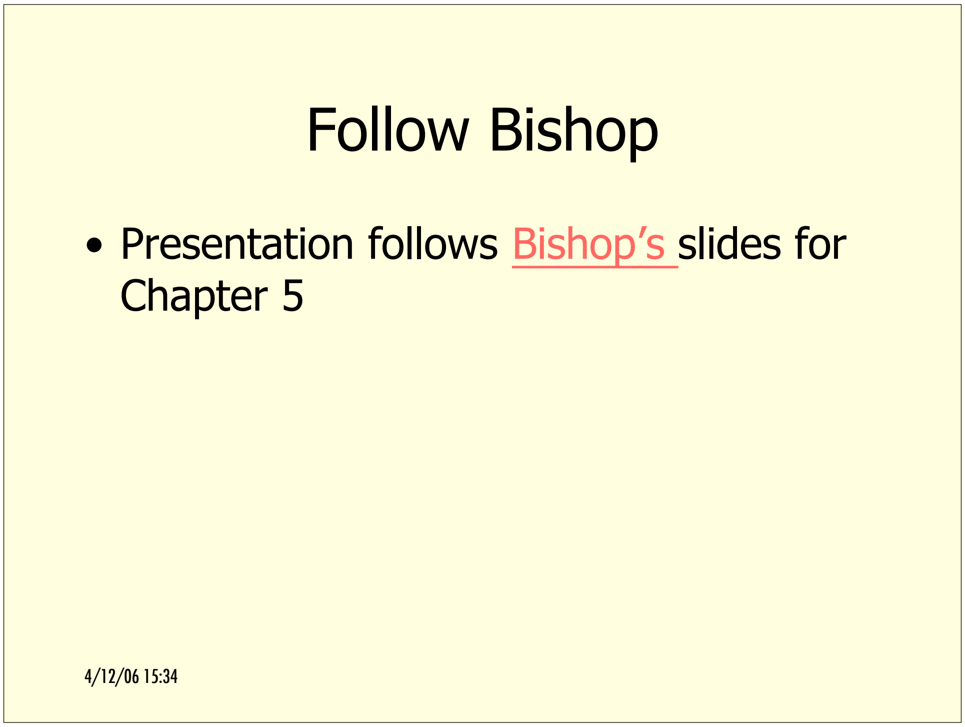
CS 591: Introduction to Computer Security

Lecture 4: Bell LaPadula

James Hook

Objectives

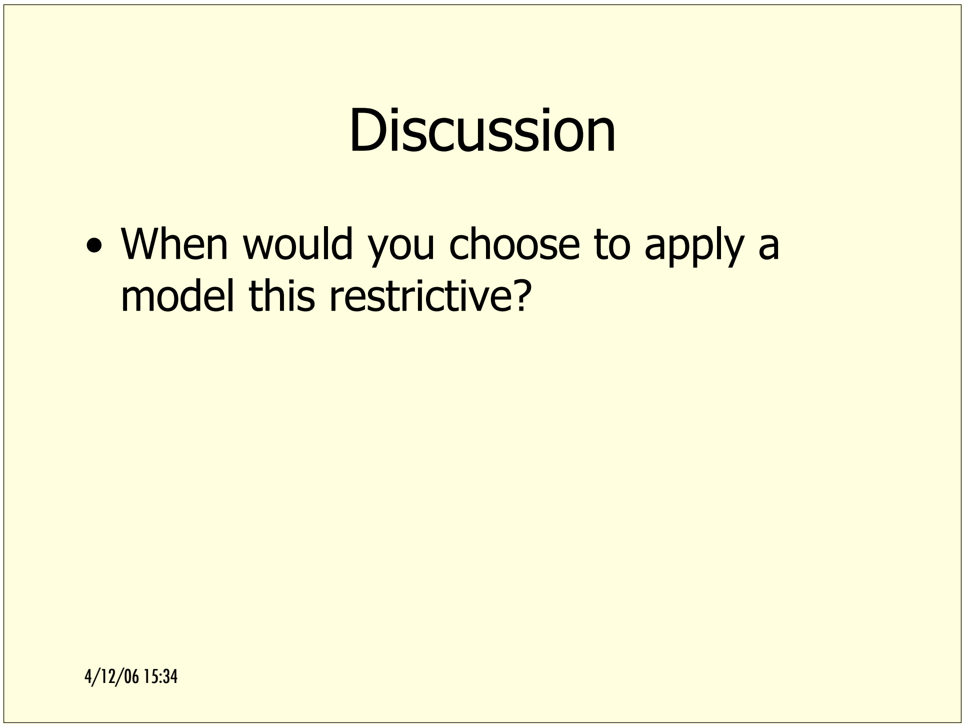
- Introduce the Bell LaPadula framework for confidentiality policy
- Discuss realizations of Bell LaPadula



