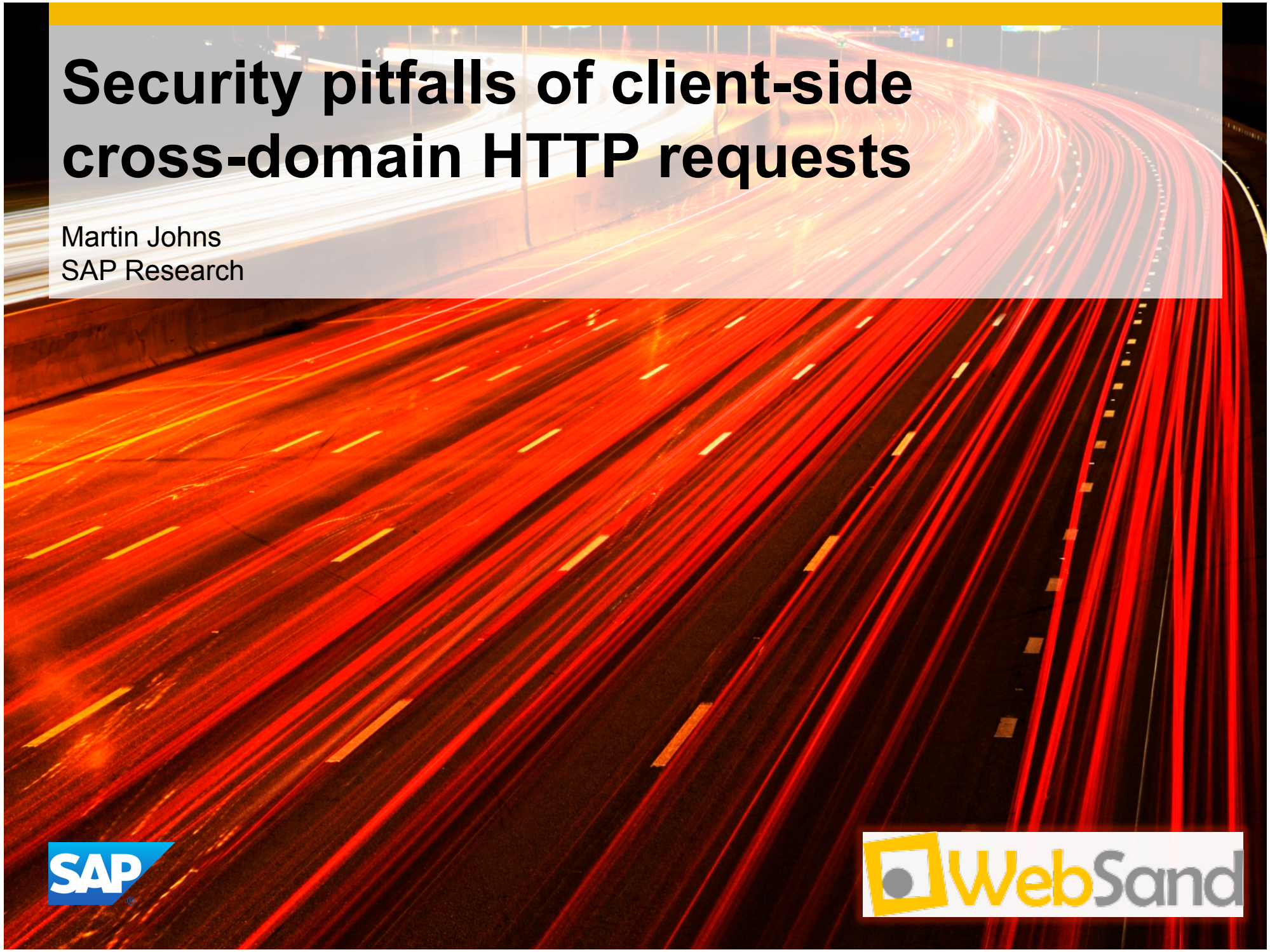


Security pitfalls of client-side cross-domain HTTP requests

Martin Johns
SAP Research

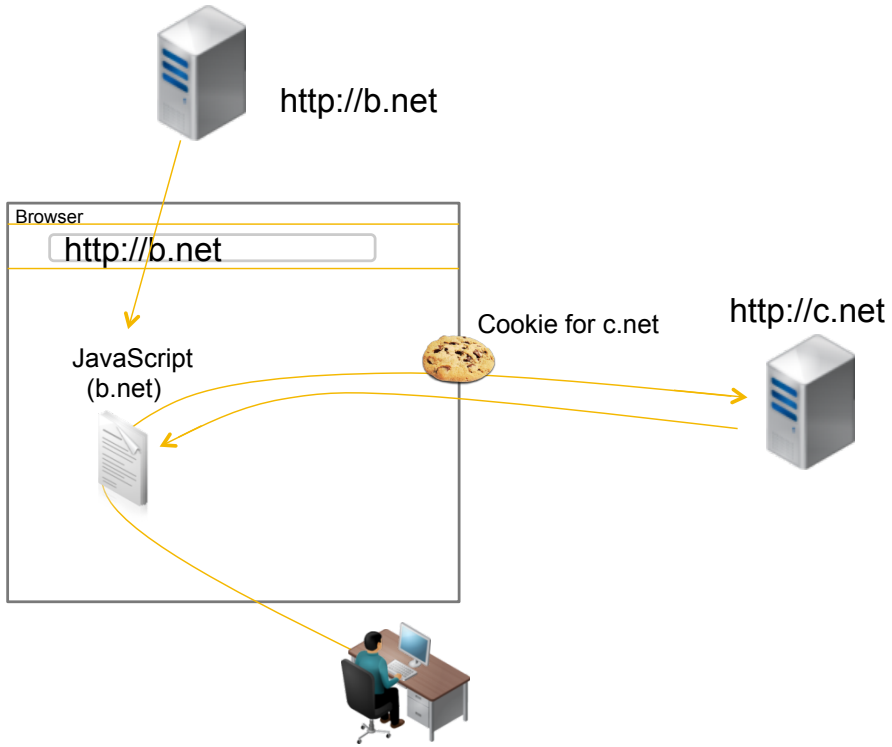
SAP

