Presented by Strom Carlson

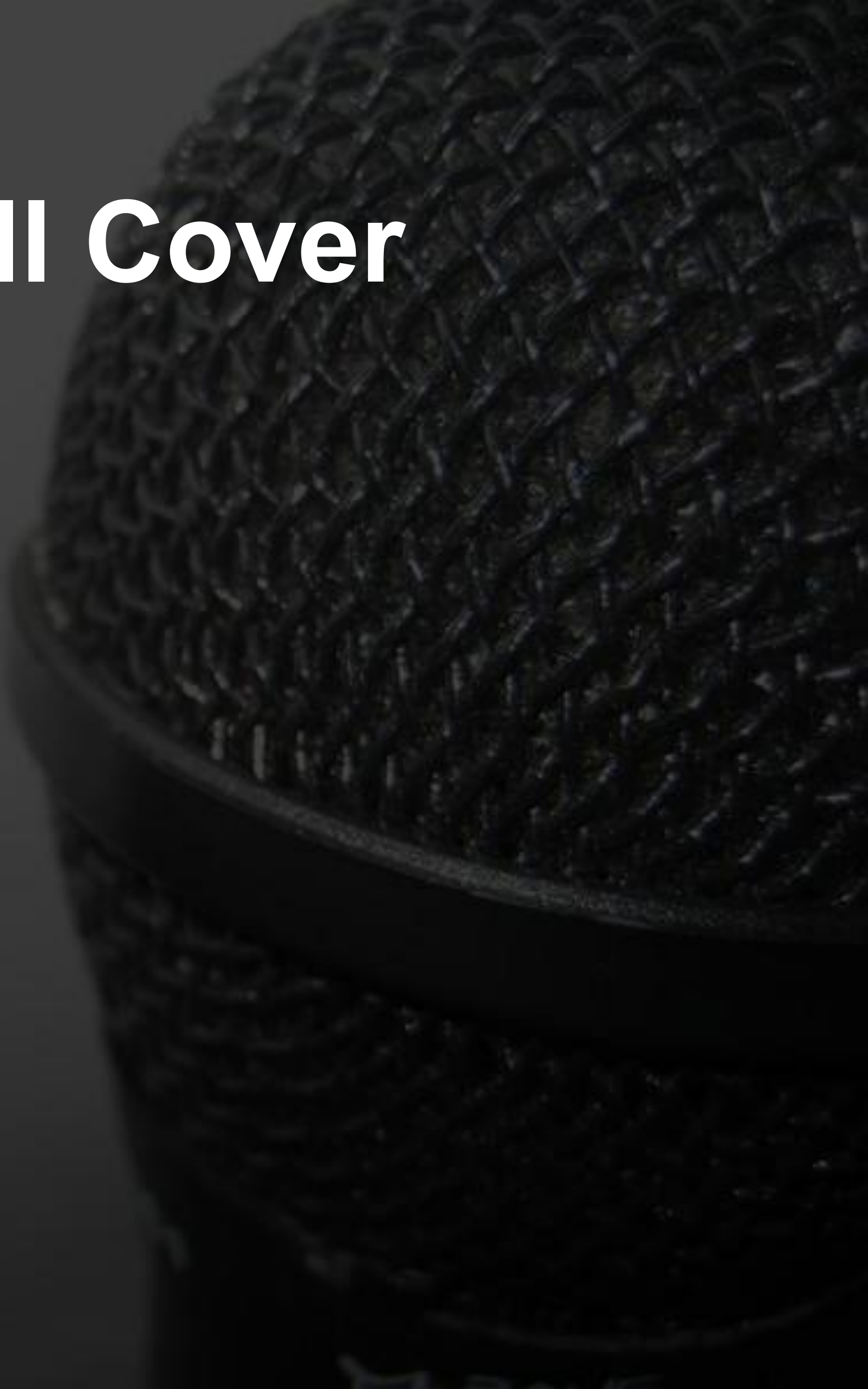
LayerONE

17 May 2008

Who This Talk is For

- Anyone technically proficient who wishes to give talks at information security conventions or at local meetings
  - Nubs
  - Experienced Speakers
  - Everyone in between

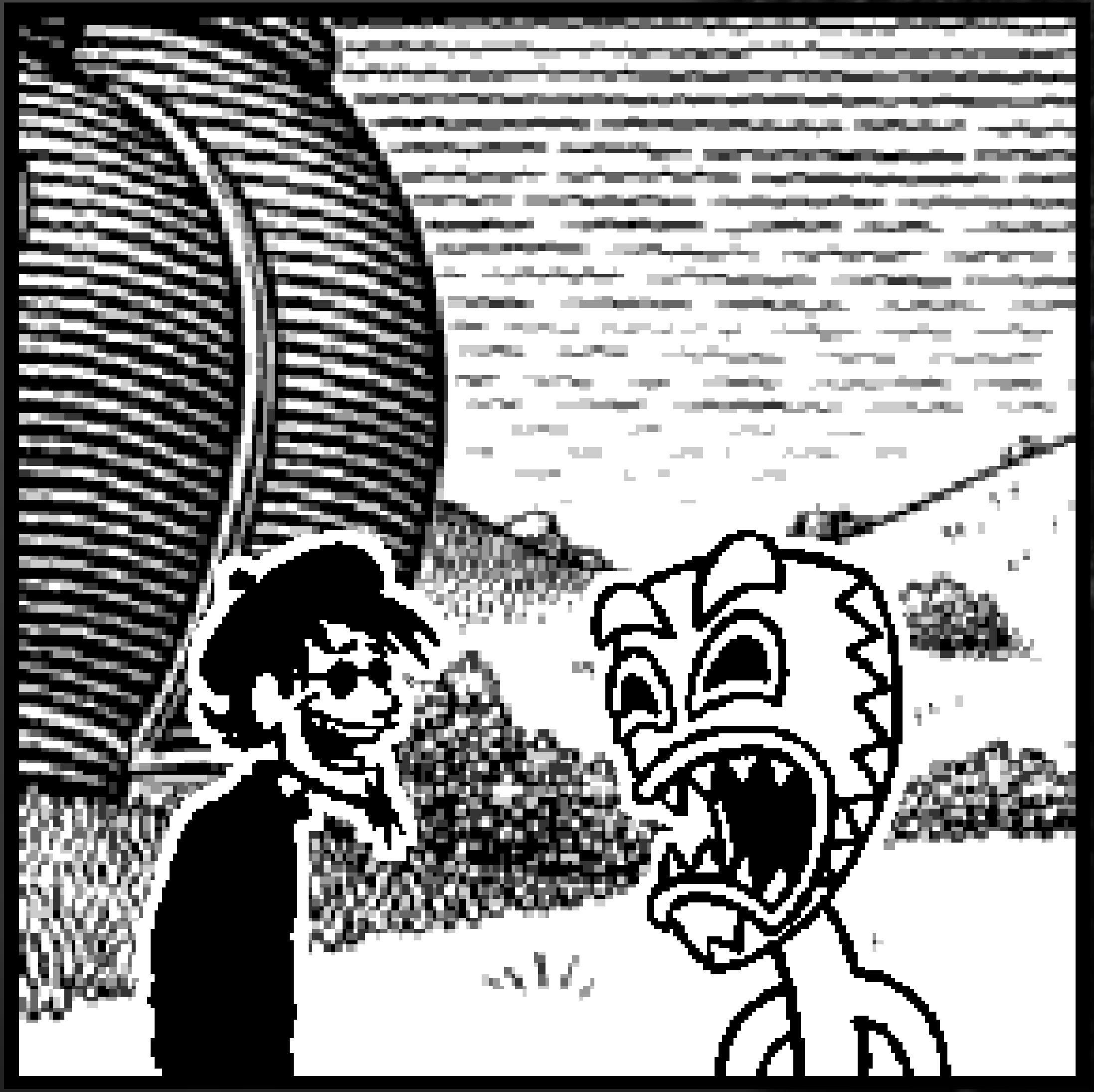
What We’ll Cover



- Planning the talk
- Preparing the talk
- Giving the talk
- After the talk

PLANNING THE TALK

Know Your Audience



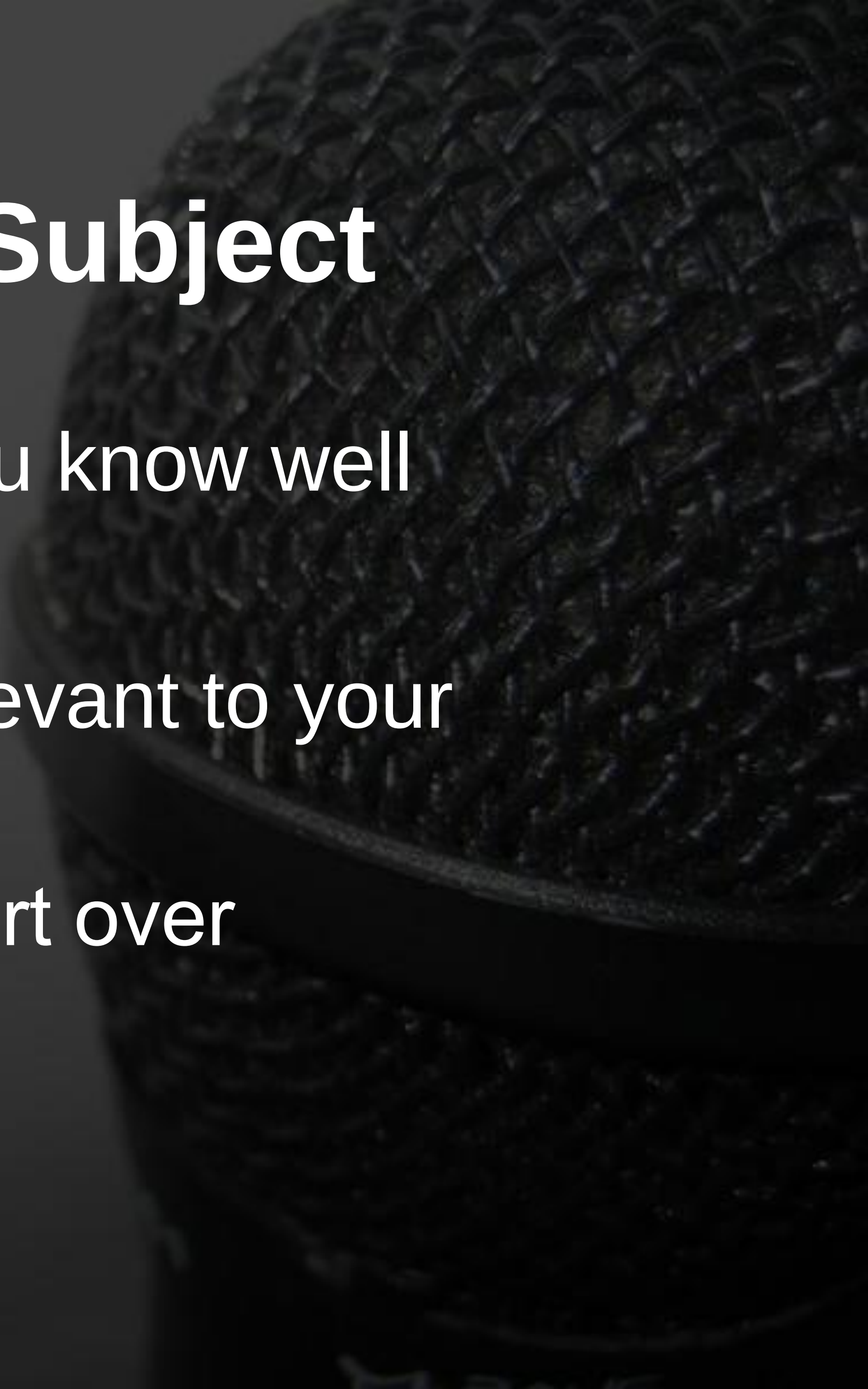
Know Your Audience

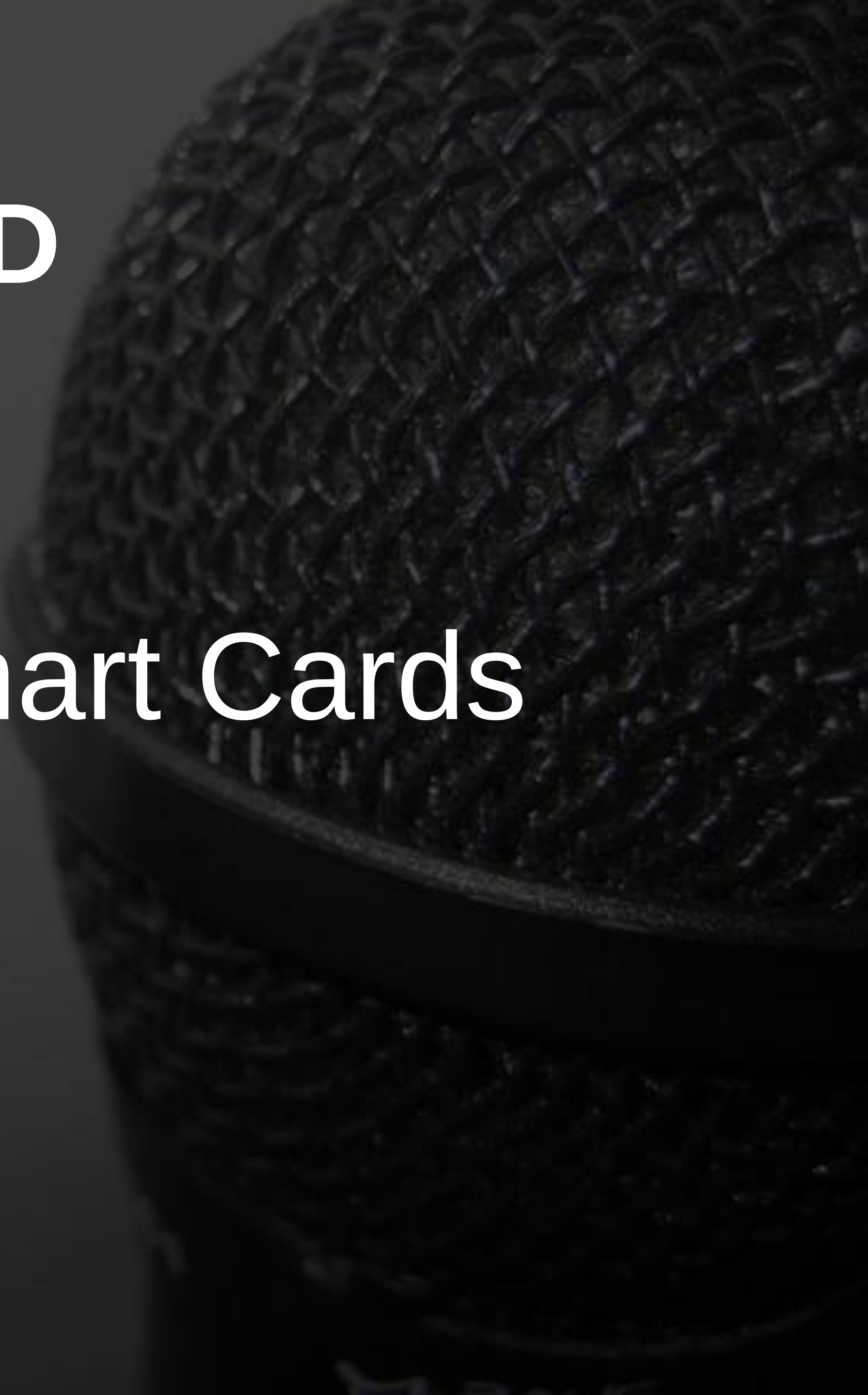
Know Your Audience

Know Your Audience

Select a Subject

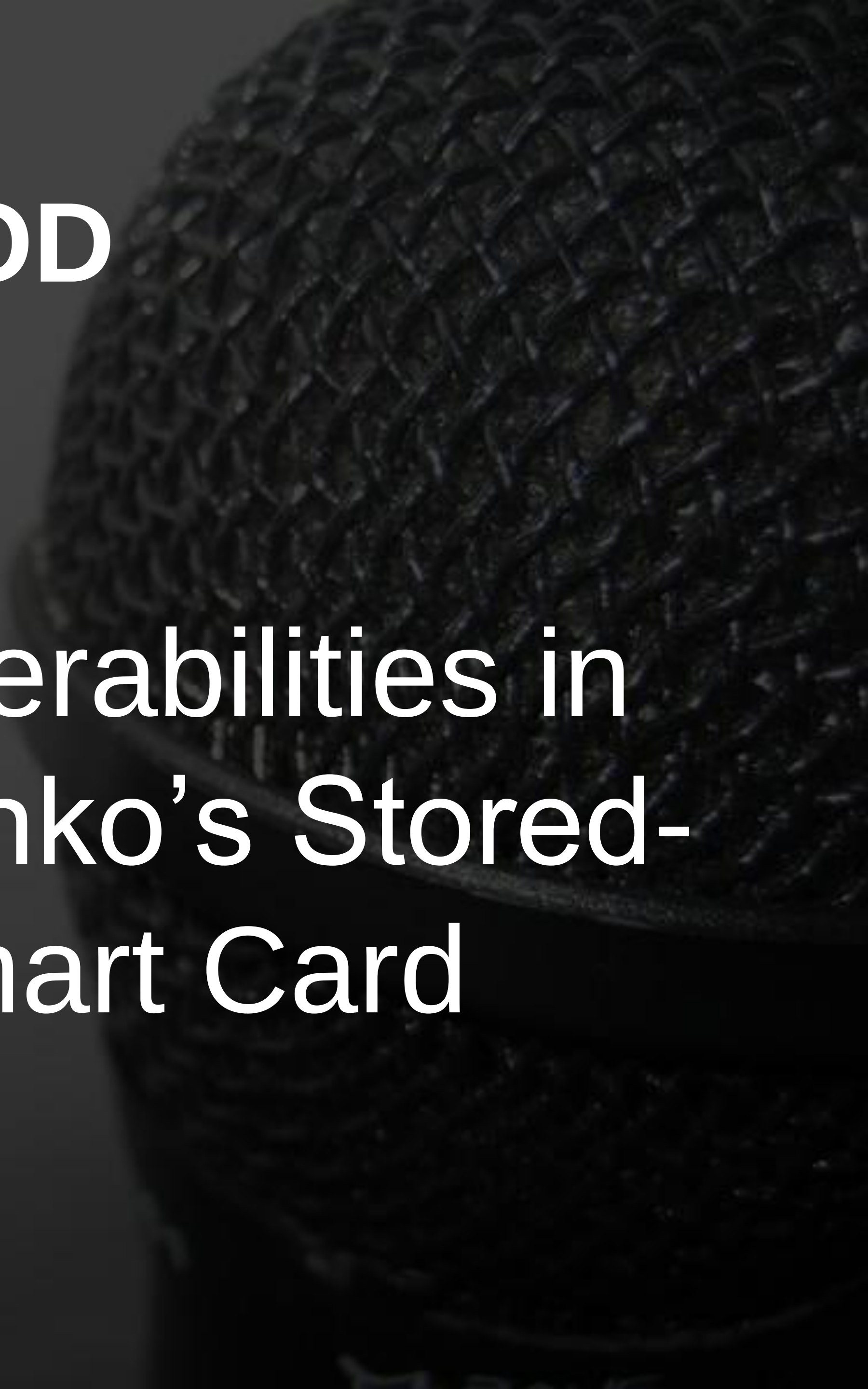
- Choose a subject you know well
- Narrow your focus
- Make the subject relevant to your audience
- Don’t be afraid to start over





