Next Slide

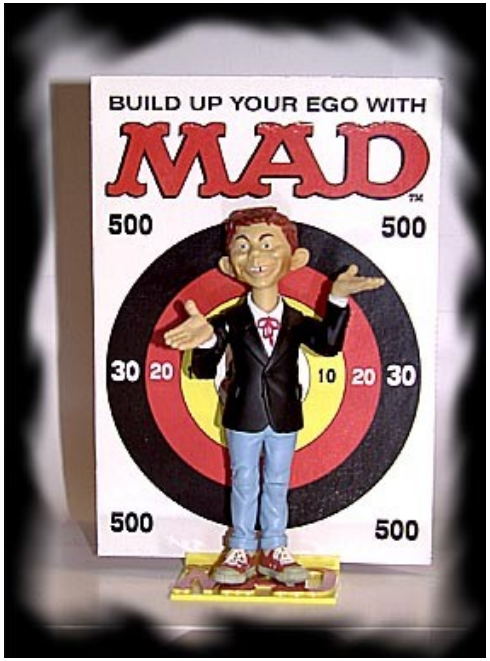
Secure, Virus-Immune & HIPAA-Compliant Health Care IT Systems

Dr. Steve G. Belovich

C 2005 IQware, Inc.

Cyber Attacks & Viruses

What, Me Worry?



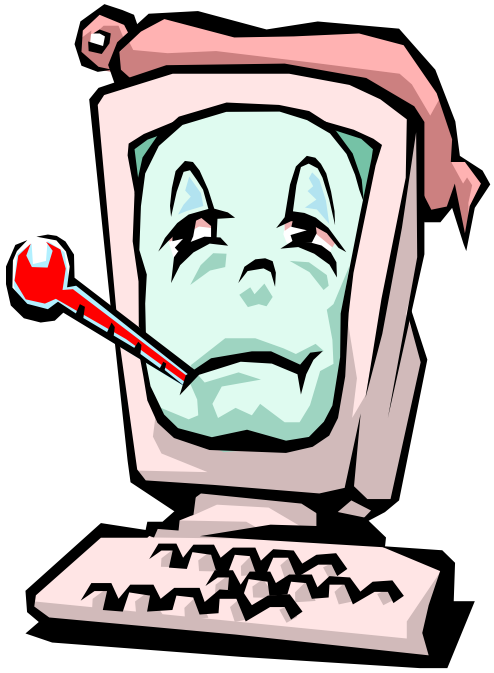
(Joe CIO)

We Care Because:

- They cause damage.
- Attacks are increasing in frequency & severity.
- Cleanup is expensive.
- Hospital operation is disrupted.
- Data loss & corruption creates potential malpractice issues (HIPAA violation)
- Potential for unauthorized data access (HIPAA violation).
- Potential for data theft (HIPAA violation).
- Insurance carriers can exclude cyber attack damage.

C 2005 IQware, Inc.

Diary of a Recent Attack



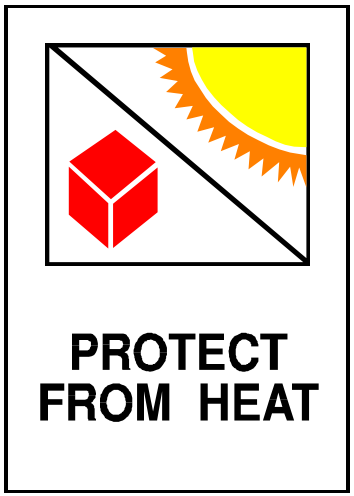
- “SQL Slammer” hit at 12:30am on 1/25/03.
- Exploited known flaws in desktop O/S, SQL Server and MDSE 2000 apps.
- Infected over 67,000 machines within 10 minutes.
- Number of copies doubled every 8.5 seconds.
- Looked for vulnerable machines at rate of 55,000,000 per second within three minutes of its appearance.
- Lack of Internet bandwidth limited replication rate.
- Bank of America lost communication with its ATMs.
- Microsoft’s own network was affected because they failed to install their own patch.
- In October 2002, Microsoft released a patch for another SQL Server problem that, if installed, would have made security-patched systems vulnerable again.

C 2005 IQware, Inc.

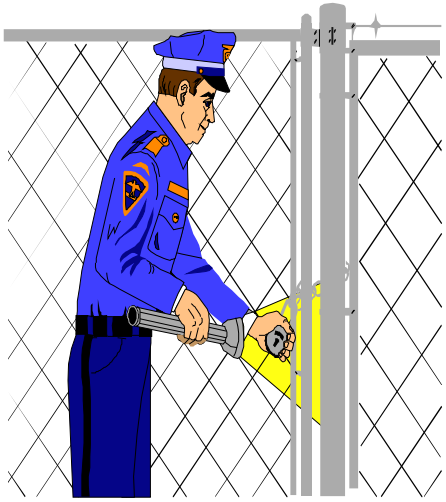
HIPAA Highlights

45CFR160, 162 and 164

February 20, 2003 (Final Rule)



