IT Security Foundations ICCM June 2003 – Session One

Today's Presenter is sponsored by
Compass Technology Management

Don Murdoch, CISSP,
MCSE, MCSD

Agenda

- Part One – Basics Topics
  - The Ten Immutable Laws of InfoSec
  - The CIA Triad
  - Some statistics and history
  - The Threat Continuum
- Part Two: Information Security Foundations
  - Discuss each of the ten knowledge domain
- Credits
  - *The overall structure of much of this presentation is based on the SANS curricula and the ISC2 Common Body of Knowledge (CBK)*
  - *www.cccure.org – the definitive CISSP study site*
  - *Some material is from MSFT Security Clinic (2800)*
  - *Mush of basic information is from www.cccure.org*

Foundational Knowledge Domains for an InfoSec Practitioner (ISC^2)

- Access Control
- Application and System Development
- Cryptography
- Disaster Recover and Business Continuity
- Law, Investigation and Ethics
- Operations Security
- Physical Security
- Security Management Practices
- Security Models
- Telecommunication and Network Security

Topic One:
The Ten Immutable Laws of Information Security

The Ten Immutable Laws from Scott Culp at Microsoft (1/2)

- Nobody believes anything bad can happen to them, until it does.
- Security only works if the secure way also happens to be the easy way.
- If you don't keep up with security fixes, your network won't be yours for long.
- It doesn't do much good to install security fixes on a computer that was never secured to begin with.
- Eternal vigilance is the price of security.

The Ten Immutable Laws from Scott Culp at Microsoft (2/2)

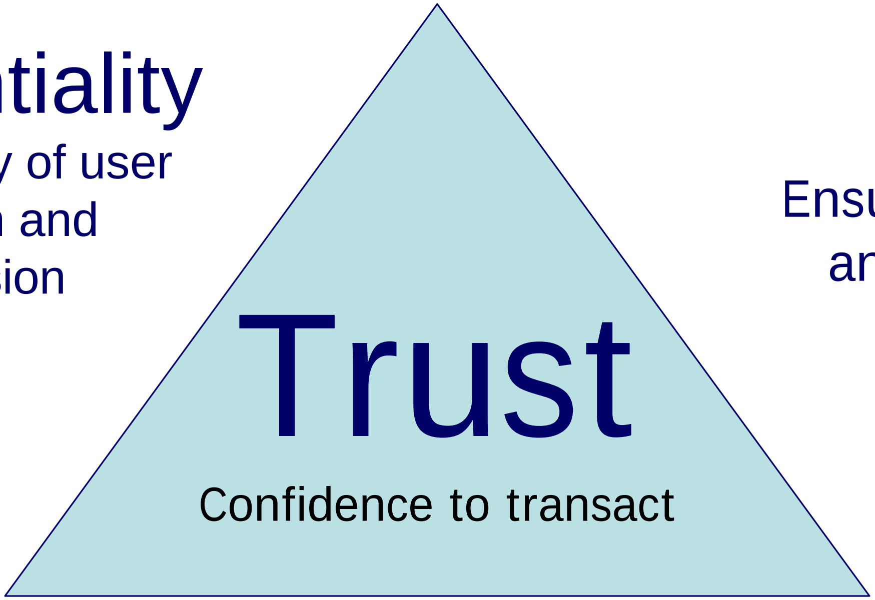
- There really is someone out there trying to guess your passwords.
- The most secure network is a well-administered one.
- The difficulty of defending a network is directly proportional to its complexity.
- Security isn't about risk avoidance; it's about risk management.
- Technology is not a panacea.

Ten Laws – Boiled Down

- Following and practicing sound Information Security is not a one time event – treating it as such is a recipe for intrusions, attacks, exploits and eventual system compromise
- The only secure machine is a disconnected machine with strong physical access controls, one door, and two operators at all times.

