USING MACHINE LEARNING TO DETECT MALICIOUS POLYGLOT IMAGES

Galit Vaknin galit1321@gmail.com
Ifat Neumann ineumann19@gmail.com
Michal Shawat m1245sh@gmail.com

Instructor: Assaf Barak

CS@BIU המחלקה למדעי המחשב אוניברסיטת בר-אילן

BIU Center for Research in Applied Cryptography and Cyber Security

אוניברסיטת בר-אילן Bar-Ilan University

BACKGROUND AND GENERAL GOALS

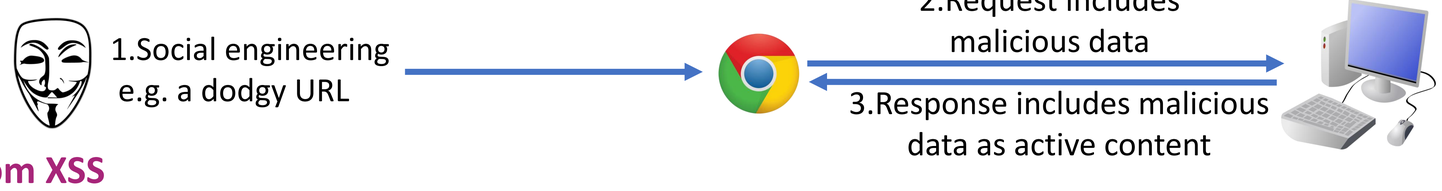
- **Stegosploit** is a browser exploit delivered as images.
- The goal was to make a tool of machine learning to detect a type of steganography called **polyglot.**
- Our project is based on Saumil Shah's article **"Exploit Delivery via Steganography and Polyglots"**

Projects stages

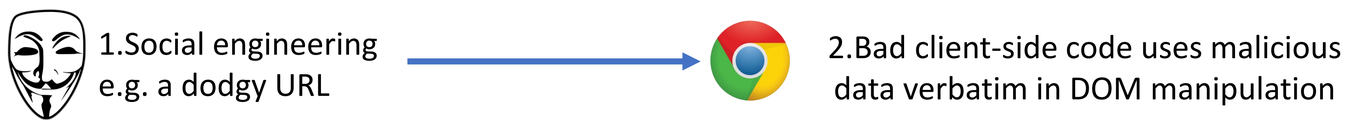
1. Studying and building XSS and CSRF attacks.
2. Creating PNG, JPG and GIF Polyglots based on Shah's article and toolkit.
3. Encoding various malicious JavaScript codes in 20,000 images taken from the CIFAR-10 dataset.
4. Training Decision Trees with various tree depths using multiple encoding methods.

