Periodical Payments Using X.509 Restricted Proxy Certificates

Lawrie Brown

Grigori Goldman

January 2010

University of New South Wales @

Australian Defence Force Academy

Who Am I?

- senior lecturer at UNSW@ADFA
- professional interests include:
  - cryptography, communications and computer systems security, and safe mobile code execution
- teaches courses in:
  - computer security, cryptography, data communications and java programming
- co-authored text on Computer Security

Research Goal

"To develop a payment framework based on the *direct debit* payment model using currently available, standards compliant and industry supported technologies."

Electronic Payment Schemes (History)

- 1980s – David Chaum, blind digital signatures, anonymous electronic cash, etc
- 1990s – Secure Electronic Transaction (SET)
- And Now
  - Visa Three Domain (3-D) Secure
  - MasterCard Secure Payment Application (SPA)
  - Single European Payments Area (SEPA)

What is missing?

- Follows paper-based model
- Insecure when used over the Internet
  - Not using cryptographic authentication
- No automated payment cancellation features
- Payment contracts are not enforceable during payment processing

X.509 Proxy Certificates

What

- Allow delegation of a user's credential to an intermediary service for execution of a task

Where

- Globus Open Grid Services Architecture, Grid Security Infrastructure (GSI)

How

- Private/Public key pair created by the recipient
- Certificate is signed by an end-entity not a CA

Periodical Payment Framework Overview

1. Periodical Payment Policy Language

   (Policies are added to X.509 Proxy Certificates)

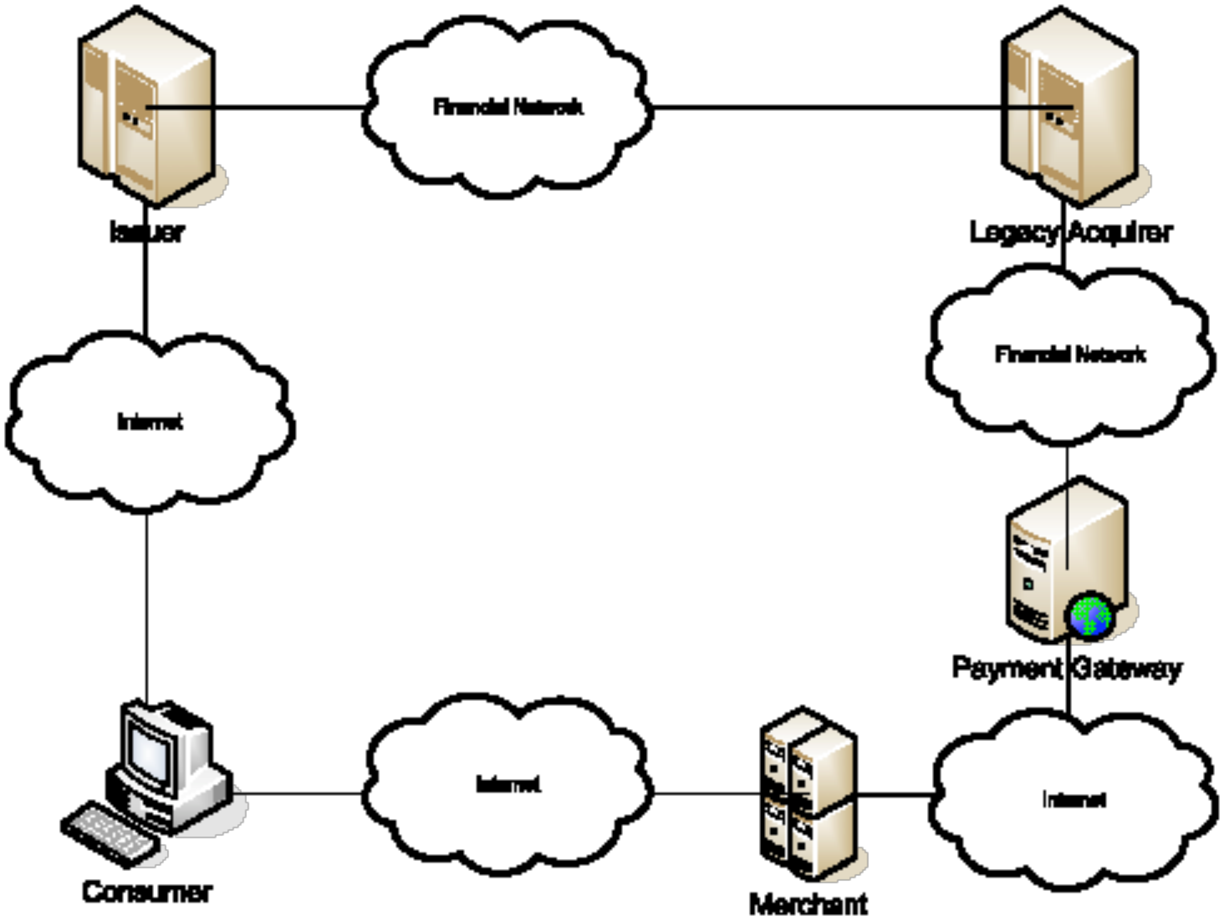
2. Client-side and Merchant libraries for:

