

FINGERPRINTING DE NAVIGATEURS

E. ABGRALL, M. MONPERUSSE, S. GOMBAULT, Y. LE
TRAON, M. HEIDERICH, A. RIBAUT

SSTIC 2013



USAGES DU FINGERPRINTING

IDENTIFICATION DES UTILISATEURS

PROFILING DES UTILISATEURS à DES FINS MERCATIQUES, STATISTIQUES, SMART ADS, MODIFICATION DES PRIX EN FONCTION DU PAYS OU DE LA RÉGION D'ORIGINE, ETC...

- * [PANOPTICCLICK](#)

- * [BROWERSPY.DK](#)

CET ASPECT NE SERA PAS ABORDÉ PENDANT LA PRÉSENTATION

IDENTIFICATION DU NAVIGATEUR

EXPLOIT KITS: LE BON EXPLOIT POUR LE BON NAVIGATEUR

OBJECTIFS POUR L'ATTAQUANT

- * EFFICACITÉ: AUGMENTER LES CHANCES D'INFECTION
- * DISCRÉTION: NE PAS DONNER SES 0-DAYS, NI SES VIRUS AUX HONEYCLIENTS

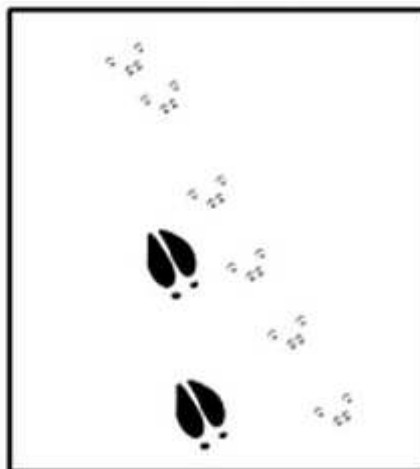
L'ÉTUDE DE CES MÉCANISMES PERMET DE MIEUX LES DÉJOUER ET DE DÉTECTER PLUS EFFICACEMENT LES ATTAQUES.

TECHNIQUES DE FINGERPRINTING

BACKYARD SNOW TRACKING GUIDE



CAT



MOOSE AND SQUIRREL



LONGCAT



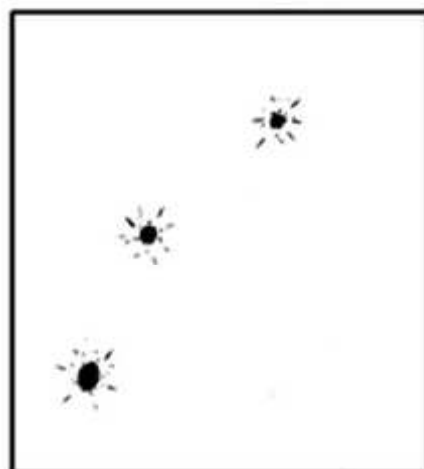
MOUSE RIDING BICYCLE



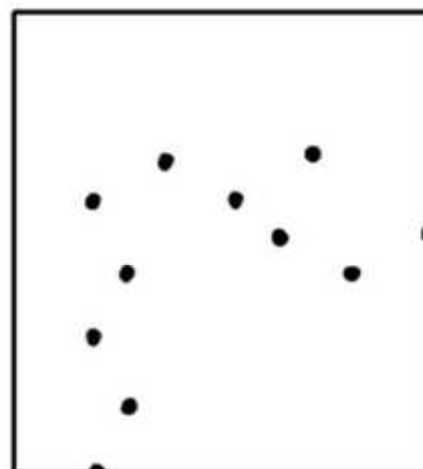
RABBIT STOPPING
TO USE HAIR DRYER



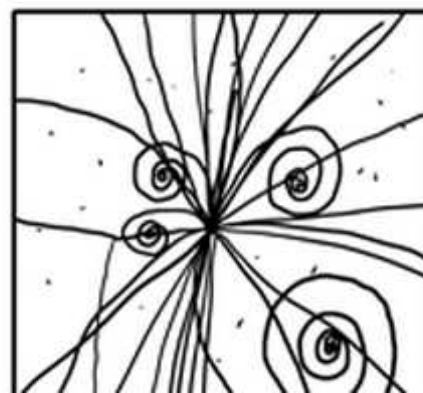
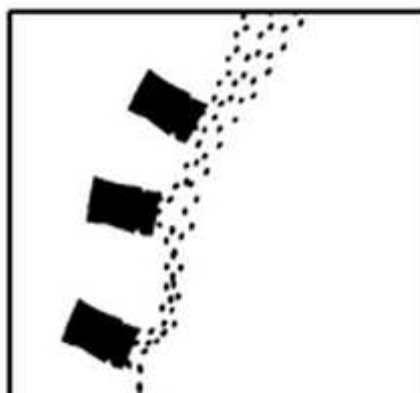
LEGOLAS



