Attack-Aware Applications

Introduction

@tolgauedev

Tolga

- Tolga Ünlü, PhD Student @AbertayCyber
- From Germany, Bavaria 🇩🇪
- **Abertay Graduate:**
  - 2012/2013 Computing & Networks (BSc. Hons)
  - 2015/2016 Ethical Hacking & Computer Security (MSc.)
- Web Engineer @OFYZ, Germany
- **Interests:** Application Security and Deception

Attack-Aware Applications

- Applications that are able to detect and respond to **attacks** and **attacker behavior**

- Utilizes **application context** for the detection process

- Enables **real-time insights** into an applications **current security posture**:

  - Is someone currently probing my application?
  - Where are the hotspots of my application?
  - In which state was the application during an attack?

BlackWatch: Increasing Attack Awareness within Web Applications

Calum C. Hall [1], Lynsay A. Shepherd [2,*] and Natalie Coull [2]

[1] MWR InfoSecurity, London SE1 3RS, UK; calumhall96@gmail.com
[2] School of Design and Informatics, Abertay University, Dundee DD1 1HG, UK; n.coull@abertay.ac.uk
* Correspondence: lynsay.shepherd@abertay.ac.uk; Tel.: +44-01382-308685

Application Intrusion Prevention Systems: A New Approach to Protecting Your Data

FMA-RMS
Fabrice A. Marie – 方政信
fabrice.marie@fma-rms.com

HITBSecConf2006 - Malaysia
September 18th - 21st 2006 :: Kuala Lumpur, Malaysia
DEEP KNOWLEDGE SECURITY CONFERENCE

Using internal sensors and embedded detectors for intrusion detection*

Florian Kerschbaum Eugene H. Spafford Diego Zamboni

Center for Education and Research in Information Assurance and Security
1315 Recitation Building
Purdue University
West Lafayette, IN 47907-1315
{kerschf,spaf,zamboni}@cerias.purdue.edu

July 24, 2001

Creating Attack-Aware Software Applications with Real-Time Defenses

Colin Watson, OWASP
Michael Coates, OWASP
John Melton, OWASP
Dennis Groves, OWASP

Application Intrusion Detection Systems: The Next Step

Robert S. Sielken
Graduate Research Assistant
University of Virginia
Department of Computer Science
Charlottesville, VA 22904
(804) 982-2298 (voice)
(804 982-2214 (fax)
rsielken@cs.virginia.edu

Application Intrusion Detection

Drew Miller
Black Hat Consulting

Research Focus

- Concept is not widely adopted or even known

- Can be automated to a certain degree but always has manual parts - Needs to be done by developers on top of other tasks

- Research Aspects:
  - Integration Methods & Automation
  - Utilization of existing Dev Roles/Frameworks/Workflows

Integrating Attack Awareness

- There are two types of integrating attack awareness into an application:

  Developer-Driven
  The detection capability is directly built into the target application by the developers

  Agent-Driven
  The detection capability is provided by a software agent that makes applications attack-aware at runtime

Developer-Driven Integration

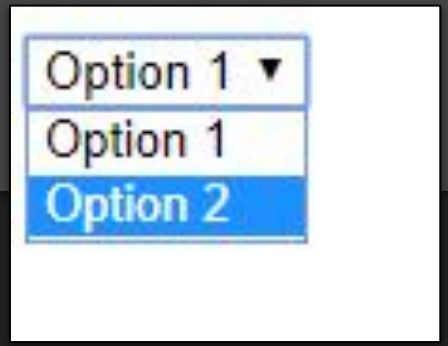
- Developers put **security controls** at strategic locations within the applications

- These security controls check for **distinct signals** of **attacker behavior**

Signals of Attacker Behavior - Examples

- Tampering of data that is not meant to be editable

```
$validOptions = [“Option1”, “Option2”];
$selectedOption = $_POST[“MenuSelection”];

if(in_array($selectedOption, $validOptions)){
   // Selected option is valid, move on
}
else {
   // Request tampering in progress
}
```



Signals of Attacker Behavior - Examples

- Errors/Exceptions that should not occur during normal operation

```
try {
    $pdo = new PDO(...);
    $preparedStatement = $pdo->prepare($dbQuery);
    $preparedStatement->execute($queryValues);
    // Check for errors and throw exception
    // ...
}
catch(SyntaxErrorException $see){ // SQLi in progress }
catch(UnknownColumnException $uce){ // SQLi in progress  }
catch(ColumnNumberMismatchException $cnme){ // SQLi in progress  }
```

```
You have an error in your SQL syntax; check the manual
that corresponds to your MySQL server...
```

