FLEX

Flow-based event exchange format

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

UNIVERSITEIT TWENTE.

CASED

da/sec
BIOMETRICS AND INTERNET-SECURITY
RESEARCH GROUP
http://www.dasec.h-da.de/

Agenda

Problem & Goal

Scenario

Exchange formats

FLEX

Discussion

Who am I ?

- Doctoral Researcher

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

UNIVERSITEIT TWENTE.

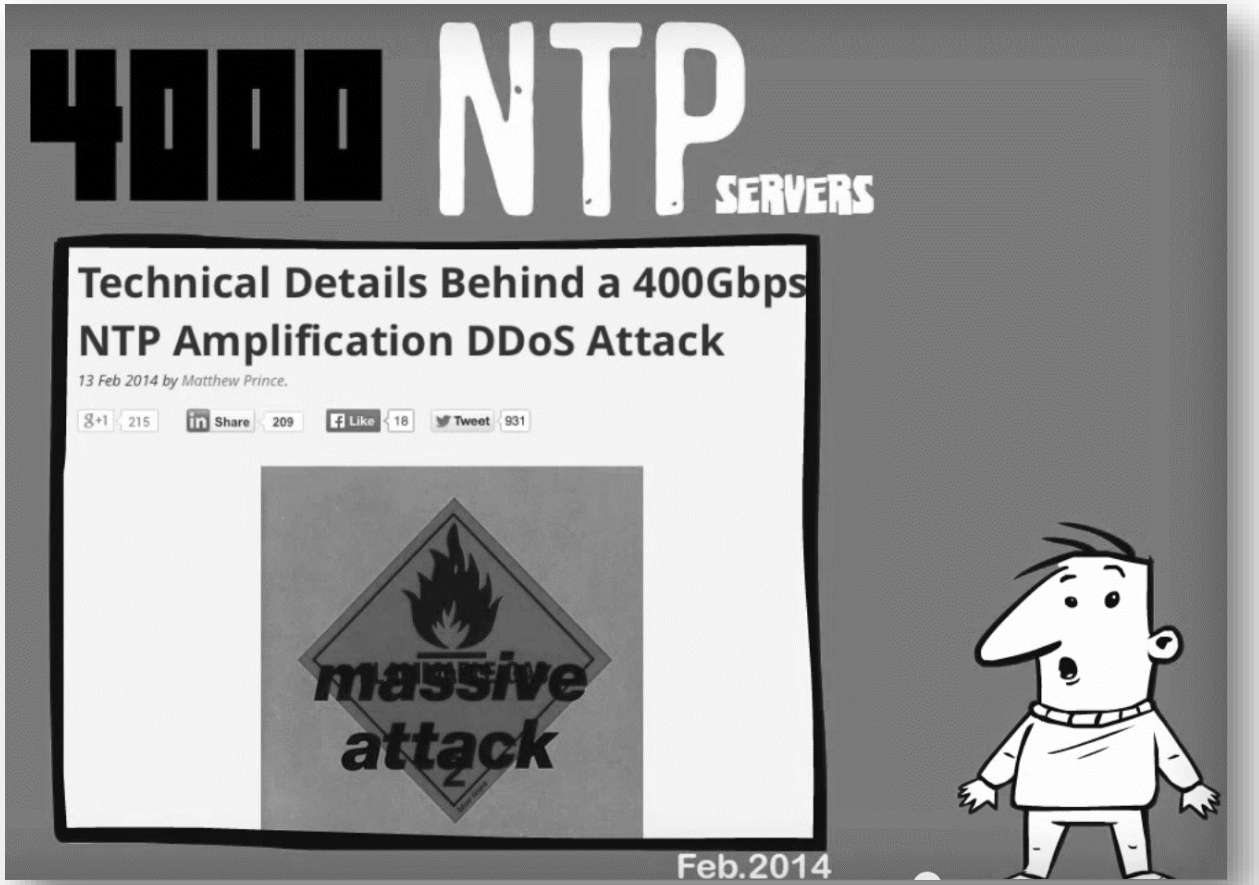
CASED

da/sec
BIOMETRICS AND INTERNET-SECURITY
RESEARCH GROUP
http://www.dasec.h-da.de/

- Mitigation and Response

Problem & Goal

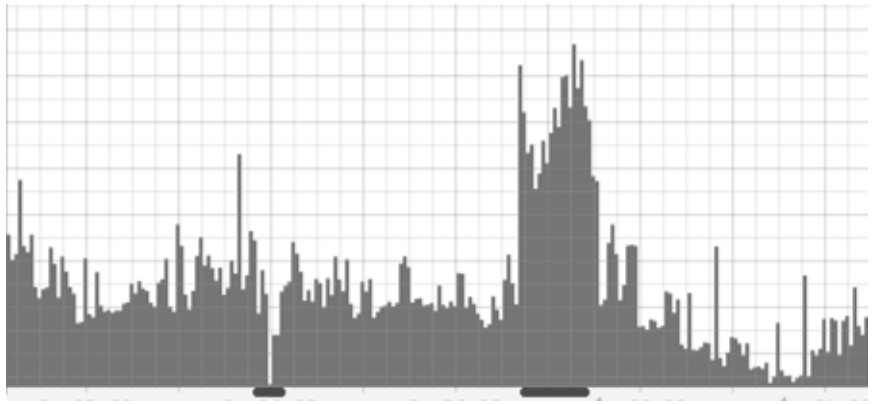
Problem

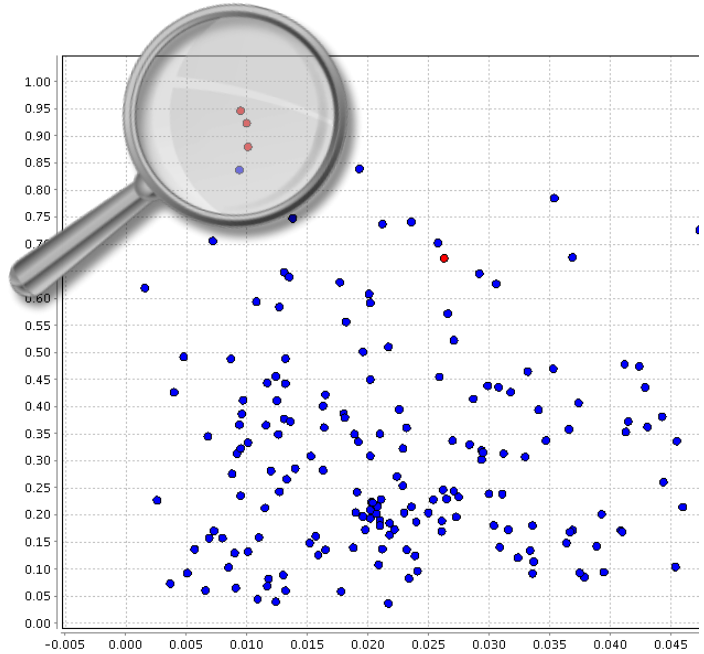