WebSand

What are client-side cross-domain requests?

They are

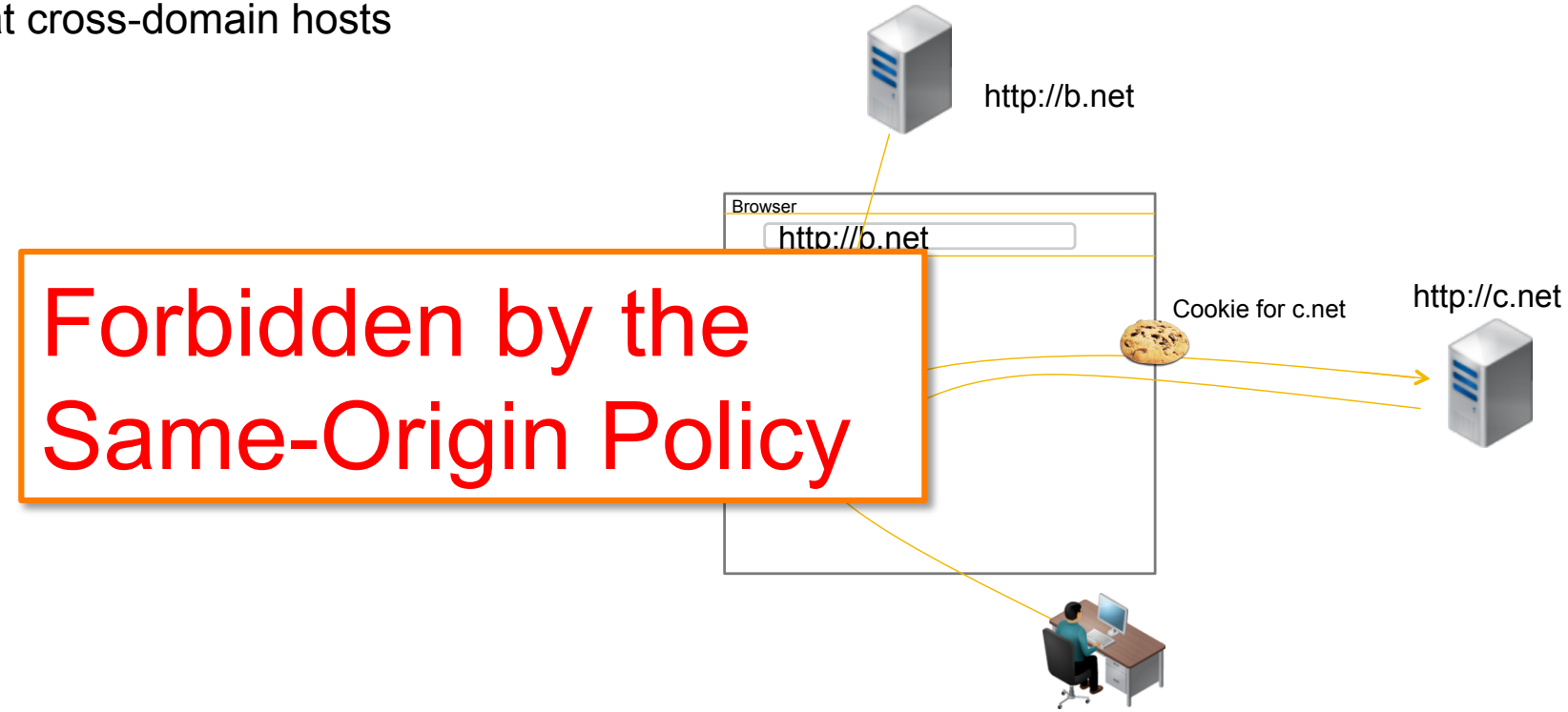
- Initiated by JavaScript via XMLHTTPRequest
- Directed at cross-domain hosts



