Introduction to Information Flow

Ana Matos
Software Security 2023/24, IST

November 22, 2023

Goals

- To become acquainted with basic concepts of **taint flow**, and understand it as a special case of information flow.
- To gain insight on capabilities and limitations of taint analysis tools, by considering the example of **Perl's Taint mode**.
- To become familiar with basic concepts for defining **information flow policies**, to understand the limitations of access control.
- To gain intuitions on how programs **encode information flows**.
- To develop the **components of a tool** for detecting code injection vulnerabilities that **configure information flow policies**.

1 Taint Flow

1. Consider the following script, discussed in the theoretical class. Does it guarantee integrity of the query to the database? Why is this a problem?

```
1 $a = $_GET['user'];
2 $b = $_POST['pass'];
3 $c = "SELECT * FROM users WHERE u = '".mysql_real_escapes_string($a)."'";
4 $b = "wap";
5 $d = "SELECT * FROM users WHERE u = '".$b."'";
6 $r = mysql_query($c);
7 $r = mysql_query($d);
8 $b = $_POST['pass'];
9 $query = "SELECT * FROM users WHERE u = '".$a."' AND p = '".$b."'";
10 $r = mysql_query($query);
```

2. **(Analysis of) Perl's Taint Analysis**

   First time with Perl? This class is *not* about the Perl language, and you do not need to know the language in order to follow these exercises. We will focus on analysing its built-in taint mode tool, perhaps the most widely used information-flow analysis mechanism.

   > [Perl's] tainting mechanism is intended to prevent stupid mistakes, not to remove the need for thought. (Wall, Christiansen and Schwartz, 1996)

   Intro to Perl: `https://perldoc.perl.org/perlintro.html`

   More on Perl Security: `https://perldoc.perl.org/perlsec.html`

   More on Perl Regular Expressions: `https://perldoc.perl.org/perlrequick.html`

(a) Write a Hello world script in Perl and run it. Turn on the taint mode by using the `-T` flag in the hashbang line, and run it again.

What programs produce executions that are never altered by activating taint mode?

(b) Run the following script, and explain what happens:

```
#!/usr/bin/perl -T
print "Give name to new file:\n";   # prints message to screen
$filename=<STDIN>;                  # assigns input to $filename
open(FOO,"> $filename");            # opens file for output, handled by FOO
```

*Can you write a program that can **both** produce executions which **are** altered by taint mode, and others which are **not**?*

(c) What kinds of information flows does Perl's taint mode catch? Which ones does it not catch? Modify the above script so that it executes in taint mode, without using Perl's endorsement mechanism (regular expressions).

(d) Add the following regular expression check, to make sure that the inputted value contains nothing but "word" characters (alphabetics, numerics, and underscores), a hyphen, an at sign, or a dot before opening the file.

```
...                                     # $filneame tainted
if ($filename =~ /^([-\@\w.]+)$/) {     # match regular expression
  $filename = $1;                       # $filename here untainted
  ...
} else {
  print "Boo!";                         # $filename tainted
}
...                                     # $filename tainted
```

Run it again (making sure that you choose a fresh name for the file!), and explain what happens.

(e) *What is Perl's endorsement mechanism (regular expressions) intended to catch? How can it be misused?* Modify the above script so that it executes in taint mode, by using Perl's endorsement mechanism to bypass the purpose of taint mode.

2 Information flow policies

1. Define the information flow policy that is implicit in Perl's Taint mode.

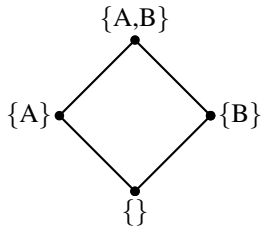
   Answer:

   - $SC = \{\textbf{Tainted}, \textbf{Untainted}\}$.
   - $\rightarrow = \{(\textbf{Tainted}, \textbf{Tainted}), (\textbf{Untainted}, \textbf{Untainted}), (\textbf{Untainted}, \textbf{Tainted})\}$
   - $\textbf{Tainted} \oplus \textbf{Tainted} = \textbf{Tainted}$, $\textbf{Untainted} \oplus \textbf{Untainted} = \textbf{Untainted}$, $\textbf{Tainted} \oplus \textbf{Untainted} = \textbf{Tainted}$, $\textbf{Untainted} \oplus \textbf{Tainted} = \textbf{Tainted}$

2. The *principal-based integrity* policy results from considering security classes as sets of principals with write-access permissions.