Source: https://www.youtube.com/watch?v=kBBIqKeVdDo

Problem

network-traffic



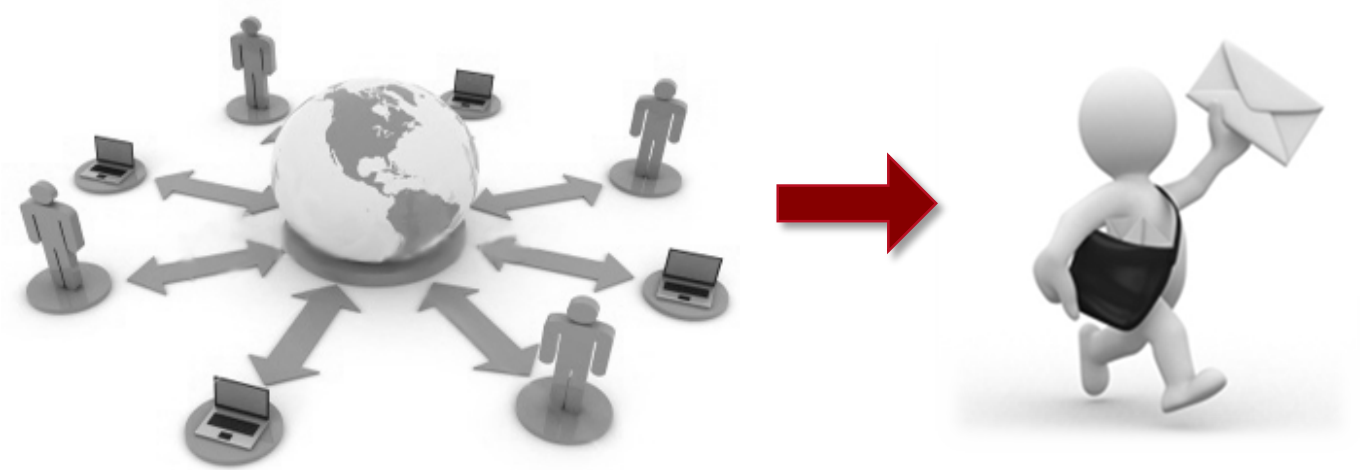


Problem

mitigation and reaction

Goal

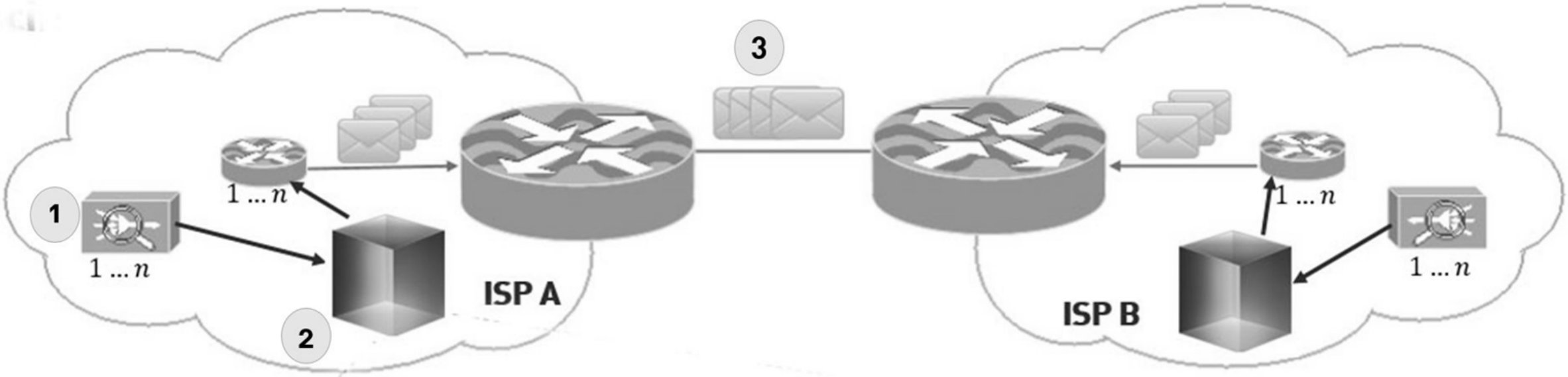
collaboration



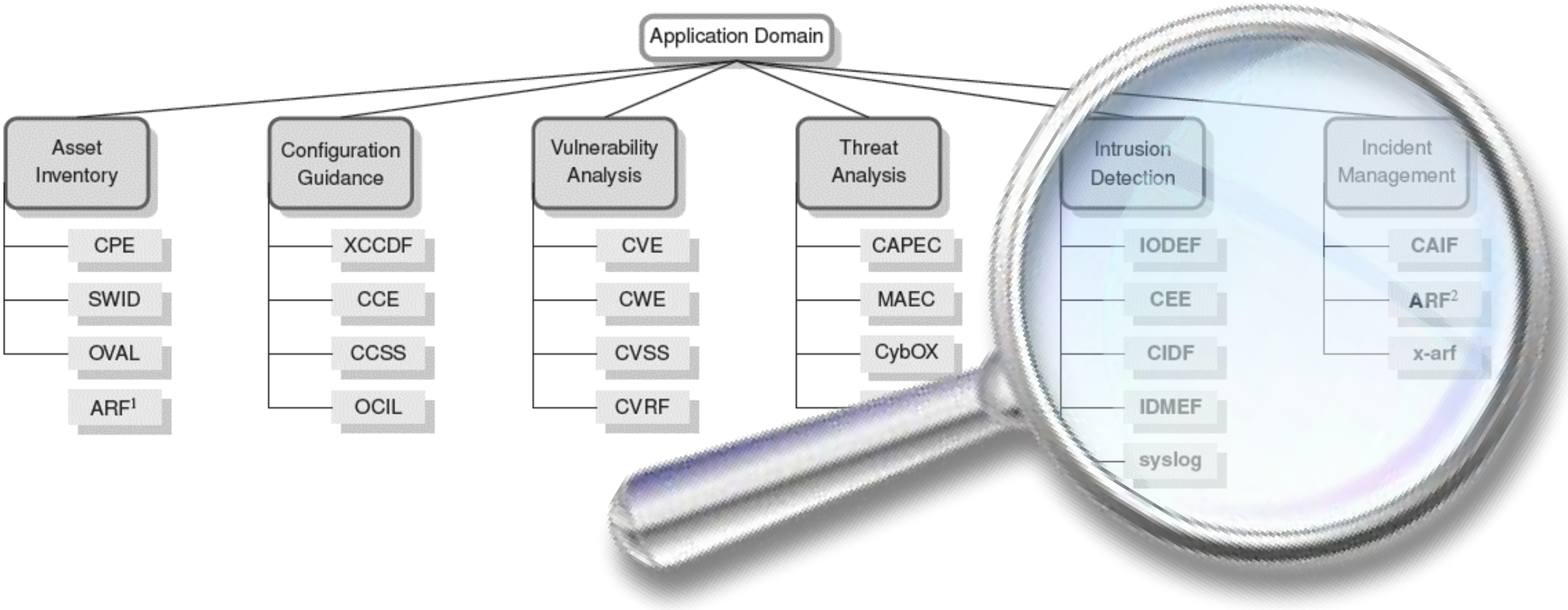
Source: https://www.gallaudet.edu/rsia/world_deaf_information_resource.html