   (Credential delegation and policy validation)

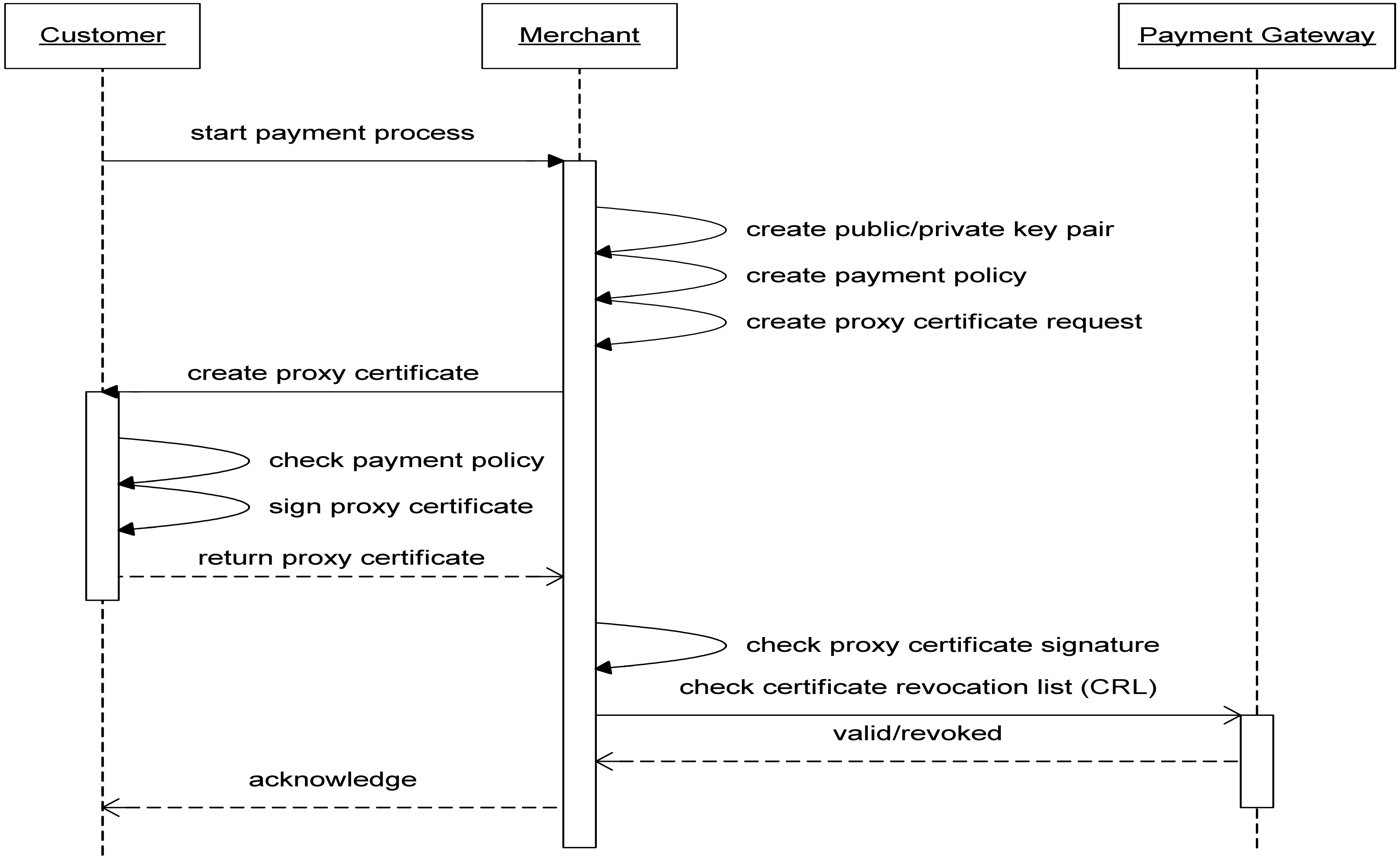
3. Payment Gateway Web Services interface

