CS 161 – Multilevel & Database Security

30 October 2006

Military models of security

- “Need to know”
- Three models of security
  - – Classification
    - unclassified, classified, secret, top secret
  - – Compartmentalization
    - nuclear, crypto, weapons specific
  - – Discretionary access control
    - Distribution lists

What clearance means

- Clearance is primarily a restriction on what you can release
- Declassification = permission to discuss
- Everyday example: Non-disclosure agreements

- Advice: Be careful before agreeing to clearance or NDAs

Two ways to rank systems

- How much do they protect military models of classification?

- What is the strength of mechanism

History

US

Orange book (Trusted Computer Security Evaluation Criteria) → TCSEC
Rainbow Series

Europe

Harmonized Criteria (UK, Germany, France, Holland) → ITSEC

Canada

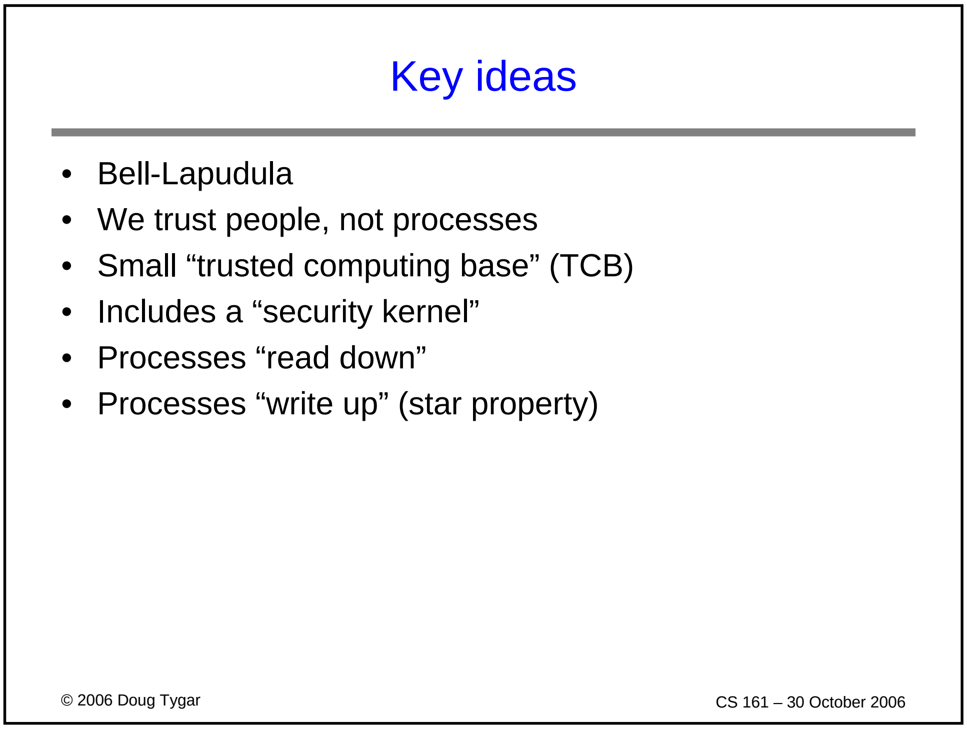
CTCPEC

Internationalization

Common Criteria (now on version 3.0)

