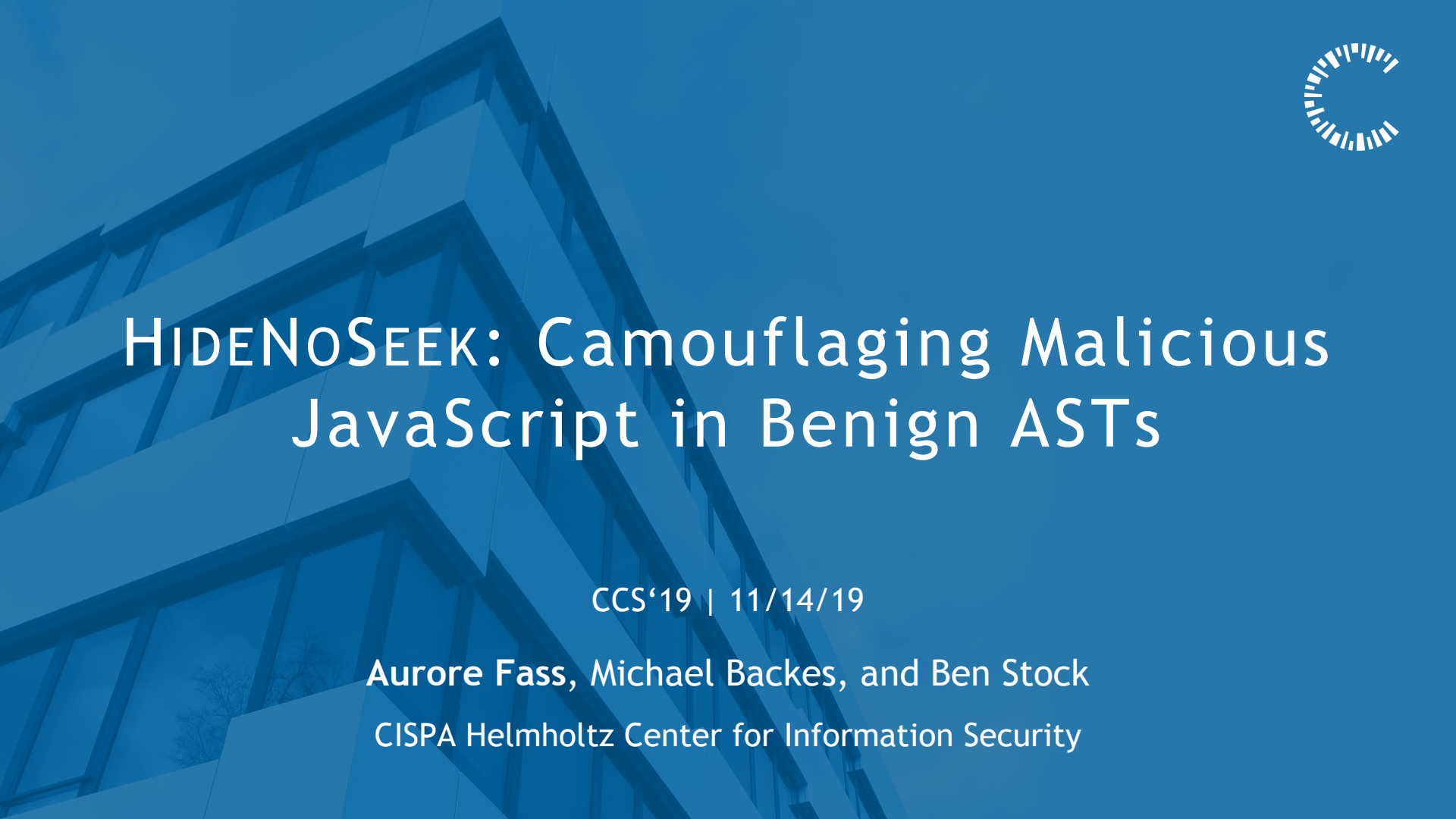


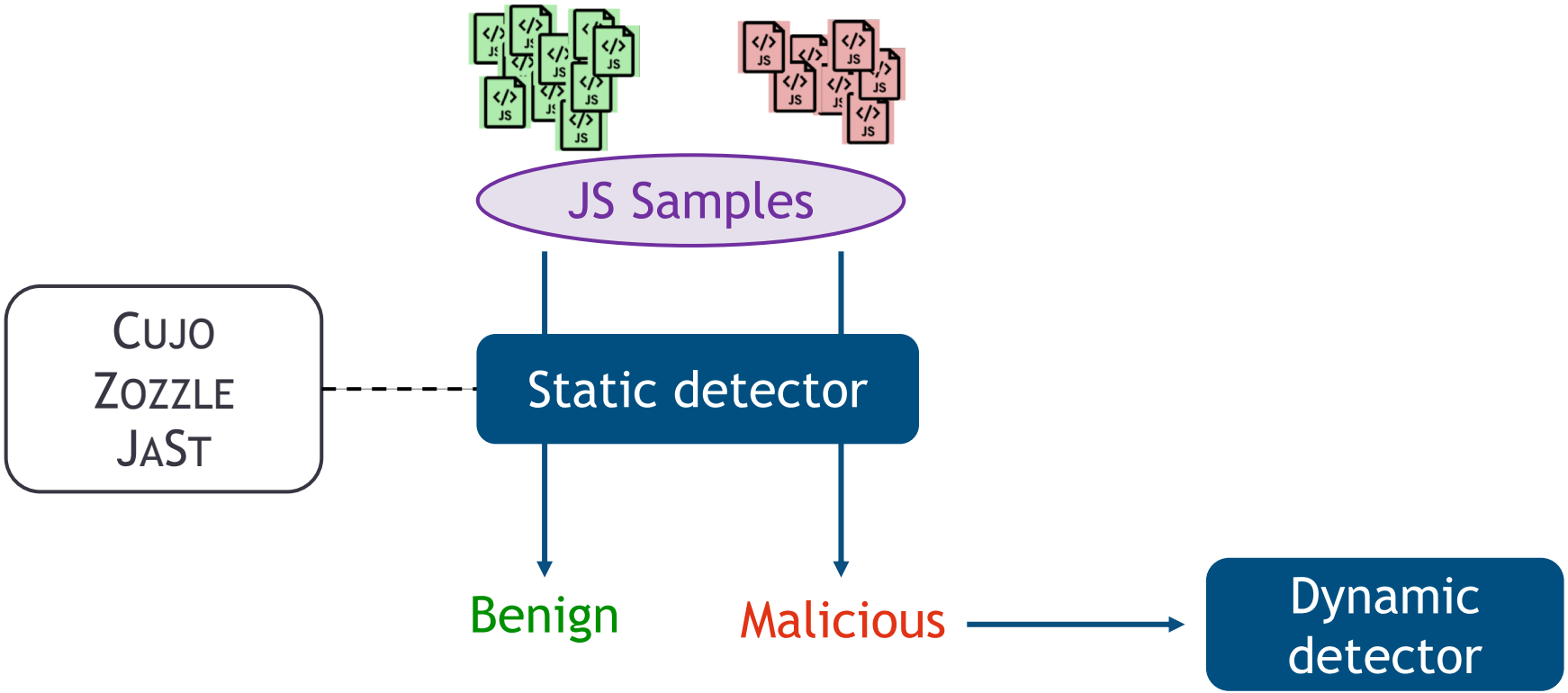
HideNoSeek: Camouflaging Malicious JavaScript in Benign ASTs

