Secure (One-Time-) Password Authentication for the Globus Toolkit

Olivier Chevassut

(Lawrence Berkeley National Laboratory)

Frank Siebenlist

(Argonne National Laboratory)

Outline

- Introduction
  - — motivations
  - — objectives

- One-Time Password Authentication
- Authenticated Key Exchange
- One-time Password Authentication and Key Exchange
- Integration with the Globus Toolkit
- Conclusion and Future Work

Motivation

- An increasing number of Grid-enabled applications have security requirements:
  - integrity and privacy of data transmitted on the wire
  - protection against viruses, trojan horses, and Spyware-like software
  - protection from hackers
- An increasing number of Grid sites are changing their security policies:
  - long-lived credentials are no longer stored on users' machines
  - long-lived credentials are stored on data centers' servers
  - users obtain short-lived credentials after successful authentication

Objectives

- A technology allowing data centers to *securely* authenticate a user connecting from un-trusted terminals (e.g, cybercafe):
  - protects against replaying of a captured user's password
  - protects against exhaustive searching for a user's password

- A technology allowing data centers to *securely* communicate a short-lived credential to a user:
  - protects against hijacking a session
  - provides data integrity and message confidentiality

⇒ A technology for One-time Password authentication and Key Exchange

Outline

- Introduction

ü One-time Password authentication (OP)

  — time-based technology

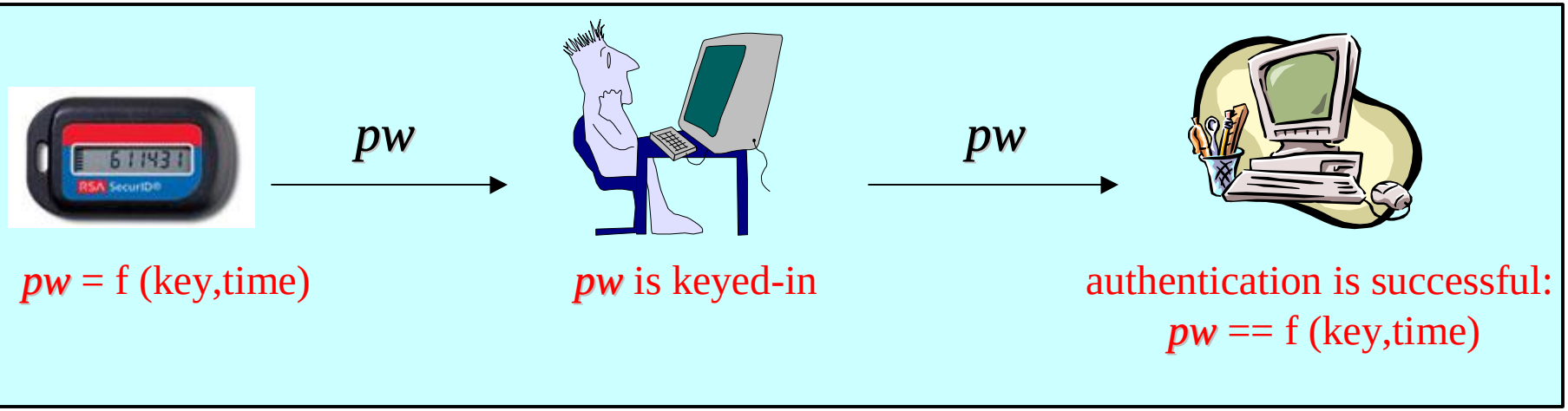
  — challenge-based technology

- Authenticated Key Exchange
- One-time Password authentication and Key-Exchange
- Integration with the Globus Toolkit
- Conclusion and Future Work

One-time Password authentication based on time

- The hand-held device derives a password *pw* as a function of its key and its clock
- The user keys *pw* into the terminal to authenticate himself to the server
- The server compares *pw* to an independently computed password