Topic Two:
The CIA Triad and Statistics

The CIA Triad



Confidentiality

Ensure privacy of user information and transmission

Integrity

Ensure accuracy of data and data processing

Trust

Confidence to transact

Availability

Maximize functionality and uptime

Lessons from history

- 2003 - According to an Information Security survey of 518 senior security managers:
  - Just over half (53%) of those surveyed said their information security budgets would increase in 2003
  - 16% said their budgets would increase by over 20%
  - 30% said their budgets would remain flat in 2003
  - 17% said their budgets would decrease
- 2001/2002 Time Frame:
  - Nearly 50% of all network attacks come from the inside. (Source: CSI/FBI/Ernst and Young)
  - Over a 12-month period, businesses lost nearly $1.6 trillion in revenue due to unplanned downtime caused by security related incidents (InformationWeek.com online)
  - Klez-H is the worst virus ever, according to figures from managed services firm MessageLabs, which has blocked 775,000 (4/15) – 1 in 300 messages are infected (the Register online).

Statistics: Universal Risk

- Computer Crime and Security Survey (01/02)
  - 90% detected computer security breaches
  - 40% detected system penetration from the outside; up from 25% in 2000
  - 40% of respondents quantified financial losses at $456 million, or $2 million per respondent
  - 85% detected computer viruses
- CERT – Misconfiguration the cause of 95% of all breaches
- InformationWeek estimates:
  - Security breaches cost businesses $1.4 trillion worldwide in 2002
  - 2/3 of companies have experienced viruses, worms, or Trojan Horses
  - 15% have experienced Denial of Service attacks

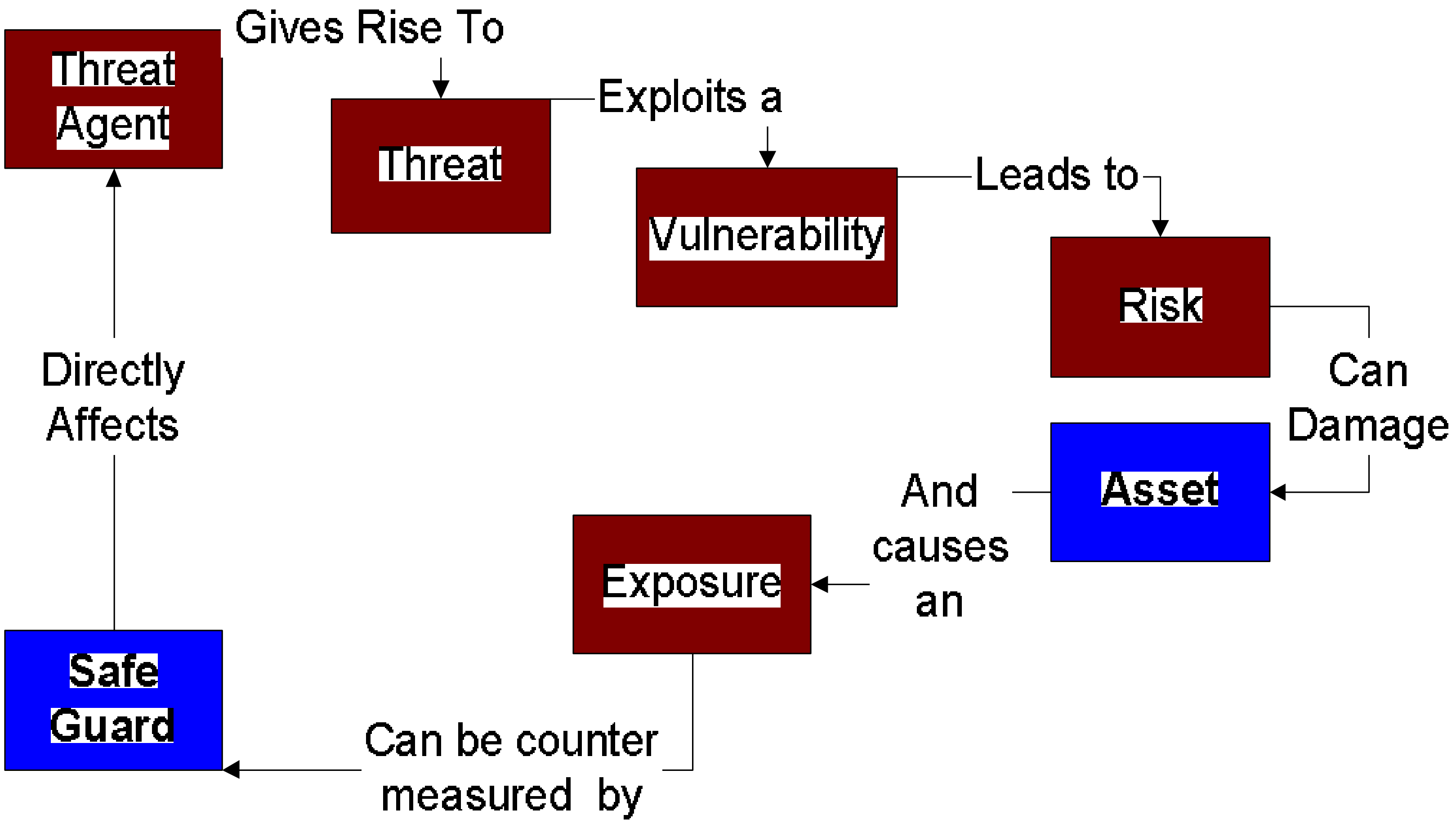
- **Sources: Computer Security Institute (CSI) Computer Crime and Security Survey 2002 and www.CERT.org (2002)**

