The secure design principles of Saltzer and Schroeder

jedimaestro@asu.edu

Plagiarized from
https://sites.psu.edu/thedeepweb/2015/09/17/captain-crunch-and-his-toy-whistle/

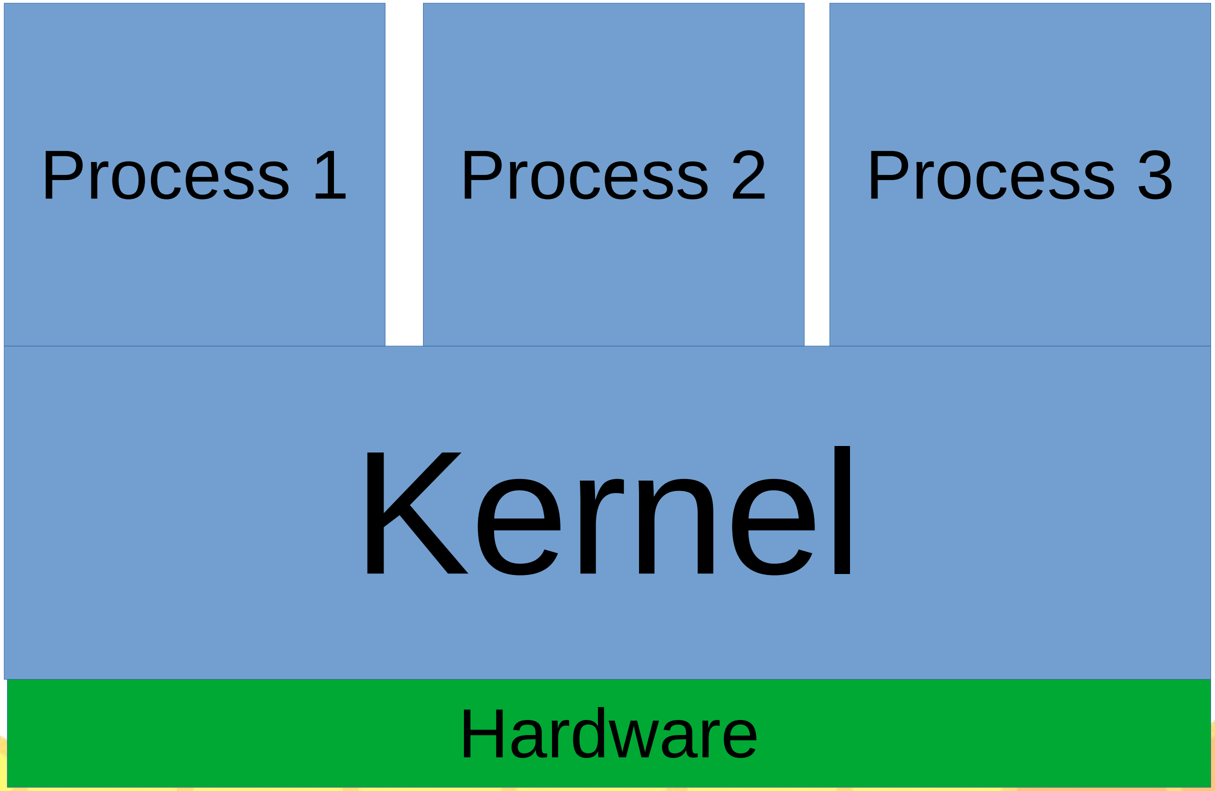
Vulnerability *vs.* exploit

Vulnerability: Condition where there is a reachable state where a security property is violated.

Exploit: The sequence of steps the attacker carries out to reach that state.

