security-assessment.com

HACKING

Ruxcon 2011

Nick Freeman

dimension data

FADE IN:

- **I'm Nick Freeman a.k.a vt**
  - I work at Security-Assessment.com in Auckland, NZ
- **I primarily spend my time hacking web applications**
  - Also thoroughly enjoy network pentests
- **I spend my free time**
  - Finding 0day
  - Making music
  - Drinking whisky
  - Watching stuff

Watching Stuff

- I have reasonably varied taste
  - Crime / serial killers
  - Comedy
  - Some Sci Fi
  - B-grade movies
  - Documentaries

- The more I watch, the more I find myself waiting
  - Seasons getting shorter, cancellations more common, often there are mid-season breaks, writers' strikes etc.

I'm not the world's most patient man.

This is a problem for me…

Solutions

- Watching more shows?
- Getting out of the house?
- Reading a book?
- Hacking stuff?
  - Hmm..

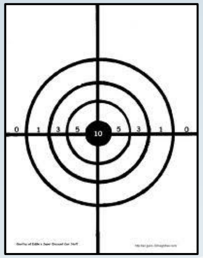
Yes.. Hacking stuff.

I know the source of a decent amount of what I watch

Hollywood films can have very large budgets

Presumably some of this is spent on shiny software

Very expensive software != very secure software



If I hack this software, perhaps I won't wait as much

Or at least if I hack enough I won't realise I'm waiting

My new purpose in life

- **Keep myself entertained**
  - And as a result of said entertainment, become more entertained
- **Find bugs that would enable me, if I were so inclined, to get the media I so desire before it is released**
- **Get shells, and lots of them.**
- **Show an entire industry that their software needs ‘additional development’**
  - Or maybe just a visit from the rm –rf fairy.