   (a) Represent this information flow policy for a system with 2 principals using a Hasse diagram.

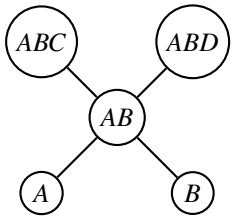
Answer:



(b) Define the above information flow policy by giving its set of classes *SC*, the can-flow relation $\rightarrow$, and the join operator $\oplus$. **Answer:**

- SC = $\{\{\},\{A\},\{B\},\{A,B\}\}$.
- $\rightarrow$ = $\subseteq$
- $\oplus$ = $\cup$

3. Consider the following Hasse diagram:



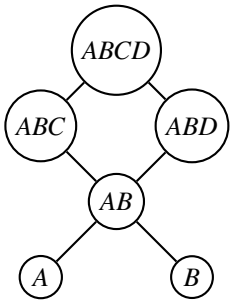
(a) Define an information flow policy that is represented by the above Hasse diagram by giving its set of classes *SC*, the can-flow relation $\rightarrow$, and a join operator $\oplus$.

Answer:

- SC = $\{A,B,AB,ABC,ABD\}$.
- $\rightarrow$ is the reflexive and transitive closure of: $\{(A,AB),(B,AB),(AB,ABC),(AB,ABD)\}$
- The symmetric closure of:
  $l \oplus l = l, \forall l \in SC$
  $A \oplus ABC = ABC$, $B \oplus ABC = ABC$, $AB \oplus ABC = ABC$
  $A \oplus ABD = ABD$, $B \oplus ABD = ABD$, $AB \oplus ABD = ABD$
  $A \oplus AB = AB$, $B \oplus AB = AB$
  $A \oplus B = AB$

(b) The above diagram does not define $\oplus$ for all pairs of security classes. Using a Hasse diagram, represent an information flow policy that contains the above policy, and for which $\oplus$ is always defined.

Answer: No. The operation $\oplus$ is not defined for the elements *ABC*, and *ABD*. There are many possible solutions to the question. For example:



4. Consider the following description of an access control policy:

   - Alice allows Eve to read and write to her objects;
   - Eve allows Bob to read and write to her objects;
   - Owners of an object have all rights over it.

   (a) Represent the access control matrix for a system that includes users Alice, Bob and Eve, and manages the rights 'r' (read) and 'w' (write) over files named Alice.txt, Bob.txt, Eve.txt (respectively owned by Alice, Bob and Eve).

   Answer:

	Alice.txt	Bob.txt	Eve.txt
Alice	o, r, w		
Bob		o, r, w	r, w
Eve	r, w		o, r, w

   (b) Consider a system that enforces the above access control policy. Are the following statements true? Why?

   i. "Only Alice and Eve will ever know the contents of file Alice.txt."

   Answer: The statement is not true because nothing prevents Eve from reading file Alice.txt and writing its contents into her own file Eve.txt, which can be read by Bob.

   ii. "Information contained in Alice.txt can only have originated from Alice or Eve"

   Answer: The statement is not true because nothing prevents Eve from reading file Eve.txt, which in turn and can have been written by Bob, and then writing its contents into file Alice.txt.

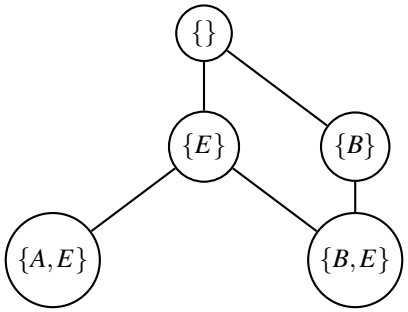
   (c) Suppose that a principal-based mandatory access control policy for confidentiality that prevents illegal information flows is imposed over the above policy. Define such an information flow policy regarding reading rights ('r') using sets of users as security classes, by giving:

   - The set of security classes SC
   - The "can-flow" relation $\rightarrow$.
   - The binary class-combining operator $\oplus$.
   - The Hasse diagram of the policy.

Note: It is enough to include the security classes that are used in the above matrix, as well as those needed for $\oplus$ to be well defined for all levels in *SC*. **Answer:** Let us represent users

Alice, Bob and Eve by the letters A, B and E respectively.

- SC = $\{\{\},\{B\},\{E\},\{A,E\},\{B,E\}\}$.
- $\rightarrow$ = $\supset$
- $\oplus$ = $\cap$



(d) Consider an extension of the information flow policy defined as above in question 4c, where security classes are pairs of security classes for rights 'r' and 'w', i.e., for confidentiality and integrity. What should be the label of an object that contains information originating from Alice.txt and Eve.txt?

