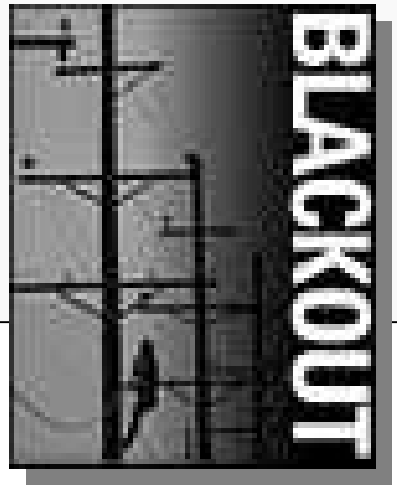
Software Security

David Wagner
University of California at Berkeley

Critical infrastructure is dependent on computer security



Electrical Grid Vulnerable to Hackers

By Jim Krane
Washington Post, Thursday, September 11, 2003; 1:57 PM

NEW YORK -- Since last month's Northeast Blackout, utilities have accelerated plans to automate the electric grid, replacing aging monitoring systems with digital switches and other high-tech gear.

But those very improvements are making the electricity supply vulnerable to a different kind of peril: computer viruses and hackers who could black out substations, cities or entire states. [...]

"I know enough about where the holes are," said Eric Byres, a cybersecurity researcher for critical infrastructure at the British Columbia Institute of Technology in Vancouver. "My team and I could shut down the grid. Not the whole North American grid, but a state, sure."

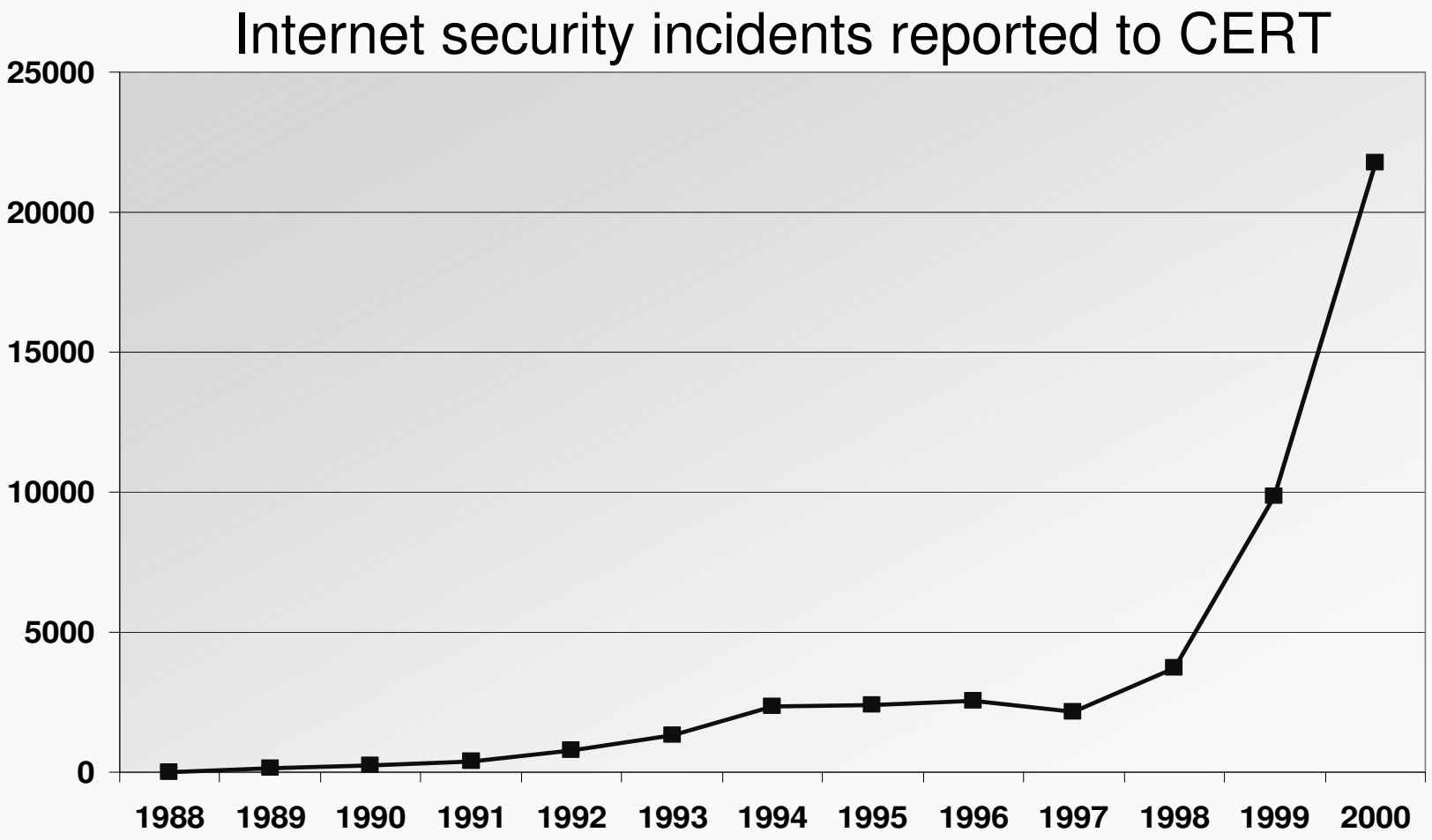
Security experts have warned about the grid's growing vulnerabilities before, especially after U.S. National Security Agency hackers showed they could break into grid control networks in 1998. [...]

Bank of America

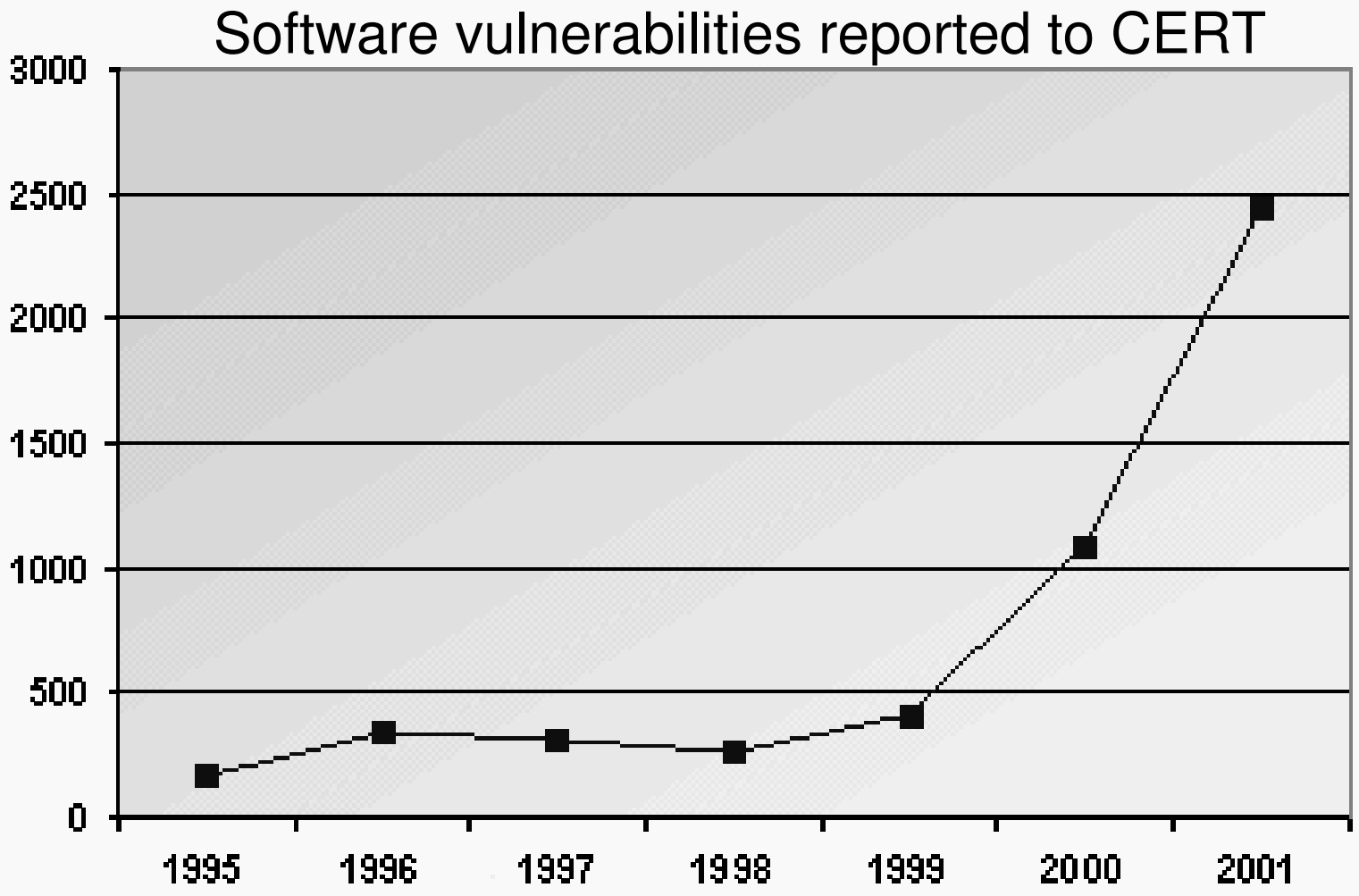
The "Blaster" worm that flummoxed an estimated half-million computers around the world last month might have exacerbated utilities' problems during the August blackout, bringing down - or perhaps blocking communications - on computers used to monitor the grid, said Joe Weiss, a utility control system expert.

"It didn't cause what happened but it could've exacerbated what happened," said Weiss, with Kema Consulting in Cupertino, Calif., The blackout followed the Aug. 11 Blaster outbreak by just three days. [...]

In January, the "Slammer" Internet worm took down monitoring computers at FirstEnergy's idled Davis-Besse nuclear plant. A subsequent report by the North American Electric Reliability Council said the infection blocked commands that operated other power utilities, although it caused no outages.



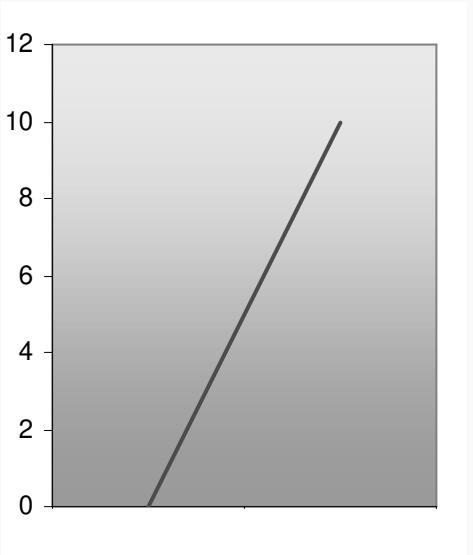
Security break-ins are all too prevalent



Typical cause: Security defects in our software

Talk Outline

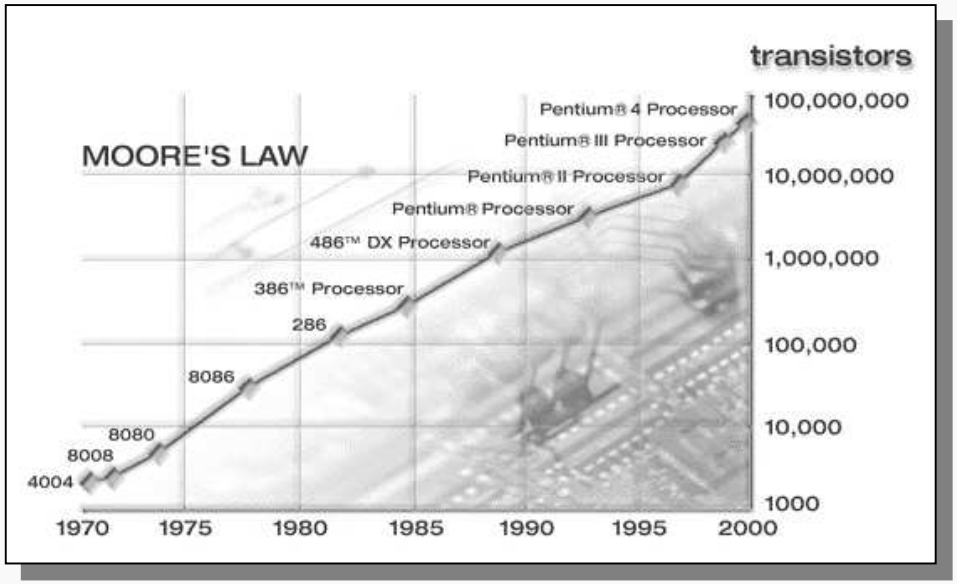
- Why is our software so buggy?
- What can we do about software security?

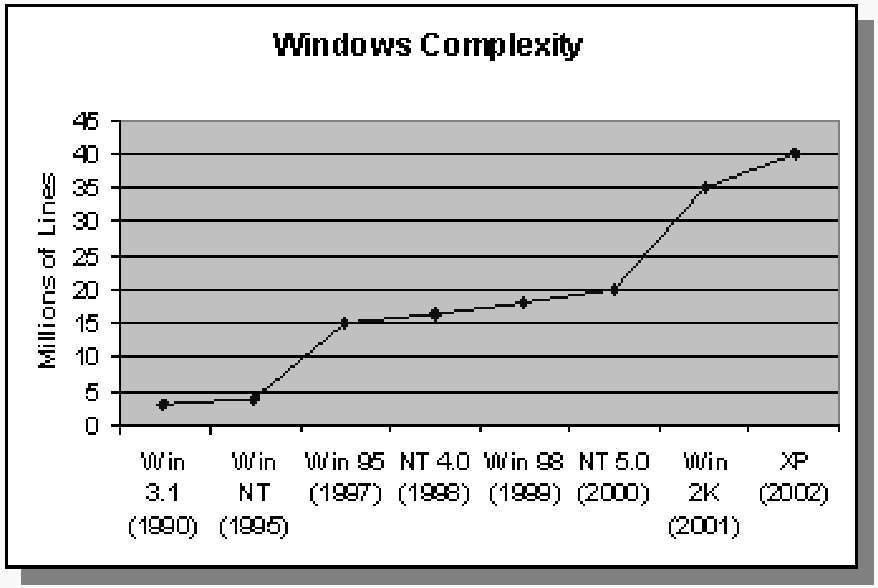


What makes simple mechanical systems predictable?

- Linearity (or, piecewise linearity)
- Continuity (or, piecewise continuity)
- Small, low-dimensional statespaces

Systems with these properties are
(1) easier to analyze, and (2) easier to test.





- Computers enable highly complex systems
- And today's software is taking advantage of this
  - Highly non-linear behavior; large, high-dim. state spaces

Problem Summary

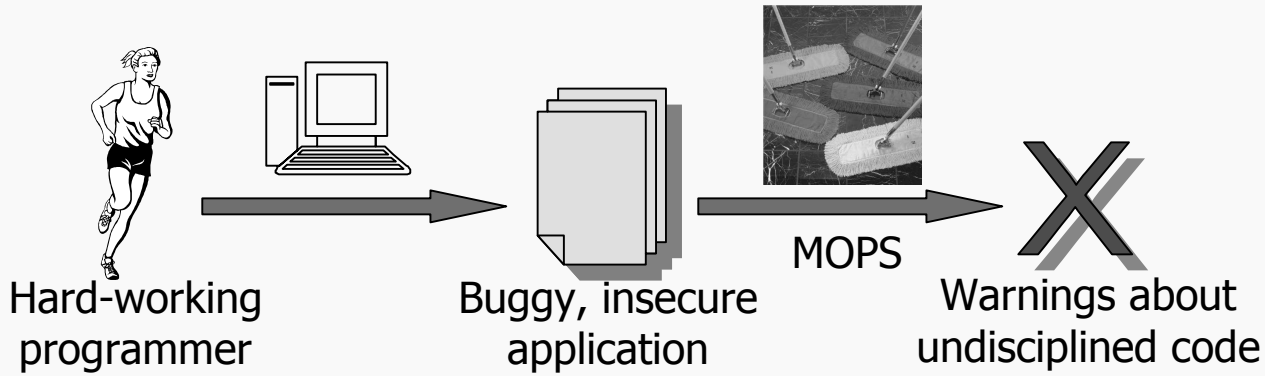
- Complexity breeds bugs and unpredictable behavior
- Bugs and unpredictability are the bane of security

Mitigating the Risks

How can we improve software security?

1. Correctness by construction
   (e.g., K.I.S.S., defensive coding, least privilege)
2. Automated analysis of software,
   new models of software behavior
3. Formal verification: proving programs free of defects

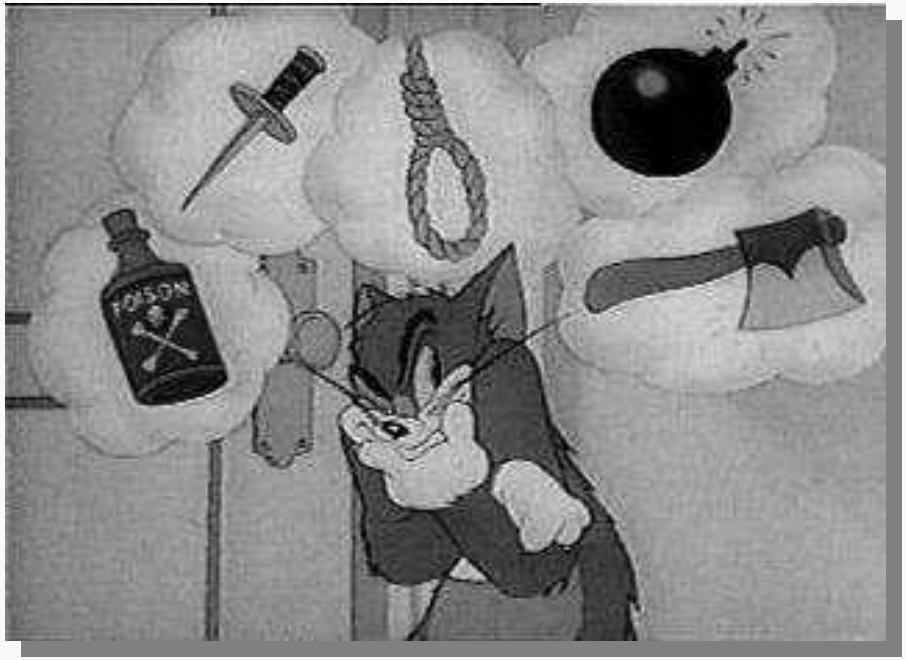
Tools for Software Security



- If secure programming is hard, let's build tools that make it easier to get security right
  - MOPS: scanning for bugs using software model checking
  - CQual: security-typed programming discipline
  - We're finding--and fixing--vulnerabilities in open-source applications (Linux kernel, sendmail, Apache, wu-ftpd, …)

Conclusion

- Computer security problems are endemic.
- Our software is a weak spot.
  Network-layer defenses must make up for software inadequacies.
- The problem will likely remain with us as long as users value features (complexity) over security (simplicity).



Questions?