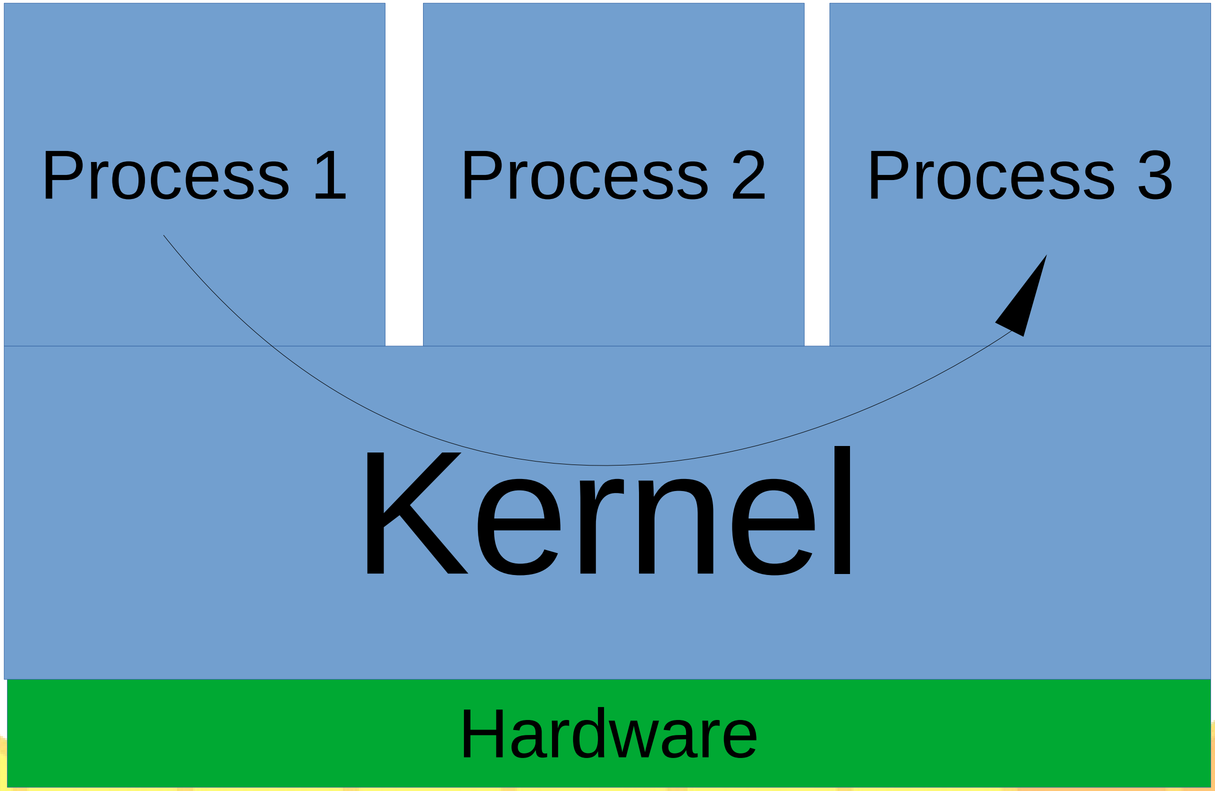
Process?

Separated by virtual memory, access system resources *via* system calls.