Topic Three:
The Threat Continuum

Your path to vigilance.

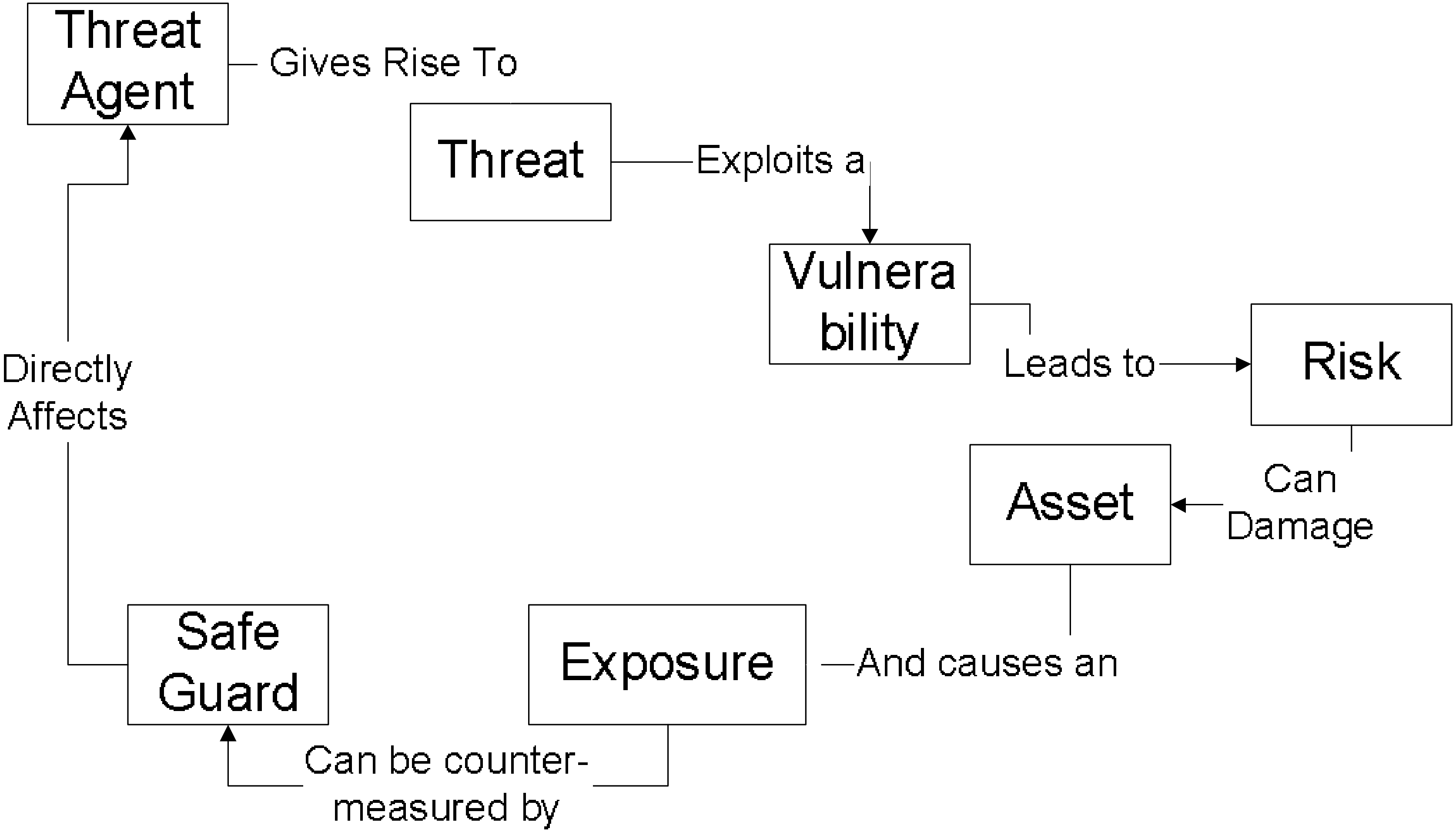
Important terms and definitions.

