



# Client-Side Cross-Domain Requests in the Web Browser: Techniques, Policies and Security Pitfalls

Sebastian Lekies – Walter Tighzert  
SAP Research - Security and Trust

[sebastian.lekies@sap.com](mailto:sebastian.lekies@sap.com)

[walter.tighzert@sap.com](mailto:walter.tighzert@sap.com)

**OWASP**

17.11.2011

Copyright © The OWASP Foundation  
Permission is granted to copy, distribute and/or modify this document  
under the terms of the OWASP License.

**The OWASP Foundation**

<http://www.owasp.org>

# Agenda

---

## 1. Technical Backgrounds

- Client-Side Cross-Domain HTTP Requests
- Security Implications

## 2. The State of the Cross-Domain Nation

- Methodology
- Results

## 3. Deploying a Policy File correctly

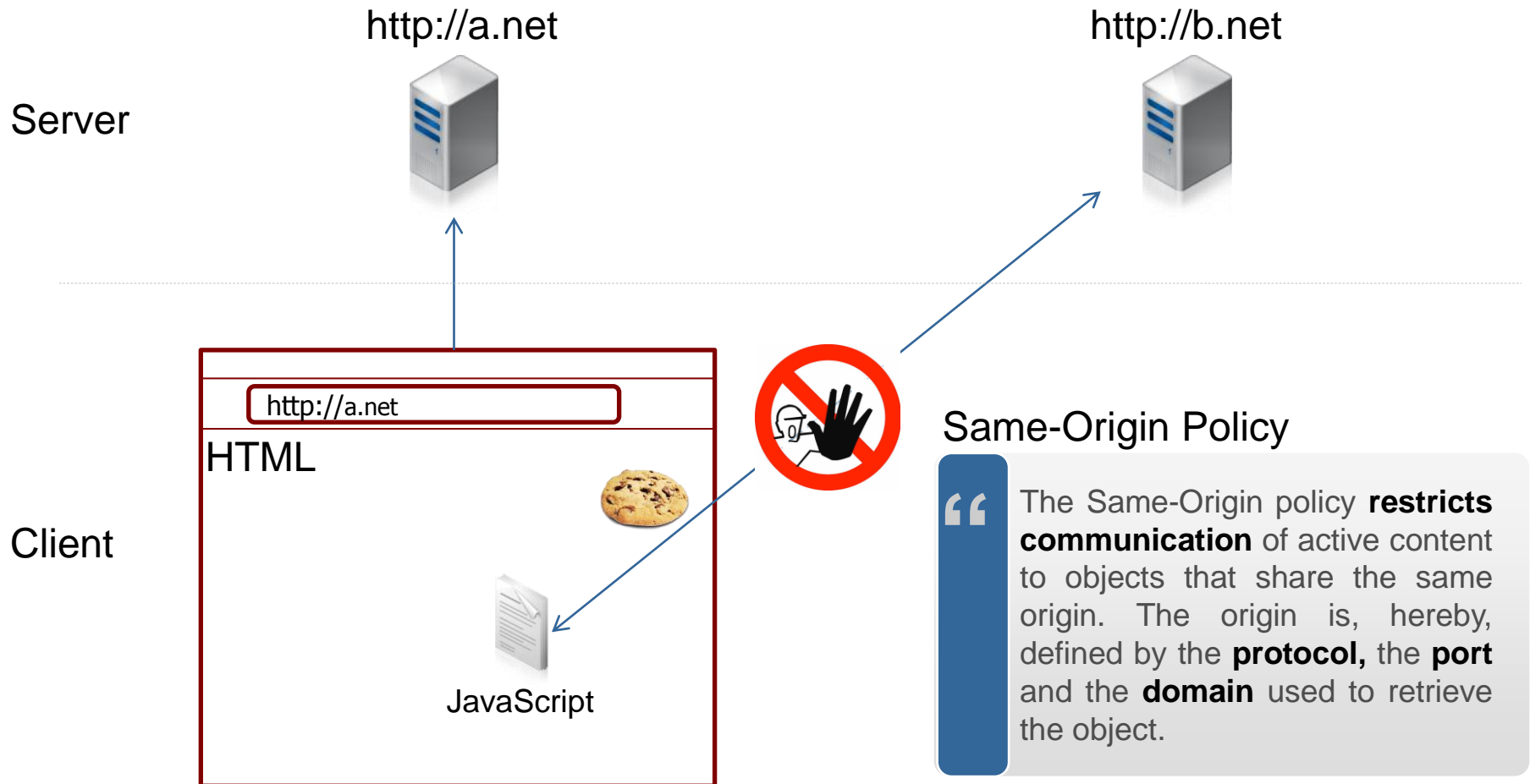
## 4. DeMaCro: Defense against Malicious Cross-Domain Requests