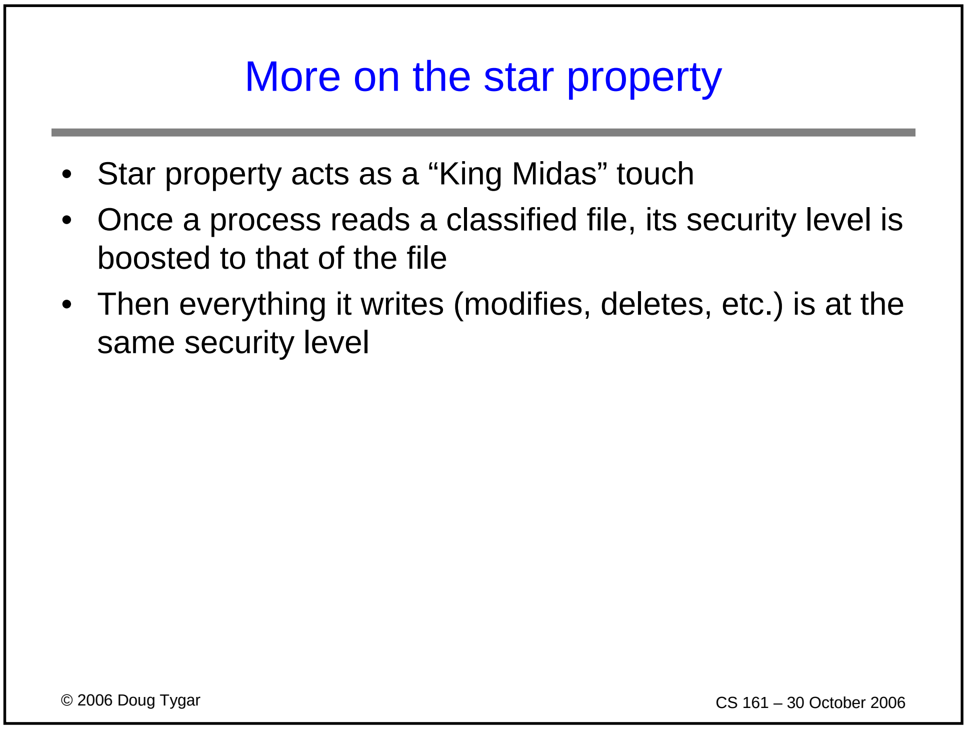
US levels

D : minimal protection
C1: discretionary access control
C2: controlled access control
B1: labeled security protection
B2: structured protection
B3: security domains
A1: verified design
A2: verified implementation (never achieved)



Key ideas

- Bell-Lapudula
- We trust people, not processes
- Small “trusted computing base” (TCB)
- Includes a “security kernel”
- Processes “read down”
- Processes “write up” (star property)



More on the star property

- Star property acts as a “King Midas” touch
- Once a process reads a classified file, its security level is boosted to that of the file
- Then everything it writes (modifies, deletes, etc.) is at the same security level

Problem: covert channels

- There is more than one way to leak information
  - Existence of a file
  - System load
  - Paging behavior
- Example: TENEX passwords

Covert channels

- Covert channels are virtually impossible to remove entirely
- So we restrict the bandwidth of what can transmitted
- This means that high-classification processes are heavily restricted

What killed the Orange Book?

- System performance was poor
  - Often 1,000 to 10,000 times worse than unsecure operating systems
- Using special hardware was expensive
- Formal methods for evaluation never really worked
- User interface was horrible
- Evaluation took years (and was expensive)

The last great evaluated system

- Windows NT was evaluated at the C-2 level of security … as long as you didn't hook it up to a network.

Today’s problems & the Orange book

- Problems we face today seem strangely distant from the Orange book
- Denial of service, worms, privacy, aggregation of data … none of these are addressed

Common Criteria

- Protection Profile
- Security Target

Common Criteria Levels

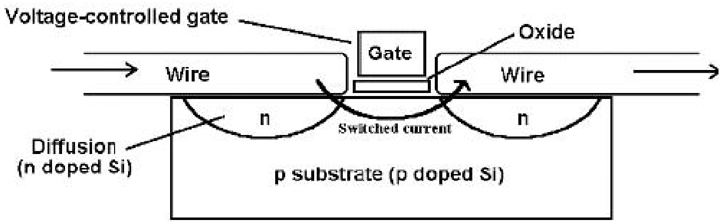
- EAL 1: functionally tested (US between D & C1)
- EAL 2: structurally tested (US C1)
- EAL 3: methodically tested & checked (US C2)
- EAL 4: methodically designed, tested, & reviewed (US B1)
- EAL 5: semiformally designed & tested (US B2)
- EAL 6: semiformally verified design & tested (US B3)
- EAL 7: formally verified design & tested (US A1)