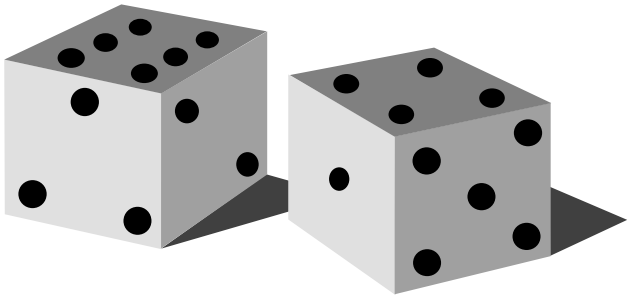
- Ensure confidentiality of all electronic records
- Protect against reasonably anticipated threats to hazards to security
- Protect against reasonably anticipated uses or disclosures
- Ensure compliance by workforce
- Security approach may be flexible
- Have to assess risks to security of information
- Can take into account existing IT infrastructure
- Implementation specifications may be required



C 2005 IQware, Inc.

45CFR 164

Implementation Specifications

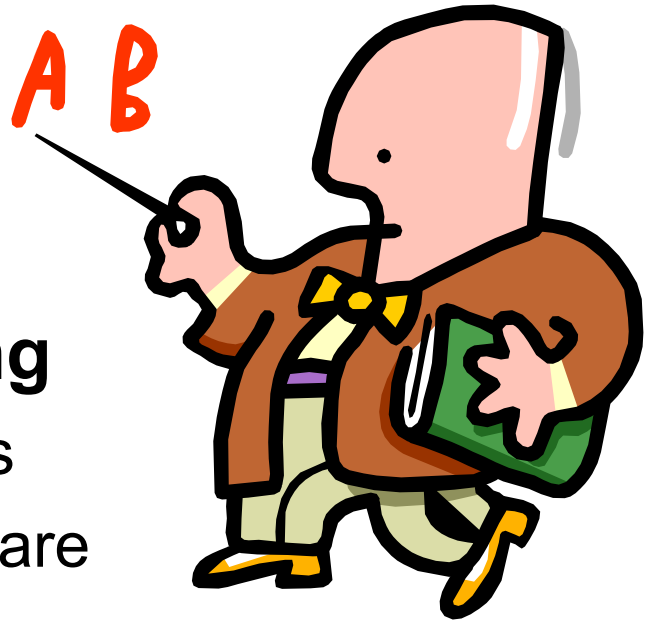


- **Risk analysis is required** - covering all potential vulnerabilities
- **Security management process is required** - implement policies to prevent, detect, contain and correct security violations
- **Risk management is required** - implement security procedures to reduce risk and vulnerabilities
- **Sanction policy is required** - apply appropriate sanctions to workforce members who do not comply with procedures
- **Information system activity review is required** - regular review of IT system activity via audit logs, security incident tracking, etc.

C 2005 IQware, Inc.

45CFR 164

Implementation Specifications



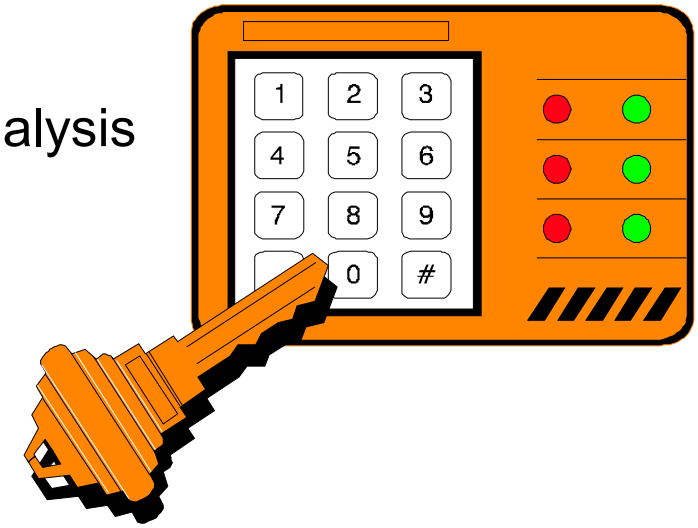
- **Security Awareness Training**
  - Security reminders and updates
  - Protection from malicious software
  - Log-in monitoring
  - Password management
- **Response and Reporting**
  - Identify & respond to security incidents (known or suspected)
  - Mitigate harmful effects
  - Document the event and outcome

C 2005 IQware, Inc.

45CFR 164

Implementation Specifications

- Contingency Plan
  - Data backup plan
  - Disaster recovery plan
  - Emergency mode operation plan
  - Testing and revision procedures]
  - Applications and data criticality analysis
- Technical Safeguards
  - Access control
  - Unique user IDs
  - Emergency access procedures
  - Automatic logoff
  - Encryption and decryption (addressable)
  - Audit trail and controls

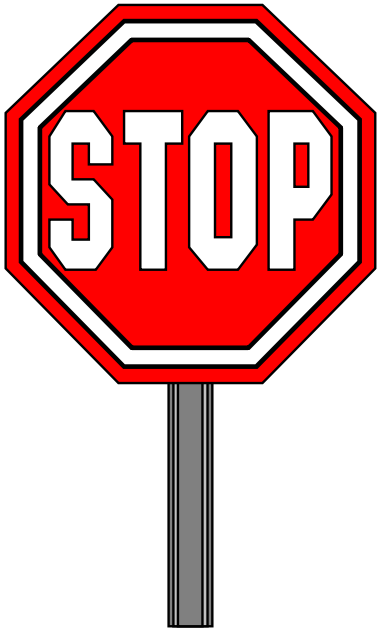


C 2005 IQware, Inc.

