CORRUPTING ANCIENT SPIRITS

Penetration Testing Oracle Forms

Bálint Varga-Perke 2017.10.20.

ABOUT

silent signal

BÁLINT VARGA-PERKE (BUHERÁTOR)

- Silent Signal - co-founder
- Pentester
  - Financial institutions
  - Healthcare
  - Development companies
- Long time Hacktivity supporter
  - ex-Orga
  - CTF/wargame creator
  - Hack the Vendor winner
- Ex-blogger and local know-it-all ☺

ORACLE FORMS

silent signal

„Oracle Forms, a component of Oracle Fusion Middleware, is Oracle's long-established technology to design and build enterprise applications quickly and efficiently.”

Name	Version	(*1) Database	Character/GUI	
IAF		2	Character	No IDE
FastForms+IAG		4	Character	
SQL*Forms	2	5	Character	
SQL*Forms	2.3	5	Character	New IDE, No PL/SQL, User Exits, INP A
SQL*Forms	3	6	Character	Major Rewrite, New IDE, PL/SQL, X Sup
Oracle Forms	4.0	6,7	GUI /	Major Rewrite, New IDE, FMB source bir

1979

1985

				v4.5 by claiming that this was a patch rel
Oracle Forms	5	7	GUI / Character	
Oracle Forms	6	8	GUI / Character	Forms Server / Web Forms introduced. C and uses a lot of memory per session.
Oracle Forms	6i	8	GUI / Character	
Oracle Forms	9i **(*2)**	9i	GUI	Client-Server runtime removed leaving F more effective communication between u
Oracle Forms	10g	10g	GUI	This is a Forms 9 release (9.0.4.0.19). R v9.0.4.0.19. Not forward compatible with
Oracle Forms	10gR2	10gR2	GUI	version 10.1.2.0.2 - registry home key m
Oracle Forms	11g	11g	GUI	version 11.1.1.X External Events, JavaSc
Oracle Forms	11gR2	11gR2	GUI	version 11.1.2.X Oracle Access Manager
Oracle Forms	12c	12c	GUI	Version 12.2.1.1 added support for Java less solution. Since April 2017 BI/Publish and Internet Developer licenses

(The WWW happened!)

1997

Solution for Error FRM-92095: Oracle Jnitiator version too low

By: Guest Author

Symtom:

After logging into application, system pop up below error message:

FRM-92095: Oracle JInitiator version too low. Please install version 1.1.8.2 or higher

Cause:

The JRE version is not incompatible.

Solution 1:

This is a workaround solution, For Window 7 user, Add a OS Parameter: JAVA_TOOL_OPTIONS, and parameter value is: -Djava.vendor="Sun Microsystems Inc."

PREVIOUS WORK

JOXEAN KORET (@MATALAZ) –
HACKPROOFING ORACLE FINANCIALS

- Examined Forms as a component of E-Business Suite
- Focus on the framework itself, multiple vulnerabilities

YOURS TRULY –
AUTOMATED SECURITY TESTING OF ORACLE FORMS APPLICATIONS

- Focus on applications implemented using Forms
- Tools on GitHub

PROTOCOL OVERVIEW

PRE-WEB CONCEPTS:

- Transport over HTTP or raw TCP
- Payload encrypted
  - „not as strong as the SSL standard”
  - HTTPS is supported - No one uses it
- Custom data serialization
- „Rapid Application Development”
  - Lots of generated code
  - Limited developer insight
- Event-driven operation
  - Server-side state storage

EVENT-DRIVEN OPERATION

silent signal

THE „STATELESS” WEB:

1. User selected item ID=1337
2. Full new state sent to client

SERVER-SIDE STATE:

1. User left-clicked at coordinates X=153 Y=246
   - Minimal delta state sent to client
2. User selected 2nd option from List 3
   - Minimal delta state sent to client
3. User left-clicked at coordinates X=84 Y=323
   - Minimal delta state sent to client

EVENT-DRIVEN OPERATION

A WORLD OF PAIN:

- Only string values can be directly manipulated
  - Numeric ID's are only valid locally
  - Custom application logic may be interesting!
- Actions become invalid as the UI state changes
  - Have to reset state before every test case
- See also: Java Servlet Faces :P
  - Testing Stateful Web Application Workflows – by Dnet

SERIALIZATION

silent signal

- Binary (== not human readable) representation
- Variable length fields
- Recursive representation
  - Messages
    - Objects (can be Messages)
      - Fields
- Caching and references to previous objects

