Welcome to

5. Hybrid Policies

KEA Kompetence Computer Systems Security 2019

Henrik Lund Kramshøj hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Github

5-hybrid-policies.tex in the repo security-courses

Plan for today

Subjects

- Chinese Wall model - Confidentiality and Integrity
- Clinical Information Systems security model
- Originator Controlled Access Control
- Role-based Access Control (RBAC)
- Break-the-glass Policies
- Side Channels and Deducibility
- Memory errors and Row hammer

Exercises

- RBAC Access permissions on GitHub

Reading Summary

Bishop chapter 8: Hybrid Policies

Browse: Using Memory Errors to Attack a Virtual Machine paper

An Experimental Study of DRAM Disturbance Errors

Exploiting the DRAM rowhammer bug to gain kernel privileges

`https://en.wikipedia.org/wiki/Row_hammer`

Chinese Wall model - Confidentiality and Integrity

A model of a security policy that refers equally to confidentiality and integrity

Designed to provide controls that mitigate conflict of interest in commercial organizations

Natural environment stock exchange or investment house

Definition 8-1. The *objects* of the database are items of information related to a company.

Definition 8-2. A *company dataset* (CD) contains objects related to a single company.

Definition 8-3. A *conflict of interest* (COI) class contains the datasets of companies in competition.

See also `https://en.wikipedia.org/wiki/Chinese_wall`
`https://en.wikipedia.org/wiki/Brewer_and_Nash_model`

Chinese Wall model - Informal Description

$PR(S)$ is the set of objects that S has read.

- ***CW-Simple Security Condition, Preliminary Version:*** S can read O if and only if either of the following is true.

  1. There is an object O' such that S has accessed O' and $CD(O') = CD(O)$.
  2. For all objects $O', O' \in PR(S) \Rightarrow COI(O') \neq COI(O)$.

You can only read future objects that will not result in a conflict of interest

Screenshot from: *Computer Security: Art and Science*, Bishop, 2019

Chinese Wall model - Informal Description

- ***CW-Simple Security Condition:*** S can read O if and only if any of the following holds.
  1. There is an object O' such that S has accessed O' and $CD(O') = CD(O)$.
  2. For all objects $O', O' \in PR(S) \Rightarrow COI(O') \neq COI(O)$.
  3. O is a sanitized object.

Adding publically accessible information, we can consider some object/informatioin can be considered sanitized - allowed for reading by all

Screenshot from: *Computer Security: Art and Science*, Bishop, 2019

Chinese Wall model - Writing objects

Suppose Anthony and Susan work in the same trading house. Anthony can read objects in Bank of America's CD, and Susan can read objects in Citibank's CD. Both can read objects in ARCO's CD. If Anthony can also write to objects in ARCO's CD, then he can read information from objects in Bank of America's CD and write to objects in ARCO's CD, and then Susan can read that information; so, Susan can indirectly obtain information from Bank of America's CD, causing a conflict of interest. The CW-simple security condition must be augmented to prevent this.

- ***CW-*-Property:*** A subject S may write to an object O if and only if both of the following conditions hold.

  1. The CW-simple security condition permits S to read O.
  2. For all unsanitized objects O', S can read $O' \Rightarrow CD(O') = CD(O)$.

In the example above, Anthony can read objects in both Bank of America's CD and ARCO's CD. Thus, condition 1 is met. However, assuming that Bank of America's CD contains unsanitized objects (a reasonable assumption), then because Anthony can read those objects, condition 2 is false. Hence, Anthony cannot write to objects in ARCO's CD.

Computer Security: Art and Science, Bishop, 2019

Clinical Information Systems security model Definitions

A model of a

Definition 8-6. A *patient* is the subject of medical records, or an agent for that person who can give consent for the person to be treated.

Definition 8-7. *Personal health information* is information about a patient's health or treatment enabling that patient to be identified.

Definition 8-8. A *clinician* is a health-care professional who has access to personal health information while performing his or her job.

Clinical Information Systems security model Principles

- **Access Principle 1:** Each medical record has Access Control List (ACL)
- **Access Principle 2:** One clinician on ACL can add others
- **Access Principle 3:** Responsible clinician must inform patient of ACL, when record opened, need consent
- **Access Principle 4:** Access to records must be logged clinician, date and time, same for deletion
- **Creation Principle:** A clinician may open a record as a result of referral
- **Deletion Principle:** Clinical information cannot be deleted from a medical record until the appropriate time has passed
- **Confinement Principle:** Information from one medical record can only be appended to another if the ACL is of the second is a subset of the ACL of the first
- **Aggregation Principle:** Measures for preventing the aggregation of patient data must be effective
- **Enforcement Principle:** Any computer system that handles medical records must have a subsystem that enforces the preceeding principes. Subject to evaluation by independent auditors.