Side channel examples

- Sound of keyboard typing
- Timing
- Power attacks

Power Analysis

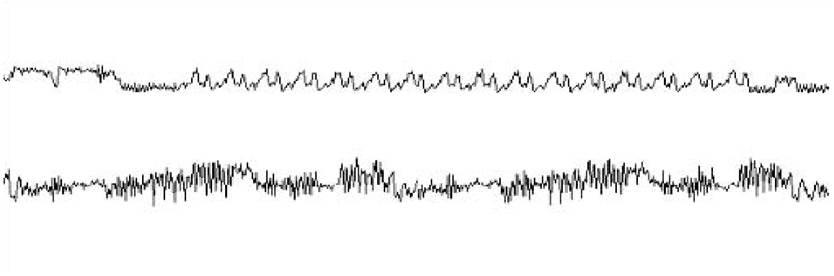
Figure: Typical MOS Transistor in an IC



nmos (n-channel) transistor

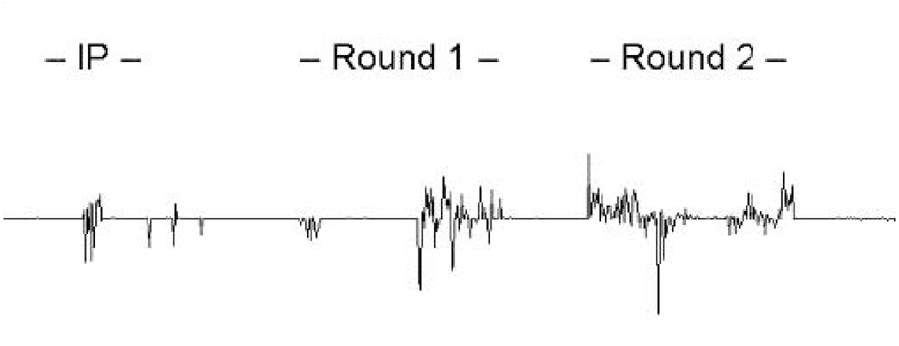
Simple Power Analysis

- Top line (DES)
- Bottom line (one cycle of DES)



Differential Power Analysis

- Repeat, and look for statistical averaging



Shamir secret sharing

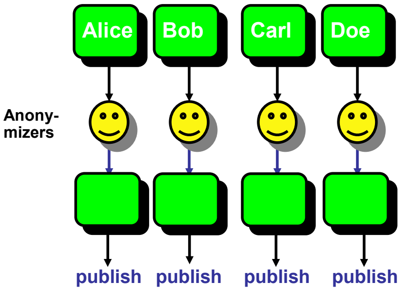
- How did this work

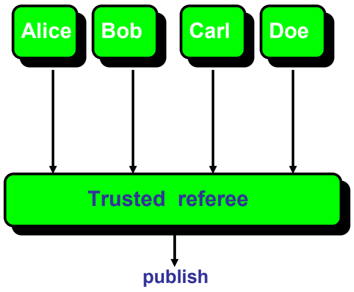
Adding with Shamir secret sharing

- Suppose we want to find everyone’s average salary

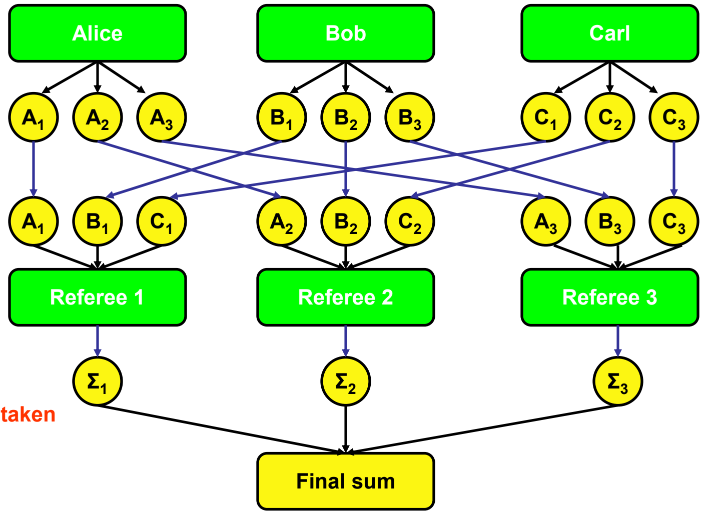
Unsatisfactory solutions to puzzle

- Mix approach:
  - Everyone sends salary anonymously to third parties who publish
- Escrow approach:
  - Everyone sends salary to trusted escrow agent





Using Shamir Secret Sharing



All sums taken modulo n

Census bureau problem

- Wants to publish average statistics
- But how do they change when a new person joins?