BOBCAT ON POGO STICK



KNIGHT



EXEMPLES TIRÉS D'EXPLOIT KITS

UNPACKING DÉPENDANT DU USER-AGENT

```
var pipe=String.fromCharCode(184-navigator.userAgent.length);
```

CONDITION SUR LA TAILLE DU USER-AGENT POUR PERMETTRE LE "DÉCHIFFREMENT" DU CODE JS PAR LA SUITE, CORRESPONDANT à UN ENSEMBLE DE NAVIGATEURS FIREFOX.

[SOURCE](#)

EXEMPLES TIRÉS D'EXPLOIT KITS

IDENTIFICATION D'UN PLUGIN CHROME

```
function fiddlercheck()  
{  
    var xmlParser = new DOMParser();  
    var xmlDom = xmlParser.parseFromString("", "text/xml");  
    var temp=xmlDom.documentElement.nodeName;  
    if(temp=="overlay"){ return "Fiddler";}  
    else{return "";}  
}
```

TECHNIQUE SIMILAIRE EMPLOYÉE POUR LES HANDLERS
D'URI STEAM ET ORIGIN (CF [NSC2013](#))

EXEMPLES TIRÉS D'EXPLOIT KITS

IDENTIFICATION DU USER-AGENT

```
getBrowser: function () {  
  if (this.browserName == null) {  
    var n = navigator.userAgent.toLowerCase();  
    g("[getBrowser()] navigator.userAgent.toLowerCase() -> " + n);  
    if ((n.indexOf("msie") != -1) && (n.indexOf("opera") == -1)) {  
      this.browserName = "MSIE";  
      this.browserName2 = "MSIE"  
    } else {  
      if (n.indexOf("iphone") != -1) {  
        this.browserName = "Netscape Family";  
        this.browserName2 = "iPhone"  
      } else {  
        if ((n.indexOf("firefox") != -1) && (n.indexOf("opera") == -1)) {  
          this.browserName = "Netscape Family";  
          this.browserName2 = "Firefox" [...]
```

EXEMPLES TIRÉS D'EXPLOIT KITS

COMPILATION CONDITIONNELLE SOUS IE

```
alert(f("return /*@cc_on!@*/false"));
```

RENVOIE TRUE SOUS IE.

!FALSE==TRUE

RÉFÉRENCE MSDN

TECHNIQUES ACADÉMIQUES

PERFORMANCE JAVASCRIPT (1)

- * BENCHMARK D'INSTRUCTIONS JS
- * BASÉ SUR LES BENCHMARKS SUNSPIDER ET V8
- * LES TEMPS DE RÉPONSE SERVENT DE SIGNATURE

RENDUS GRAPHIQUES VIA WEBGL(2)

- * MESURE DE LA COULEUR DES PIXELS APRÈS RENDU GRAPHIQUE
- * HASH ISSUE DE L'ENSEMBLE DES PIXELS SERT DE SIGNATURE

TECHNIQUES (MOINS) ACADÉMIQUES

TESTS DE CONFORMITÉ ECMASCRIPT(3)

- * EXÉCUTION DE LA SUITE DE TEST
- * LES TESTS RATÉS SERVENT DE SIGNATURE

DONNÉES NETFLOW(4)

- * MESURE DU RYTHME D'ÉTABLISSEMENT DES CONNEXIONS TCP

STRUCTURE DES EN-TÊTES HTTP(5)

- * MESURE DU RYTHME D'ÉTABLISSEMENT DES CONNEXIONS TCP

YO DAWNG I HEARD U LIKE DYNAMIC WEB PAGES, SO
HERE AT GOOGLE WE PUT A JS ENGINE IN YOUR
BROWSER SO POWERFULL YOU'LL BE ABLE TO RUN
A LINUX KERNEL IN IT WHILE BROWSING THE WEB !