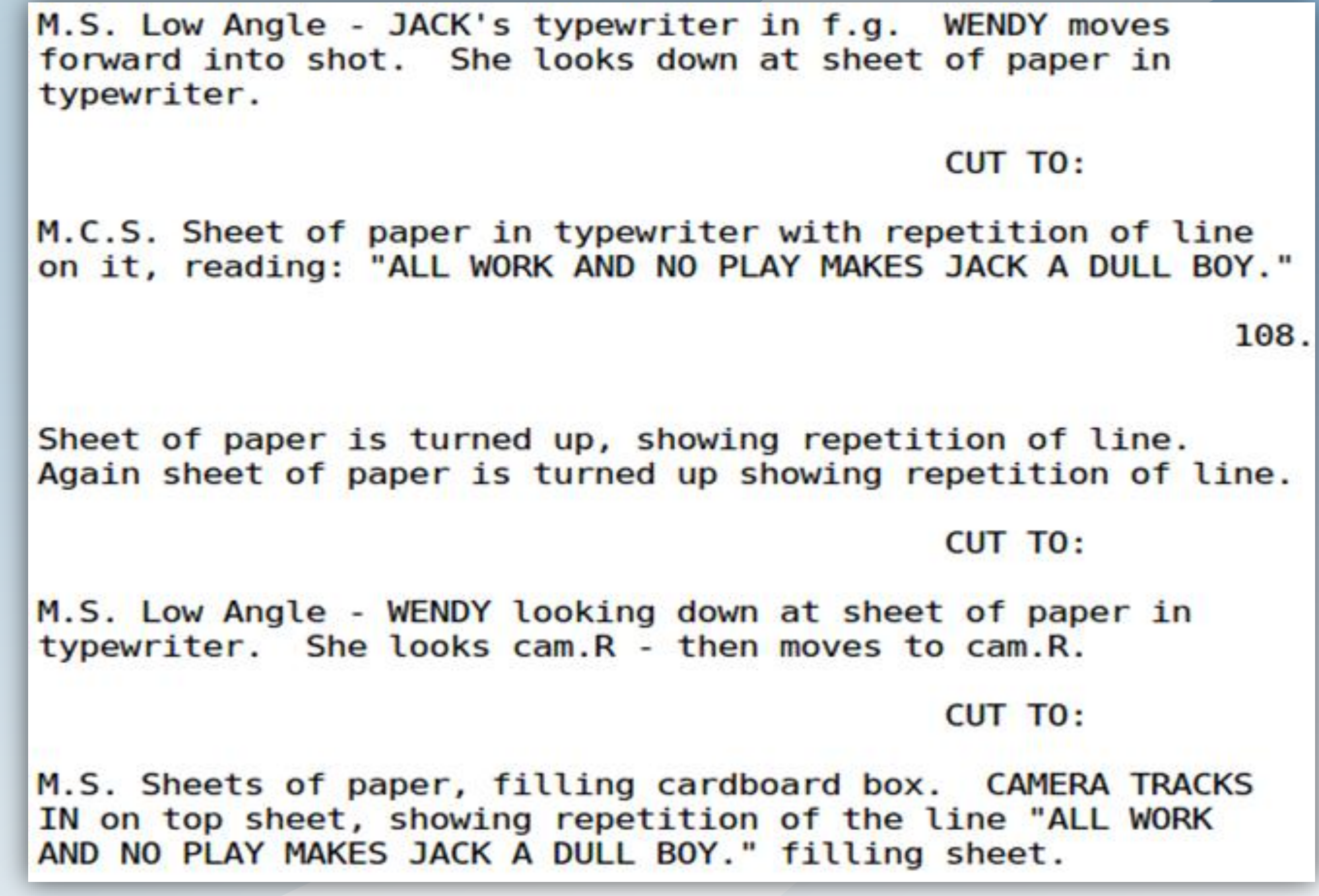
My methodology

- I didn’t fuzz the apps you will see me own today

- I looked for the software with the most testimonials from highest grossing films
  - Specifically targeting industry standard / preferred apps

- This would give the greatest chance of penetrating a studio network and making off with their loot. Woot!

ACT I: Script Writing



M.S. Low Angle - JACK's typewriter in f.g. WENDY moves forward into shot. She looks down at sheet of paper in typewriter.

CUT TO:

M.C.S. Sheet of paper in typewriter with repetition of line on it, reading: "ALL WORK AND NO PLAY MAKES JACK A DULL BOY."

108.

Sheet of paper is turned up, showing repetition of line.
Again sheet of paper is turned up showing repetition of line.

CUT TO:

M.S. Low Angle - WENDY looking down at sheet of paper in typewriter. She looks cam.R - then moves to cam.R.

CUT TO:

M.S. Sheets of paper, filling cardboard box. CAMERA TRACKS IN on top sheet, showing repetition of the line "ALL WORK AND NO PLAY MAKES JACK A DULL BOY." filling sheet.

ACT I: Script Writing

- **Every production created needs a story and a script.**
- **Scriptwriting software was designed to make this easier**
  - Automatic formatting
  - Linking of characters, scenes, actions
  - Spellchecking
- **Collaboration functionality**
  - Write together over the internet between multiple script writers.

App #1: Final Draft < 8.02

- *"The number-one selling scriptwriting software in the world."*

- **Vendor Response: 4/5**
  - Initially very positive
  - Then stopped responding to my emails :(
  - Bug successfully patched

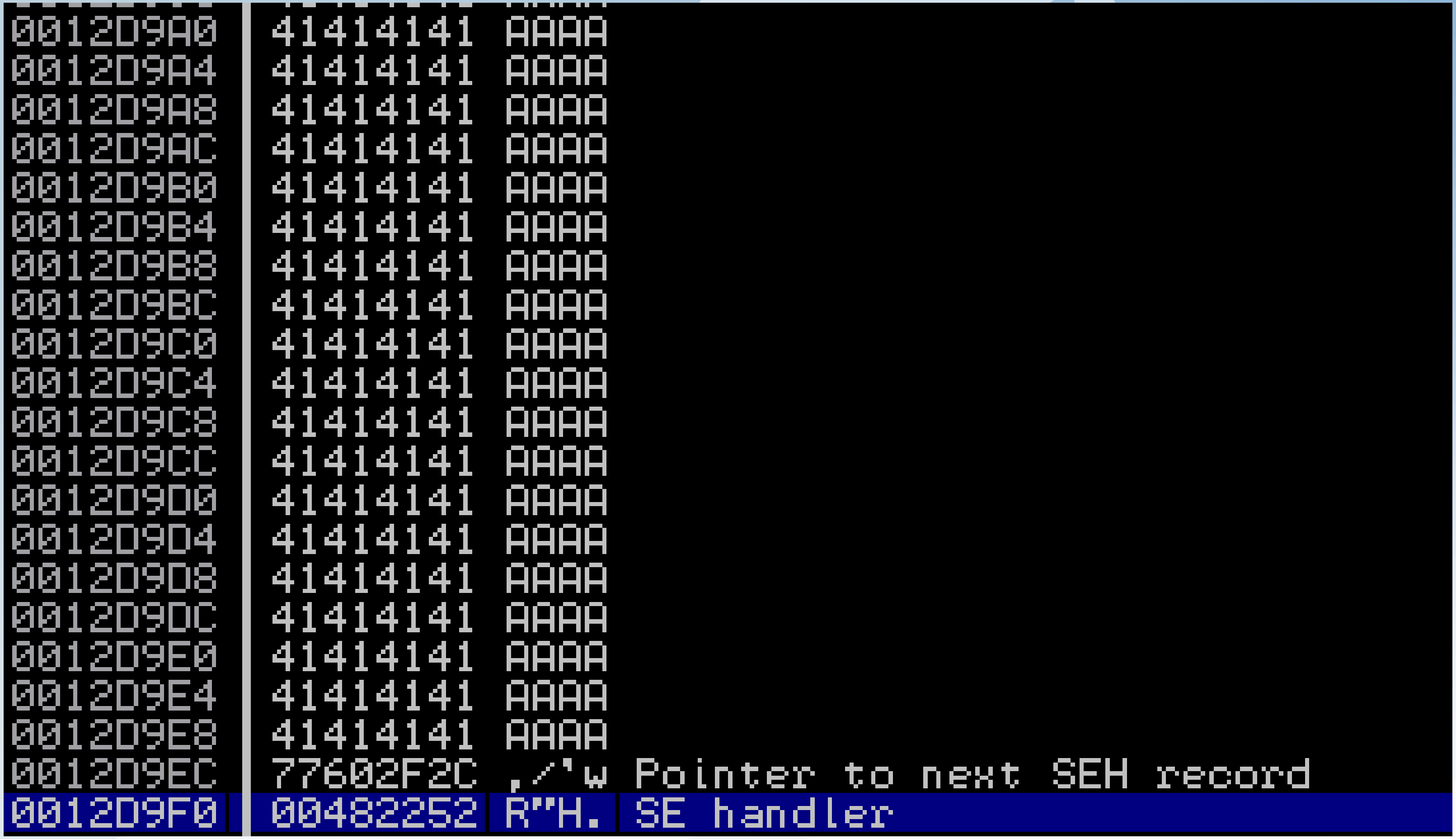
- **Example users**
  - James Cameron (Avatar, Titanic, Aliens.)
  - Wes Craven (Nightmare on Elm St, The Hills Have Eyes II)

