Aalto University
School of Science

Tekes

Collaborative Research Institute
for Secure Computing

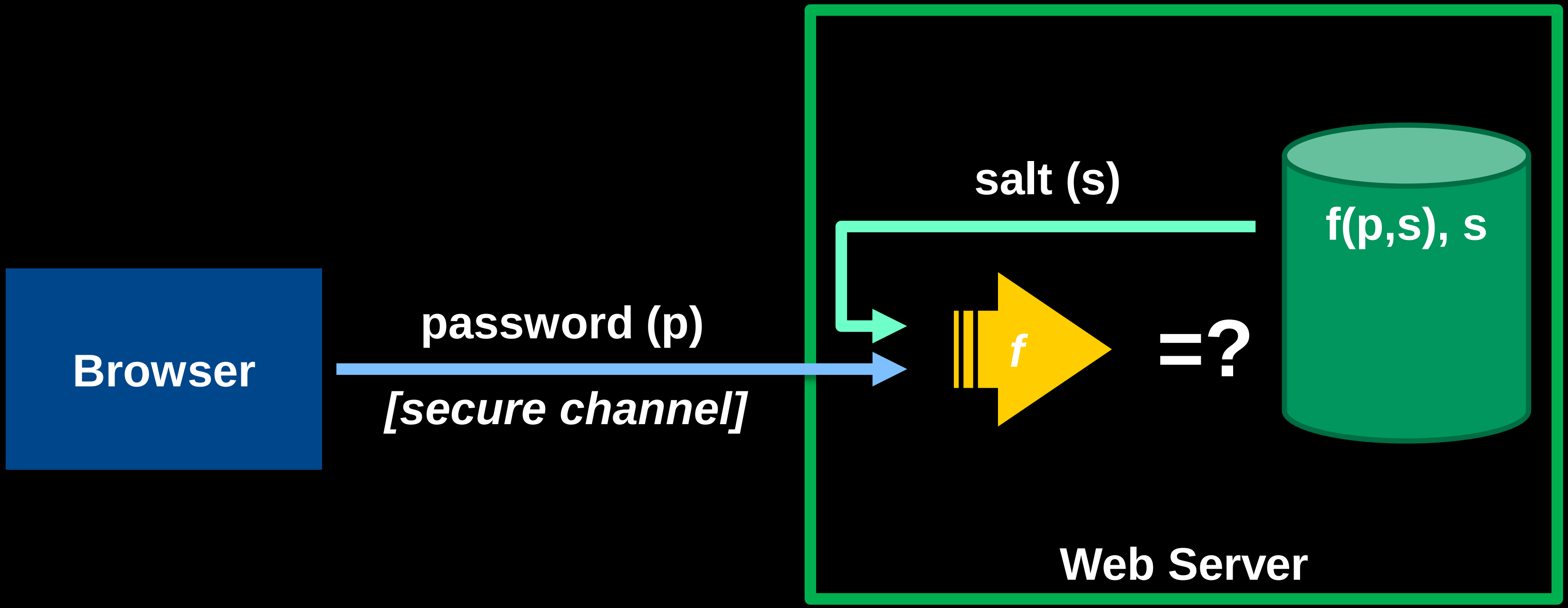
Protecting Password Databases using Trusted Hardware

Klaudia Krawiecka, Andrew Paverd, N. Asokan

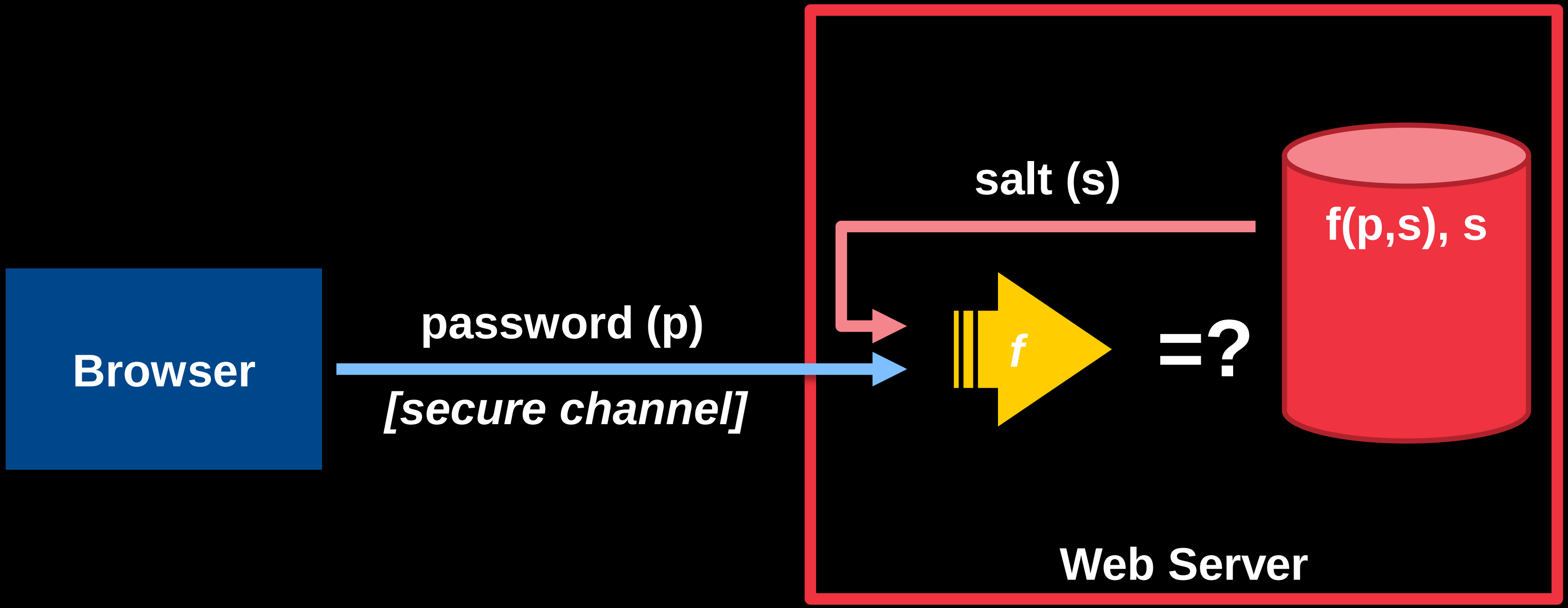
Aalto University, Finland

This work was supported by the Cloud Security Services (CloSer) project funded by Tekes - the Finnish Funding Agency for Innovation, and the Intel Collaborative Research Institute for Secure Computing.