BAD

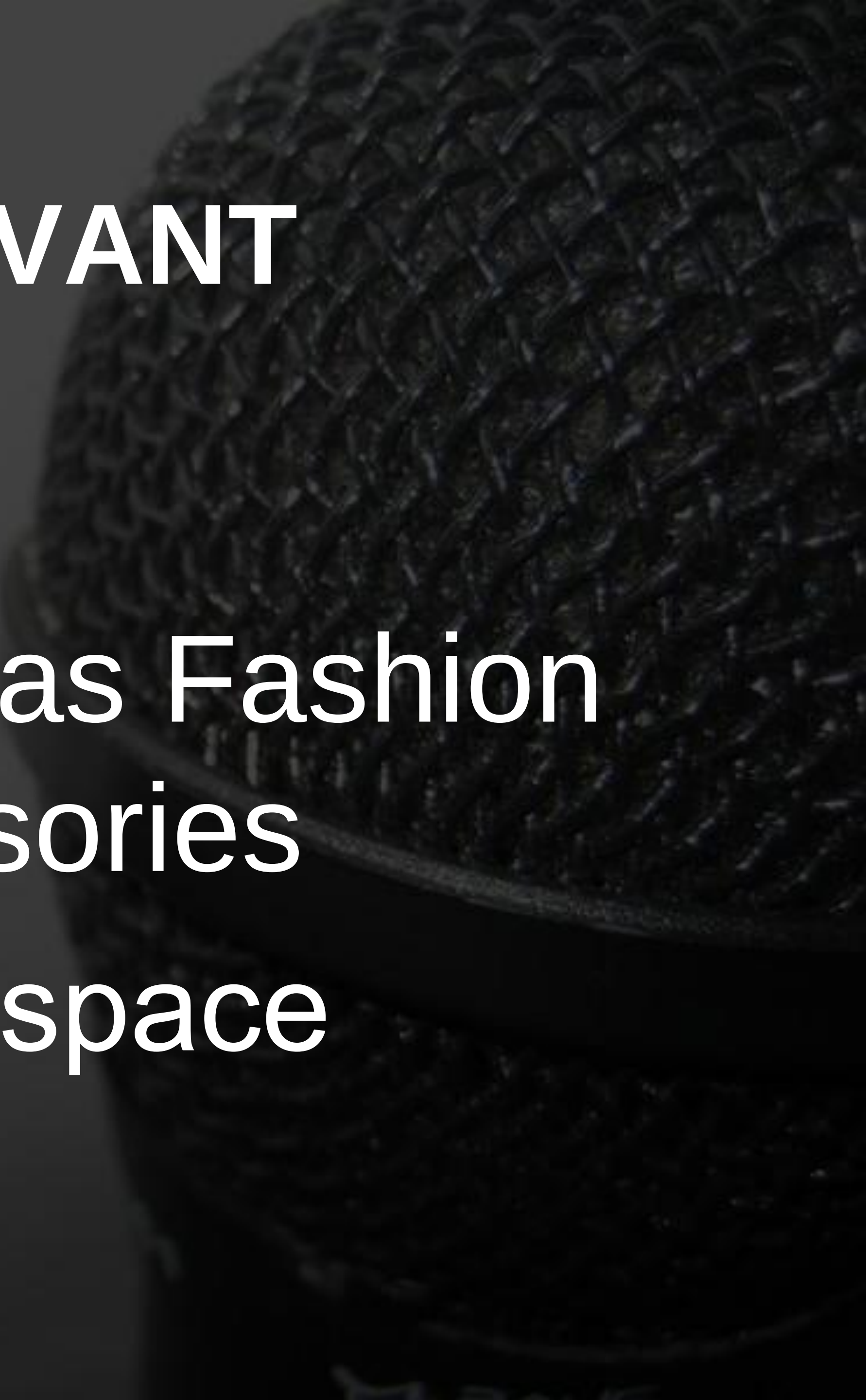
Hacking Smart Cards



GOOD

Security Vulnerabilities in the FedEx Kinko's Stored-Value Smart Card

IRRELEVANT

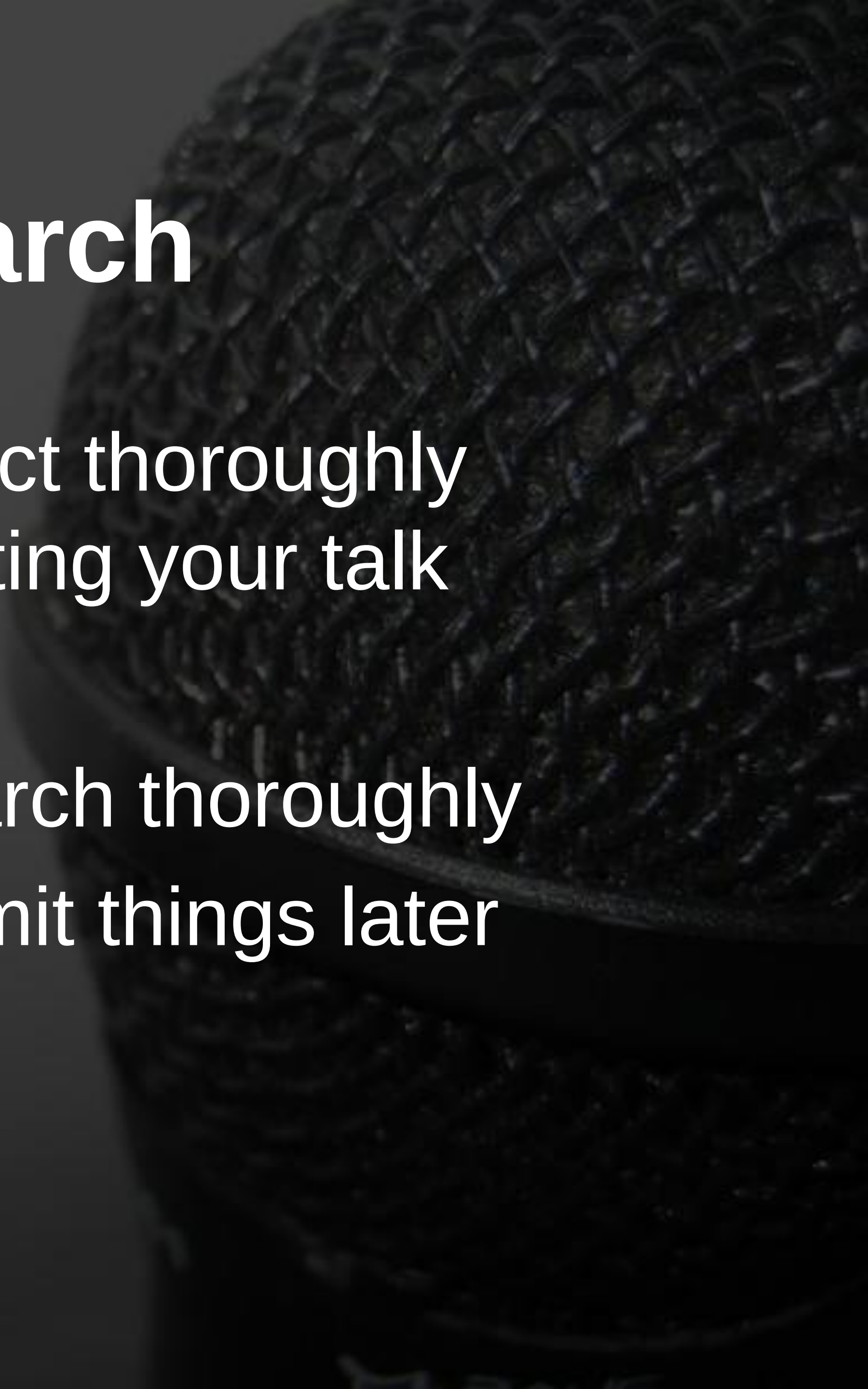


Smart Cards as Fashion Accessories

…on Myspace

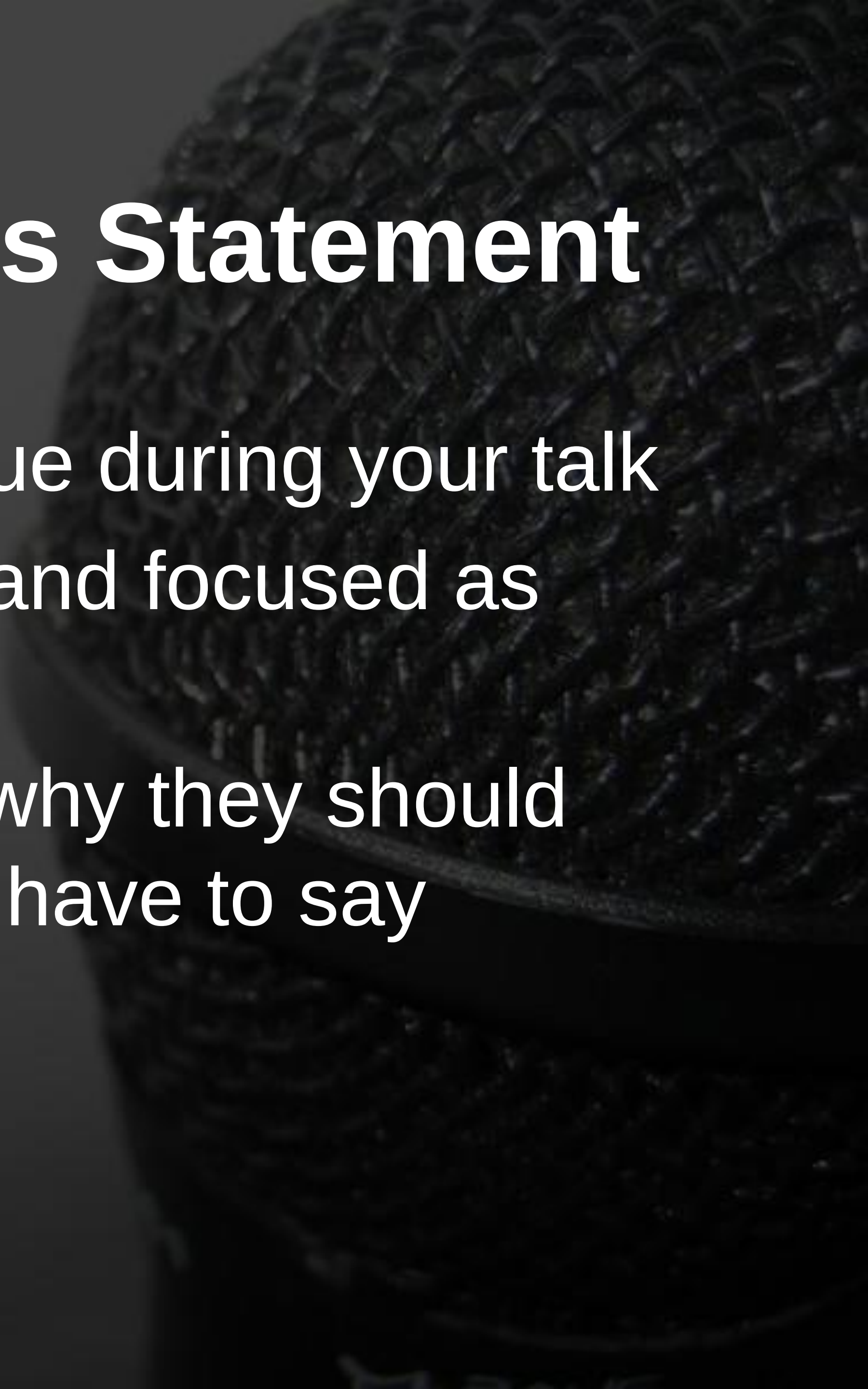
Research

- Research your subject thoroughly before you begin writing your talk
- Take copious notes
- Document any research thoroughly
- You can (and will) omit things later

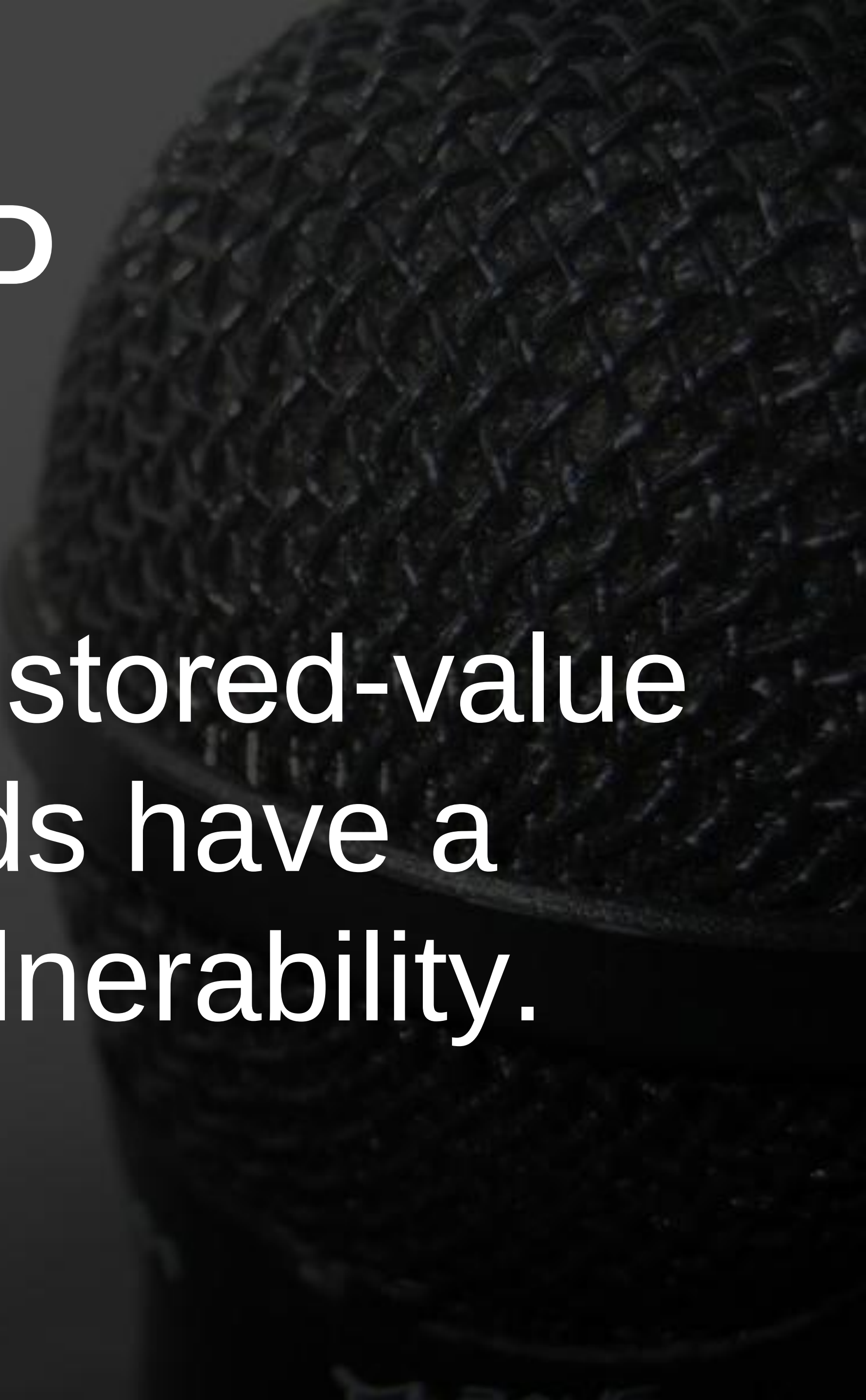


Select a Thesis Statement

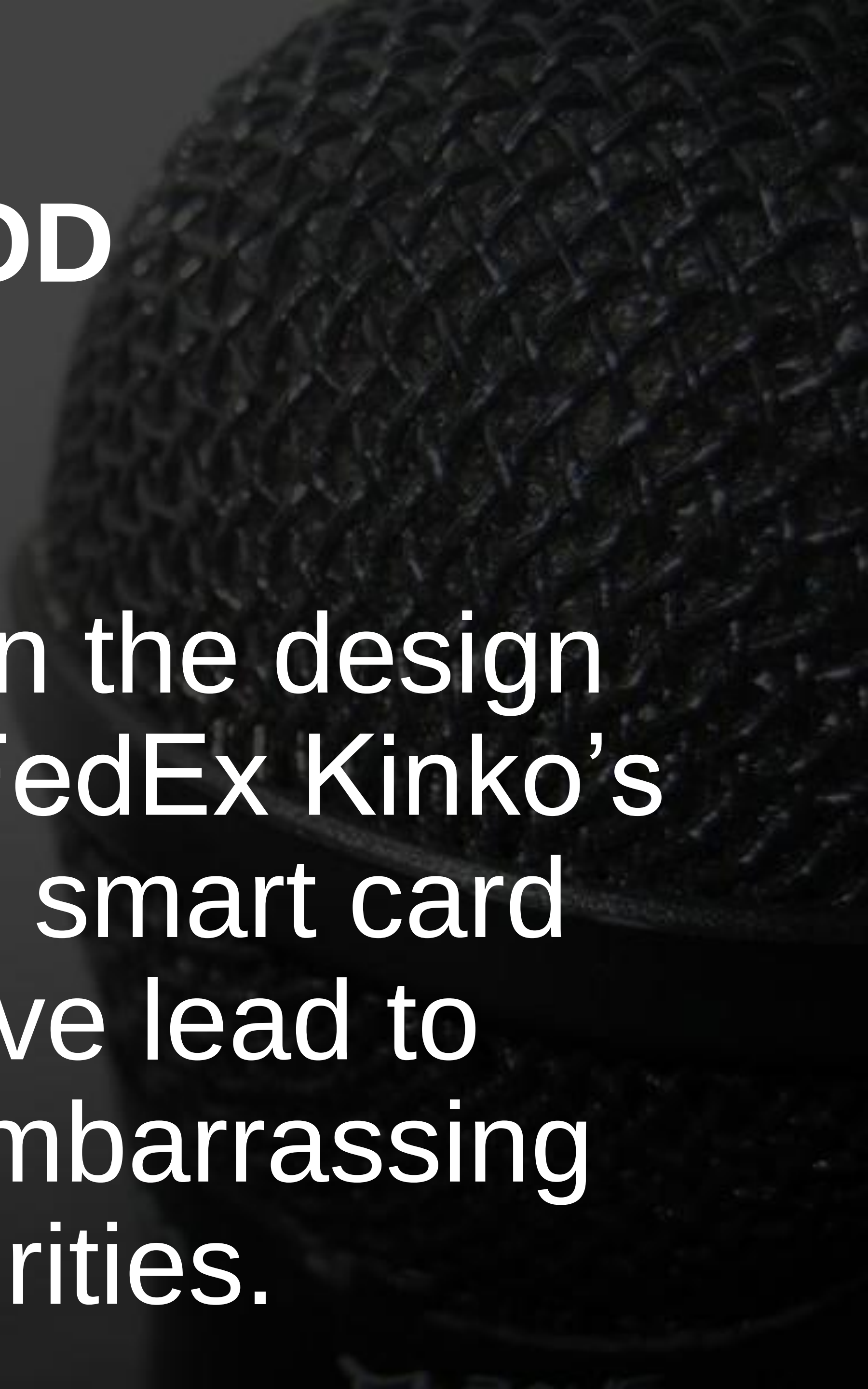
- A single claim to argue during your talk
- Must be as relevant and focused as your chosen subject
- Tells your audience why they should care about what you have to say



BAD



FedEx Kinko’s stored-value smart cards have a security vulnerability.