- Methodology
- Evaluation

## 5. Conclusion

# Technical Backgrounds

## Client-Side Cross-Domain HTTP Requests



# Technical Backgrounds

## Security Implications

http://kittypics.org



http://webmail.com



Server

Leakage of sensitive information



Circumvention of CSRF protection



# Session Hijacking Vulnerability

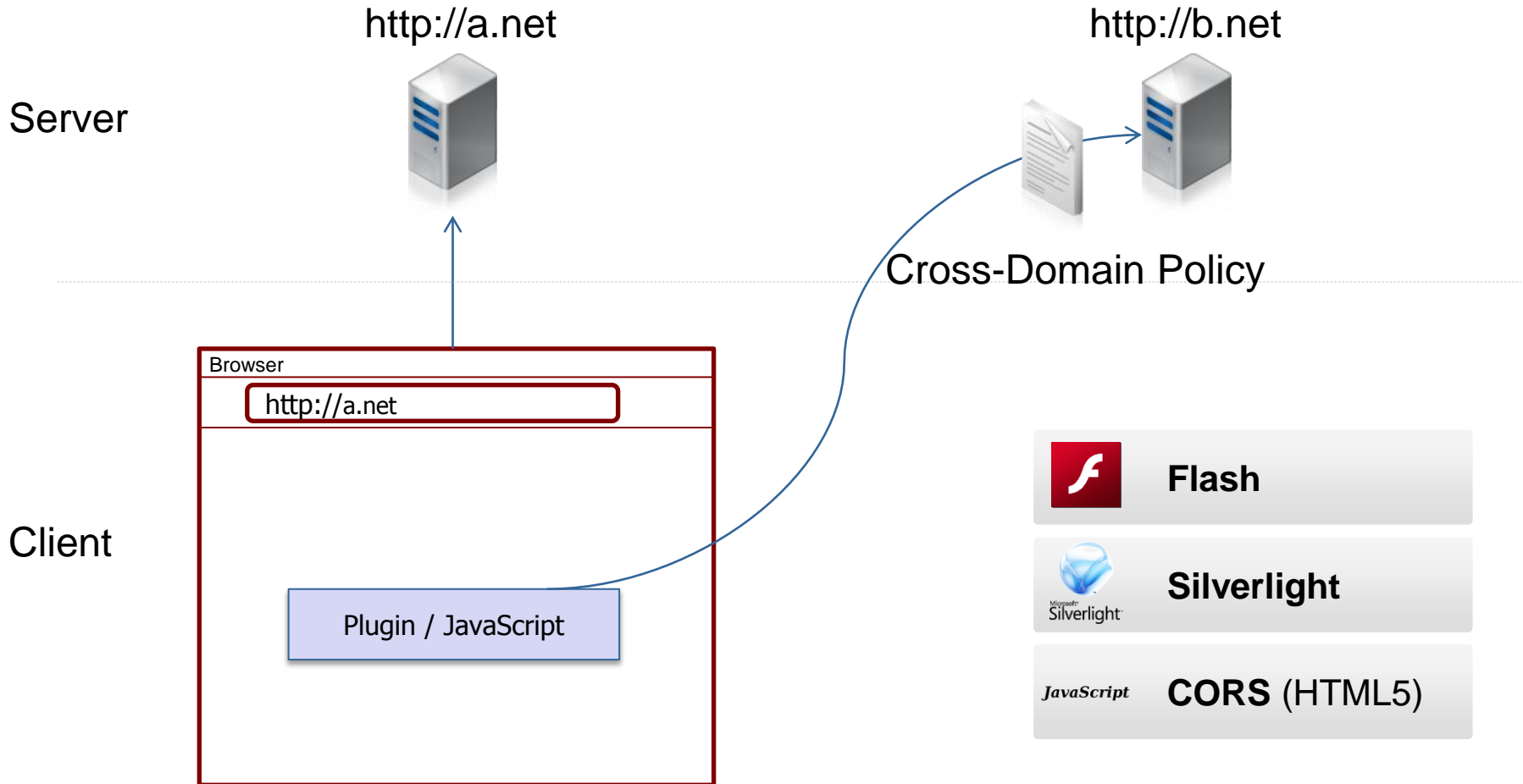




JavaScript



# Technical Backgrounds

## Secure Client-Side Cross-Domain Requests



-  **Flash**
-  **Silverlight**
- JavaScript* **CORS (HTML5)**

# Technical Backgrounds

## Insecure Conditions

---

```
<cross-domain-policy>  
  <allow-access-from domain="a.net" />  
</cross-domain-policy>
```

```
<cross-domain-policy>  
  <allow-access-from domain="*" />  
</cross-domain-policy>
```

## Wildcard policies

- "\*"
  - Whitelists all existing domains
  - Giving up the protection capabilities implied by the Same-Origin Policy

## Further Insecurities

- Transitivity of vulnerabilities
- Vulnerabilities in client-side cross-domain Flash proxies

# The State of the Cross-Domain Nation

Methodology



# The State of the Cross-Domain Nation

## Methodology

---

Shallow crawl of the top 1,000,000 sites in the Alexa index

Collect Flash, Silverlight and CORS Policies

### **(R1) Penetration**

How prevalent are cross-domain policies?

Which technologies are used for this purpose?