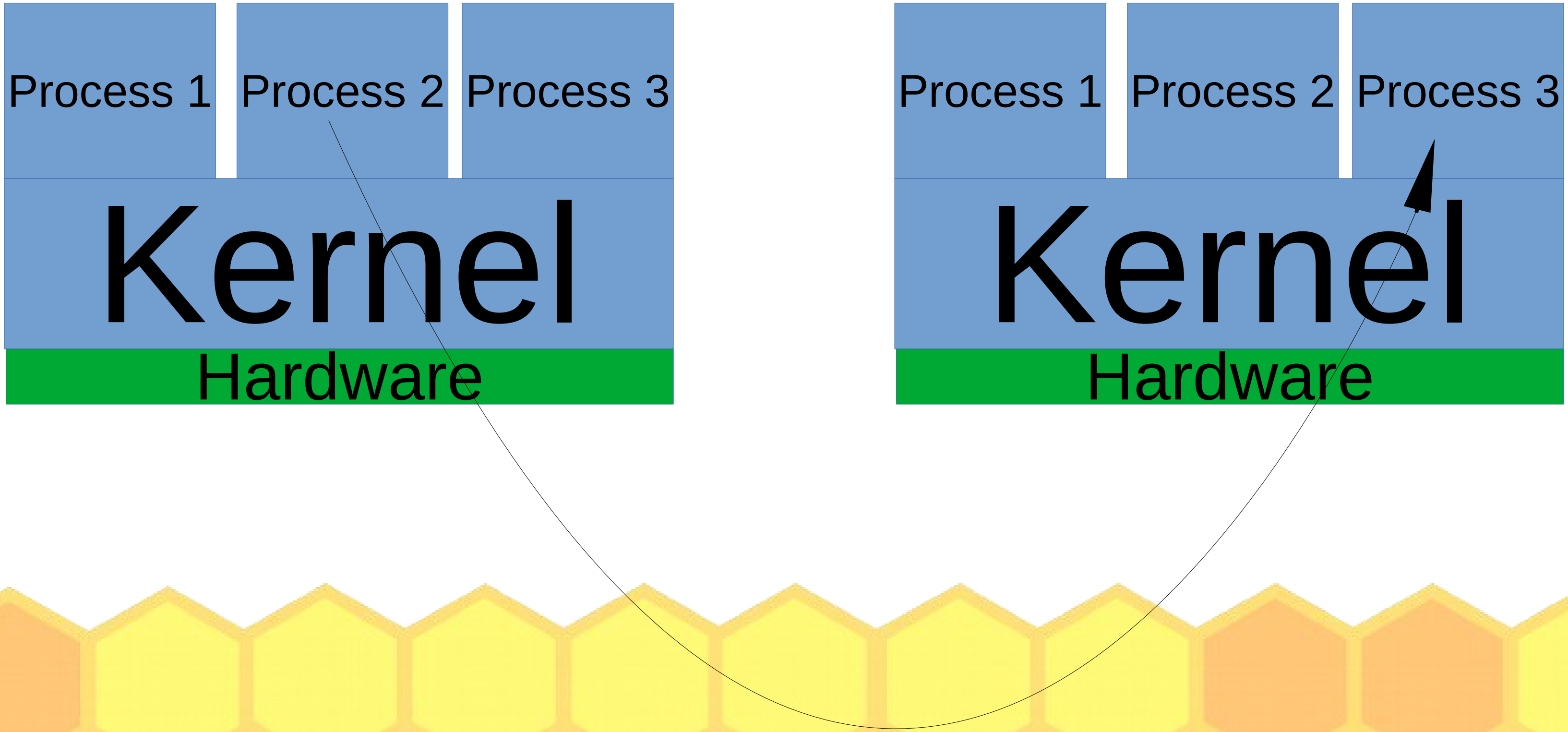
Local exploit

Privilege escalation



Remote exploit across a network

Remote shell



Process 1

Process 2

Process 3

Kernel

Hardware

Process 1

Process 2

Process 3

Kernel

Hardware

What is a vulnerability?

- Management information stored in-band with regular information?
- Programming the weird machine?
- A failure to properly sanitize inputs?