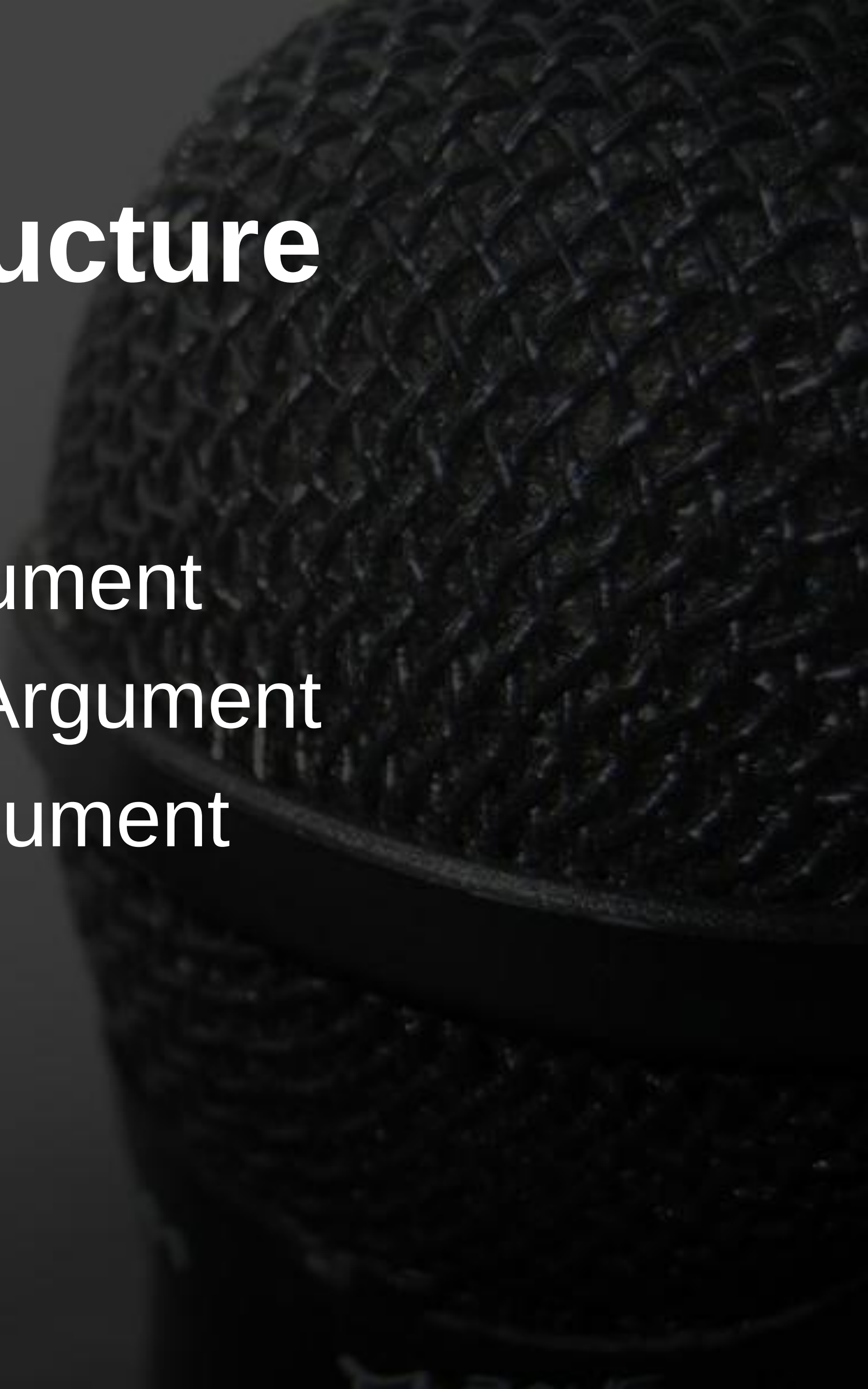


GOOD

Poor choices in the design phase of the FedEx Kinko’s stored value smart card system have lead to pervasive, embarrassing insecurities.

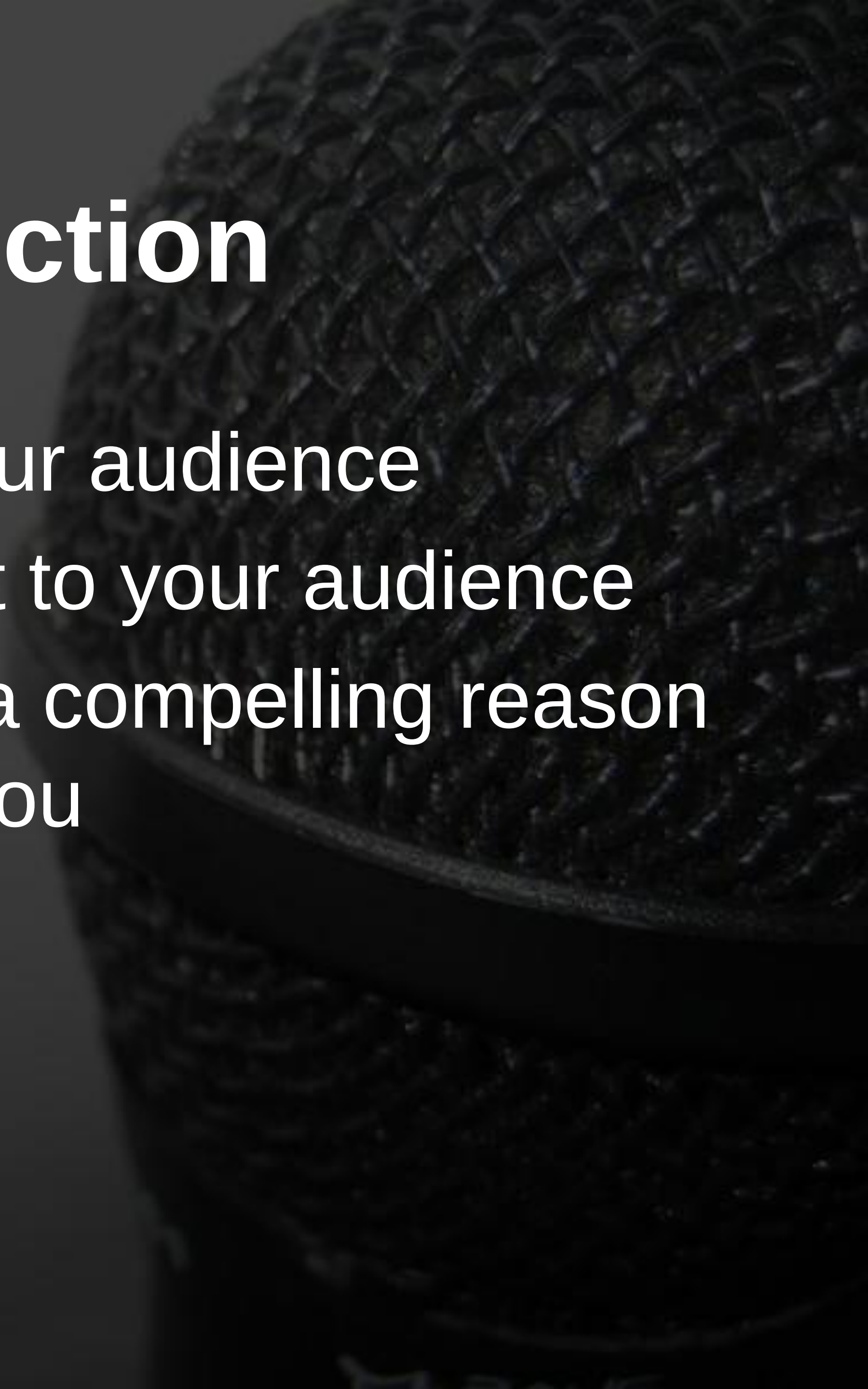
Talk Structure

- Introduction
- First Supporting Argument
- Second Supporting Argument
- Third Supporting Argument
- Conclusion



Introduction

- Make friends with your audience
- Introduce the subject to your audience
- Give your audience a compelling reason to keep listening to you

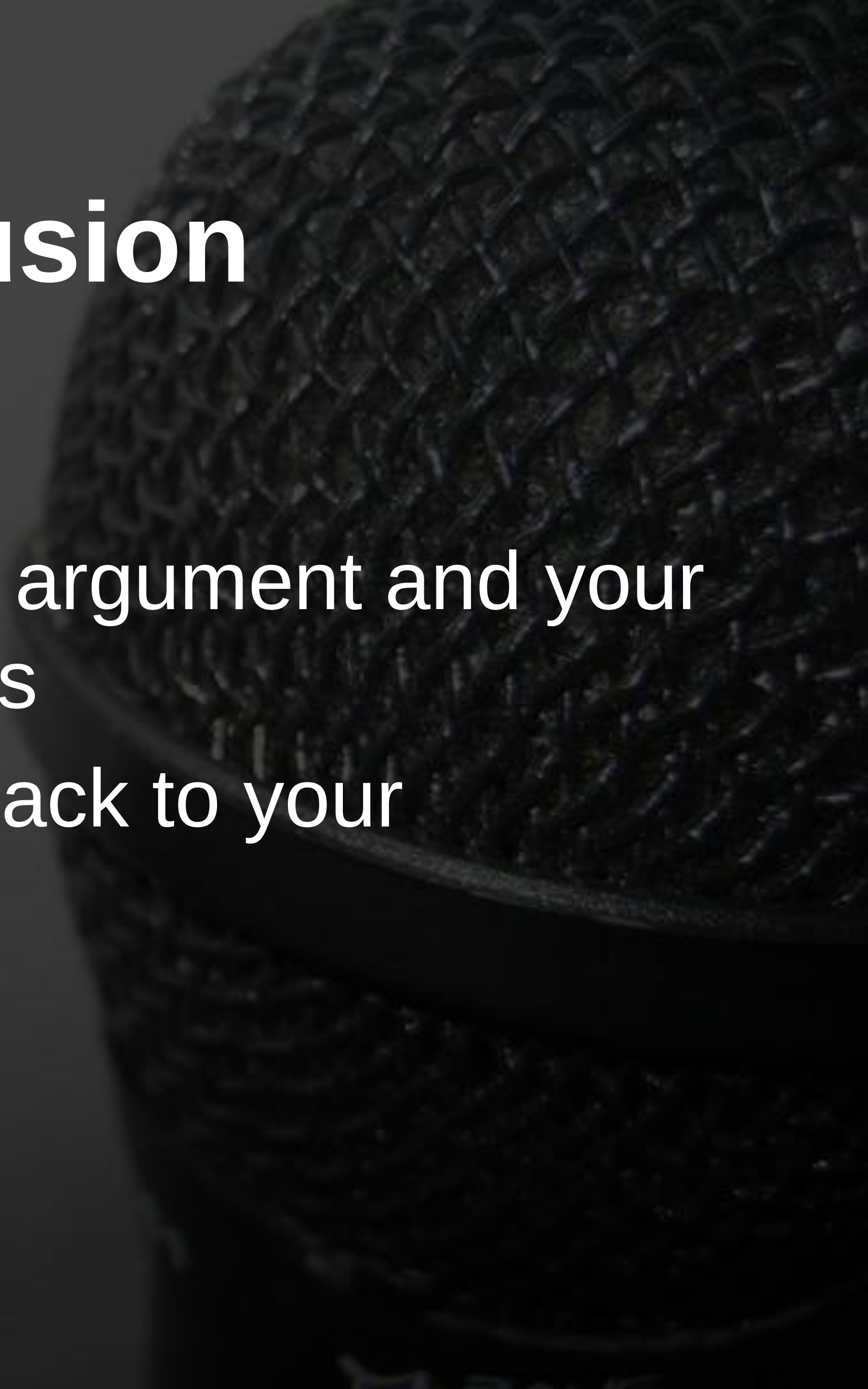


Supporting Arguments

- Smaller, more focused versions of your primary argument
- These must support and reinforce your primary argument
- You should have at least three but no more than five supporting arguments

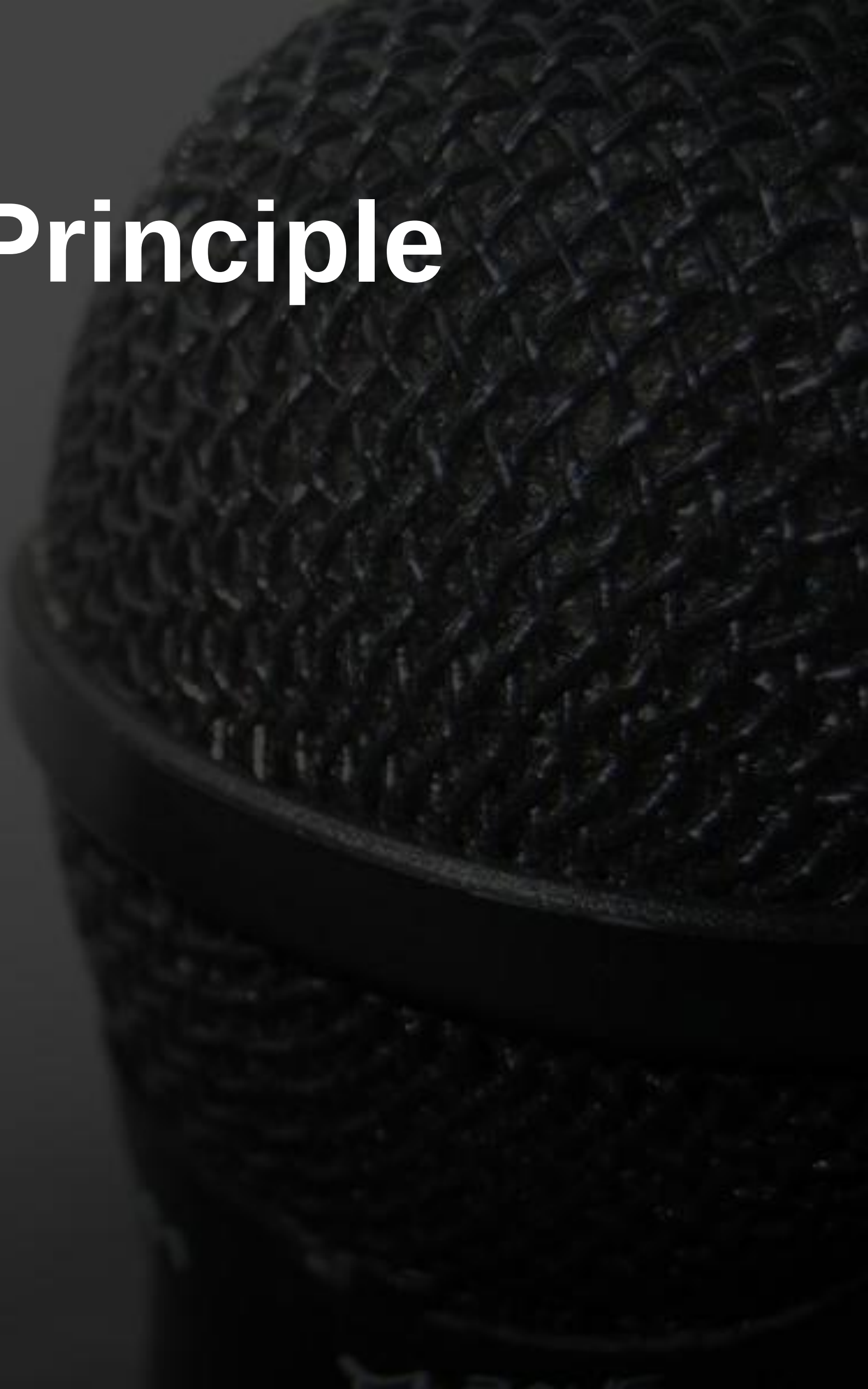
Conclusion

- Wrap up the talk
- Review your primary argument and your supporting arguments
- Make a connection back to your introduction