Approaches that don’t work

- Adding noise
  - Why not?
- Thresholding
  - Why not?

Census bureau problem

- Wants to publish average statistics
- But how do they change when a new person joins?

Approaches that don’t work

- Adding noise
  - Why not?
- Thresholding
  - Why not?
- Revealing Medians
  - Why not

Example

Name	Sex	Race	Aid	Fines	Drugs	Dorm
Adams	M	C	5000	45	1	Holmes
Bailey	M	B	0	0	0	Grey
Chin	F	A	3000	20	0	West
Dewitt	M	B	1000	35	3	Grey
Earhart	F	C	2000	95	1	Holmes
Fein	F	C	1000	15	0	West
Groff	M	C	4000	0	3	West
Hill	F	B	5000	10	2	Holmes
Koch	F	C	0	0	1	West
Liu	F	A	0	10	2	Grey
Majors	M	C	2000	0	2	Grey

- List NAME where SEX=M ∧ DRUGS=1
- List NAME where (SEX=M ∧ DRUGS=1) ∨ (SEX≠M ∧ SEX ≠ F) ∨ (DORM=AYRES)

Census rules

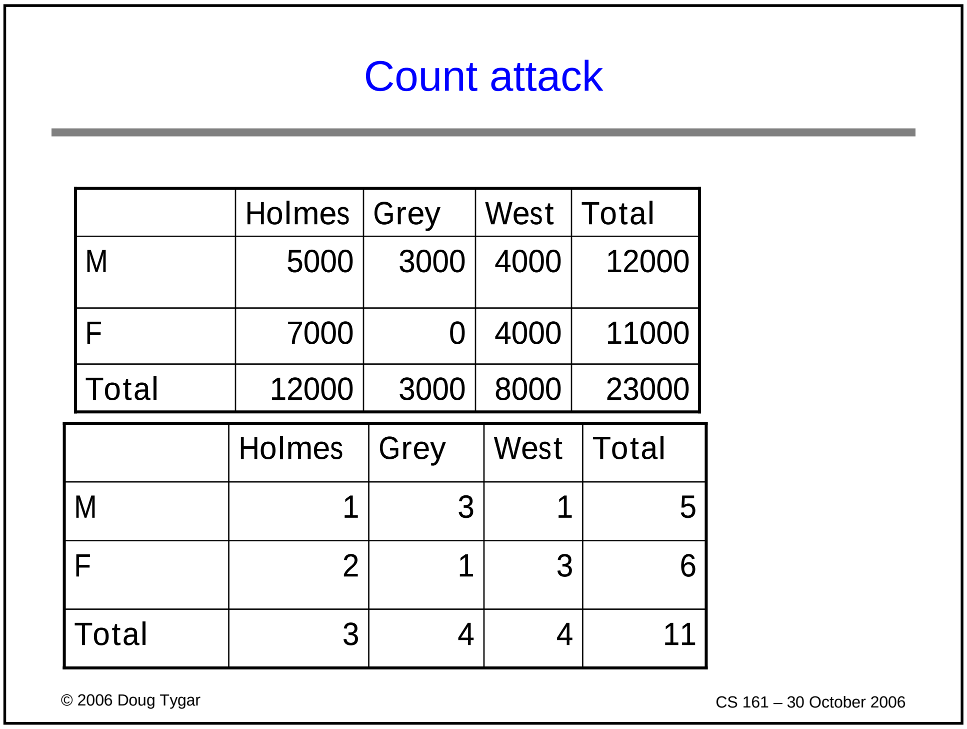
- “n items over k percent”
- Withhold data if n items represent over k percent of data reported.