Threat/Countermeasure Analysis Process



Source: CISSP Certification Handbook,
Shon Harris, © 2002 & US DoD Common Criteria

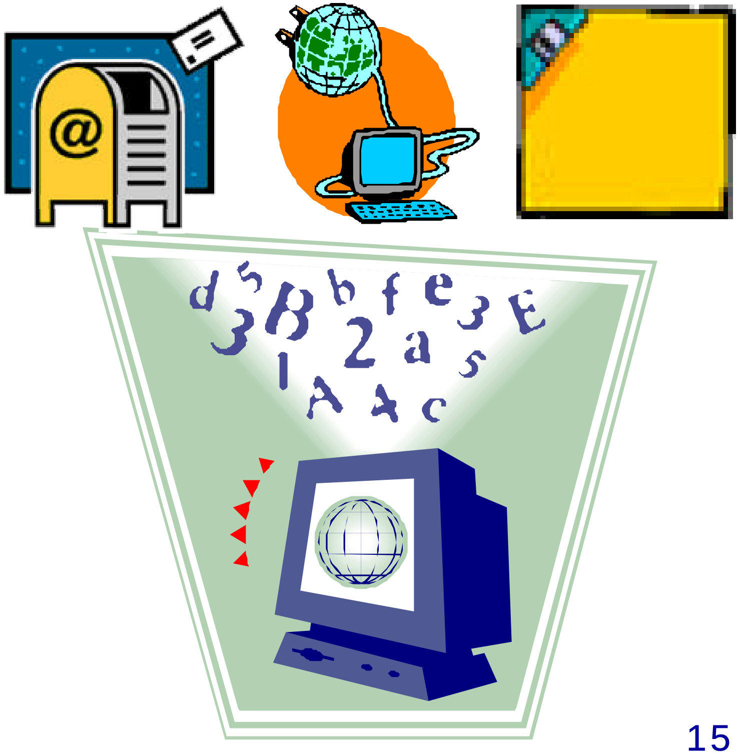
Threat/Countermeasure Analysis Process



Source: CISSP Certification Handbook,
Shon Harris, © 2002 & US DoD Common Criteria

Threat Agents

- *Any* way that a threat can be delivered to your system
- Web, diskette, email, shareware, macros
- Accidental or sabotage
- CIA
  - *How can your messages and data be compromised?*



Threats

- *Any* potential danger to a system
- From within and without
- More complex systems have larger surface area

Threat - Vulnerability – Risk

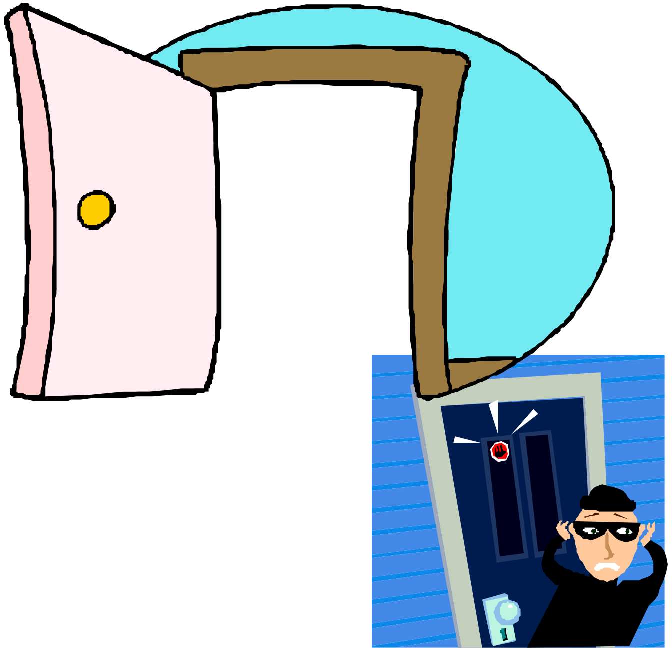
- Threat: Any potential danger to a system
  - Receiving Viruses; Information Theft
- Vulnerability: A weakness in the system
  - Older AV definitions; Information Leakage
- Risk: The loss potential or probability
  - Document archive infected; trade secrets lost
- CIA
  - Where can integrity break down?