Final Draft 8 – The Bug

- Final Draft uses multiple file formats – one being .fdx (XML)
- Several fields in a .fdx file have no bounds checking when parsed by FD
  - <IgnoredWords> (used for spellchecking whitelist)
  - <Character>
  - <Transition>
  - <Location>
  - <Extension>
  - <SceneIntro>
  - <TimeOfDay>

Final Draft 8 – The Bug

- Lack of bounds checking caused a stack buffer overflow



```
0012D9A0   41414141  AAAA
0012D9A4   41414141  AAAA
0012D9A8   41414141  AAAA
0012D9AC   41414141  AAAA
0012D9B0   41414141  AAAA
0012D9B4   41414141  AAAA
0012D9B8   41414141  AAAA
0012D9BC   41414141  AAAA
0012D9C0   41414141  AAAA
0012D9C4   41414141  AAAA
0012D9C8   41414141  AAAA
0012D9CC   41414141  AAAA
0012D9D0   41414141  AAAA
0012D9D4   41414141  AAAA
0012D9D8   41414141  AAAA
0012D9DC   41414141  AAAA
0012D9E0   41414141  AAAA
0012D9E4   41414141  AAAA
0012D9E8   41414141  AAAA
0012D9EC   77602F2C  ,/'w  Pointer to next SEH record
0012D9F0   00482252  R"H.  SE handler
```