PIMP MY BROWSER

FINGERPRINTING à BASE DE VECTEURS DE XSS

PRINCIPE DE FONCTIONNEMENT

JOUER SUR LES SPÉCIFICITÉ DE COMPORTEMENT DES
MOTEURS HTML.

EXEMPLE:

```
<DIV>Q: HOW DO YOU ANNOY A WEB DEVELOPER?</SPAN>
```

"MOI LE HTML ÇA ME FAIT BALISER" PIERRE C.

PRINCIPE DE FONCTIONNEMENT

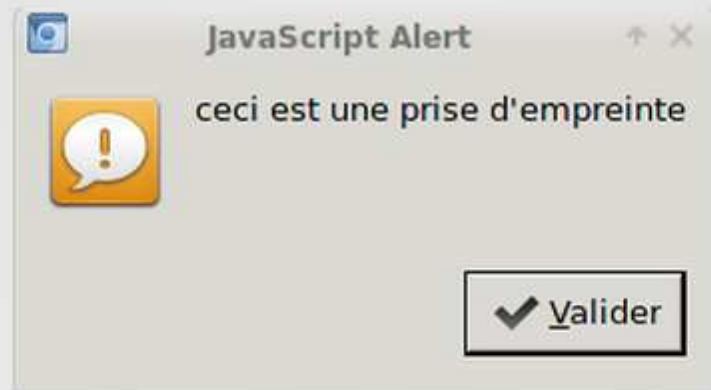
JOUER SUR L'INTERPRÉTATION DE CERTAINS
CARACTÈRES.



POURQUOI DES VECTEURS DE XSS ?

- * SON EXÉCUTION EST DÉTERMINÉE PAR LA CAPACITÉ DU NAVIGATEUR à COMPRENDRE (OU PAS) UNE PORTION DE HTML DONNÉE
- * C'EST TESTABLE DEPUIS UN SERVEUR, ET AUTOMATISABLE
- * J'AI DÉJÀ UN FRAMEWORK QUI PERMET DE LES TESTER
- * PLEIN DE VECTEURS à DISPOSITION DANS LA COMMUNAUTÉ

JEDI MIND TRICK



PRISE D'EMPREINTE

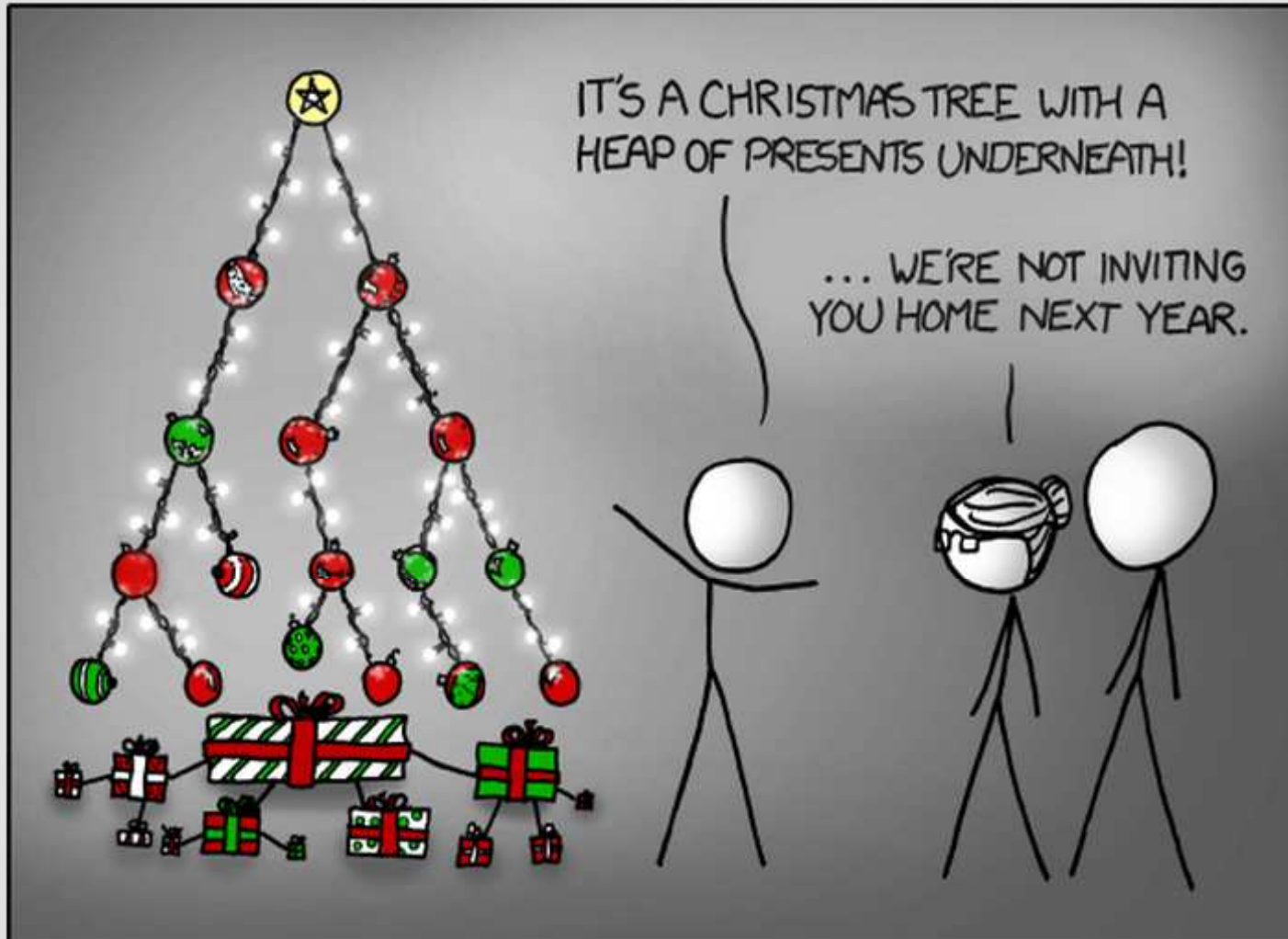
EXÉCUTION DE N VECTEURS DE XSS DANS DIVERS
CONTEXTES INFLUENÇANT LE COMPORTEMENT DU
MOTEUR HTML DU NAVIGATEUR

