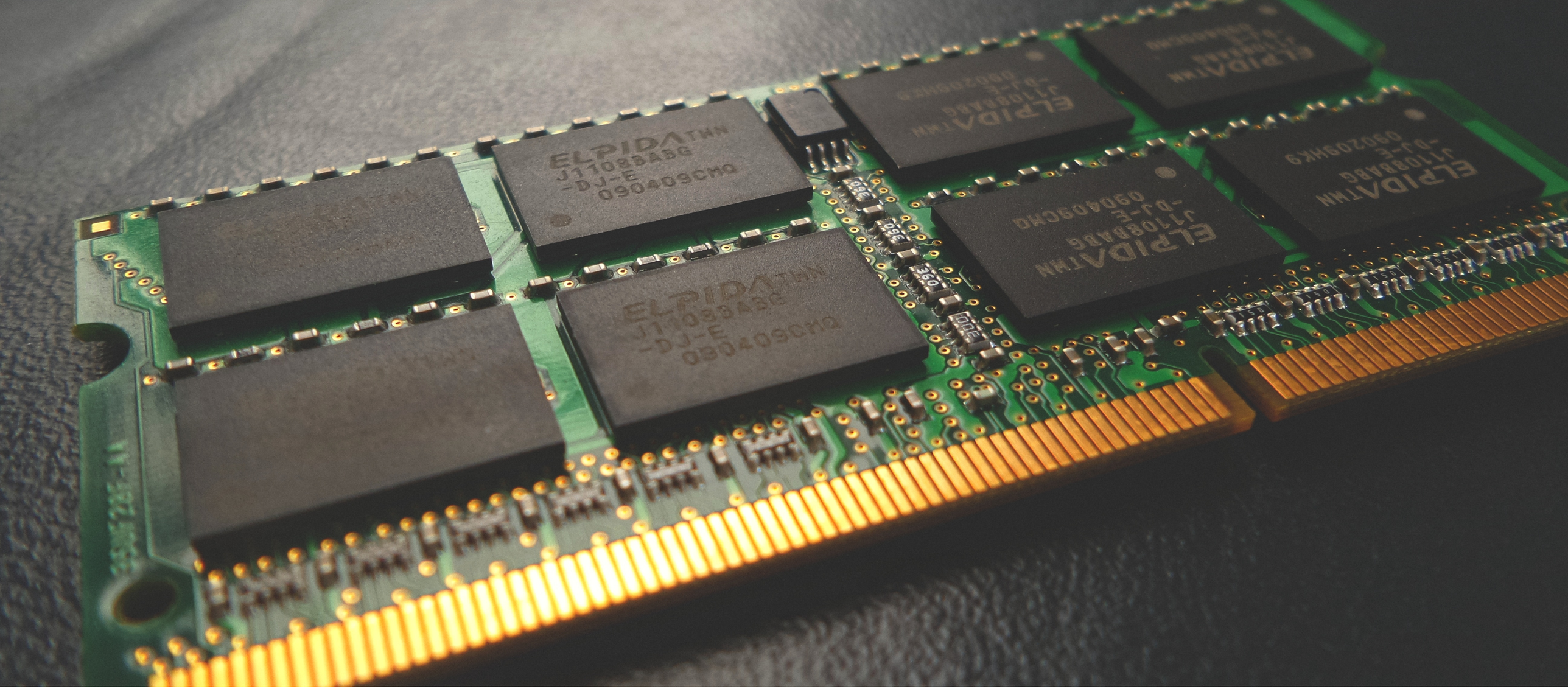


Hybrid Policies Breaking Out

Kresten Jacobsen

Intro to System Security

Goals

Prevention

Detection

Recovery

C-I-A

Confidentiality

Integrity

Availability

Threats

Snooping

Modification

Spoofing

Repudiation of Origin

Denial of Receipt

Delay

Security Policies

Requirements

- Common understanding (implicit / explicit)
- Trust (in people and computers)
- Assumption (that policies are enforced)

