

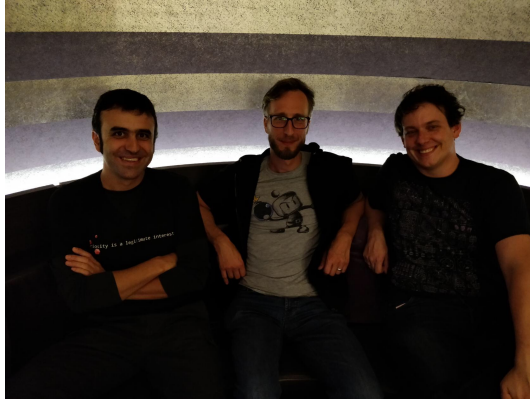
# Zero Fax Given

@zeronights - 2018

---

Luis Merino, Eric Sesterhenn, Markus Vervier  
2018

X41 D-SEC GmbH



Luis, Eric, Markus



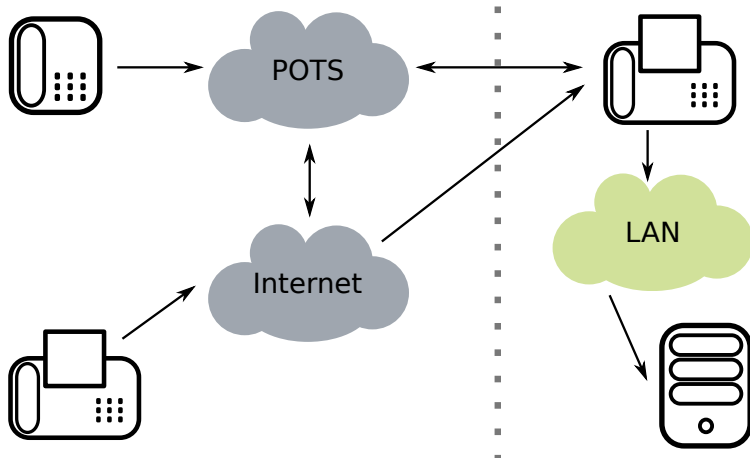
- Fax machines still present in private and public spaces
- Its technology matured decades ago and might not get much love since then
- All-in-one usually connected to phone and Ethernet networks
- Usually not considered as an attack vector

# Premature Disclosure?



- Preview peak into DEF CON schedule
- What the Fax?!
- Parallel research
- Great job by Eyal Itkin & Yaniv Balmas
- Video: <https://www.youtube.com/watch?v=qLCE8spVX9Q>