45CFR 164

Implementation Specifications

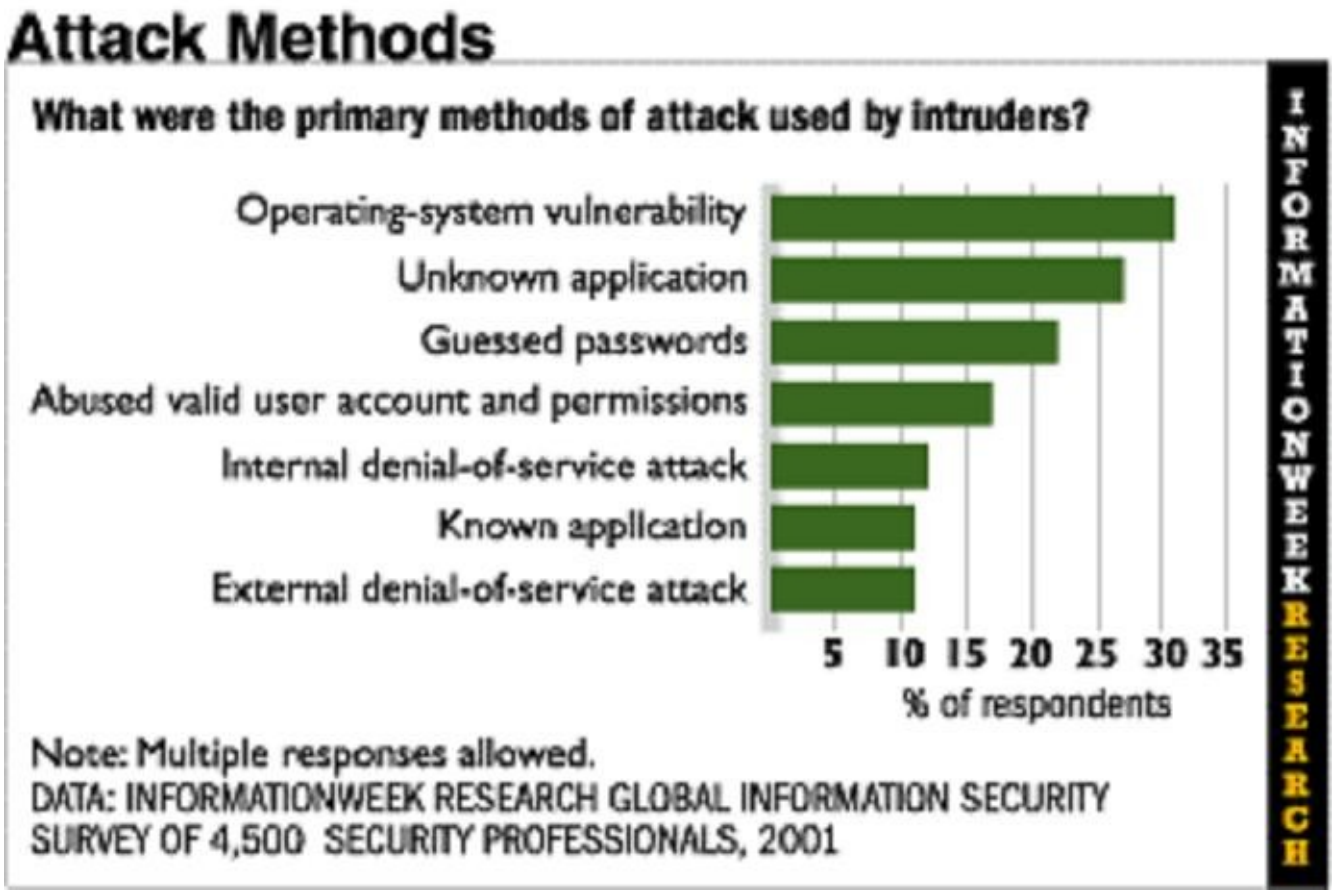
- More Technical Safeguards
  - Integrity
    - Implement policies & procedures to protect records from improper alteration or destruction
  - Authentication
    - Implement mechanism to authenticate records
    - Implement mechanism to corroborate that record has not been altered or destroyed in an unauthorized manner
  - Person or entity authentication
    - Verify that entity accessing record is the one claimed
  - Transmission security
    - Implement procedure to protect record from unauthorized access when transmitted over a network.



C 2005 IQware, Inc.