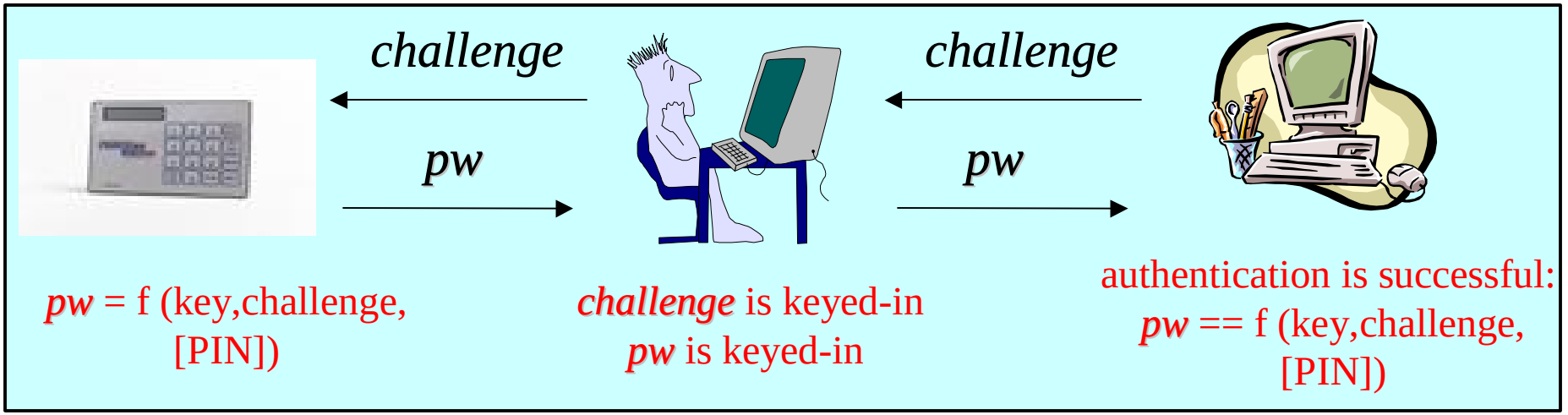
- RSA SecureID is an example of this technology:
  - advantages: simplicity of utilization, …
  - drawbacks: synchronization, secure-channel needed,…



One-time Password authentication based on a challenge

- The hand-held device derives a password *pw* as a function of its key, a keyed-in challenge [and secret pass-phrase]
- The user keys in a challenge [and pass-phrase] to obtain *pw,* and then in turn keys *pw* into the terminal
- The server compares *pw* to an independently computed password

- CryptoCard is an example of this technology:
  - advantages: no synchronization, …
  - drawbacks: key-in a challenge, …



Outline

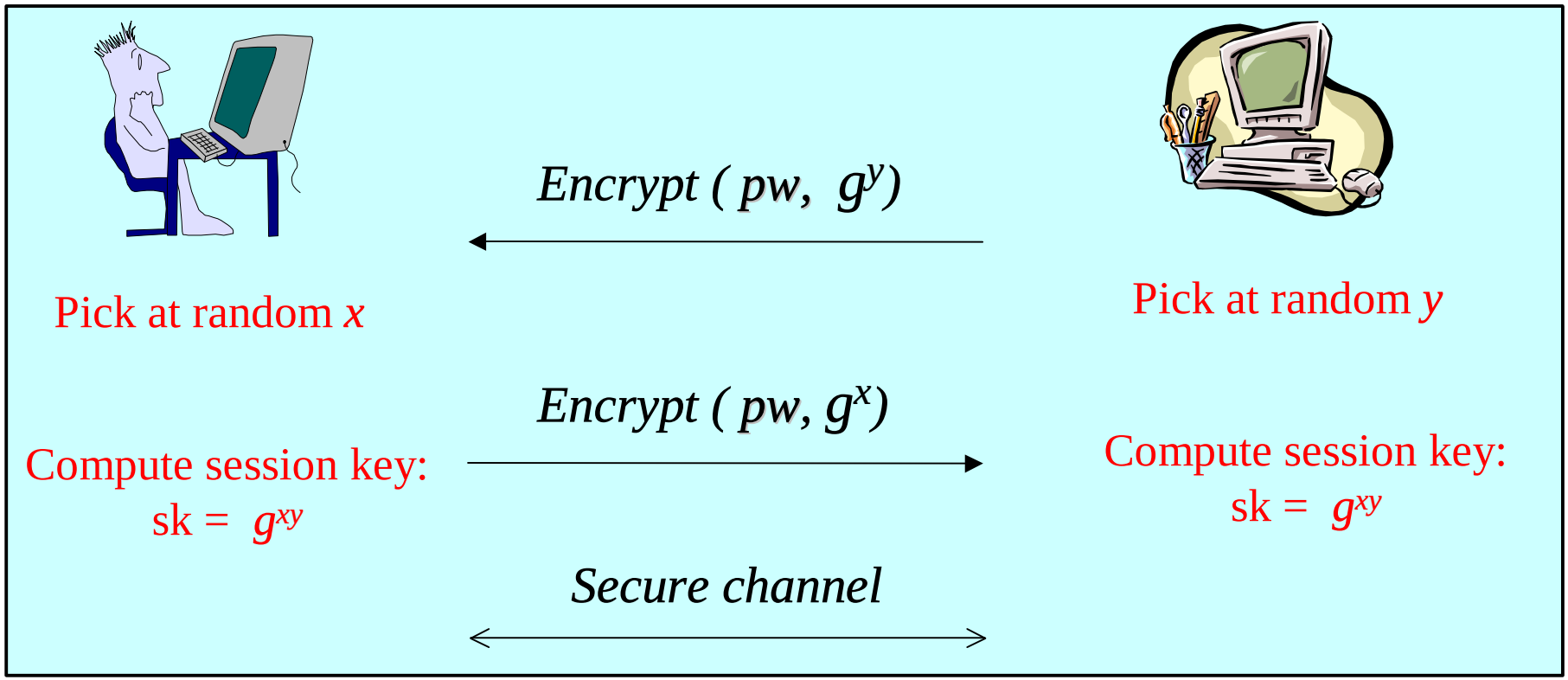
- Introduction
- One-time Password authentication (OP)