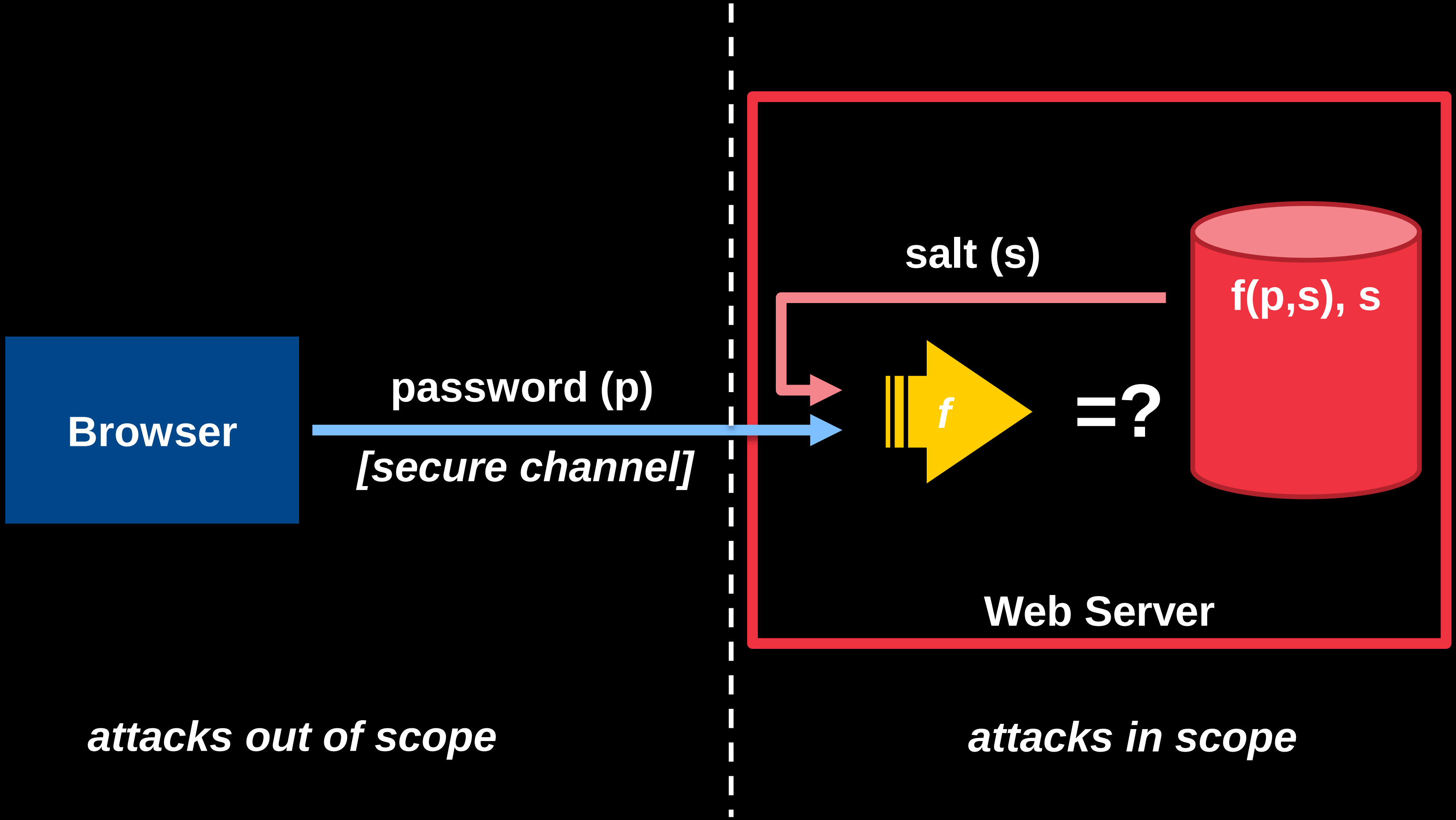
Storing Passwords



Storing Passwords


Browser
password (p)
[secure channel]
salt (s)
f
=?
f(p,s), s
Web Server

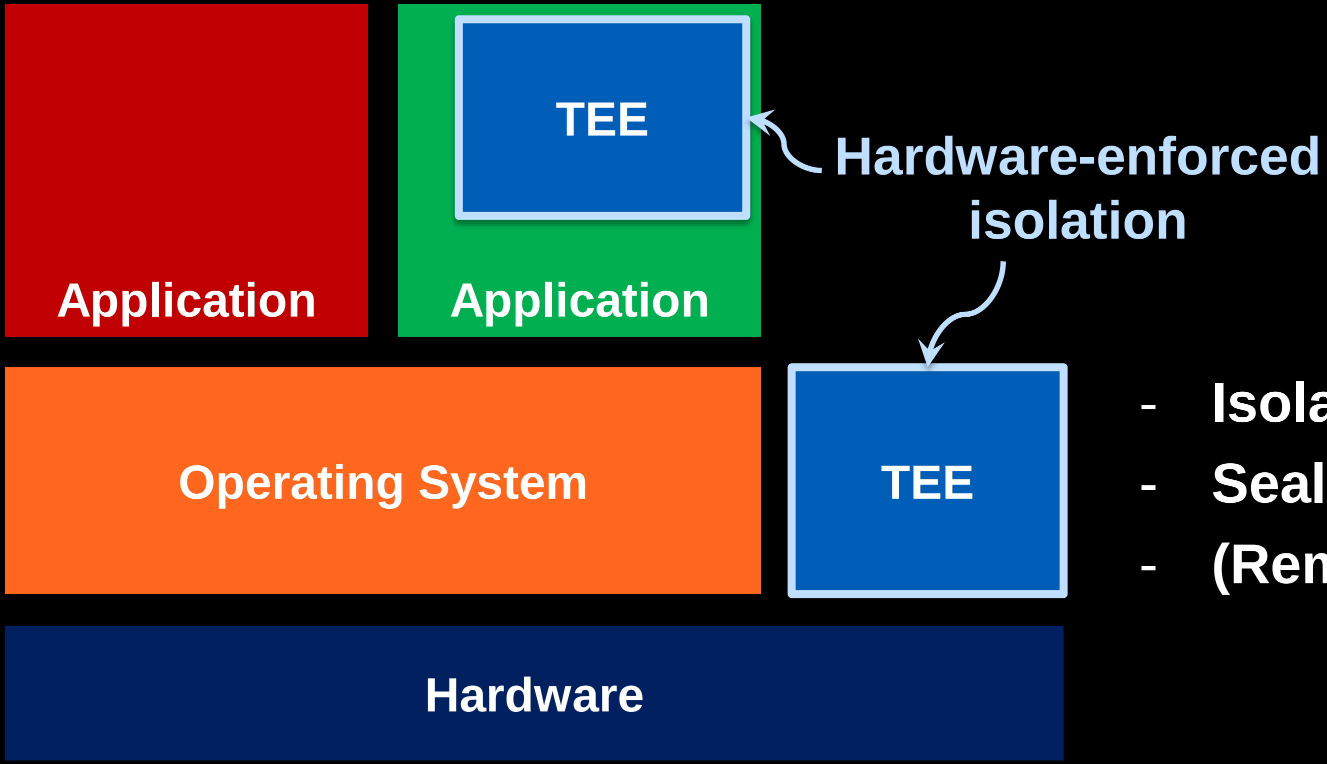
Storing Passwords