Next Slide

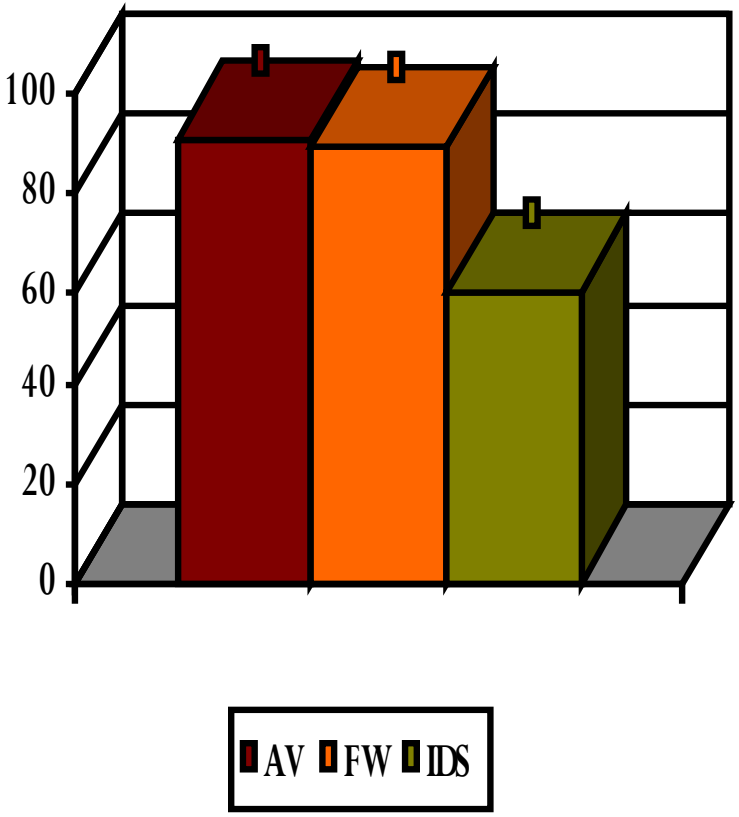
Cyber Attack Facts



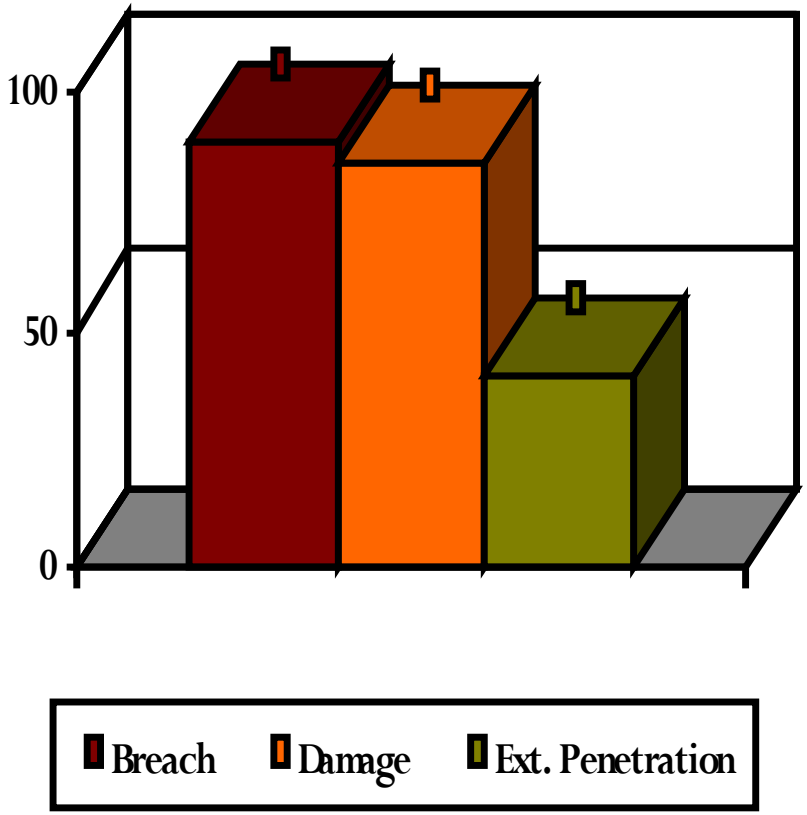
C 2005 IQware, Inc.

Cyber Attack Survey

Defense Methods



Defense Effectiveness



Source: Computer Security Institute, Computer Crime and Security Survey, April 7, 2002

C 2005 IQware, Inc.

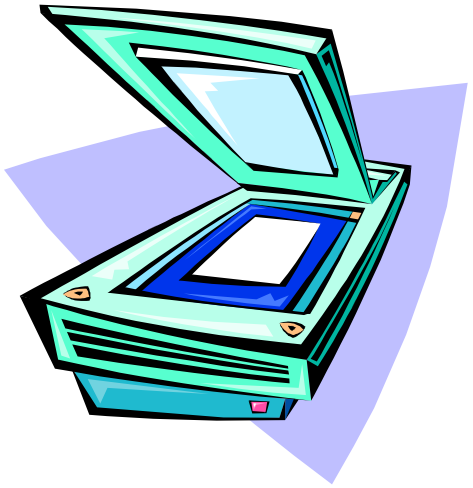
Hacker Methods: Footprinting

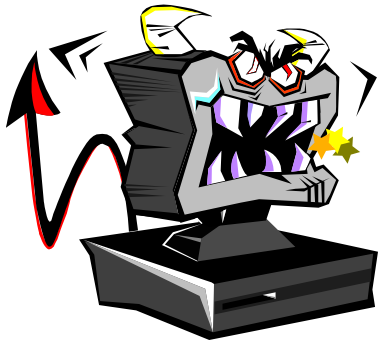
- Footprinting - discovering an organization's network information:
  - Internet - domain names, network blocks, TCP services, system architecture, IDS, ACLs, banners, routing tables, SNMP, etc.
  - Intranet - protocols in use (e.g., IP, IPX, NetBUI, etc.), network blocks, IP addresses of reachable systems, etc.
  - Remote access - VPNs & related protocols, phone numbers
  - Extranet - Access control mechanism, connection origination/destination.

