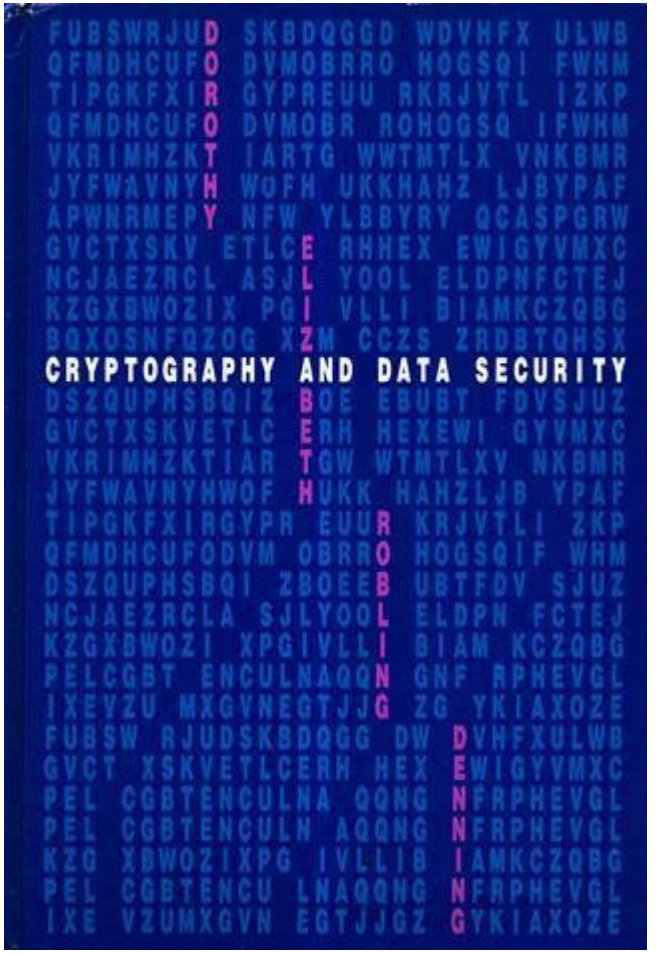
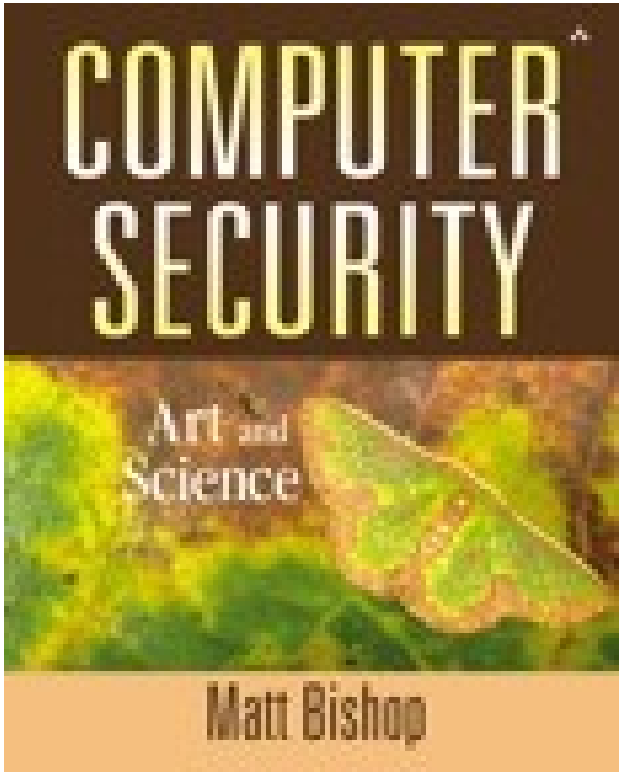
Information flow and policy