attacks out of scope

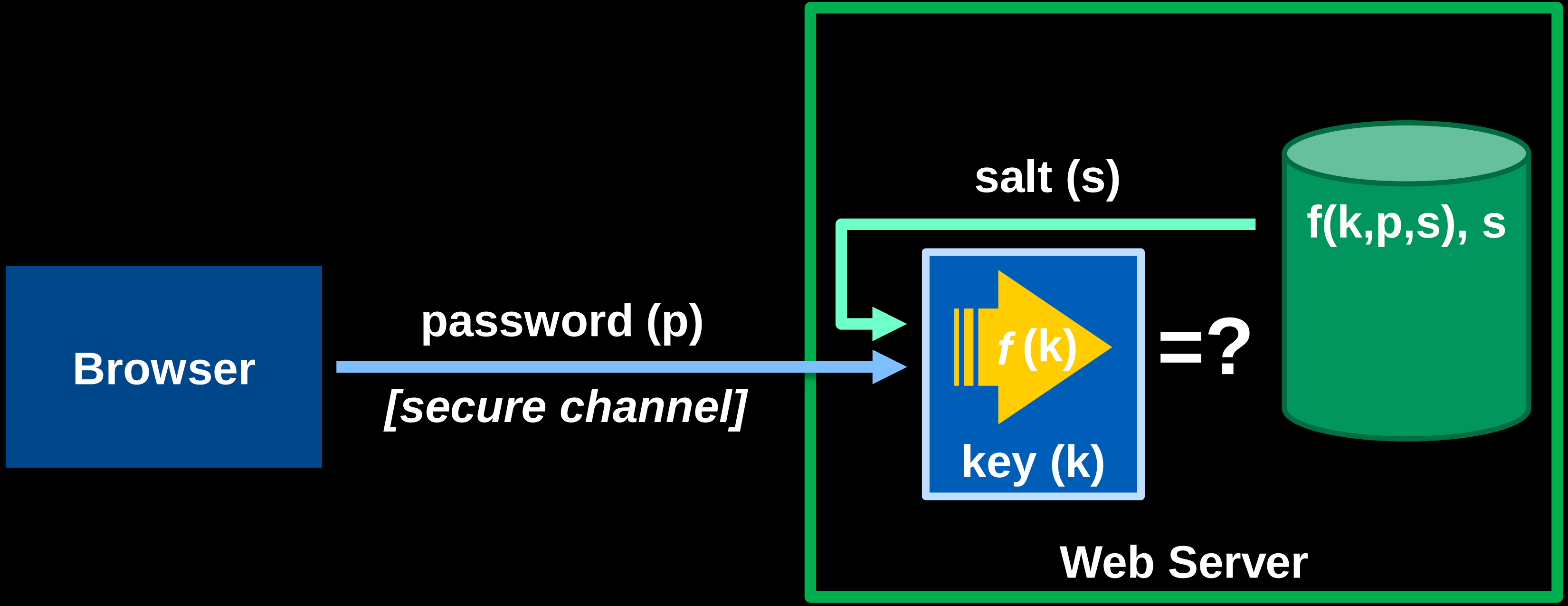
attacks in scope

Trusted Execution Environments

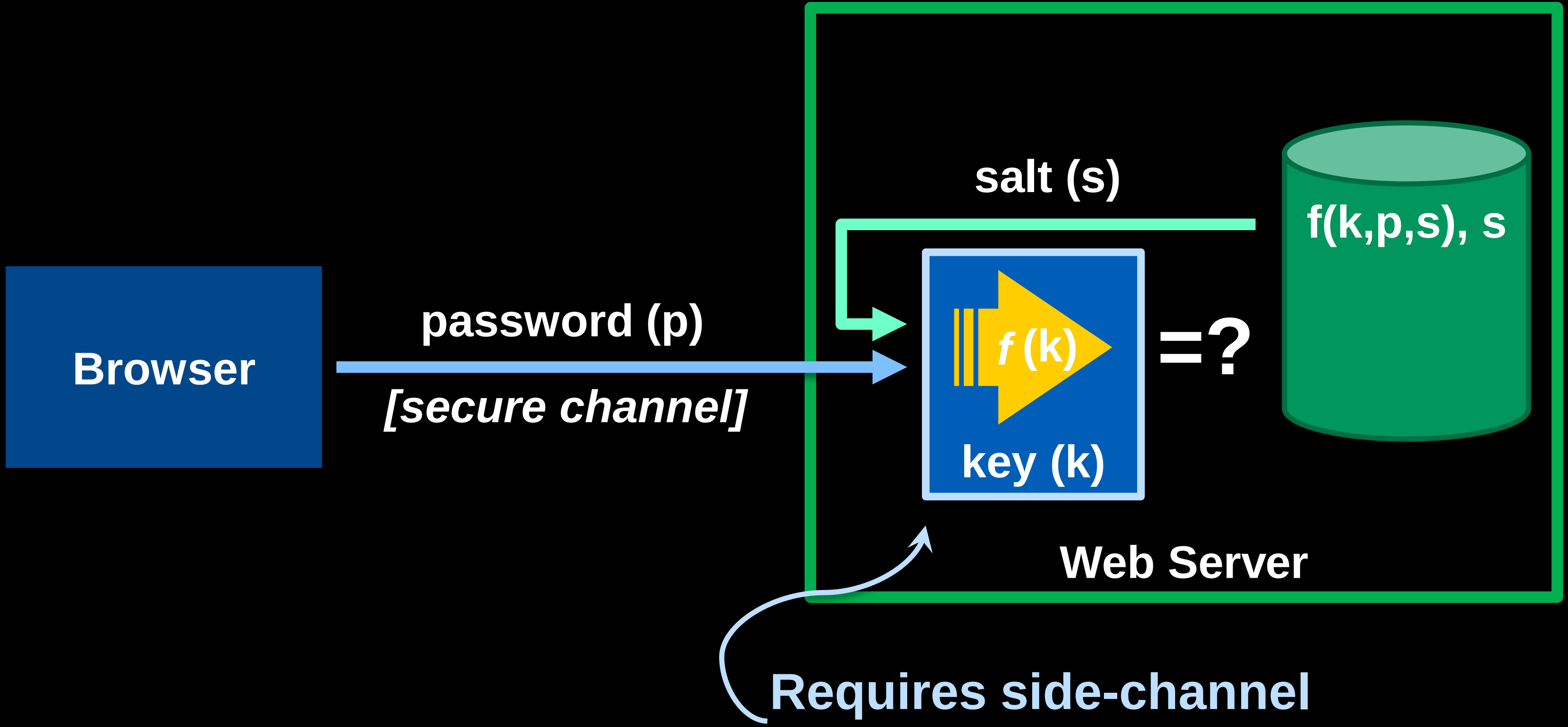


- Isolated execution
- Sealed storage
- (Remote attestation)

