

SSL Performance:

a dedicated coprocessor opportunity

RSA Data Security Conference
January 30, 1997

Shawn Abbott,
Chief Scientist
Rainbow Technologies

sabbott@tcel.com
<http://isg.rnbo.com>



Applicability of SSL

- Broad Services
- Widely deployed
- Interoperable
- Model for other protocols
- PCT, SET, S-HTTP, ISAKMP, S/TCP, S/MIME, S/WAN, IPSEC

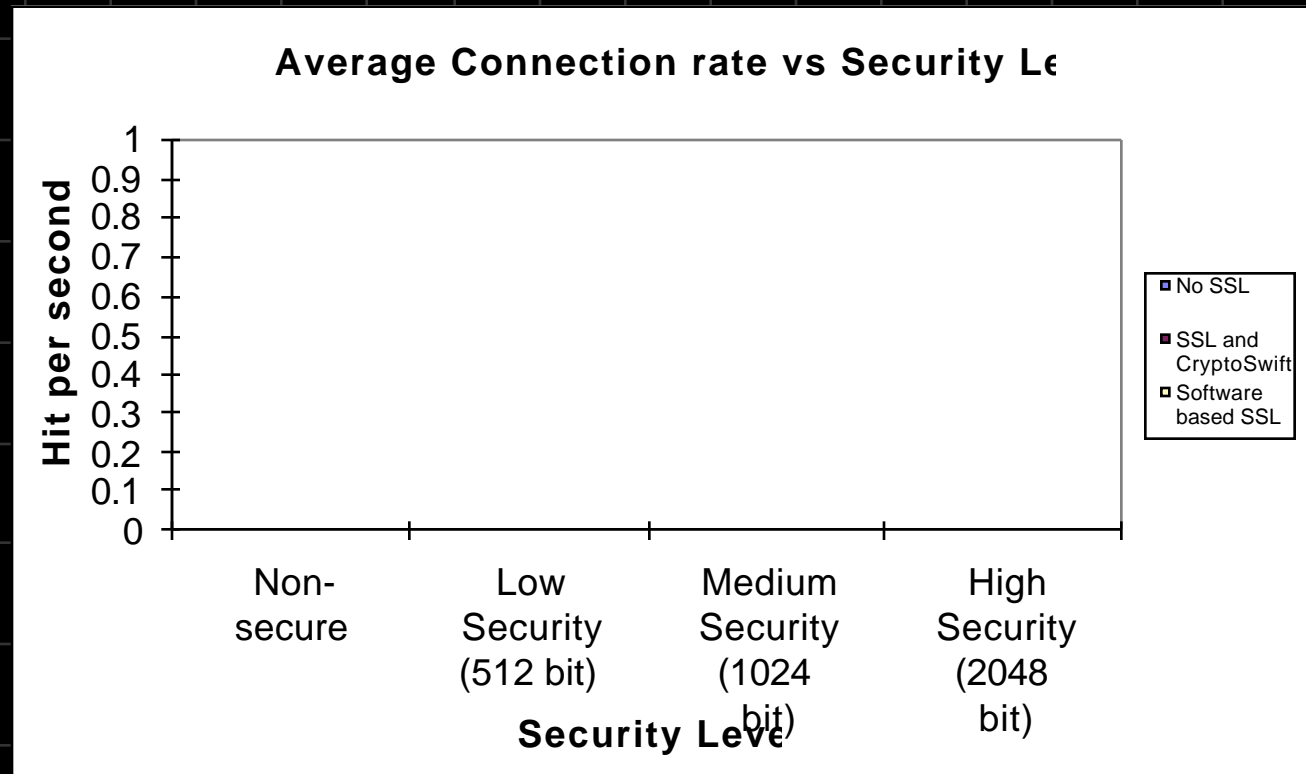


Transaction Rates

- connection v. transaction v. hit
- performance: speed or capacity?
- capacity requirements
 - 1 tps... 10tps... 100tps... 1000tps

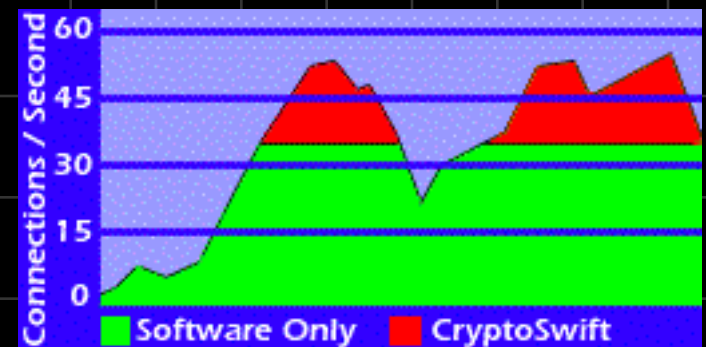


SLL: cpu v. dedicated processor



How to measure performance

- hps, cps, tps
- WebStone, WebSpec
- Where is the bottleneck?
 - Intranet v. Internet