   (Abstracting the existing payment infrastructure)

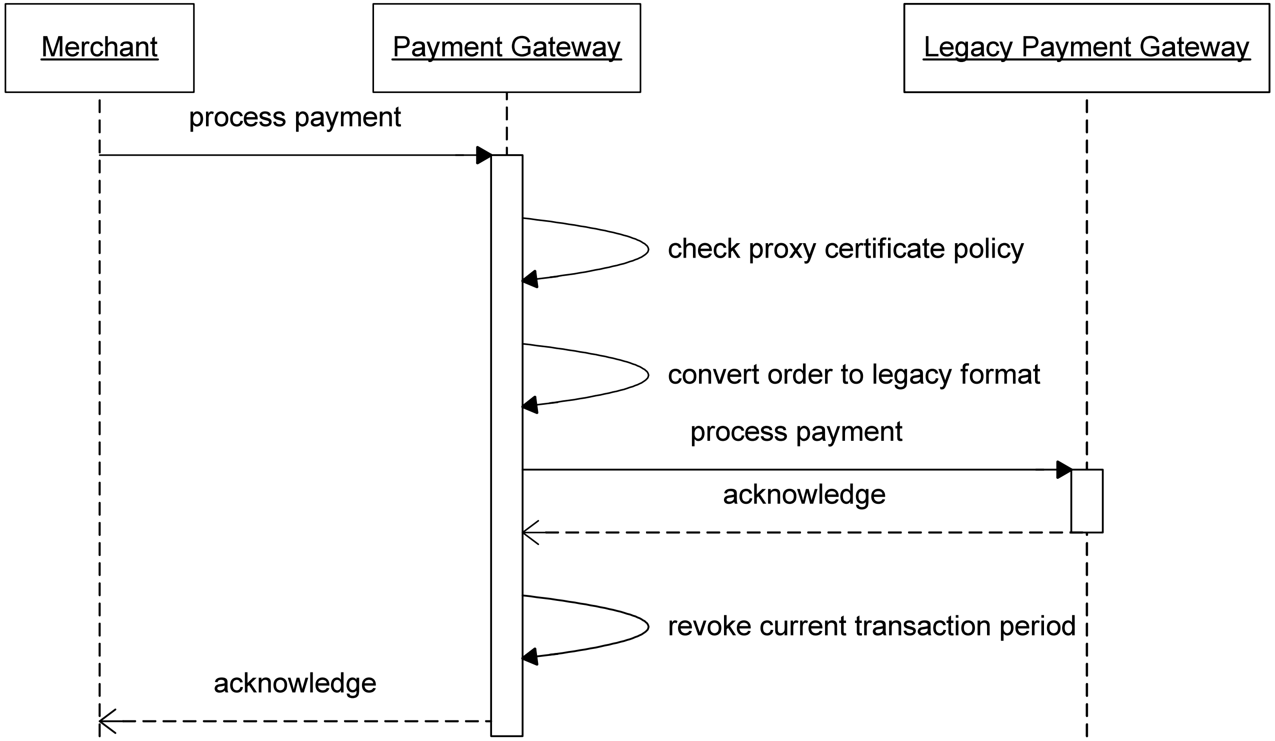
Periodical Payment Framework Architecture



Certificate Delegation Process



Payment Process



Periodical Payment Certificate Policy Language

What is it?

- XML document representing contract between customer and merchant

How is it used?

- Proxy certificate asserts that merchant is valid customer delegate
- Policy is added to the proxy certificate
- Policy asserts that merchant can execute payment transactions on behalf of its customers

Periodical Payment Certificate Policy Language (cont)

```
<payment-policy>
      <pay currency=“aud” amount=“20” on=“* * * 1W * ? 2010” />
</payment-policy>
```

```
<payment-policy>
      <pay currency=“aud” limit=“20” on=“* * * 1W * ? 2010” />
</payment-policy>
```

```
<payment-policy>
      <pay currency=“aud” on=“* * * 1W * ? 2010” />
</payment-policy>
```

Periodical Payment Certificate Policy Language (cont)

Normal Case:

- Only one assertion of each type per policy

Special case:

- Declare an odd-assertion to handle a specific scenario, eg. discounted first/last payment, etc.