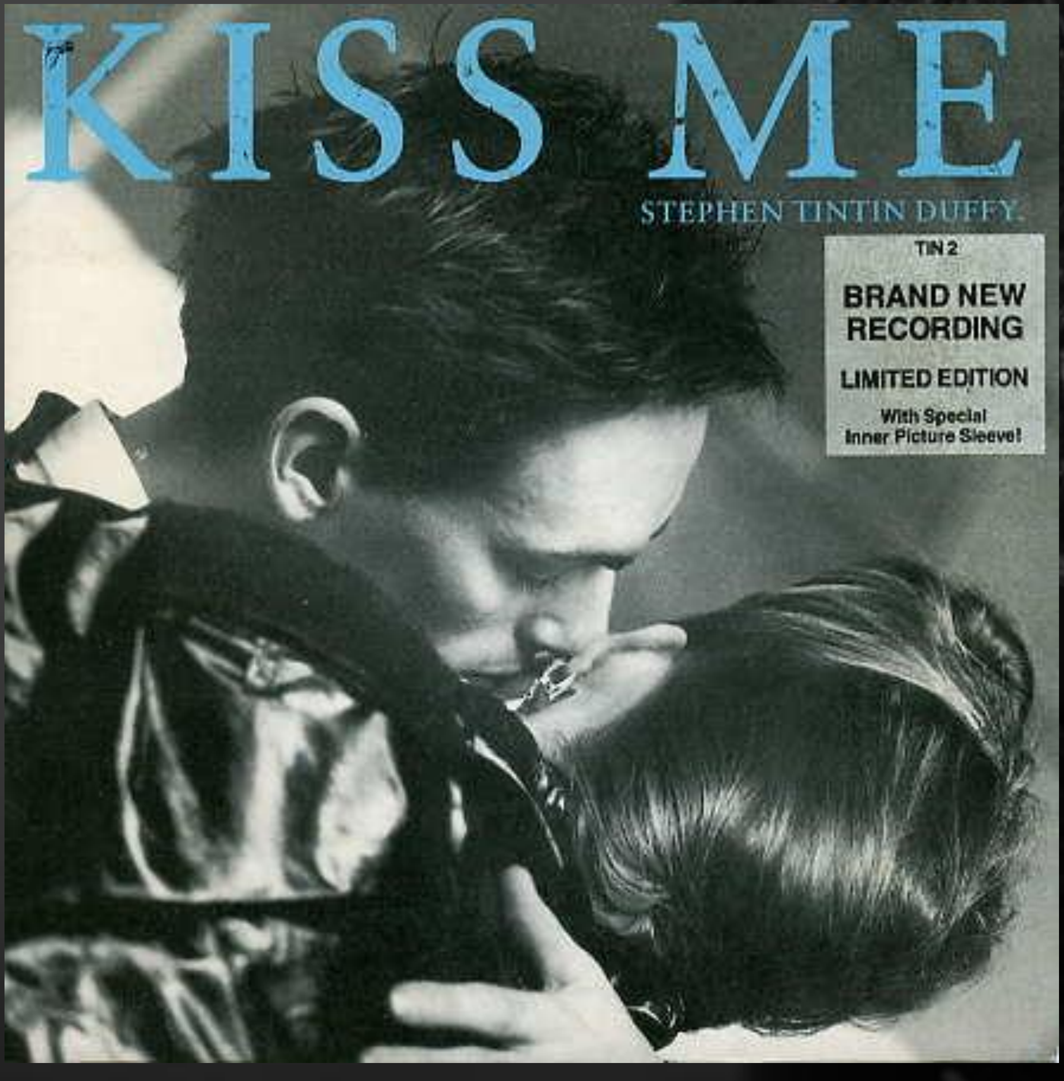


PREPARING THE TALK

The KISS Principle

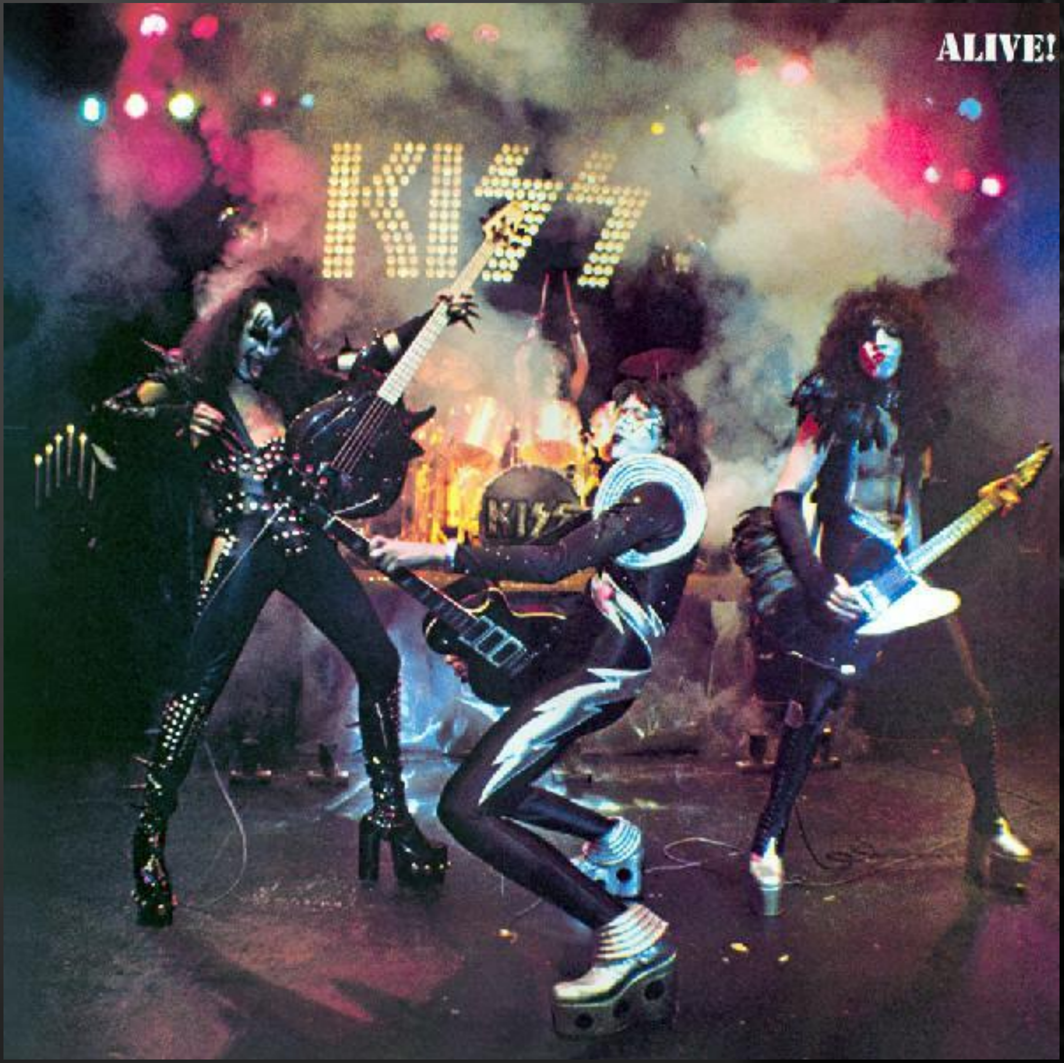


The KISS Principle

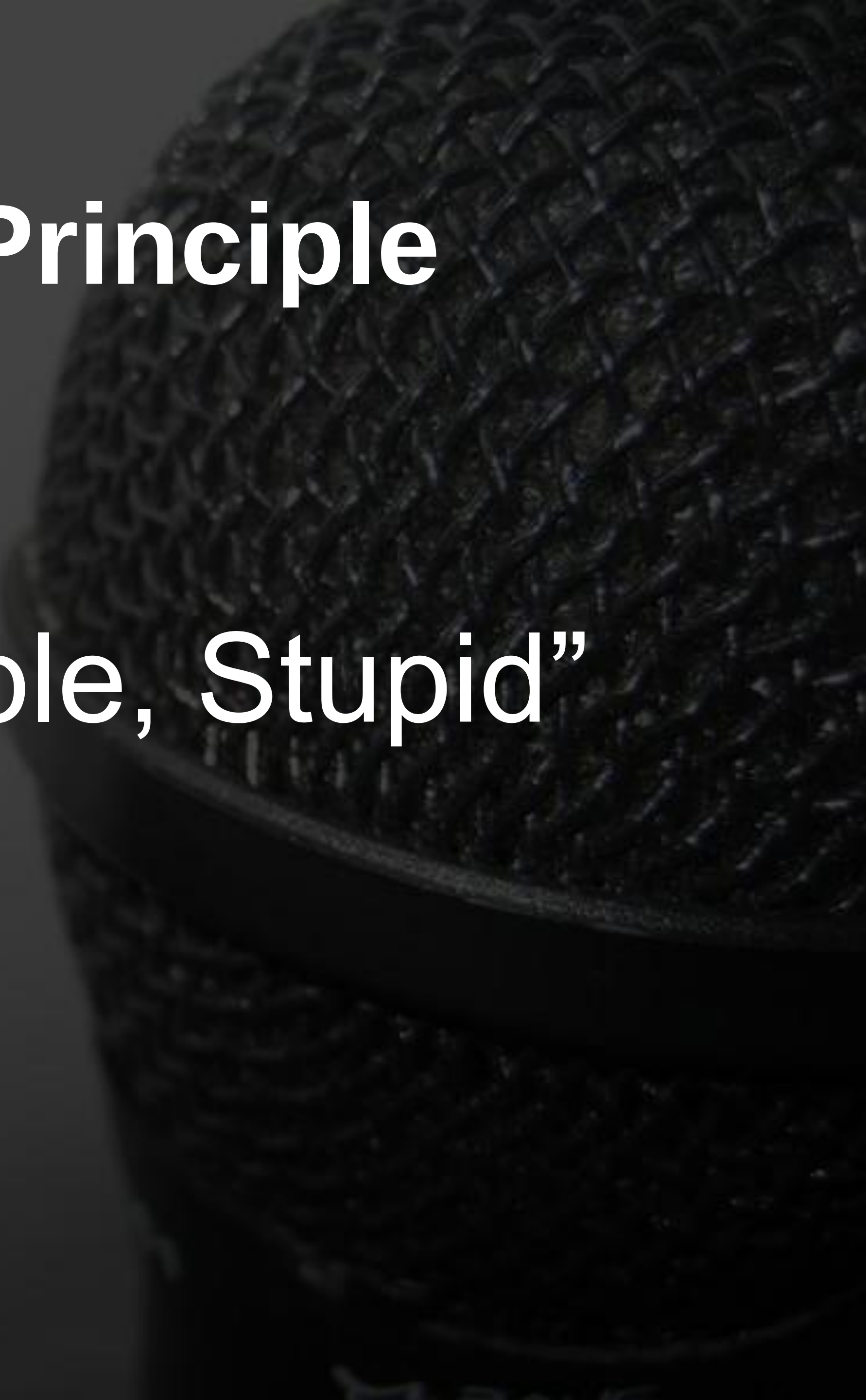


The KISS Principle

The KISS Principle



The KISS Principle

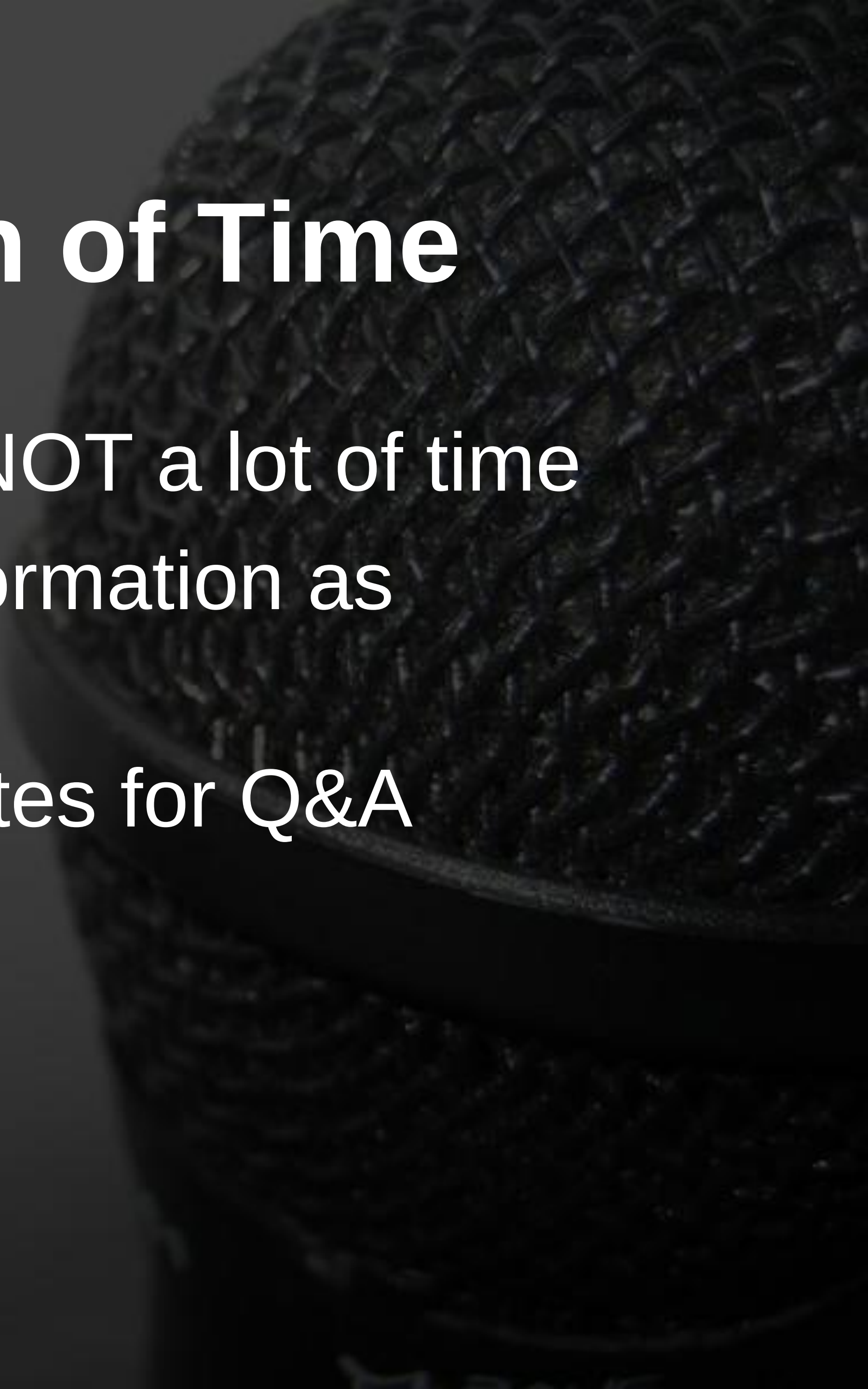


“Keep It Simple, Stupid”

Filter Your Research

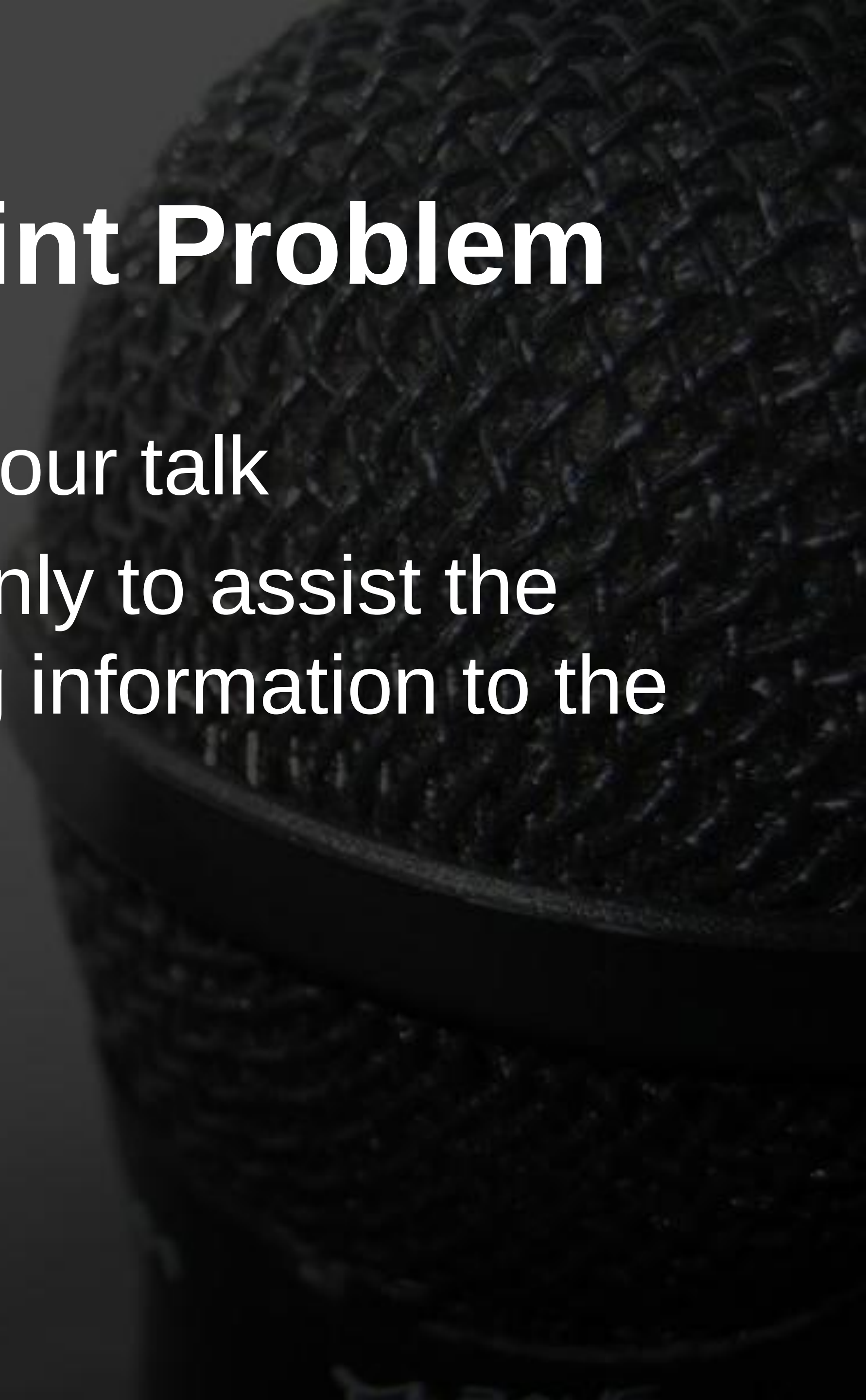
A Question of Time

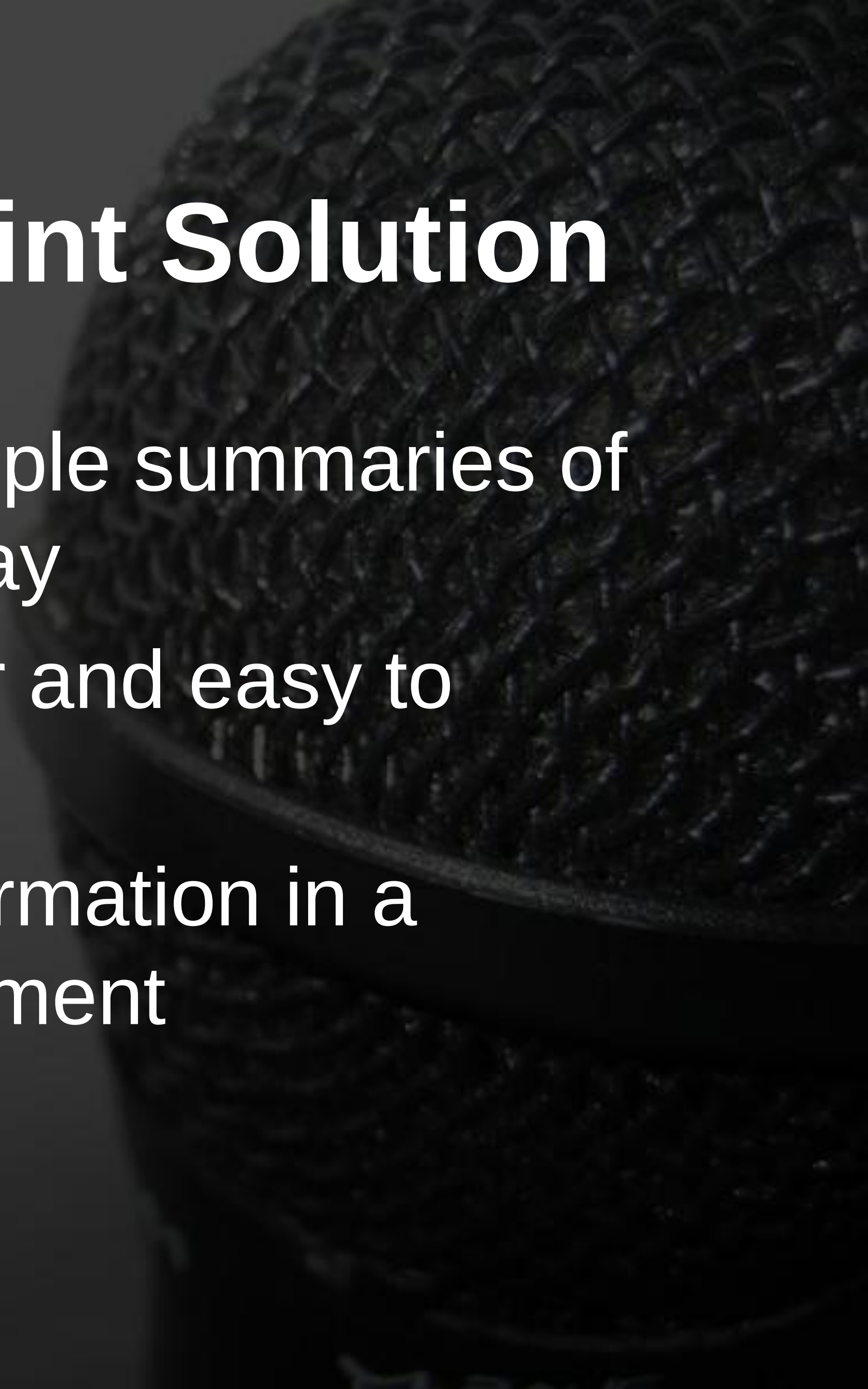
- 20 or 50 minutes is NOT a lot of time
- Discard as much information as possible
- Save at least 5 minutes for Q&A



The PowerPoint Problem

- PowerPoint is NOT your talk
- PowerPoint serves only to assist the speaker in conveying information to the audience