Storing Passwords *Securely*

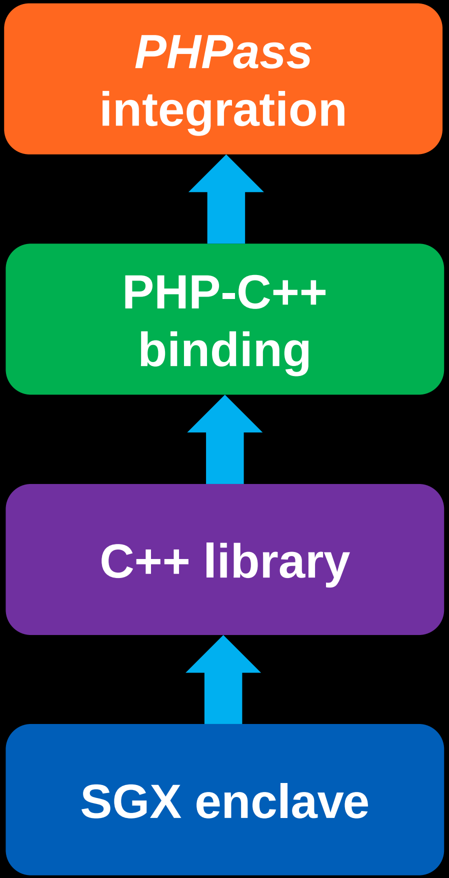


Storing Passwords *Securely*



Requires side-channel resistant design

Prototype



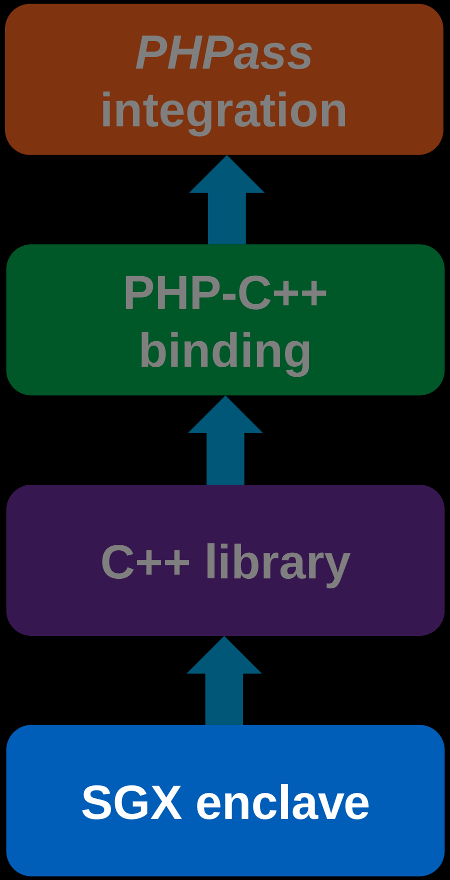
PHPass integration

PHP-C++ binding

C++ library

SGX enclave

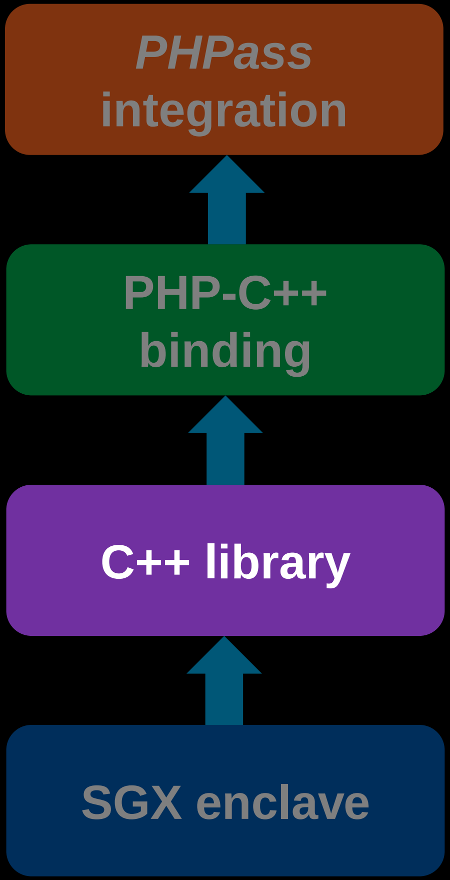
Prototype



- **Key generation or import**
- **Key sealing (MRENCLAVE)**
- **Keyed one-way function**
  - CMAC from *sgx_tcrypto* library
  - 128 bit key
  - AES-NI hardware acceleration
- **Lines of code: 60**

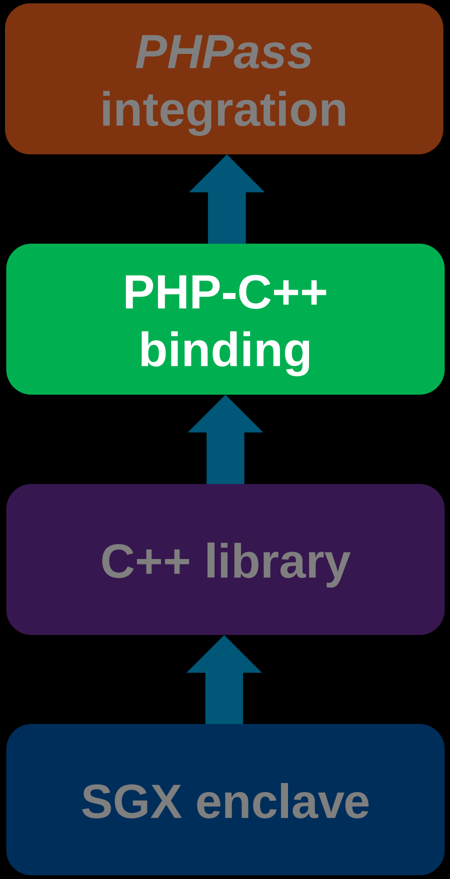
(+ Intel trusted libraries)

Prototype



- Enclave initialization
- Sealed data storage/retrieval

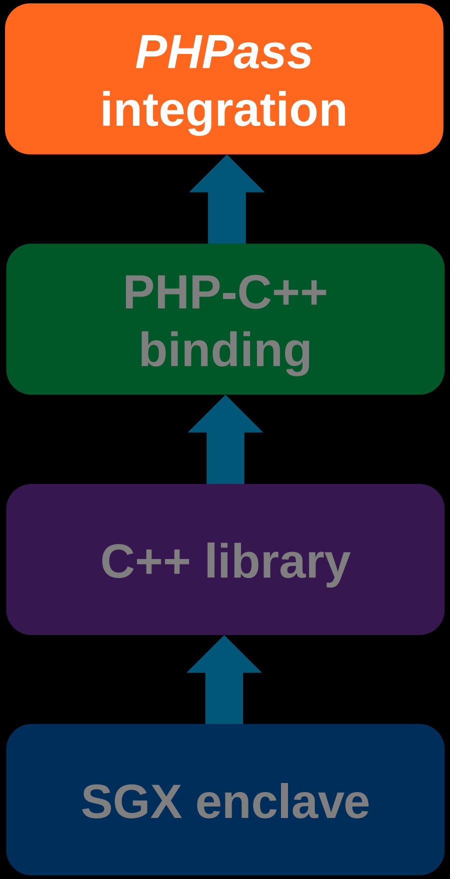
Prototype



- **PHP-CPP**
  - “C++ library for writing PHP extensions”

