Application Security Principles

Making your Applications Hacker Resistant

Security should be considered during the entire application lifecycle and may need to deeply influence a system's design.

Security must be part of the system design and specifications, and based on the product security goals.

Added "security" later is difficult

1. It is more expensive
2. Can cause changes to features and/or application interfaces
3. Is more likely to be skipped or not given due diligence

If a system hasn't been designed to be secure, its possible that overall design may be insecure!

What Areas of Programming Should Be Secure

Basically, all code needs to be secure, especially:

1. Servers
2. Programs that communicate with core software or hosts
3. Programs that accept input from outside or use information from the environment (in particular - web applications)
4. Programs that handle mission-critical or sensitive data
5. System administration programs, as well as administration interfaces to all programs.

Even a very simple game or utility could be a Trojan or otherwise harbor malicious code.

Security Issues in Development (1)

1. Rush to complete software
2. Low user expectations
3. Security/usability balance
4. Software developers vs. Security experts
5. Programmers are not cryptographers!
6. Lack of buy in from Management
7. Lack of awareness/education
8. End users unwilling to pay required premium for security
9. Security is seldom considered in the initial stages

Security is an Issue during the entire Application Lifecycle

1. The Architecture/Design must be secure
2. The Implementation must be secure
3. The Operational environment and procedures must be secure

Vulnerability risk areas