Why Software?

* Why is software as important to security as crypto, access control and protocols?
* Virtually all of information security is implemented in software
* If your software is subject to attack, your security is broken
  * Regardless of strength of crypto, access control or protocols
* Software is a poor foundation for security

Bad Software

* Bad software is everywhere!
* NASA Mars Lander (cost $165 million)
  * Crashed into Mars
  * Error in converting English and metric units of measure
* Denver airport
  * Buggy baggage handling system
  * Delayed airport opening by 11 months
  * Cost of delay exceeded $1 million/day
* MV-22 Osprey
  * Advanced military aircraft
  * Lives have been lost due to faulty software

Software Issues

"Normal" users

- Find bugs and flaws by accident
- Hate bad software…
- …but must learn to live with it
- Must make bad software work

Attackers

* Actively look for bugs and flaws
* Like bad software…
* … and try to make it misbehave
* Attack systems thru bad software

Complexity

* "**Complexity is the enemy of security**", Paul Kocher, Cryptography Research, Inc.

system	Lines of code (LOC)
Netscape	17,000,000
Space shuttle	10,000,000
Linux	1,500,000
Windows XP	40,000,000
Boeing 777	7,000,000

- A new car contains several orders of magnitude more LOC than was required to land the Apollo astronauts on the moon

Lines of Code and Bugs

* Conservative estimate: 5 bugs/1000 LOC
* **Do the math**
  * Typical computer: 3,000 exe's of 10K LOC each
  * Conservative estimate of 50 bugs/exe
  * About 150k bugs per computer
  * 30,000 node network has 4.5 billion bugs
  * Suppose that only 10% of bugs security-critical and only 10% of those remotely exploitable
  * Then **"only" 4.5 million critical security flaws**!

Counter-Measurements: Skynet

* Fault Intrusion Tolerance
* **Features**
  * Zero-day detection
    * Risk Analysis
    * Graph mining
  * **Degradation under intrusion but maintains correctness**
  * Self-Testing
    * Introspection
    * Secure Enclaves as secure anchors
  * Self-healing

Counter-Measurements: Skynet's Architecture