What kind of sites issue cross-domain policies?

### **(R2) Security**

How high is the ratio of potentially insecure policies?

What is the relationship between (in)security and site category?

Is there a correlation between (in)security and site popularity?



# The State of the Cross-Domain Nation

## Identifying insecure Policies

---

### **Observation: a wildcard alone does not cause insecurities**

A necessary condition is that the permissive site indeed conducts authentication tracking

### **Approach:**

- Check for evidence indicating that an authentication state can be provided by the site
  - Login forms (password fields)
  - Session identifiers (HTTP-only cookies, naming conventions)
- If authentication forms pointed to different (sub)domains, we also checked the policy file for the form's target domain

# The State of the Cross-Domain Nation

Results

# The State of the Cross-Domain Nation

## Results - Penetration

---

**1,093,127 domains scanned**

	Total	Percentage
Flash	82,052	8%
Silverlight	995	0.09%
Cors	215	0.02%

# The State of the Cross-Domain Nation

## Results – Penetration: Comparison to 2008

---

### Grossman study in 2008

- Alexa Top 500 and Fortune 500
  - 28% providing a crossdomain.xml policy
  - 7% with a wildcard policy

### Our results (2011)

- Alexa Top 1000
  - 48% providing a crossdomain.xml policy
  - 12% with a wildcard policy