Signals of Attacker Behavior - Examples

- Patterns that can only be attributed to an attack or attack tool/malware

```
$fileContent = file_get_contents(...);

if(in_array($fileType, $validFileTypes)){
    // File type is valid, move on
}
elseif(substr($fileContent, 0, 2) === "<?"){
    // PHP script upload attempted

    if(strpos($fileContent, "Safe0ver") !== false){
        // Safe0ver web shell detected
    }
}
```

```
<?php

/* ...
  Safe0ver
  Shell
```

Image.png

Signals of Attacker Behavior - Examples

- Traps/Honey tokens that can not be activated by benign users

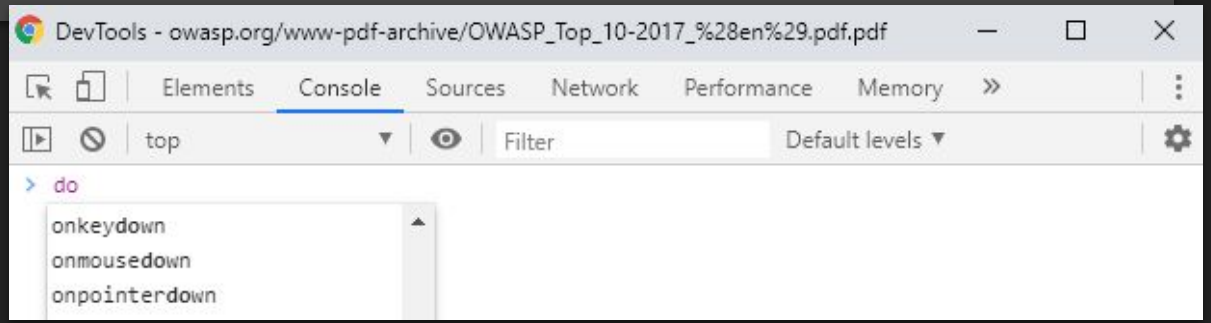
```
$requestHeaders = apache_request_headers();

if($requestHeaders !== false){
    if(!array_key_exists("X-Its-A-Trap", $requestHeaders)){
        // Honey token removed
    }
    elseif($requestHeaders["X-Its-A-Trap"] !== $honeyToken){
        // Honey token modified
    }
}
```

```
HTTP/1.1 200 OK
Connection: close
X-Powered-By: PHP/5.2.4-2
…
X-Its-A-Trap: ChangeMe
```

Signals of Attacker Behavior - Examples

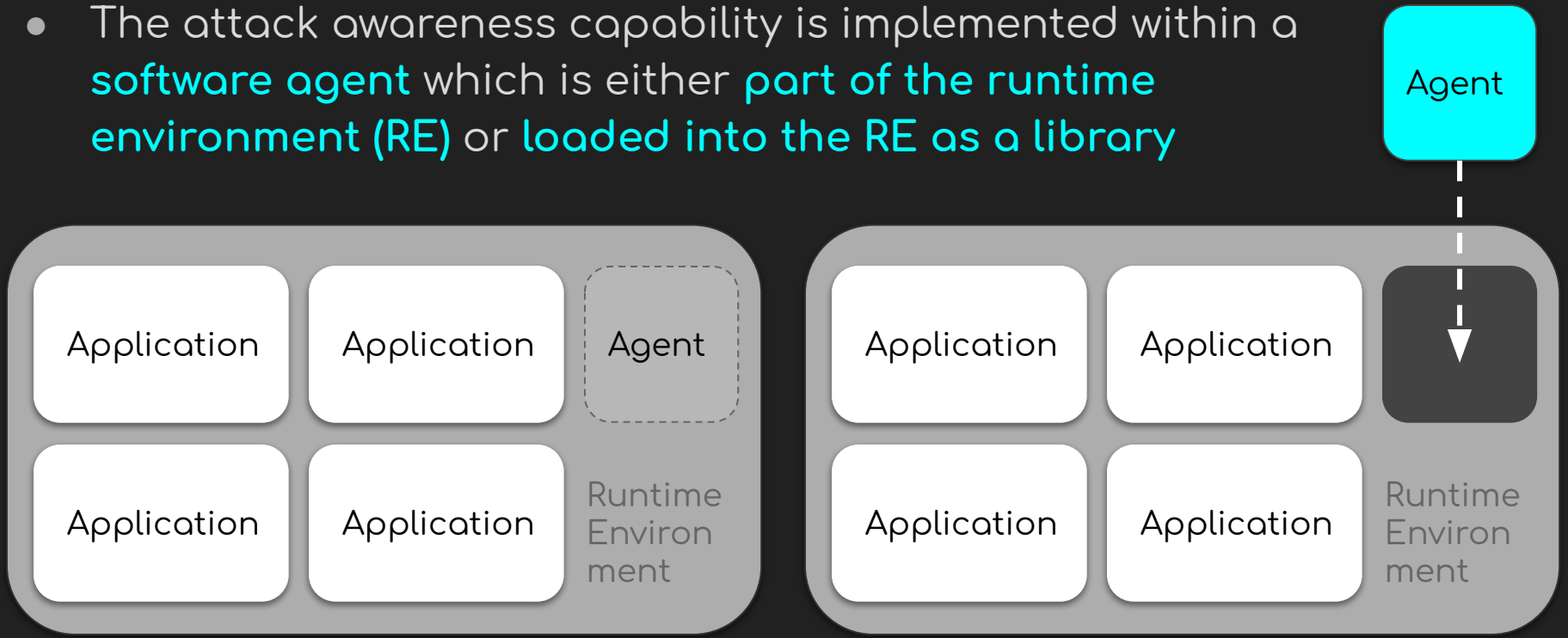
- Use of assets/resources meant for development purposes

```
//# sourceMappingURL=https://yourwebsite.com/getSourceMap.php?ID=2343

$sourceMap = loadSourceMap($_GET["id"]);

header("application/json");
echo $sourceMap;

// Web page is inspected with the developer tools in the Browser
```