CCS'19 | 11/14/19

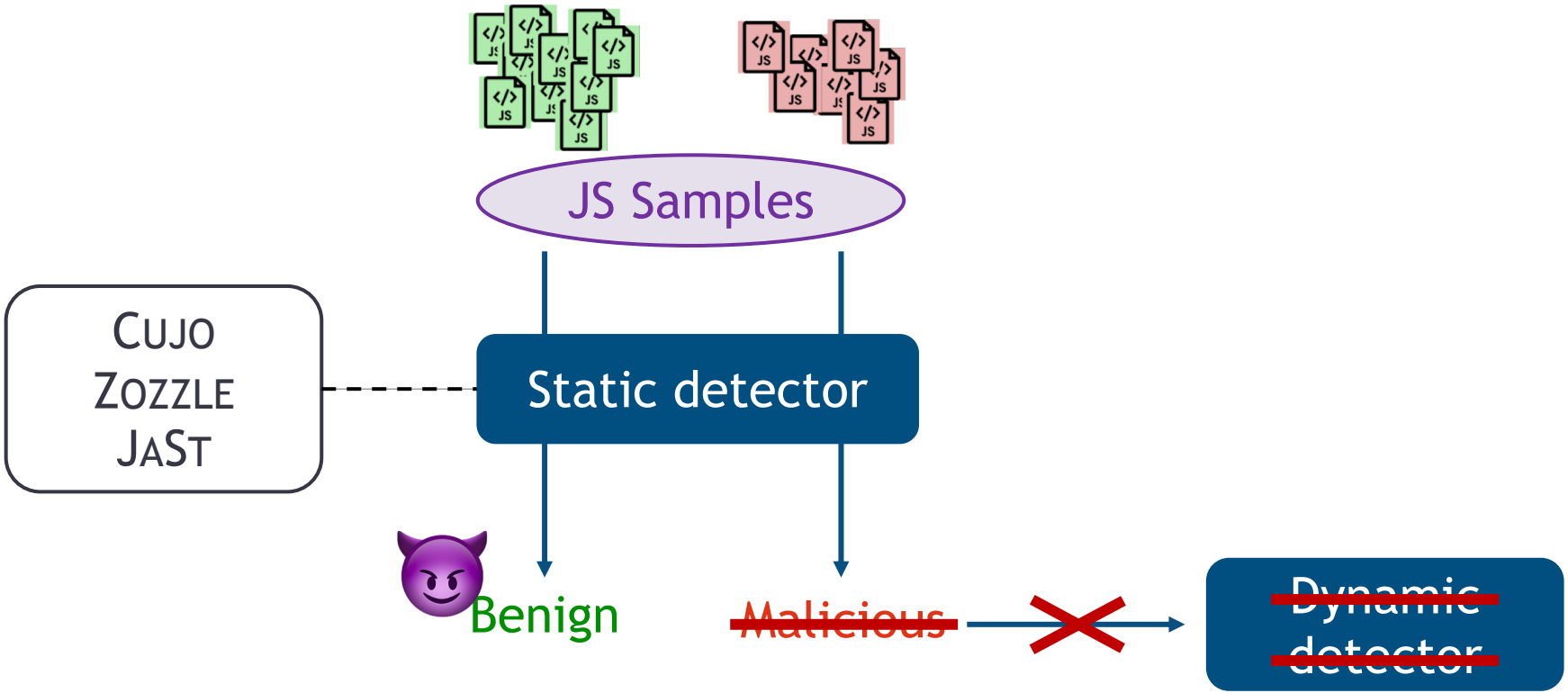
Aurore Fass, Michael Backes, and Ben Stock

CISPA Helmholtz Center for Information Security

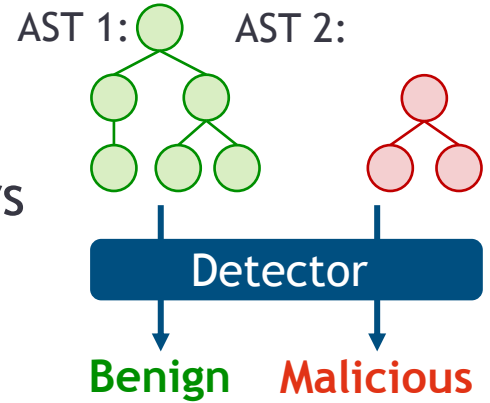
Motivation


JS Samples
CUJO
ZOZZLE
JAST
Static detector
Benign
Malicious
Dynamic detector

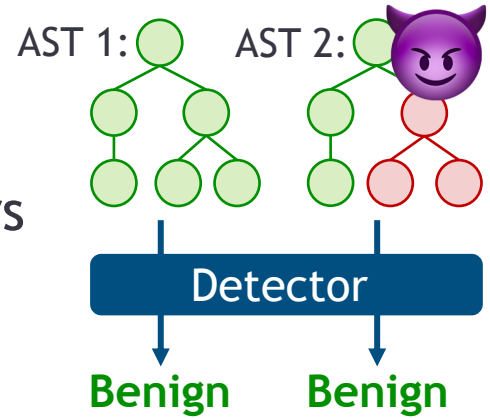
Motivation


JS Samples
CUJO
ZOZZLE
JAST
Static detector
Benign
Malicious
Dynamic detector

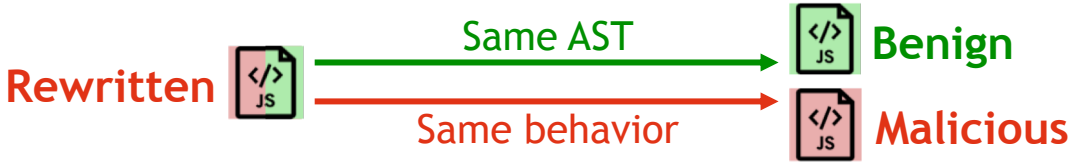
- Generic camouflage attack
  - ➢ Effective against static JavaScript detectors



- Generic camouflage attack
  - ➢ Effective against static JavaScript detectors



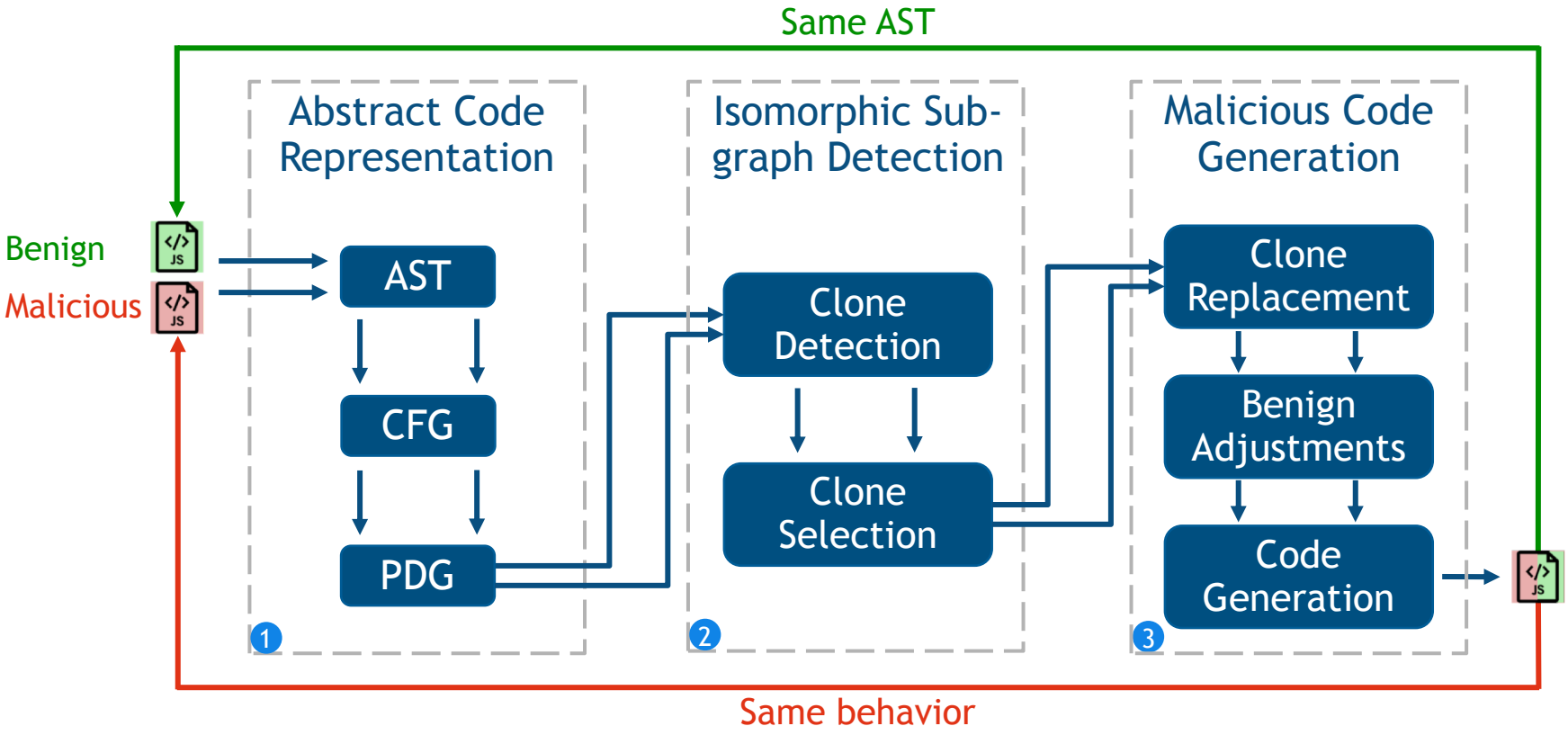
- Rewrites malicious JavaScript files



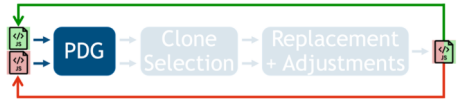
Contributions

- Perfect mapping onto a benign AST → very effective attack
- Generic attack, can be applied to several static detectors
- Independent of any machine learning systems
- Does not need any internal knowledge (e.g., model, dataset)

