can enter different password guesses to the program
- If the amount leaked is very small, the program might be considered secure even though there is some information leakage

Quantitative information flow

- The goal of quantitative information flow techniques is to quantify the amount of information leaked from a given program

- Quantitative information flow techniques can also be used to detect the amount of information leaked from side channels

Some questions that we will discuss in this course

How should we quantify the information leakage?

How should we detect the amount of information leaked?

How should we specify properties related to information leakage?

Should we use static or dynamic analysis techniques?

Should we use symbolic or concrete analysis techniques?

If there is information leakage, can it be exploited to detect the secret information? How can it be exploited

Can we do these automatically?