Protocol Analysis (SSL)

- [protocol diagram]
- observations:
 - designed for maximum efficiency
 - not a convenient basis for key recovery
 - one full RSA private operation per connection on server side
- Effect of client side authentication
- Fortezza suite

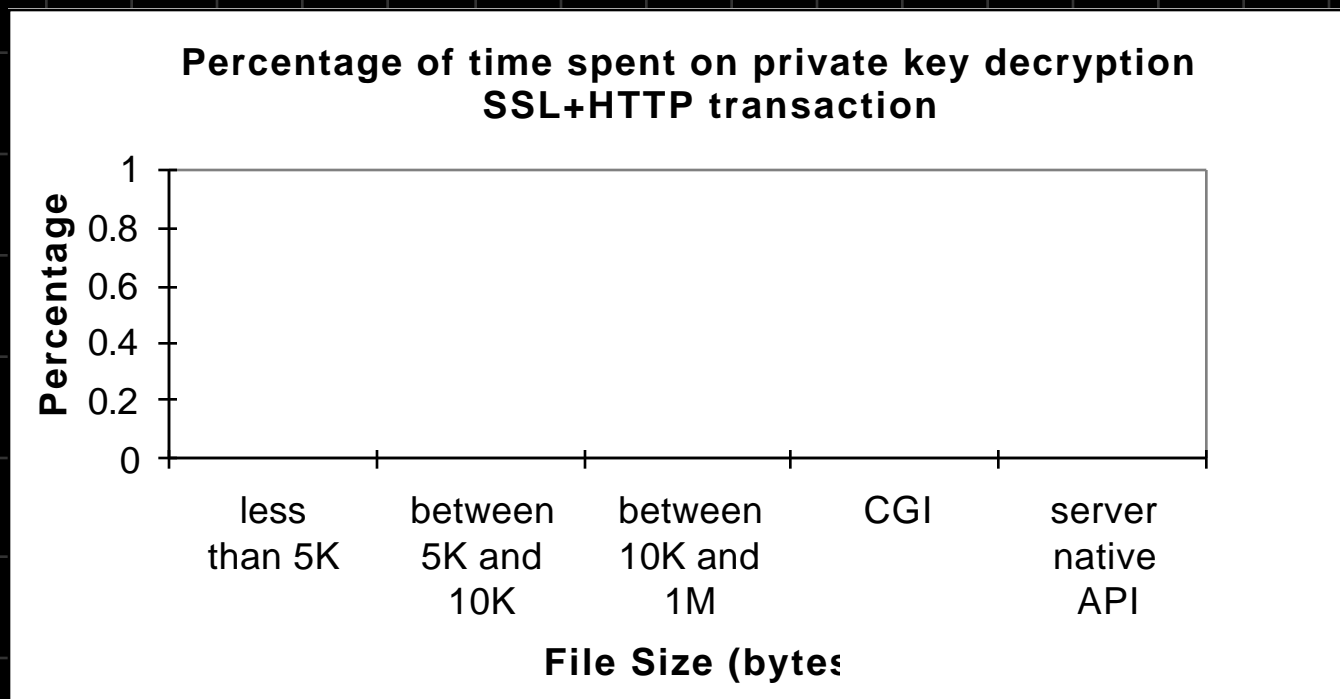


Discussion of variables

- Traffic pattern
- Key size
- Session ID caching
- Content and CGI use
- OS Threading ability
- Platform and server software