ü Authenticated Key eXchange (KeyX)
  — password-authenticated technology
  — security measurement

- One-time Password authentication and Key-eXchange
- Integration with the Globus Toolkit
- Conclusion and Future Work

Authenticated Key eXchange based on a short password (KeyX)

- The password *pw* is used to encrypt the Key eXchange algorithm's flows
- The KeyX algorithm allows the two-parties to agree on a session key sk
- The session key *sk* implements an encrypted and authenticated channel



O. Chevassut, GlobusWorld 2005, February 7-11.

The KeyX Algorithm: Security Measurement

- The algorithm relies on the impossibility of solving a *hard problem*:
  - the Diffie-Hellman problem (DH): given (g^a, g^b) compute g^{ab}
- The algorithm is secure against *dictionary attacks*:
  - the attacker does not gain any information about the user's password by mounting an exhaustive searching attack (off-line attack)
  - the attacker eliminates one password from the dictionary by interacting with either the client or the server (on-line attack)
- The theorem shows that the advantage of the adversary essentially grows with the ratio of interactions q to the size N of the dictionary:

$$Adv^{ake}(t,q,\ldots) \leq 2 \cdot q/N + 4 \cdot Succ^{dh}(t, \ldots) + Cte$$

Outline

- Introduction
- One-time Password authentication (OP)
- Authenticated Key eXchange (KeyX)

ü One-time Password authenticated Key eXchange (OPKeyX)