The PowerPoint Solution

- Keep your slides simple summaries of what you intend to say
- Make diagrams clear and easy to understand quickly
- Provide detailed information in a supplementary document

BAD SLIDES

VIEWER DISCRETION IS ADVISED

Countermeasures

- Assume an intelligent and well informed adversary
- Design system with malicious data in mind
- Assume your tool (and source) are in the hands of an attacker
- Train users to be alert for manipulation
- Validate data
- Assume your infrastructure will be attacked
- In worst case, assume your attacker has knowledge about specific users
- Design visualizations/vis systems that are resistant to attack
- If you can’t defeat attack, at least facilitate detection
- Use intelligent defaults
- Provide adequate customization

Code templates common in GCC-3

```
                 sendmail-8.13.5-1.i386.rpm                     sendmail-8.13.4-2.i386.rpm

                 _init:                                         _init:
        push     ebp                                   push     ebp
        mov      ebp,esp                               mov      ebp,esp
        sub      esp,0x8                               sub      esp,0x8
        call     9f08 (chroot@plt+0x4c)                call     9f08 (__memmove_chk@plt+0x48)
        call     9f88 (chroot@plt+0xcc)                call     9f88 (__memmove_chk@plt+0xc8)
        call     991bc (sleep+0x2b82)                  call     9a048 (sleep+0x2b96)
        leave                                          leave
        ret                                            ret
                 SSL_CTX_set_tmp_                               SSL_CTX_set_tmp_
                 rsa_calback@plt-0x10:                          rsa_callback@plt-0x10:
        push     DWORD PTR [ebx+4]                     push     DWORD PTR [ebx+4]
        jmp      DWORD PTR [ebx+8]                     jmp      DWORD PTR [ebx+8]
        add      BYTE PTR [eax],al                     add      BYTE PTR [eax],al
                 SSL_CTX_set_tmp_                               SSL_CTX_set_tmp_
                 rsa_calback@plt:                               rsa_callback@plt:
        jmp      DWORD PTR [ebx+12]                    jmp      DWORD PTR [ebx+12]
        push     0x0                                   push     0x0
        jmp      8c3c (_init+0x18)                     jmp      8c20 (_init+0x18)
                 ...                                            …
```

Typical GCC-3 entry point

GCC-3 external symbol resolutions

Most common GCC-3 external call invocation

Stepping through the data

```
11111111
11111111
11111111
11111111
11111111
00000000
00000000
00000000  [END OF MAIN MEMORY]

0

10001100  READ SECURITY MEMORY
11111111  FF
11111111  FF
11110000
00000000
00000000
00000000
00
10011100  UPDATE SECURITY MEMORY
00000000
01100000
10000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
```

```
00000000
00000000
00000000
00000000
00000
11001100  COMPARE VERIFICATION DATA
10000000  01
XXXXXXXX  XX
1000
11001100  COMPARE VERIFICATION DATA
01000000  02
XXXXXXXX  XX
1000
11001100  COMPARE VERIFICATION DATA
11000000  03
XXXXXXXX  XX
1000
10011100  UPDATE SECURITY MEMORY
00000000
11100000
10000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
```

```
00000000
00000000
00000
10001100  READ SECURITY MEMORY
11111111
11111111
11110000


....


WHY AM I STILL ANALYZING THIS?
```

```
           )      WHY HELLO THERE !!!!!!!!
          (.)     I'M THE INFORMATION SECURITY
          .|.     RESPONSIBILITY CUPCAKE
          17J     AND IT'S MY JOB TO TELL YOU
          | |        THAT YOU ARE GOING TO HAVE TO
      _.--| |--._      FIGURE OUT THE SECURITY CODE
   .-';  ;`-'& ; `&.      FOR YOURSELF !!!!!!!!!
  & &  ;  &   ; ;   \
  \      ;    &   &_/
   F""""---...---""""J
   | | | | | | | | |
   J | | | | | | | F      ALSO: DEAD HOOKERS
    `---.|.|.|.---'
```

Let's talk about Vulnerability Statistics

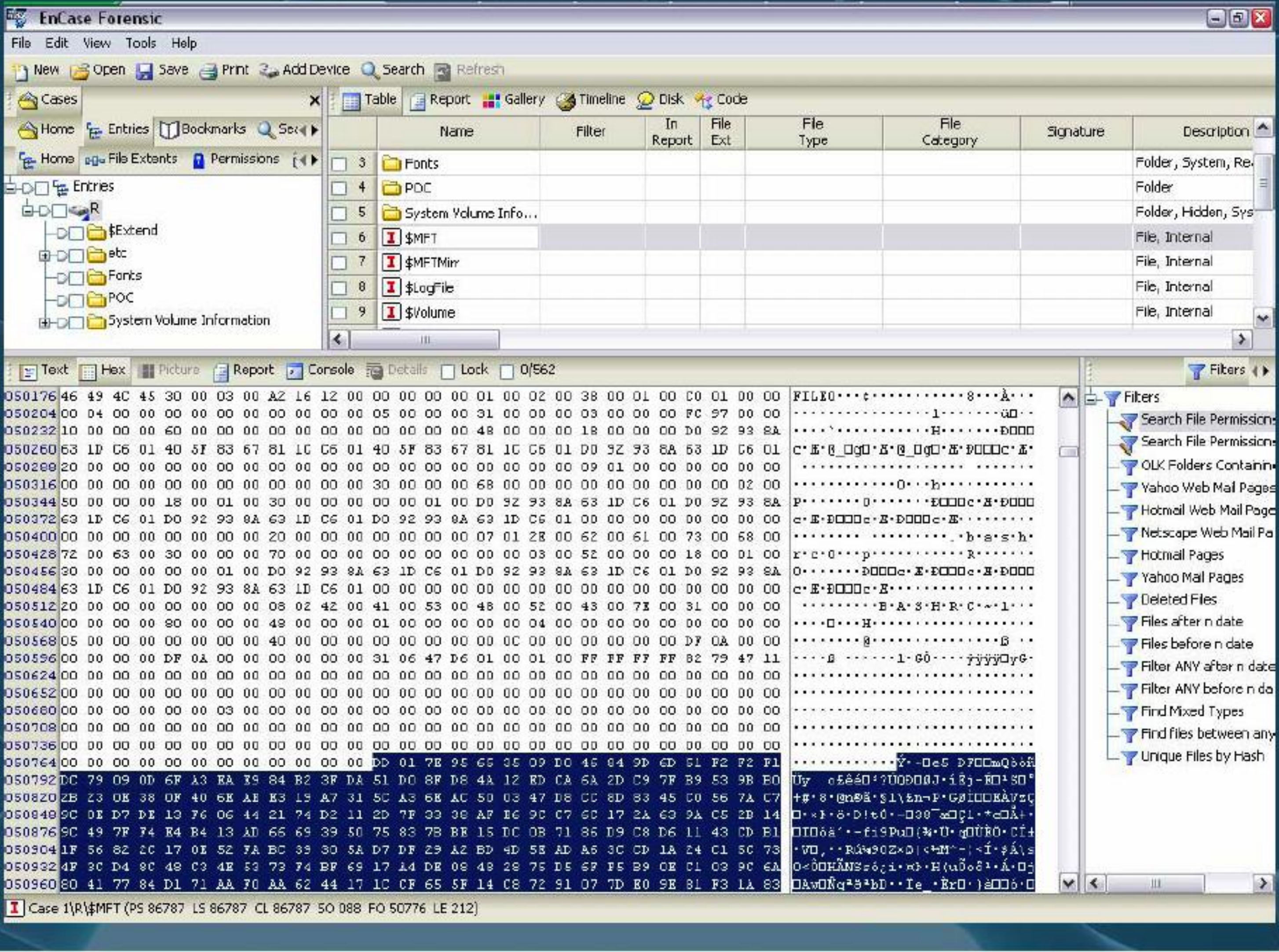
- Vulnerability stats are (generally) an artifact of tactical coding errors, not bigger problems
- "In the last year we cut the number of patches we released from 35 to 12"
  - – Well, if you're rolling up many vuln fixes to one patch, it doesn't count
  - – Further, the impact from the vulns may vary as well
  - – Not just an MS problem… MDKSA-2004-037
- Whose code was the vuln in?
  - – Kernel? Integrated Application? Third Party?

The SSN

SSN Area Numbers

001 thru 003 - New Hampshire
004 thru 007 - Maine
008 thru 009 - Vermont
010 thru 034 - Massachusetts
035 thru 039 - Rhode Island
040 thru 049 - Connecticut
050 thru 134 - New York
135 thru 158 - New Jersey
159 thru 211 - Pennsylvania
212 thru 220 - Maryland
221 thru 222 - Delaware
223 thru 231 - Virginia
232 thru 236 - West Virginia
237 thru 246 - North Carolina
247 thru 251 - South Carolina
252 thru 260 - Georgia
261 thru 267 - Florida
268 thru 302 - Ohio
303 thru 317 - Indiana
318 thru 361 - Illinois
362 thru 386 - Michigan
387 thru 399 - Wisconsin
400 thru 407 - Kentucky
408 thru 415 - Tennessee
416 thru 424 - Alabama
425 thru 428 - Mississippi
429 thru 432 - Arkansas
433 thru 439 - Louisiana
440 thru 448 - Oklahoma
449 thru 467 - Texas
468 thru 477 - Minnesota
478 thru 485 - Iowa
486 thru 500 - Missouri
501 thru 502 - North Dakota
503 thru 504 - South Dakota
505 thru 508 -Nebraska
509 thru 515 - Kansas
516 thru 517 - Montana
518 thru 519 - Idaho
520 ONLY - Wyoming
521 thru 524 - Colorado
525 AND 585 - New Mexico
526 thru 527 - Arizona
528 thru 529 - Utah
530 ONLY - Nevada
531 thru 539 - Washington
540 thru 544 - Oregon
545 thru 573 - California
602 thru 626 - California
574 ONLY - Alaska
575 thru 576 - Hawaii
577 thru 579 - Washington, DC
585 AND 525 - New Mexico
586 thru 595 - Issued Outside Continental U.S.
700 thru 728 - Railroad Employees *

Encase - FragFS


EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh
Cases
Home Entries Bookmarks Sea
Home File Extents Permissions
Table Report Gallery Timeline Disk Code
Text Hex Picture Report Console Details □ Lock □ 0/562
Filters

- Entries
  - R
    - $Extend
    - etc
    - Fonts
    - POC
    - System Volume Information

	Name	Filter	In Report	File Ext	File Type	File Category	Signature	Description
□ 3	Fonts							Folder, System, Re
□ 4	POC							Folder
□ 5	System Volume Info...							Folder, Hidden, Sys
□ 6	$MFT							File, Internal
□ 7	$MFTMirr							File, Internal
□ 8	$LogFile							File, Internal
□ 9	$Volume							File, Internal

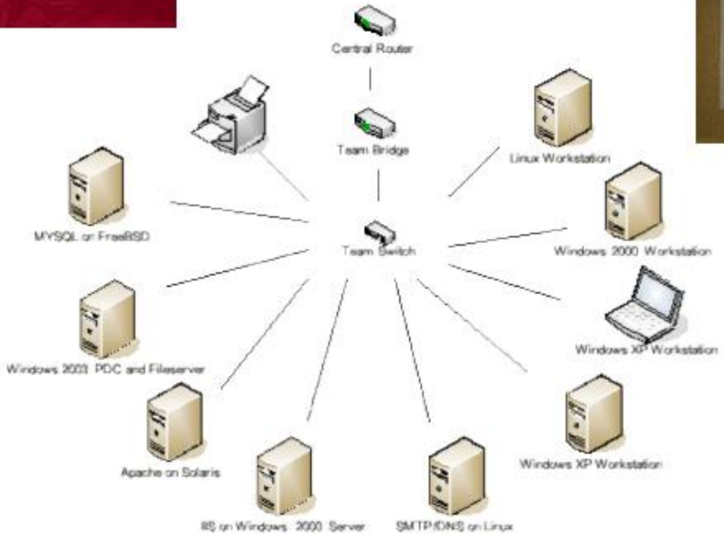
```
050176 46 49 4C 45 30 00 03 00 A2 16 12 00 00 00 00 00 01 00 02 00 38 00 01 00 C0 01 00 00  FILE0···¢···········8···À···
050204 00 04 00 00 00 00 00 00 00 00 00 00 05 00 00 00 31 00 00 00 03 00 00 00 FC 97 00 00  ················1·······ü□··
050232 10 00 00 00 60 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 18 00 00 00 D0 92 93 8A  ····`···········H·······Ð□□□
050260 63 1D C6 01 40 5F 83 67 81 1C C6 01 40 5F 83 67 81 1C C6 01 D0 92 93 8A 63 1D C6 01  c·Æ·@_□g□·Æ·@_□g□·Æ·Ð□□□c·Æ·
050288 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 01 00 00 00 00 00 00   ···························
050316 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 00 00 00 00 00 00 00 02 00  ············0···h···········
050344 50 00 00 00 18 00 01 00 30 00 00 00 00 00 01 00 D0 92 93 8A 63 1D C6 01 D0 92 93 8A  P·······0·······Ð□□□c·Æ·Ð□□□
050372 63 1D C6 01 D0 92 93 8A 63 1D C6 01 D0 92 93 8A 63 1D C6 01 00 00 00 00 00 00 00 00  c·Æ·Ð□□□c·Æ·Ð□□□c·Æ·········
050400 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 07 01 2E 00 62 00 61 00 73 00 68 00  ········ ·········.·b·a·s·h·
050428 72 00 63 00 30 00 00 00 70 00 00 00 00 00 00 00 00 00 03 00 52 00 00 00 18 00 01 00  r·c·0···p···········R·······
050456 30 00 00 00 00 00 01 00 D0 92 93 8A 63 1D C6 01 D0 92 93 8A 63 1D C6 01 D0 92 93 8A  0·······Ð□□□c·Æ·Ð□□□c·Æ·Ð□□□
050484 63 1D C6 01 D0 92 93 8A 63 1D C6 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  c·Æ·Ð□□□c·Æ·················
050512 20 00 00 00 00 00 00 00 08 02 42 00 41 00 53 00 48 00 52 00 43 00 7E 00 31 00 00 00   ·········B·A·S·H·R·C·~·1···
050540 00 00 00 00 80 00 00 00 48 00 00 00 01 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00  ····□···H···················
050568 05 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 0C 00 00 00 00 00 00 DF 0A 00 00  ········@················ß··
050596 00 00 00 00 DF 0A 00 00 00 00 00 00 31 06 47 D6 01 00 01 00 FF FF FF FF 82 79 47 11  ····ß·······1·GÖ····ÿÿÿÿ□yG·
050624 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····························
050652 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····························
050680 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····························
050708 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····························
050736 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····························
050764 00 00 00 00 00 00 00 00 00 00 00 00 DD 01 7E 95 65 35 09 D0 46 84 9D 6D 51 F2 F2 F1  ············Ý·~□e5 ÐF□□mQòòñ
050792 DC 79 09 0D 6F A3 EA E9 84 B2 3F DA 51 D0 8F D8 4A 12 ED CA 6A 2D C9 7F B9 53 9B B0  Üy  o£êé□²?ÚQÐ□ØJ·íÊj-É□¹S□°
050820 2B 23 0E 38 0F 40 6E AE E3 15 A7 31 5C A3 6E AC 50 03 47 D8 CC 8D 83 45 C0 56 7A C7  +#·8·@n®ã·§1\£n¬P·GØÌ□□EÀVzÇ
050848 9C 0E D7 DE 13 F6 06 44 21 74 D2 11 2D 7F 33 38 AF E6 9C C7 6C 17 2A 63 9A C5 2B 14  □·×Þ·ö·D!tÒ·-□38¯æ□Çl·*c□Å+·
050876 9C 49 7F F4 E4 B4 13 AD 66 69 39 50 75 83 7B BE 15 DC 0B 71 86 D9 C8 D6 11 43 CD B1  □I□ôä´·fi9Pu□{¾·Ü·q□ÙÈÖ·CÍ±
050904 1F 56 82 2C 17 0E 52 FA BC 39 30 5A D7 DF 29 A2 BD 4D 5E AD A6 3C CD 1A 24 C1 5C 73  ·V□,··Rú¼90Z×ß)¢½M^¦<Í·$Á\s
050932 4F 3C D4 8C 48 C3 4E 53 73 F4 BF 69 17 A4 DE 08 48 28 75 D5 6F F5 B9 0E C1 03 9C 6A  O<Ô□HÃNSsô¿i·¤Þ·H(uÕoõ¹·Á·□j
050960 80 41 77 84 D1 71 AA F0 AA 62 44 17 1C CF 65 5F 14 C8 72 91 07 7D E0 9E 81 F3 1A 83  □Aw□Ñqªðªb D··Ïe_·Èr□·}à□□ó·□
```

- Filters
  - Search File Permission
  - Search File Permission
  - OLK Folders Containin
  - Yahoo Web Mail Pages
  - Hotmail Web Mail Page
  - Netscape Web Mail Pa
  - Hotmail Pages
  - Yahoo Mail Pages
  - Deleted Files
  - Files after n date
  - Files before n date
  - Filter ANY after n date
  - Filter ANY before n da
  - Find Mixed Types
  - Find files between any
  - Unique Files by Hash

Case 1\R\$MFT (PS 86787 LS 86787 CL 86787 SO 088 FO 50776 LE 212)