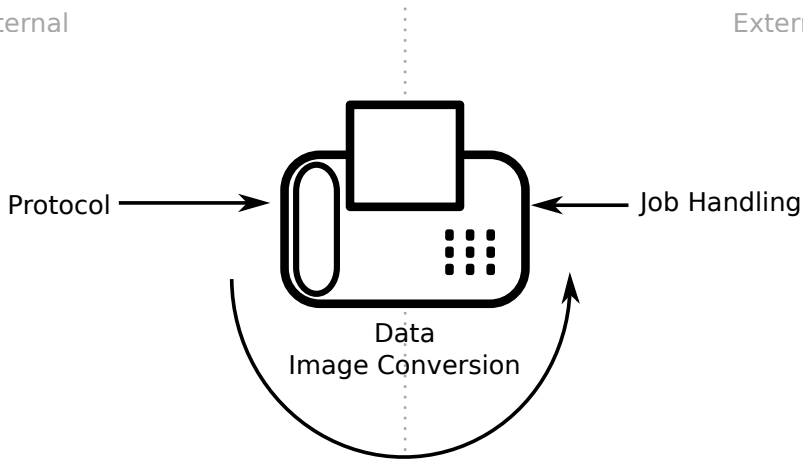
# Attack Surface - Global



# Attack Surface - Local

Internal

External





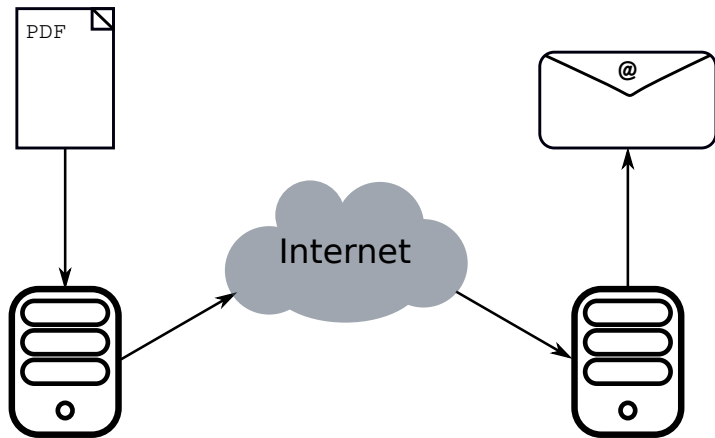
- Specified in ITU recommendations
- Analog (mostly obsolete):
  - Group 1 / Group 2, similar to Analog-TV transmission (hello scanlines..)
- Digital:  $\leq$  **we looked at this**
  - Group 3 / Group 4
  - Supports compression, TIFF / JPEG
- The Fax Class specifies what is offloaded to the actual fax modem hardware



- Fax protocols were originally designed to go over telephone lines
- VoIP is killing them due to variances in latency and high-compression encoding omitting signals
- T.38 was developed to counter this



# Internet Fax - Additional Attack Surface



# Fax Security Features That You Encounter



- NO Encryption
- NO Integrity
- *Yet, it seems to be somewhat reliable (you can be quite confident a fax was received.)*
- A fax is officially accepted in many countries by courts as a reliable way of transmitting documents

# Encrypted Fax Anyone?



## Annex H

### Security in facsimile G3 based on the RSA algorithm

#### H.1 Preamble

(The preamble is left blank on purpose)

**WANTED**

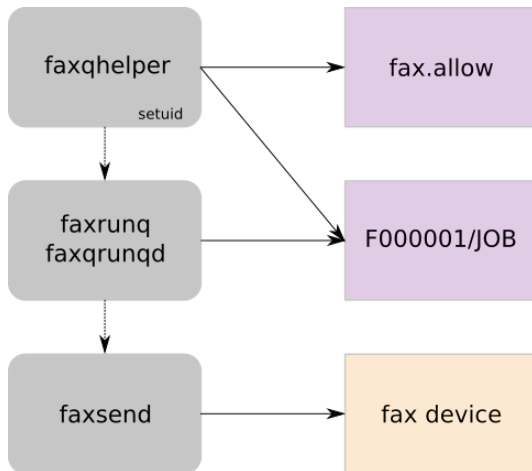
#### H.2 Introduction

This annex specifies the mechanisms to offer security features based on the RSA cryptographic mechanism. The coding scheme of the document transmitted with security features may be of any kind defined in Recommendations T.4 and T.30 (Modified Huffman, MR, MMR, Character mode as defined in Annex D/T.4, BFT, other file transfer mode defined in Annex C/T.4).



mgetty is a modem-aware getty. It supports modems with the Hayes AT command set and is especially designed for supporting modems that are used to send faxes and to dial out as well as dial in.

# mgetty flow



# mgetty - faxqhelper

---

```
/* replace all quote characters, backslash and ';' by '_' */
for( q = buf; *q != '\0'; q++ )
{
    if ( *q == '\\' || *q == '"' || *q == '\'' ||
         *q == '\\\' || *q == ';' )
        { *q = '_'; }
}
```