CRYPTOGRAPHY AND DATA SECURITY
DOROTHY
ELIZABETH
ROBLING
DENNING


COMPUTER
SECURITY
Art and
Science
Matt Bishop

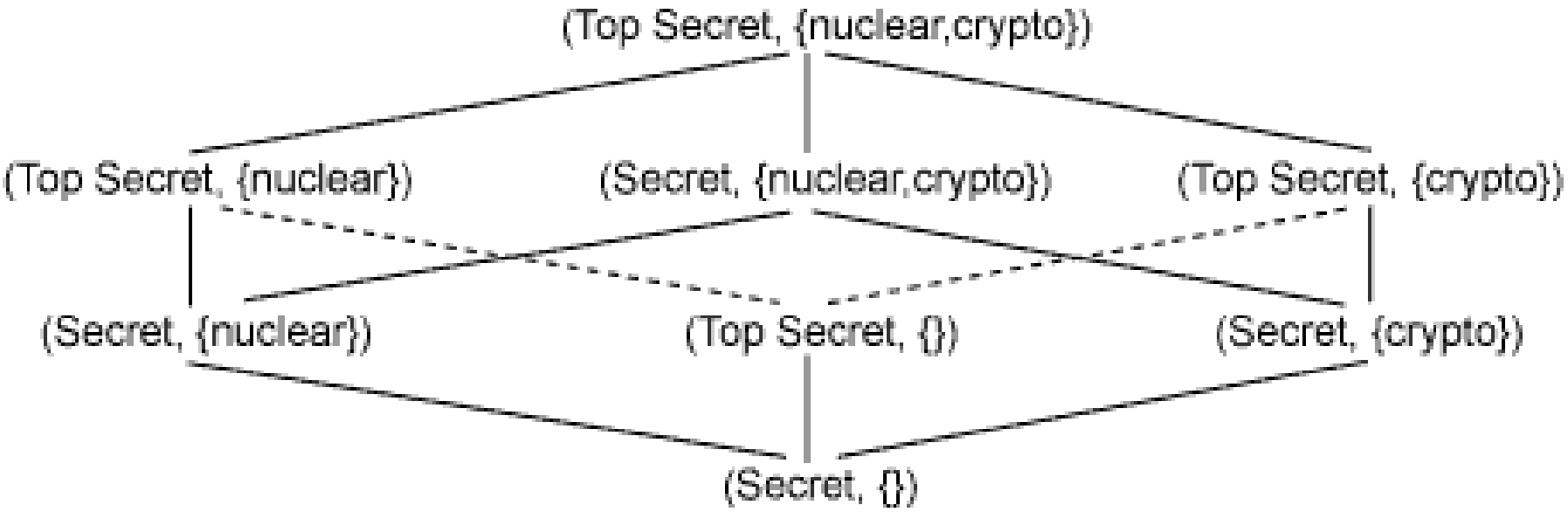
Foundational results

- Access Control Matrix
  - Formally undecidable if a right leaks
- Take-grant model
  - Transitive closure

Policies

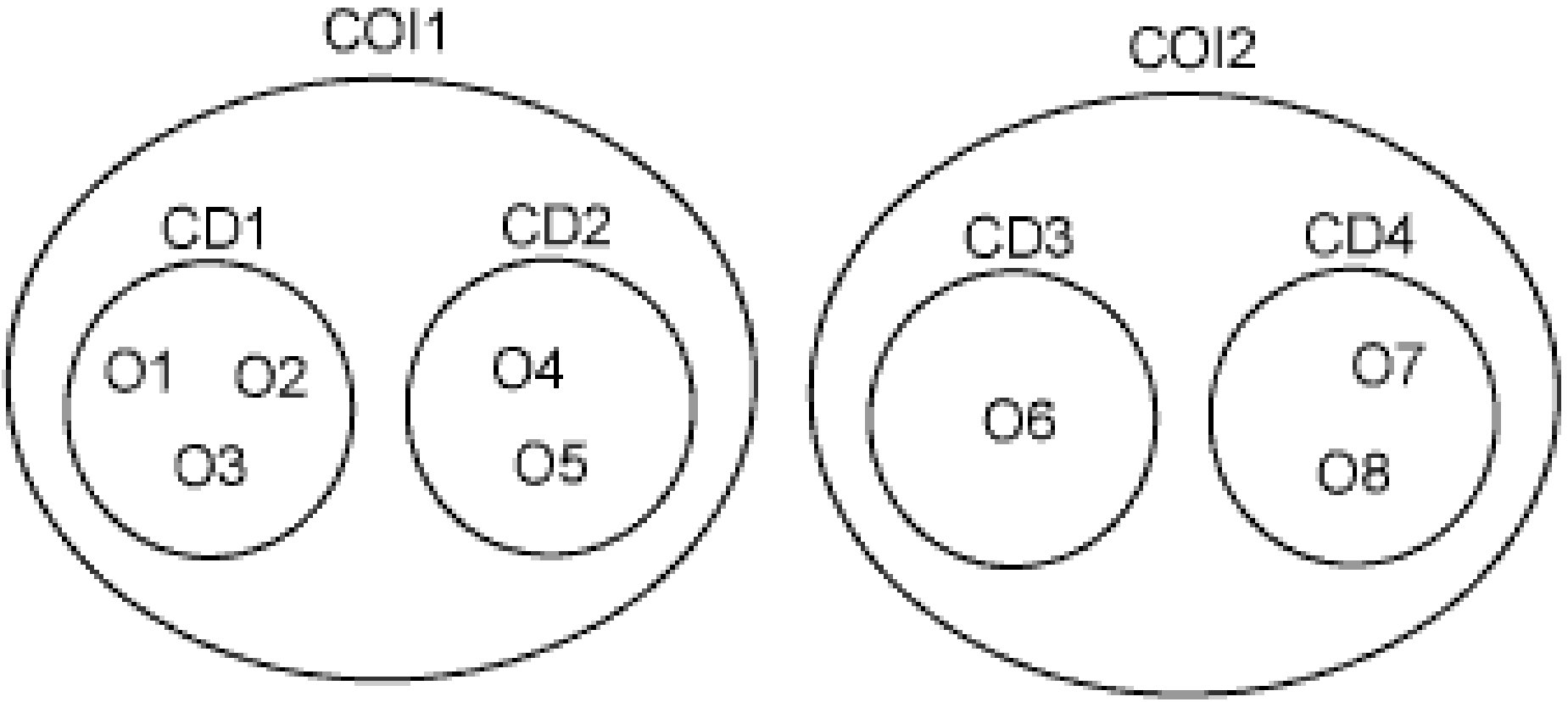
- Confidentiality
  - Bell-LaPadula: no reads up, no writes down
- Integrity
  - Biba's low-water-mark policy (if you read it, your integrity becomes the minimum of what it is already and that of what you read)
  - Biba's ring policy (read if you're interested)
  - Biba's Model (Bell-LaPadula upside down)
  - Lipner (read if you're interested) and Clark-Wilson (for business)
- ~~Availability~~ Hybrid Policies
  - Chinese Wall model (for conflicts of interest)
  - CISSP (had its acronym stolen)