Agent-Driven Integration

- The attack awareness capability is implemented within a **software agent** which is either **part of the runtime environment (RE)** or **loaded into the RE as a library**

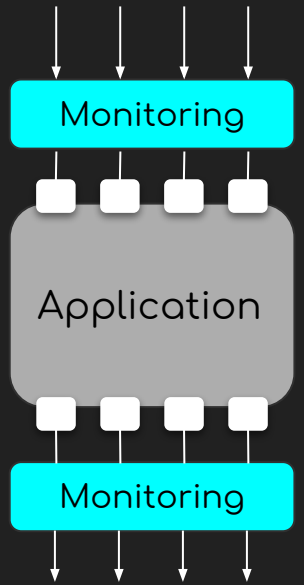


Runtime Application Self-Protection (RASP)

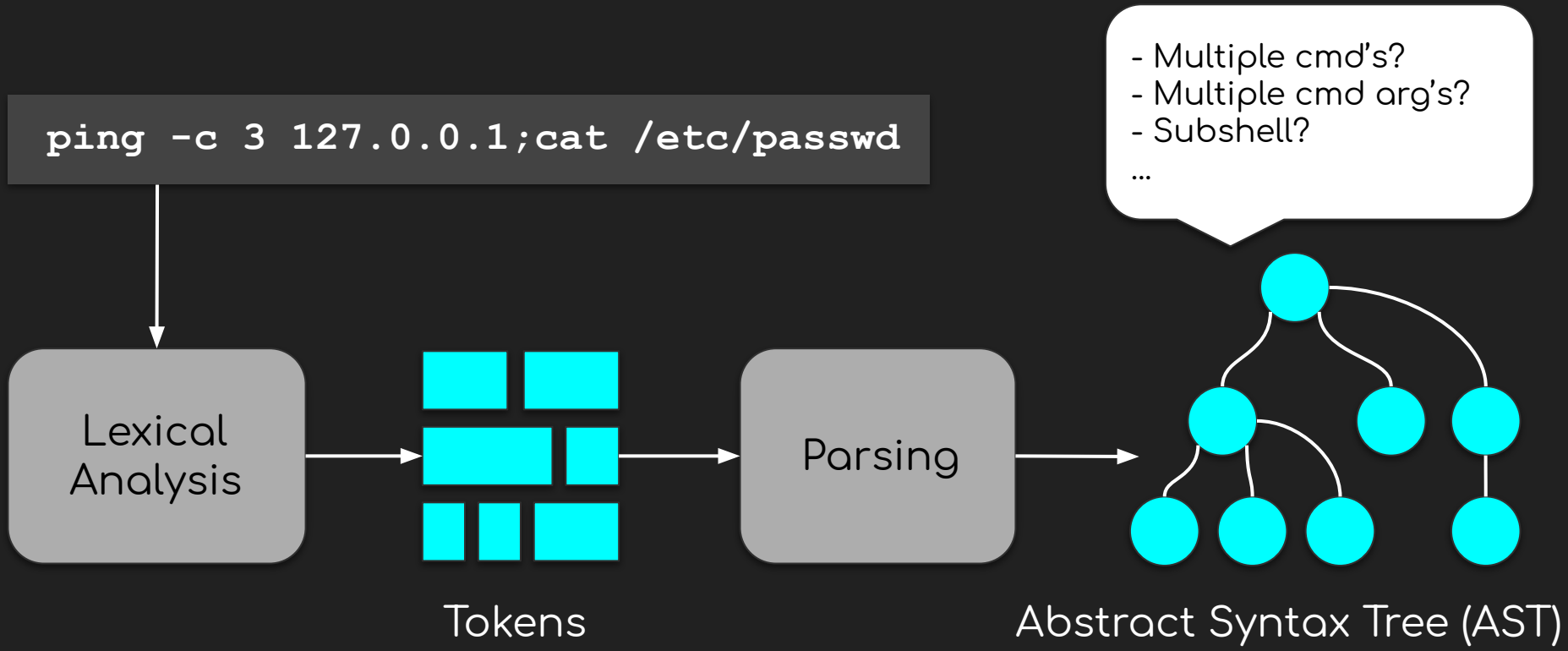
- **RASP** solutions take the agent-driven approach and apply **runtime instrumentation** on common data **sinks** and **sources** of the target platform

