MULTILATERAL SECURITY

Based on chapter 9 of “Security Engineering” by Ross Anderson

Presenter: Omer Paparo – עומר פפרו

Outline

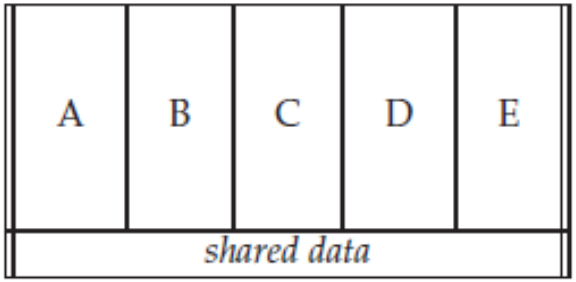
- Introduction
- Motivation
- Data flow models
  - Compartmentation and the lattice model
  - The Chinese wall model
  - The British Medical Association (BMA) model
- Inference control
  - What is Inference control?
  - Control types
  - Limitations of generic approaches
- The residual problem
- Summary

What is multilateral security?

- In one sentence: controlling information flow across a database or shared data
  - Ideally, anyone will have access to exactly what he needs, and nothing more
  - This is not so easy, as we will See
- Centralization of systems makes this issue critical

Multilevel security

Credit: “Security Engineering” by Ross Anderson



Multilateral security

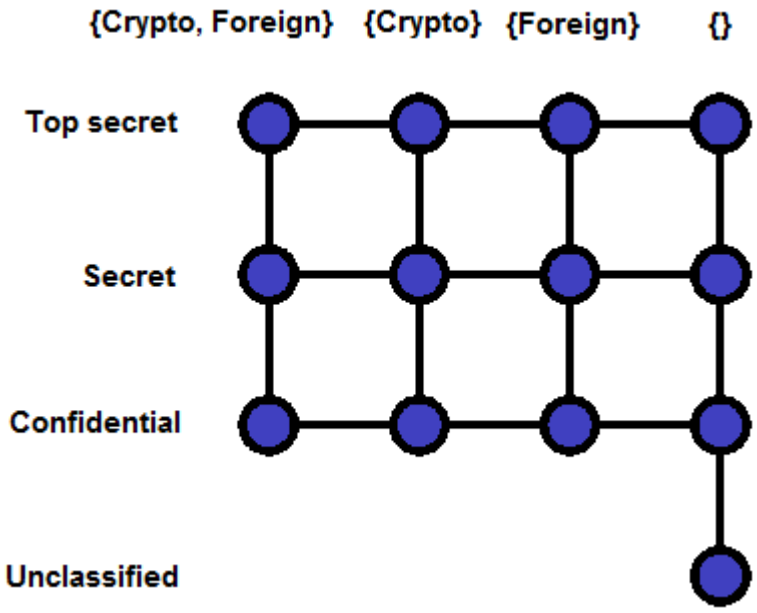
Credit: “Security Engineering” by Ross Anderson

The many faces of our adversary

- Loss of sensitive information is dangerous
  - Medical, intelligence, individuals' private information is sensitive
- Motivation of attacker can vary
  - Military superiority, commercial use, blackmail and even worse
- Adversary types
  - An individual inside an organization
  - An individual outside of organization that used a policy exploit
- Attacks
  - Countless. Comes in all sizes, shapes and colors

