Security Challenges

Steven M. Bellovin

`smb@research.att.com`

`http://www.research.att.com/~smb`

AT&T Labs Research

The Central Challenge: Security at Scale

- We know how to secure any one application (but only if it’s small enough)
- We can secure any single machine (if it does little enough)
- But we can’t secure large-scale systems

Cryptography

- We have good cryptography, but it’s not used very much
- Sometimes we’re waiting for the engineering and coding
- More often, it’s available but not used
- Lots of reasons; one is that we don’t know how to scale up key management in large, heterogeneous networks (especially while preserving privacy)

Human Factors

- Security mechanisms are hard to use
- It isn't clear, especially to non-experts, what the consequences are of bad choices, nor what the right choices are
- Often, there's a tradeoff between security and usability. Is this inherent, or is it an artifact of insufficient attention to human factors?
- Prime example: passwords

Intrusion-Tolerant Systems

- Most intrusion-tolerance relies on N-version programming or IDS. Both are flawed
- N-version development is expensive, and leaves systems vulnerable to common-mode bugs
- IDSs get false negatives, false positives, or both

Complex Topologies

- Most successful security mechanisms assume an “inside”, an “outside”, and a gate
- Internet, organization, firewall
- Userland, kernel, system call
- Today’s real world topologies are far more complex

Composition and COTS

- Even if we know the security properties of single systems, we don’t know the properties of composed systems
- Many essential building blocks are off-the-shelf, black boxes, whose functions — and security properties — change over time

How Secure is It?

“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.”

—Lord Kelvin

Measuring Security

- We have no quantitative measurements for security
- The best we can do — evaluations for the Orange Book or Common Criteria — is extremely expensive and of questionable general relevance
- A single programming bug can still result in a security failure

The Challenge

Given a small number of well-understood tools, an unpredictable mix of well-understood and poorly-understood components, and an arbitrarily complex topology, build a usable, secure system of known strength and resilience to component failure.

Note that we're building such systems today, but they're not secure, they're not usable, they're not resilient, and we don't understand by how much. . .