Vulnerability

- A weakness in the system
  - Software and / or hardware
  - Procedures and policies
- Provides an attacker with a “way in”
- New vulnerabilities are discovered all the time
- See cve.mitre.com

Risk

- The likelihood that a threat agent will take advantage of a vulnerability
- The loss potential or probability of a loss to an information asset



(Information) Assets

- Information owned by the company
- Information company is responsible for
- Resources the company has / uses / needs
- Company image
- CIA
  - How open is your system internally within your company?

Confidential Data
Trade Secrets

Defining Acceptable Risk - Part 1

- Quantitatively – each risk is measured
  - Determine the value of information
  - Estimate potential loss and frequency
  - Analyze threats to the assets
  - Determine ALE
  - Cost of remedial measures
  - Reduce/Assign/Accept
- CIA
  - Cost of availability?

$ALE = AV * EF * ARO$

ALE: Annualized Loss Expectancy

AV: Asset Value

EF: Exposure Factor

ARO: Annualized Rate of Occurrence

Defining Acceptable Risk - Part 2

- Qualitatively – each scenario is considered
  - Review risks and apply judgment, intuition, experience about the threats
  - Apply history and intestinal fortitude
  - Write scenarios and determine and match threats, likelihood, safeguards to assets
- CIA
  - How confidential is your information?
  - When has data been unavailable in the past?

Access Control

Access Control Systems & Methodology – the mechanisms that systems managers can use to influence the system’s behavior.

Access Control Topics

- IAAA
  - Identification
  - Authentication
  - Authorization
  - Accountability
- Techniques, technologies
- Monitoring and Auditing
- Methods
  - Administrative
  - Physical
  - Technical
  - Layers

- Access Control Implementation
- MAC & DAC
- Authentication
- Passwords
- Tokens/SSO
  - Kerberos
- Intrusion Detection Systems
- RAS Access Control
- Penetration Testing

What is Access Control?

- Access control is the heart of security
- Definitions:
  - The ability to allow only authorized users, programs or processes system or resource access
  - The granting or denying, according to a particular security model, of certain permissions to access a resource
  - An entire set of procedures performed by hardware, software and administrators, to monitor access, identify users requesting access, record access attempts, and grant or deny access based on preestablished rules.

Access Control Nomenclature

- Identification
  - Process through which one ascertains the identity of another person or entity
- Authentication
  - Process through which one proves and verifies certain information
- Authorization
  - The user has permissions to access data/resource
- Confidentiality
  - Protection of private data from unauthorized viewing
- Integrity
  - Data is not modified in any unauthorized manner
- Availability
  - System is usable. Contrast with DoS.

Authentication (1/2)

- 3 types of authentication:
  - Something you know
    - Password, PIN, mother’s maiden name, passcode, fraternity chant/handshake
  - Something you have
    - ATM card, smart card, token, key, ID Badge, driver license, passport
  - Something you are
    - Fingerprint, voice scan, iris scan, retina scan, body odor 7(hopefully not …), DNA

Authentication Practical Examples

- Anonymous access – any ole’ Joe
- Network Credentials
  - NT Domain, Kerberos
- IIS Web Server– various levels
  - Basic (clear text password)
  - Digest authentication
  - Integrated Windows authentication (NTLM)
  - Certificate – PKI based
- Remote Access
  - RAS – PAP, CHAP, MSCHAP, ...
  - Hardware Based (SecureID)

How is Access Control Implemented?

- Administrative
  - includes policies and procedures, security awareness training, background checks, work habit checks, a review of vacation history, and increased supervision.
- Logical or Technical
  - Involves the restriction of access to systems and the protection of information. Examples of these types of controls are encryption, smart cards, access control lists, and transmission protocols.
- Physical
  - incorporates guards and building security in general, such as the locking of doors, securing of server rooms or laptops, the protection of cables, the separation of duties, and the backing up of files.

