MTAT.07.017
Applied Cryptography

Rakenduslik krüptograafia
Прикладная криптография

Juri Hudolejev
University of Tartu
Spring 2011

Topics for This Week

ASN.1: Abstract Syntax Notation One

ASN.1 encodings (BER, DER, etc.)

BouncyCastle:

- **`org.bouncycastle.asn1.*`**
- **`org.bouncycastle.asn1.util.ASN1Dump`**

Abstract Syntax Notation One

Notation to describe abstract types and values

Describes information, not representation

ASN.1 Example

```
-- Describes today's date
Today ::= Sequence {
    year         Number, -- 2011
    month        String, -- 'March'
    dayOfMonth   Number, -- 11
    dayOfYear    Number, -- 70
    dayOfWeek    String  -- 'Friday'
}
```

Value Assignment

`variable = expression`

(BASIC, C/C++, Java, Perl, PHP, Python, …)

`variable := expression`

(Ada, ALGOL, Eiffel, Pascal, …)

`variable ::= expression`

(ASN.1)

ASN.1 Primitive Types

```
BOOLEAN          (universal tag: 1)
INTEGER          (universal tag: 2)
OCTET STRING     (universal tag: 4)
NULL             (universal tag: 5)
SEQUENCE         (universal tag: 16)
```

… and others:

http://www.obj-sys.com/asn1tutorial/node124.html

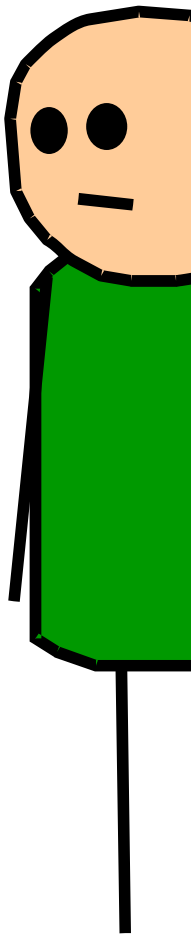
ASN.1 Example

```
Protocol DEFINITIONS ::= BEGIN
    Question ::= SEQUENCE {
        id INTEGER,
        questionText UTF8String
    }
    Answer ::= SEQUENCE {
        id INTEGER,
        questionId INTEGER,
        answerText UTF8String
    }
END
```

ASN.1 Example


```
myQuestion Question ::= {
   id 42,
   questionText "Chuck Norris"
}
```

```
myAnswer Answer ::= {
   id 100500,
   questionId 42,
   answerText "1 page found"
}
```



ASN.1 Encoding Rules

Basic Encoding Rules (BER)

Canonical Encoding Rules (CER)

Distinguished Encoding Rules (DER)

Packed Encoding Rules (PER)

XML Encoding Rules (XER)

Generic String Encoding Rules (GSER)

XML Encoding Rules

```
-- ASN.1 type definition
Question ::= SEQUENCE {
    id INTEGER,
    questionText UTF8String
}

<!-- XML-encoded object -->
<Question>
  <id>42</id>
  <questionText>Chuck Norris</questionText>
</Question>
```

Type-Length-Value (TLV)

```
msg UTF8String ::= “Friday”
```

Type: UTF8String

Length: 6 characters

Value: “Friday”

```
[UTF8String][6][F][r][i][d][a][y]
0x0c 0x06 0x46 0x72 0x69 0x64 0x61 0x79
```

ASN.1 Primitive Types

```
BOOLEAN          (universal tag: 0x01)
INTEGER          (universal tag: 0x02)
OCTET STRING     (universal tag: 0x04)
NULL             (universal tag: 0x05)
UTF8String       (universal tag: 0x0c)
SEQUENCE         (universal tag: 0x10)
UTCTime          (universal tag: 0x17)
```

Next Lecture

More ASN.1 types:

- SEQUENCE, SET, *Time, etc.
- Tagged objects
- Complex types

Exercises on BER/DER

Questions?

Further Reading

ASN.1 basics and useful links:

http://en.wikipedia.org/wiki/ASN.1

Tutorial on ASN.1, BER and DER (nice to start from):

http://luca.ntop.org/Teaching/Appunti/asn1.html

Another tutorial (more detailed):

http://www.obj-sys.com/asn1tutorial/asn1only.html

ASN.1 Tools

`dumpasn1` – available in most Linux distros

http://www.cs.auckland.ac.nz/~pgut001/#standards

Windows users: google for 'ASN.1 dump'

Write your own in Java (really simple), use

`org.bouncycastle.asn1.ASN1InputStream`

`org.bouncycastle.asn1.util.ASN1Dump`

Libs for other languages: OpenSSL, PyASN1

Home Tasks

http://courses.cs.ut.ee/2011/appcrypto/Main/Lab04

Questions?

0c 10 47 6f 6f 64 20 6c 75 63 6b 21

Tasks and additional info:

http://courses.cs.ut.ee/2011/appcrypto/Main/Lab04

Deadline: 2011-03-25 08:00 EET

Contact: Juri Hudolejev <juri@ut.ee>

Next lab session:

Friday 2011-03-18 **08:30** EET @ Liivi 2 - 205