Final Draft 8 – The Exploit

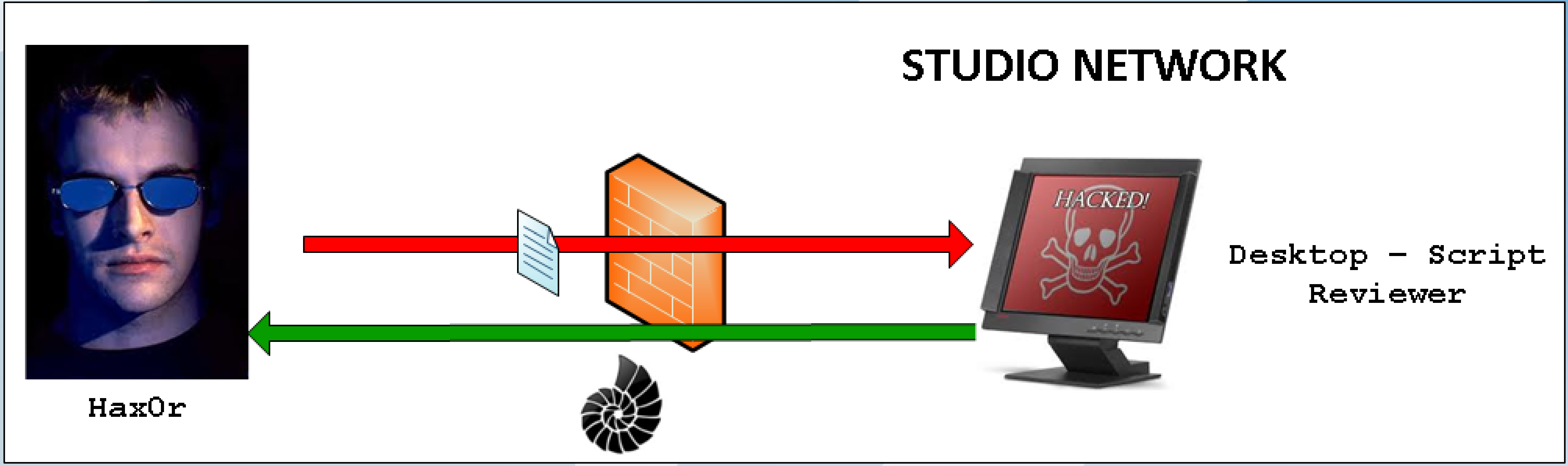
- **Exploit Constraints:**
  - Exploit code must be ASCII printable
  - For all cases except <IgnoredWords>, must also be uppercase
  - SafeSEH in all app components except the base executable
  - The executable itself is somewhat lacking any useful op-codes

- **The value of IgnoredWords is null terminated**
  - So we can use a location within the base executable as our SEH