- Detection techniques applied on the instrumented sinks/sources are:

  - Signature/Pattern Matching
  - Error/Exception Monitoring
  - Language-Theoretic Security (LangSec)



Security Analysis with Language Theory



Demo Application

```
/ping/127.0.0.1
```

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0
ttl=64 time=0.047 ms
...
```

Web Service
(main.js:9000)

Conclusions & Future Work

- Applications can be made attack-aware using different methods
- It is subject to further research whether there are other methods and whether the implementation effort of those and the existing methods can be reduced or automated
- Part of the research is also to investigate methods that can utilize existing development practices, roles and fit into a modern development environment

Thank you!

References

- Slide 4:
  - BlackWatch: Increasing Attack Awareness Within Web Applications - https://arxiv.org/pdf/1901.04243.pdf
  - Creating Attack-Aware Software Applications with Real-Time Defenses - https://pdfs.semanticscholar.org/0236/5631792fa6c953e82cadb0e7268be35df905.pdf
  - Using internal sensors and embedded detectors for intrusion detection - http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.5323&rep=rep1&type=pdf
  - Application Intrusion Detection Systems: The Next Step - https://pdfs.semanticscholar.org/fbe5/52fdab7323a216c3e152bce2db3707acd1a6.pdf
  - Application Intrusion Detection - https://www.blackhat.com/presentations/bh-federal-03/bh-fed-03-miller.pdf
  - Application Intrusion Prevention Systems: A New Approach to Protecting Your Data - https://conference.hitb.org/hitbsecconf2006kl/materials/DAY%201%20-%20Fabrice%20Marie%20-%20AIPS.pdf

References

- Slide 5:
  - OWASP Top 10 - https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf
  - What happened to Attack Aware Applications ? - https://youtu.be/HQxs3xn7tLA
- Slide 12:
  - Abusing SourceMappingURL - https://medium.com/@weizmangal/javascript-anti-debugging-some-next-level-sh-t-part-1-abusing-sourcemappingurl-da91ff948e66
- Slide 14:
  - Baidu's OpenRASP solution describes the use of signature/pattern matching and exception monitoring in the documentation (needs translation) - https://rasp.baidu.com/doc/usage/web.html
  - NodeRASP by SAP combines lexical analysis with taint tracking to detect SQLi attacks - https://github.com/SAP/node-rasp/wiki/Taint-Analysis-for-PostreSQL

Resources

Conference Talks:

- Creating Self Defending Applications to Repel Attackers - https://youtu.be/YOtTPr8r0tI
- AppSensor: Real-Time Event Detection and Response - https://youtu.be/1imlD1O4HrY
- What happened to Attack Aware Applications? - https://youtu.be/HQxs3xn7tLA
- Attack Aware Applications - https://youtu.be/u4AVrj-6drc
- Application Intrusion Detection - https://youtu.be/H6YGG_i8Z3I
- Sinking Your Hooks in Applications - https://youtu.be/syymoKlNp3w
- Monkey Patching CSRF Away - https://youtu.be/lquCROhi9k0
- Using language-theoretics and runtime visibility to align AppSec with DevOps - https://youtu.be/SVssGylyVkc
- Prevent Business Logic Attacks using Dynamic Instrumentation - https://youtu.be/Bttl22BJQ1Y
- Interactive Application Security Testing (IAST), Beyond SAST/DAST - https://youtu.be/sUNsPBb6NPA

Resources

- Using Aspect Oriented Programming to Prevent Application Attacks