C 2005 IQware, Inc.

Hacker Methods: Scanning

- Scanning - discovering which systems are alive and what they are running.
  - Ping Sweeps - sending ICMP ECHO(type 8) packets to target systems in a range of IP addresses to get ICMP ECHO_REPLY.
  - Port Scans - connecting to TCP (or UDP) ports on target system to identify services that are running.
  - Active Stack Fingerprinting - sending packets to target system and examining IP stack to detect an O/S specific implementation (e.g.,FIN packet probe, TCP initial window size, ACK value, ICMP message quoting, etc.).
  - Passive Stack Fingerprinting - passively monitoring network traffic for same purpose as above.





Automated tools

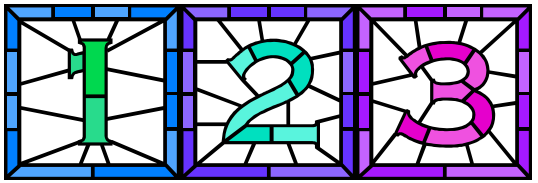
1) Superscan - www.foundstone.com/rdlabs/termsofuse.php?filename=superscan.exe
2) NetScanTools Pro 2000 - www.nwpsw.com

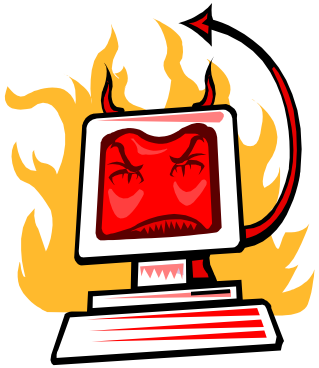
ICMP: Internet Control Messaging Protocol
TCP: Transmission Control Protocol
UDP: User Datagram Protocol

C 2005 IQware, Inc.

Hacker Methods: Enumeration

- Enumeration - identifying valid information about the following areas:
  - Network Resources and Shares
  - Users and Groups
  - Applications and Banners
- Enumeration techniques are O/S specific, including:
  - Password guessing
  - Eavesdropping on network password exchange
  - Denial-of-Service (DOS)
  - Buffer Overflows





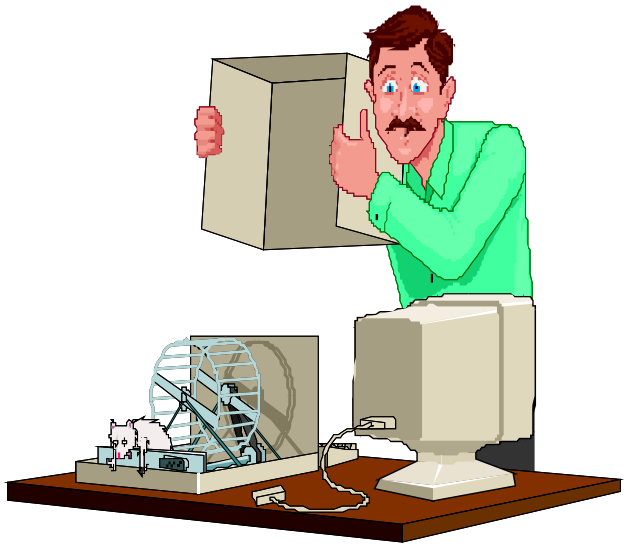
Buffer Overflow Exploiting

1) Phrack 49/14 & 55/15, www.phrack.org
2) www.cultdeadcow.com (general hacking stuff)

C 2005 IQware, Inc.

Health Care Implications:

- There are a lot of hacker tools & techniques available on the web.
- IT skill sets are global.
- Anti-virus software helps.
- Firewalls help.
- Intrusion detection systems help.
- All of them can be penetrated!

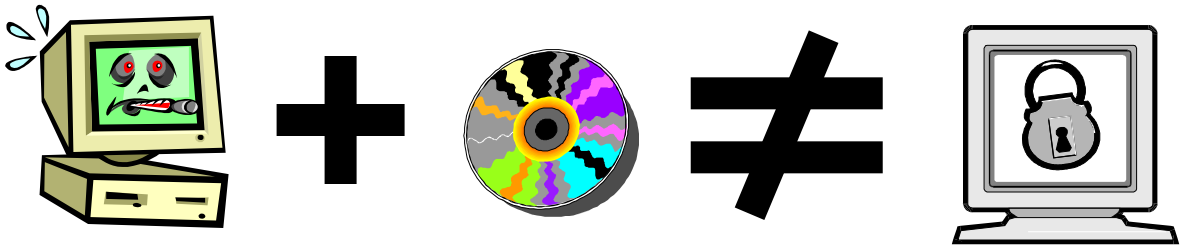


Health Care Conclusion:

- Current cyber defense schemes aren't 100% effective.
- Have to use a different approach.