NATIONAL
COLLEGIATE
CYBER
DEFENSE
COMPETITION

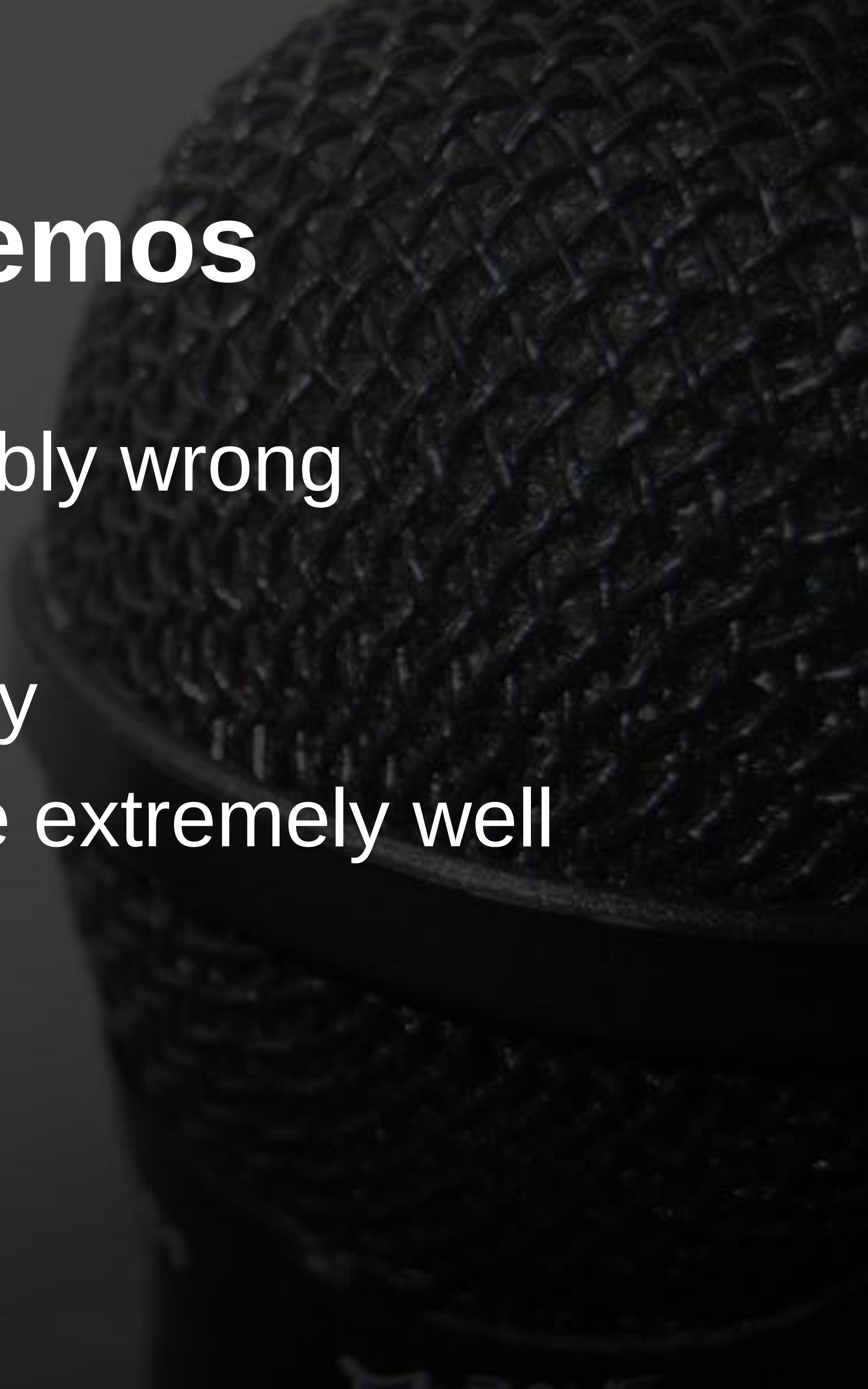
Collegiate Cyber Defense Competition



```
2005-11-01 22:56:05.097681 IP (tos 0x0, ttl 52, id 16855, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.198.48839:  42684 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.097786 IP (tos 0x0, ttl 50, id 43395, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.2.63170:  26885 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.097800 IP (tos 0x0, ttl 56, id 55748, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.17.20879:  44337 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.097854 IP (tos 0x0, ttl 56, id 29724, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.53.27800:  63317 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.097976 IP (tos 0x0, ttl 51, id 51511, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.66.28903:  57713 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.098119 IP (tos 0x0, ttl 50, id 62401, offset 0, flags [+, DF], length: 1500) ___.___.___.___.53 > ___.___.81.191.53122:  33503 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.098155 IP (tos 0x0, ttl 52, id 64104, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.41.24793:  47330 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.098330 IP (tos 0x0, ttl 46, id 3664, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.211.8611:  47954 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.098372 IP (tos 0x0, ttl 56, id 55745, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.13.42959:  46611 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.098386 IP (tos 0x0, ttl 50, id 30744, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.63.55986:  31023 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.098390 IP (tos 0x0, ttl 57, id 9044, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.141.3515:  49050 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.098435 IP (tos 0x0, ttl 52, id 18930, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.154.17100:  32920 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.098575 IP (tos 0x0, ttl 56, id 10261, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.129.14305:  59559 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.098596 IP (tos 0x0, ttl 46, id 40892, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.242.49588:  12522 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.098600 IP (tos 0x0, ttl 38, id 58544, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.15.34671:  47017 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.098665 IP (tos 0x0, ttl 53, id 29641, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.235.37975:  17249 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.098688 IP (tos 0x0, ttl 48, id 1884, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.75.33947:  19706 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.098767 IP (tos 0x0, ttl 49, id 34677, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.56.63871:  55960 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.098775 IP (tos 0x0, ttl 46, id 12769, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.152.2405:  53129 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.098800 IP (tos 0x0, ttl 51, id 46446, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.87.40717:  61969 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.098854 IP (tos 0x0, ttl 48, id 51236, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.224.64893:  64302 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.098888 IP (tos 0x0, ttl 54, id 59295, offset 0, flags [+, DF], length: 1500) ___.___.___.___.53 > ___.___.81.95.62365:  62957 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.098928 IP (tos 0x0, ttl 47, id 16978, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.67.7364:  63079 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.098956 IP (tos 0x0, ttl 48, id 61759, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.57.51718:  23794 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.099068 IP (tos 0x0, ttl 47, id 42163, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.120.40134:  25812 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.099096 IP (tos 0x0, ttl 46, id 20111, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.77.14744:  28858 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.099100 IP (tos 0x0, ttl 49, id 56186, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.75.27962:  17931 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.099135 IP (tos 0x0, ttl 46, id 20887, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.125.50722:  54041 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.099217 IP (tos 0x0, ttl 47, id 47286, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.222.24260:  8686 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.099423 IP (tos 0x0, ttl 49, id 32788, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.13.13267:  5990 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.099509 IP (tos 0x0, ttl 55, id 59656, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.12.61916:  27493 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.099564 IP (tos 0x0, ttl 52, id 6780, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.105.60774:  15646 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.099584 IP (tos 0x0, ttl 53, id 18124, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.56.51438:  18284 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.099624 IP (tos 0x0, ttl 48, id 13089, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.176.48381:  26259 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.099657 IP (tos 0x0, ttl 55, id 20940, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.67.850:  39904 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.099663 IP (tos 0x0, ttl 39, id 35434, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.16.10535:  44987 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.099687 IP (tos 0x0, ttl 51, id 9536, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.206.62136:  42472 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.099732 IP (tos 0x0, ttl 56, id 23195, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.53.50843:  21918 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.099767 IP (tos 0x0, ttl 47, id 51216, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.123.25447:  44605 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.099867 IP (tos 0x0, ttl 52, id 11502, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.60.29083:  18080 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.099918 IP (tos 0x0, ttl 45, id 17913, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.234.15614:  7372 1/2/1 e._______.com TXT[|domain]
2005-11-01 22:56:05.099979 IP (tos 0x0, ttl 47, id 41606, offset 0, flags [+], length: 1500) ___.___.___.___.53 > ___.___.81.121.46332:  46093 1/2/1 e._______.com TXT[|domain]
```

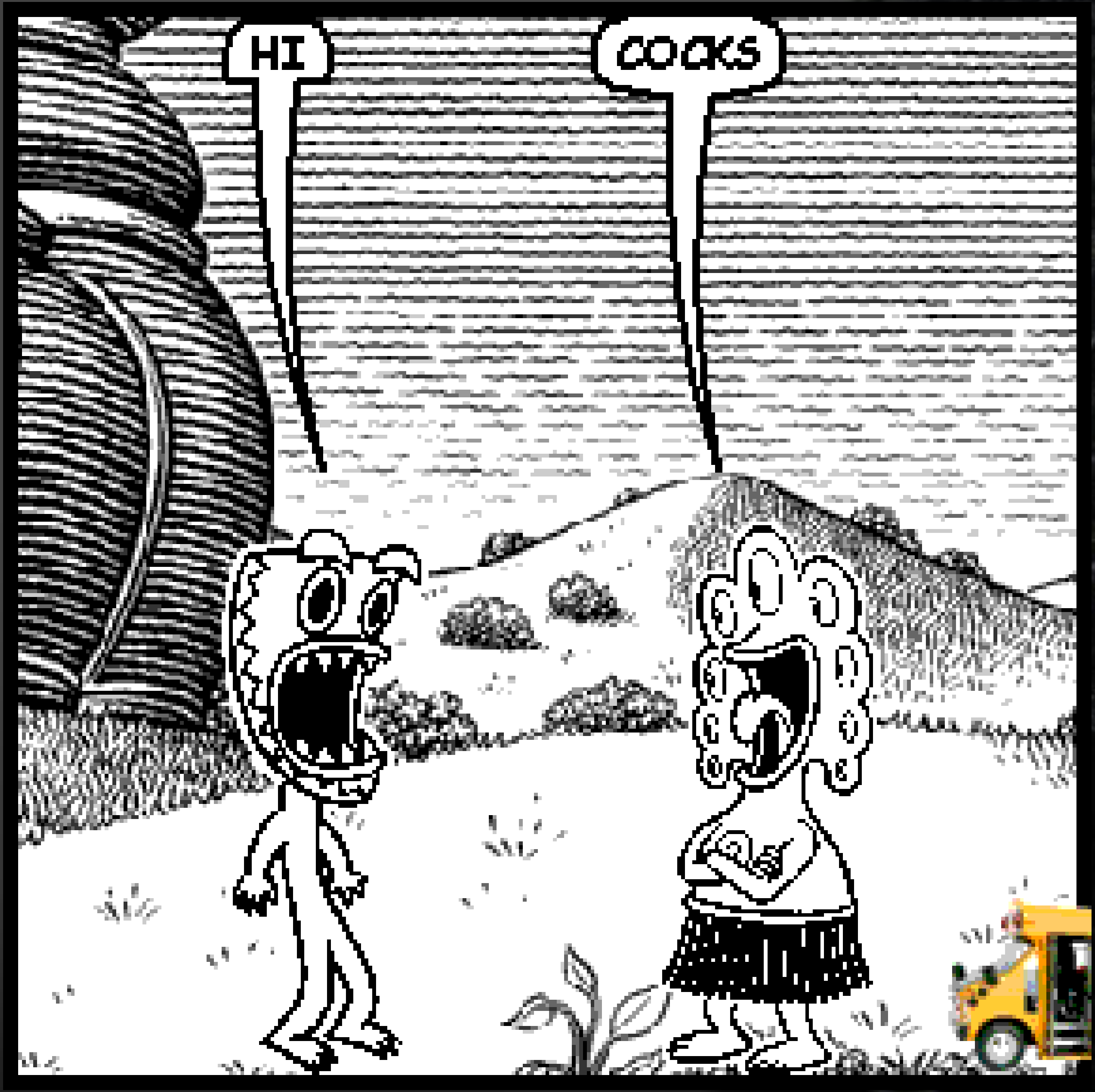
Live Demos

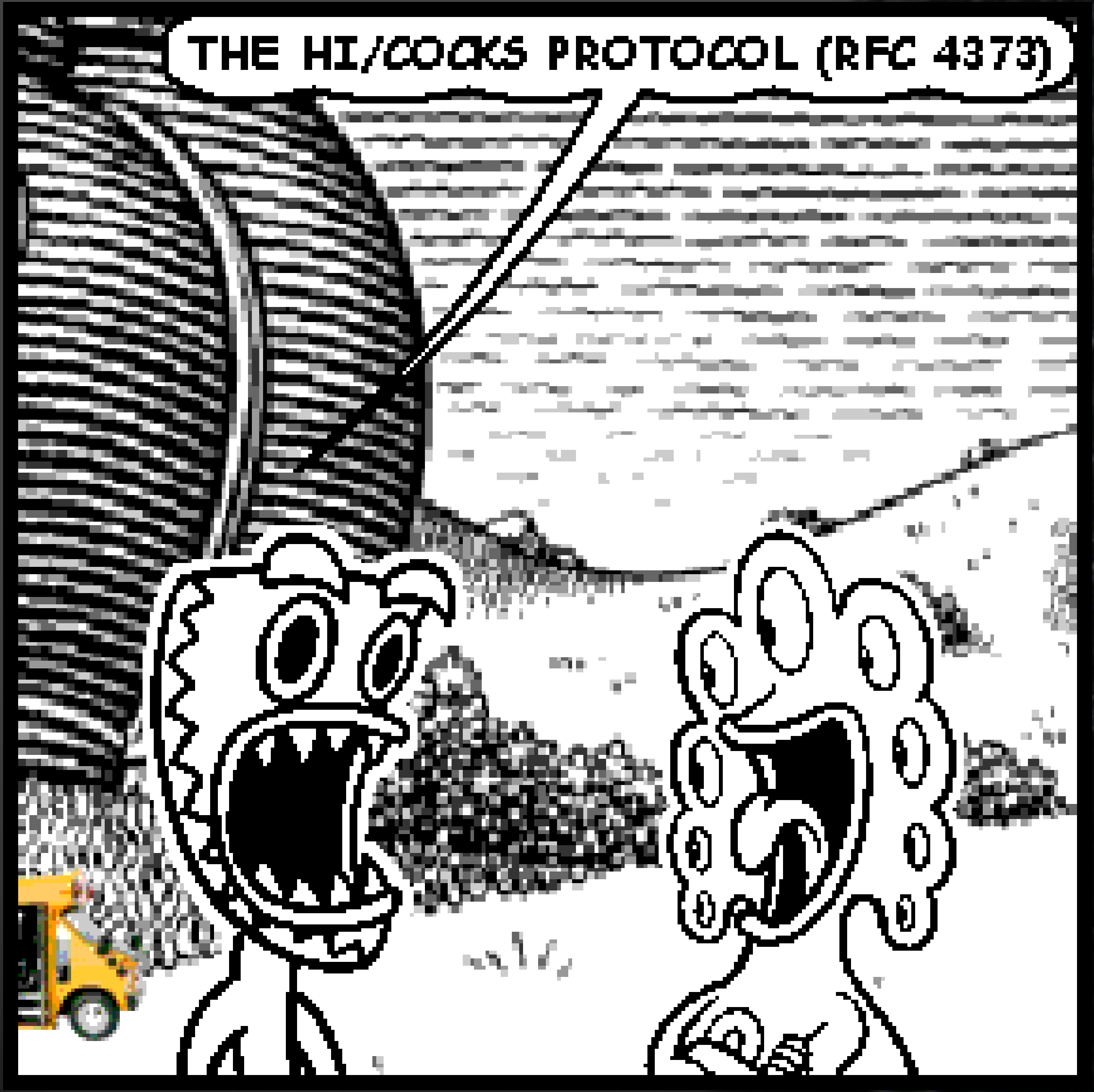
- Can and will go horribly wrong
- Must be short
- Must progress quickly
- Only effective if done extremely well



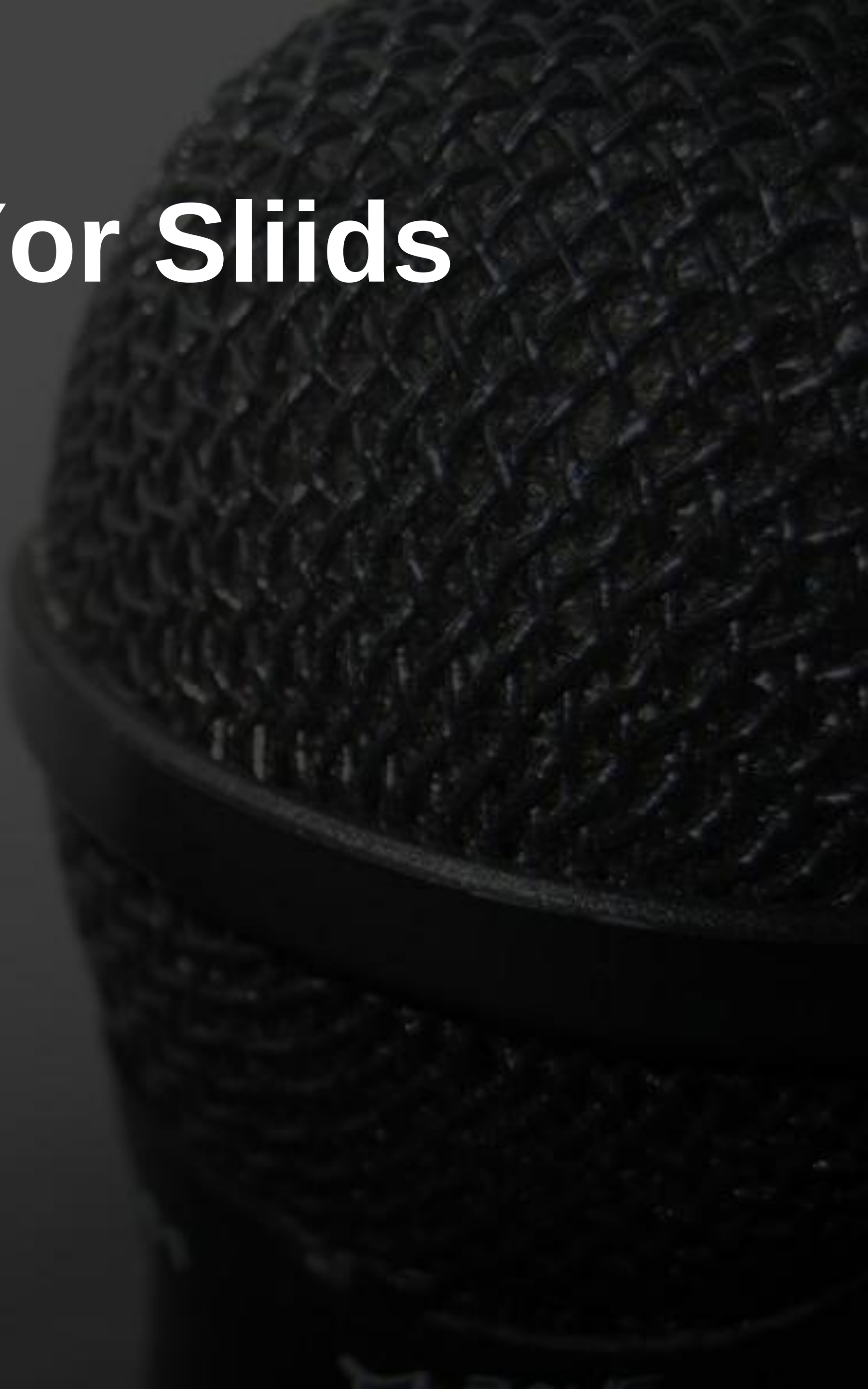
Live Demos

```
hinkpad ~]$
hinkpad ~]$ i fail at x configuration : (
```