Scenario

Scenario



Application Domain



Exchange formats

Security Event


```
{"dstIP": "65.55.162.200", "flags": "0x00 Unsampled", "
   proto":"tcp", "srcIP": "10.0.2.15", "aType": "C&C-
   Server", "dstPort": "25", "srcPort": "1036","
   relatedFlows": [["2014-09-08 00:56:23", "2014-09-08
   00:56:23", "1.2.3.4", "9.8.7.6,80", "34833", "4", "634
   ", "tcp", "2", "0", "27", "13", "13", "1"], ["
   2014-09-08 00:56:23", "2014-09-08 00:56:23", "1.2.3.4"
   , "9.8.7.6", "80", "42512", "4", "634", "tcp", "2", "0
   ", "27", "13", "13", "1"], ["2014-09-08 00:56:23", "
   2014-09-08 00:56:24", "1.2.3.4", "188.140.172.14", "
   52767", "80", "6", "520", "tcp", "2", "0", "30", "14",
    "14", "1"]]}
```

NetFlow meets IODEF / IDMEF

Listing 3 IODEF message including NetFlow

```
<IODEF-Document>
<Incident>
<EventData>
<Flow>
<System category="source">
<Node>
<Address category="ipv4-addr">127.0.0.1</Address>
<Address category="scr-mask">0 /0</Address>
</Node>
<Service>
<Port>54586</Port>
</Service>
</System>
<System category="target">
<Node>
<Address category="ipv4-addr">127.0.0.2</Address>
<Address category="dst-mask">0 /0</Address>
</Node>
<Service>
<Port>80</Port>
</Service>
</System>
</Flow>
<AdditionalData dtype="string" meaning="proto">6</
   AdditionalData>
...
<AdditionalData dtype="string" meaning="(in)packets">5</
   AdditionalData>
</EventData>
</Incident>
</IODEF-Document>
```

Listing 4 IDMEF message including NetFlow

```
<IDMEF-Message>
<Alert>
<CreateTime>2013-01-05T17:33:52.904+01:00</CreateTime>
<Source>
<Node>
<Address category="ipv4-net-mask">
<address>127.0.0.1</address>
<netmask>0 /0</netmask>
</Address>
</Node>
</Source>
<Target>
<Node>
<Address category="ipv4-net-mask">
<address>127.0.0.2</address>
<netmask>0 /0</netmask>
</Address>
</Node>
</Target>
<AdditionalData type="string" meaning="proto">
<string>6</string>
</AdditionalData>
....
<AdditionalData type="string" meaning="(in)packets">
<string>5</string>
</AdditionalData>
<AdditionalData type="string" meaning="(in)bytes">
<string>661</string>
</AdditionalData>
</Alert>
</IDMEF-Message>
```

Netflow meets MIME

Dat:
From:
To:
Message-ID:
Subject:
MIME-Version:
Content-Type:"multipart/report; report-type=feedback-report;"
Auto-submitted: auto-generated

——=_Part_5_255604560.1357480202349
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit
<E-Mail message>

——=_Part_5_255604560.1357480202349
Content-Type: message/feedback-report
Content-Transfer-Encoding: 7bit
<Meta-Data>

——=_Part_5_255604560.1357480202349
Content-Type: message/rfc822
Content-Transfer-Encoding: 7bit
Content-Disposition: inline
<Original message in its entirety>

Dat:
From:
To:
Message-ID:
Subject: abuse report about <source> - <date>
MIME-Version:
X-XARF:SECURE
Content-Type:"multipart/signed;
protocol="application/pgp-signature"; micalc=pgp-...
Auto-submitted: auto-generated