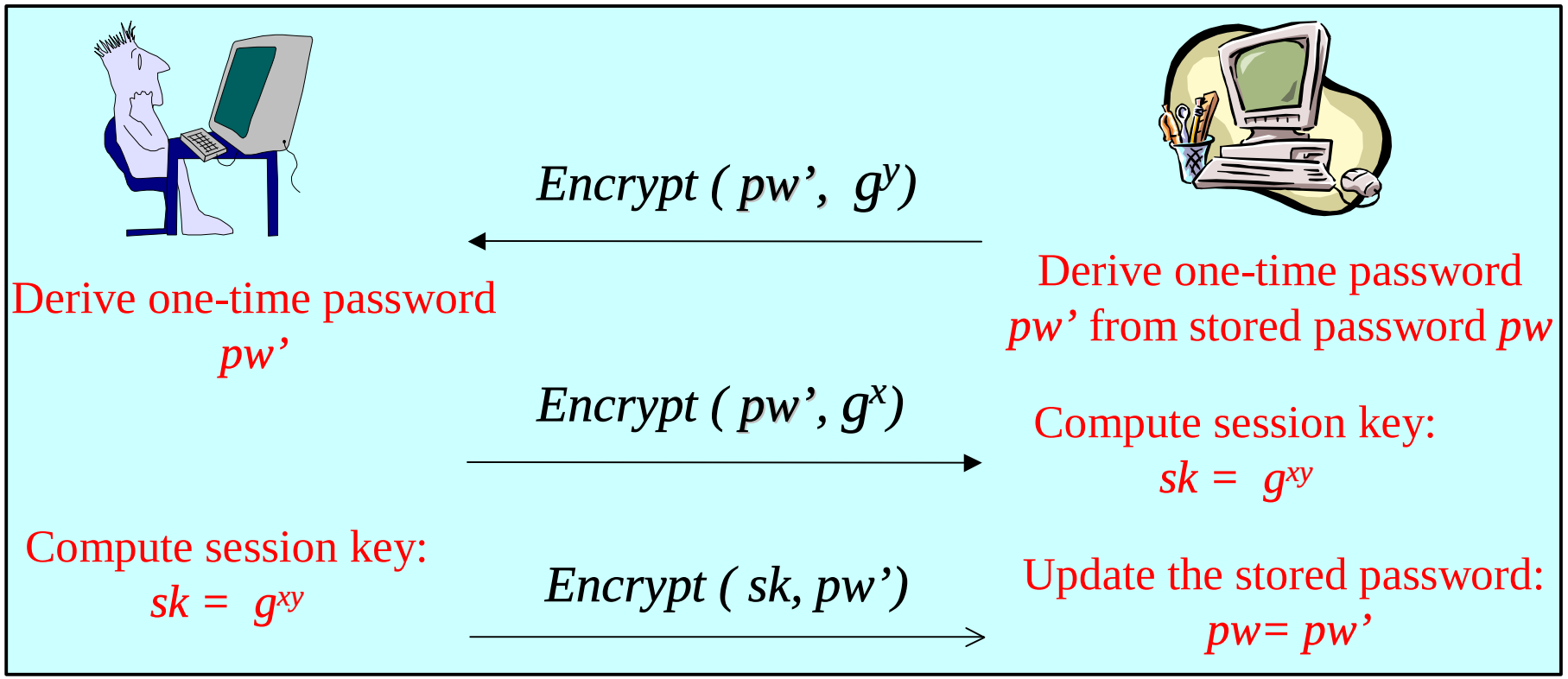
— a new technology

— security measurement

- Integration with the Globus Toolkit
- Conclusion and Future Work

One-time Password authentication and Key eXchange (OPKeyX)

- A one-time password *pw'* is derived and used to encrypt the flows of the Key eXchange algorithm
- The KeyX algorithm computes a session-key allowing the two parties to implement an encrypted and authenticated channel



O. Chevassut, GlobusWorld 2005, February 7-11.

The OPKeyX Algorithm: Security Measurement

- The algorithm relies on the difficulty of solving the DH problem
- The algorithm is secure against off-line dictionary attacks:
  - the attacker does not gain any information about the user's password by mounting an exhaustive searching attack
- The algorithm is secure against replaying of a captured user's password assuming the *one-wayness* of the password-derivation function
- The algorithm provides *mutual authentication*:
  - the two parties prove each other's identity by proving that they know the session key
- Security theorem:

$$Adv^{ake}(t,q,\ldots) \leq 2 \cdot q/N + 4 \cdot Succ^{dh}(t, \ldots) + Cte$$

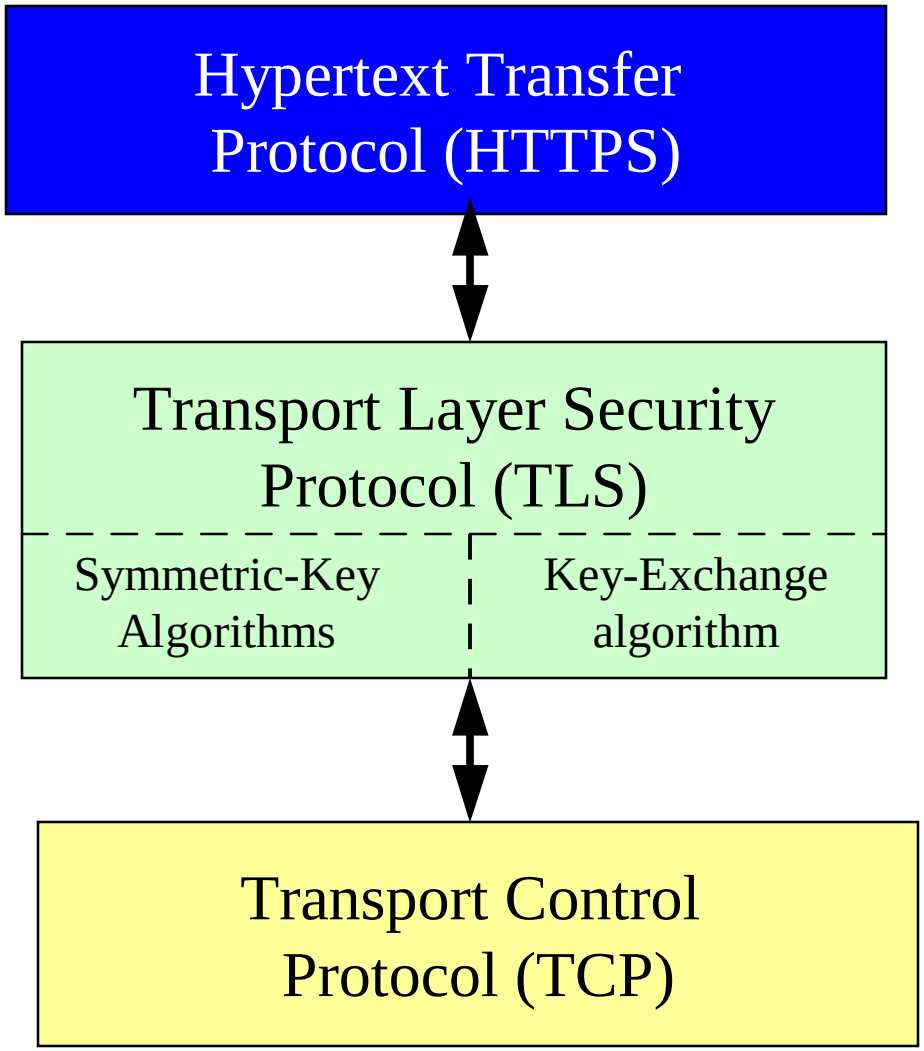
Outline

- Introduction
- One-time Password authentication (OP)
- Authenticated Key eXchange (KeyX)
- One-time Password authenticated Key eXchange (OPKeyX)

ü Integration with the Globus Toolkit
  - — using OPKeyX in the Grid Security Architectreure (GSI)
  - — using OPKeyX in the Web Services Resource Framework (WSRF)