---

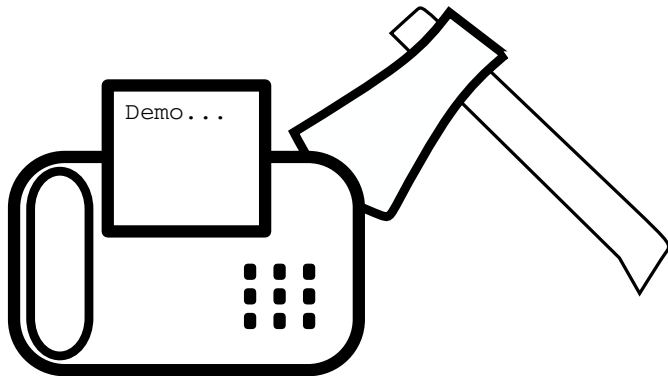
# mgetty - faxrunq



---

```
/* replace all quote characters, backslash and ';' by '_' */
command=`tr -d '\042\047\140\134\044\073' <JOB | \
$AWK 'BEGIN { phone="-"; flags=""; pages="" }
$1=="phone" { phone=$2 }
$1=="pages" { for( i=2; i<=NF; i++) pages=pages$i" " }
END { printf "'"$FAX_SENDER"' -v%s %s %s", \
flags, phone, pages }' -`
```

```
# execute faxsend command
eval $command
```

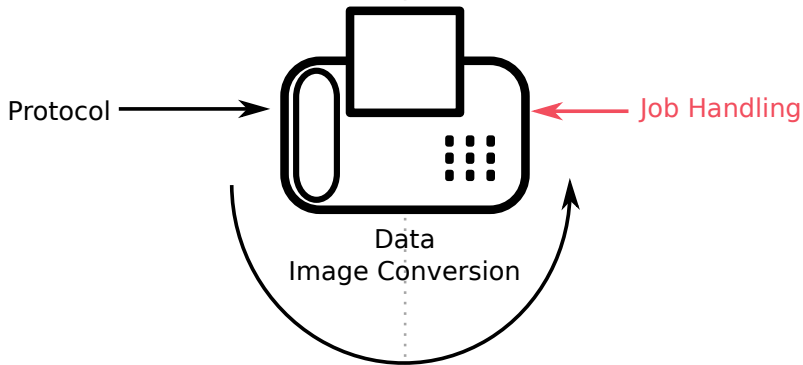




# Attack Surface

Internal

External



efax is smaller and easier to install than HylaFAX or mgetty+sendfax. As one user put it “EFAX is a nice simple program for single user systems.”



- Several bugs found
- Only lightly explored
- Should not be used where security is relevant

---

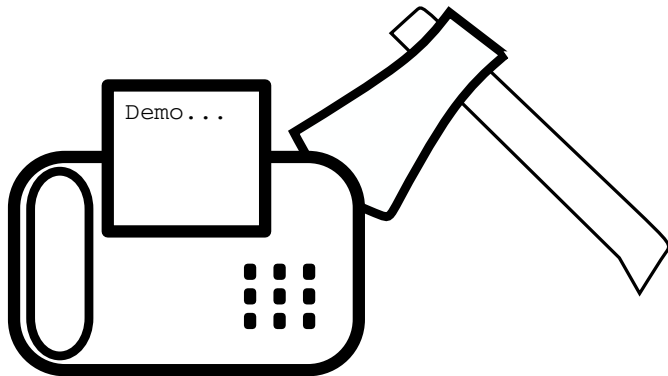
```
int readline ( IFILE *f, short *runs, int *pels )
{
    int nr = 0, nb ;
    uchar bits [ MAXBITS ] ;

    case P_PBM:
        if ( fread ( bits, 1, f->page->w/8, f->f ) !=
            f->page->w/8 )
```

---



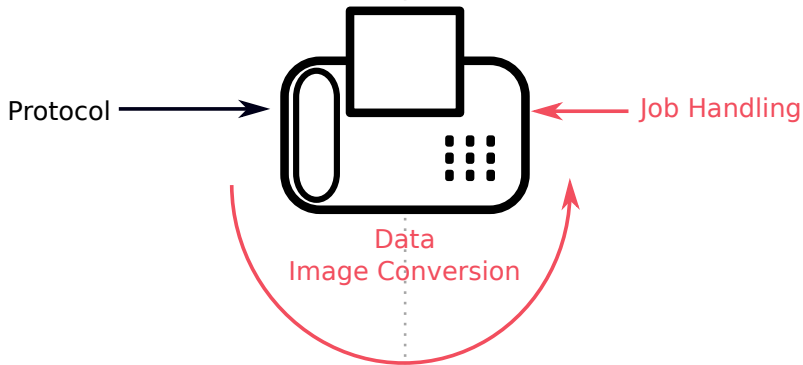
- Just a stack based buffer overflow...
- What about ASAN?
- Debian Stable / gcc 6.3.0 20170516
- *fread()* not checked