Compartmentation and the lattice model

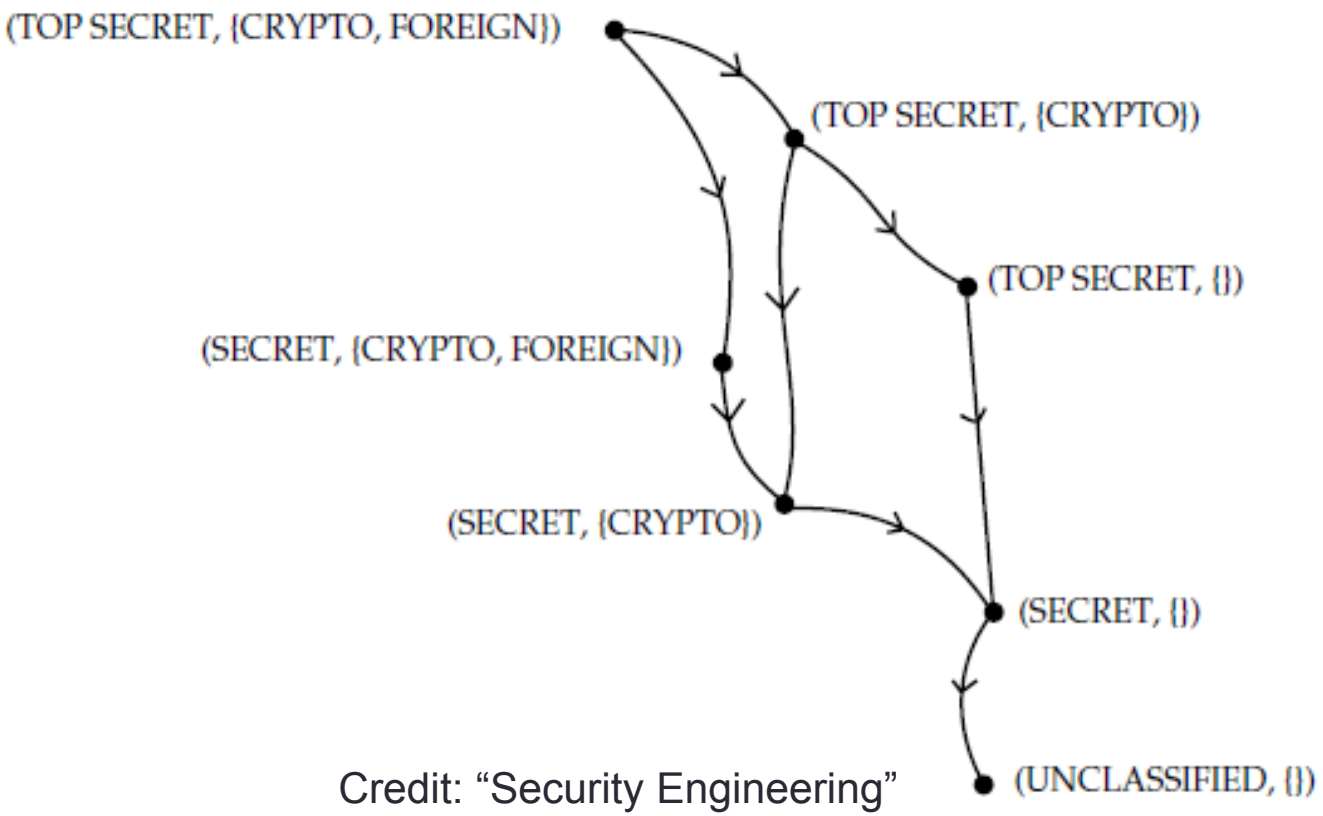
- Problem: Clearance levels just are not enough
  - Add codewords
- Basic idea: accessing the information requires both clearance and membership in the suitable group
  - Information flows in a lattice like manner
  - Each two nodes A, B can be in a dominance relation, A > B or B > A, but they do not have to be



Credit: physics.bu.edu

Compartmentation and the lattice model – continued

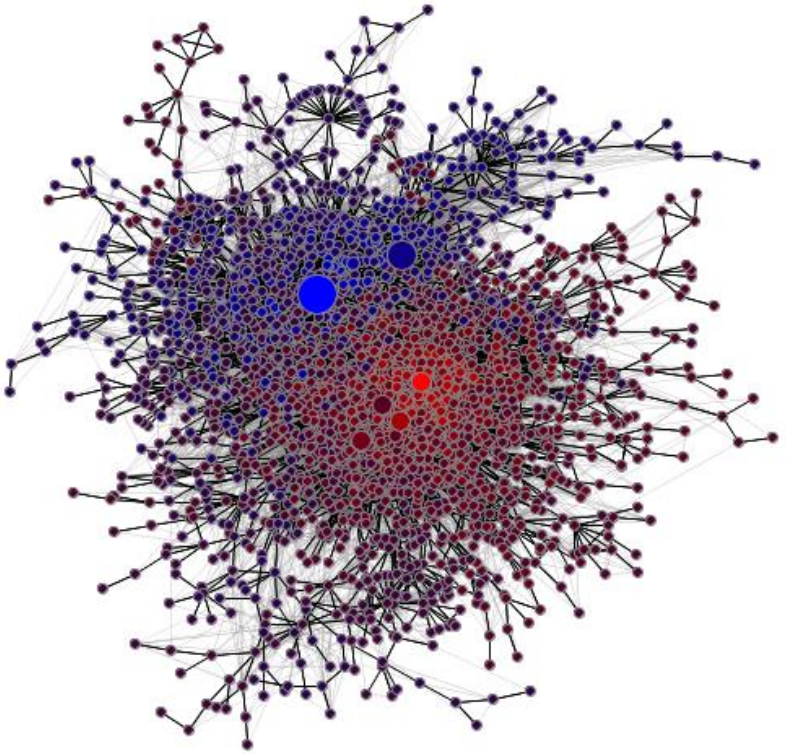
- An individual from compartment A may access information from compartment B if and only if A dominates B