Periodical Payment Certificate Policy Language (cont)

Cancelling a periodical payment example:

```
<payment-policy>
  <pay currency=“aud” amount=“20” on=“* * * 1W * ? 2010” />
   <cancellation-policy>
     <pay currency=“aud” amount=“100” on=“* * * * 1-6   ? 2010” />
     <pay currency=“aud” amount=“50”   on=“* * * * 7-12 ? 2010” />
   </cancellation-policy>
</payment-policy>
```

Double Charging Problem

Question:

- How does the payment gateway detect a request replay attack (i.e. merchant is double charging the customer)?

Answer

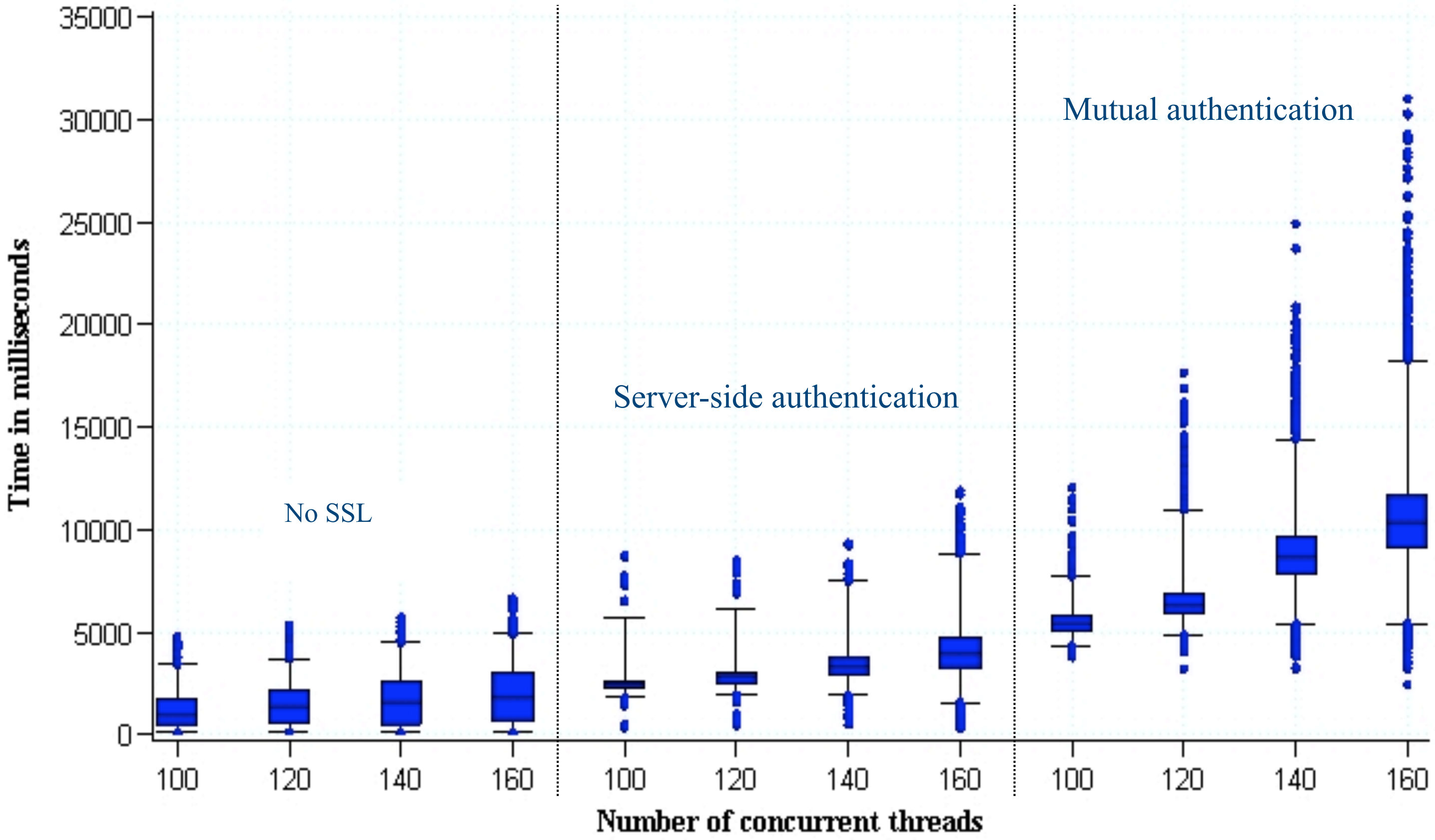
- A transaction revocation list (TRL)