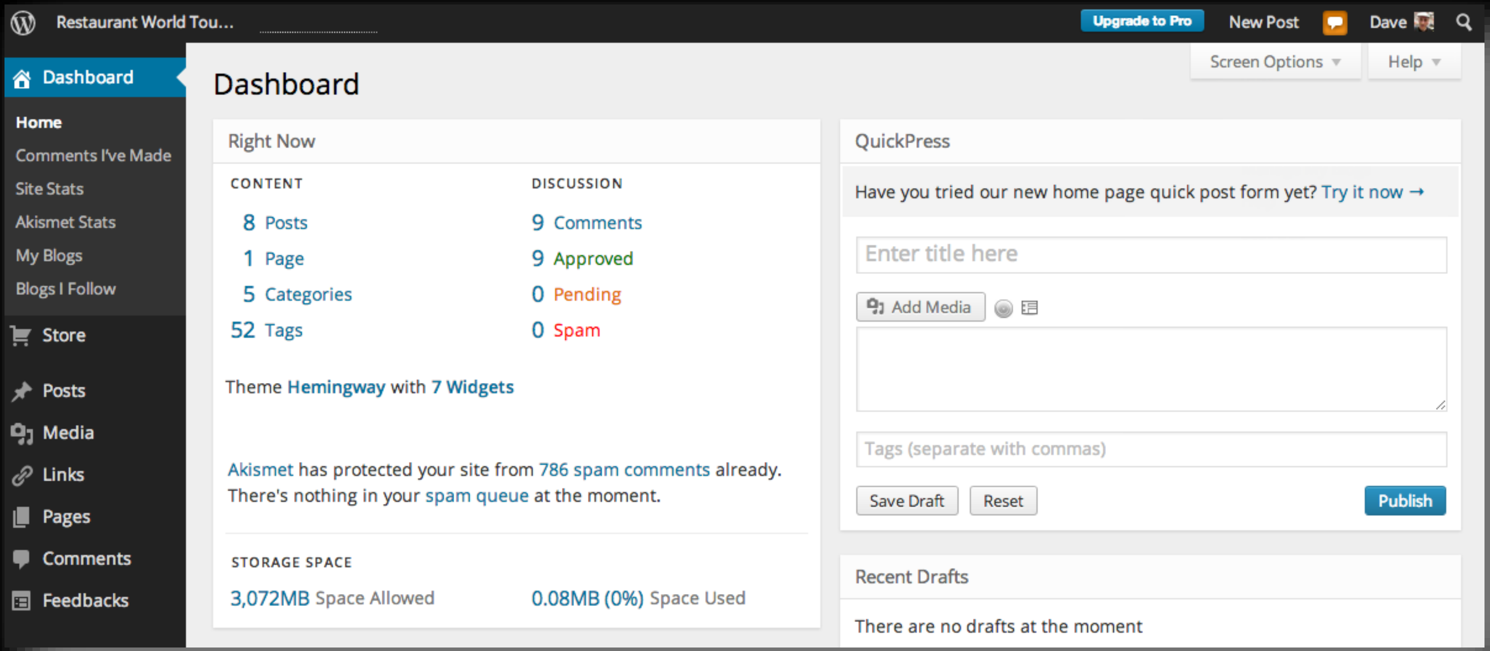
http://www.php-cpp.com/

Prototype



- Used by WordPress, Joomla, etc.
- Default: multi-round MD5 (!)
- Enhanced to use our SGX enclave

Prototype



Dashboard

Right Now

CONTENT		DISCUSSION	
8	Posts	9	Comments
1	Page	9	Approved
5	Categories	0	Pending
52	Tags	0	Spam

Theme Hemingway with 7 Widgets

Akismet has protected your site from 786 spam comments already. There's nothing in your spam queue at the moment.

STORAGE SPACE

3,072MB Space Allowed 0.08MB (0%) Space Used

QuickPress

Have you tried our new home page quick post form yet? Try it now →

Enter title here

Add Media

Tags (separate with commas)