Proactive Access Controls

- Awareness training
- Background checks
- Separation of duties
- Split knowledge between staff
- Policies (which are followed...)
- Data classification
- Effective user registration
- Termination procedures
- Change control procedures

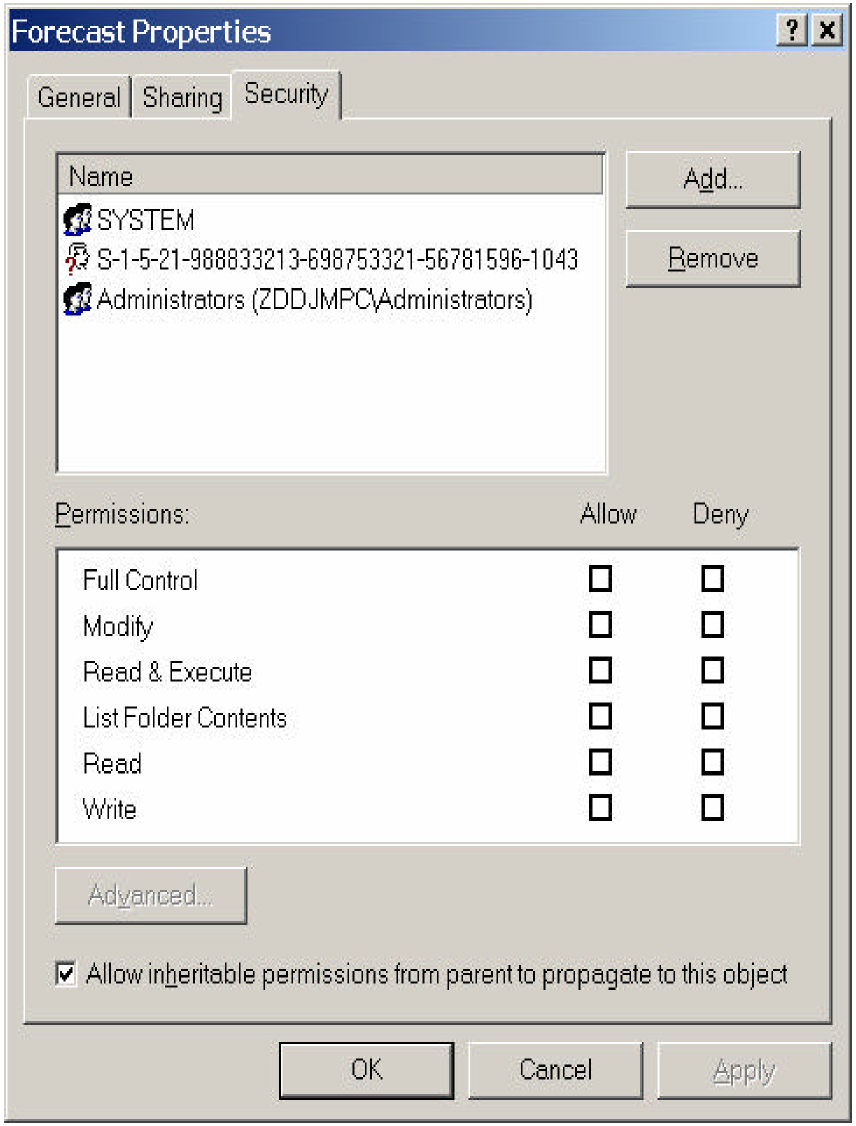
Access Control Models in Use

- Mandatory Access Control
  - Labels
  - Classification or Sensitivity
  - Rule Based
- Discretionary Access Control
  - User-directed
  - Identity-based
- Hybrid
  - Non-Discretionary Access Control
  - Role Based
  - Task Based

Mandatory vs. Discretionary

- Discretionary Access Control
  - You (the user or operator) decided how you want to protect and share your data
  - Relies on the user
- Mandatory Access Control
  - The system decided how the data will be shared
  - Based on policies in place and objective standards
  - Implemented by someone other than the user
  - Costs more to implement