		'-o-link- source:current">X	X

DéMO... (OU PAS)

IDENTIFICATION DU NAVIGATEUR

PAR ARBRE DE DÉCISION



UN PEU COMME UN "QUI EST-CE" MAIS AVEC DES IFRAMES

IDENTIFICATION DU NAVIGATEUR

PAR ARBRE DE DÉCISION



IDENTIFICATION DU NAVIGATEUR

PAR ARBRE DE DÉCISION

DÉFAUTS

- * PEU FIABLE
- * NOUVELLE VERSION D'UN NAVIGATEUR = ARBRE à REFAIRE
- * FACILE à ANALYSER/CONTOURNER

AVANTAGES:

- * RAPIDE
- * LÉGER

IDENTIFICATION DU NAVIGATEUR

PAR MESURE DE DISTANCES

N RÉSULTATS DE TESTS = SIGNATURE

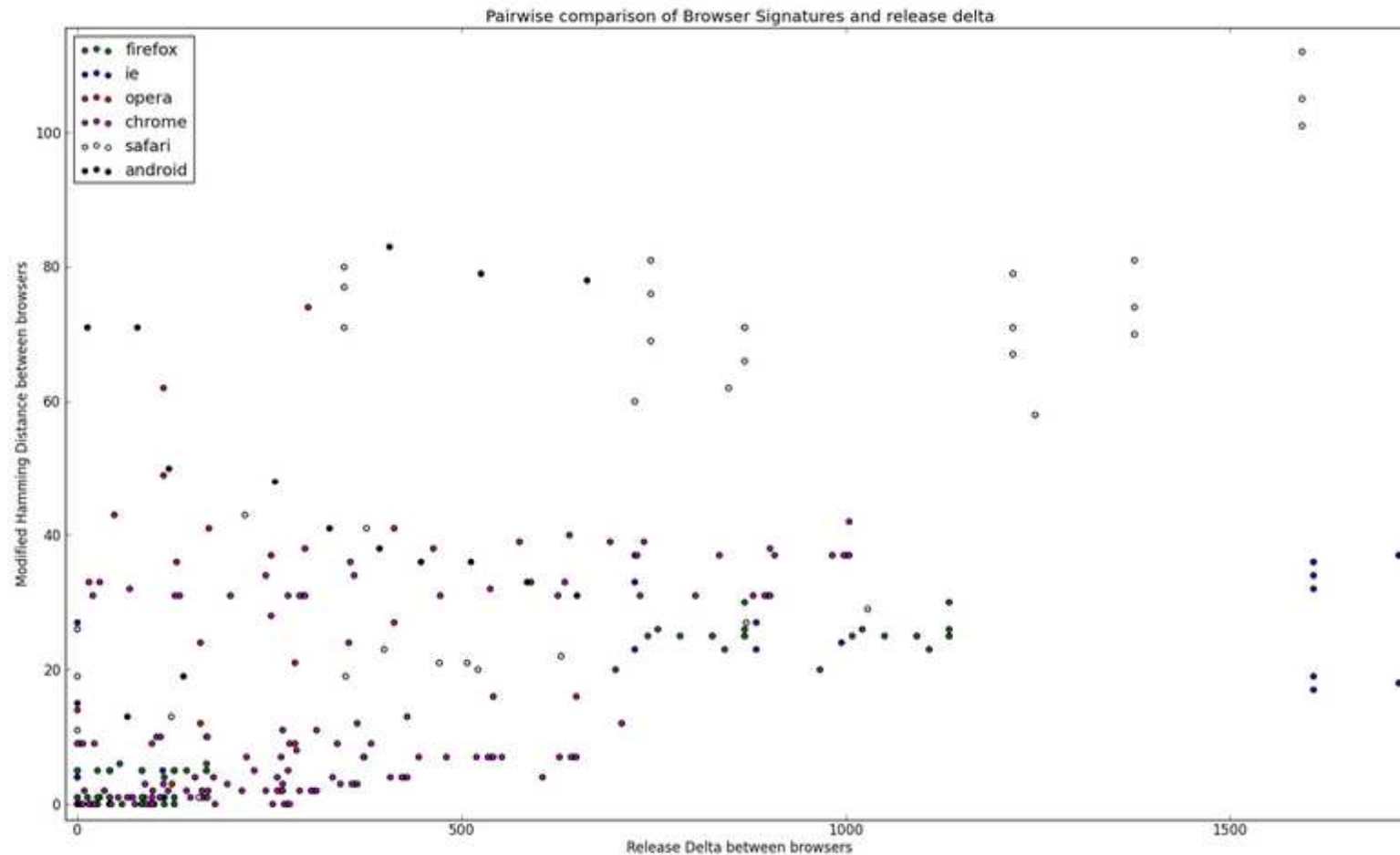
RESTE à DÉTERMINER LE PLUS PROCHE VOISIN PAR SIGNATURE

CHAQUE RÉSULTAT DE TEST EST UNE COMPOSANTE D'UN VECTEUR à N DIMENSIONS

ON UTILISE LA DISTANCE DE HAMMING POUR MESURER LA SIMILARITÉ ENTRE LES DEUX SIGNATURE

ON L'A LÉGÈREMENT MODIFIÉE POUR ESTIMER LA DISTANCE AVEC DES SIGNATURES PARTIELLES

RELATION DISTANCE COMPORTEMENTALE - DISTANCE TEMPORELLE



CREDITS



, GOOGLE HTML5