→ Indicator that the adoption of the technology is increasing

# Results

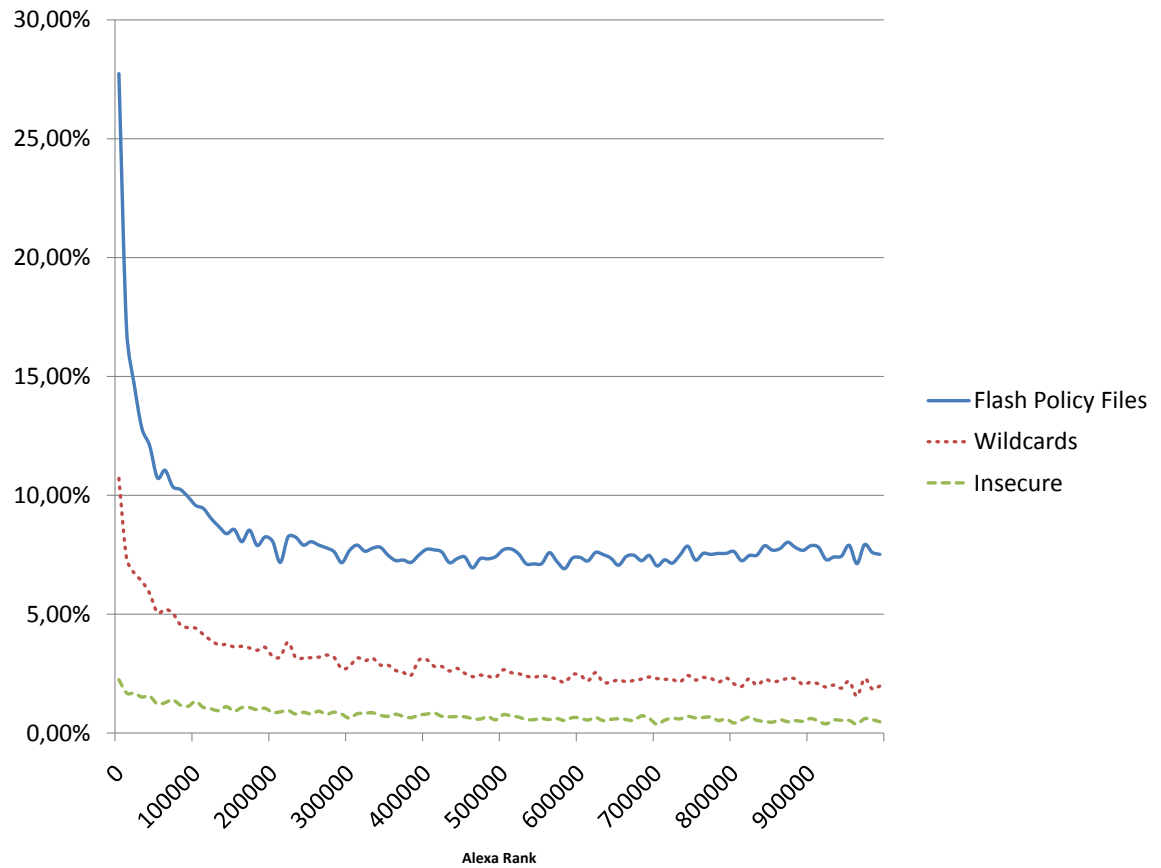
## Penetration / Security - Flash

### Wildcard policy

31,011 files (37.7% of all crossdomain.xml) resulting in 2,8% potentially insecure sites

### When checking for authentication

15,060 sites (1.3% of all analyzed sites)