HI
COCKS

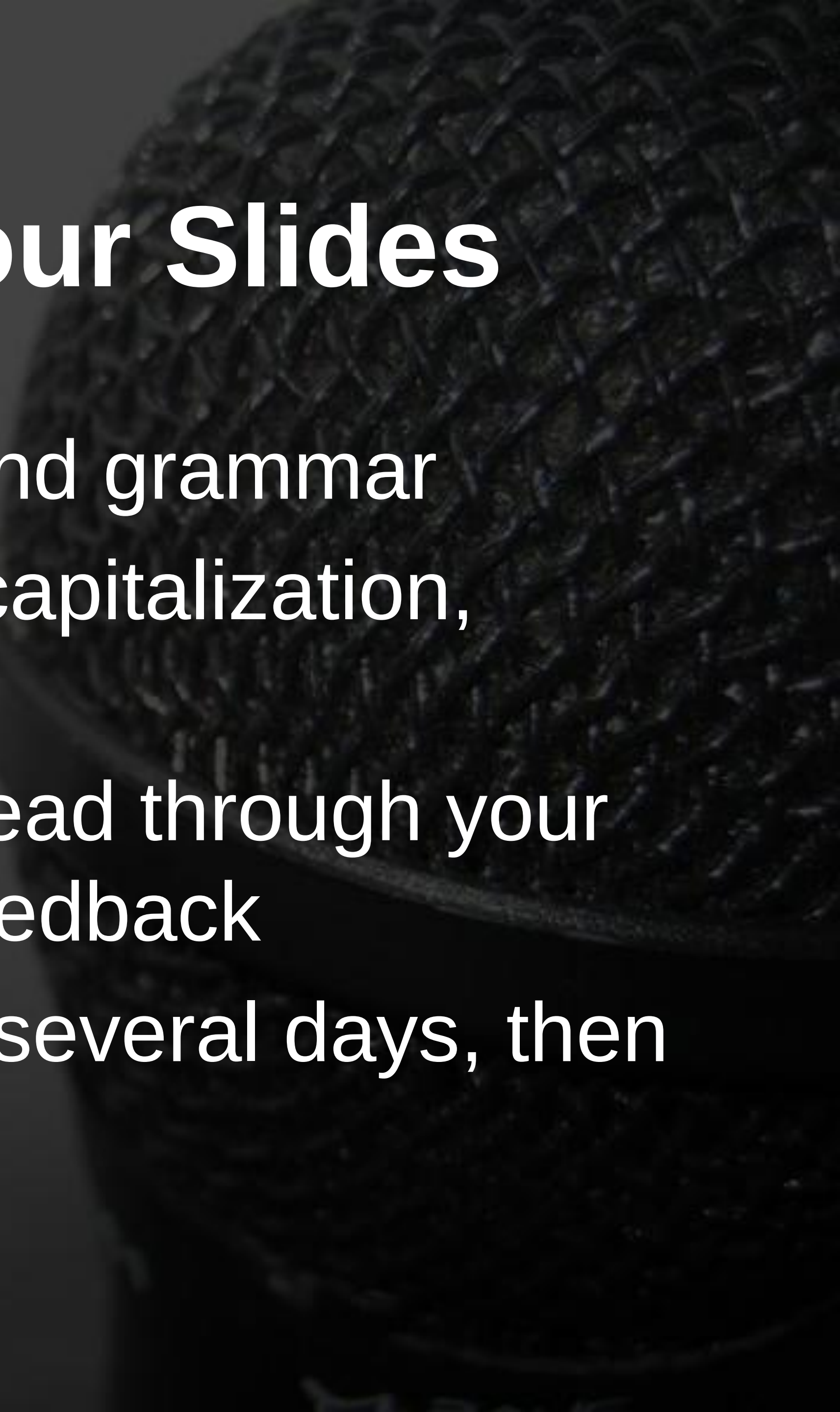

THE HI/COCKS PROTOCOL (RFC 4373)

Proofred Yor Sliids



Proofread Your Slides

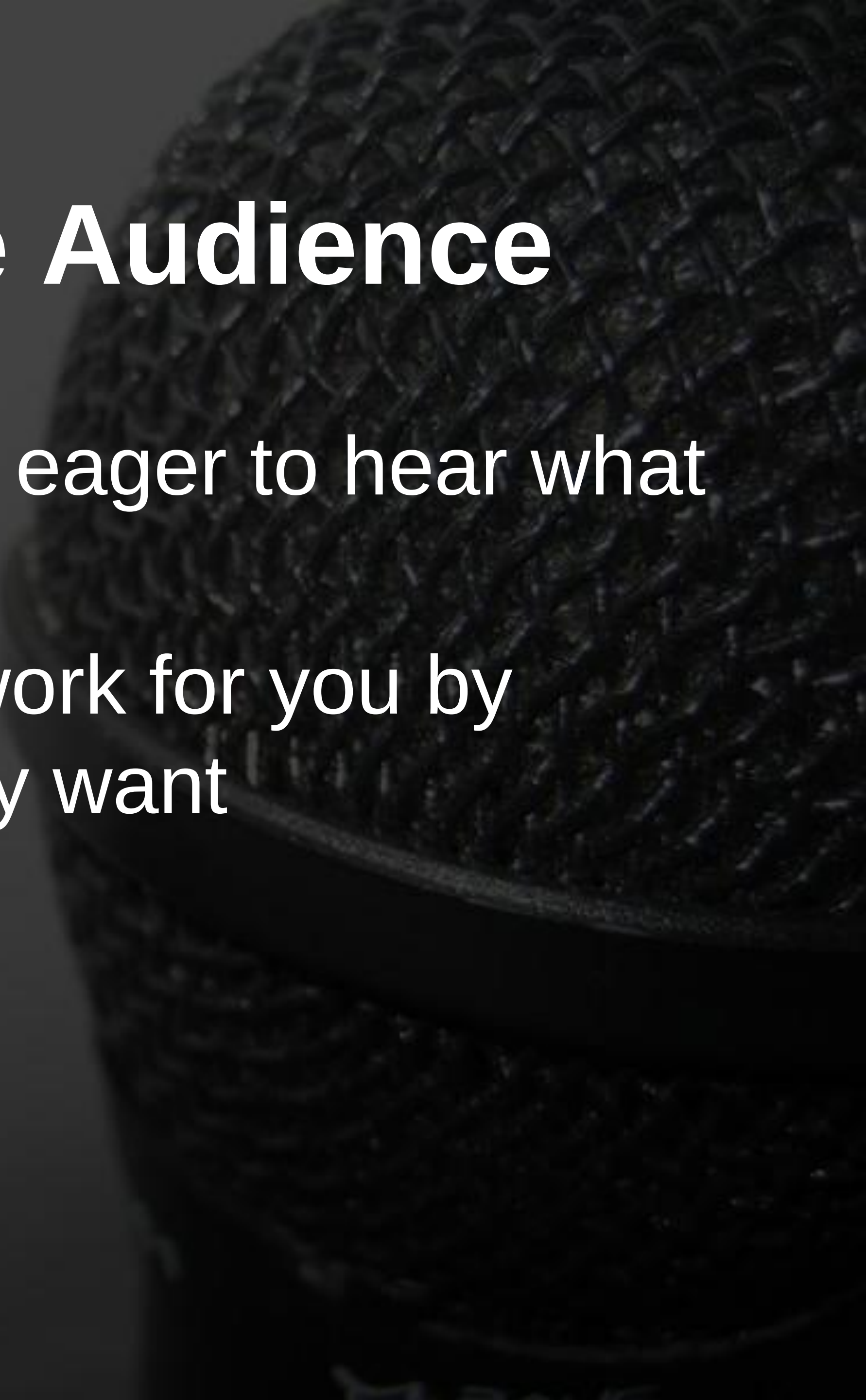
- Check your spelling and grammar
- Check for consistent capitalization, layout, and formatting
- Have someone else read through your slides and give you feedback
- Ignore your slides for several days, then proofread them again



GIVING THE TALK

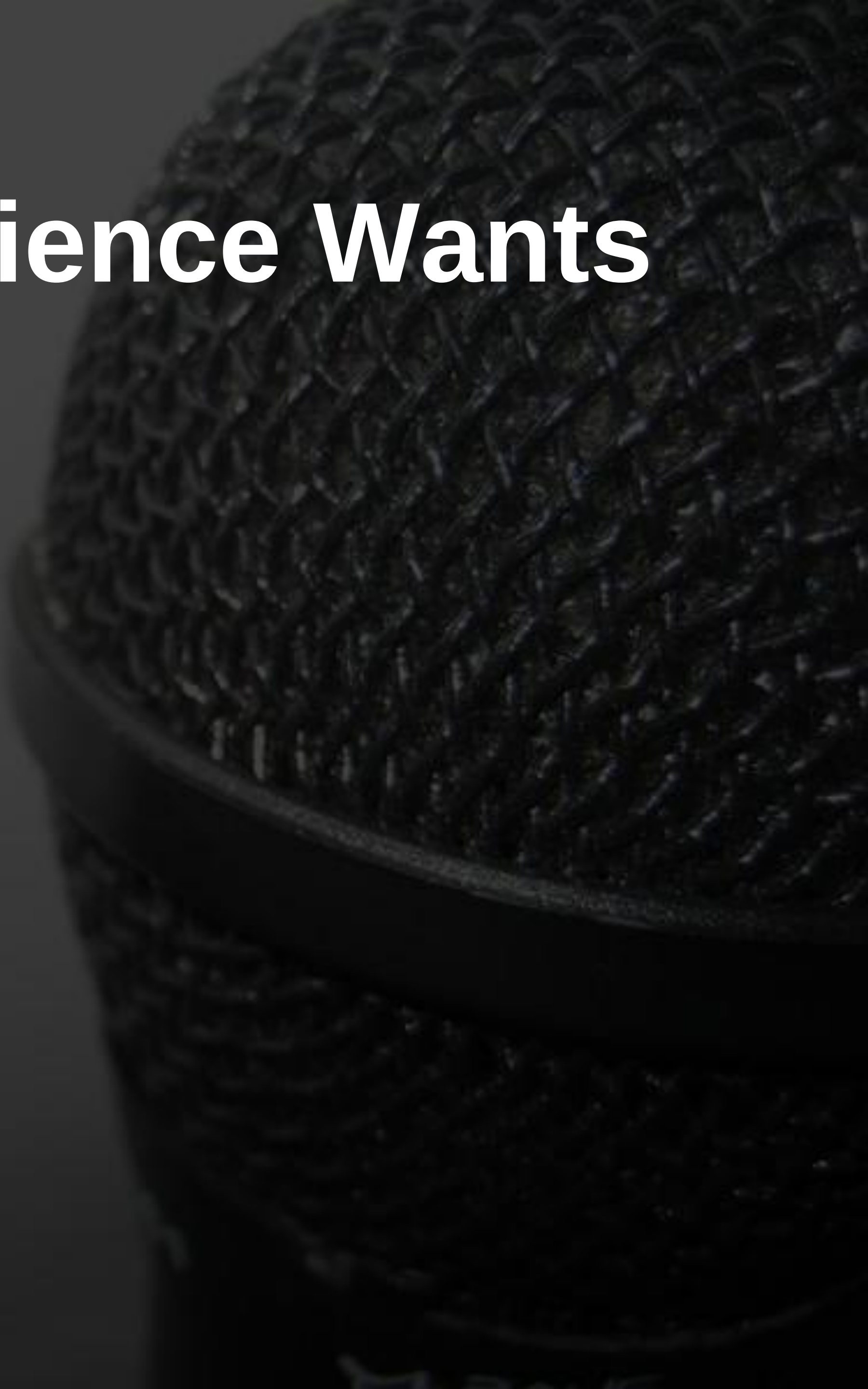
Consider the Audience

- The audience is very eager to hear what you have to say
- Make the audience work for you by giving them what they want