SLIDES, XKCD, HTML5 SECURITY CHEAT SHEET,
SHAZZER

QUESTIONS ?



ET LES SOURCES?

ELLES SONT SUR

[GITHUB](https://github.com/G4L4DR1M/XSS-TEST-DRIVER) [HTTPS://GITHUB.COM/G4L4DR1M/XSS-TEST-DRIVER](https://github.com/G4L4DR1M/XSS-TEST-DRIVER)

[HTTPS://TRAC.WEBKIT.ORG/WIKI/FINGERPRINTING](https://trac.webkit.org/wiki/Fingerprinting)

[HTTP://CAPEC.MITRE.ORG/DATA/DEFINITIONS/472.HTML](http://capec.mitre.org/data/definitions/472.html)

[HTTP://BROWSERSPY.DK/](http://browserspy.dk/) [HTTP://FINGERPRINT.PET-PORTAL.EU/](http://fingerprint.pet-portal.eu/)

[HTTP://PROGRAMMERS.STACKEXCHANGE.COM/QUESTIONS/122372
BROWSER-FINGERPRINTING-A-VIABLE-TECHNIQUE-FOR-
IDENTIFYING-ANONYMOUS-USERS](http://programmers.stackexchange.com/questions/122372/browser-fingerprinting-a-viable-technique-for-identifying-anonymous-users)

[HTTPS://WIKI.MOZILLA.ORG/FINGERPRINTING](https://wiki.mozilla.org/Fingerprinting)

IDENTIFICATION DU NAVIGATEUR