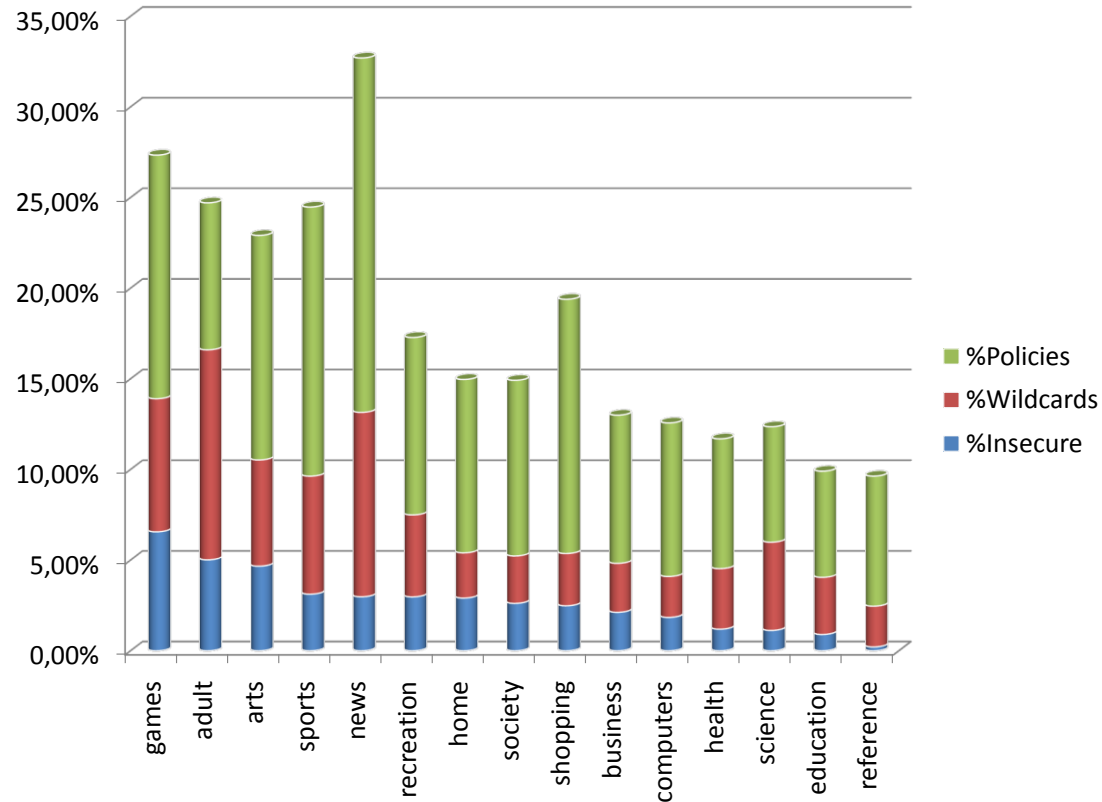


Collected crossdomain.xml files

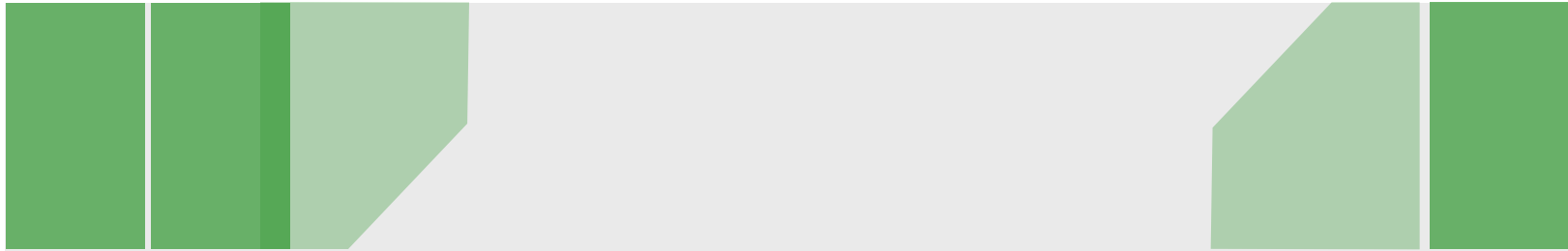
# Results

## Penetration / Security - Flash

Mapping policy files to the top categories



# Deploying a Policy File correctly



# Deploying a Policy File correctly

---

## Goal

- Share **public** data via cross-domain requests
- Protect **private** data from being stolen