1. Table Object serialization formats

Type	Property Type Header	Representation
Boolean (true)	0x5000	N/A
Boolean (false)	0x6000	N/A
Integer (0)	0x1000	N/A
Integer (0-255)	0x2000	Integer value as 1 byte
Integer (255-65535)	0x3000	Integer value as 2 bytes
Integer (other)	0x0000	Value as 4 bytes
String	0x4000	1 byte identifier (see description below) Length: 2 bytes UTF-8 string buffer
String reference	0x9000	1 byte identifier 1 byte new identifier (see description below)
Byte	0x7000	Byte value

1. Table Object serialization formats

Type	Property Type Header	Representation
Boolean (true)	0x5000	N/A
Boolean (false)	0x6000	N/A
Integer (0)	0x1000	N/A
Integer (0-255)	0x2000	Integer value as 1 byte
Integer (255-65535)	0x3000	Integer value as 2 bytes
Integer (other)	0x0000	Value as 4 bytes
String	0x4000	1 byte identifier (see description below) Length: 2 bytes UTF-8 string buffer
String reference	0x9000	1 byte identifier 1 byte new identifier (see description below)
Byte	0x7000	Byte value

SERIALIZATION

silent signal

NON-TRIVIAL FORMAT

- Tried reimplementation in Java and Python
  - FAIL
- Tried code generation with Kaitai Struct
  - Unfortunately it was designed for sane formats...
  - FAIL

BUT IT'S JAVA!

- Message parsing code is 100% reusable!
  - frmall.jar
  - oracle.forms.engine.Message
  - readDetails(), writeDetails()

ENCRYPTION

silent signal

„NOT AS STRONG AS THE SSL STANDARD”

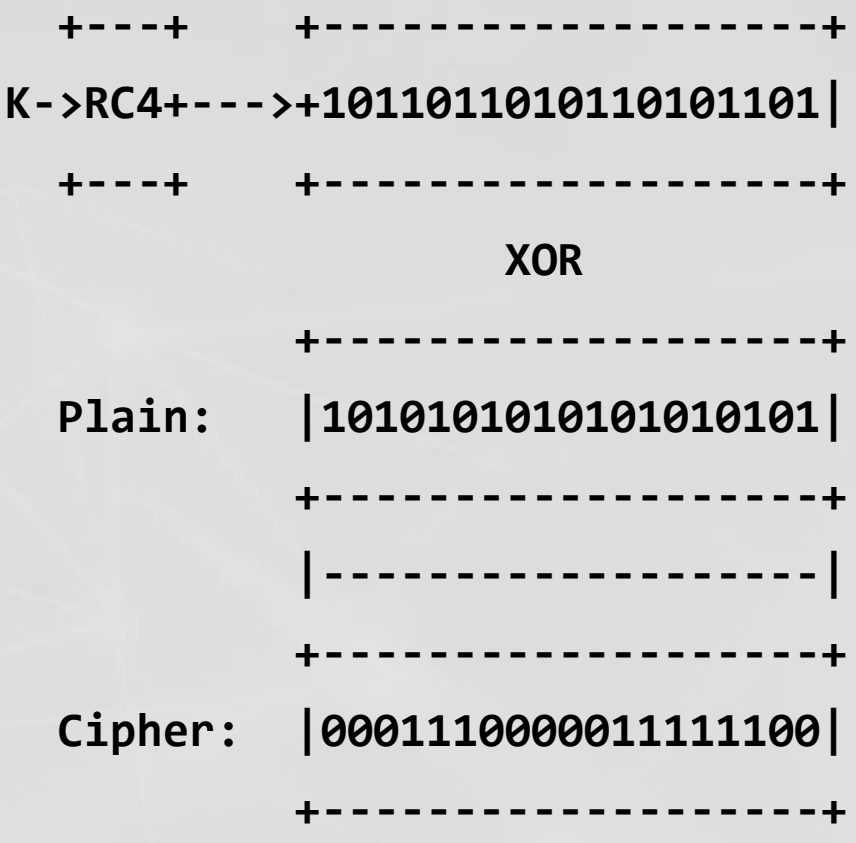
- Easy to spot:
  - EncryptedInputStream
  - EncryptedOutputStream
- RC4 can be identified easily
- Standard implementation

```
public synchronized void setEncryptKey(byte[] paramArrayOfByte)
{
  if ((paramArrayOfByte == null) || (paramArrayOfByte.length == 0) || (p
    throw new RuntimeException();
  }
  this.mSeedBuffer = new int['Ā'];
  this.mI = (this.mJ = 0);
  for (int i = 0; i < 256; i++) {
    this.mSeedBuffer[i] = i;
  }
  int k;
  int j = k = 0;
  for (int i = 0; i < 256; i++)
  {
    k = (k + (paramArrayOfByte[j] & 0xFF) + this.mSeedBuffer[i]) % 256;
    int m = this.mSeedBuffer[i];
    this.mSeedBuffer[i] = this.mSeedBuffer[k];
    this.mSeedBuffer[k] = m;
    j = (j + 1) % paramArrayOfByte.length;
  }
}
```