C 2005 IQware, Inc.

Why is There No Simple Security Solution?

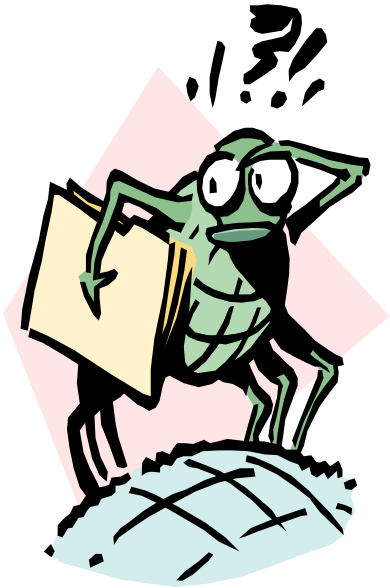


Insecure System "Magic Software" Secure System

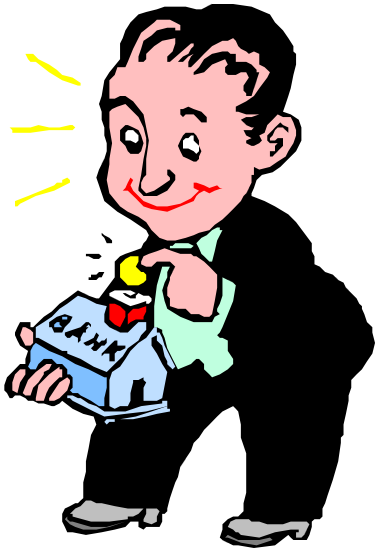
- Software ***architecture*** is critical to security and reliability - the language or development environment is not.
- Proper security-oriented changes to desktop O/S would force significant changes to the ***entire installed application software base.***
- Security is more of an economic issue than a technical one.
- Security cannot be just "added-on".
- A mythical desktop security "add-on" cannot be compatible with existing IT infrastructure.
- A "magic-CD" that will 100% protect your desktop ***without any other changes*** is not possible now.

C 2005 IQware, Inc.

Health Care IT Issues



- How can I be HIPAA compliant (and convince the auditors)?
- How can I be compliant with other regulatory agencies?
- How can I implement new functionality across existing IT systems?
- How can I be secure and immune to cyber attacks?
- How can I integrate different facilities' disparate IT systems?
- How can I take advantage of new technology?
- How can I do all of this and still save money?

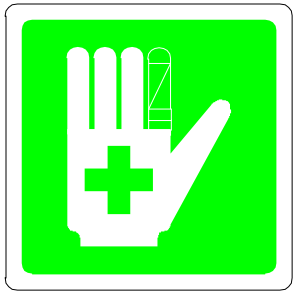


C 2005 IQware, Inc.

Firewalls & Anti-Virus Software

What They Can Do

- Firewalls help protect desktops against network transmitted viruses.
- Anti-virus software scans and finds instances of known viruses.



What They Cannot Do

- Prevent damage from new viral strains.
- Clean up damage from cyber attacks.
- Prevent critical data loss from cyber-thieves.
- Prevent damage from operator error(s)
- Ensure proper operation of application software
- Make the IT system tamper-proof.
- Provide 100% security.

C 2005 IQware, Inc.

Next Slide

The OSI 7-Layer Model

Of network-oriented software

Protection Methods

IQware™

No method to guarantee that your applications work correctly.

Encryption, firewalls, anti-virus software, intrusion detection systems, etc.

Cardkeys, Biometrics, etc.

Applications
Admitting
Clinical & LIMS
Patient Tracking
Reporting & Scheduling
Financial/HR

Presentation

Session

Transport

Network

Data Link

Physical

- The applications do the useful work - they are the “payload” of your IT system.
- The 6 underlying logical layers are there to support and enable the application.
- All seven layers must be protected to have 100% security.
- Protecting just the lower layers via firewalls and anti-virus software is not enough - as experience has proven.

C 2005 IQware, Inc.

Security Research Results

- Security has been important (to "techies") for about 40 years.
- Research on security which started in the 1960s (and through the 1980s) led to three important conclusions:
  - Discovering security flaws then fixing them one-by-one will NOT work.
  - Effective security can only be achieved by **architecting** a system in accordance with a secure system model.
  - Effective security requires proper architecture, coding and deployment of the O/S, the application and all layers in between.

Putting out fires doesn't work!

C 2005 IQware, Inc.

What Secure Systems Must Do

- **Policy**
  - **Security Policy** - System must enforce a well-defined security policy.
  - **Marking** - System must associate all objects with access control labels (sensitivity & access modes).
- **Accountability**
  - **Identification** - System must identify individuals and their various authorizations in a secure manner.
  - **Audit Trail** - System must keep & protect audit trail so actions may be traced to responsible party.
- **Assurance**
  - **Evaluation** - System must have hardware/software mechanisms that can be independently evaluated to assure that policy & accountability are enforced.
  - **Continuous Protection** - System must continuously protect trusted mechanisms that enforce policy & accountability from tampering.

C 2005 IQware, Inc.