RFC822 Container
Content-Type: mesage/rfc822; name="xarf.eml"
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="xarf.eml"

embedded mail header
X-XARF: PLAIN
Auto-Submitted: auto-generated
Subject: abuse report about <source> - <date>
Content-Type: multipart/mixed

1st MIME part
Content-Type: text/plain
charset=utf-8 *<human readable text>*

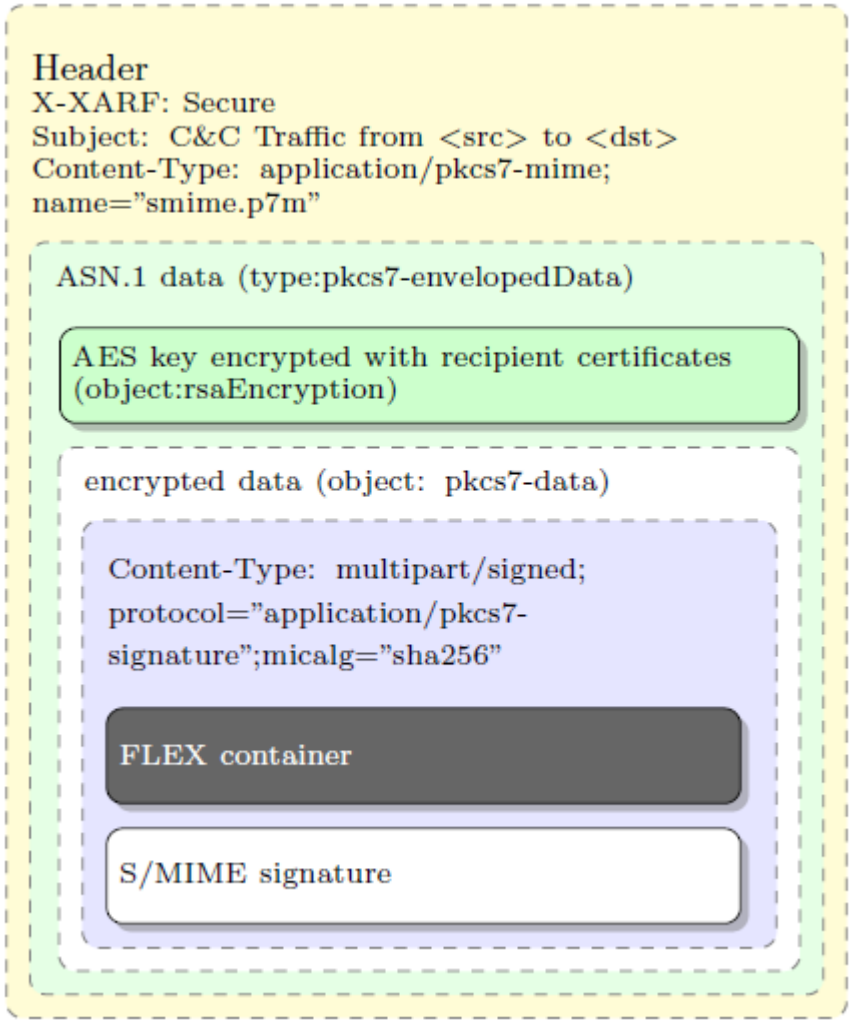
2nd MIME part
Content-Type: text/plain
charset=utf-8
name="report.txt"
<YAML notation of a JSON object>

3rd MIME part
Content-Type: message/rfc822
Content-Transfer-Encoding: 7bit
Content-Disposition: inline
<any content>

PGP/MIME signature
Content-Type: application/pgp-signature
<signature>

FLEX

FLEX - Components



- Transport:
  - SMTP

FLEX - Container

Listing 5 ASN.1 structure of a FLEX message

```
FLEXRecord ::= [APPLICATION 0] SEQUENCE {
settings    [0] Settings,
flowFields  [1] FlowFieldTypes,
detection   [2] Detection,
correlation [3] SEQUENCE OF CorrelatedFlows DEFAULT {}}
```

Listing 6 Settings of a FLEX message

```
Settings ::= [APPLICATION 1] SEQUENCE {
id         [0] INTEGER,
msgType    [1] ENUMERATED{alert(0), request(1), feedback
   (2)}
eventType  [2] ENUMERATED{CuC(0), DDoS(1)}
type       [3] ENUMERATED{netflow(0), ipfix(1)},
version    [4] ENUMERATED{two(0), four(1), five(2), nine
   (3)}}
```

Discussion

Source: http://www.prosperitycometh.com/wp-content/uploads/2012/11/business_conference_1600_clr_3835.png