## Important Guideline

- Never combine cross-domain access with private data



# Deploying a Policy File correctly

Using distinct Domains

---

static.example.org/crossdomain.xml

```
<cross-domain-policy>  
  <allow-access-from domain="*" />  
</cross-domain-policy>
```

private.example.org/crossdomain.xml

```
<cross-domain-policy>  
  <site-control permitted-cross-domain-policies="none" />  
</cross-domain-policy>
```

# Deploying a Policy File correctly

## Using Subfolders

---

Flash and Silverlight have the option of defining policies for specific subfolders

```
<access-policy>
  <cross-domain-access>
    <policy>
      <allow-from>
        <domain uri="*" />
      </allow-from>
      <grant-to>
        <resource path="/static/" include-subpaths="true" />
      </grant-to>
    </policy>
  </cross-domain-access>
</access-policy>
```

# Defense against malicious Cross-Domain Requests

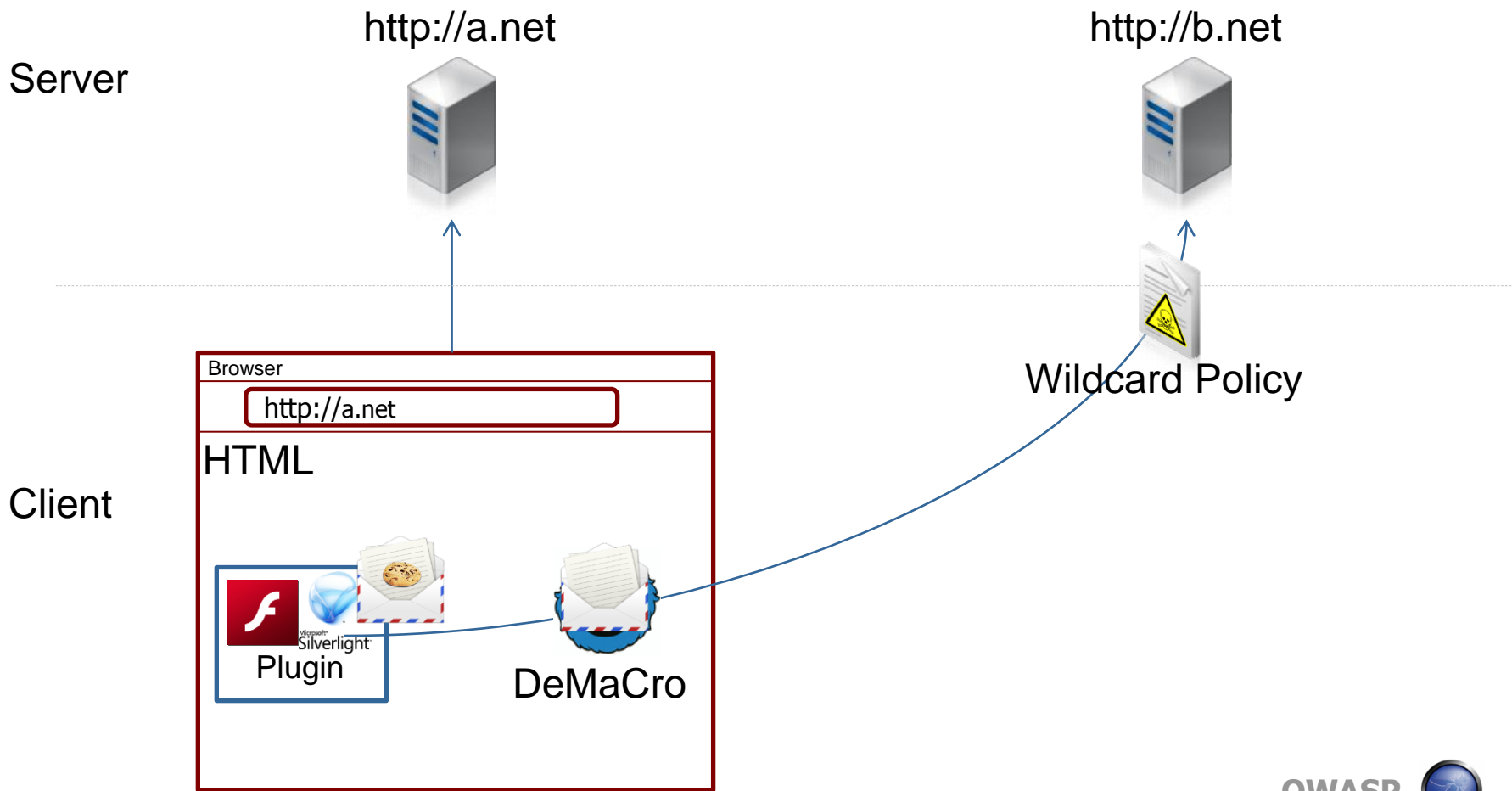
Methodology

A decorative graphic on the left side of the slide. It consists of a vertical stack of colored bars: a medium blue bar at the top, a dark blue bar, a light blue bar, a white bar, a medium green bar, a dark green bar, and a black bar at the bottom. To the right of these bars, there are several geometric shapes in various shades of green. One shape is a trapezoid with a diagonal cut on its right side. Another is a trapezoid with a diagonal cut on its left side. There are also some rectangular blocks and thin vertical lines.

# DeMaCro

## Methodology

### DeMaCro: Defense against Malicious Cross-Domain Requests



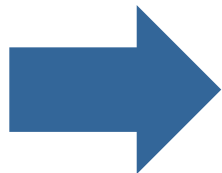
# DeMaCro

## Evaluation

---