Shortened by me. From: *Computer Security: Art and Science*, Bishop, 2019

Clinical system security: Interim guidelines

Nine principles of data security

(1) **Access control**—Each identifiable clinical record shall be marked with an access control list naming the people or groups of people who may read it and append data to it. The system shall prevent anyone not on the list from accessing the record in any way.

(2) **Record opening**—A clinician may open a record with herself and the patient on the access control list. When a patient has been referred she may open a record with herself, the patient, and the referring clinician(s) on the access control list.

(3) **Control**—One of the clinicians on the access control list must be marked as being responsible. Only she may change the access control list and she may add only other health care professionals to it.

(4) **Consent and notification**—The responsible clinician must notify the patient of the names on his record's access control list when it is opened, of all subsequent additions, and whenever responsibility is transferred. His consent must also be obtained, except in emergency or in the case of statutory exemptions.

(5) **Persistence**—No one shall have the ability to delete clinical information until the appropriate time has expired.

(6) **Attribution**—All accesses to clinical records shall be marked on the record with the name of the person accessing the record as well as the date and time. An audit trail must be kept of all deletions.

(7) **Information flow**—Information derived from record A may be appended to record B if and only if B's access control list is contained in A's.

(8) **Aggregation control**—Effective measures should exist to prevent the aggregation of personal health information. In particular, patients must receive special notification if any person whom it is proposed to add to their access control list already has access to personal health information on a large number of people.

(9) **Trusted computing base**—Computer systems that handle personal health information shall have a subsystem that enforces the above principles in an effective way. Its effectiveness shall be evaluated by independent experts.

Source: *Clinical system security: Interim guidelines*, Ross Anderson, 1996

Originator Controlled Access Control

Problem: MAC and DAC does not handle environments in which the originators of documents retain control over them even after dissemination

- 1. The owner of an object cannot change the acccess controls of the object
- 2. When an object is copied, the acess controle restrictions of that source are copied and bound to the target of the copy.
- 3. The creator (originator) can alter the access control restrictions on a per-object and per-object basis.

1. and 2. are MAC, 3. DAC

While important I dont see much talk about originator controlled models in the real world, except for DRM

Digital Rights Management

The owner of content, movies, books, may wish to control its distribution.

Definition 8-9. *Digital rights management* (DRM) is the persistent control of digital content

Computer Security: Art and Science, Bishop, 2019

Relates to copyright, fair use, quoting stuff

huge controversies in this space, newest examples:
"link-skatten"(artikel 11/15) og uploadfiltrene (artikel 13/17)

Most often based on some crypto and keys

DRM also is used to prevent people from upgrading devices they *own*

Role-based Access Control (RBAC)

In computer systems security, **role-based access control (RBAC)**[1][2] or role-based security[3] is an approach to restricting system access to unauthorized users. It is used by the majority of enterprises with more than 500 employees,[4] and can implement mandatory access control (MAC) or discretionary access control (DAC).

Role-based access control (RBAC) is a policy-neutral access-control mechanism defined around **roles and privileges**. The components of RBAC such as role-permissions, user-role and role-role relationships make it simple to perform user assignments. A study by NIST has demonstrated that RBAC addresses many needs of commercial and government organizations[citation needed]. RBAC can be used to facilitate administration of security in large organizations with hundreds of users and thousands of permissions. Although RBAC is different from MAC and DAC access control frameworks, it can enforce these policies without any complication.

Quote from `https://en.wikipedia.org/wiki/Role-based_access_control`

Role-based Access Control (RBAC), *Computer Security* Bishop

This suggests associating access with the particular job of the user.

Definition 7–8. A *role* is a collection of job functions. Each role r is authorized to perform one or more transactions (actions in support of a job function). The set of authorized transactions for r is written $trans(r)$.

Definition 7–9. The *active role of a subject* s, written $actr(s)$, is the role that s is currently performing.

Definition 7–10. The *authorized roles of a subject* s, written $authr(s)$, is the set of roles that s is authorized to assume.