- Conclusion and Future Work

Transport Layer Security : Architecture



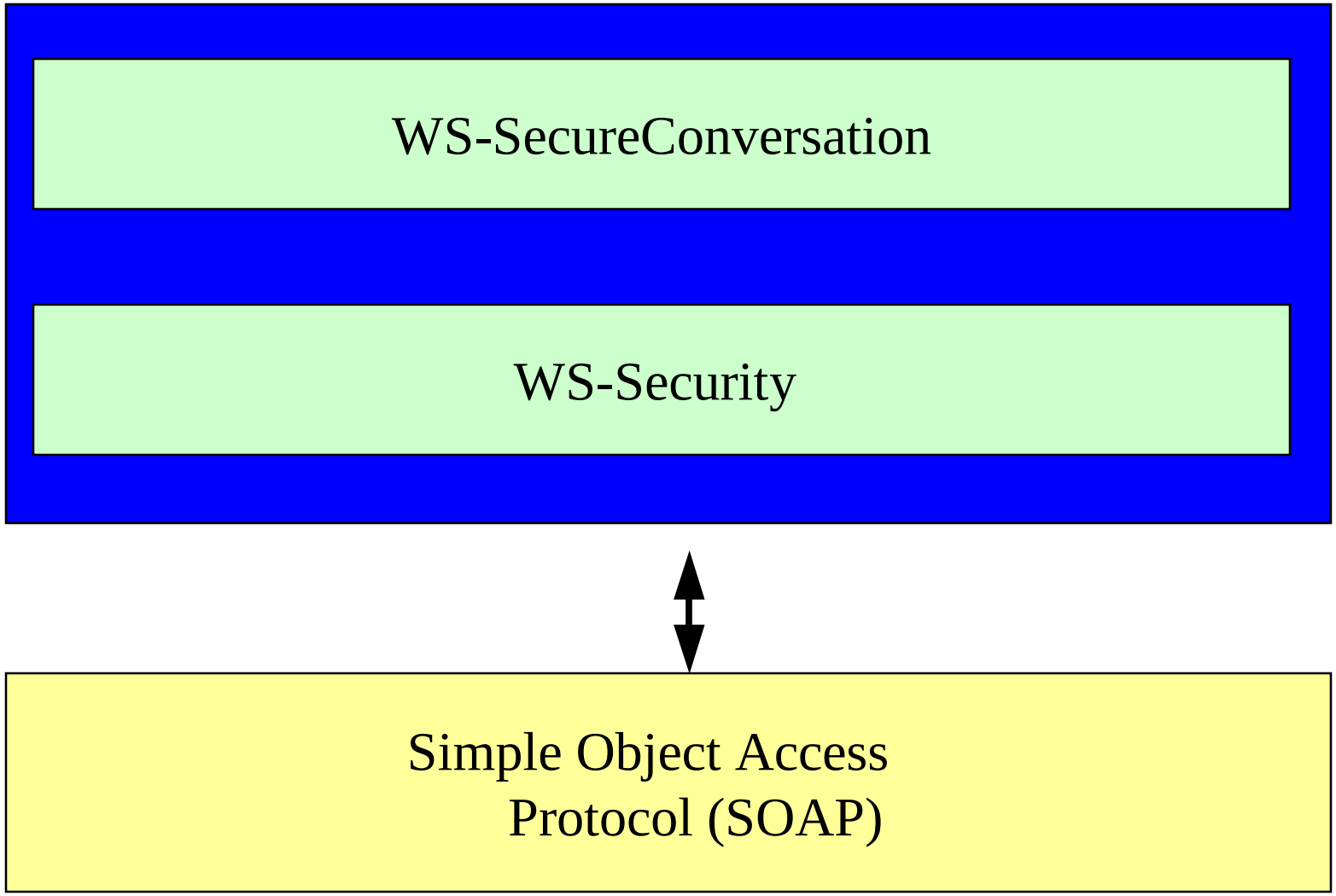
Using OPKeyX at the Transport Level

- The TCP protocol provides the *reliable communication* channel between the client and the server

- The TLS protocol provides the *secure communication channel* between the client and the server
  - confidentiality, authenticity, and integrity
  - authorization and access control
  - security services optional

- *A OPKeyX cipher suite for the Grid Security Architecture (GSI)*
  - OPKeyX is used as the key-exchange algorithm in TLS
  - Rijndael and HMAC are used for encryption and authentication in TLS

Application Layer Security : Architecture



Using OPKeyX at the Application Level

- The SOAP protocol provides the reliable message-level communication channel between the requestor and the Web Service provider

- The WS-SecureConversation specification is a security message-level protocol (similar to TLS)
  - use WS-Security to achieve confidentiality, authenticity, integrity
  - use WS-Policy and WS-Trust specifications to achieve authorization and access control

- *A OPKeyX cipher suite for the WSRF-compliant GT s GSI*
  - OPKeyX is used as the key-exchange algorithm in WS-SecureConversation
  - Rijndael and HMAC are used for encryption and authentication in WS-Security

Conclusion and Future Work

- Accomplishments
  - "One-time Verifier-based Encrypted key Exchange (OPKeyX)", M. Abdalla, O. Chevassut, and D. Pointcheval, International Workshop on Theory and Practice in Public Key Cryptography (PKC), Feb 05.
  - "Secure Password-based Authenticated Key Exchange (OPKeyX) for Web Services" , L. Fang, S. Meder, o. Chevassut, and F. Siebenslits, ACM Workshop on Secure Web Services, Nov 2004.

- Work in progress
  - OPKeyX as a new cipher suite in the OpenSSL software
  - using OPKeyX for MyProxy and GridLogon authentication
  - using OPKeyX within Esnet's Authentication and Authorization Fabric for Office Science