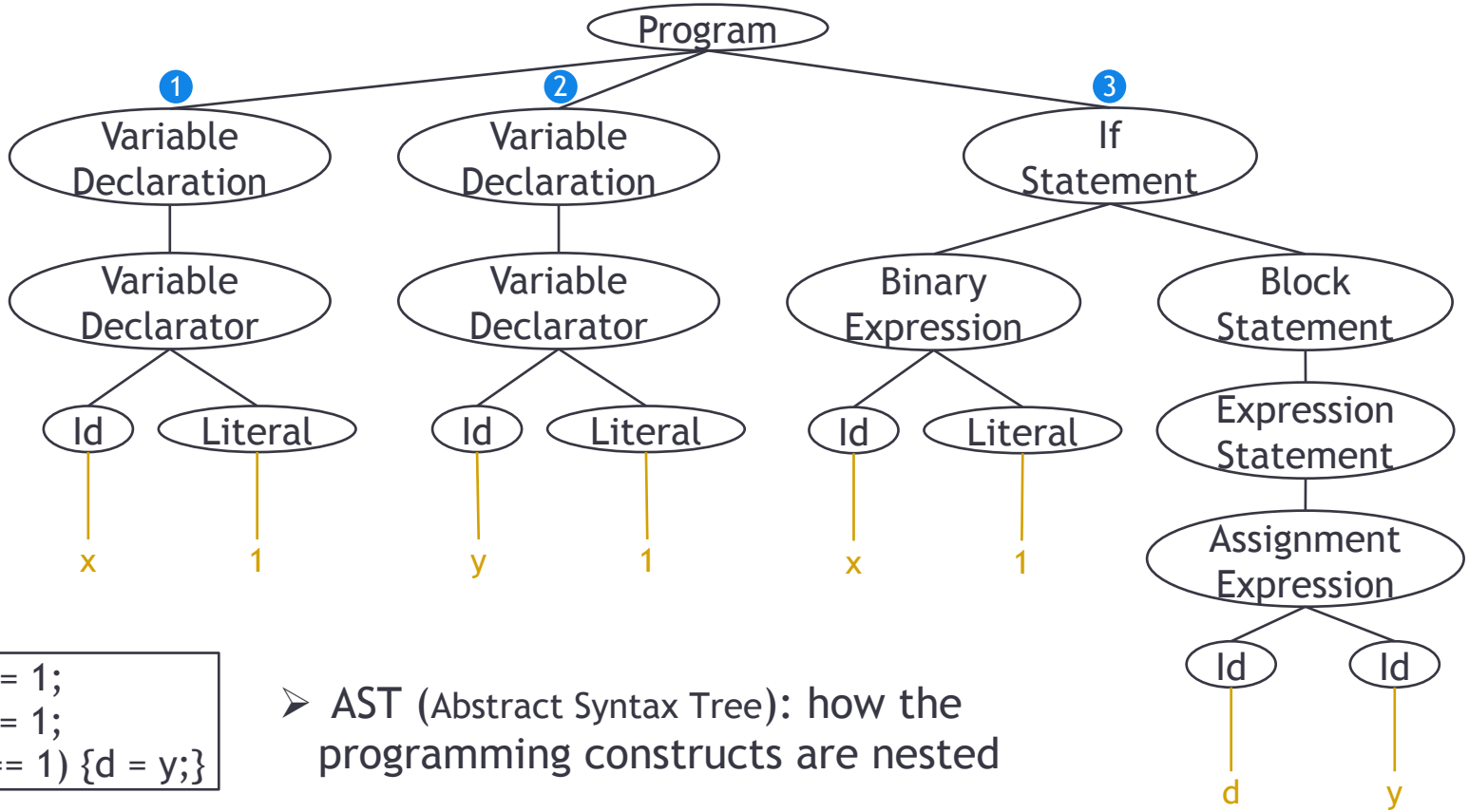
Methodology



Abstract Code Representation: PDG



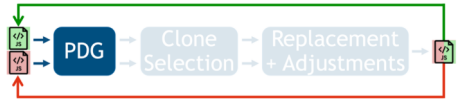
CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY



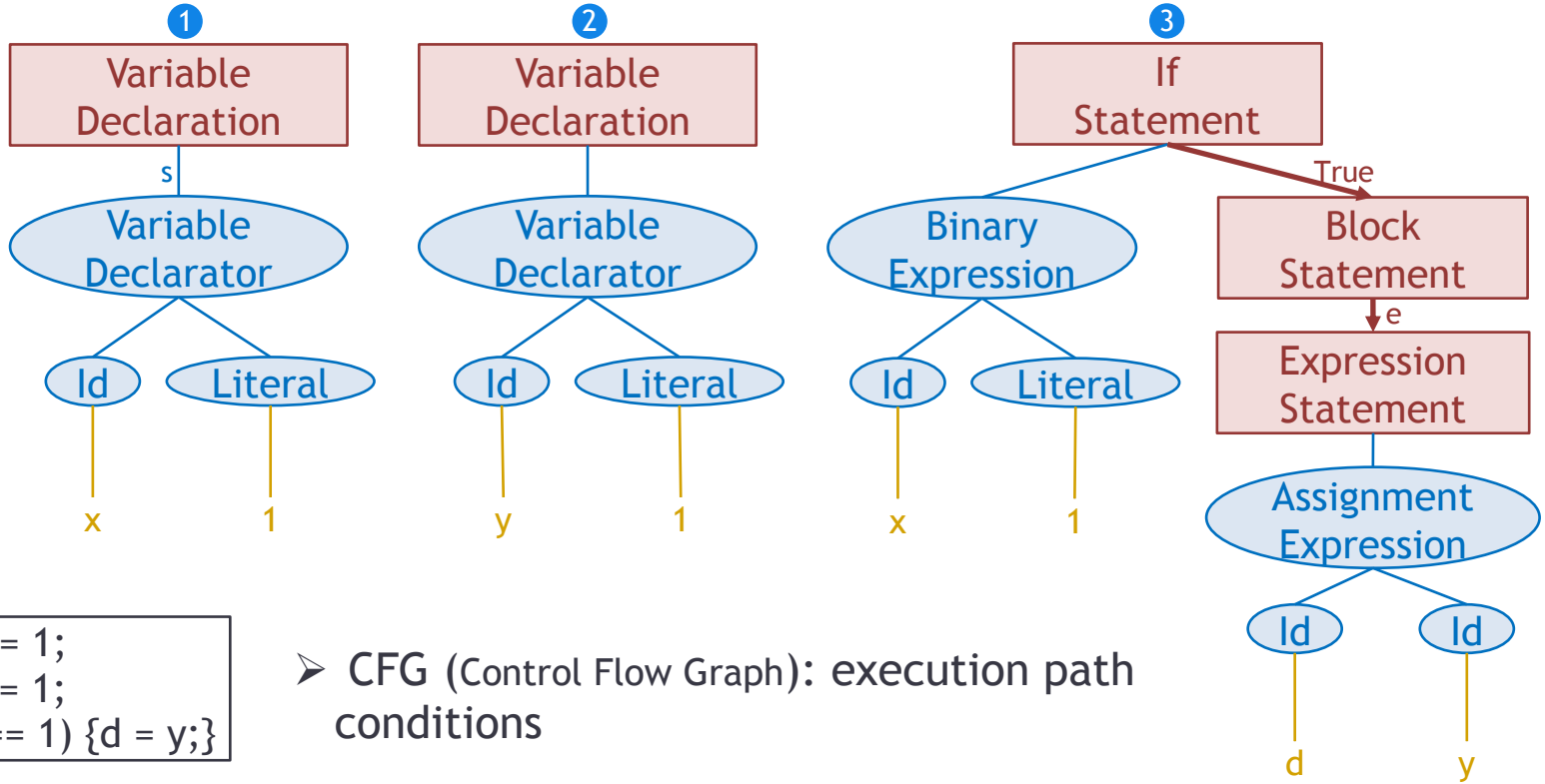

```
1 var x = 1;
2 var y = 1;
3 if (x == 1) {d = y;}
```

- AST (Abstract Syntax Tree): how the programming constructs are nested

Abstract Code Representation: PDG



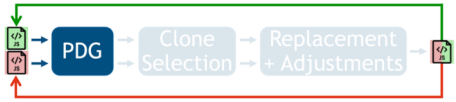
CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY



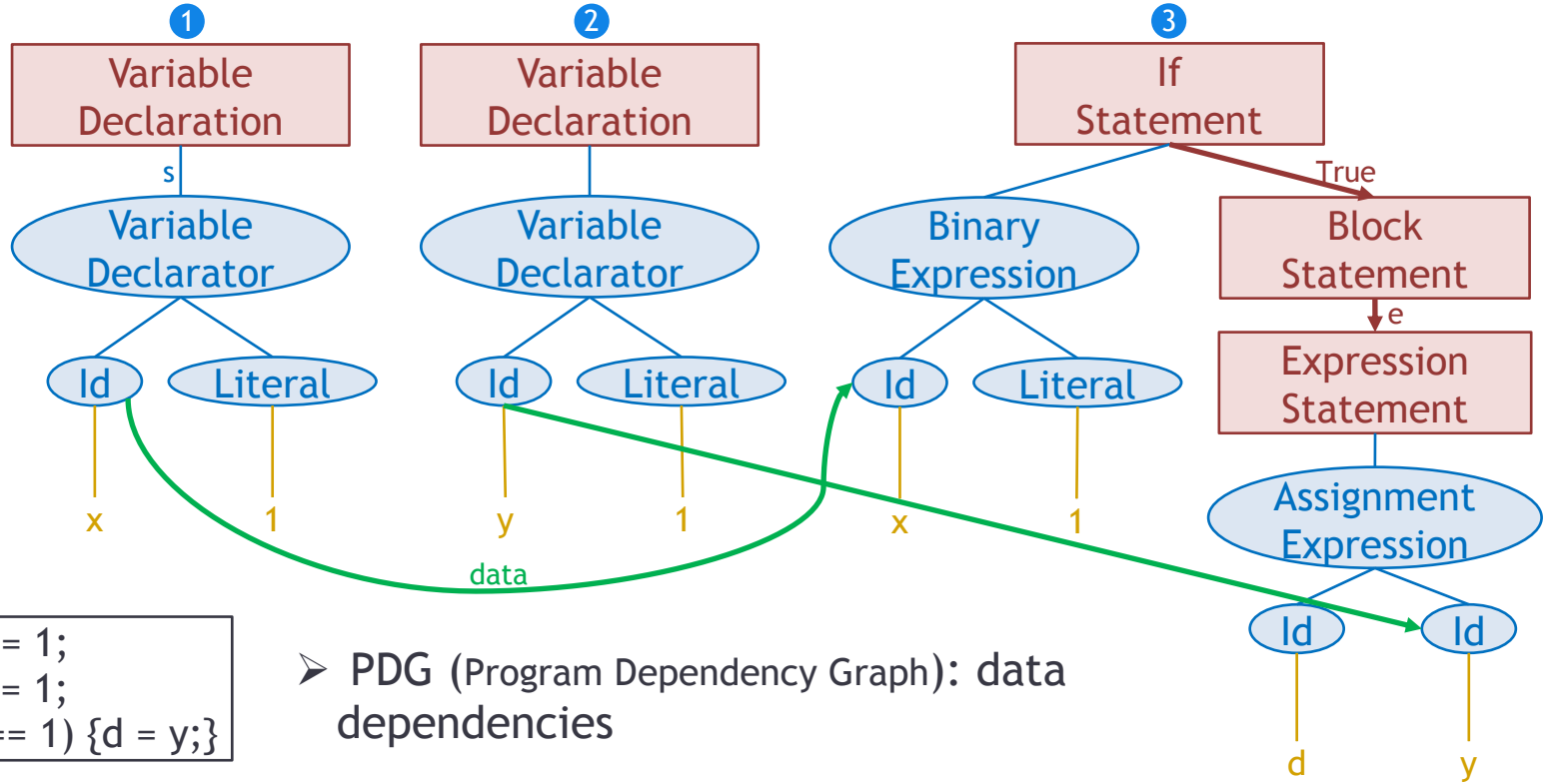
1. `var x = 1;`
2. `var y = 1;`
3. `if (x == 1) {d = y;}`

- CFG (Control Flow Graph): execution path conditions

Abstract Code Representation: PDG



CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY




```
1 var x = 1;
2 var y = 1;
3 if (x == 1) {d = y;}
```

- PDG (Program Dependency Graph): data dependencies

Clone Detection – Code Level

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Malicious seed

```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Clone:

```
Identifier = Identifier . Identifier ( Literal )

Identifier . Identifier ( Literal , Literal )
```

Clone Detection – PDG Level

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Malicious seed

```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Benign PDG

```
1 Identifier = Identifier . Identifier ( Literal )
2 Identifier . Identifier ( Literal , ThisExpression )
3 Identifier . Identifier ( Literal , Literal )
4 Identifier ( Identifier , Literal , ThisExpression )
5 Identifier ( Identifier , Literal , ThisExpression )
```

Malicious PDG

```
A Identifier = Identifier . Identifier ( Literal )
B Identifier . Identifier ( Literal , Literal )
```

Clone Detection – PDG Level

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Malicious seed

```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Benign PDG

```
1 Identifier = Identifier . Identifier ( Literal )
2 Identifier . Identifier ( Literal , ThisExpression )
3 Identifier . Identifier ( Literal , Literal )
4 Identifier ( Identifier , Literal , ThisExpression )
5 Identifier ( Identifier , Literal , ThisExpression )
```

Malicious PDG

```
A Identifier = Identifier . Identifier ( Literal )
B Identifier . Identifier ( Literal , Literal )
```

=

	Benign	Malicious
Clone 1	1	A

Clone Detection – PDG Level

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Malicious seed

```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Benign PDG

```
1 Identifier = Identifier . Identifier ( Literal )
2 Identifier . Identifier ( Literal , ThisExpression )
3 Identifier . Identifier ( Literal , Literal )
4 Identifier ( Identifier , Literal , ThisExpression )
5 Identifier ( Identifier , Literal , ThisExpression )
```

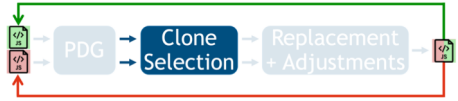
Malicious PDG

```
A Identifier = Identifier . Identifier ( Literal )
B Identifier . Identifier ( Literal , Literal )
```

≠

	Benign	Malicious
Clone 1	1	A

Clone Detection – PDG Level



CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Malicious seed

```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Benign PDG

```
1 Identifier = Identifier . Identifier ( Literal )
2 Identifier . Identifier ( Literal , ThisExpression )
3 Identifier . Identifier ( Literal , Literal )
4 Identifier ( Identifier , Literal , ThisExpression )
5 Identifier ( Identifier , Literal , ThisExpression )
```

Malicious PDG

```
A Identifier = Identifier . Identifier ( Literal )
B Identifier . Identifier ( Literal , Literal )
```

≠

	Benign	Malicious
Clone 1	1	A

Clone Detection – PDG Level

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Malicious seed

```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Benign PDG

```
1 Identifier = Identifier . Identifier ( Literal )
2 Identifier . Identifier ( Literal , ThisExpression )
3 Identifier . Identifier ( Literal , Literal )
4 Identifier ( Identifier , Literal , ThisExpression )
5 Identifier ( Identifier , Literal , ThisExpression )
```

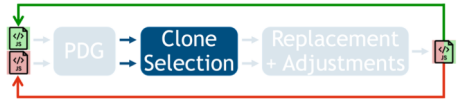
Malicious PDG

```
A Identifier = Identifier . Identifier ( Literal )
B Identifier . Identifier ( Literal , Literal )
```

≠

	Benign	Malicious
Clone 1	1	A

Clone Detection – PDG Level



CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Malicious seed

```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Benign PDG

1. Identifier = Identifier . Identifier (Literal)
2. Identifier . Identifier (Literal , ThisExpression)
3. Identifier . Identifier (Literal , Literal)
4. Identifier (Identifier , Literal , ThisExpression)
5. Identifier (Identifier , Literal , ThisExpression)

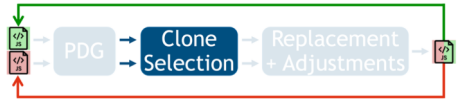
≠

Malicious PDG

A. Identifier = Identifier . Identifier (Literal)
B. Identifier . Identifier (Literal , Literal)

	Benign	Malicious
Clone 1	1	A

Clone Detection – PDG Level



CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Malicious seed

```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Benign PDG

```
1 Identifier = Identifier . Identifier ( Literal )
2 Identifier . Identifier ( Literal , ThisExpression )
3 Identifier . Identifier ( Literal , Literal )
4 Identifier ( Identifier , Literal , ThisExpression )
5 Identifier ( Identifier , Literal , ThisExpression )
```

Malicious PDG

```
A Identifier = Identifier . Identifier ( Literal )
B Identifier . Identifier ( Literal , Literal )
```

≠

	Benign	Malicious
Clone 1	1	A

Clone Detection – PDG Level

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Malicious seed

```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Benign PDG

```
1 Identifier = Identifier . Identifier ( Literal )
2 Identifier . Identifier ( Literal , ThisExpression )
3 Identifier . Identifier ( Literal , Literal )
4 Identifier ( Identifier , Literal , ThisExpression )
5 Identifier ( Identifier , Literal , ThisExpression )
```

Malicious PDG