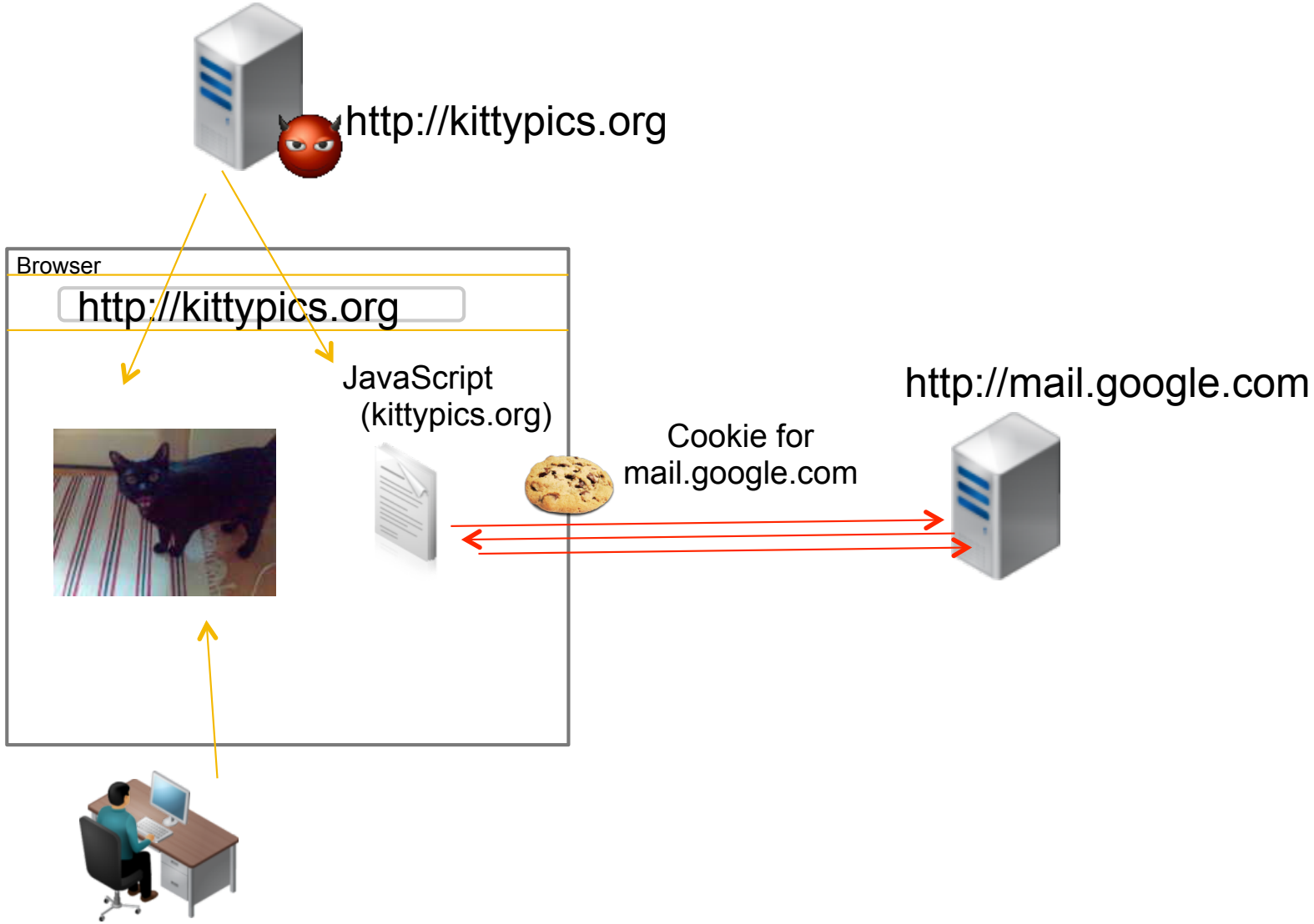
What are client-side cross-domain requests?

