Advantages of an Adversarial Mindset

Wesley McGrew
wesley@mcgrewsecurity.com

Mississippi State University
Center for Computer Security Research
Critical Infrastructure Protection Center
Questions that drive development

Is this [x] efficient?

How can I optimize [x] for efficiency?

What are the weaknesses in [x]?

How could [x] be attacked?

What could be gained by attacking [x]?
Good design and careful implementation will only take you so far

For example...

"Every access to every object must be checked for authority"

Saltzer & Schroeder's principle of Complete Mediation
Good design and careful implementation will only take you so far

Systems
Good design and careful implementation will only take you so far

Systems

Made up of complex objects
Good design and careful implementation will only take you so far.

Systems

Made up of complex objects

Communicating with other systems/objects
Good design and careful implementation will only take you so far

"Every access to every object must be checked for authority"

What constitutes an object? Where does the check take place? Access by humans, other objects?

The devil is in the details...
Good design and careful implementation will only take you so far

Implementation is even worse:

Subtle errors with serious consequences

Image Source: ms08-067 decompilation by Alexander Sotirov
http://www.phreedom.org/blog/2008/decompiling-ms08-067/
“Mainstream” IT

- Lots of experience and solid research on security
- Still has plenty of problems discovered and resolved as a result of an adversarial mindset
  - Local, Remote, Web vulnerabilities
  - Protocol issues: DNS, WEP, TKIP
Form

- Adversarial mindset takes the form of
  - Red-Teaming
  - Independent research/verification
  - Educating developers on attacks
Focus Areas

- Protocols
- Boundaries between independent systems
- Communications over distance
- Attack Surface
- Interfaces: Human-Computer
- Plug for the In-Depth Discussion on HMI :)
• It’s not perfect:
  • Different attackers find different problems
  • ...but it does fill in gaps
  • Mistakes made in design, implementation
  • Part of a process