Secure System Classifications

- **DoD Rating System**
  - 7 levels of security.
  - Grades are level D (lowest), C1, C2, B1, B2, B3, A1 (highest).
  - Emphasis is on structure.
  - All desktops in in level D - too low to even bother rating.
- **NIST and NIAP Rating System**
  - 7 levels of security.
  - Grades are EAL-1 (lowest) thru EAL-7 (highest).
  - Emphasis is on external testing.
  - Better definitions than DoD but not as rigorous.

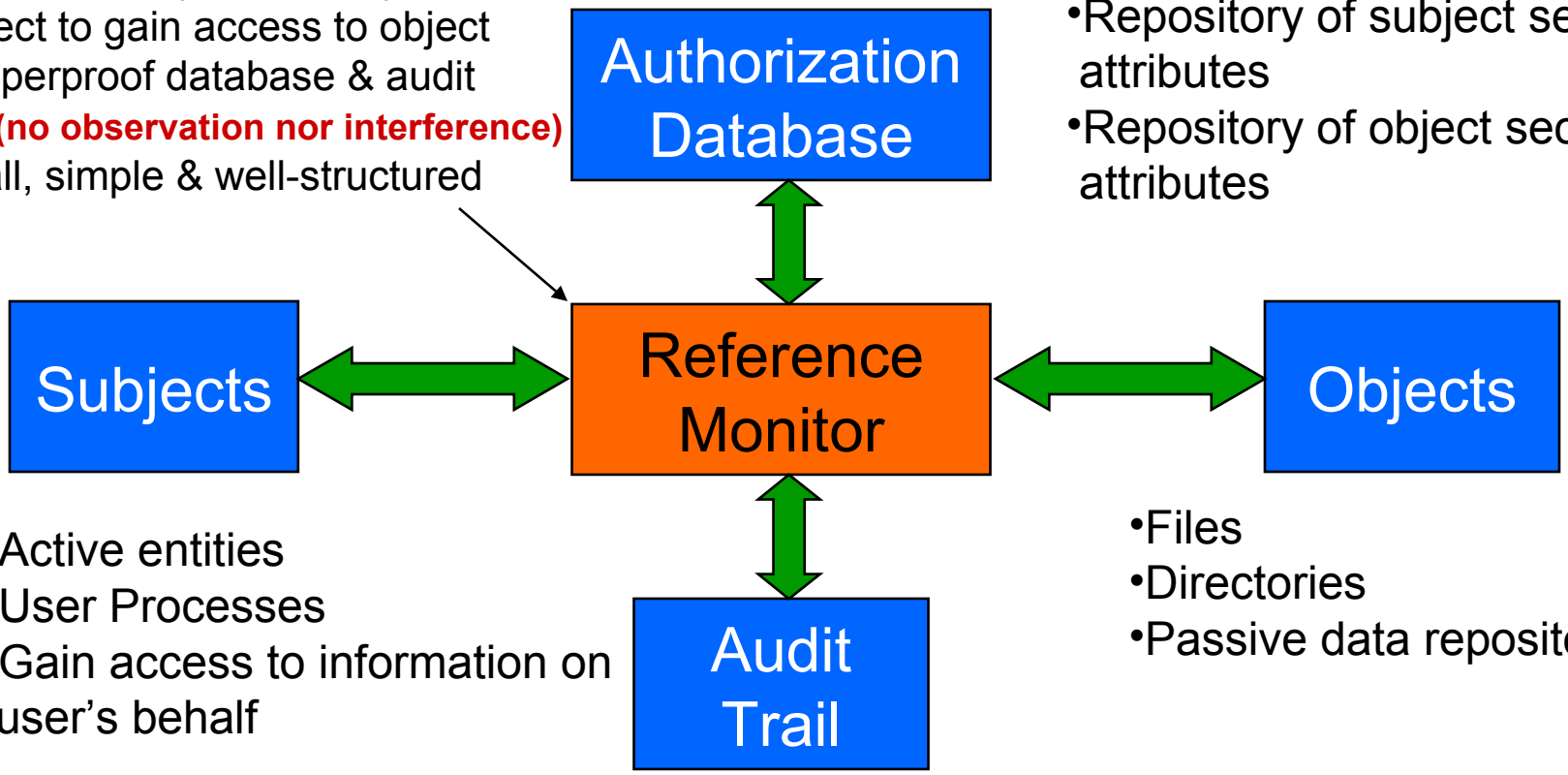
(NIST - National Institute of Standards & Technology)
(NIAP - National Information Assurance Partnership)
ISO 15408

C 2005 IQware, Inc.

The Reference Monitor

(A Secure System Architecture)

- Enforces security policy
- Mediates every attempt by subject to gain access to object
- Tamperproof database & audit trail **(no observation nor interference)**
- Small, simple & well-structured



- Repository of subject security attributes
- Repository of object security attributes

- Active entities
- User Processes
- Gain access to information on user's behalf

- Files
- Directories
- Passive data repositories

- Record of all security-related events

C 2005 IQware, Inc.

