R&D Challenges: Notes from the "Trust in Cyberspace" Report

Dr. Stephen Kent
Chief Scientist- Information Security
BBN Technologies
GTE Internetworking

Another Problem Statement

- We could not build a high assurance, network information system (NIS) if our lives depended on it
- Whoops, our lives DO depend on it!
- Industry has NOT addressed this problem in almost any widely deployed products
- Government has spent lots of R&D $, but technology transfer has been relatively ineffective
- So, is there a light at the end of the security R&D tunnel (and is it other than an oncoming train?)

Other R&D Topics

- Old and new security paradigms
- A theory of insecurity
- Fine-grained access control
- Security management
- User authentication

Old & New Security Paradigms

- Emphatic assertion
- Security criteria, take 1: TCSEC, TNI, TDI
- Security criteria, take 2: ITSEC, FC, CC
- “Prevent, detect, respond”
- Immune model intrusion detection
- “Wrappers are your friends”

A Theory of Insecurity

- Must build systems from insecure COTS components, but maybe we can sprinkle in some custom stuff
- No good formal security models for real systems
- Strive for appropriate (not perfect) system security, relative to perceived (and evolving) threats
- Monitor threats and adjust countermeasures
- Recognize problem of vulnerable components; try to achieve “defense in depth”
- Need methodology for engineering “defense in depth,” vs. current ad hoc approaches
- Don’t use as an excuse for mediocre countermeasures

Fine-Grained Access Control

- Risks associated with execution of foreign code (e.g., applets) might be mitigated by use of FGAC
- For a given module, characterize “appropriate” access to system resources, and then constrain access accordingly
- Requires more than current, coarse-grained access controls in most operating systems, initial JVM, etc.
- May be enforced in various ways, e.g., interpretation, PCC, SFI, type-safe compilers, ...
- But, can users/administrators manage FGAC?

Security Management

- Many security problems can be traced to faulty configurations (ACLs, router/firewall tables, …)
- Many security-relevant products provide poor Human Machine Interfaces (HMIs), abetting misconfiguration!
- Research is needed on how to represent (to administrators) the complex NISs we are building
- Two examples
  - Tools to check for configuration problems that cross vendor and system boundaries
  - Real-time analysis of intrusion detection sensor outputs

User Authentication

- Passwords are bad! (in almost all cases)
- Encrypting passwords for transmission helps, but is not a panacea, e.g., guessing and denial of service problems remain
- Hardware tokens that act as personal cryptography devices (vs. OTP generators) are the best solutions, based on currently available technology
- Biometrics are poor choices for distributed systems
  - Biometric templates accessible at authentication servers
  - Capture of biometrics not secure, can be any bit string
  - Access to template plus ability to offer bit string response allows identity spoofing!

Conclusions

- A “target rich” environment?
- Time to revisit old assumptions about what works and what does not, to see if they are still valid
- Remember, different is not necessarily better
- If we do nothing, something will happen, and it’s not likely to be a good something