Answer: The labels associated to Alice.txt and Eve.txt would be, respectively $(\{A,E\},\{A,E\})$ and $(\{B,E\},\{B,E\})$. The label describing information that is influenced by the contents of both objects would be $(\{E\},\{A,B,E\})$.

5. A lattice $(L,\sqsubseteq,\sqcap,\sqcup,\top,\bot)$ is a partially ordered structure for which there is a greatest lower bound operation $\sqcap$ and a least upper bound $\sqcup$ that are defined for all elements of L, a top element $\top$ and a bottom element $\bot$.

(a) Show that any lattice $(L,\sqsubseteq,\sqcap,\sqcup,\top,\bot)$ can be seen to represent an information flow policy.

Answer:

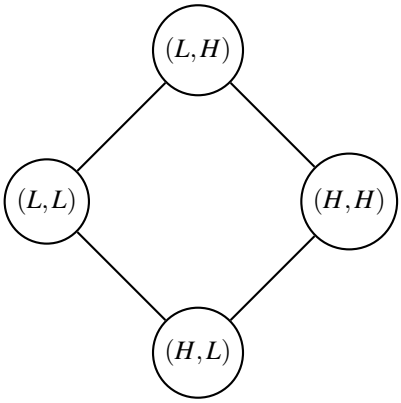
- $SC = L$
- $\rightarrow$=$\sqsubseteq$
- $\oplus = \sqcup$

(b) Given two lattices $(L_1,\sqsubseteq_1,\sqcap_1,\sqcup_1,\top_1,\bot_1)$ and $(L_2,\sqsubseteq_2,\sqcap_2,\sqcup_2,\top_2,\bot_2)$, then a new *product* lattice $(L_1 \times L_2,\sqsubseteq,\sqcap,\sqcup,\top,\bot)$ can be obtained by defining $\sqsubseteq$ as:

$$(l_1,l_2) \sqsubseteq (l_1',l_2') \textit{ iff } l_1 \sqsubseteq_1 l_1' \textit{ and } l_2 \sqsubseteq_2 l_2'$$

As a result, two lattice-based information flow policies can be combined by defining their product. Define the product of the High-Low information flow policies for integrity and for confidentiality using a Hasse diagram.

Answer:



3 Encoding Information Flow

1. Consider a *High (H) - Low (L)* security policy. For each of the following programs written in a standard imperative language, say whether they preserve confidentiality with respect to an attacker of level L. For each program, justify your answers by arguing why the program does not leak information, or give two inputs (initial values for variables) that would reveal the existance of an information leak.

   (a) $y_H := x_L; x_L := y_H + 1$

   Answer: Preserves confidentiality (with respect to level L) because, whatever the initial value of x_L, the final value of x_L is $x_L + 1$, regardless of the initial value of y_H.

   (b) $x_L := 42; x_L := y_H$

   Answer: Does not preserve confidentiality (with respect to level L) because the variable x_L is assigned different values that depend on (in this case, are exactly) the different possible values of a higher variable y_H. As counter-example consider two inputs that coincide on the values of x_H but differ on the values of y_H.

   (c) $x_L := y_H; x_L := 42$

   Answer:

   - If the attacker is able to see the intermediate values of computations, then the program does not preserve confientliatiy with respect to level L, as justified in 1b. As counter-example consider two inputs that coincide on the values of x_H but differ on the values of y_H.
   - If the attacker can only see final values, then the program does preserve confidentiality, as justified in 1d.

   (d) if $y_H = 0$ then $x_L := 42$ else $x_L := 42$

   Answer: Preserves confidentiality (with respect to level L) because every time the program runs, the variable x_L is always assigned the same value 42.

(e) if $x_L = 0$ then $x_L := 42$ else $x_L := 4242$

Answer: The program preserves confidentiality because the possible values that are assigned to variable x_L are determined solely by the initial value of x_L.

(f) $x_L := y_H$; if $x_L = 0$ then $x_L := 42$ else $x_L := 4242$

Answer:

- If the attacker is able to see the intermediate values of computations, then the program does not preserve confidentiality, as justified in 1c or 1e. As counter-example consider two inputs that coincide on the values of x_H but differ on the values of y_H.
- If the attacker can only see final values, then the program also does not preserve confidentiality, because the variable x_L is assigned different values (42 or 4242) depending on whther the initial value of a higher variable y_H is 0 or not. As counter-example consider two inputs that coincide on the values of x_H but on one input the value of y_H is 0 and on the other it is not.