  - Part 1 https://youtu.be/c-492qXrT6w
  - Part 2 https://youtu.be/jOqQpbk--jQ
  - Part 3 https://youtu.be/tMHr34Empvo
  - Part 4 https://youtu.be/A63g4xSvb1Y
  - Part 5 https://youtu.be/-0U5LzLkPkY
  - Part 6 https://youtu.be/PygweFC5VKM
- Injecting Security Controls in Software Applications - https://youtu.be/kByRUyiqVyA
- Jumpstarting Your DevSecOps Pipeline with IAST and RASP - https://youtu.be/9QJZkPISB58
- Injecting Security into Web Apps at Runtime - https://youtu.be/GBNiZDgmkyU
- Repsheet: A Behavior Based Approach to Web Application Security - https://youtu.be/KMxJf_JEP40
- 20K Lines under the C: A Guide to the PHP Startup Process and Hooking Absolutely Everything - https://youtu.be/iXoG_ccTHmk
- Building Self-Defending Applications with OWASP AppSensor - https://youtu.be/zTRN120Uu28?t=5593

Resources

Conference Slides:

- Application Intrusion Detection - https://www.blackhat.com/presentations/bh-federal-03/bh-fed-03-miller.pdf
- Application Intrusion Prevention Systems: A New Approach to Protecting Your Data - https://conference.hitb.org/hitbsecconf2006kl/materials/DAY%201%20-%20Fabrice%20Marie%20-%20AIPS.pdf

Resources

Blog Articles:

- Sqreen - How to build a dynamic instrumentation agent
  - Java https://blog.sqreen.com/building-a-dynamic-instrumentation-agent-for-java/
  - Python https://blog.sqreen.com/dynamic-instrumentation-agent-for-python/
  - Ruby https://blog.sqreen.com/dynamic-instrumentation-agent-for-ruby/
  - PHP https://blog.sqreen.com/dynamic-instrumentation-agent-php/
  - Node.js https://blog.sqreen.com/building-a-dynamic-instrumentation-agent-for-node-js/
- Playing with the acusensor - https://dustri.org/b/playing-with-the-acusensor.html
- Behind enemy lines: bug hunting with Burp Infiltrator - https://portswigger.net/blog/behind-enemy-lines-bug-hunting-with-burp-infiltrator

Resources

Projects and Tools:

- Node RASP - https://github.com/SAP/node-rasp
- OpenRASP - https://github.com/baidu/openrasp
- OWASP AppSensor - http://appsensor.org/
- Immunizer - https://github.com/oiraqi/immunizer
- Hdiv - https://github.com/hdiv/hdiv
- Ensnare - https://github.com/ahoernecke/ensnare
- Repsheet - https://github.com/repsheet
- ZenIDS - https://github.com/uci-plrg/zen-ids
- Sqreen - https://github.com/Sqreen

Resources

Academic Papers:

- BlackWatch: Increasing Attack Awareness Within Web Applications - https://arxiv.org/pdf/1901.04243.pdf
- Application-Level Unsupervised Outlier-Based Intrusion Detection and Prevention - https://www.hindawi.com/journals/scn/2019/8368473/
- SecuriFly: Runtime Protection and Recovery from Web Application Vulnerabilities - https://pdfs.semanticscholar.org/9383/b08dc5bc6ecbc48e10d5ea181e34eb60faea.pdf
- Lightweight Self-Protecting JavaScript - http://www.cse.chalmers.se/~dave/papers/ASIACCS09.pdf
- Application Intrusion Detection Systems: The Next Step - https://pdfs.semanticscholar.org/fbe5/52fdab7323a216c3e152bce2db3707acd1a6.pdf
- Creating Attack-Aware Software Applications with Real-Time Defenses - https://pdfs.semanticscholar.org/0236/5631792fa6c953e82cadb0e7268be35df905.pdf
- Using internal sensors and embedded detectors for intrusion detection - http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.5323&rep=rep1&type=pdf