Comparing the Performance of Abstract Syntax Notation One (ASN.1) vs. eXtensible Markup Language (XML)

Presented By: Prof. D.W.Chadwick

Other Author: D.Mundy

Thanks to:

EPSRC Engineering and Physical Sciences Research Council

Entrust Securing the Internet

ISSRG Information Systems Security Research Group

Contact: d.w.chadwick@salford.ac.uk

http://sec.isi.salford.ac.uk

Agenda

- Motivation
- Introduction to
  - ASN.1
  - XML
- Testing Technology Used
- Performance Measurements
- Results
- Conclusions

Motivation

- We have built an Electronic Transfer of Prescriptions system, in which prescriptions are transferred as digitally signed X.509 attribute certificates
- The system must be fast, especially for pharmacists who can currently process paper prescriptions in 30 seconds
- The UK Dept of Health has specified electronic prescriptions in XML format, so we wanted to know the implications of this from a performance perspective

Introduction to Abstract Syntax Notation One (ASN.1) (1)

- Designed to describe the structure and syntax of transmitted information content
- Provides for the definition of the abstract syntax of a data element (or data type)
- The language is based firmly on the principles of type and value, with a type being a (non-empty) set of values
- e.g.**AllowedAccess ::= BOOLEAN**
- The type defines what values can subsequently be sent at runtime, and the value is what is actually conveyed across the medium at runtime according to specified encoding rules

Abstract Syntax Notation One (ASN.1) (2)

- Standard encoding rules
  - Basic Encoding Rules (BER)
  - Distinguished Encoding Rules (DER)
  - Packed Encoding Rules (PER)
  - XML Encoding Rules (XER)
- During the transmission the ASN.1 data stream is never in a form readable by human operators
- Only when it has been transformed into some local data display format, prior to encoding or after decoding, can it be easily read by humans.

Introduction to eXtensible Markup Language (XML) (1)

- Set of rules that allows data values to be encoded in text format
- Subset of the Standard Generalized Markup Language (SGML), but is also infinitely extensible
- Contains the information for transmission and consists of markup and character data
- Constraints can be imposed on the XML document structure with the provision of Document Type Definitions (DTD's) or XML Schemas
- Major backing from Sun, IBM, Microsoft etc.

Introduction to eXtensible Markup Language (XML) (2)

- E.g. **<!ELEMENT allowedAccess (#PCDATA)>**

  <allowedAccess>TRUE</allowedAccess>
- XML is very verbose, and consequently creates large data streams
- XML is transferred in textual format with no binary encodings or compression
- the recipient has to examine every byte received in order to determine the end of a data value
- DTD's / schemas map to the abstract syntax type definitions within ASN.1

Testing Technology Used

- Java - IBM JDK (Suganuma et al, "Overview of the IBM Java Just-in-Time Compiler", See http://www.research.ibm.com/journal/sj/391/suganuma.html)
- Hardware - CPU: P3 650MHz, 256Mbytes memory
- Operating System - RedHat Linux
- System measurement code written in C using libgtop. Measures
  - User mode CPU utilisation
  - System mode CPU utilisation
  - Total number of pages in memory
  - Number of minor and major page faults

Technology Used - Attribute Certificates

- The DOH has issued a number of DTD's describing the expected structure of all electronic prescriptions
- No definition for an attribute certificate in XML and there is equally no definition of the DOH prescription structures in ASN.1
- We generated these structures using our knowledge of ASN.1 and XML and taking into account the existing XML definitions for public key certificates and signatures
- Used DER encoding within our application to generate the encoded ASN.1 certificates

Testing Application

- System Operation with no security
  - attribute certificate is created by the client and then transmitted to the server using standard sockets
  - The recipient parses it into a data structure for easy access to any of its data elements
- Secure System Operation
  - attribute certificate is created by the client, digitally signed, and then transmitted to the server using standard sockets
  - The recipient firstly verifies the signature and then parses the certificate into a data structure for easy access to any of its data elements
- Used 3 complexities of attribute certificate
  - Very Complex – auditCertificate (defined in a previous research project)
  - Semi-Complex – etpPrescribe certificate (defined by Dept of Health)
  - Simple – boolean attribute value

