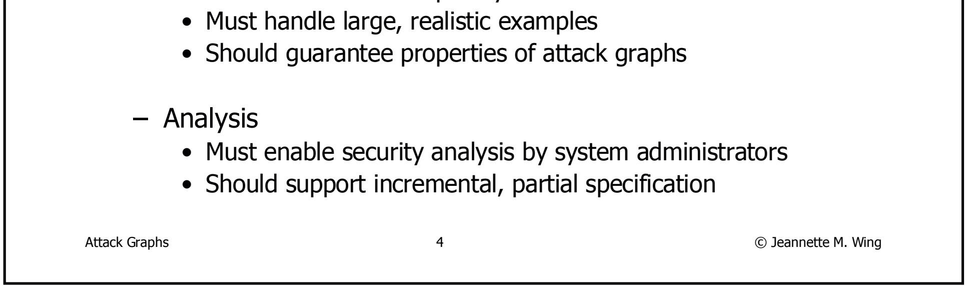
        - Limited privilege
    - Achieving root access on machine X may require multiple steps
        - Get inside firewall
        - Scan network for vulnerabilities
        - Get user access to machine
        - Get root access to machine
- Question: how does security of whole system depend on parts?



- Must handle large, realistic examples
- Should guarantee properties of attack graphs

– Analysis

- Must enable security analysis by system administrators
- Should support incremental, partial specification

- Handles safety and liveness properties
- *Generates counterexamples*

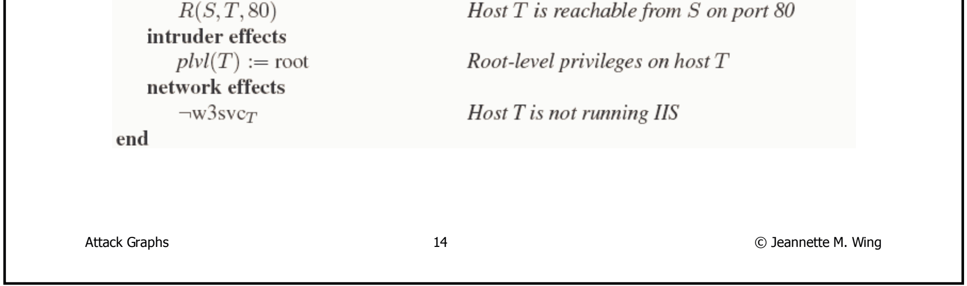
- An attack graph is a set of attacks of M.

[Gerth et al.95].

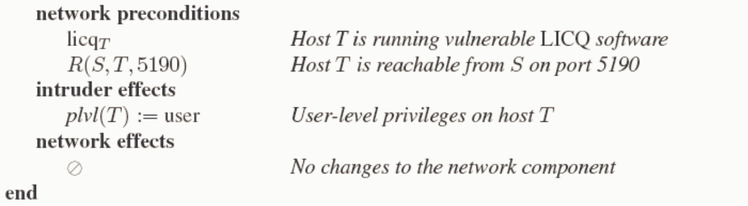
- M and Φ induce languages L(M) and L(Φ).

2. Compute intersection M $\cap$ ~Φ of Buchi automata.
   - L(M $\cap$ ~Φ) = L(M)\L(Φ) = executions of M that violate Φ.
3. Derive G from strongly connected components of intersection automaton [Tarjan72].

IIS buffer overflow:	remotely get root	✗
Squid portscan:	port scan	✗
LICQ remote-to-user:	gain user privileges remotely	✓
scripting exploit:	gain user privileges remotely	✗
local buffer overflow:	locally get root	✗



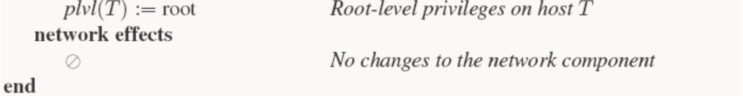
```
        $R(S, T, 80)$                              Host $T$ is reachable from $S$ on port 80
    **intruder effects**
        $plvl(T)$ := root                          Root-level privileges on host $T$
    **network effects**
        $\neg \mathrm{w3svc}_T$                    Host $T$ is not running IIS
**end**
```



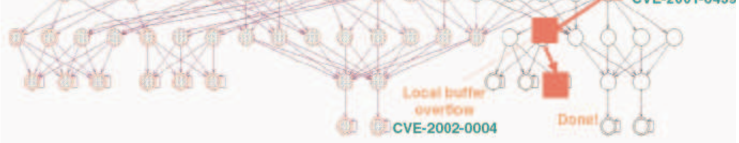
network preconditions

licq_T	*Host T is running vulnerable* LICQ *software*
$R(S, T, 5190)$	*Host T is reachable from S on port 5190*
intruder effects	
$\mathit{plvl}(T) := \text{user}$	*User-level privileges on host T*
network effects	
$\oslash$	*No changes to the network component*

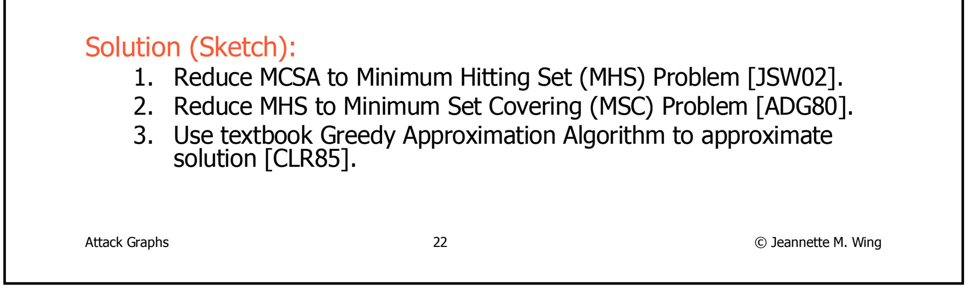
end



```
        $plvl(T)$ := root                Root-level privileges on host $T$
    network effects
        $\oslash$                        No changes to the network component
end
```



Local buffer overflow
CVE-2002-0004
Done!



Solution (Sketch):

1. Reduce MCSA to Minimum Hitting Set (MHS) Problem [JSW02].
2. Reduce MHS to Minimum Set Covering (MSC) Problem [ADG80].
3. Use textbook Greedy Approximation Algorithm to approximate solution [CLR85].

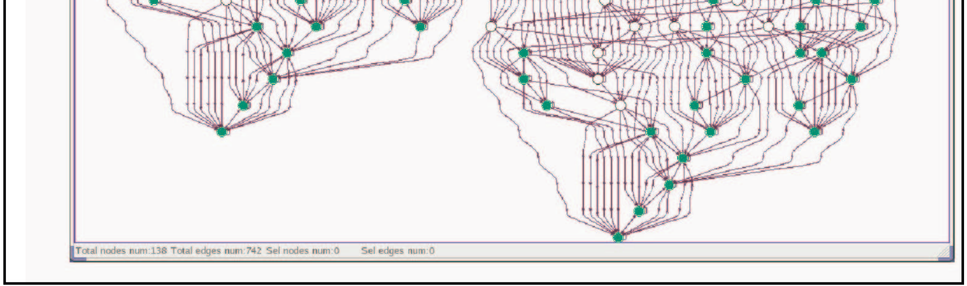
MCSA and MHS are polynomially-equivalent.

[JSW02b] Jha, Sheyner, Wing, “Two Formal Analyses of Attack Graphs,” Computer Security Foundations Workshop, Nova Scotia, June 2002.

Use textbook Greedy Approximation Algorithm for MSC [CLR85, p. 975.]

deploy to make the system safe? [S04]

Solution Approach: Greedy algorithm with provable bounds. General case is NP-complete (slightly more complex than minimum cover problem).



Total nodes num:138 Total edges num:742 Sel nodes num:0 Sel edges num:0

```
        <ftp/> <sshd/> </remote>
    </connectivity>
    <cve>
      <CVE_2002_0004/>
      <CVE_2001_1030/>
      <CVE_2001_0439/>
    </cve>
  </host>
```