### Security Evaluation

- DeMaCro was evaluated against malaRIA<sup>1</sup>, a real-world exploitation tool
- Additionally it was tested against three real-world use cases (domains from the Alexa Top 500)
- Additional generic test cases



DeMaCro prevented any attack that was possible without the extension

<sup>1</sup><http://erlend.oftedal.no/blog/?blogid=107>

# DeMaCro

## Evaluation

---

### Performance Evaluation

- Overhead of about 0,82 ms in the best case (no plugin-based cross-domain requests at all)
- Overhead of about 17 ms in the worst case (only plugin-based cross-domain requests on a page)



Flash-based image gallery  
<http://www.flash-gallery.org>

# DeMaCro

## Evaluation

---

### Functional Evaluation

Crawling the Alexa Top 500 websites with DeMaCro

	Total Numbers	Percentage
Total requests	33,260	100%
Cross-domain	366	1.1%
Wildcard requests	176	0.5%

Cookies were stripped from wildcard requests

Do we break any **legitimate** functionality by doing so?

# DeMaCro

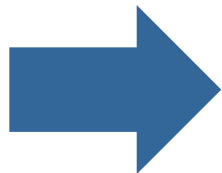
## Evaluation

---

Do we break any **legitimate** functionality by doing so?

Manual checks of the 42 webpages that were involved in creating these requests

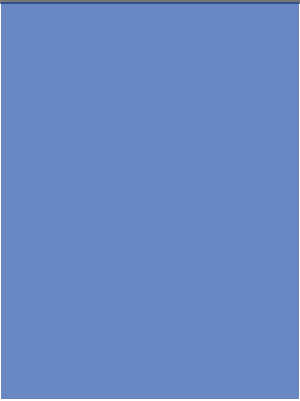
60% of the cross-domain requests are ad related, the others are used in flash-based video players or image galleries



No indication found that DeMaCro breaks legitimate functionality, but ad tracking may be affected



# Conclusion



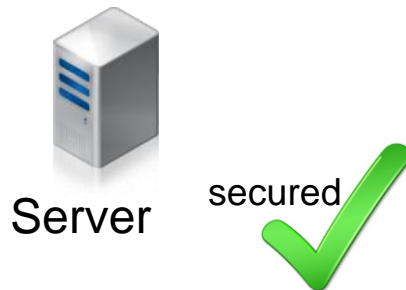
# Conclusion

---

## Key facts

- 15,060 insecure sites
- Legitimate to use wildcard policies

### State of the Cross-Domain Nation



### DeMaCro




# Conclusion

Never again... =)