XSS AND CSRF ATTACKS

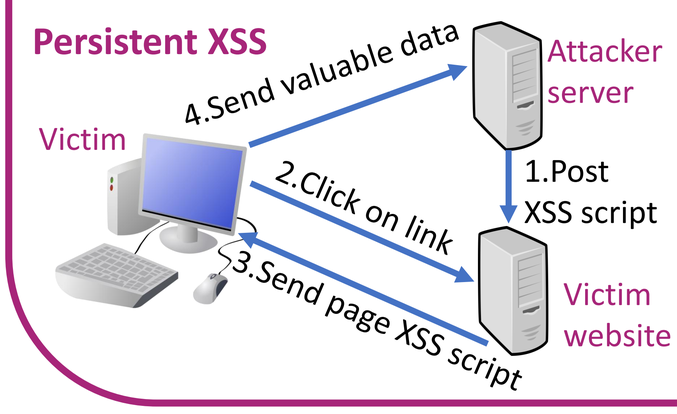
Reflected XSS



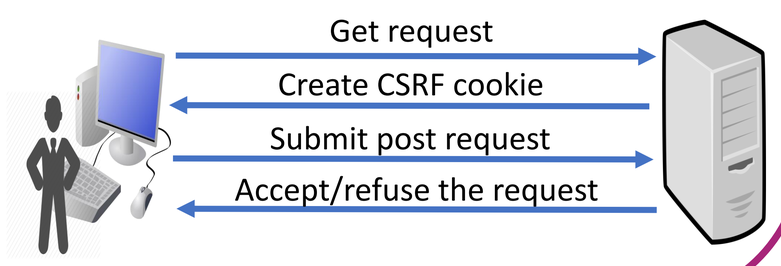
Dom XSS



Persistent XSS



CSRF



CREATING A POLYGLOT

- Encode the browser exploit's bits in a layer of the image to create an **encoded image**.
- Insert a decoder in the **image header** to create **IMAJS,** forming **a Polyglot.**
- Attacking a web server (for example with a XSS attack) with the polyglot as resource

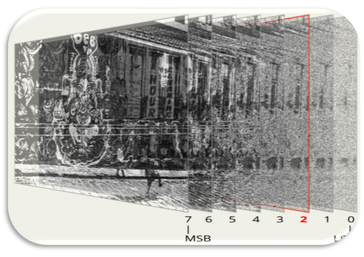
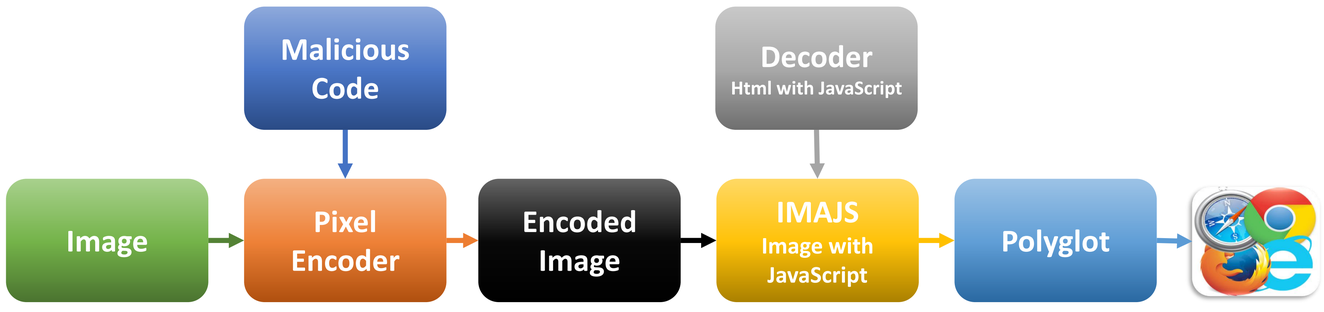
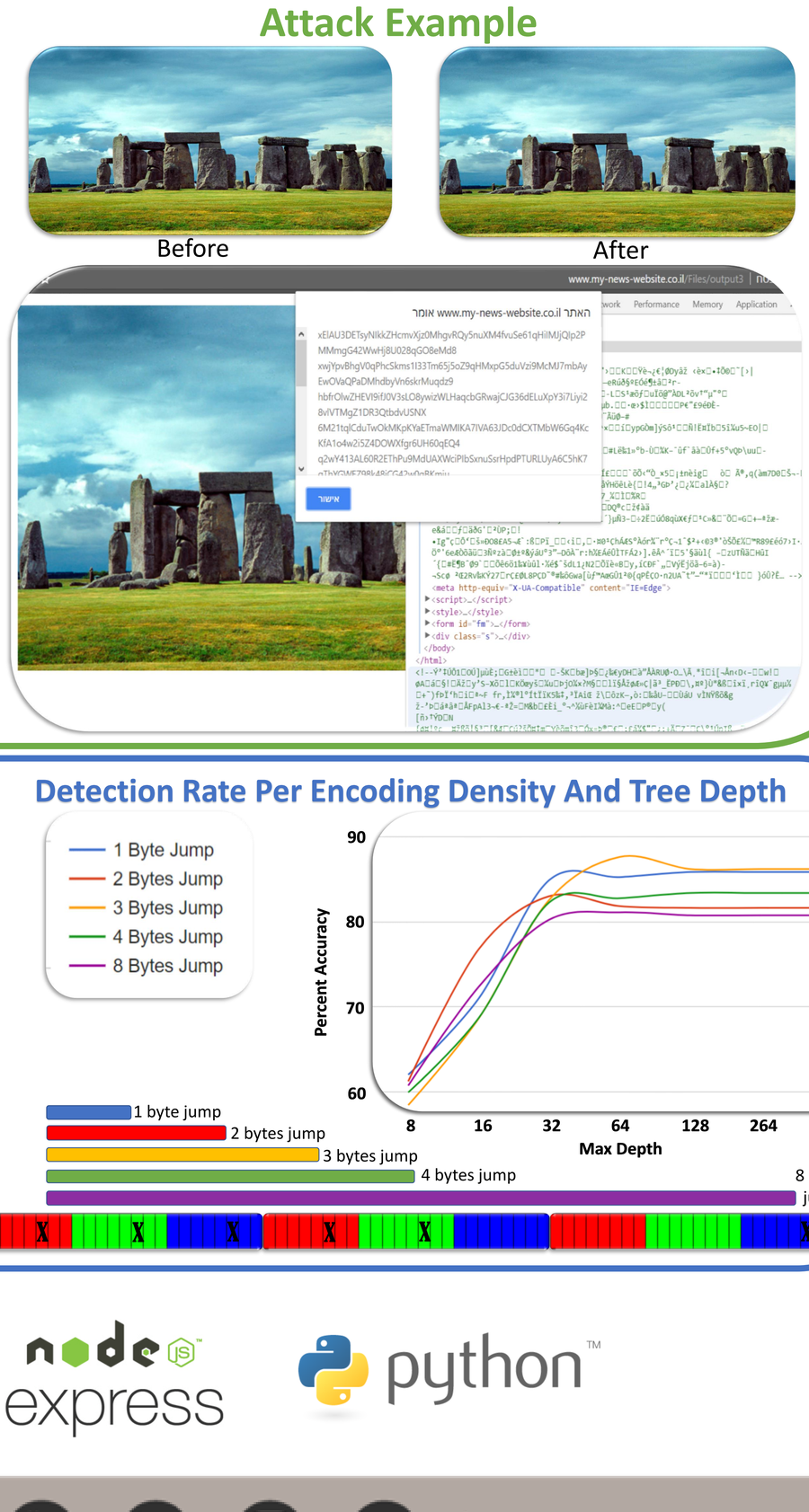