Sum attack

- Sums of Financial Aid by Dorm and Sex

	Holmes	Grey	West	Total
M	5000	3000	4000	12000
F	7000	0	4000	11000
Total	12000	3000	8000	23000

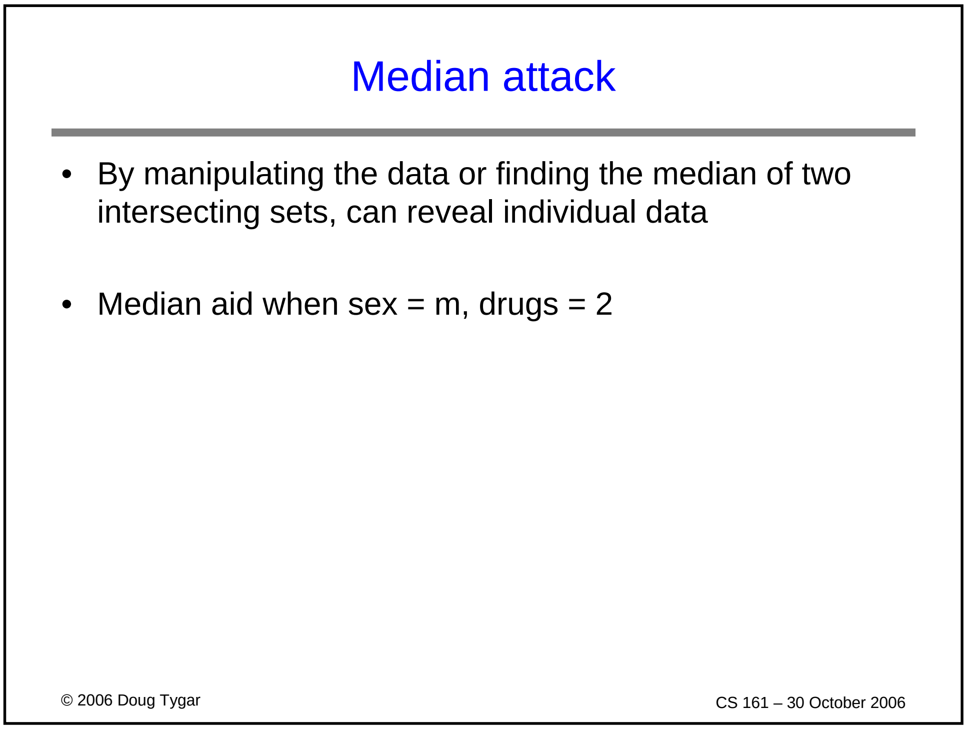
- Conclusion – no woman in Grey receives financial aid



Count attack

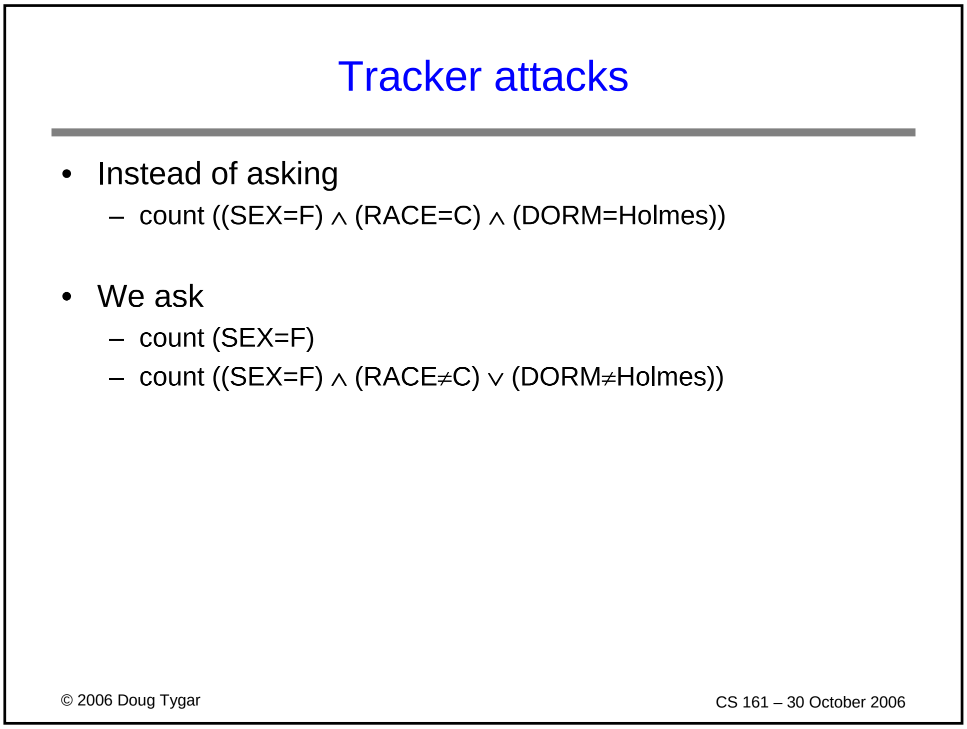
	Holmes	Grey	West	Total
M	5000	3000	4000	12000
F	7000	0	4000	11000
Total	12000	3000	8000	23000