Follow Bishop

- Presentation follows Bishop’s slides for Chapter 5

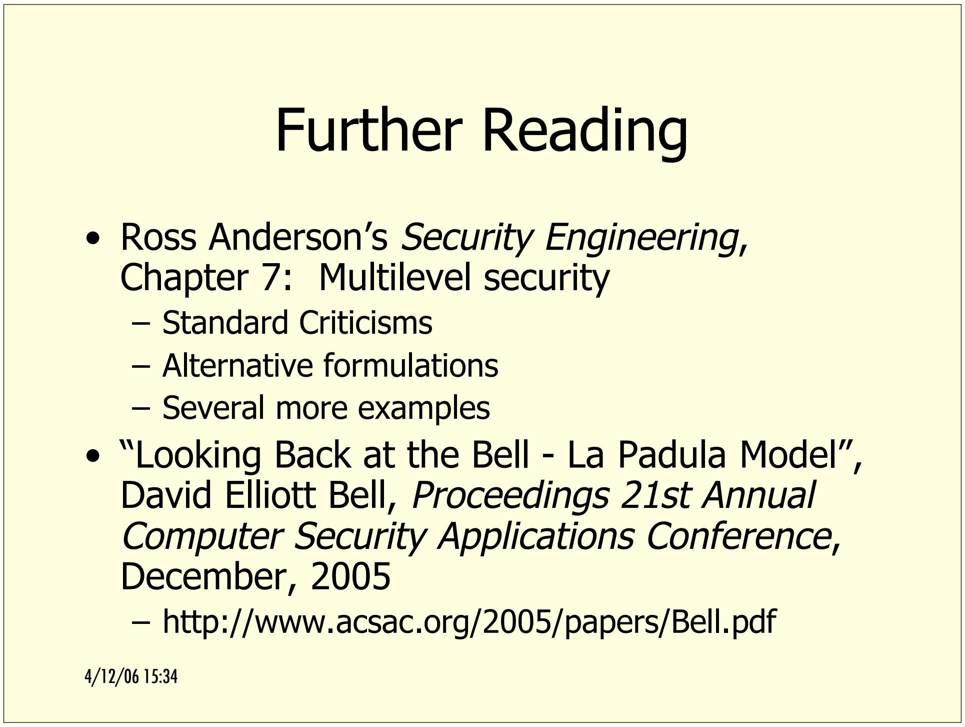
4/12/06 15:34



Discussion

- When would you choose to apply a model this restrictive?

