On the Brittleness of Software and the Infeasibility of Security Metrics

Steven M. Bellovin
http://www.cs.columbia.edu/~smb
Columbia University

November 21, 2006

Lord Kelvin's View

"If you can not measure it, you can not improve it."

"When you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely in your thoughts advanced to the state of *Science*, whatever the matter may be."

What About Security?

- I'd really like to know how well software resists attacks.
- Other fields have such numbers.
- Example: a wood frame wall with 2×4 studs on 16" centers, 3.5" mineral wool batt insulation, and 5/8" Type X gypsum wallboard is rated for 1 hour fire resistance. If has 2×6 studs on 24" centers with 5.5" insulation, it's rated for 2 hours.
- What is the software equivalent?
- Reluctant assertion: we not only don't have such a number, we *can't* without a major technology change

Why Not?

- Axiom: All software is buggy
- Axiom (Murphy): Anything that can go wrong, will
- Theorem: In security software, some of the bugs will be security-critical

In other words, no matter how well-audited security software is, it can contain an unsuspected hole that can be exploited very rapidly. Nor do we have any metric for how much effort a smart enemy may have to expend to find it.

Examples

- The Witty (Black Ice) worm
- Kerberized telnet encryption
- Buffer overflows and more in ssh

Software is brittle — one bug can shatter it!

What About Layered Defenses?

- Suppose we have several layers of defense
- Each layer is easily penetrated, as above
- As soon as a layer is penetrated, it doesn't hinder attacks on the next layer
- Strength is thus (at best) linear in the number of layers, and the strength of each layer is very, very low

Composition Can Introduce Flaws

- We have no science of security mechanism composition
- Incommensurate layers can result in destructive interference
- Example: Java versus firewall FTP proxies (Martin, Rajagopalan, and Rubin)
- Example: misrouting by switches and overenthusiastic firewalls

Intrusion Detection

- Intrusion Detection Systems are famous for false negatives
- Besides, an attacker can buy a copy of your system and practice attacks at home (Karger and Schell, 1974)
- Even if an IDS can detect it, it can't react fast enough against an automated attack

What We Need

- We need a way to make software less brittle
- Perhaps self-healing software will do the trick, where a hole can be closed behind the attacker
- Alternatively, we need a science of composition that gives us more than a linear increase in strength
- Until we have at least one of these, we will not have useful security strength metrics