	Holmes	Grey	West	Total
M	1	3	1	5
F	2	1	3	6
Total	3	4	4	11



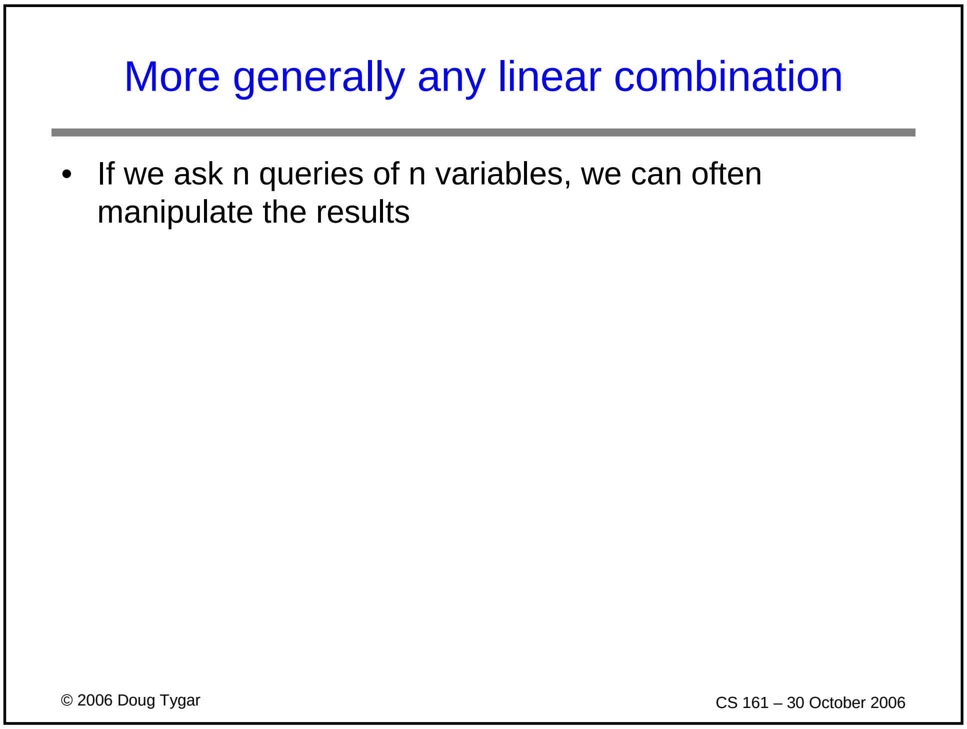
Median attack

- By manipulating the data or finding the median of two intersecting sets, can reveal individual data
- Median aid when sex = m, drugs = 2



Tracker attacks

- Instead of asking
  - count ((SEX=F) ∧ (RACE=C) ∧ (DORM=Holmes))
- We ask
  - count (SEX=F)
  - count ((SEX=F) ∧ (RACE≠C) ∨ (DORM≠Holmes))



More generally any linear combination

- If we ask n queries of n variables, we can often manipulate the results

Approaches to control

- Limited response supression
  - But vulnerable to trackers
- Combined results and rounding
  - Vulnerable to iterated queries
- Random sample
  - Inaccurate results, vulnerable to iterated queries
- Random data pertubation
  - Vulnerable to interated queries
- Query analysis
  - Really hard

Imperfect solutions for inference

- Suppress obviously sensitive information
- Track what the user knows
- Disguise the data