They are

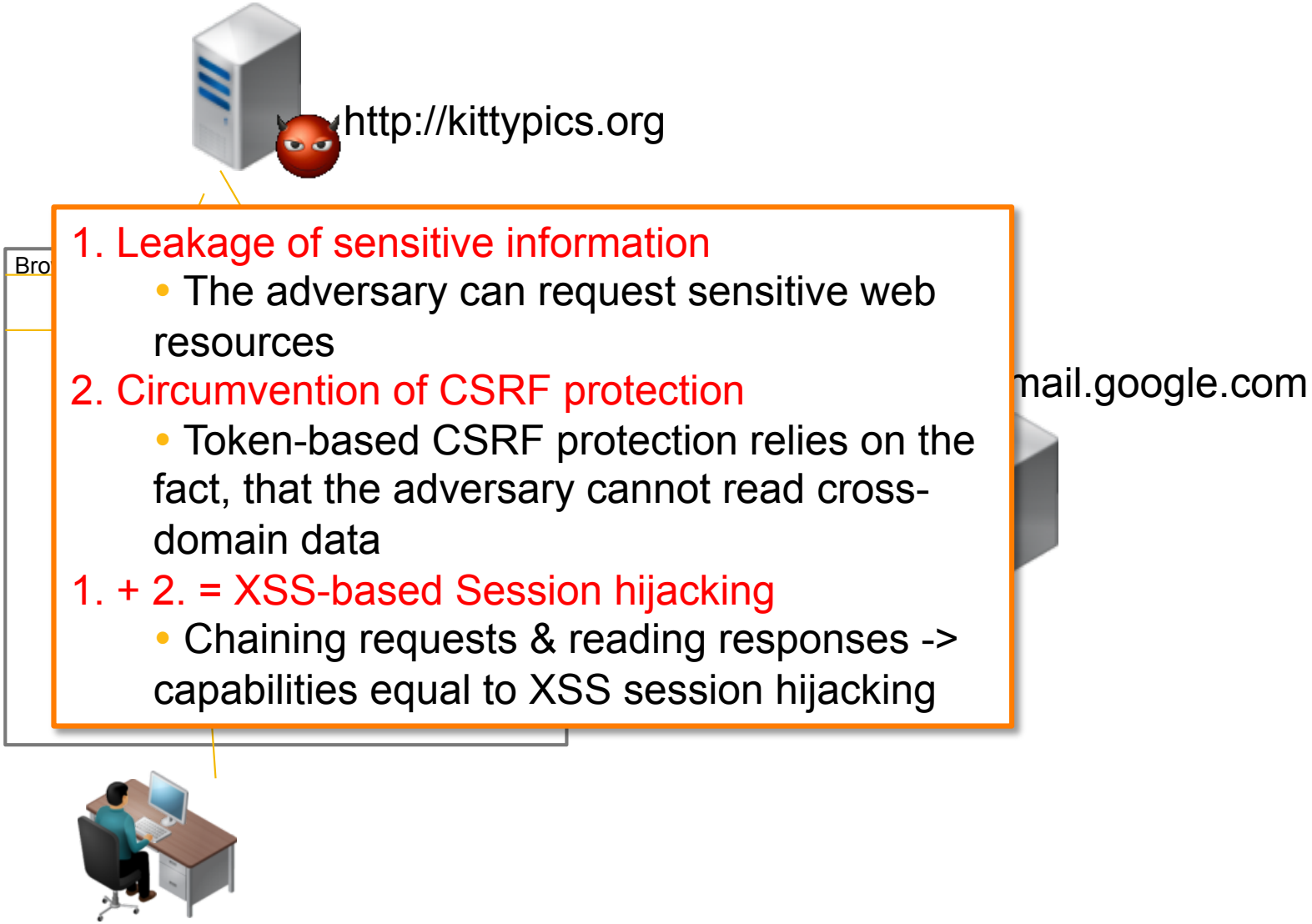
- Initiated by JavaScript via XMLHTTPRequest
- Directed at cross-domain hosts