Save Draft Reset Publish

Recent Drafts

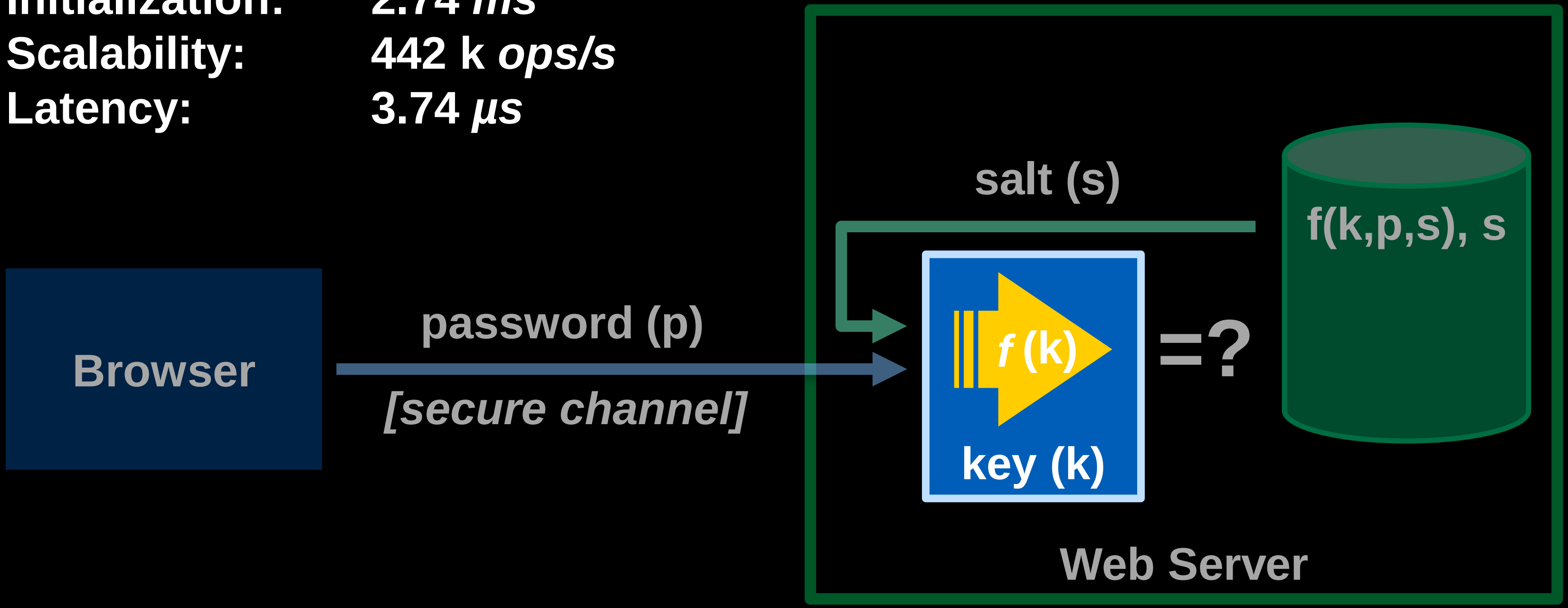
There are no drafts at the moment

Setup: Intel Core i5 6500 3.2 GHz, 8 GB RAM, Ubuntu 14.04
WordPress 4.5.3, PHP 5.5.9, Apache 2.4.7

Performance

single threaded

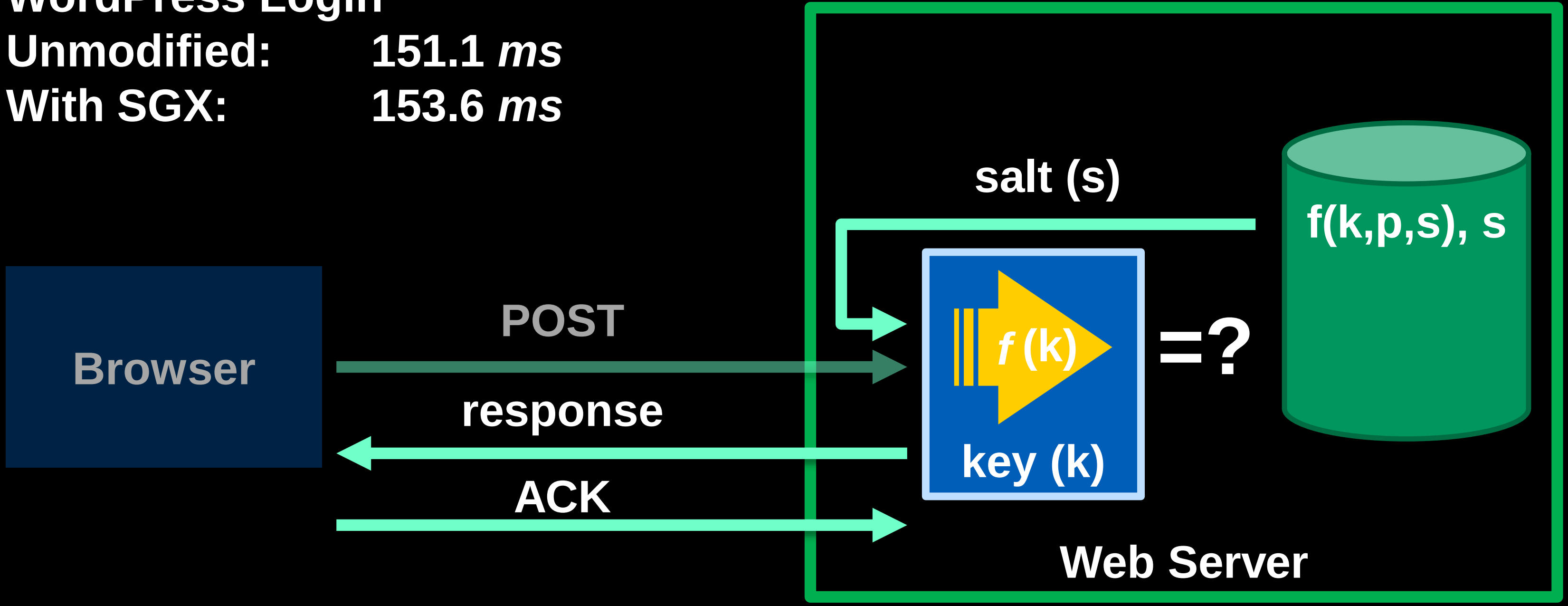
Initialization:	2.74 *ms*
Scalability:	442 k *ops/s*
Latency:	3.74 *µs*



Setup: Intel Core i5 6500 3.2 GHz, 8 GB RAM, Ubuntu 14.04

Performance

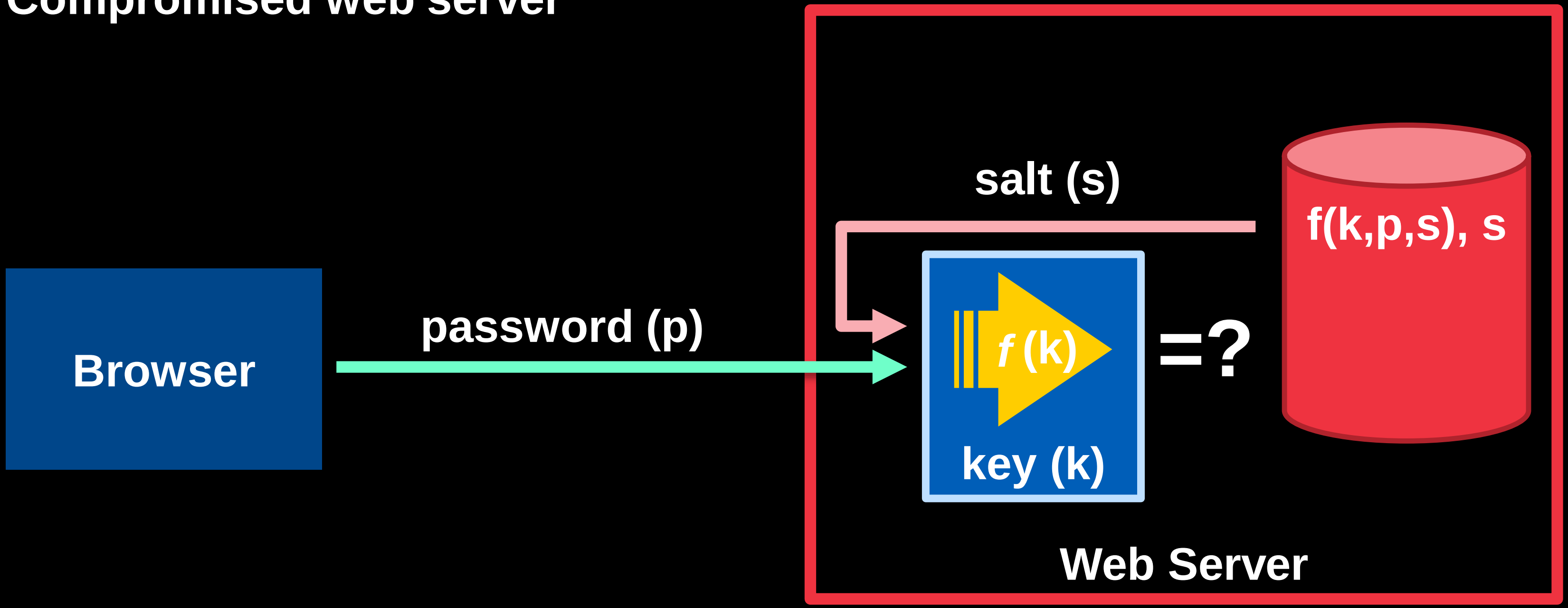
WordPress Login
Unmodified: 151.1 *ms*
With SGX: 153.6 *ms*