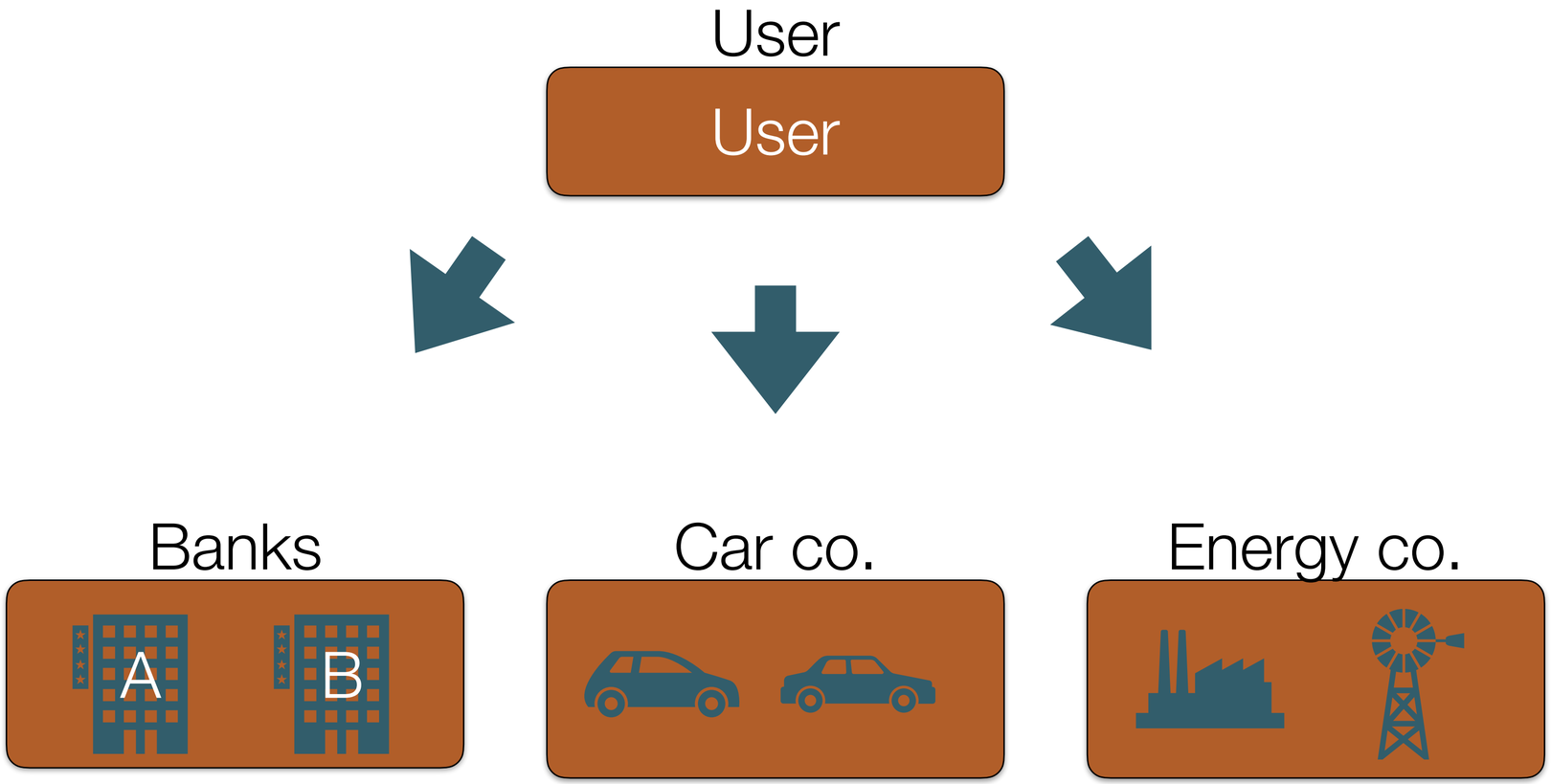
Policy types

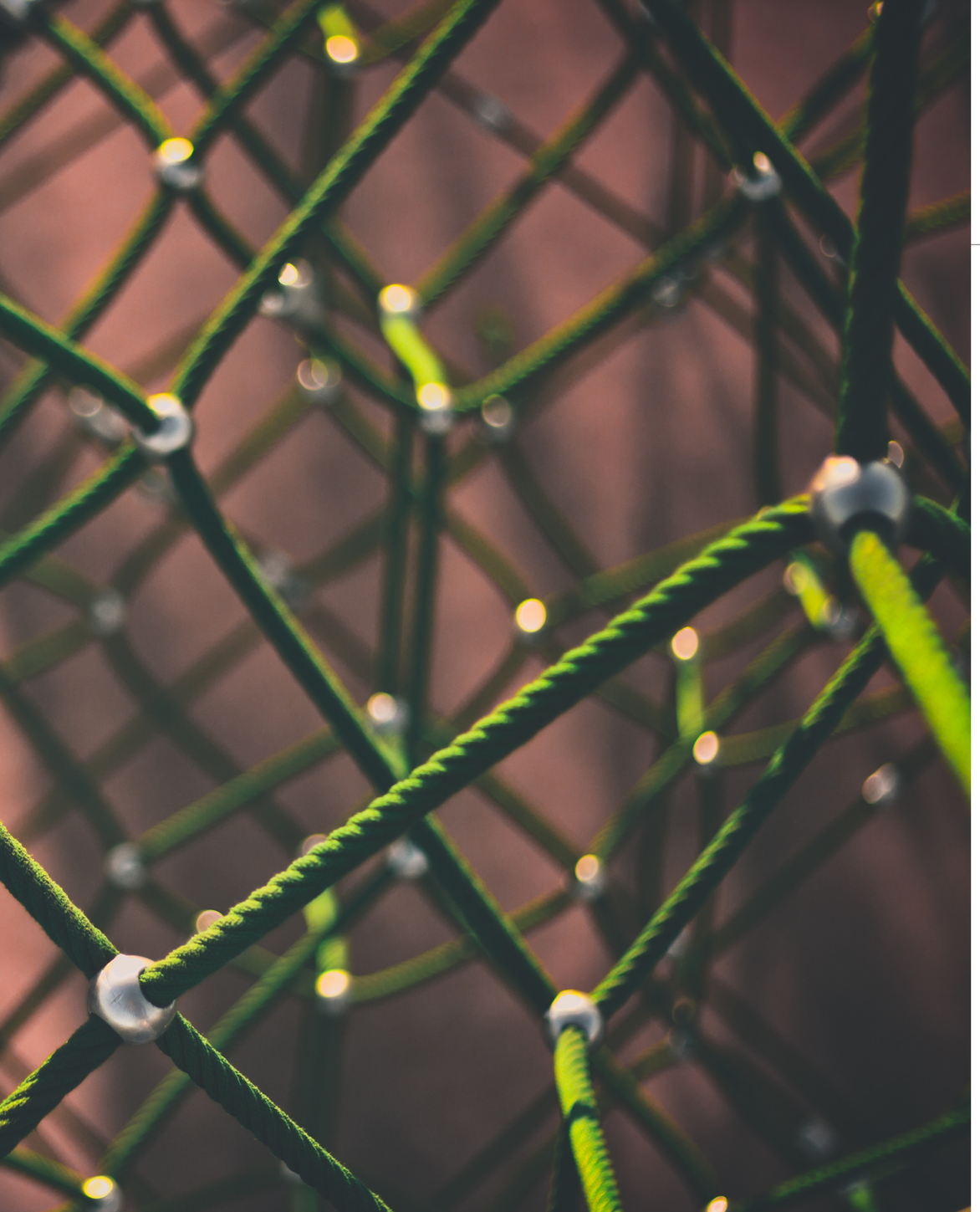
- Confidentiality
- Integrity Policy
- Availability Policy

Hybrid Policies

- Chinese Wall
- Originator Controlled Access Control
- Clinical Informational Systems Security
- Break the Glass