Credit: “Security Engineering” by Ross Anderson

Compartmentation and the lattice model – continued

- Issues:
  - Data derived from two compartments effectively creates a third compartment
  - Information sharing or searching becomes a hard task
  - Needs additional information on how to sanitize subjects with high clearance back to lower compartments



Credit: datamining.typepad.com

The Chinese wall model

- Problem: Some services firms provides services to companies or organizations that are in competition
  - Need to prevent conflict of interests inside the firm
- Solution: Chinese walls

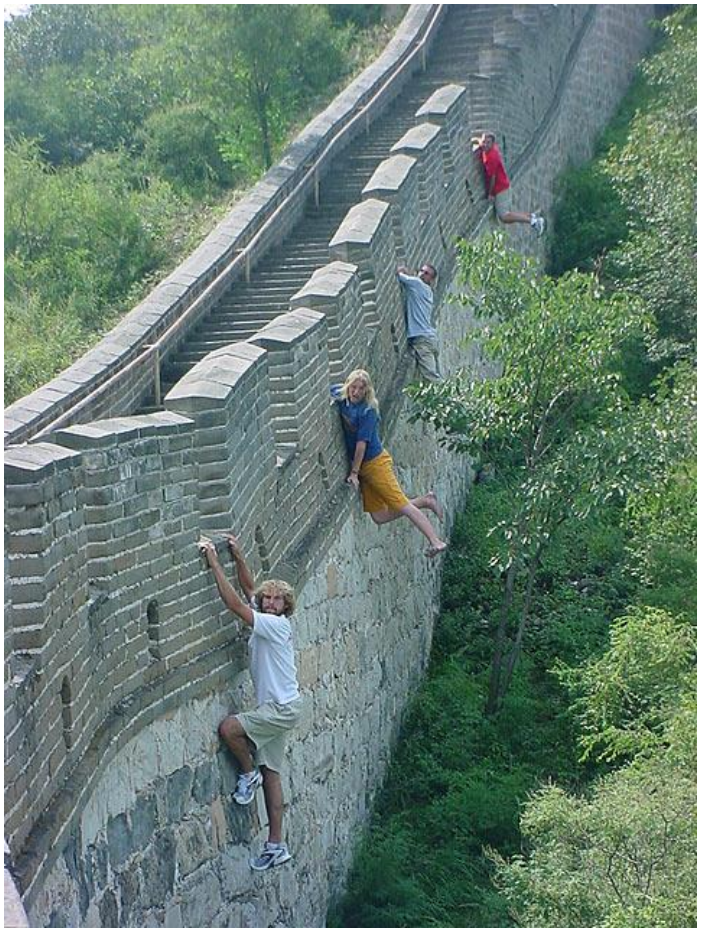
The Chinese wall model – continued

- Chinese walls: rules to prevent conflicts of interests
  - E.g., a partner who has worked recently for one company in a business sector may not see the papers of any other company in that sector

Credit: alpenrosewealth.com

The Chinese wall model – continued

- This can raise interesting questions
  - Is two competing companies A and B are both clients of the same investment bank, is B's data truly inaccessible to A?
  - Maybe they can gather information from side channels?