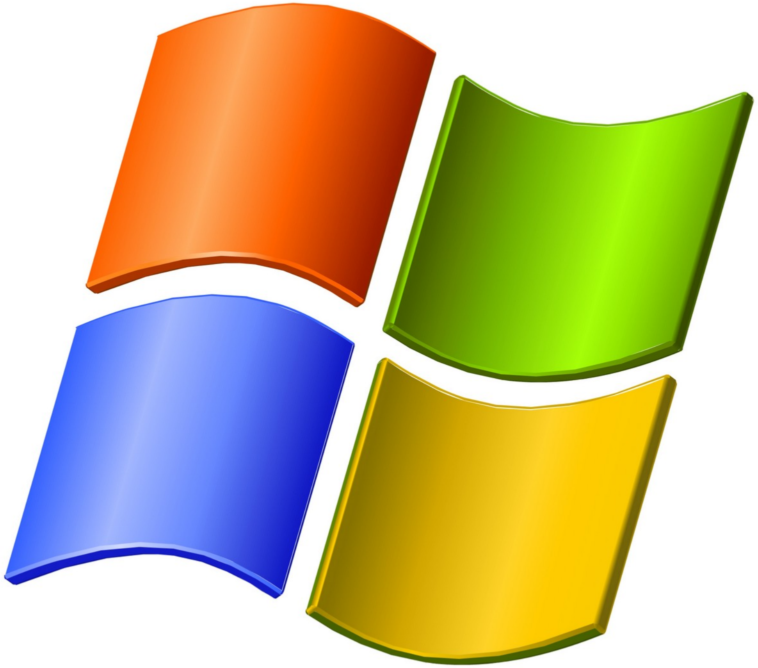
Remember: Information only has meaning in
that it is subject to interpretation.
(Also, information is inherently physical.)
(Also, the only laws on the Internet are
assembly and RFCs.)

Saltzer and Schroeder's secure design principles

- Originally published in 1973
- Amazingly prescient
- There's a cool Star Wars version online, but not everyone has seen Star Wars...

Economy of Mechanism

- “Keep the design as simple and small as possible”



Fail-safe defaults

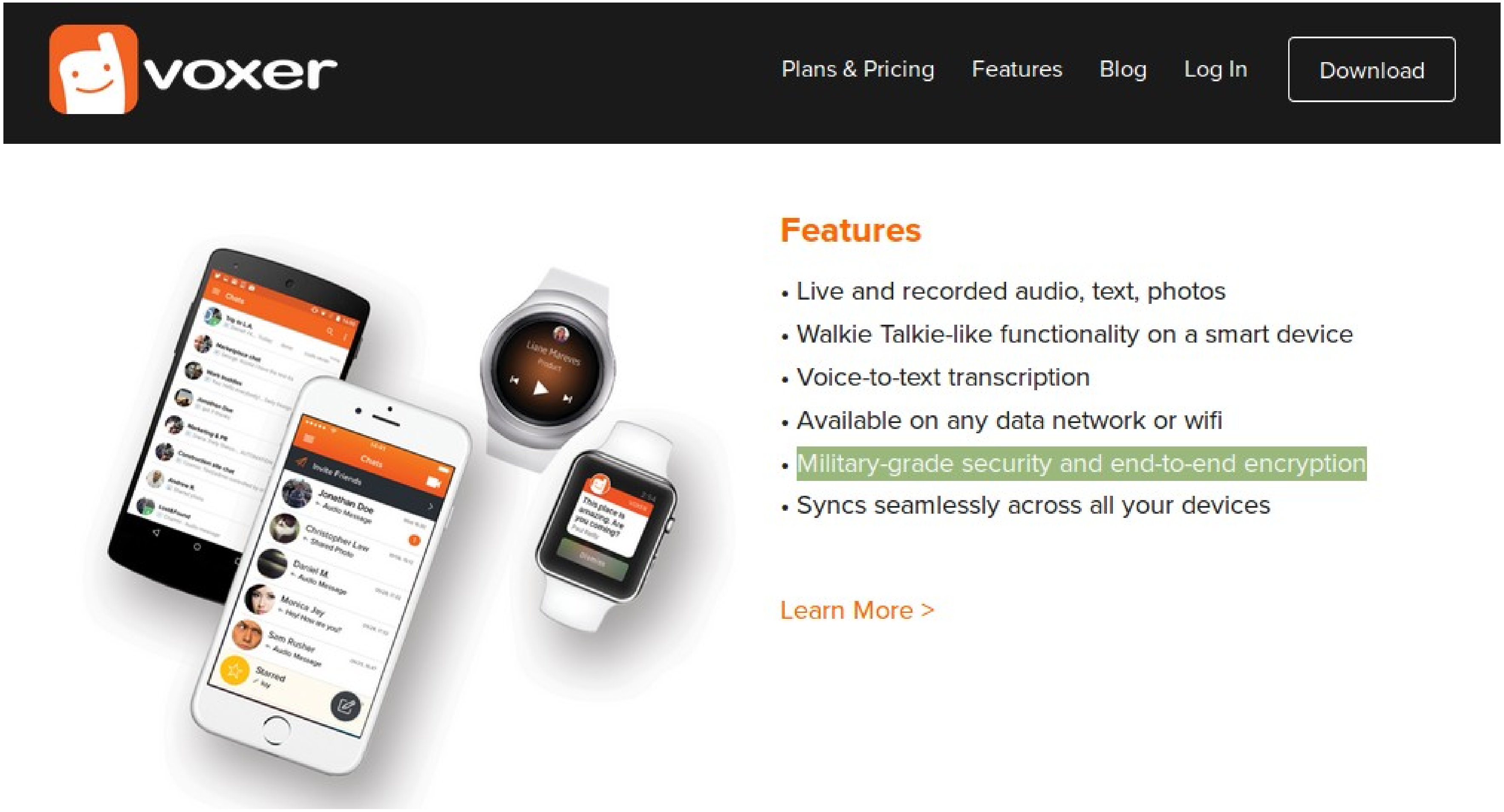
- “Base access decisions on permission rather than exclusion”