Lattice = partial ordering



Plagiarized from
http://www.cs.cornell.edu/courses/cs5430/2012sp/mls.gif

Chinese Wall Model



Plagiarized from http://www.cs.cornell.edu/courses/cs5430/2012sp/chinWall.gif

Mechanisms

- Mandatory Access Control
  - System won't let users change, like SELinux
- Discretionary Access Control
  - Users can change, like UNIX file permissions
- Capabilities *vs.* access control lists
- Weak Windows DACLs is a fascinating topic
  - https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2013/november/windows-dacls-why-there-is-still-room-for-interest/
  - *Gray Hat Hacking, 4th Edition* by Harper *et al.*
  - https://www.blackhat.com/presentations/bh-dc-07/Cerrudo/Paper/bh-dc-07-Cerrudo-WP.pdf

Information flow

- Multi-Level Security (Top Secret, Secret, Unclassified, *etc.* all on the same machine)
  - Kind of a stupid idea (think rainbow series)
- Noninterference (Goguen and Meseguer in 1982)
  - “A computer has the non-interference property if and only if any sequence of low inputs will produce the same low outputs, regardless of what the high level inputs are.” (https://en.wikipedia.org/wiki/Non-interference_(security))

Information flow (continued)

- Denning's Lattice-based access control (1976)
- Fenton's Data Mark Machine (1974)
- Dynamic Information Flow Tracking (Suh *et al.*, ASPLOS 2004, Crandall and Chong MICRO 2004)
  - *A.k.a.* Dynamic Taint Analysis (Newsome and Song 2005)
  - Indirect flows are a problem

```
x = A[y]        if (y==1)
                  X = 1
```

Implicit flows

```
if (y == 1)
    x = 1
```

Even if y != 1, information flows from y to x

Covert channels

- Confinement problem
  - Defined by Lampson in 1973
- Covert channel = path of communication that was not designed to be used for communication [Bishop, Chapter 17]
- Lipner (1975) distinguishes between timing channels and storage channels
  - Kemmerer's (1983) Shared Resource Matrix Methodology can be used for storage channels, basically a transitive closure
  - Wray (1992) considered timing channels, can compare all pairs of “clocks”

Examples of covert channels

- Hard drive timings
- Locks

Side channels

- Covert channels assume *collusion*
- Side channels can be used to infer information
  - Key stroke timings leaking through entropy pool (Silence on the Wire by *Zalewski*)
  - Keyboard Acoustic Emanations https://www.davidsalomon.name/CompSec/auxiliary/KybdEmanation.pdf
  - Cache missing for fun and profit http://www.daemonology.net/papers/cachemissing.pdf
- “Information wants to be free”