---

The classical \* + x



```
<?xml version="1.0" ?>
- <cross-domain-policy>
  <allow-access-from domain="*" />
  <allow-access-from domain="*. [redacted].com" />
  <allow-access-from domain="*. [redacted].ru" />
  <allow-access-from domain="78.140.145.148" />
  <allow-access-from domain="78.140.145.151" />
```

with more than 950 entries!

# Conclusion

Never again... =)

The "I tell you what my network looks like"

http://www.██████████.crossdomain.xml

```
<?xml version="1.0" ?>
<!-- http://www.adobe.com/crossdomain.xml -->
<!-- Wildcards are not allowed in IP domain specifications. -->
- <cross-domain-policy>
  <allow-access-from domain="*██████████.de" />
  <allow-access-from domain="angebote.t-online.de" />
  <allow-access-from domain="*██████████.com" />
  <allow-access-from domain="localhost" />
  <!-- Test-Server -->
  <allow-access-from domain="kda-office.dyndns.org" />
  <allow-access-from domain="192.168.160.144" />
  <allow-access-from domain="192.168.160.145" />
  <allow-access-from domain="192.168.160.146" />
  <!-- office dev ips -->
  <allow-access-from domain="192.168.160.5" />
  <allow-access-from domain="192.168.160.6" />
  <allow-access-from domain="192.168.160.10" />
  <allow-access-from domain="192.168.160.11" />
  <allow-access-from domain="192.168.160.12" />
  <allow-access-from domain="192.168.160.18" />
  <allow-access-from domain="192.168.160.13" />
  <allow-access-from domain="192.168.160.15" />
```

```
<allow-access-from domain="192.168.160.27" />
<allow-access-from domain="192.168.160.28" />
<allow-access-from domain="192.168.160.29" />
<allow-access-from domain="192.168.160.30" />
<allow-access-from domain="192.168.160.31" />
<allow-access-from domain="192.168.160.32" />
<allow-access-from domain="192.168.160.33" />
<allow-access-from domain="192.168.160.34" />
<allow-access-from domain="192.168.160.35" />
<allow-access-from domain="192.168.160.36" />
<allow-access-from domain="192.168.160.37" />
<allow-access-from domain="192.168.160.38" />
<allow-access-from domain="192.168.160.39" />
<allow-access-from domain="192.168.160.42" />
<allow-access-from domain="192.168.160.66" />
<allow-access-from domain="192.168.160.70" />
<allow-access-from domain="192.168.160.73" />
<!-- Thomas dev (home) -->
<allow-access-from domain="192.168.161.63" />
<!-- Flash Dev -->
<allow-access-from domain="*.media-artwork.com" />
</cross-domain-policy>
```



# Literature

---

S. Lekies & M.Johns & W. Tighzert: "***The State of the Cross-Domain Nation***", In Proceedings of the 5th Workshop on Web 2.0 Security and Privacy (W2SP), 2011.

S. Lekies & N.Nikiforakis & F. Piessens & W. Tighzert & M.Johns: "***DeMaCro: Defense against malicious Cross-Domain Requests***", (under submission).

M.Johns & S. Lekies: "***Biting the hand that serves you: A closer look at client-side Flash proxies for cross-domain requests***", in the proceedings of the 8th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2011)



**Thank you!**

Contact information:

**OWASP**

[sebastian.lekies@sap.com](mailto:sebastian.lekies@sap.com)

[walter.tighzert@sap.com](mailto:walter.tighzert@sap.com)

Copyright © The OWASP Foundation  
Permission is granted to copy, distribute and/or modify this document  
under the terms of the OWASP License.

**The OWASP Foundation**

<http://www.owasp.org>