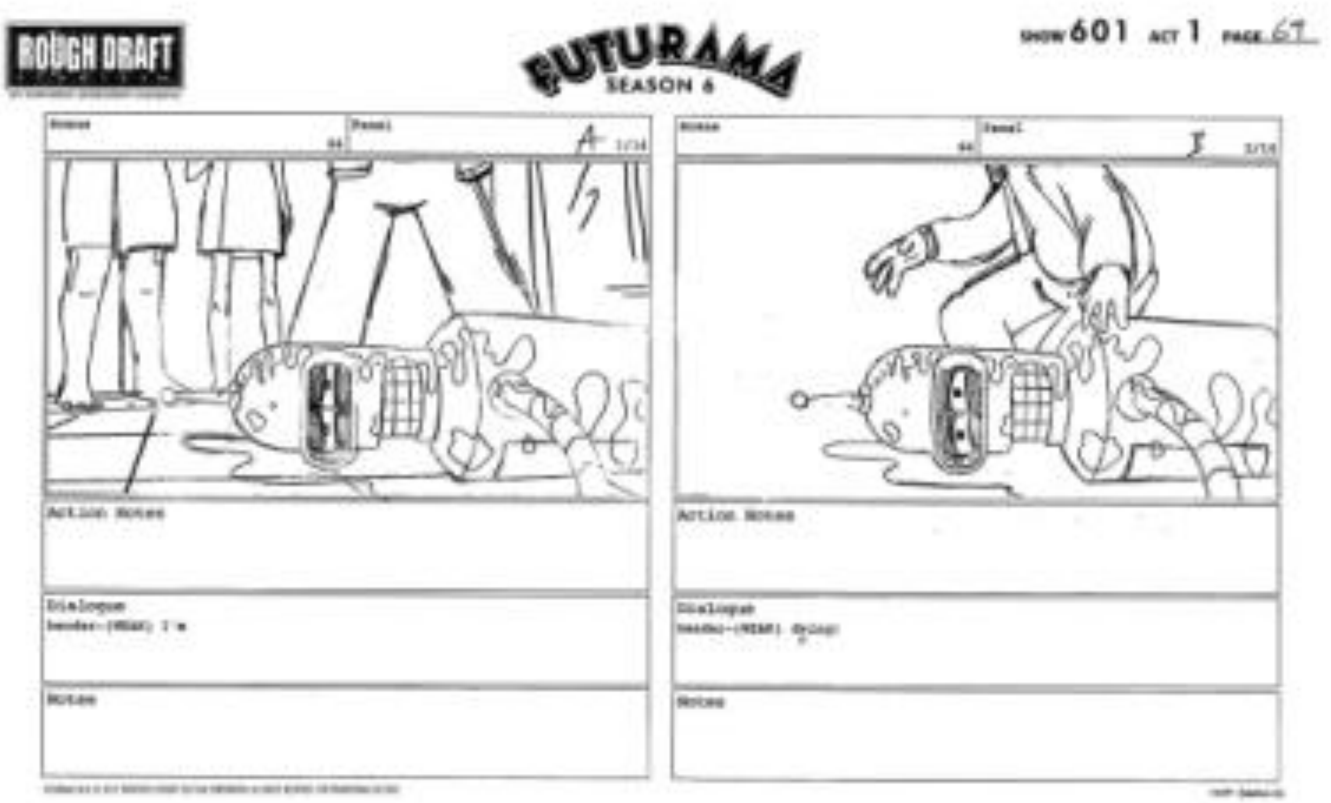
- **Game on!**

DEMO

Attack progress



ACT II: Storyboarding



ROUGH DRAFT

FUTURAMA SEASON 6

SHOW 601 ACT 1 PAGE 67

Scene 44	Panel A 1/14

Action Notes

Dialogue
Bender-(WEAK) I'm

Notes

Scene 44	Panel B 2/14

Action Notes

Dialogue
Bender-(WEAK) dying!

Notes

Act II: Storyboarding

- Storyboards are created to help plan shots for a film

- Simple images illustrate
  - Character positions
  - Camera actions (pan, zoom etc.)
  - What the script intends to depict on the screen

- The de facto storyboarding process was created at the Walt Disney Studio in the early 1930s

- Still widely used today for film and animation projects

App #2: StoryBoard Quick 6

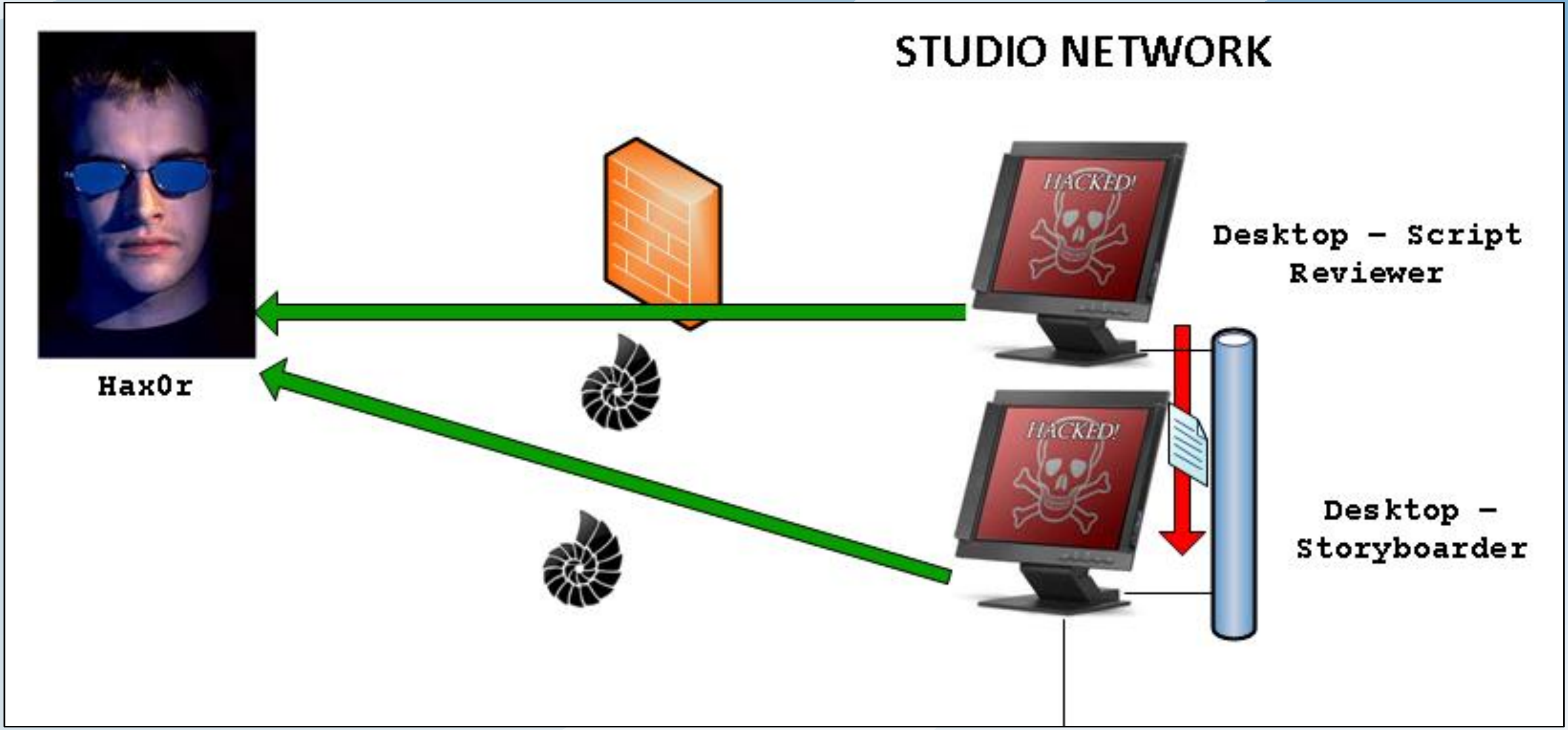
- **Created by PowerProduction Software**
- **Vendor Response: 0/5**
  - Took 2 emails to 3 different addresses to get a (poor) response
  - Refused to respond to me once they figured out I didn’t pay for it
- **Example users:**
  - Ken Harsha (Shrek, The Simpsons, Director of Concept - EA Games)
  - Doug Liman (Mr. & Mrs Smith, Bourne trilogy, Jumper)
- **Other versions of the product are likely also vulnerable**