(g) $x_L := 0$; while $y_H = 0$ do $x_L := 1$

Answer:

- If the attacker is able to see the intermediate values of computations, then the program does not preserve confidentiality because the variable x_L, after being assigned the level 0, can be assigned or not a new value (1) depending on whether the initial value of a higher variable y_H is 0 or not (respectively). As counter-example consider two inputs that coincide on the values of x_H but on one input the value of y_H is 0 and on the other it is not.
- If the attacker can see non-terminating computations, or the duration of computations, then the program does not preserve confidentiality because computation will terminate or not, or take a different time, depending on whether the initial value of variable y_H is 0 or not. As counter-example consider two inputs that coincide on the values of x_H but on one input the value of y_H is 0 and on the other it is not.
- If the attacker can only see final values, then the program preserves confidentiliaty because the final value of x_L will always be 0.

(h) $x_L := y_H$; while $x_L \neq 0$ do $x_L := x_L - 1$

Answer:

- If the attacker is able to see the intermediate values of computations, then the program does not preserve confidentiality, as justified in 1c. As counter-example consider two inputs that coincide on the values of x_H but differ on the values of y_H.
- If the attacker can only see final values, then it preserves confidentiality because the final value of x_L is always the same (0).

(i) $x_L := 0$; while $x_L \neq y_H$ do $x_L := x_L + 1$

Answer:

- If the attacker can only see final values, then the program does not preserve confidentiality because for different initial values of y_H that are not lower than 0, the final value of x_L will be different (in this case, the same as y_H). As counter-example consider two inputs that coincide on the values of x_H but differ on the values of y_H, that are non-negative.

- If the attacker can see non-terminating computations then the program does not preserve confidentiality, because the program will terminate or not depending on whether the initial value of y_H is non-negative 0 or not (respectively). As counter-example consider two inputs that coincide on the values of x_H but for one input the value of y_H is greater or equal than 0 and for the other it is not.
- If the attacker can see computation duration, then the program does not preserve confidentiality, because the number of steps that the program will take will coincide with the initial value of y_H when it is non-negative. As counter-example consider two inputs that coincide on the values of x_H but differ on the values of y_H, while being non-negative.

Answer: Note: This exercise was presented before the class on formalizing Noninterference, so the answers can be informal. Note that for this exercise the power of the attacker is not specified. For a formal justification using Deterministic Input-Output Noninterference, see exercise **4.ii** in the following exercise sheet.

4 Tool development - Patterns and Flow Labels

As we have seen, and you will study further in future classes, programs can encode security vulnerabilities in the form of potentially dangerous information flows, by enabling untrusted information inserted by an attacker via input functions (known as *sources*) to reach the arguments of sensitive functions or variables (so called *sinks*) and induce the program to perform security violations.

It is possible to develop tools for detecting such vulnerabilities by tracking illegal flows from sources to sinks, and analysing whether they are processed by *sanitizers*, which are special functions that can neutralize the potential vulnerability, or validate that there is none. Such a tool will need to receive as input information about vulnerability *patterns* that should be detected. It will also need to work with an *information flow policy* that determines which *security labels* should be assigned to resources in a program, and how these labels can be combined and updated.

1. Develop a class Pattern, that represents a vulnerability pattern, including all its components. It should include at least the following basic operations:

   (a) Constructor of a Pattern object, receiving as input a vulnerability name, lists of possible source, sanitizer and sink names.

   (b) Selectors for each of its compomnents.

   (c) Tests for checking whether a given name is a source, sanitizer or sink for the pattern.

2. Develop a class Label, that represents the integrity of information that is carried by a resource. It should capture the sources that might have influenced a certain piece of information, and which sanitizers might have intercepted the information since its flow from each source. It should include at least the following basic operations:

   (a) Constructors of a Label object, and operations for adding sources to the label, and sanitizers that are intercepting the flows.

   (b) Selectors for each of its components.

   (c) Combinor for returning a new label that represents the integrity of information that results from combining two pieces of information.

   Note: Labels must be mutable, which means that the new labels should be independent from the original ones.

3. Develop a class MultiLabel, that generalizes the Label class in order to be able to represent distinct labels corresponding to different patterns. It should include corresponding constructors, selectors and combinor. Have in mind that sources and sanitizers should only be added to labels corresponding to patterns for which that name is a source/sanitizer.