Setup: Intel Core i5 6500 3.2 GHz, 8 GB RAM, Ubuntu 14.04
WordPress 4.5.3, PHP 5.5.9, Apache 2.4.7

Work in Progress

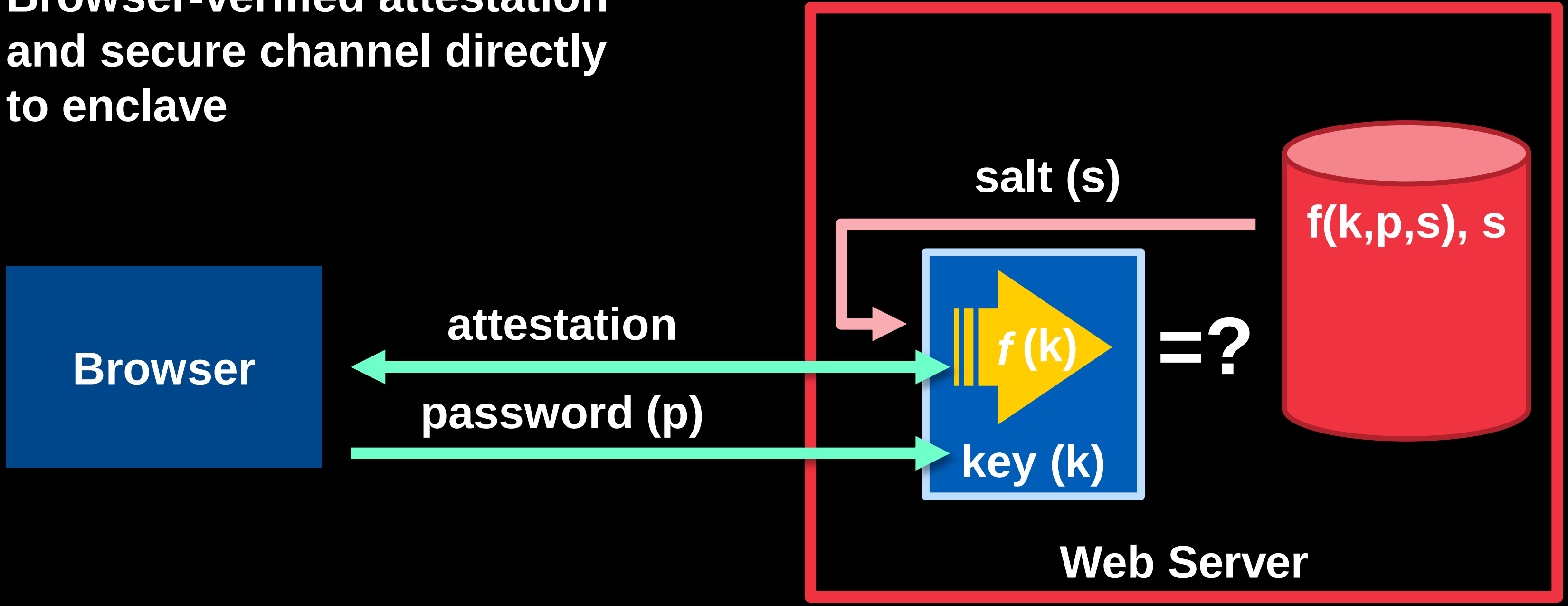
Compromised web server



Attacker learns passwords immediately

Work in Progress

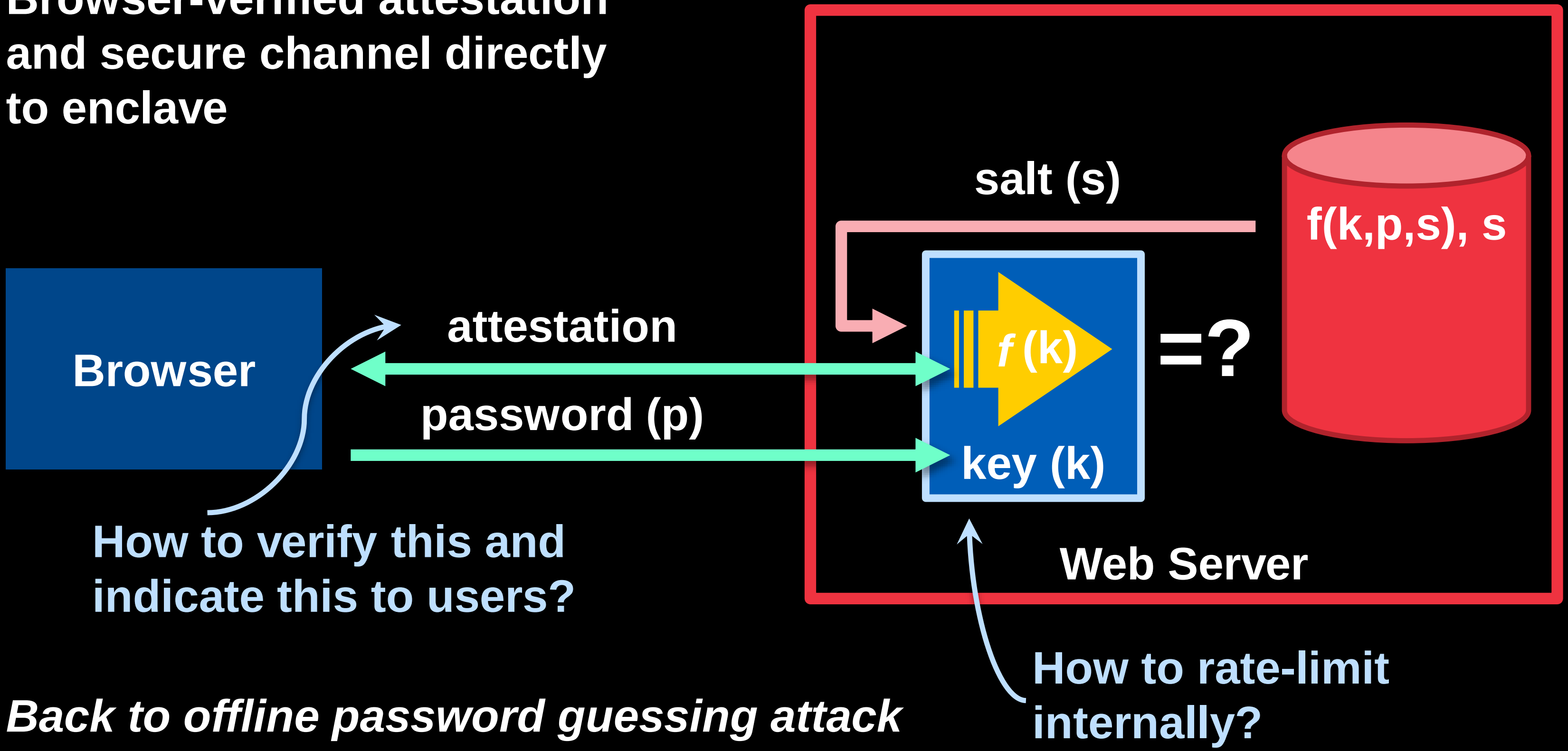
Browser-verified attestation and secure channel directly to enclave