```
A Identifier = Identifier . Identifier ( Literal )
B Identifier . Identifier ( Literal , Literal )
```

≠

	Benign	Malicious
Clone 1	1	A

Clone Detection – PDG Level

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Malicious seed

```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Benign PDG

```
1 Identifier = Identifier . Identifier ( Literal )
2 Identifier . Identifier ( Literal , ThisExpression )
3 Identifier . Identifier ( Literal , Literal )
4 Identifier ( Identifier , Literal , ThisExpression )
5 Identifier ( Identifier , Literal , ThisExpression )
```

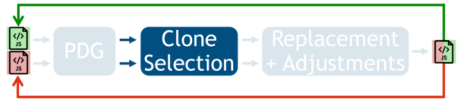
Malicious PDG

```
A Identifier = Identifier . Identifier ( Literal )
B Identifier . Identifier ( Literal , Literal )
```

=

	Benign	Malicious
Clone 1	1	A
Clone 2	3	B

Clone Detection – PDG Level



CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Malicious seed

```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Benign PDG

```
1 Identifier = Identifier . Identifier ( Literal )
2 Identifier . Identifier ( Literal , ThisExpression )
3 Identifier . Identifier ( Literal , Literal )
4 Identifier ( Identifier , Literal , ThisExpression )
5 Identifier ( Identifier , Literal , ThisExpression )
```

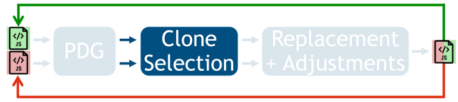
Malicious PDG

```
A Identifier = Identifier . Identifier ( Literal )
B Identifier . Identifier ( Literal , Literal )
```

≠

	Benign	Malicious
Clone 1	1	A
Clone 2	3	B

Clone Detection – PDG Level



CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Malicious seed

```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Benign PDG

```
1 Identifier = Identifier . Identifier ( Literal )
2 Identifier . Identifier ( Literal , ThisExpression )
3 Identifier . Identifier ( Literal , Literal )
4 Identifier ( Identifier , Literal , ThisExpression )
5 Identifier ( Identifier , Literal , ThisExpression )
```

Malicious PDG

```
A Identifier = Identifier . Identifier ( Literal )
B Identifier . Identifier ( Literal , Literal )
```

=

	Benign	Malicious
Clone 1	1	A
Clone 2	3 1	B A

Clone Detection – PDG Level

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Malicious seed

```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Benign PDG

```
1 Identifier = Identifier . Identifier ( Literal )
2 Identifier . Identifier ( Literal , ThisExpression )
3 Identifier . Identifier ( Literal , Literal )
4 Identifier ( Identifier , Literal , ThisExpression )
5 Identifier ( Identifier , Literal , ThisExpression )
```

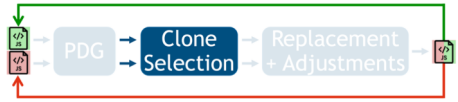
Malicious PDG

```
A Identifier = Identifier . Identifier ( Literal )
B Identifier . Identifier ( Literal , Literal )
```

≠

	Benign	Malicious
Clone 1	1	A
Clone 2	3 1	B A

Clone Detection – PDG Level



CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Malicious seed

```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Benign PDG

```
1 Identifier = Identifier . Identifier ( Literal )
2 Identifier . Identifier ( Literal , ThisExpression )
3 Identifier . Identifier ( Literal , Literal )
4 Identifier ( Identifier , Literal , ThisExpression )
5 Identifier ( Identifier , Literal , ThisExpression )
```

Malicious PDG

```
A Identifier = Identifier . Identifier ( Literal )
B Identifier . Identifier ( Literal , Literal )
```

≠

	Benign	Malicious
Clone 1	1	A
Clone 2	3 1	B A

Clone Selection

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Malicious seed

```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Clone:

```
Identifier = Identifier . Identifier ( Literal )
Identifier . Identifier ( Literal , Literal )
```

	Benign	Malicious
~~Clone 1~~	~~1~~	~~A~~
Clone 2	3 1	B A

Clone Replacement

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

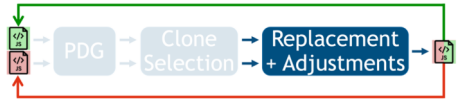
Malicious seed

```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Crafted sample

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Clone Replacement



CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

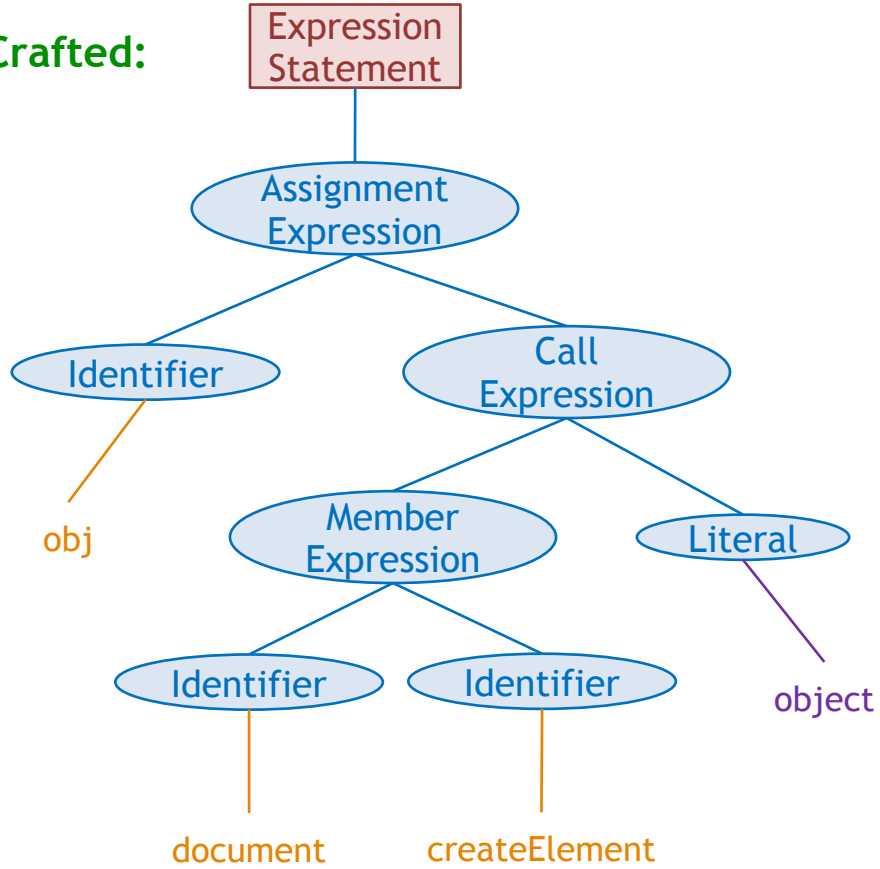
Benign:

```
obj = document.createElement("object");
```

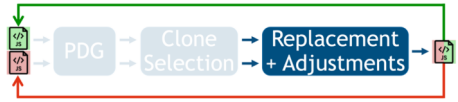
Malicious:

```
wscript = WScript.CreateObject('WScript.Shell');
```

Crafted:



Clone Replacement



CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

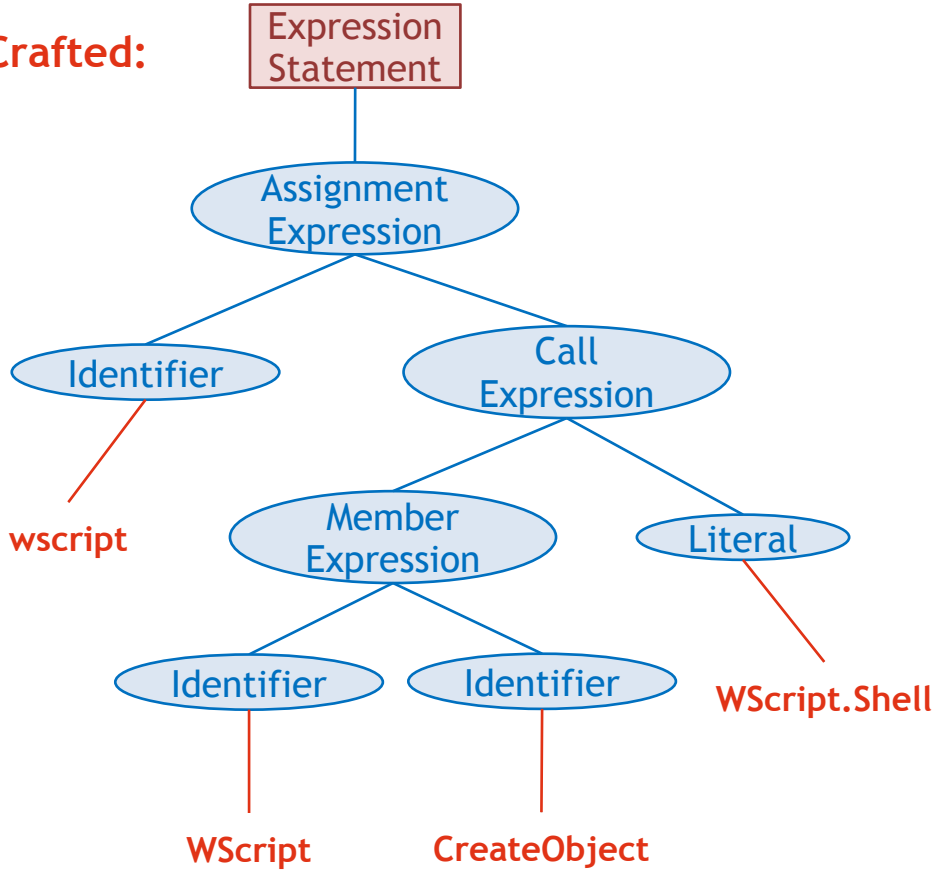
Benign:

```
obj = document.createElement("object");
```

