Dumb Ideas in Computer Security

Dr Charles P Pfleeger
Pfleeger Consulting Group
11 April 2007
chuck@pfleeger.com

© Pfleeger Consulting Group 2007
Marcus Ranum’s Six Dumbest Ideas

  http://www.certifiedsecuritypro.com/content/view/154/90/
  - Default permit
  - Enumerating badness
  - Penetrate and patch
  - Hacking is cool
  - Educating users
  - Action is better than inaction
Struck a Nerve

- Google Results 1-10 of about 3,510,000 for dumb ideas computer security. (0.31 seconds)
- Or ... there are lots of dumb ideas related to computer security
This Talk: Misperceptions of Computer Security

- Security professionals talk to each other
- Outsiders don’t understand us
  - Outsiders aren’t dumb, just uninformed
  - People hear what they want to hear
- Dumb ideas are not new
  - References from 30+ years ago
- We have to communicate both simplicity and complexity
We’ll Do Security Later
You Can’t Retrofit Security

- Defense Science Board report
  - “It is virtually impossible to verify that a large software system is completely free of errors and anomalies
  - “System failure modes are not thoroughly understood, catalogued, or protected against
- Patches galore
- Penetrate and patch doesn’t work

Reference: Anderson
We’ll Do Privacy Later
You Can’t Retrofit Privacy

- Fair Information Practices
- Banking, medical, education, government mishmash

References: Ware, Sweeney
Encryption Cures All
Encryption is Overrated

- Key management
- Implementation flaws
- Algorithm weaknesses
- Data in the clear
  - Architecture
  - Insiders
You Have Either Perfect Security or Nothing
Security Is a Continuum

- Impossible to counter all threats
- Residual risk remains
- Need
  - Metrics to measure risk
  - Justification for stopping point
  - Creative architecture to maximize coverage for money spent
Separation is Unnecessary
Controlled Sharing Requires Separation

- 1970
  - IBM 2-state mainframes
  - DEC PDP-11 4-state minicomputers
- 1983
  - First IBM PC, Intel 8008 processor
  - Apple II, Motorola 6502 processor
- 2007
  - Intel Core, Xeon/Windows
  - IBM z/OS
  - Linux, Unix

Reference: Neumann, Karger et al
It’s Easy—We Can Do Security Ourselves
Program Complexity Inhibits Security

“By the time machines are able to do such things we shan’t know how they do it” --Turing

- Applications, utilities, infrastructure, and operating system mixed
- Web data delivery, display, fetch mixed
- Sony rootkit
- IP stack in cell phones, PDAs, gaming consoles, refrigerators, thermostats

References: Hoglund & McGraw, Whitaker & Thompson, Schneiderman
Smart Ideas in Computer Security and Privacy

- Security (professionals) can help
  - But only if we are involved early
- Beware the *widget du jour*
- Even well-known failings fail
References

References (2)


Sweeney, L., Finding Lists of People on the Web,” *ACM Computers and Security*, v37 n1 Apr 2004