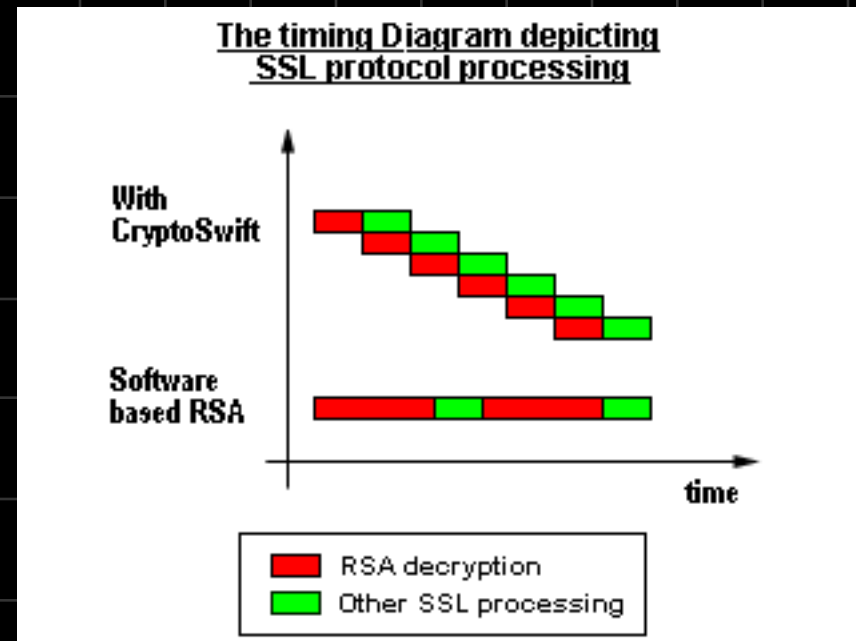


Variable #1: processor load



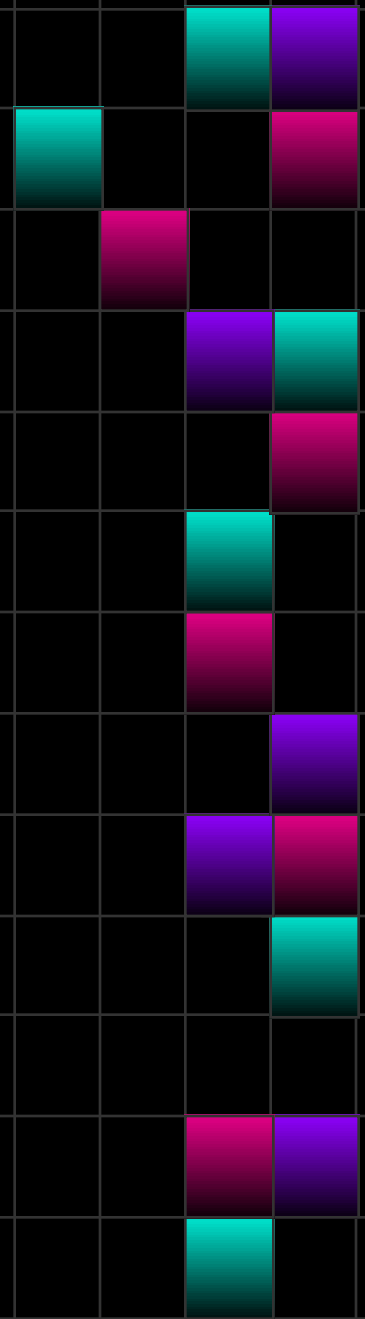
Integration

- Form factor
- CAPI selection
 - swiftapi
 - cryptoki
 - CryptoAPI
 - CDSA
- Threads



The math

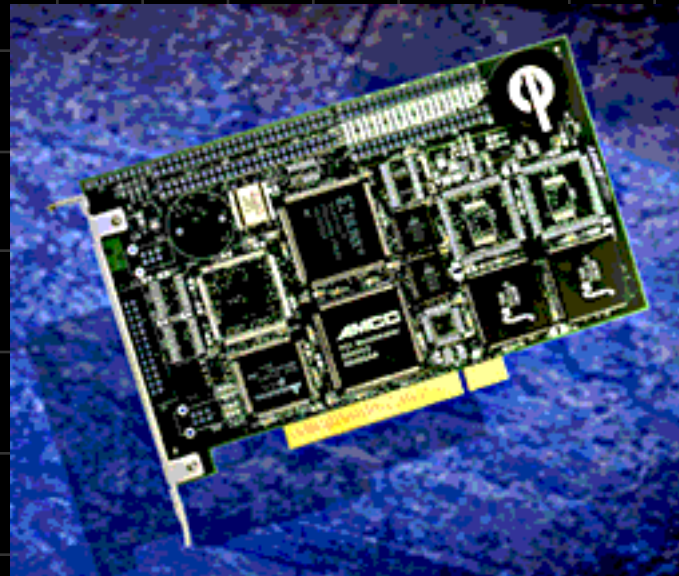
- Fundamental to all PK algorithms
 - DH, RSA, DSA...
- Modular exponentiation
- Mykotronx math (patent pending)
- Multiplier designs and key size



CryptoSwift

- Development units already seeded
- Beta sites being established today
- Quantity production in under 90 days

crypto**SWIFT**



Conclusions

- SSL and other public key protocols will be “on by default”
- 1024 bit math cripples 32 bit processors
- cryptographic coprocessors will be as commonplace as floating point, video and I/O coprocessors

Questions

Rainbow's CryptoSwift accelerators: Dedicated to Performance

Shawn Abbott,
Chief Scientist
Rainbow Technologies

sabbott@tcel.com
<http://isg.rnbo.com>