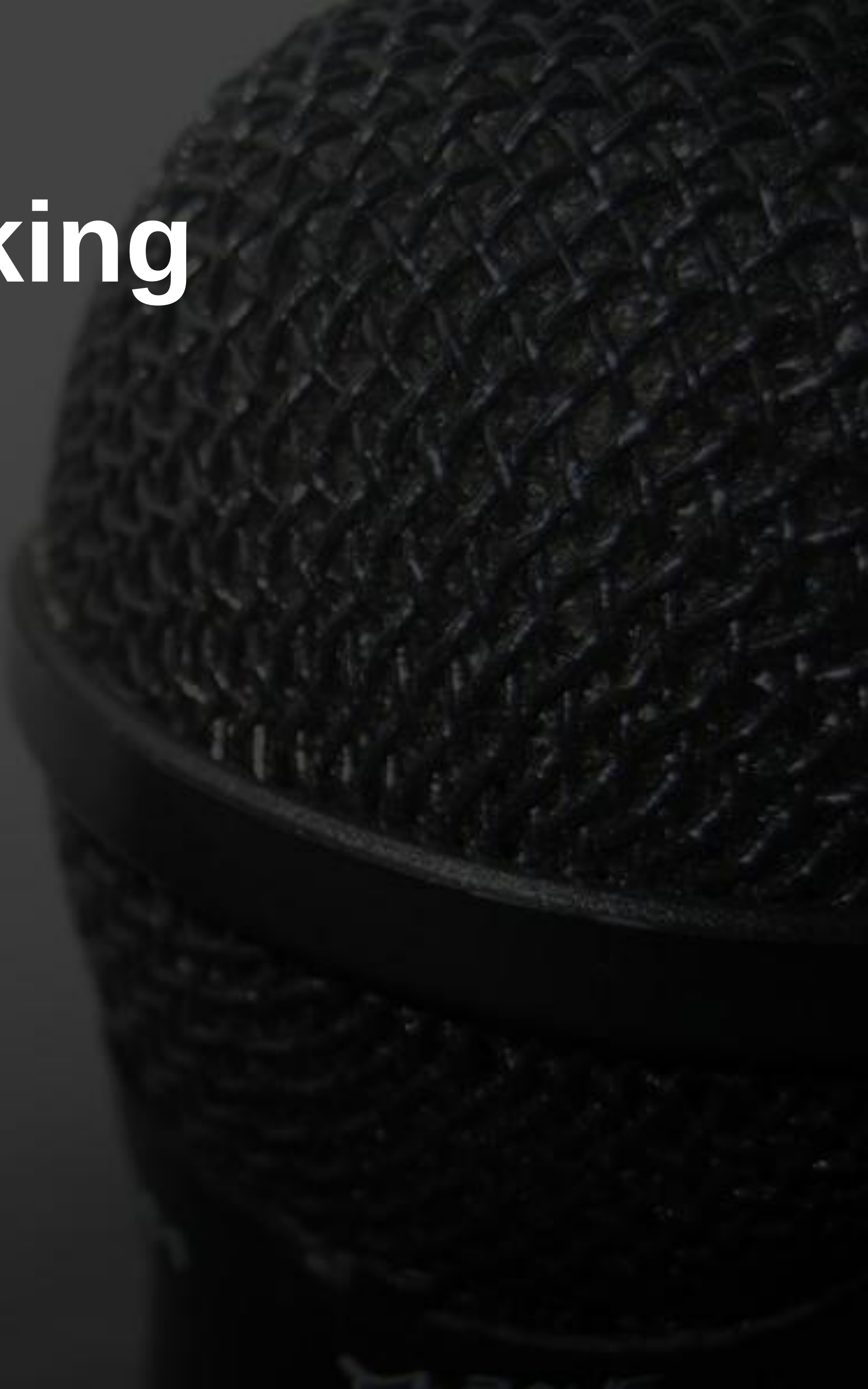
What The Audience Wants

- Knowledge
- Entertainment



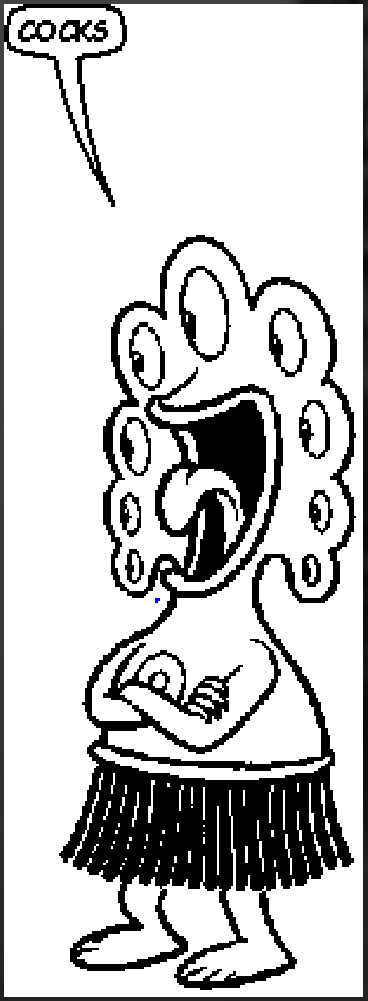
Speaking

- Slow down
- Enunciate
- Relax

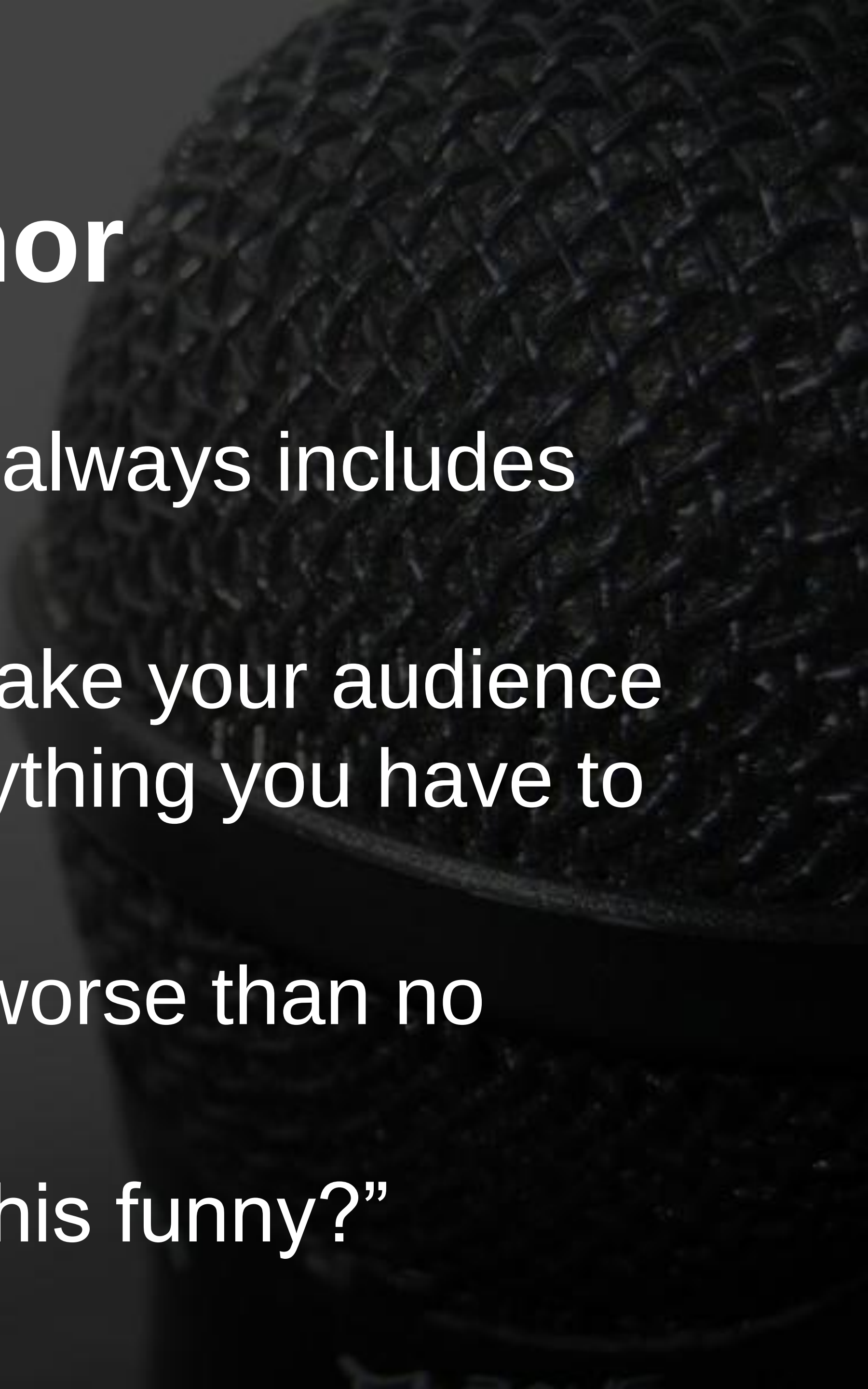


Get Away from the Lectern

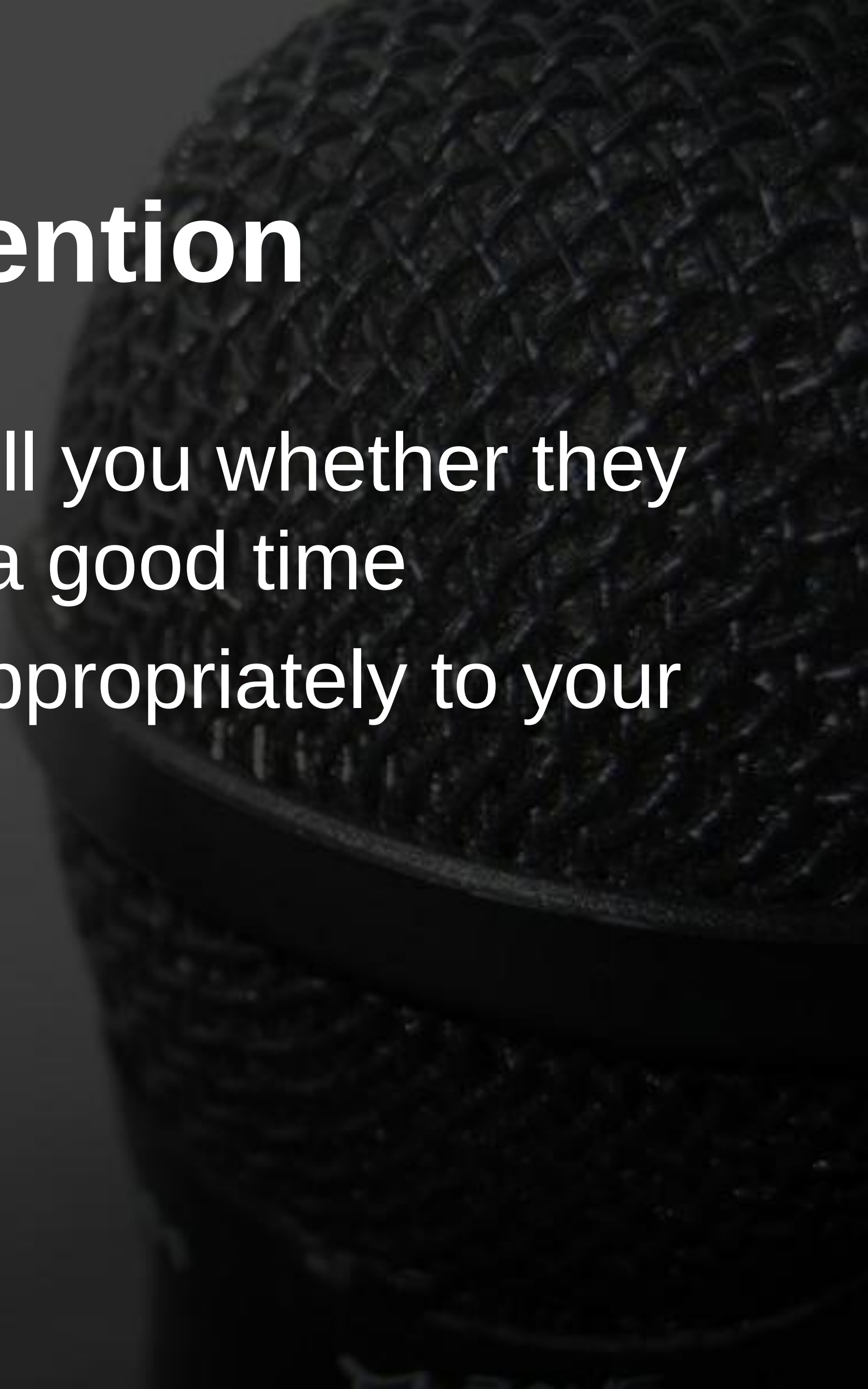
Humor



Humor



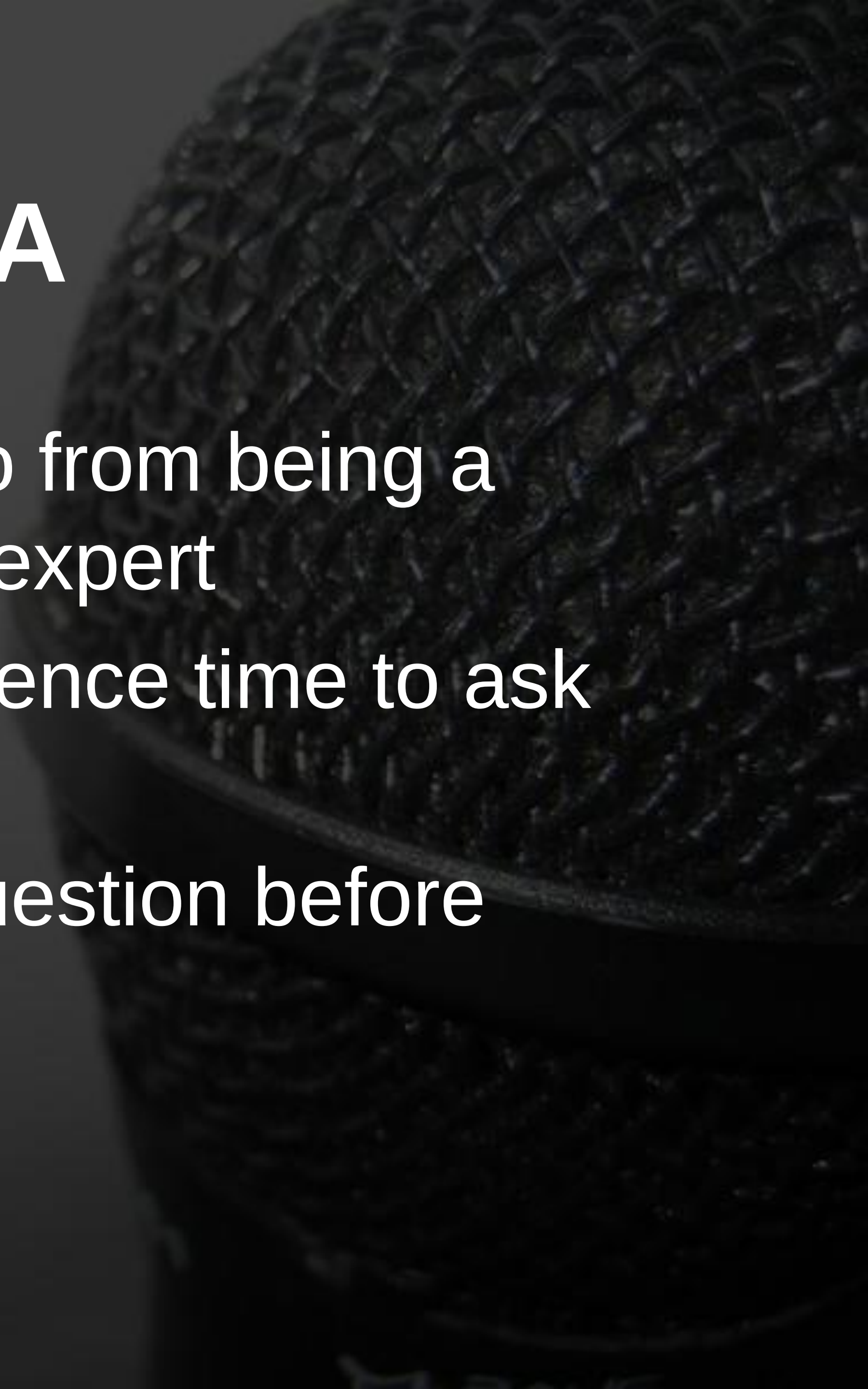
- A good presentation always includes humor
- Unfunny jokes will make your audience disinterested in everything you have to say
- Too much humor is worse than no humor
- Ask your friends “is this funny?”



Pay Attention

- Your audience will tell you whether they are bored or having a good time
- You must respond appropriately to your audience

AFTER THE TALK

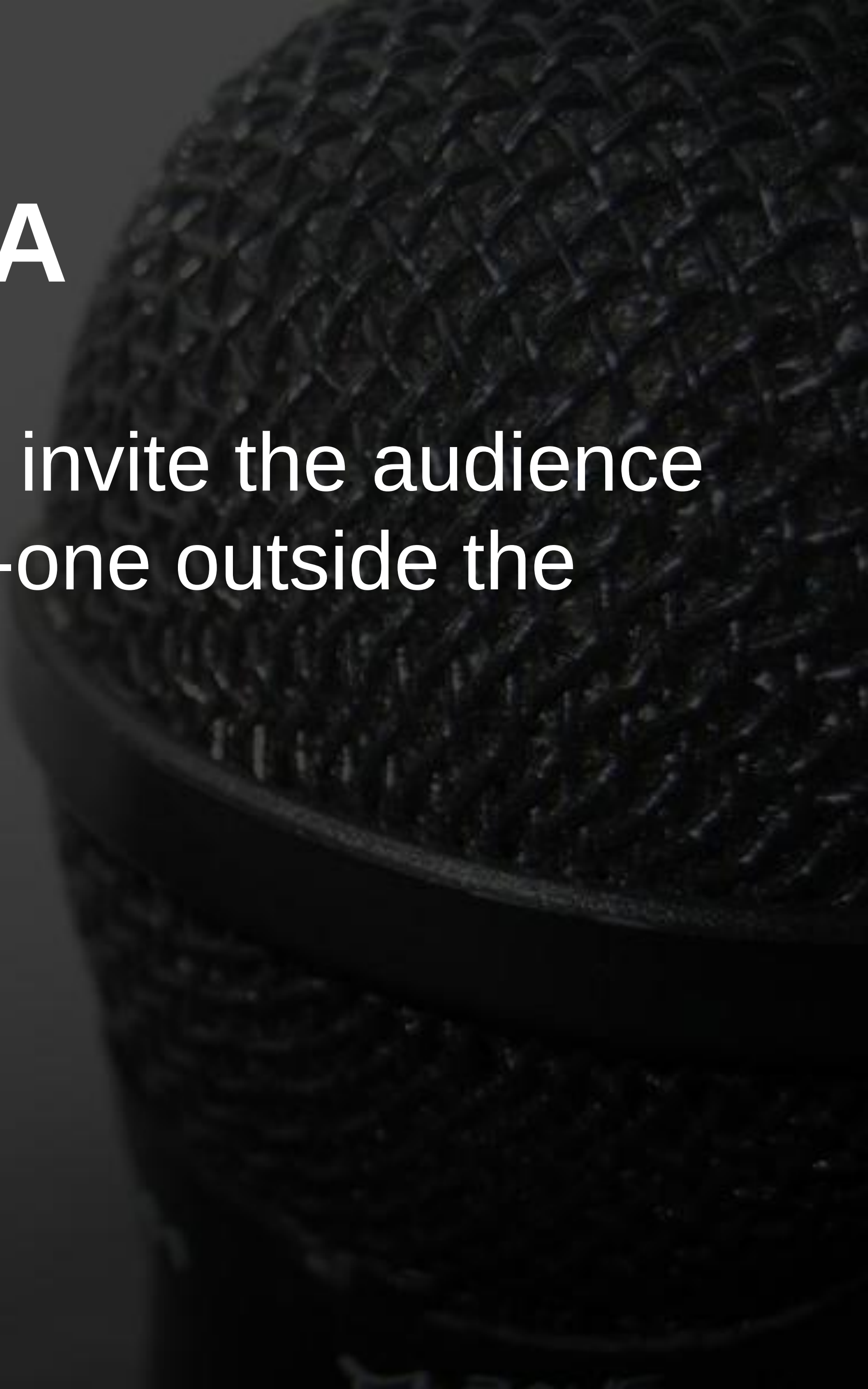


Q&A

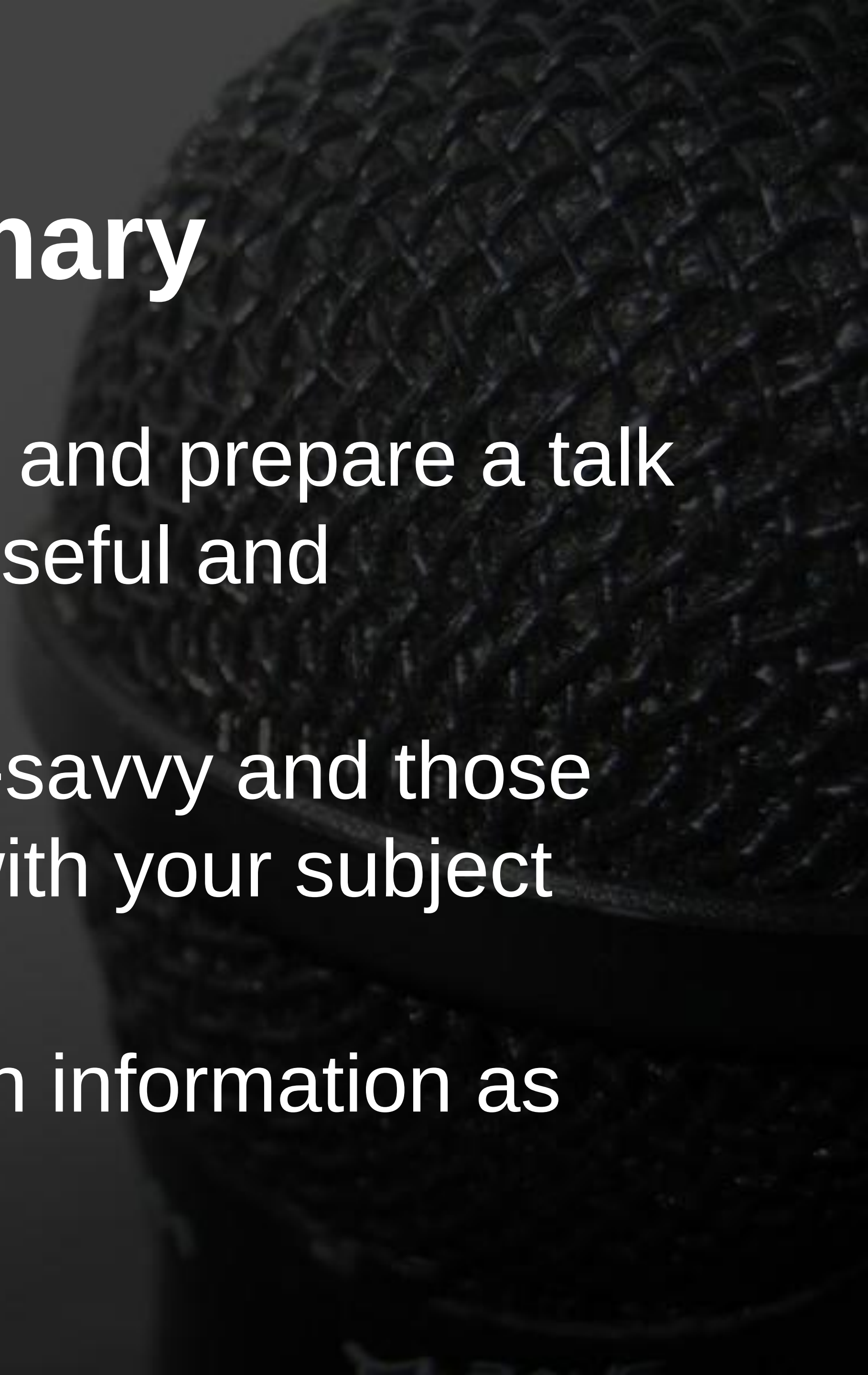
- Q&A is where you go from being a speaker to being an expert
- Always give the audience time to ask questions
- Always repeat the question before answering it

Q&A

- After your time is up, invite the audience to talk to you one-on-one outside the presentation

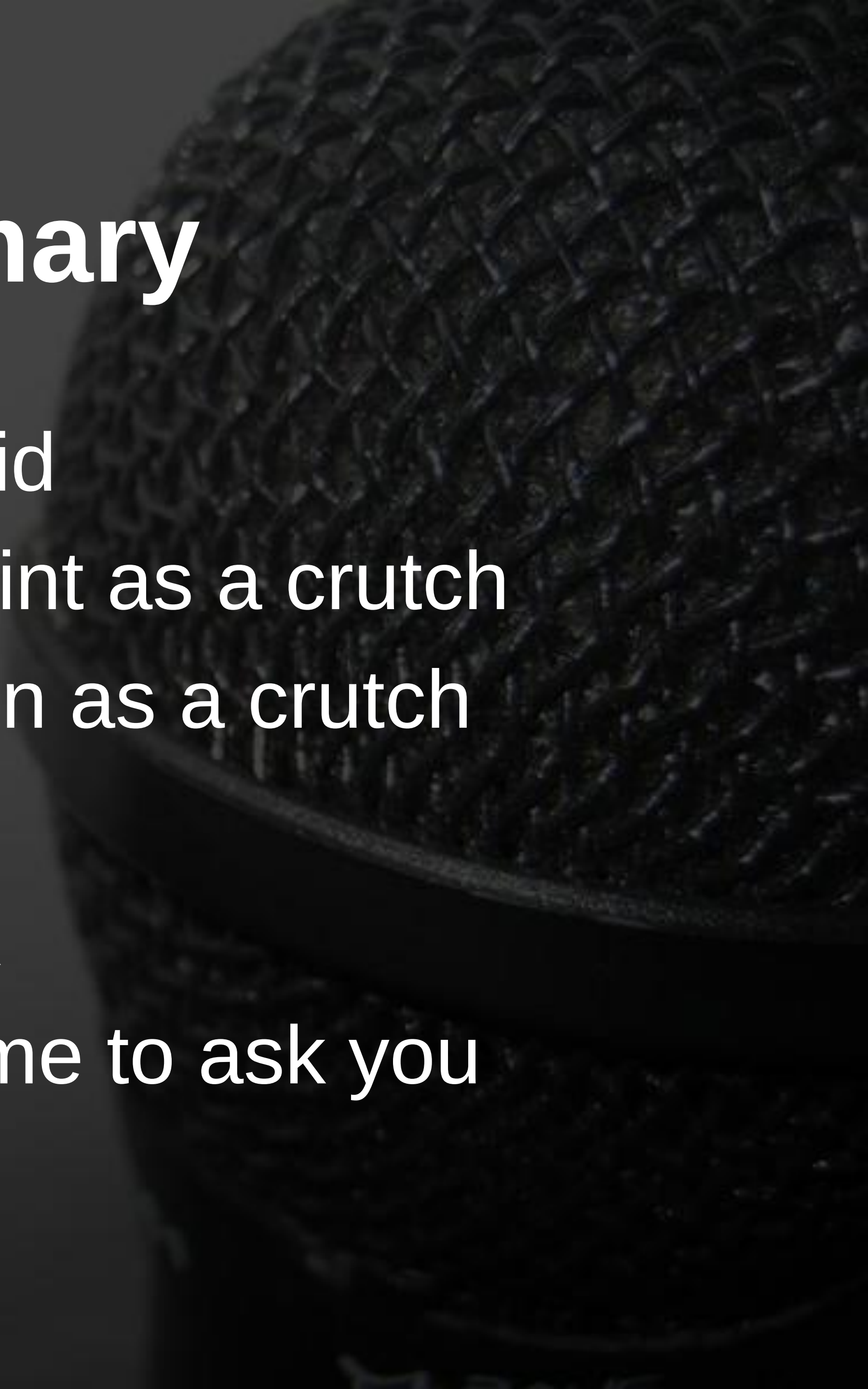


Summary



- Know your audience and prepare a talk which they will find useful and interesting
- Teach both the tech-savvy and those who are unfamiliar with your subject matter
- Throw away as much information as you possibly can

Summary



- Keep It Simple, Stupid
- Do not use PowerPoint as a crutch
- Do not use the lectern as a crutch
- Avoid live demos
- Slow down and relax
- Give the audience time to ask you questions

Q&A