Lecture 17 - 15/11/2019

Info flow

Fenton data mark machine

- Goal was to take implicit assignments/flows and make them explicit
- He did this by looking at the program counter
- All the variables had their respective information flow classes, now the PC had its own class, PC

E.g.

If x = 0 then goto n;
Else x := x-1;

Is equivalent to
If x = 0 then { push(PC,PC), PC = lub(PC, x), pc := n}
else { if PC < x then {x := x-1} else skip }

Explicit flow from PC -> y therefore we need to verify that PC < y

E.g.

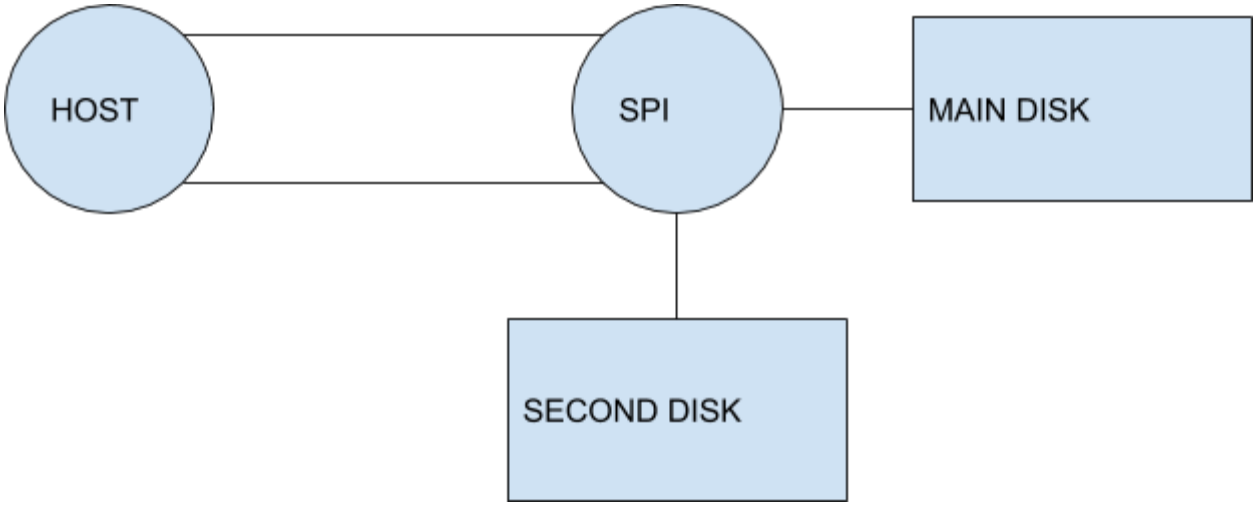
Line 5000 y := 2;

If this assignment happens and we observe it, we can tell that line 5000 has been hit

(x,pc) -> y therefore need lub{x,pc} < Y

We can set the pc = lub(x,px) and check that pc < y

Info flow through channels



SPI holds Hashes and MACs of files in the main disk,
If any files have been corrupted it retrieves the file from the second disk instead

This verifies integrity

E.g. Security network server mail forward

A mailguard system is a series of queues and filters that sits between two networks so that information can be shared between two workstations in these networks.

Secure information is filtered or encrypted when sent from the secure network to the unclassified network

When mail is sent from the unclassified network to the classified one, authenticity is checked to ensure that the message and the sender can be trusted.

S/KEY

- One called S/KEY
- Alice pics some seed value k
- $h(k_0) = k_1$ $h(k_1)=k_2$ $h(k_2)=k_3$ … until K_n
- Send k_0 to the system
- System stores the end of the chain, $\{n,k_n\}$
- Alice wants to log in:
    - Enters username “Alice”

- System challenges her with i-1
- Alice responds with k_{i-1}
- System checks $h(k_{i-1}) = k_i$
- If so, then she is granted access
- System updates to store $\{i-1, k_{i,-1}\}$

Public key based challenge response

- Alice shares her public key with the system
- The system sends a challenge in the form of a random value N
- Alice is just going to sign it with her private key and send the signature
- This signature can be verified with the public key

Note: Covert Channels

- A way that two devices can communicate without anyone knowing
- E.g. Acoustic covert channels
    - Using a speaker and a microphone

Protection

- Injection of randomness
    - Make the channels noisy
- System appropriate
    - Give every process the same amount of resources.

Containment/isolation

- We can prevent unwanted flow of information via containment and isolation
- We want partial isolation so we can still have functionality
- Partial
    - VM
    - Containers
    - Sandboxes

Sandboxes

- Default
- Broad
- Open