Credit: mangolianbox.com

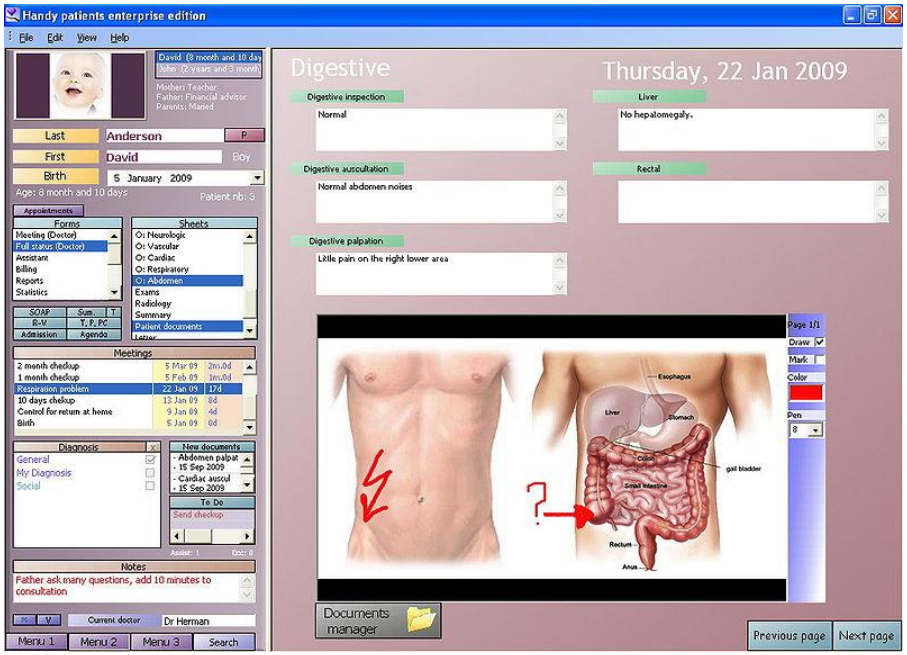
The British medical association (BMA) model

- Threat model:
  - Medical information is often quite controversial
    - Needs to be available on one hand (especially on emergencies)
    - Can be very sensitive on the other hand
    - Also, use secondary uses can have privacy and ethical issues
  - Centralization is a double-edge sword
    - more and more public agencies will come up with arguments why they need access to the data

Credit: communityhealthpartnership.co.uk

The British medical association (BMA) model – continued

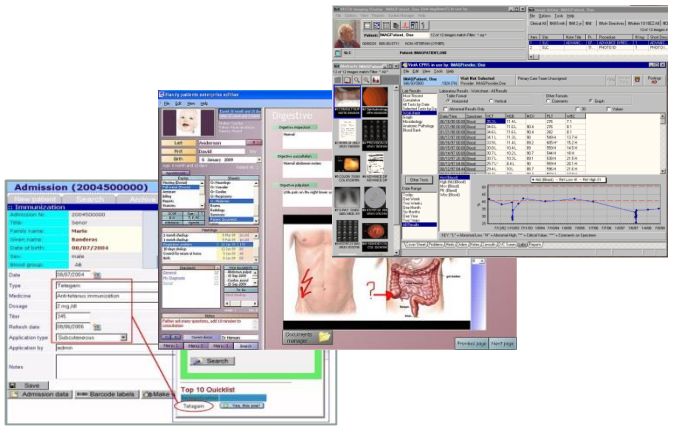
- Security policy first solution attempt: multilevel
  - E.g., AIDS database would be secret, patient records are classified, drug prescriptions are restricted
  - Based on a single Electronic Patient Record (EPR)
  - This had several problems:
    - The levels division is not always a clean cut
    - Single EPR is often not a good idea



Credit: wikipedia.org

The British medical association (BMA) model – continued

- Security policy outline:
  - Patient consent to information access is mandatory
  - Prevent too many people from getting access to too many identifiable records
- Basic principles:
  - Each patient will have several records
  - Each record has an access control list
  - Every change in the access list must be approved by the patient
  - There shall be effective measures to prevent the aggregation of personal health information



Credit: wikipedia.org
Arstechnica.com

What is inference control?

- Medical information, for example, is often released for research purposes
  - Information needs to be anonymous
  - Remove names and other identifiers, this should be enough!
    - Nope
- Inference is the ability to deduce information
  - From the given database alone or combined with another
- Of course, we do not want to restrict the queries more than needed

Credit: pixgood.com

Control types

- Query set size control
  - E.g., specify a minimum query size
- Trackers control
  - Solving this issue involves serious restrictions on the queries
- More sophisticated query controls
  - E.g., '*n*-respondent, *k*%-dominance rule'

Person	Drugs bought
A	55
B	32
C	16
D	5
E	4

For n=3 and k=75, the answer for the query "Total number of drugs bought" (=112) will be rejected