StoryBoard Quick 6 – The Bug

- **A SBQ6 project is made up of several files, most are XML**
  - A memory corruption vulnerability exists due to insufficient bounds checking for a file name field contained within an XML file defining a frame.
- **Overflowed address is used as the source for a strcpy**
  - The destination is the stack..
  - .. and there's no sauce like stacks of sauce
- **Race condition on app start up = no license required**
  - Also if you start the app with an argument, it loads everything before checking licensing

DEMO

Attack progress



ACT III: 3DFX & Animation

Sure you can stop bullets
But do you have shells?

ACT IV: 3DFX & Animation

- **Software used to render Computer-generated imagery (CGI)**
  - Fires / explosions
  - Bullets dropping out of mid-air
  - Entire movies
- **Used by the majority of productions in some capacity**
- **Typically support scripting languages to automate tasks**
  - VBScript
  - JavaScript
  - Python!
  - Various proprietary scripting languages

The Apps: Maya & Houdini

- **Autodesk – Maya**
  - A world leader for 3D animation, rendering, and effects software
- **Example users:**
  - DreamWorks, Lucas film, Sony Pictures, games studios
- **Side Effects Software – Houdini**
  - Another world leader for 3D animation & Visual effects software
- **Example users:**
  - Pixar, Framestore, Sony Pictures, Asylum, games studios

Feature Details

- Both Maya and Houdini support Python for automation

- No restrictions for built in functions
  - sys, socket – no worries

- Need to coerce a render wrangler into submitting / loading the file.. (or have access to a system that lets you submit them yourself :D)

Houdini Exploitation

- Add your Python as part of a session variable in a .hipnc file

```
<snip>
HouNC
1033600ba004df1dd2f0e36d4a79.hou.sess
ion import subprocess
subprocess.Popen(‘C:\\windows\\system
32\\calc.exe’)
</snip>
```

Maya Exploitation

- All about nodes. Create your own ‘script’ node and set the appropriate attributes

```
<snip>
createNode script –n “naughty”;
setAttr “.b” –type “string”
“callPython \”subprocess\” \”Popen\”
{
\”C:\\windows\\system32\\calc.exe\”
}“;
</snip>
```

DEMO

ACT IV: Render Farms

ACT IV: Render Farms

- **Creating badass 3D animations uses lots of CPU power**
  - Render farms allow animation teams to spread the load across several machines to minimise render time
  - Each farm member will likely be running something like Maya, Houdini or RenderMan
  - Render farm management software dictates which hosts will be rendering what, when and how

App #3: Muster < 6.20

- Created by Virtual Vertex
- Vendor response: 5/5
  - Prompt, friendly response
  - Active interest in fixing the vulnerability
- Can be used to control Maya, 3D Studio Max, Nuke, Combustion, Houdini and many more
- Example users:
  - Battlestar Galactica