  Based on X.509 Certificate Revocation List (CRL)

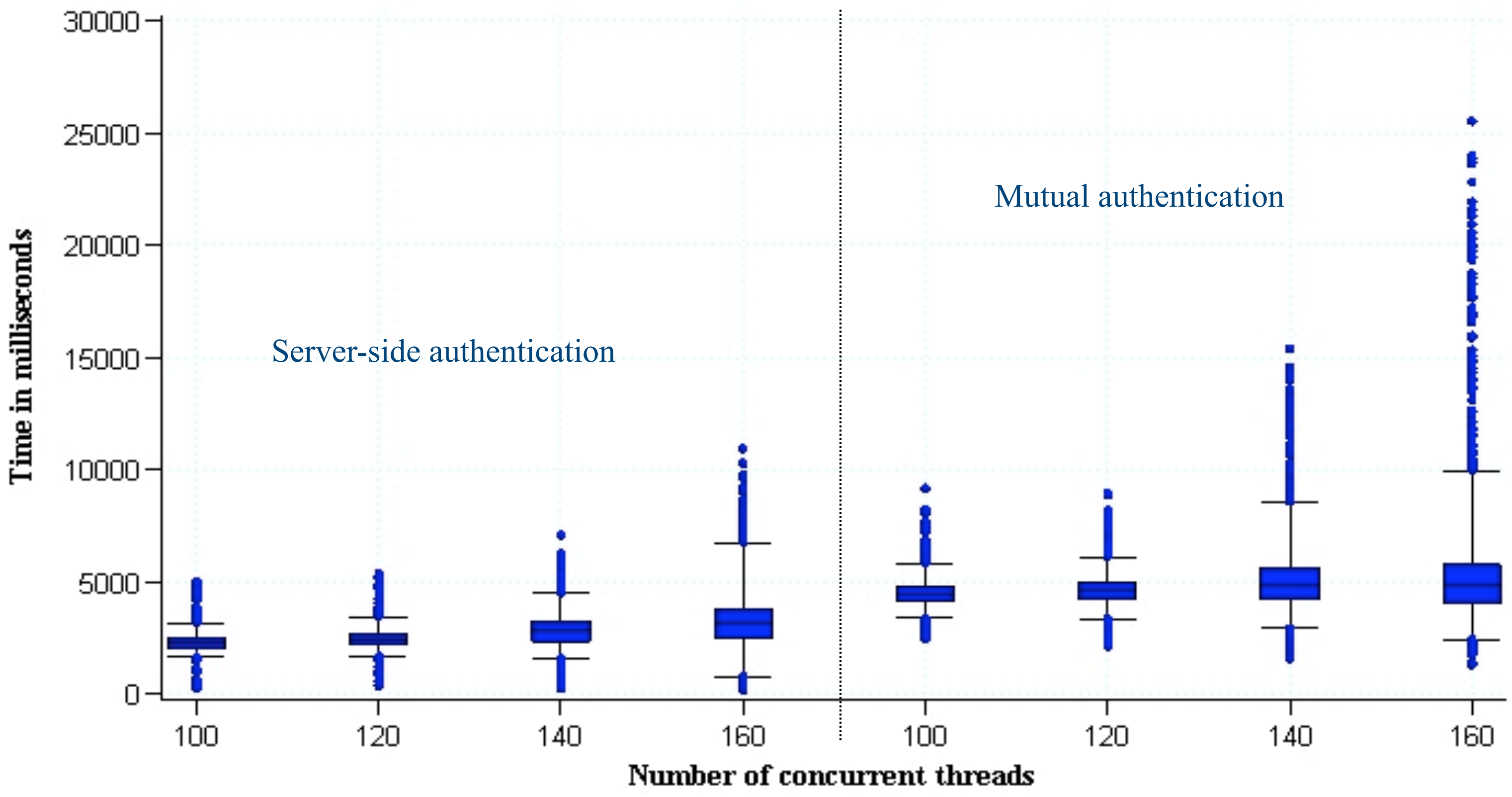
revoke = “* * * * MAR ? 2009”

