Outrageous Opinion

Securing Bits with Atoms

(and Vices with Verses)

David Evans
evans@cs.virginia.edu
http://www.cs.virginia.edu/evans

University of Virginia
Department of Computer Science

Non-Outrageous Opinion #1

Trustworthy software is hard

...and its not getting any easier

- Software is getting more complex faster than software engineering methods are improving
- Humans aren't getting any smarter

Non-Outrageous Opinion #2

Most physical things are very trustworthy

- Bridges rarely fall down
- 13 million commercial airline takeoffs/landings in 2002 with 0 fatalities! (CNN.com, 3 Jan)
  - Hmm…there was a lot of software involved too, maybe opinion #1 needs reconsideration!

Why Software is Harder

Hardware	Software
• Continuous – Adjacent states are similar	• Discrete – Adjacent states can be completely different
• Inertia – Changes require force – Big changes require more force	• Weightless – No force required – Changing a single bit can break everything
• Visible and Touchable – Easy to see tampering	• Invisible and Odorless – Hard to smell tampering

Can we make software more like hardware?

- Yes! Computing is becoming embedded in physical stuff
- Computing elements live in physical worlds – are beginning to interact with them directly
- …but mostly indirect: sensors and actuators attached to computing devices, but programs do not integrate computing and physical environment

Tip-of-Iceberg Examples

- Location-Limited Channels [Stajano & Anderson 99 ("Resurrecting Duckling")], [Balfanz, et. al., NDSS 02]
  - Exploit physical properties of communication medium for authentication and confidentiality
- Physical One-Way Functions [Gershenfeld & Pappu, 02]
- Amorphous Computing [Abel, et. al., CACM00], Cell-Based Computing [George & Evans, WOSS 02]
  - Program global behaviors using local interactions

Motto

The Future of Software is "Shardware"

(not "Shaftware")

Any questions?

David Evans
evans@cs.virginia.edu
http://www.cs.virginia.edu/evans


University of Virginia
Department of Computer Science