Definition 7–11. The predicate $canexec(s, t)$ is true if and only if the subject s can execute the transaction t at the current time.

Three rules reflect the ability of a subject to execute a transaction.

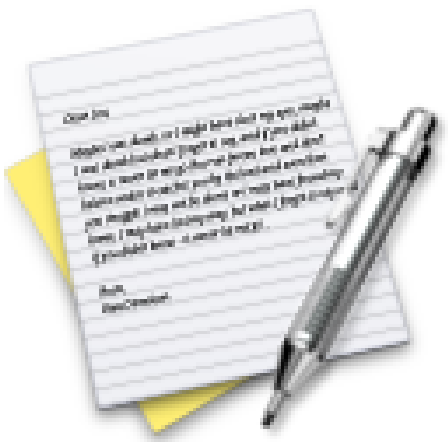
Axiom 7–7. Let S be the set of subjects and T the set of transactions. The *rule of role assignment* is $(\forall s \in S)(\forall t \in T)[\ canexec(s, t) \rightarrow actr(s) \neq \varnothing\ ]$.

This axiom simply says that if a subject can execute *any* transaction, then that subject has an active role. This binds the notion of execution of a transaction to the role rather than to the user.

Axiom 7–8. Let S be the set of subjects. Then the *rule of role authorization* is $(\forall s \in S)[\ actr(s) \subseteq authr(s)\ ]$.

This rule means that the subject must be authorized to assume its active role. It cannot assume an unauthorized role. Without this axiom, any subject could assume any role, and hence execute any transaction.

Exercise



Now lets do the exercise

RBAC Access permissions on GitHub 30-45min

which is number **12** in the exercise PDF.

Break-the-glass Policies

Definition 8-19. A *break-the-glass* policy allows access controls to be overriden in a controlled manner.

Example uses may be:

Getting the root password for a server

Getting access to someones email inbox

Covert Channels

> Definition: A covert channel is a path for the illegal flow of information between subjects within a system, utilizing system resources that were not designed to be used for inter-subject communication.

Note several features of this definition:

- Information flows in violation of the security metapolicy though not necessarily in violation of the policy.
- The flow is between subjects within the system; two human users talking over coffee is not a covert channel.
- The flow occurs via system resources (file attributes, flags, clocks, etc.) that were not intended as communication channels.

List from William D. (Bill) Young `https://www.cs.utexas.edu/~byoung/cs361/lecture14.pdf`

Side Channels and Deducibility

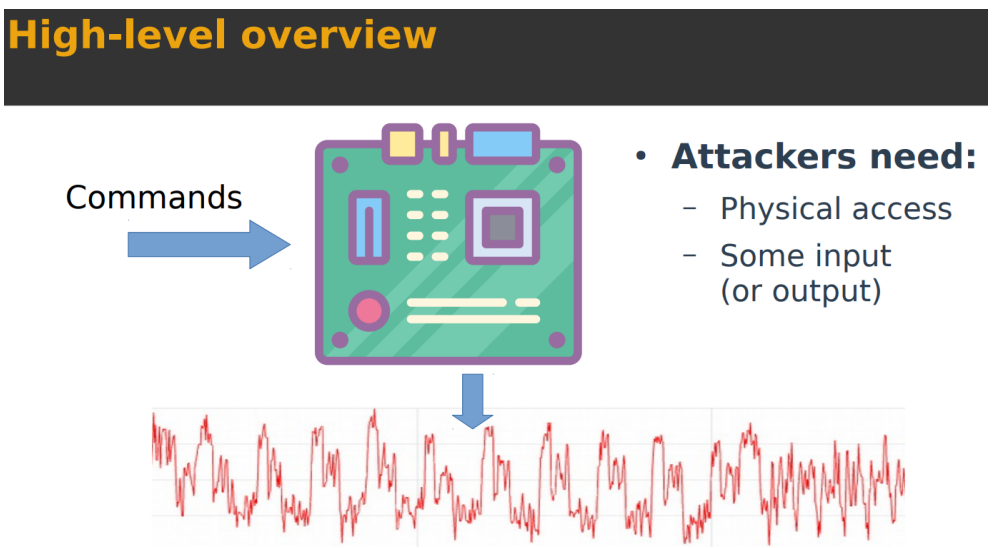
It is possible to distinguish many types of covert channels, depending on the attribute manipulated:

- Timing: how much time did a computation take?
- Implicit: what control path does the program take?
- Termination: does a computation terminate?
- Probability: what is the distribution of system events?
- Resource exhaustion: is some resource depleted?
- Power: how much energy is consumed?