Control types – continued

- Cell suppression:
  - E.g.,

Major:	Biology	Physics	Chemistry	Geology
Minor:				
Biology	–	16	17	11
Physics	7	–	32	18
Chemistry	33	41	–	2
Geology	9	13	6	–

Credit: “Security Engineering”
by Ross Anderson

Major:	Biology	Physics	Chemistry	Geology
Minor:				
Biology	–	blanked	17	blanked
Physics	7	–	32	18
Chemistry	33	blanked	–	blanked
Geology	9	13	6	–

Credit: “Security Engineering”
by Ross Anderson

Control types – continued

- Maximum order control
  - Limit the number of attributes in a query
  - Reject queries that would partition the sample population into too many sets
- Query overlap control
- Randomization
  - Perturbation
  - Random sample queries

Limitations of generic approaches

- Specific applications will have specific inference attacks
  - E.g., a system used for analyzing trends in drug prescribing

Week:	1	2	3	4
Doctor A	17	26	19	22
Doctor B	25	31	9	29
Doctor C	32	30	39	27
Doctor D	16	19	18	13

Sample of de-identified drug prescribing data

Credit: “Security Engineering”
by Ross Anderson

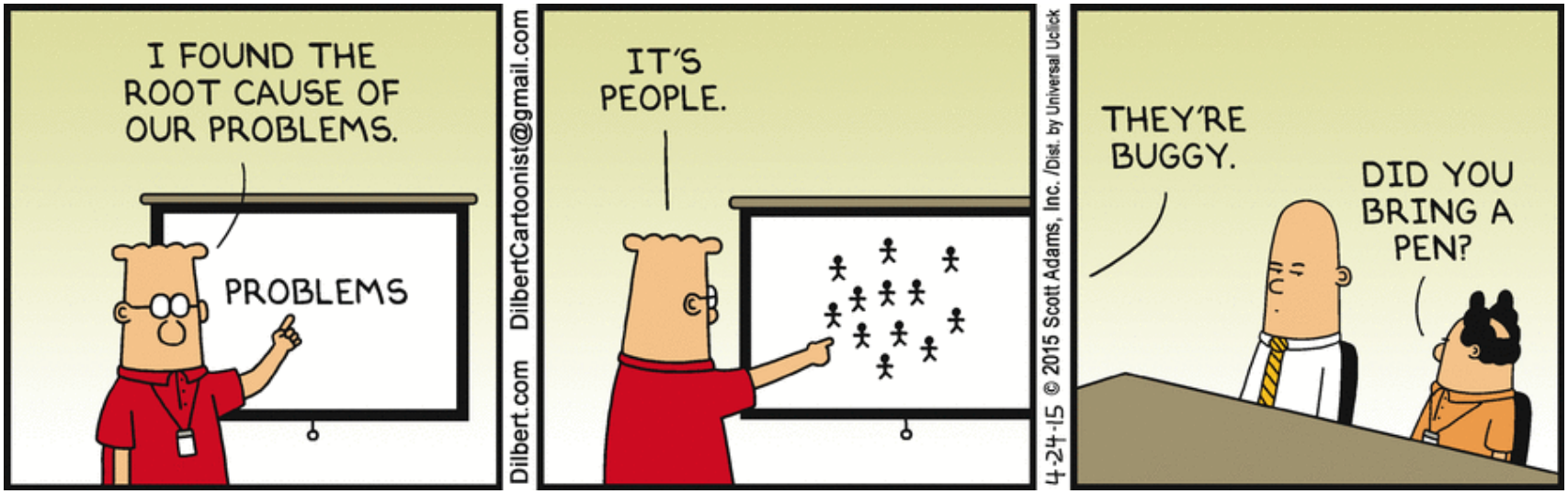
  - The general case is harder
- Active attacks
  - Where users have the ability to insert or delete records into the database

The residual problem

- Ok, so we know what data to protect
- We know good ways to protect it
  - In the immediate context, such as an hospital for medical data
  - In the secondary context, such as for research

The residual problem - continued

- But we have many real-life problems
  - Determining the sensitivity level of the information
  - Excluding single points of failure
  - Other problems dictated by real needs
    - E.g., processing medical claims for payment by the insurance companies



Credit: Dilbert.com

Summary

- Sensitive information is priceless
- Multilateral security has many sides and aspects
  - Attacks types are countless and keep evolving, especially when it comes to inference attacks
- When it comes to designing a multilateral security policy, it is almost impossible to create a watertight solution
  - Still, we must not give up

Questions?