# Attack Surface

Internal

External





---

```
> ATD10000  
< CONNECT  
< HylaFAX (tm) Version 6.0.6
```

---



Devices announce their capabilities

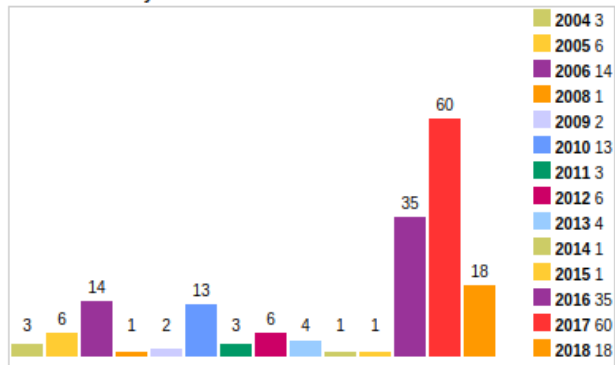
- Compression
- Resolution
- Transmission Rate
- Error Correction
- JBIG and JPEG



- T.4 Recommendation specifies just Modified Huffman (MH) and Modified READ compression
- T.30 added JBIG, JPEG, and MRC as compression, even supporting color
- *In other words: a lot of parsers and complex formats, great!*

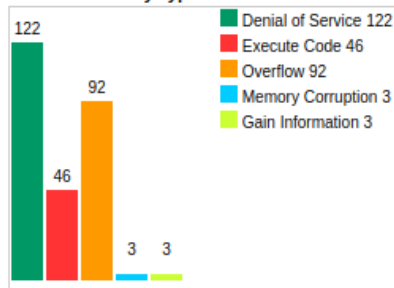
# Compression Libraries and Known Vulnerabilities - Fun With libtiff

Vulnerabilities By Year



zeronights 2018

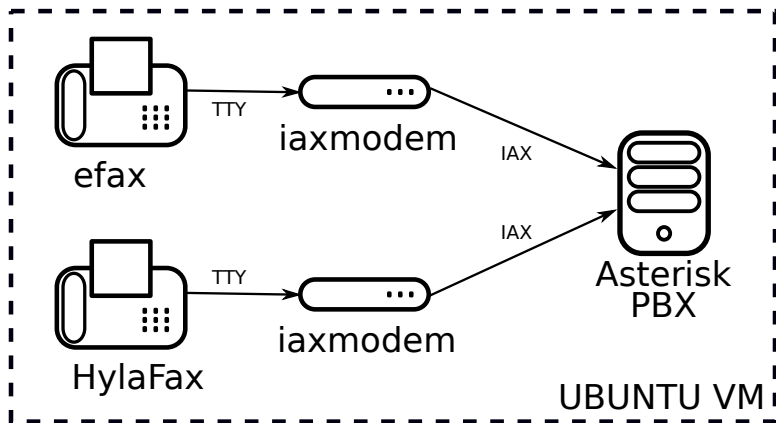
Vulnerabilities By Type



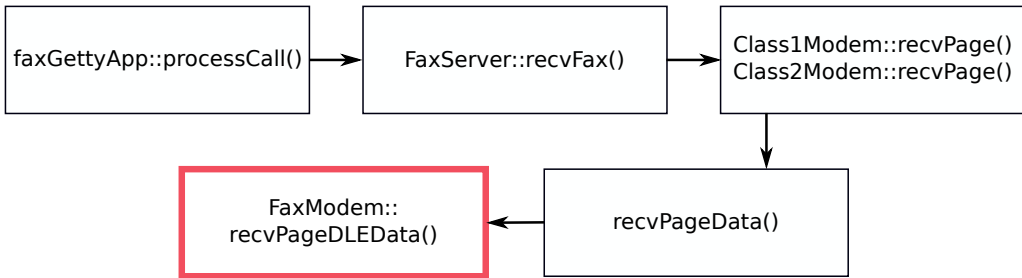


HylaFAX Open Source is designed around a client-server architecture. Fax modems may reside on a single machine on a network and clients can submit an outbound job from any other machine on the network. Client software is designed to be lightweight and easy to port.