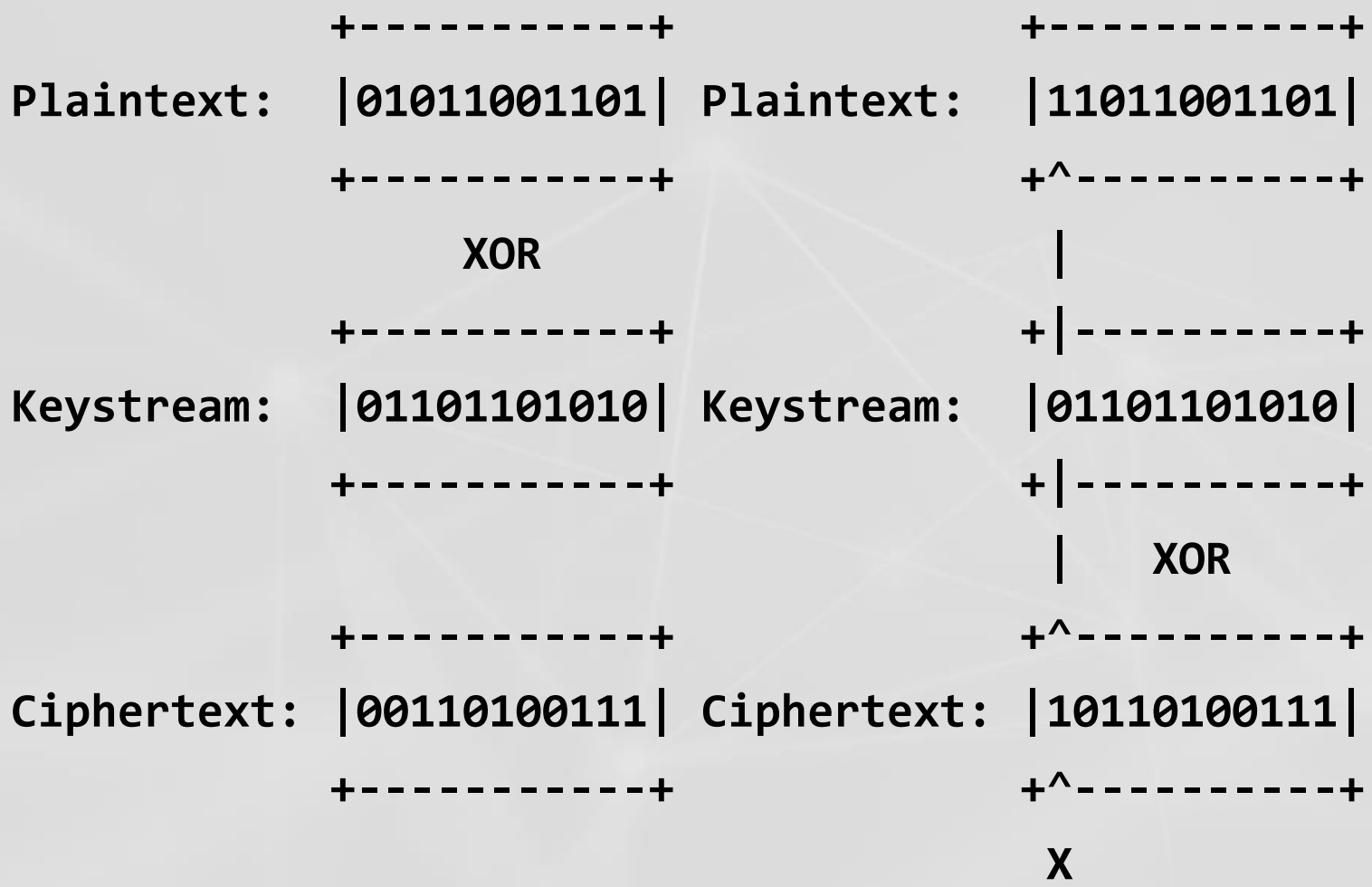
RC4

RC4 IS BROKEN

- But we are not the NSA!
  - Bar-Mitzvah, NOMORE are against SSL/TLS
  - Exploitation impractical
- Still, RC4 is a simple stream cipher ☺
  - Trivial attacks if not used carefully
  - It is not used carefully…