Complete mediation

- “Every access to every object must be checked for authority”

Open design

- “The design should not be secret.”



Features

- Live and recorded audio, text, photos
- Walkie Talkie-like functionality on a smart device
- Voice-to-text transcription
- Available on any data network or wifi
- Military-grade security and end-to-end encryption
- Syncs seamlessly across all your devices

Learn More >

Separation of privilege

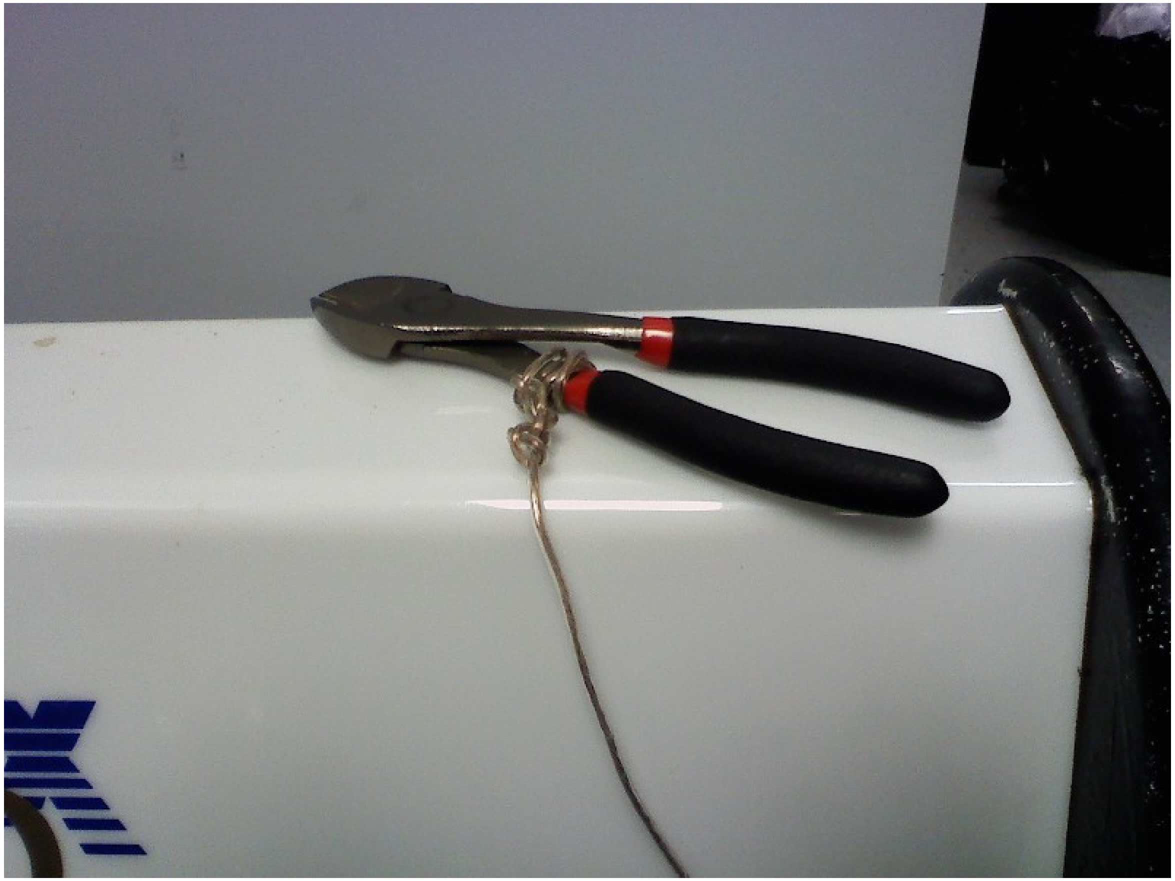
- “a protection mechanism that requires two keys to unlock it is more robust and flexible than one that allows access to the presenter of only a single key”

