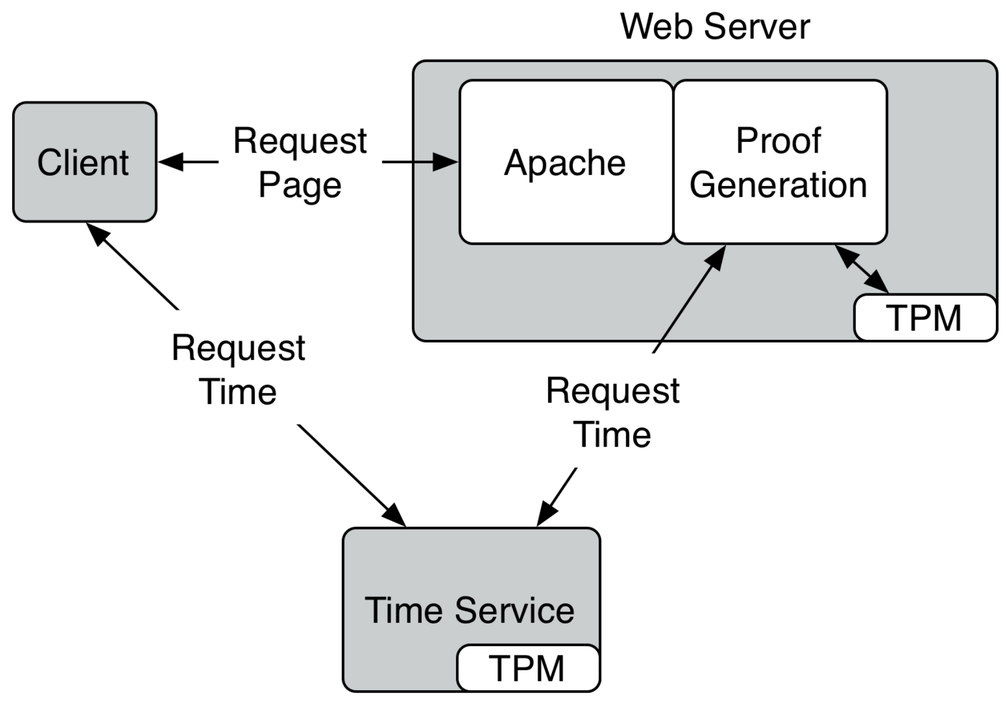
Scalable Web Content Attestation

Thomas Moyer, Kevin Butler, Joshua Schiffman,
Patrick McDaniel and Trent Jaeger

When using the web, there is little that can be done to validate the integrity of the server, or of the content that it delivers. We develop and evaluate a system enabling the use of the TPM to tie the web server integrity state to the web content delivered to browsers. However, the TPM does not scale well to high demand services, with operations taking on the order of 900 milliseconds per request. We develop an asynchronous usage model which removes the TPM from the critical path of serving content to users.
Our system protects a server from several types of threats including rootkits and malicious patches through the use of integrity measurement. It is possible to augment other web security tools such as SSL with our asynchronous content attestations.

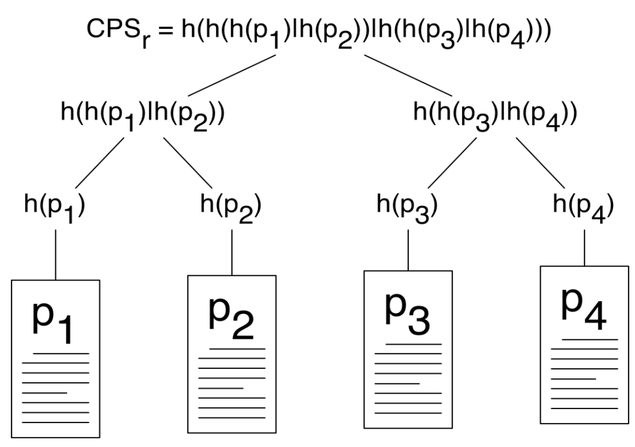


Asynchronous Model

-Since TPM is a slow device, we need to keep it out of the critical path of high demand services.

-The web server creates request-independent attestations by combining the time with a hash tree of the served content.

-A *root of trust time service* provides verifiable attestations of the current time to ensure freshness.



Challenges

-Attestations using IMA are large (relative to the content size), so we explore different optimizations to reduce the size.

-We can use policy to reduce the monitored subjects in the system (PRIMA)

-Per web-object proof requests cause too much overhead per client

-Create one proof that covers the source page and all embedded content

  -Images, scripts, etc.

Optimizations

	μ	ϵ	**Expected**		**Actual**	
			$\mathcal{P}$	Web Objects	$\mathcal{P}$	Web Objects
Baseline with Static Root Page	10769	4485.5	868.4	9552.5	867.4	9541.5
Baseline with Dynamic Root Page	10769	4507.8	869.2	9561.7	745.9	8204.8
Integ. Measured Static Root (Full IMA)	10769	968.1	509.8	5607.8	494.9	5444.4
Integ. Measured Static Root (Comp. PRIMA)	10769	1526.8	631.5	6946.4	724.3	7967.4
Integ. Measured Dynamic Root (Full IMA)	10769	1130.7	551.6	6067.3	494.4	6438.3
Integ. Measured Dynamic Root (Comp. PRIMA)	10769	1127.2	550.7	6058.1	650.5	7155.1

-Amortize proof for a *single client* over the source page and all embedded objects

-With optimizations, we can achieve 8000 static requests per second or 7000 dynamic requests per second

Publications

T. Moyer, K. Butler, J. Schiffman, T. Jaeger and P. McDaniel, **Scalable Web Content Attestation**, Proceedings of the 2009 Annual Computer Security Applications Conference (ACSAC), December 2009

Sponsored by NSF (CNS-0643907 and CNS-0627551).