# HylaFax Setup



# HylaFax - Callchain



# faxgetty - Heap Overflow While Fax Reception

---

```
// FaxModem::recvPageDLEData(...) excerpt  
recvRow = (u_char*) malloc(1024*1000); // 1M should do it?  
do {  
    // ...buf is filled with contents from calling party...  
    // ...fin=true; when receiving EOF or timing out...  
    memcpy(recvRow, (const char*) buf, cc);  
    recvRow += cc;  
} while (!fin);
```

---

# faxgetty - Heap Overflow? Are you sure?



There is **another more powerful bug**

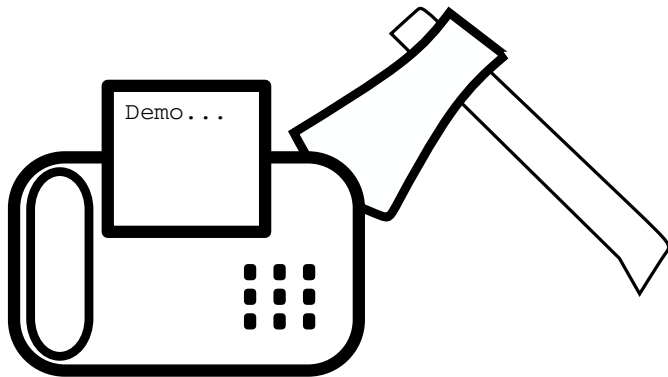
By messing with format flags during a call, *recvRow* could:

- remain uninitialized
- point to a heap buffer
- point to a stack buffer
- offset it before triggering *memcpy()*





Step Through The Code

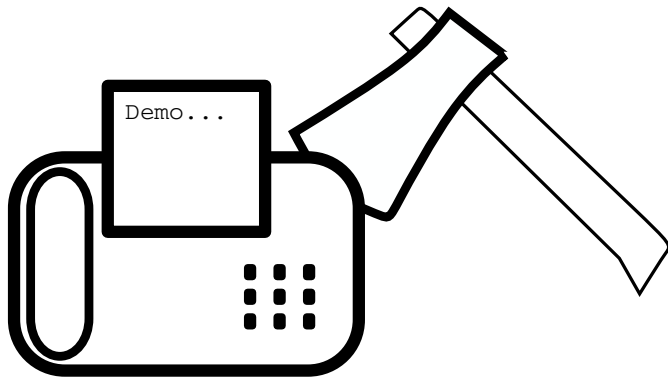


# faxgetty - Uninitialized Pointer - Exploitation

1. Hit a code path that makes it point to something interesting (Heap or Stack)
2. Hit a code path where this will be allocated to another object
3. Hit a code path that allows you to write into the newly allocated object

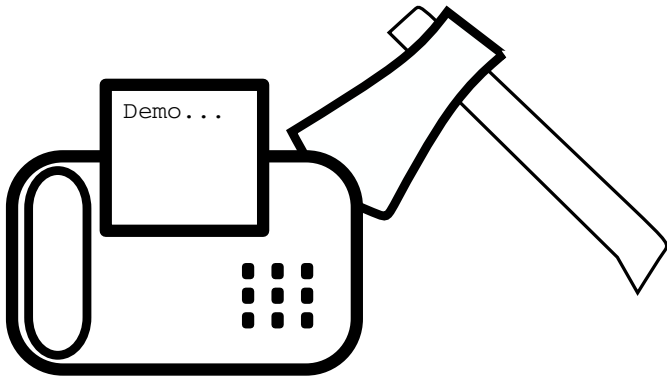
# faxgetty - Uninitialized Pointer - Exploitation