Performance Measurements

- Performance measurements made on a single machine
- Following measurements taken:
  - CPU ticks for attribute certificate construction and verification
  - Process memory use for structure construction
  - Number of page faults (minor and major) for structure construction and verification
  - The size in bytes of the completed certificates
  - The size in bytes of the zipped certificates
  - Elapsed time for construction and verification
- Tests repeated 100 times to allow for statistical variations in the results

Size Comparison (bytes)

	ASN.1 Unsigned	DOM XML Unsigned	Zipped XML Unsigned	ASN.1 Signed	DOM XML Signed	Zipped XML Signed
Simple Attribute	235	2880	710	384	3704	913
Semi-Complex	944	6210	1532	1060	7043	1737
Complex Attribute	1351	18297	4514	1483	19184	4733

Conclusion: XML creates data blocks approximately an order of magnitude greater than BER encoded ASN.1

Theoretical Transmission Times over a 64kbps / 256 kbps link (ms)

	ASN.1 Unsigned	DOM XML Unsigned	ASN.1 Signed	DOM XML Signed
Simple Attribute	29/7	352 / 88	47 / 12	452 / 113
Semi-Complex	115 / 29	758 / 190	129 / 32	860 / 215
Complex Attribute	165 / 41	2234 / 558	181 / 45	2342 / 585

Conclusion. Broadband is needed for pharmacist's shops

Sender Encoding Times of Unsigned Data (ms)

	ASN.1	DOM XML	Comparison XML/ASN.1
Simple Attribute	6.83	2.66	-60%
Semi-Complex	8.98	4.46	-50%
Complex Attribute	10.54	14.88	40%

Conclusion. ASN.1 has a larger initialisation time, but is faster encoding each data item

Recipient Decoding Times of Unsigned Data (ms)

	ASN.1	DOM XML	Comparison XML/ASN.1
Simple Attribute	1.63	4.46	170%
Semi-Complex	2.49	5.5	120%
Complex Attribute	3.52	9.07	157%

Conclusion. XML takes much longer to decode each value due to having to parse each character

Sender Signing and Encoding Times (ms)

	ASN.1	DOM XML	Comparison XML/ASN.1
Simple Attribute	94.82	113.36	20%
Semi-Complex	100.28	125.85	26%
Complex Attribute	102.79	184.12	80%

Conclusion. XML signing takes much longer per data item

Recipient Signature Validation and Decoding Times (ms)

	ASN.1	DOM XML	Comparison XML/ASN.1
Simple Attribute	5.92	26.62	350%
Semi-Complex	6.01	38.96	550%
Complex Attribute	6.16	67.22	1000%

Conclusion. Double whammy on XML.
Slow validation and slow decoding

Other Results

- In secure operations ASN.1 requires lower CPU user time than XML for both sender and recipient for all attribute complexities
- The system time required by XML in almost every case was more than the system time required for ASN.1
- Without the overhead of security XML required lower amounts of dynamic memory allocation than ASN.1
  - ASN.1 requires a large number of class instantiations and ultimately destructions, whereas the XML application uses fewer classes and therefore has lower initial memory requirements

Conclusions

- In environments where simple XML messages are required without secure operations then XML performs adequately
- For critical real time systems where digital signing of complex data structures is required, and where performance is a key success factor, such as in an electronic prescribing system, signed complex XML messages can be up to a 1000% slower to decode than an equivalent ASN.1 message
- We believe that in a real time system dealing in multiple transactions a second and requiring strong authentication through digital signatures, XML formatting is not a good protocol to choose

Questions

ISSRG Information Systems Security Research Group

Contact: d.w.chadwick@salford.ac.uk

http://sec.isi.salford.ac.uk