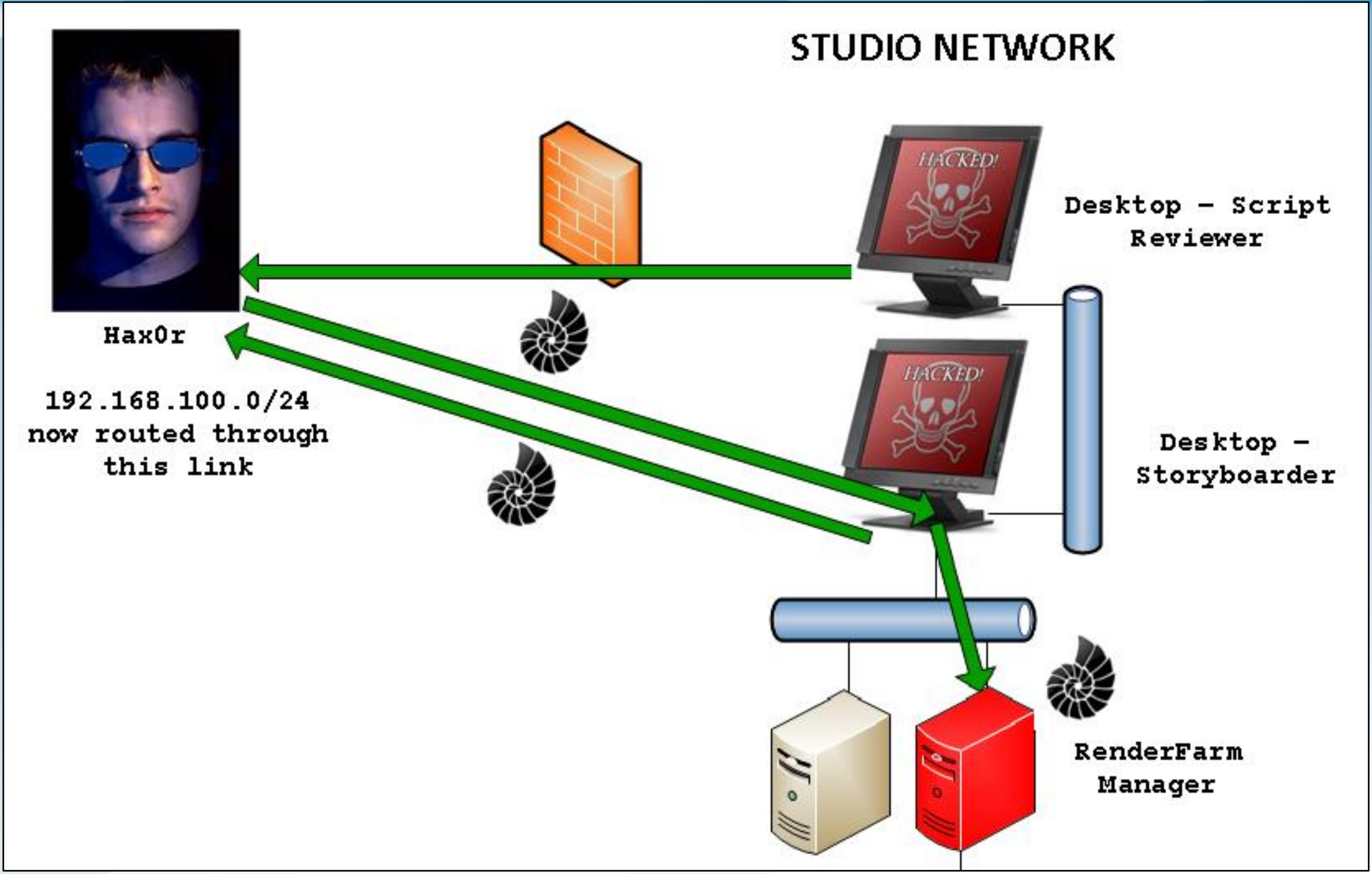
Muster – The Bug

- Muster’s management interface includes a custom built web server, running on port 8690
- Due to a lack of URL input sanitation a directory traversal and arbitrary file read vulnerability exists.

```
GET /a\..\..\asdf.txt HTTP/1.1
Host: musterserver:8690
```

DEMO

Attack progress



ACT V: Editing / Compositing

ACT V: Editing / Compositing

- **Takes places near the end of the filmmaking process**
- **Takes the various clips from the production process**
  - Arranges them on a coherent timeline (most of the time)
  - Makes images from different sources look like they belong together
- **Lets you fix stuff**
  - Colour tweaks for consistency
  - Visual effects
  - Remove camera shakiness