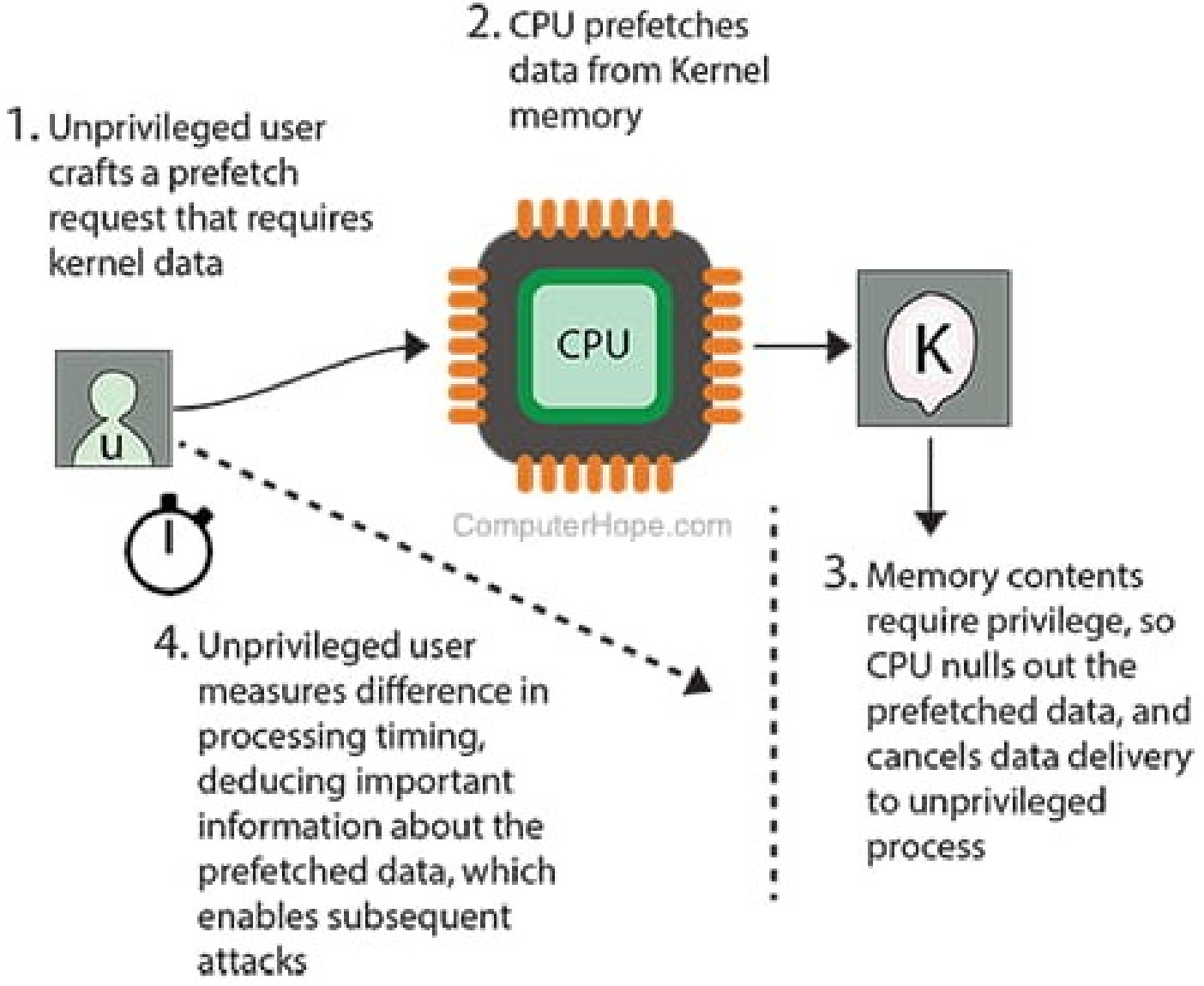
Examples of side channels

- Microarchitectural
- TCP/IP side channels
- Crypto timing channels in power, over the network, *etc.*

Thomas Jefferson said...

“That ideas should freely spread from one to another over the globe, for the moral and mutual instruction of man, and improvement of his condition, seems to have been peculiarly and benevolently designed by nature, when she made them, like fire, expansible over all space, without lessening their density in any point, and like the air in which we breathe, move, and have our physical being, incapable of confinement or exclusive appropriation.”

Generalization of a Meltdown attack



https://www.computerhope.com/jargon/m/meltdown-and-spectre.htm

Resources

- *Cryptography and Data Security* by Dorothy Elizabeth Denning
- *Computer Security: Art and Science* by Matt Bishop
- The Light Pink Book
- https://www.youtube.com/watch?v=kO8x8eoU3L4