Chinese Wall Model





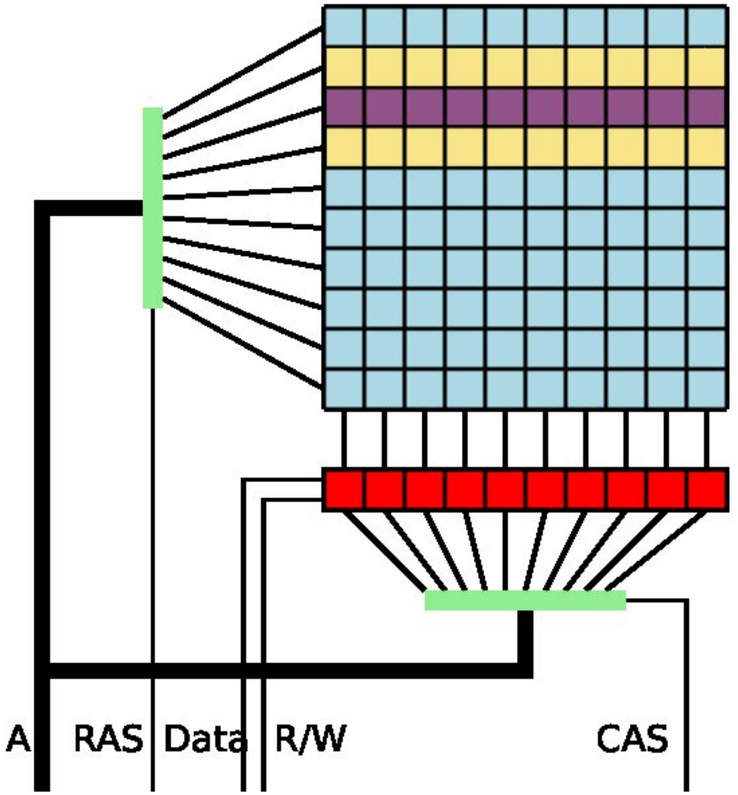
Side channels

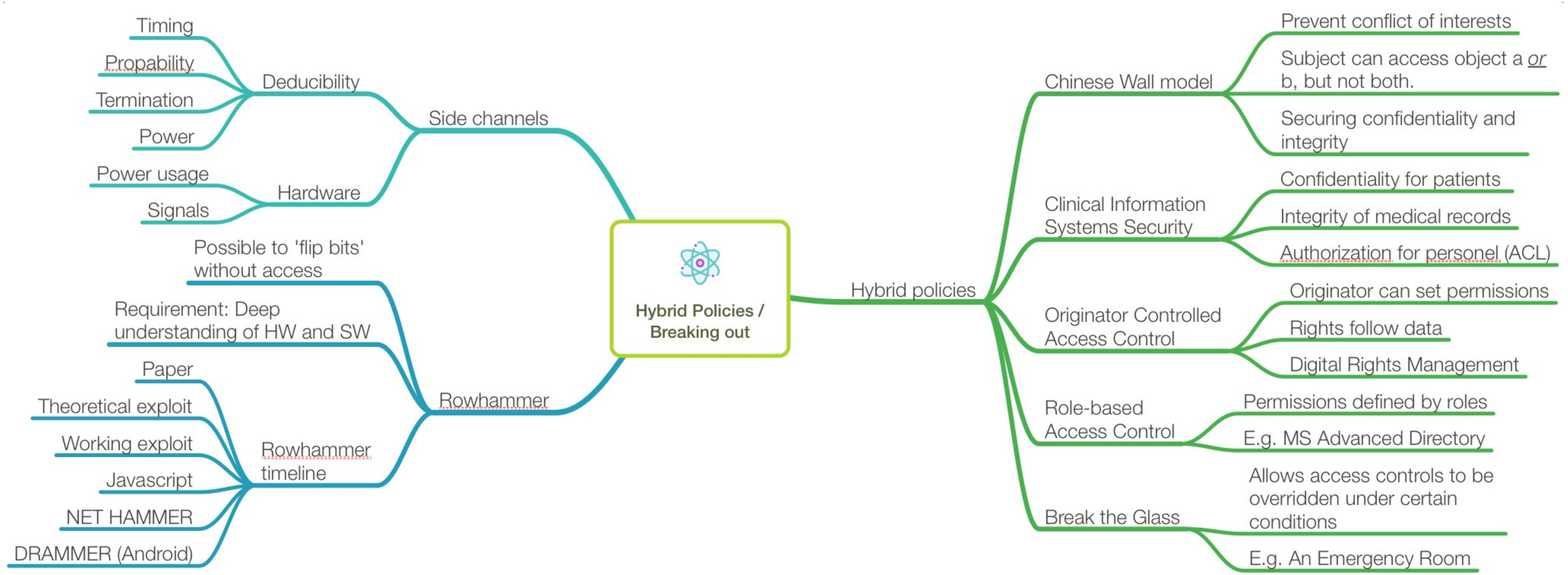
- Timing attack
- Power-analysis attack
- Electromagnetic emanations
- ...
- Row Hammer

Breaking out - Row Hammer

Timeline

- 2014 (june) - Original paper
- 2015 (march) - Theoretical exploit (PoC)
- 2015 (july) - Javascript exploit
- 2016 (october) - Exploit for Android
- 2018 (may) - Remote Rowhammer




Hybrid Policies / Breaking out
Side channels
Deducibility
Timing
Propability
Termination
Power
Hardware
Power usage
Signals
Rowhammer
Possible to 'flip bits' without access
Requirement: Deep understanding of HW and SW
Rowhammer timeline
Paper
Theoretical exploit
Working exploit
Javascript
NET HAMMER
DRAMMER (Android)
Hybrid policies
Chinese Wall model
Prevent conflict of interests
Subject can access object a or b, but not both.
Securing confidentiality and integrity
Clinical Information Systems Security
Confidentiality for patients
Integrity of medical records
Authorization for personel (ACL)
Originator Controlled Access Control
Originator can set permissions
Rights follow data
Digital Rights Management
Role-based Access Control
Permissions defined by roles
E.g. MS Advanced Directory
Break the Glass
Allows access controls to be overridden under certain conditions
E.g. An Emergency Room