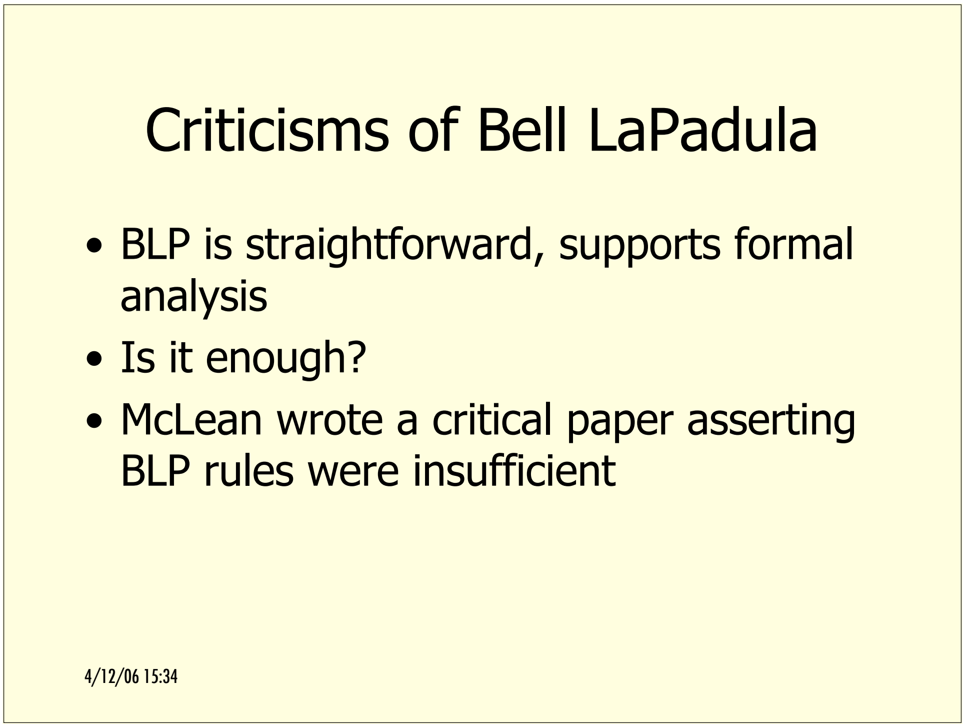
4/12/06 15:34



Further Reading

- Ross Anderson’s *Security Engineering*, Chapter 7: Multilevel security
  - Standard Criticisms
  - Alternative formulations
  - Several more examples
- “Looking Back at the Bell - La Padula Model”, David Elliott Bell, *Proceedings 21st Annual Computer Security Applications Conference*, December, 2005
  - http://www.acsac.org/2005/papers/Bell.pdf

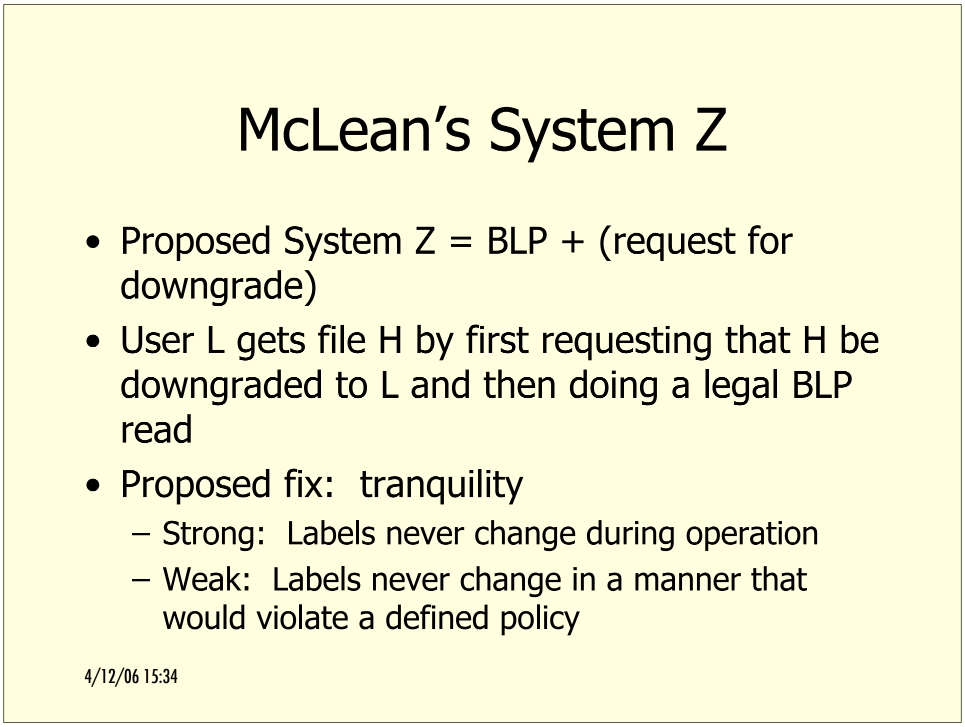
4/12/06 15:34



Criticisms of Bell LaPadula

- BLP is straightforward, supports formal analysis
- Is it enough?
- McLean wrote a critical paper asserting BLP rules were insufficient