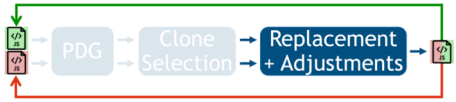
Malicious:

```
wscript = WScript.CreateObject('WScript.Shell');
```

Crafted:



Clone Replacement



CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Malicious seed

```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Crafted sample

```
1 wscript = WScript.CreateObject('WScript.Shell');
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Clone Replacement

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

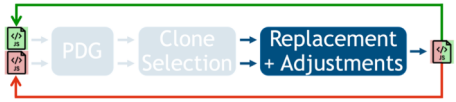
Malicious seed

```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Crafted sample

```
1 wscript = WScript.CreateObject('WScript.Shell');
2 obj.setAttribute("id", this.internal.flash.id);
3 wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Benign Adjustments



CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Malicious seed

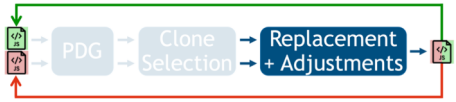
```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Crafted sample

- obj?
- setAttribute?
- createParam?

```
1 wscript = WScript.CreateObject('WScript.Shell');
2 obj.setAttribute("id", this.internal.flash.id);
3 wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Benign Adjustments



CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Malicious seed

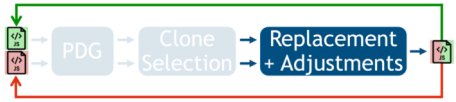
```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Crafted sample

```
1 wscript = WScript.CreateObject('WScript.Shell');
2 obj.setAttribute("id", this.internal.flash.id);
3 wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

- obj?
- setAttribute?
- createParam?

Benign Adjustments



CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Malicious seed

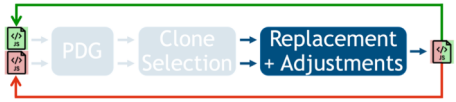
```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Crafted sample

- ~~obj?~~
- setAttribute?
- createParam?

```
1 wscript = WScript.CreateObject('WScript.Shell');
2 wscript.setAttribute("id", this.internal.flash.id);
3 wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
4 createParam(wscript, "bgcolor", this.options.backgroundColor);
5 createParam(wscript, "wmode", this.options.wmode);
```

Benign Adjustments



CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Malicious seed

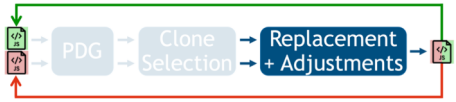
```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Crafted sample

- ~~obj?~~
- setAttribute?
- createParam?

```
1 wscript = WScript.CreateObject('WScript.Shell');
2 wscript.setAttribute("id", this.internal.flash.id);
3 wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
4 createParam(wscript, "bgcolor", this.options.backgroundColor);
5 createParam(wscript, "wmode", this.options.wmode);
```

Benign Adjustments



CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Malicious seed

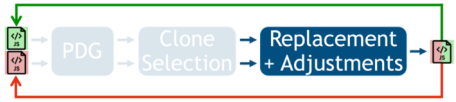
```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Crafted sample

- ~~obj?~~
- ~~setAttribute?~~
- createParam?

```
1 wscript = WScript.CreateObject('WScript.Shell');
2 wscript.toString("id", this.internal.flash.id);
3 wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
4 createParam(wscript, "bgcolor", this.options.backgroundColor);
5 createParam(wscript, "wmode", this.options.wmode);
```

Benign Adjustments



CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Malicious seed

```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Crafted sample

- ~~obj?~~
- ~~setAttribute?~~
- createParam?

```
1 wscript = WScript.CreateObject('WScript.Shell');
2 wscript.toString("id", this.internal.flash.id);
3 wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
4 createParam(wscript, "bgcolor", this.options.backgroundColor);
5 createParam(wscript, "wmode", this.options.wmode);
```

Benign Adjustments

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Malicious seed

```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Crafted sample

- ~~obj?~~
- ~~setAttribute?~~
- ~~createParam?~~

```
1 wscript = WScript.CreateObject('WScript.Shell');
2 wscript.toString("id", this.internal.flash.id);
3 wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
4 decodeURI(wscript, "bgcolor", this.options.backgroundColor);
5 parseFloat(wscript, "wmode", this.options.wmode);
```

Code Generation With Escodegen

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Benign input

```
1 obj = document.createElement("object");
2 obj.setAttribute("id", this.internal.flash.id);
3 obj.setAttribute("type", "application/x-shockwave-flash");
4 createParam(obj, "bgcolor", this.options.backgroundColor);
5 createParam(obj, "wmode", this.options.wmode);
```

Malicious seed

```
A wscript = WScript.CreateObject('WScript.Shell');
B wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
```

Same behavior

Crafted sample

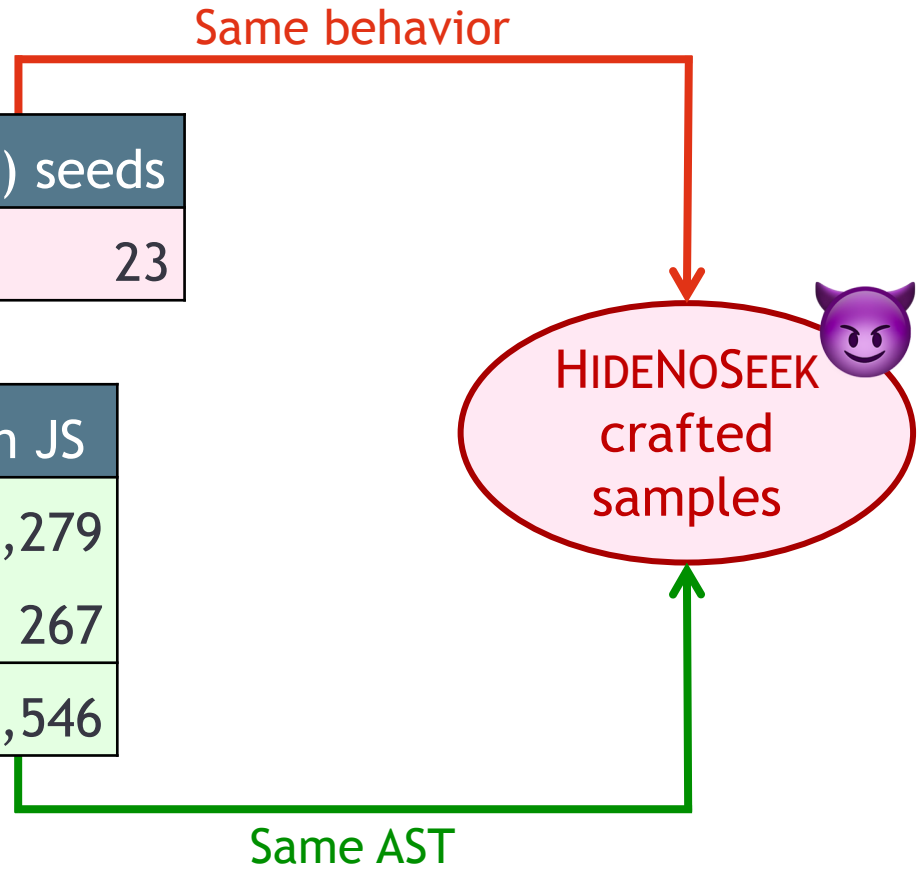
Same AST

