Patch-and-Catch

Matt Bishop
Department of Computer Science
University of California at Davis
Davis, CA 95616-8562

email: bishop@cs.ucdavis.edu
phone: (916) 752-8060

Key Points

Not sharing attack and vulnerability data

- poorer software
- poorer security practices
- increased vulnerability

Internet Security

- depends upon intermediate and end hosts
- security services assume (some of) these are trustworthy within context of service needs

Cycle of Securing

1. something broken into
   – what that means depends on context
2. gets patched, reconfigured, or redesigned
3. go to step 1

Security Is Not "Add-on"

- simply good software engineering
- need to discuss failure
  - gain insight into a specific problem
  - generalize to a type of problem
  - build on past work (RISOS, PA)
- need to use this to improve understanding of how flaws arise

My Point

If attack techniques not shared, programmers and developers will not profit from the errors made by others, so quality will continue to drop

Benefits to Sharing

- knowledge of past failures
- ability to detect and repair (or warn) of them in existing software
- ability to design software to minimize threat
- ability to predict where problems might arise

Rule for Sharing Information

"Three can keep a secret ...

if two of them are dead."

- Benjamin Franklin