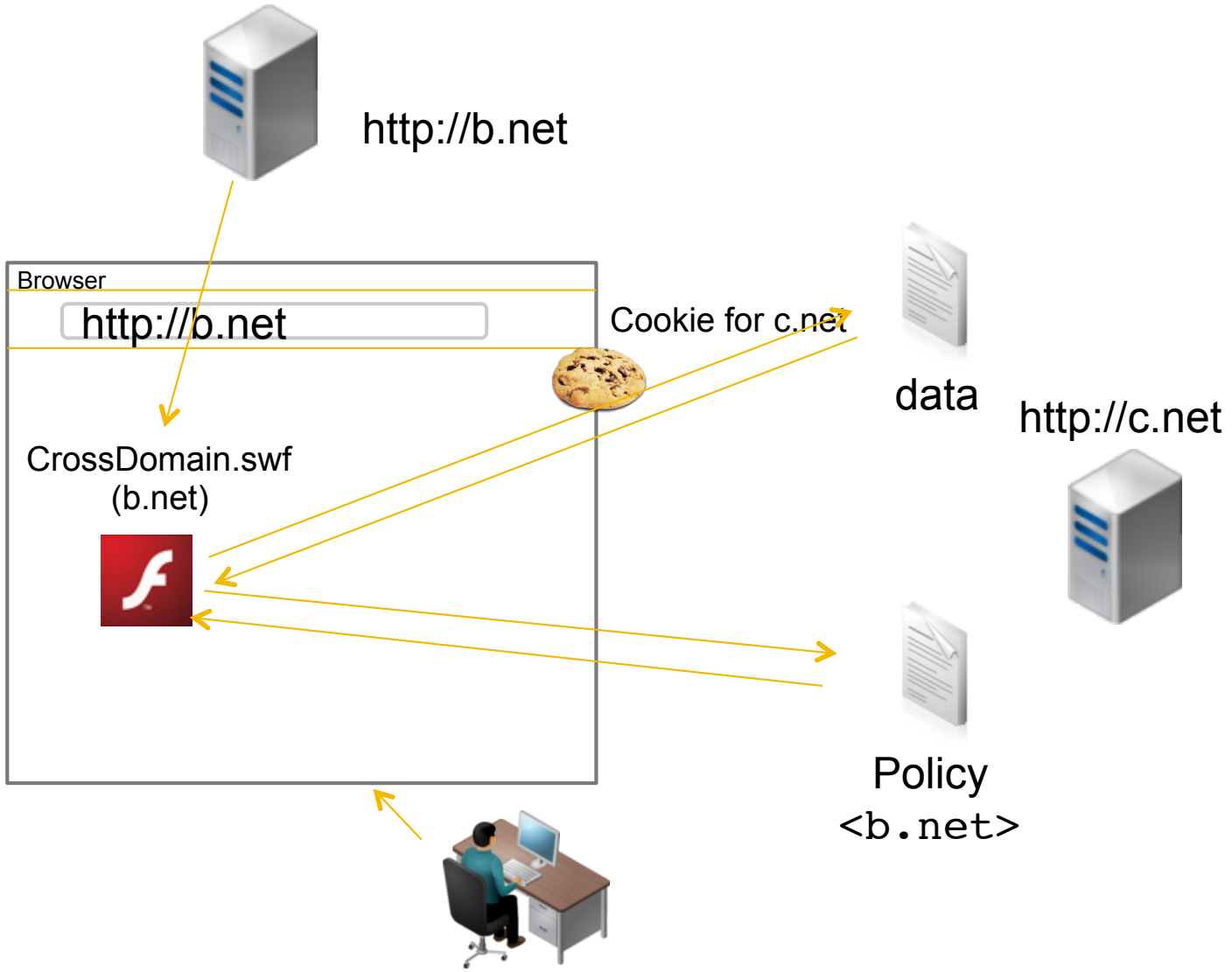
Security implications



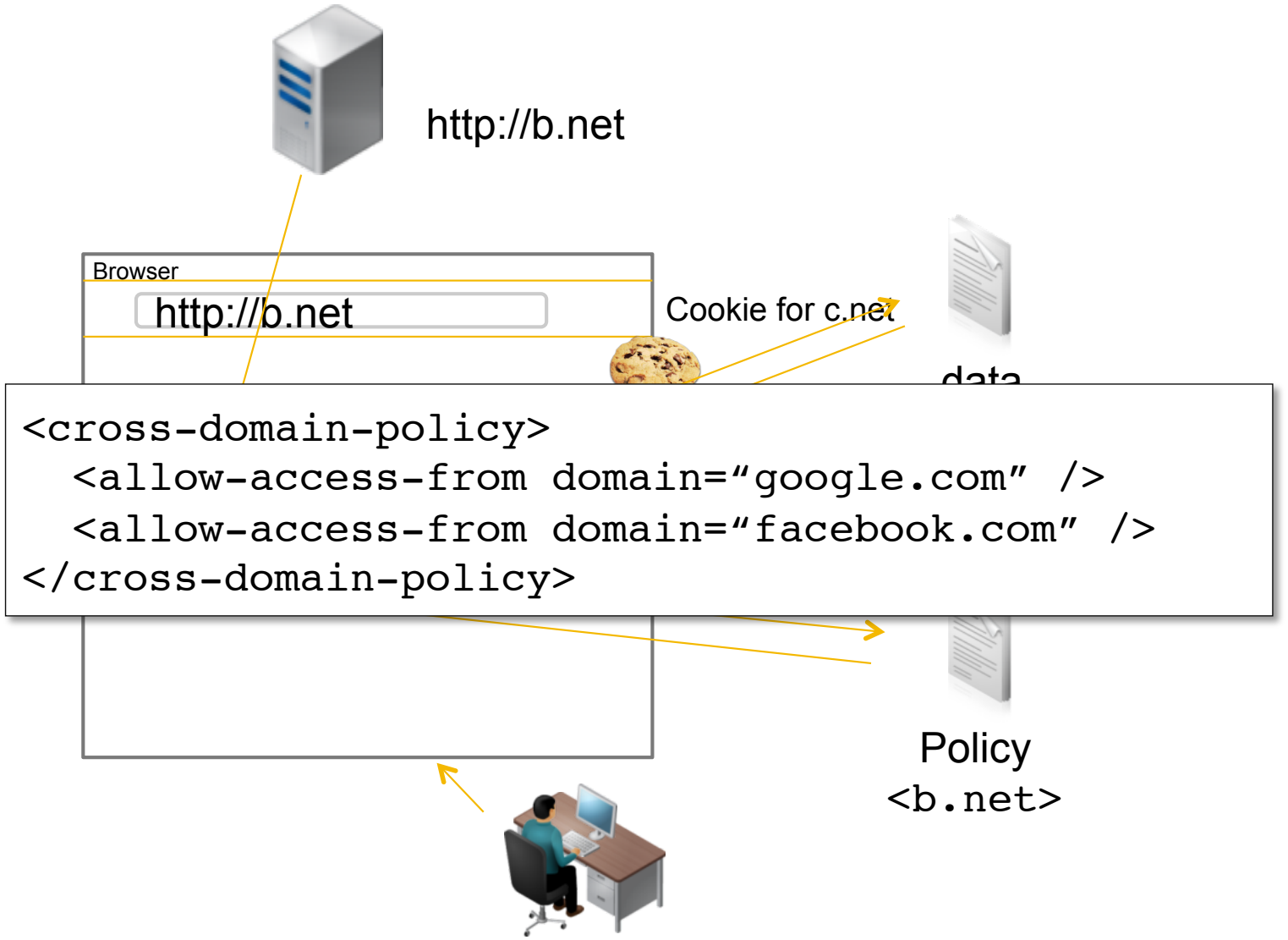
Security implications