```
wscript = WScript.CreateObject('WScript.Shell');
wscript.toString("id", this.internal.flash.id);
wscript.run("cmd.exe /c \"<malicious powershell command>;\"", "0");
decodeURI(wscript, "bgcolor", this.options.backgroundColor);
parseFloat(wscript, "wmode", this.options.wmode);
```

Experimental Setup

#Malicious JS	#Malicious (deobf) seeds
122,345	23

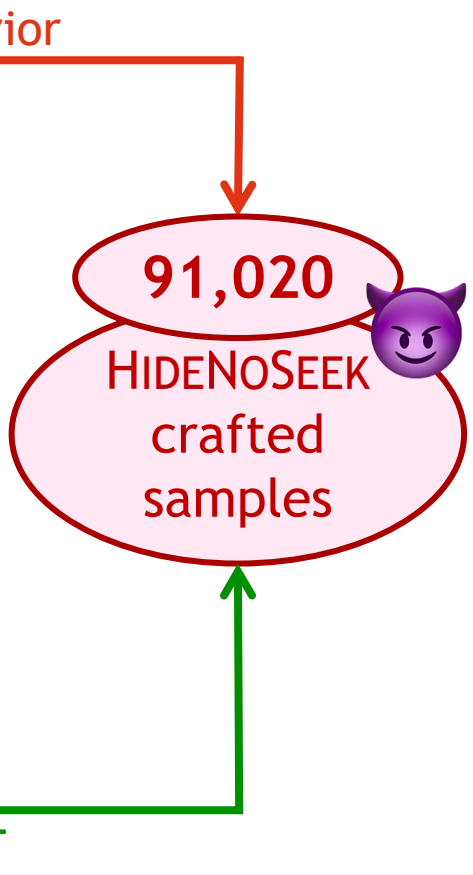
Benign JS - Source	#Benign JS
Alexa Top 10k	8,279
Libraries	267
Sum	8,546



Evasive Samples Generation

#Malicious JS	#Malicious (deobf) seeds
122,345	22 / 23

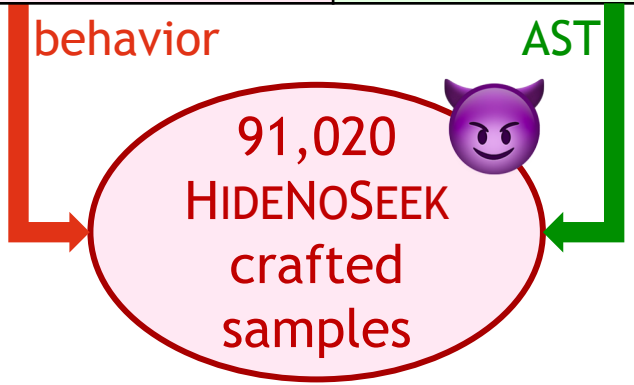
Benign JS - Source	#Benign JS
Alexa Top 10k	8,279
Libraries	267
Sum	8,546



Evasive Samples Generation – per Seed

Malicious seeds	#Crafted samples
Misc	6,487
EK	6,487
Injected1	6,447
…	…
RIG1	244
Dropper	10
RIG2	0
Sum	91,020

#Malicious seeds	#Alexa Top 10k
22 / 23	8,279



- Success: depends on common syntactic structures between seeds and benign scripts

Impact of our Attack

Alexa Top 10	#Seeds hidden (/23)
1 google.com	18
2 youtube.com	18
3 facebook.com	13
4 baidu.com	8
5 wikipedia.org	0
6 qq.com	14
7 yahoo.com	14
8 taobao.com	19
9 tmall.com	17
10 amazon.com	17

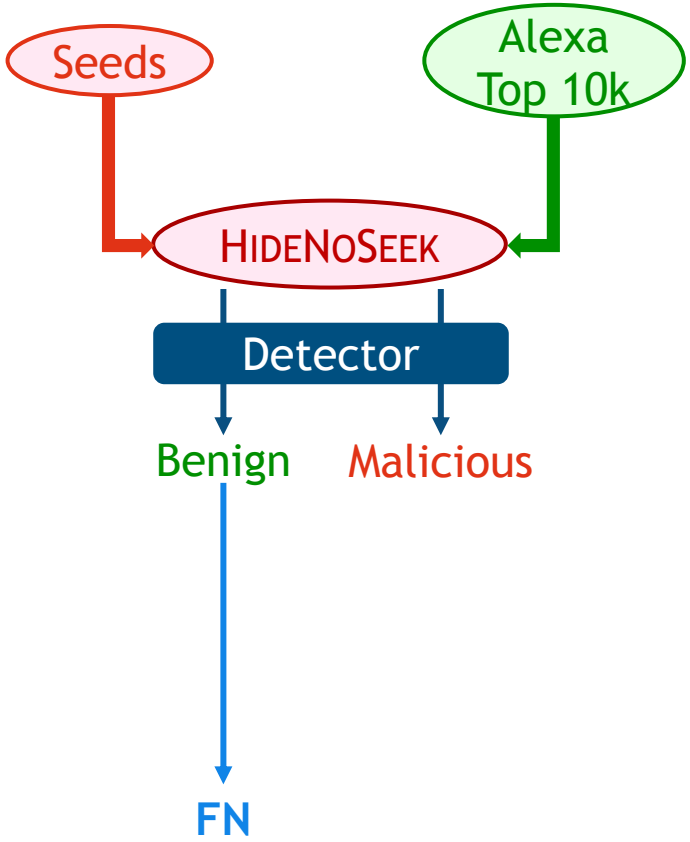
Libraries	#Seeds hidden (/23)
jQuery	17
Bootstrap	12