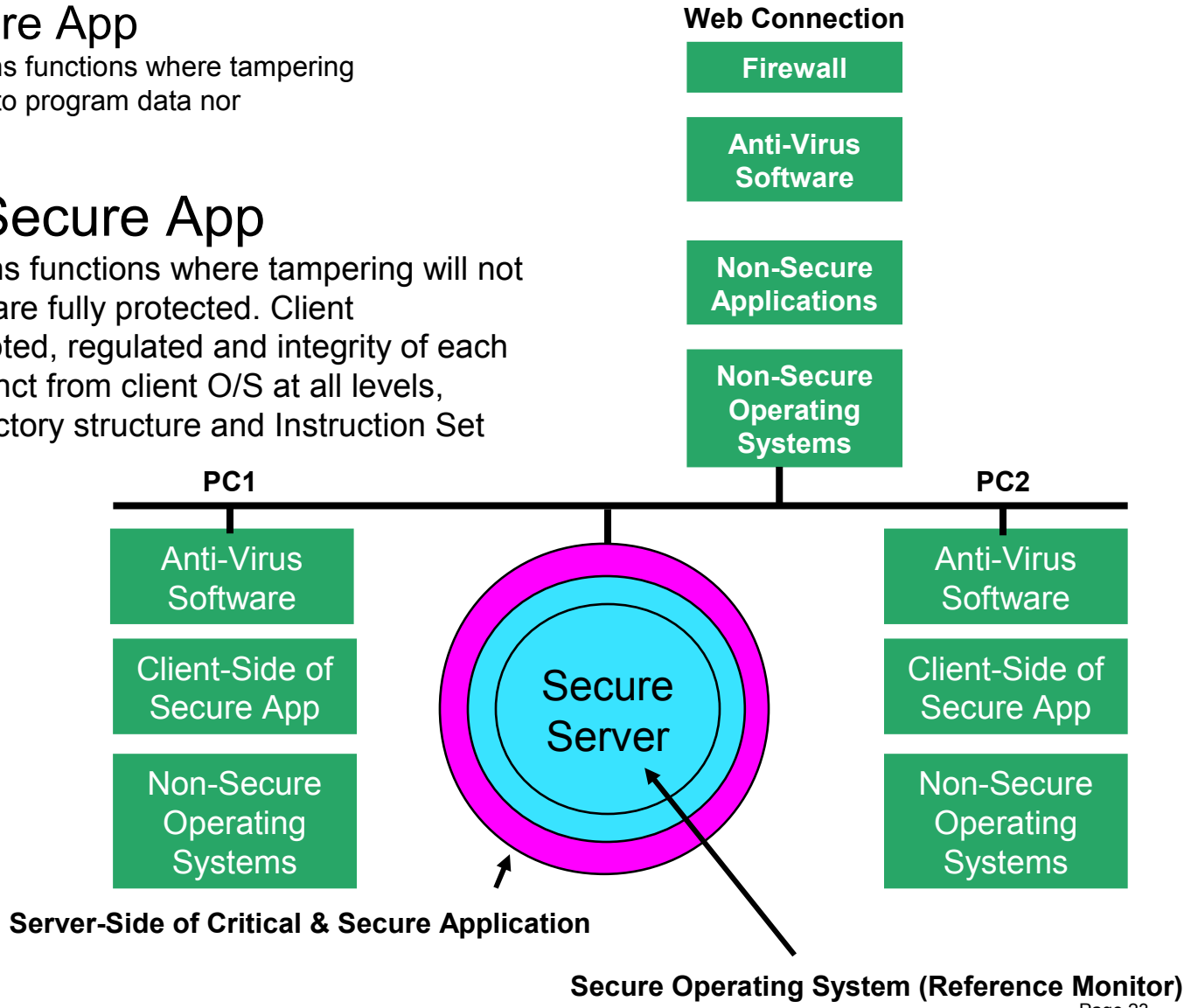
A Secure HCIS Architecture

Client Side of Secure App

Performs non-critical applications functions where tampering may occur but is not damaging to program data nor program operation

Server Side of Secure App

Performs critical applications functions where tampering will not occur. Data and programs are fully protected. Client communications are encrypted, regulated and integrity of each transaction is verified. Distinct from client O/S at all levels, including file structure, directory structure and Instruction Set Architecture (ISA)



C 2005 IQware, Inc.

IQware Software Advantages

(Patent-Pending)

- **Secure and Virus-Immune -** The only one in the business, full protection from cyber attacks, hackers & malicious software.
- **HIPAA compliant -** Exceeds most 45CFR164 rules, full protection from unauthorized health care data access.
- **Rule-Based -** can alter/upgrade the functionality on-the-fly without writing costly, high-risk code.
- **Interoperable -** Can work with any desktop or palmtop, including Linux, Mac, Windows, PDAs, etc.
- **Non-intrusive installation -** No need for an expensive overhaul of existing IT infrastructure to deploy - in sharp contrast to traditional HCIS and ERP systems.

C 2005 IQware, Inc.

Final Thoughts

- Unique software technology delivers HIPAA compliance at reasonable cost.
- 100% defense against critical data loss from cyber attacks.
- Prevent malpractice issues due to patient data corruption.
- Reduce insurance costs by implementing best practice and reduce uninsur(able) exposures.
- Reduce IT costs across the enterprise.
- Effective decision-making using real-time, accurate information.
- Facilitate outsourcing by rule-based architecture.

C 2005 IQware, Inc.