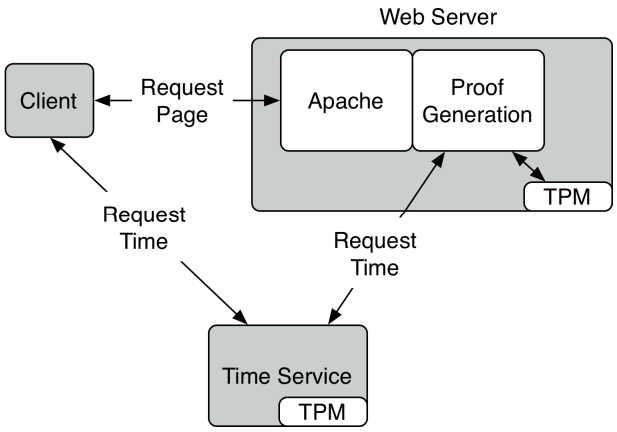
Scalable Asynchronous Web Content Attestations

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 content being delivered by the server. 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.

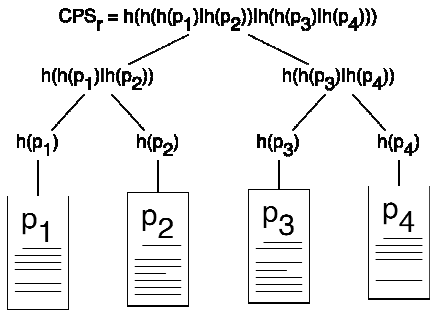


Asynchronous Model

-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)

Future Work: Dynamic Content

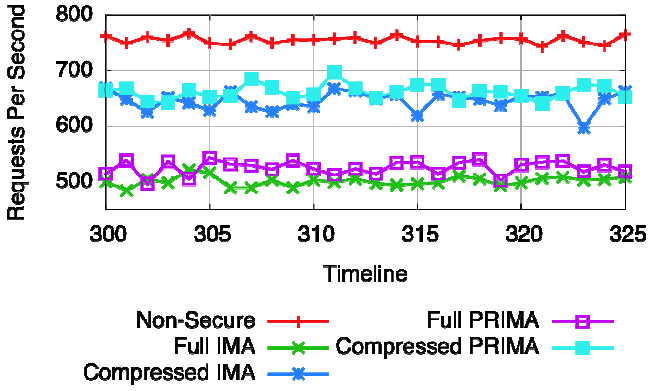
-We extend our architecture to handle dynamic content

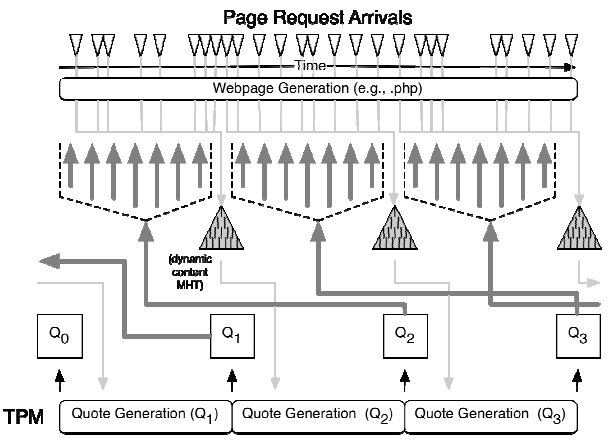
-Unlike static content, hash tree cannot be generated before requests arrive.

-We cache responses and periodically generate hash tress for client requests.

Optimizations

-With Compressed PRIMA, we were able to come within **12.5%** of an unmodified Apache web server's throughput.





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