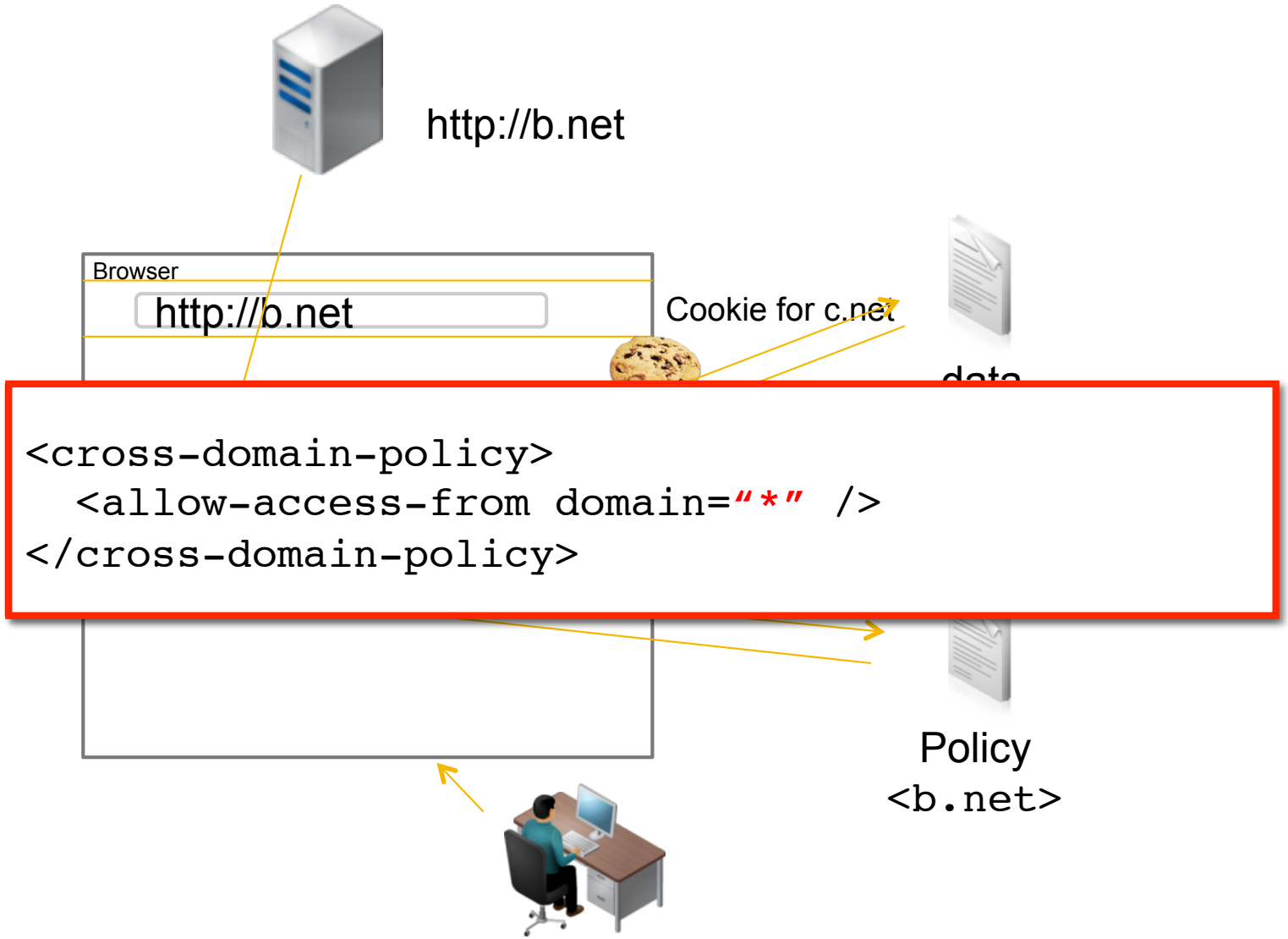
Opt-in model for client-side cross-domain requests