In practice, many researchers distinguish only storage and timing channels.

List from William D. (Bill) Young `https://www.cs.utexas.edu/~byoung/cs361/lecture14.pdf`

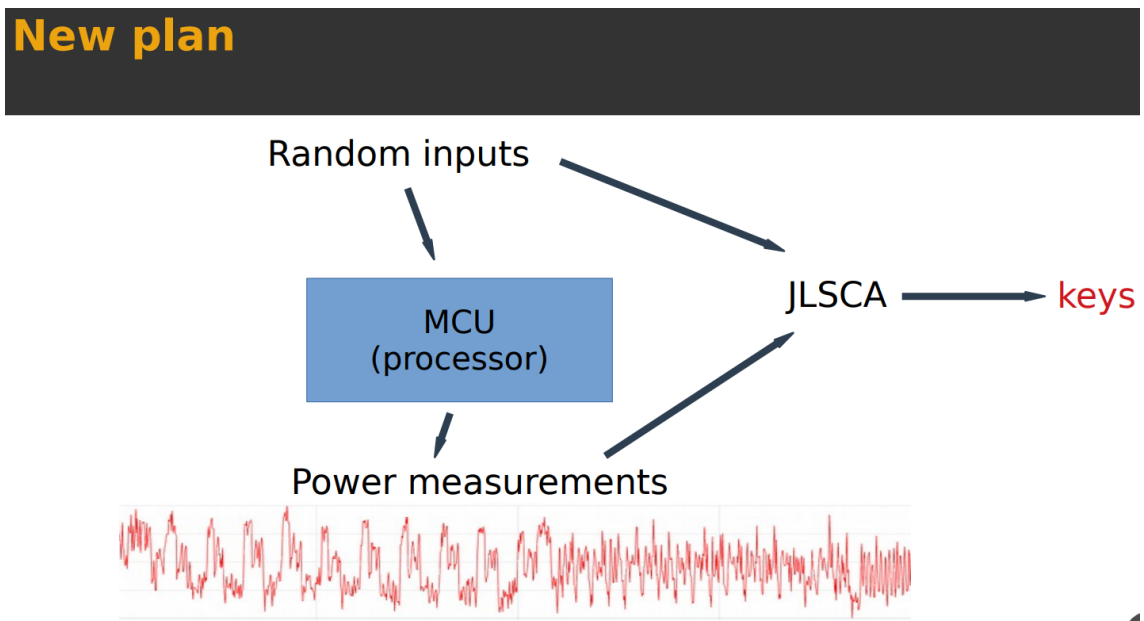
Hardware Side Channels – deducting AES keys 1



Hardware was Arduino Nano 16 MHz, Not secure

Picture from *Hardware Side Channel attacks on the cheapest*, Alyssa Milburn and Albert Spruyt, `https://troopers.de/downloads/troopers19/TROOPERS19_NGI_RT_Hardware_Side_Channels.pdf`

Hardware Side Channels – deducting AES keys 2



Picture from *Hardware Side Channel attacks on the cheapest*, Alyssa Milburn and Albert Spruyt, `https://troopers.de/downloads/troopers19/TROOPERS19_NGI_RT_Hardware_Side_Channels.pdf`

Memory errors and Row hammer

Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors Yoongu Kim, Ross Daly, Jeremie Kim, Chris Fallin, Ji Hye Lee, Donghyuk Lee, Chris Wilkerson, Konrad Lai, Onur Mutlu

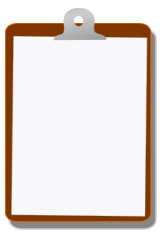
`http://users.ece.cmu.edu/~yoonguk/papers/kim-isca14.pdf`

Exploiting the DRAM rowhammer bug to gain kernel privileges Project Zero blog, Posted by Mark Seaborn, sandbox builder and breaker, with contributions by Thomas Dullien, reverse engineer

`https://googleprojectzero.blogspot.com/2015/03/exploiting-dram-rowhammer-bug-to-gain.html`

`https://en.wikipedia.org/wiki/Row_hammer`

For Next Time



Think about the subjects from this time, write down questions

Check the plan for chapters to read in the books
Most days have less than 100 pages, but some days may have more!

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools