Implementation Issues for Electronic Commerce: What Every Developer Should Know

Chair: Avi Rubin, AT&T Labs

Panelists: Donald Eastlake, Cybercash

Kevin McCurley, IBM

Gary McGraw, RST

Cliff Neuman, USC-ISI

Most computer security problems are caused by buggy software

Most computer security problems are caused by buggy software

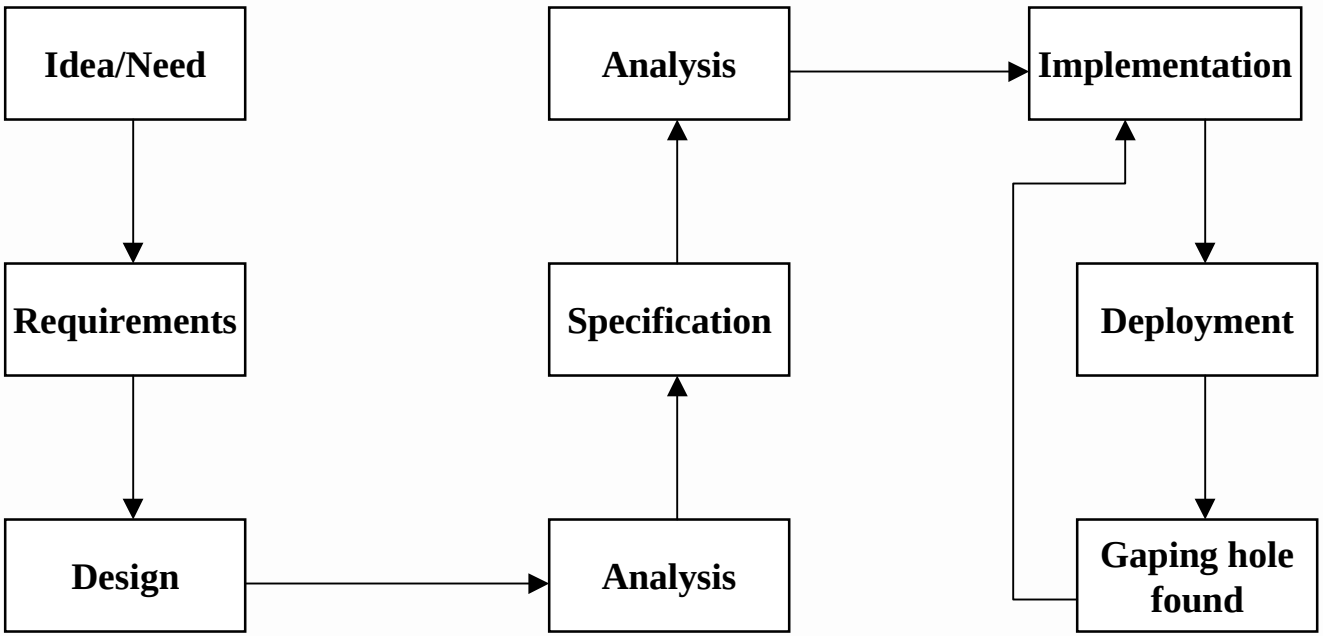
Most computer security problems are caused by buggy software

Most computer security problems are caused by buggy software

Some components of a secure system

- ✔ Sound requirements
- ✔ Flaw-free design and specification
  - automatic specification tools (*formal*)
- ✔ “Provably” secure protocols
  - logics, model checkers, complexity theoretic arguments (*formal*)
- ✔ Strong crypto algorithms
  - rigorous analysis by the whole community (*formal*)
- ✔ bug-free implementation
  - code review (*eyeballing it*)
- ✔ Others:
  - bug-free compiler, bug-free O/S, bug-free hardware (*hopeless?*)

Security system development



Examples

- ✔I.E. flaw led to shortcut files executing when URL is accessed
  - 400K patch delivered in 48 hours
- ✔PGP Passphrase cached
- ✔I.E. Res parsing problem
- ✔Netscape Mail in “secure” mode
- ✔SSH AF_Unix problem
  - users can authenticate as other users

Challenges

- ✔ E-commerce systems are being deployed
  - as fast as they can be built
  - all over the place
- ✔ How can we do more at the development stage?
- ✔ Can formal methods be applied to implementation?
- ✔ Need to educate implementers about security
- ✔ Not enough to know the API
  - must know something about how algorithms work, choices for parameters, etc.