Opt-in model for client-side cross-domain requests



Opt-in model for client-side cross-domain requests



Survey

Mission statement

Find out if cross-domain policies are used insecurely in the wild

Method

Examine the policies of the Alexa top 1.000.000

1,093,127 domains scanned

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

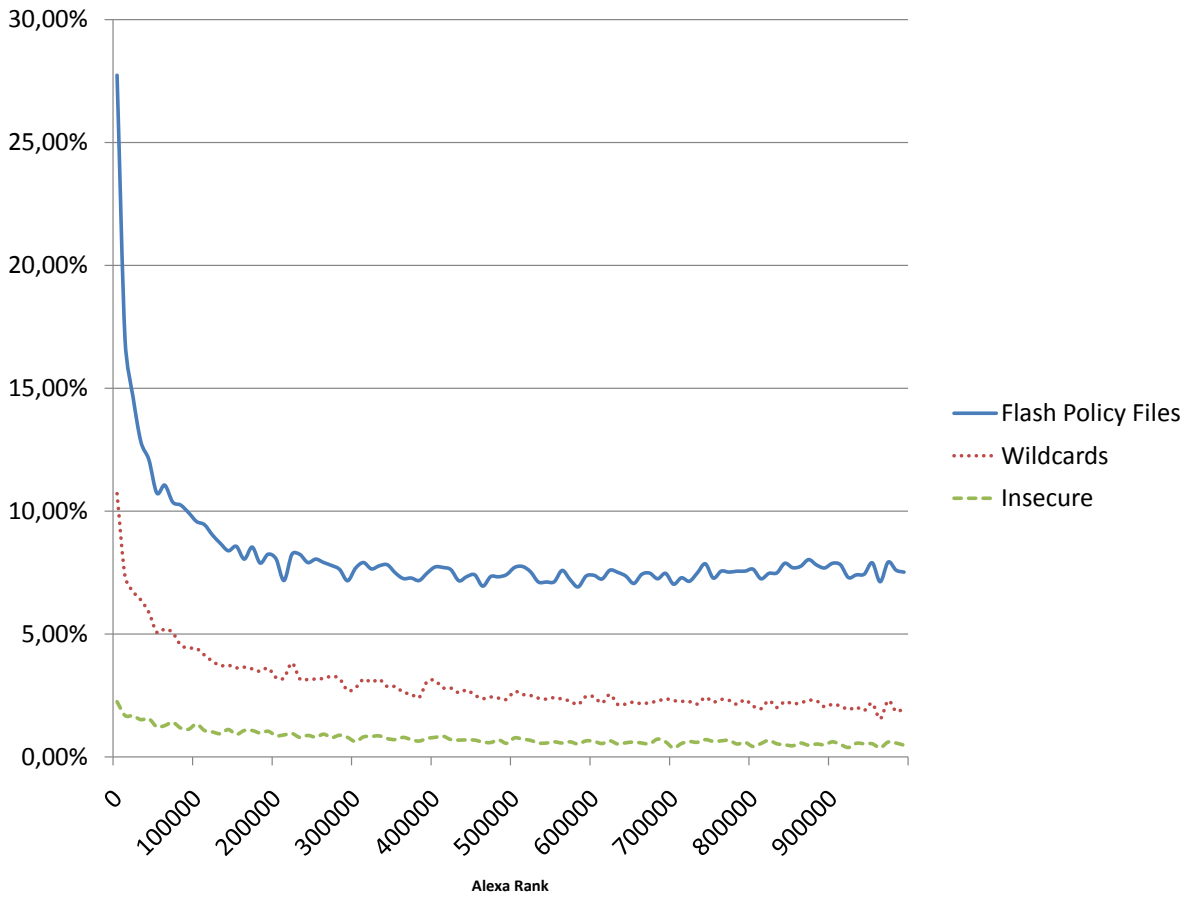
Results
Penetration / Security - Flash

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

Conclusion

Check your site's crossdomain.xml files

- You might be surprised…

Only allow trusted domains

Or even better – Use CORS (cross-origin resource sharing)

- However, that is a topic for another talk

Thank You!

Contact information:

Martin Johns
SAP Research
martin.johns@sap.com