Showing the code paths



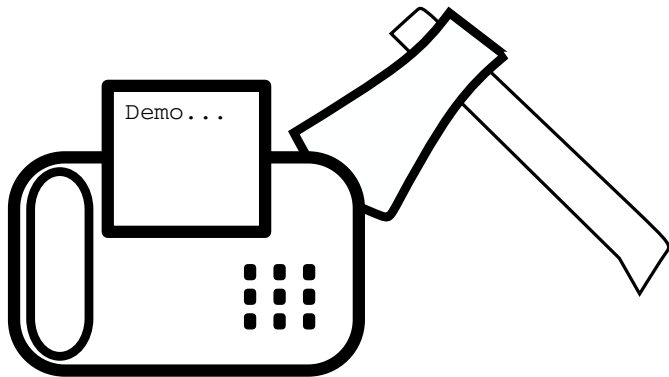


*mmap()* is not our friend





Exploiting it by pointing to the Stack



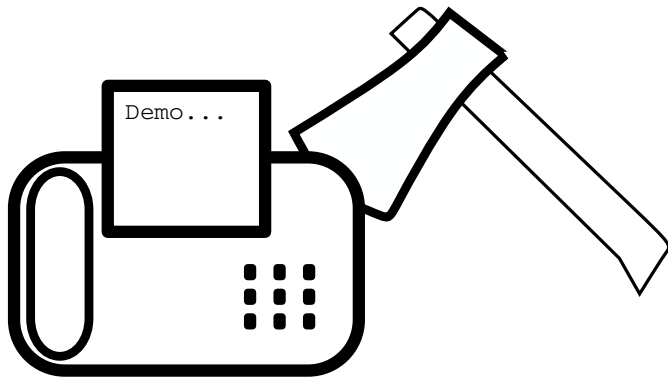


How to get control flow:

1. Submit a TIFF Using DLE Transmission → will point *recvBuf* to the stack
2. Submit a ECM transmission setting JPEG + 2DMR flags
3. Profit

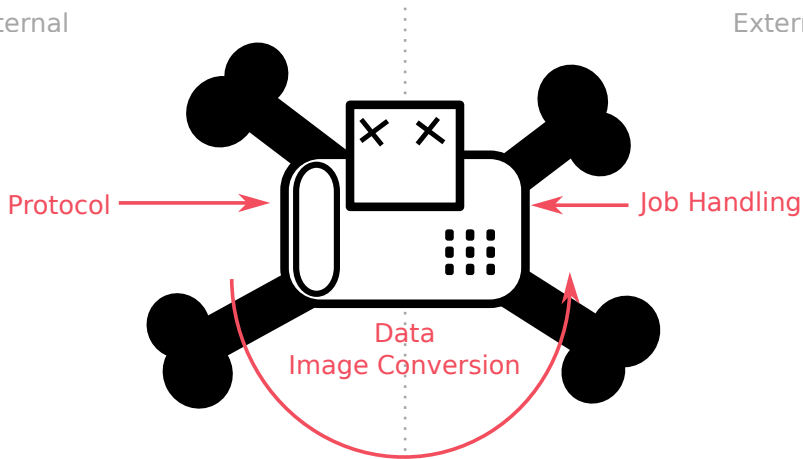
# faxgetty - Uninitialized Pointer - PoC Demo

Exploiting it by pointing to the stack



Internal

External







- Use different compilers, hardening and optimization settings during fuzzing
- Revisit old technology, do not simply follow the new hype train



- Internet Fax T.38
- Audit the 1000s of different hardware faxes out there
- Reverse-exploitation of the caller
- Build a global Fax database using capability fingerprinting

# Q & A - Thanks for listening!



Contact us at:

{luis.merino, eric.sesterhenn,  
markus.vervier}@x41-dsec.de

<https://x41-dsec.de>