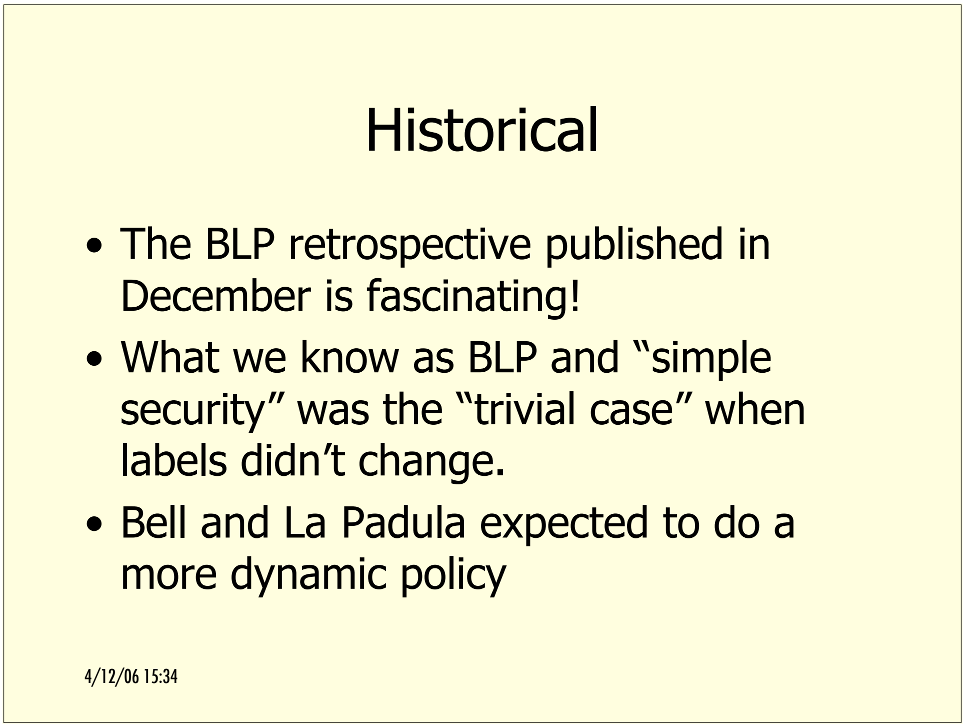
4/12/06 15:34



McLean’s System Z

- Proposed System Z = BLP + (request for downgrade)
- User L gets file H by first requesting that H be downgraded to L and then doing a legal BLP read
- Proposed fix: tranquility
  - Strong: Labels never change during operation
  - Weak: Labels never change in a manner that would violate a defined policy