Back to offline password guessing attack

Work in Progress

Browser-verified attestation and secure channel directly to enclave



How to verify this and indicate this to users?

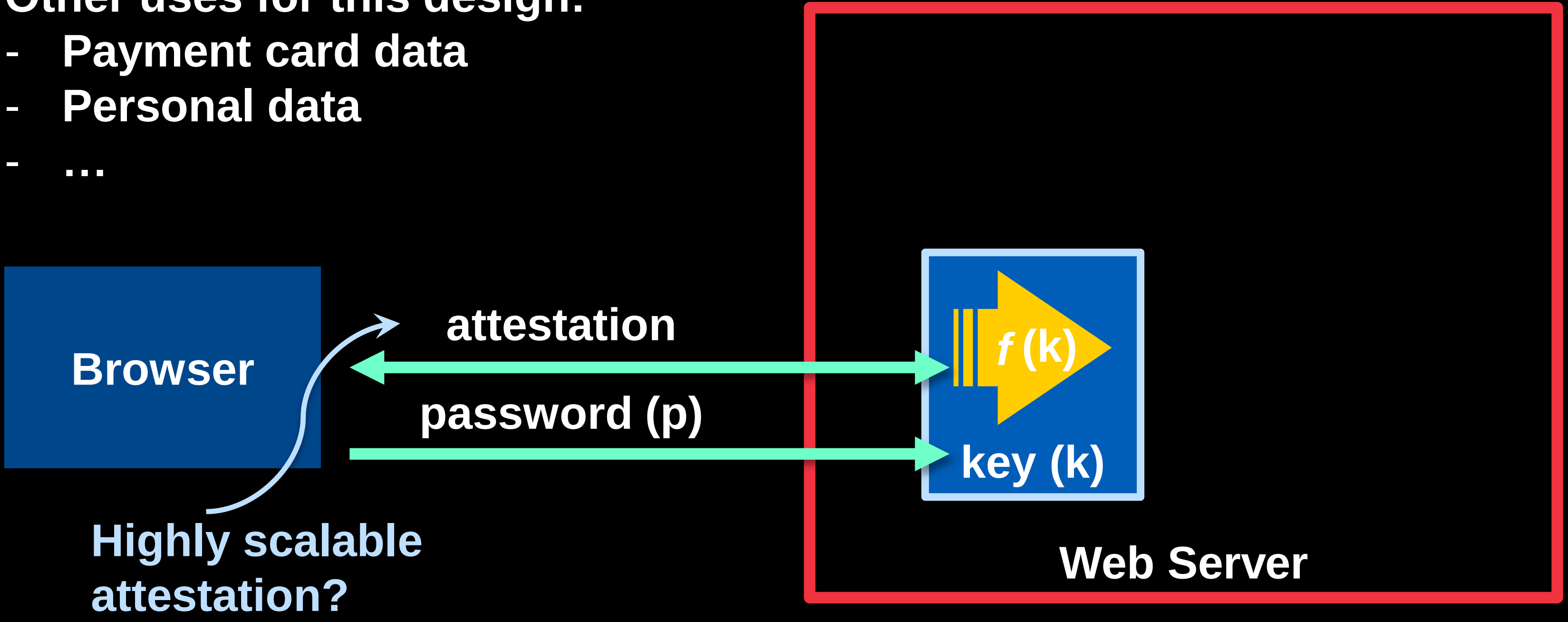
How to rate-limit internally?

Back to offline password guessing attack

Work in Progress

Other uses for this design:

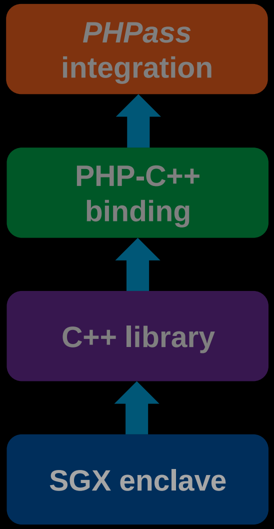
- Payment card data
- Personal data
- …



c.f. Lyle & Martin. "Engineering attestable services" *TRUST*, 2010.

Conclusion

- TEEs can help to protect password databases
- Can be integrated into existing systems
- Performance is sufficient
- Some challenges still remain
- Potential for future work

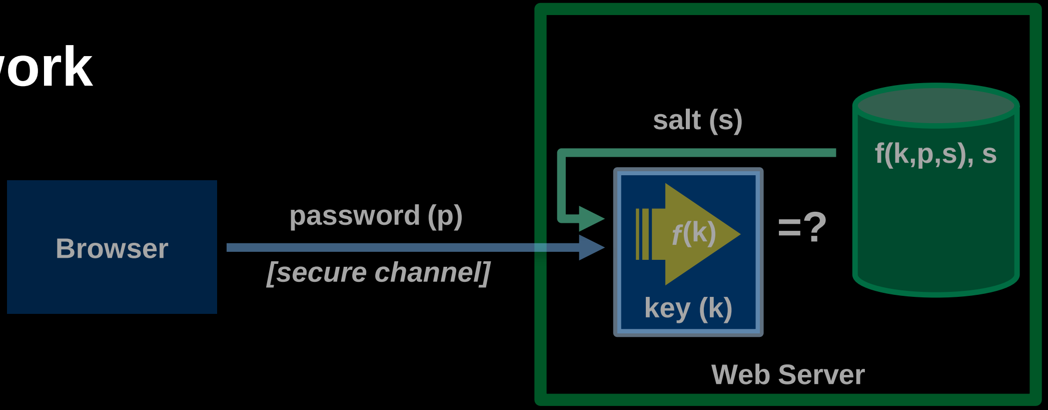


PHPass integration

PHP-C++ binding

C++ library

SGX enclave



Browser

password (p)

[secure channel]

salt (s)

f(k)

key (k)

=?

f(k,p,s), s

Web Server