Performance Analysis

(Total Request Processing Time)

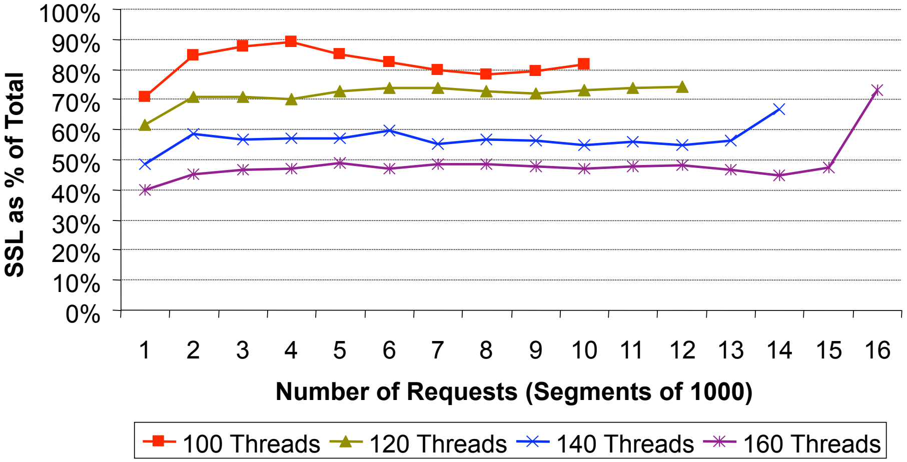


Performance Analysis
(SSL Handshake Processing Time)



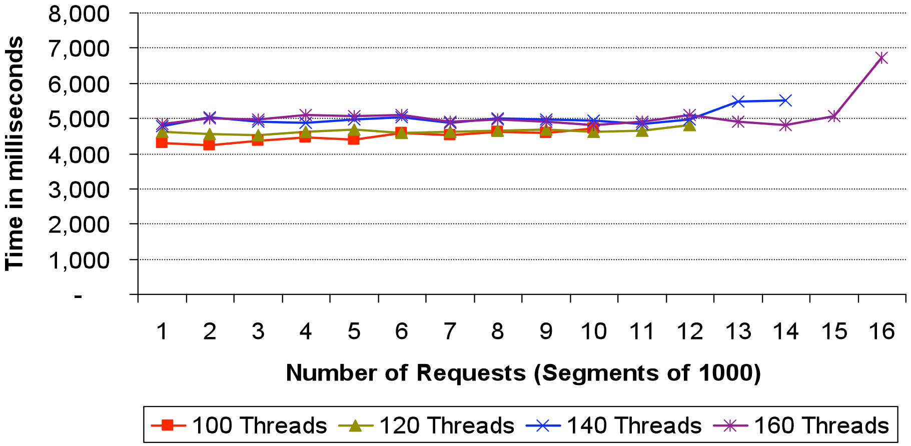
Performance Analysis

(SSL Impact on Performance)



SSL handshake percentage of total time

Average SSL handshake processing time



Future Work

Performance Improvements

- Replacing SOAP based Web Services with a light-weight alternative, e.g. using Representational State Transfer (REST) architectural style
- Integrating native SSL libraries instead of using the default Sun JSSE implementation

Client-side Enhancements

- Integrating USB token support into the existing Firefox extension
- Investigating the use of Subscriber Identity Module (SIM) cards as cryptographic tokens

Conclusion

- Periodical payments are different to traditional e-commerce payments:
  - No customer involvement during each transaction
  - Allow merchants access to customer accounts
- No alternatives currently exist even though this payment method is popular
- Restricted proxy certificates provide a strong cryptographic foundation for this framework making it a viable commercial alternative

Any Questions?

Reference:

Grigori Goldman and Lawrie Brown, “Analysis of the Periodical Payment Framework using Restricted Proxy Certificates”, ACSC2010, Brisbane, Australia; Conferences in Research and Practice in Information Technology (CRPIT), Vol. 102, Jan 2010, B. Mans and M. Reynolds, eds.