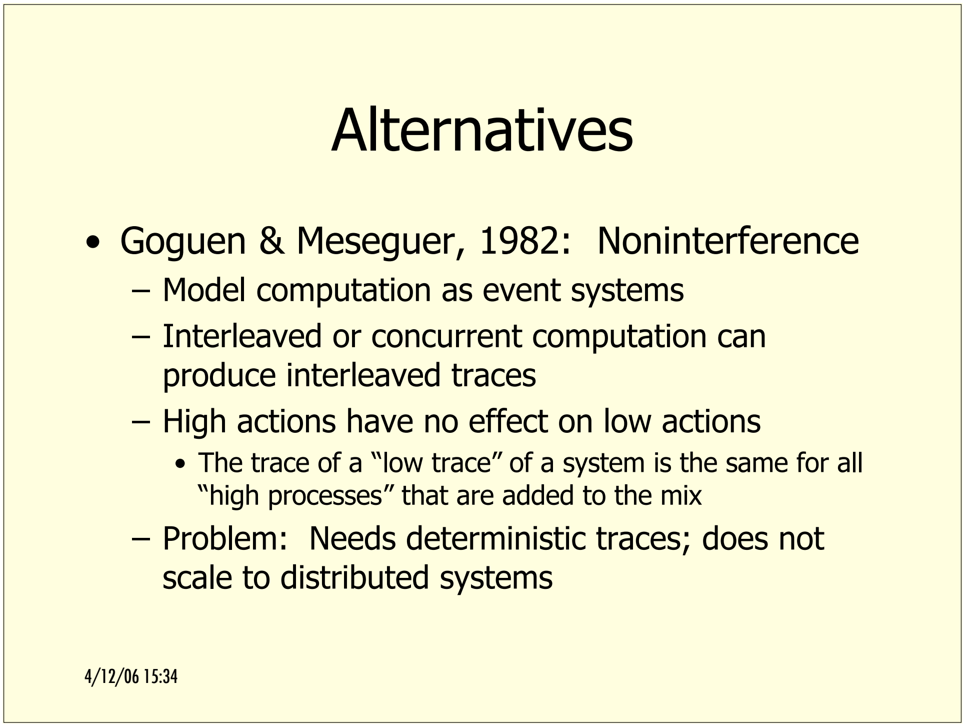
4/12/06 15:34



Historical

- The BLP retrospective published in December is fascinating!
- What we know as BLP and “simple security” was the “trivial case” when labels didn’t change.
- Bell and La Padula expected to do a more dynamic policy

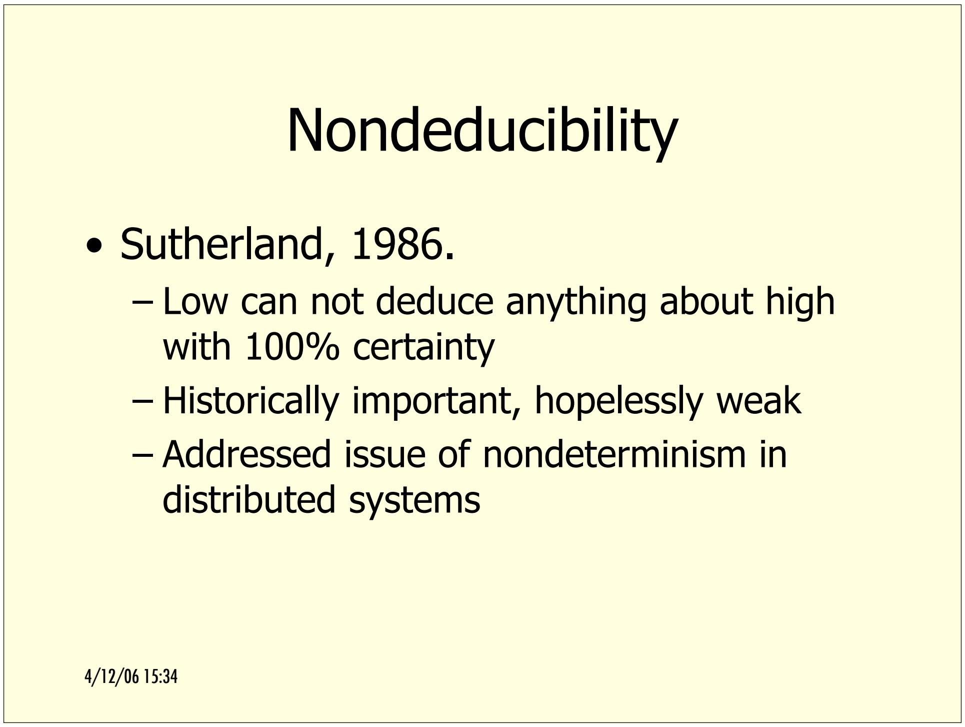
4/12/06 15:34



Alternatives

- Goguen & Meseguer, 1982: Noninterference
  - Model computation as event systems
  - Interleaved or concurrent computation can produce interleaved traces
  - High actions have no effect on low actions
    - The trace of a “low trace” of a system is the same for all “high processes” that are added to the mix
  - Problem: Needs deterministic traces; does not scale to distributed systems

4/12/06 15:34



Nondeducibility

- Sutherland, 1986.
  - Low can not deduce anything about high with 100% certainty
  - Historically important, hopelessly weak
  - Addressed issue of nondeterminism in distributed systems

4/12/06 15:34

Intranstitive non-interference

- Rushby, 1992
  - – Updates Goguen & Meseguer to deal with the reality that some communication may be authorized (e.g. High can interefere with low if it is mediated by crypto)

Looking forward

- Chapter 6: Integrity Policies