App #4: Media Composer < 5.5.3

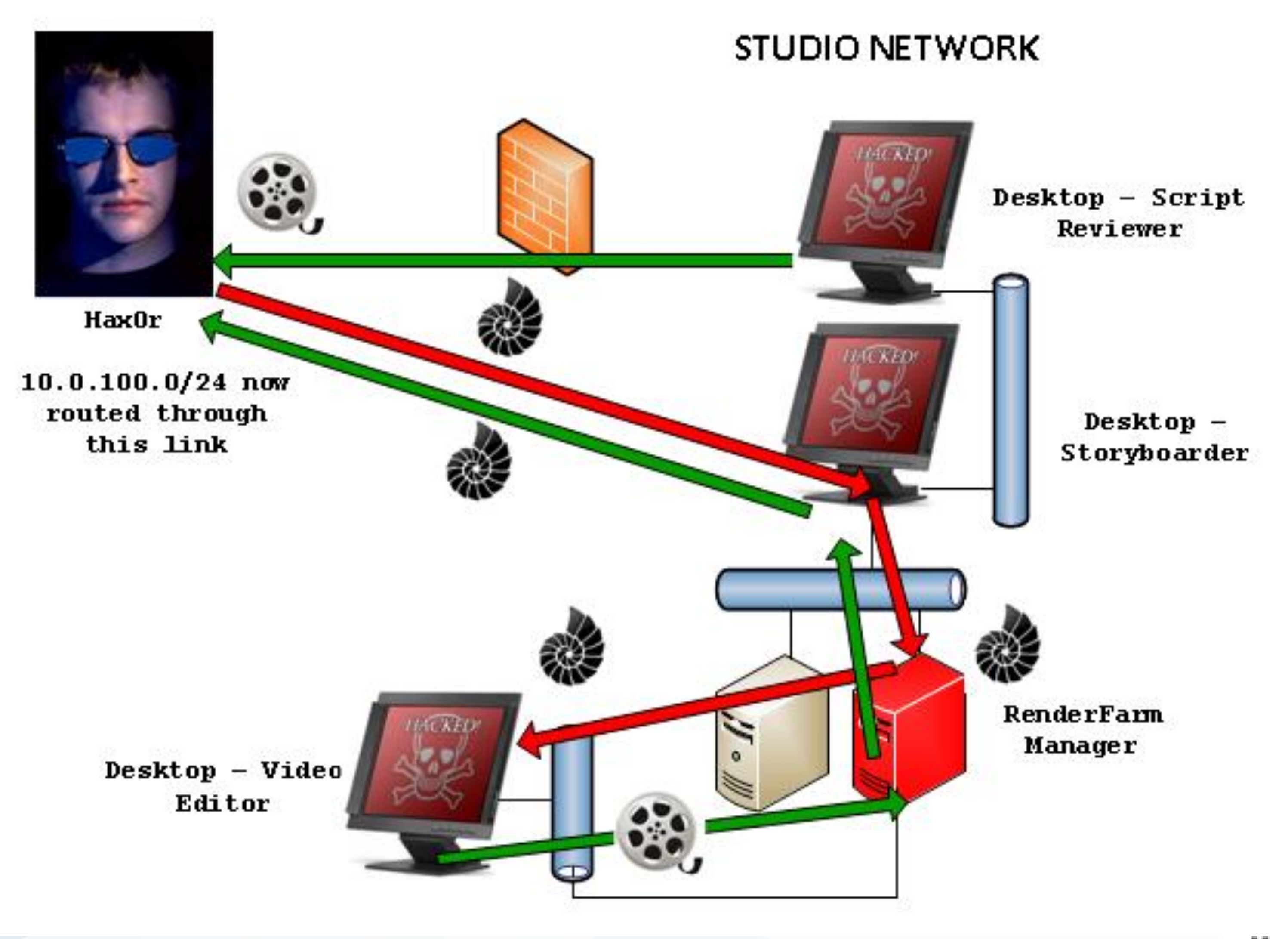
- **Produced by Avid**
  - *'the most trusted video editing system in the entertainment industry'*
- **Vendor response: -1/5**
  - 'Application Security Manager' refuses to take calls or answer emails
  - 'Principal Developer' suggests I ask reception for advice
  - 'Director of Product Management' tells me they're already patching my bugs, before I've told him what they are
    - Is not interested in hearing about where they are either
    - They've released 2 versions since I approached them.. My bugs are still there.
- **Example users:**
  - Iron Man 2, Avatar, Star Trek, CSI, even Coronation St

Avid Media Composer – The Bug

- **Avid MC ships with a network daemon, AvidPhoneticIndexer**
  - This network daemon listens on all interfaces..
  - **Question: ‘WTF happens if I send it 20,000 x “A”s?’**
  - **Answer: Oh you’re kidding me…**
  - **Brutal stack overflow with very little exploit constraints**
    - **The program loads over 30 DLLs**
  - **Gone in 60 Minutes: < 1hr from installation to shell**

DEMO

Attack progress



Conclusion

- **Turns out that Hollywood is very, very hack-able**
  - A multi-billion dollar industry and I didn’t even have to try that hard.
  - Poster child for Same Bug, Different App
    - I could give this talk again in a month with 5 new bugs
  - By chaining these bugs together with a bit of social engineering, you can get to a studio’s crown jewels.
  - I succeeded in keeping myself well entertained for a few months
  - Averaged one shell every 9.6 slides

Roll Credits

- **Hopefully this presentation has lifted the carpet a bit**
  - No studios were harmed in the making of this presentation
  - Advisories and exploit code for today's demonstrations will be released in the near future
  - Thanks for coming along, and enjoy the rest of the con
  - If you have questions, come find me later on!
    - nick.freeman@security-assessment.com
    - @0x7674 on Twitter