Least privilege

- “Every program and every user of the system should operate using the least set of privileges necessary to complete the job”

Least common mechanism

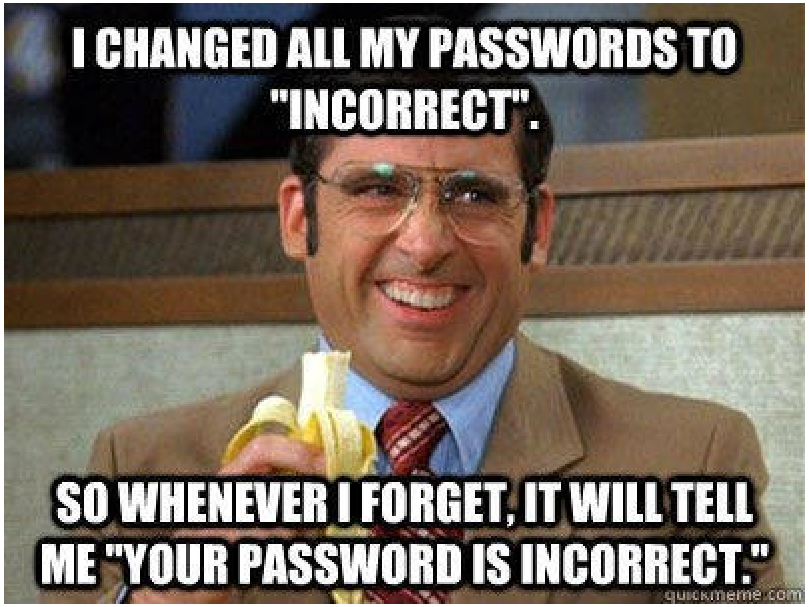
- “Minimize the amount of mechanism common to more than one user and depended on by all users”



Plagiarized from http://i.imgur.com/uWIXA.png

Psychological acceptability

- “It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly”


I CHANGED ALL MY PASSWORDS TO "INCORRECT".
SO WHENEVER I FORGET, IT WILL TELL ME "YOUR PASSWORD IS INCORRECT."
quickmeme.com

Resources

- http://www.cs.virginia.edu/~evans/cs551/saltzer/
- http://emergentchaos.com/the-security-principles-of-saltzer-and-schroeder
- Matt Bishop's *Computer Security: Art and Practice*
- *http://langsec.org/*
- *Gray Hat Hacking, 4th Edition* by Harper *et al.*
- *phrack.org*

Examples (this is my cheat sheet)

- LSASS, DACLs
- WebCT
- AS-400
- Voting machines
- Tor directory servers
- IIS in kernel
- Linking and loading
- Safety numbers