Paweł Rajba
pawel@cs.uni.wroc.pl
http://itcourses.eu/

Application Security

Infrastructure security

Agenda

- Security zone
- Firewalls
- IDS/IPS
- Platform Security
- Hardware Security
- Special Hosts
- Hardening
- Resilience

Security zone

- A set of network elements under a common policy
- Usually we can identify security zone
  - Provider, owner, policy
- Common zone types
  - Untrusted, trusted, restricted, DMZ
- Zones can split a network to the following parts:
  - External, Outside, Inside

Firewalls

- Filter traffic, separate networks
- Several firewall categories
  - Packet-filtering
    - It can be also with stateful packet inspection (SPI)
  - Proxy, reverse-proxy
    - Verifies higher levels, e.g. allows only specific users
  - Application gateways
    - E.g. allows only GET command in FTP

IDS/IPS

- Intrusion Detection/Prevention System
- Main types
  - Network IDS (NIDS)
    - Deployed as as network component
  - Host IDS (HIDS)
    - Agent on host monitoring system calls, app logs, file system modifications
  - VM Based IDS (VMIDS)
    - Monitor the VM environment

Platform security

- Platform is based on host computer
  - From smartphone to superextraserver
- Combination of hardware and OS
- Some good practices for production platforms:
  - Production env. must be separated from dev and test
  - Regular scans for changes in executables
  - Strict maintenance procedures
    - Both for hardware and software
  - Non-production software should be removed (e.g. text editors, compilers, etc.)
    - If needed they can be installed temporarily
  - Software and OS upgrades procedures should be very strict
  - Access control designed with care and based on requirements
  - Admin accounts mustn’t be used for routine operations
  - Malware protection

Hardware security

- Lack of hardware control implies problems with security in the logical layer
- Main ways to mitigate that
  - Environment under control (e.g. physical security)
  - Usage of tamper-resistant modules
    - Box protected from unauthorised use
    - Storage for cryptokeys (both symmetric & asymmetric)

Special hosts

- Dual-homed host
  - Host with multiple network interfaces
  - Can offer routing or not
  - If not, can offer shared application for different subnets
- Jump host
  - A hardened host which is an entry point to secured area
- Bastion host
  - Any firewall critical to network infrastructure

Hardening

- Reducing its surface of vulnerability
- Can be applied to any component of the IT infrastruture
  - But can be also adding a new component (e.g. IDS)
- Some examples
  - Closing selected opened ports
  - Strict access control policy
  - Applying hardening scripts changing options in OS
- Why system is not hardened by default?

Resilience

- Avoid single point of failure
  - Double everything
- Automated recovery and configuration
  - Remember about regular tests
- Comprehensive loggin and monitoring
  - To detect coming failure before it occurs
- Performance and capacity planning
  - Very connected to resilience