Image layers

The Structure



Attack Example



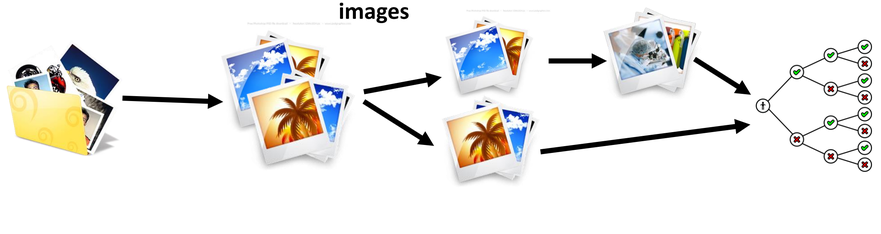
USING MACHINE LEARNING TO DETECT MALICIOUS POLYGLOT IMAGES

The Procedure

Extract 20,000 images from the CIFAR-10 data set

Insert a malicious code into 10,000 of the images

Perform a decision forest with 80:20 train-test ratio



Malicious Code Examples

```
var xhttp = new XMLHttpRequest();
xhttp.open("GET",
"malicious.asp?fname=Marco&lname=polo",
true);
xhttp.send();
```

```
try{document.getElementById("frm")
.submit();
catch(err){alert(""+document.cookie;)}
```

```
var
x=document.getElementById("inform")
.target;
```

```
function Redirect()
{window.location="https://www.youtube.com/
results?search_query=stenography+tutorial";
}
setTimeout('Redirect()', 10000);
```

Detection Rate Per Encoding Density And Tree Depth

git dmlc XGBoost CSS HTML JavaScript node express python