

## LCLint

- Lightweight static analysis tool [FSE'94, PLDI'96] "quick and dirty"
- Simple dataflow analyses
- Unsound and Incomplete
- Several thousand users...perhaps ¼ adding annotations to code: gradual learning curve
- Detects inconsistencies between code and specifications annotations documented assumptions
- Examples: memory management (leaks, dead references), null dereferences, information hiding, undocumented modifications, etc.

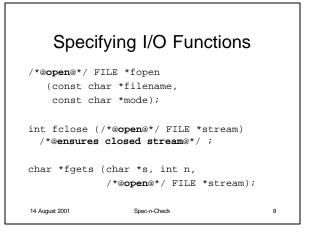
Spec-n-Check

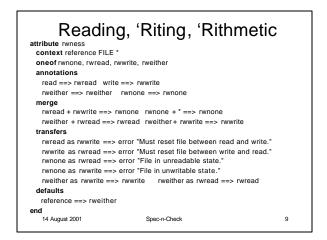
5

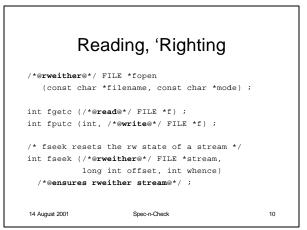
14 August 2001

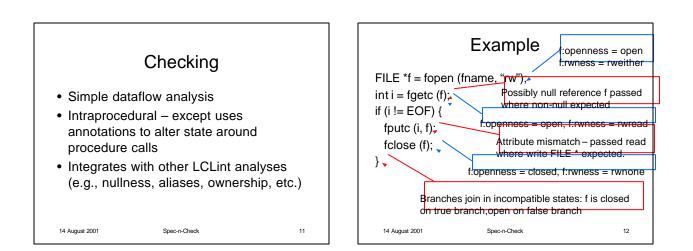
## I/O Streams Challenge Many properties can be described in terms of state attributes A file is open or closed fopen: returns an open file fclose: open - closed fgets, etc. require open files Reading/writing - must reset between certain operations

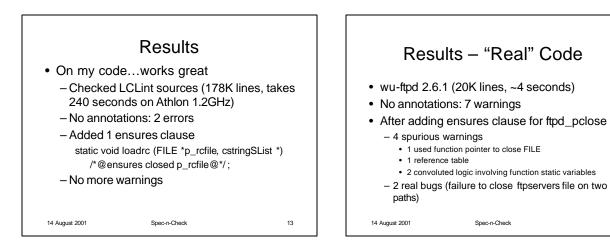
Defining Openness				
attribute openness context reference FILE * oneof closed, open annotations open ==> open closed =	=> closed			
transfers open as closed ==> error closed as open ==> error merge open + closed ==> e losereference open ==> error "file not cl	Object cannot be open     on one path, closed on     another			
defaults reference ==> open end 14 August 2001	Cannot abandon FILE in open state Spec-n-Check 7			





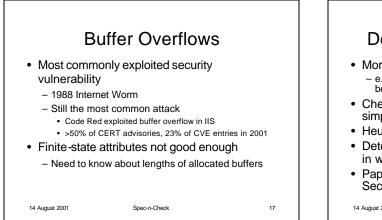


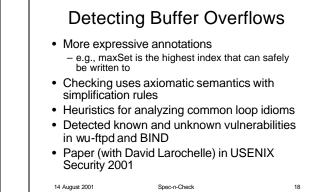




attribute taintedness	Taintedness		
context reference ch	nar *		
oneof untainted, tair annotations	nted		int fprintf *format,
tainted reference = untainted reference anytainted parame	e ==> untainted		/*@tainted@* /*@ensures
transfers			char *strcpy
tainted as untainte	d ==> error		
merge			/*@ensures
tainted + untainted	tainted ==> tainted		
defaults			char *strcat
reference ==> tair literal ==> untainted null ==> untainted	ed		/*@ensures
end 14 August 2001	Spec-n-Check	15	14 August 2001
14 August 2001	Opeonrolleck	15	August 2001

tainted.xh	
<pre>int fprintf (FILE *stream, /*@untainted@*/ ch  *format,);</pre>	ar
<pre>/*@tainted@*/ char *fgets (char *s, int n, FI /*@ensures tainted s@*/ ;</pre>	LE *)
<pre>char *strcpy (/*@returned@*/ /*@anytainted@*/</pre>	
<pre>char *strcat (/*@returned@*/ /*@anytainted@*/</pre>	
14 August 2001 Spec-n-Check	16





Will Programmers Add Annotations?
<ul> <li>C in 1974: char *strcpy ();</li> </ul>
<ul> <li>C in 1978: char *strcpy (char *s1, char *s2);</li> </ul>
• C in 1989: char *strcpy (char *s1, const char *s2);
• C in 1999: char *strcpy (char * restrict s1,
const char * restrict s2);
• C in 20??:
nullterminated char *strcpy
(returned char *restrict s1,
nullterminated const char *restrict s2)
requires maxSet(s1) >= maxRead (s2)
ensures s1:taintedness = s2:taintedness
ensures maxRead(s1) = maxRead (s2);

Spec-n-Check

14 August 2001

19