Modernizr	5
MooTools	15
Angular	17

- jQuery 1.12.4 → 30% websites
- HIDENOSEEK can craft on average:
  - 14 malware for each Alexa Top 10
  - 13 malware for each Top 5 library

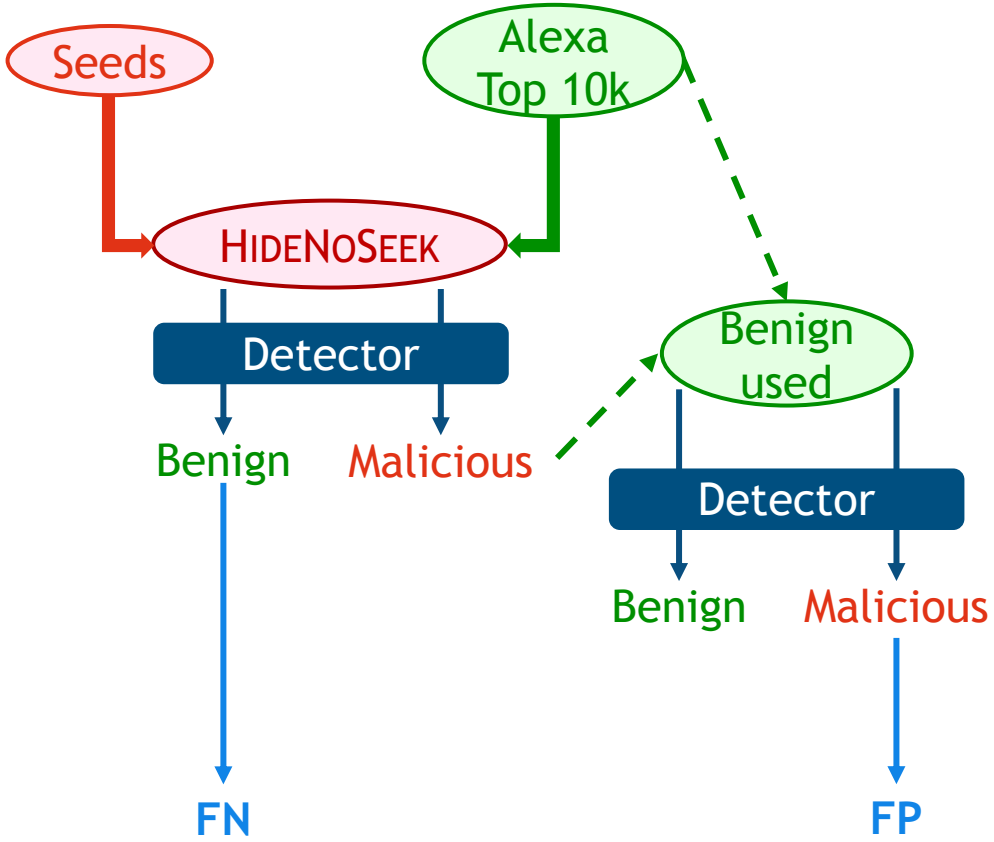
Properties of the Crafted Samples

- Same AST for crafted and benign samples
- Most of the tokens: identical between crafted and benign samples
- 72% of the crafted samples are still running
- 67% of the running samples have a malicious behavior

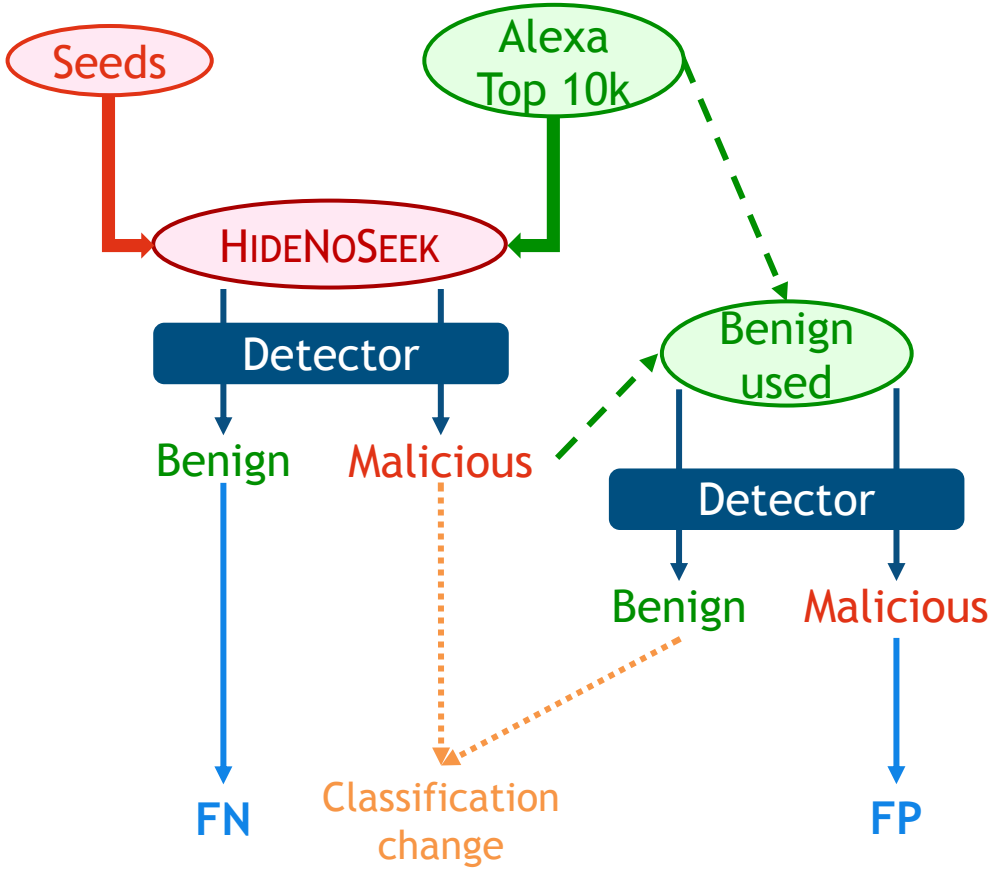
Evaluation Against Real-World Classifiers



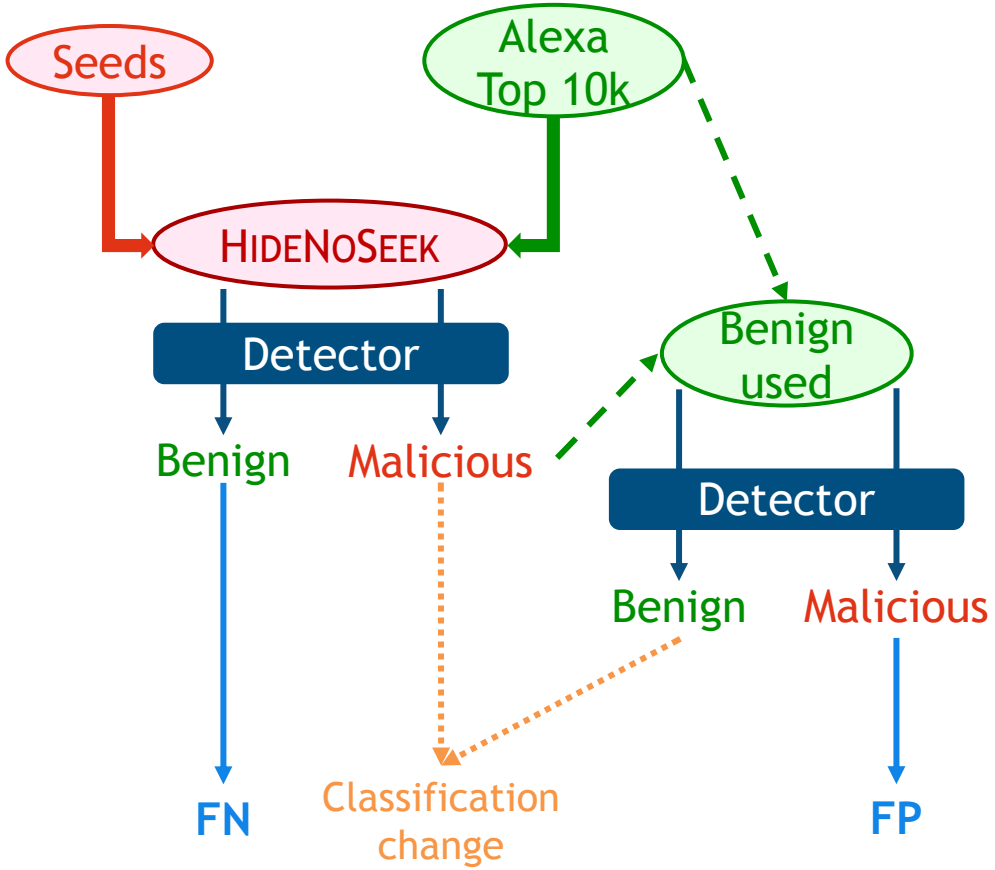
Evaluation Against Real-World Classifiers



Evaluation Against Real-World Classifiers



Evaluation Against Real-World Classifiers



	Training set from the wild	Training set from the wild + HIDENOSEEK	
	FN	FN	FP
JAST (syntactic)	99.98%	4.32%	100.00%
ZOZZLE (syntactic)	~100.00%	8.44%	88.74%
CUJO (lexical)	99.99%	4.04%	95.96%

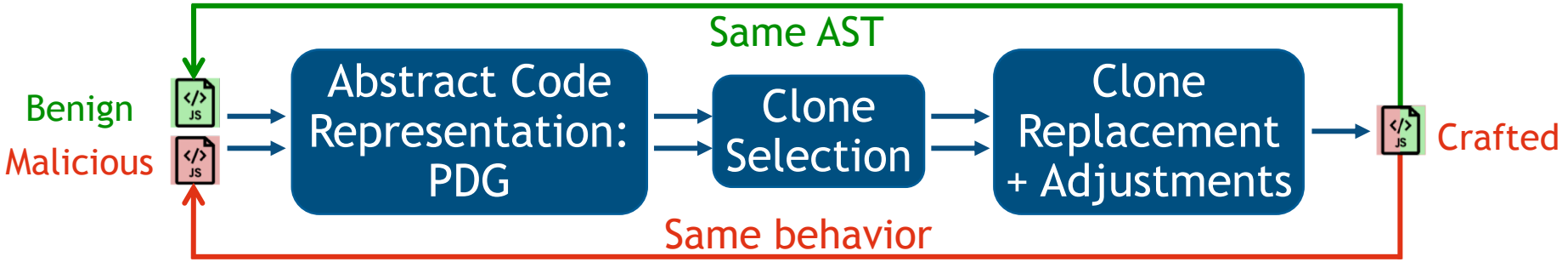
0.57%

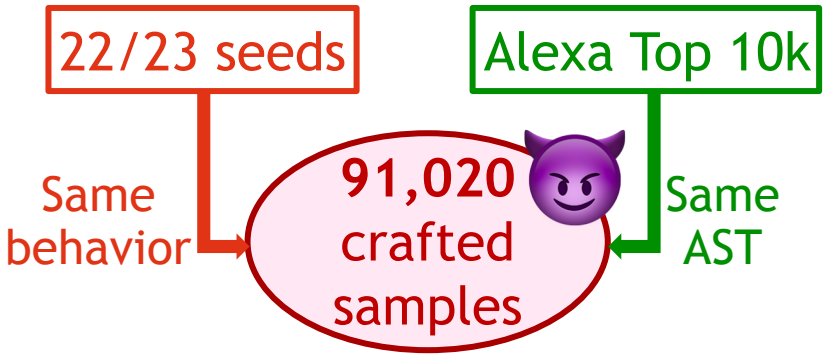
0.33%

≥ 99.98% FN

> 88.74% FP

Conclusion: HIDENOSEEK





- ✓Standard training set: ≥ **99.98% FN**
- ✓HIDENOSEEK in training set: > **88.74% FP**
- ➢Lexical/syntactic detectors: not reliable

Thank you

@AuroreFass @kcotsneb

Aurore54F/HideNoSeek