NO INTEGRITY CHECKS



KNOWN-PLAINTEXT ATTACK

KNOWN-PLAINTEXT ATTACK

$$Cq = K + Pq$$
$$Cp = K + Pp$$
$$Cq + Cp = Pq + Pp$$
$$\mathbf{Pp = Cq + Cp + Pq}$$

```
+----------------------------+
|KSKSKSKSKSKSKSKSKSKSKSKSKS|
+----------------------------+
+----------------------------+
|PqPqPqPqPqPqPqPqPqPqPqPqPq|
+----------------------------+
```

```
+----------------------------+
|KSKSKSKSKSKSKSKSKSKSKSKSKS|
+----------------------------+
+----------------------------+
|CpCpCpCpCpCpCpCpCpCpCpCpCp|
+----------------------------+
```

KEY EXCHANGE

silent signal

```
localDataOutputStream.writeInt(NEG_SEND);
localDataOutputStream.writeInt(i = new
Random().nextInt());
localDataOutputStream.flush();
k = localDataInputStream.readInt();
j = localDataInputStream.readInt();
```

```
byte[] arrayOfByte = new byte[5];
arrayOfByte[0] = ((byte)(i >> 8));
arrayOfByte[1] = ((byte)(j >> 4));
arrayOfByte[2] = -82;
arrayOfByte[3] = ((byte)(i >> 16));
arrayOfByte[4] = ((byte)(j >> 12));
if (this.mUseNativeHTTP) {
this.mHNs.setEncryptKey(arrayOfByte);
}
```

```
POST http://192.168.124.139:8889/forms/lservlet;jsessionid=c0a87c8b22b9597488f1bd2d4be1a139d429a14af91a HTTP
Pragma: 3
Content-type: application/octet-stream
Cache-Control: no-cache
User-Agent: Mozilla/4.0 (Windows 2003 5.2) Java/1.8.0_25
Host: 192.168.124.139:8889
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-Length: 463
Connection: close

□□□□□□□q □□``□□□ □XA    c□@server escapeParams=true module=tuto_forms.fmx userid=SYSTEM/oracle@127.0.0.1/XE
sso_subDN= sso_usrDN= debug=yes host=172.16.110.143 port=7777 buffer_records=no debug_messages=no array=no c
tracegroup= log=forms_log_s2.txt term=1
□□□□!□□1□□□□□□@@@□□□□□□1□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□A□c□□Dialog1y□□qz□q(□□□□□a#B□c□Europe/B
```

THE DEADLY MIXTURE

silent signal

ACCIDENTAL SECURITY?

- HTTP is message based - RC4 is a stream cipher
- HTTP is stateless - The cipher is stateful

PERFECT SYNC NEEDED!

- No extra/missing messages
  - Can't use Repeater
  - Can’t use Scanner
- No extra/missing bytes
  - Can only do length preserving transformations on strings

FIRST SOLUTION

ORACLEFORMSTESTER

- Burp plugin written in Java
- Intercepts key exchange and de/encrypts HTTP bodies
- Reuses the vanilla frmall.jar for serialization
- Saves every (SHA(cipher text);[cipher state]) pair
- Looks up the matching cipher state when an encrypted req. is sent to Scanner and decrypts it
- Creates new Scanner insertion points for String properties
- Serializes and encrypts for sending

ORACLEFORMSTESTER

PROBLEMS

- Client inevitably gets desynchronized
  - Client cut-off is needed to avoid interference
  - Needs client restart after every scan
- Most messages are not editable
- Macros not supported
  - Critical for stateful testing!
- Complex design + mostly unmaintained *whistles*
  - Prone to bugs
  - Hard to debug
  - Hard to fix

IDEAS FOR FIXING

silent signal

RESYNCING THE CIPHER

- We only need to set a byte array that is the RC4 state
- Java debuggers?
  - Mostly for graphical IDE's (assuming src availability)
  - JDB is pain
  - Attaching a debugger to archaic applets is pain
  - How to handle object lifecycle?
  - Scriptability?
- Patching a „debugger” into the client
  - Java Security Policy
  - No high-level communication primitives

ZERO-STATE

silent signal

STRIPPING CRYPTO OFF THE CLIENT

- Preventing the client from encrypting Messages
- Tools consume plain (==stateless) traffic
- Upstream proxy performs crypto
  - Simple KEX
  - Standard algorithm
- New tools: OracleFormsSerializer + MitMproxy inline script

DEMO

AUTOMATED TESTING

STILL NOT EASY

- Application state still needs to be taken care of
- Short output
  - + string caching hides relevant information
- Noisy output

PRO TIPS

KNOW YOUR TARGET

- Don’t rely solely on automated results
- Focus on relevant weaknesses
- Manually review Scanner outputs
  - And write application specific tools
- Source code review can be highly effective
  - For injection-style issues
- Special care for AUTHN/AUTHZ

THANK YOU!

BÁLINT VARGA-PERKE

VPBALINT@SILENTSIGNAL.HU

FACEBOOK.COM/SILENTSIGNAL

@SilentSignalHU

@buherator

silent signal