Windows NT/2000 Discretionary Access Control Example



Forecast Properties

General | Sharing | Security

Name
SYSTEM
S-1-5-21-988833213-698753321-56781596-1043
Administrators (ZDDJMPC\Administrators)

Permissions:	Allow	Deny
Full Control	□	□
Modify	□	□
Read & Execute	□	□
List Folder Contents	□	□
Read	□	□
Write	□	□

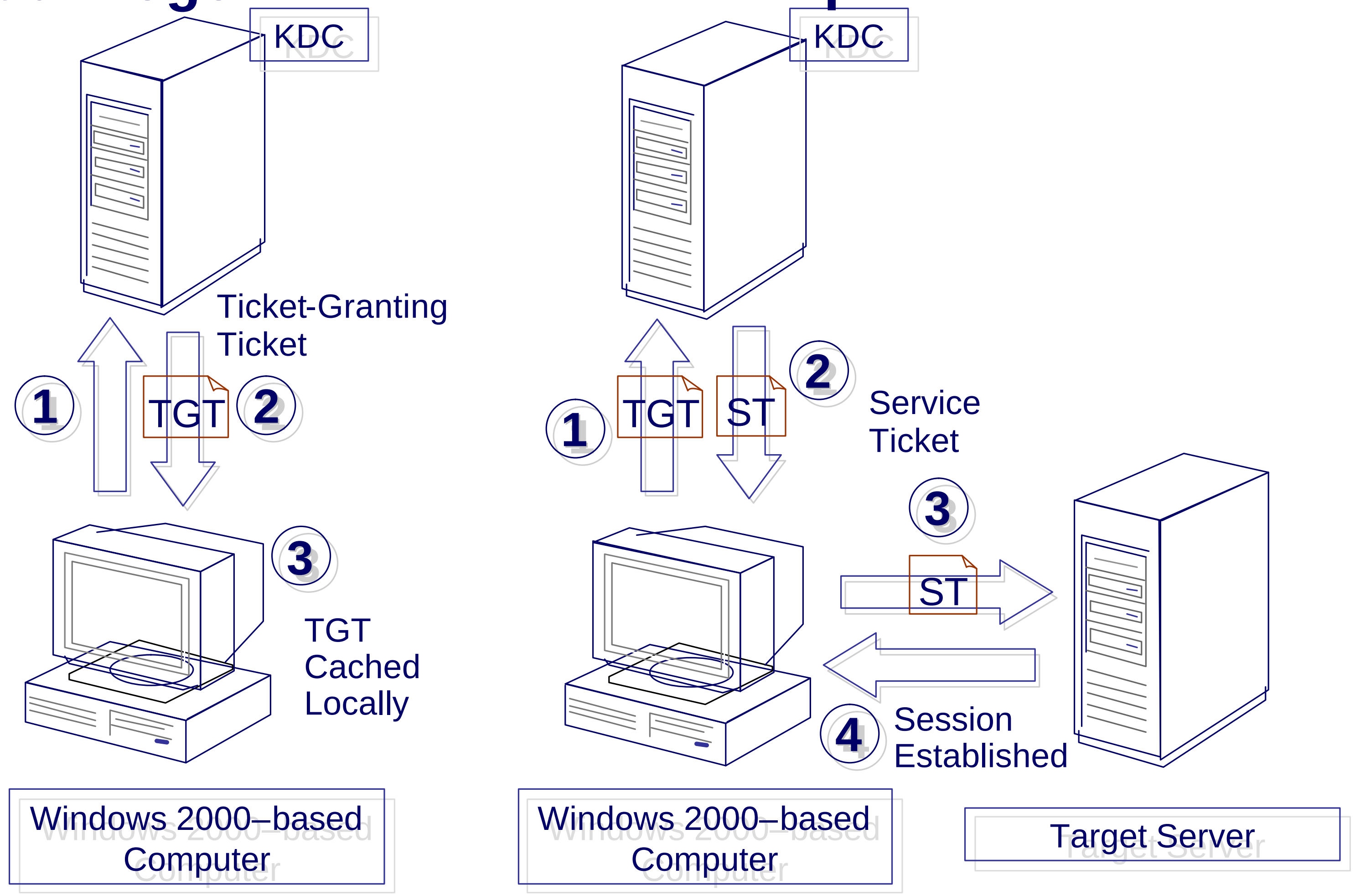
☑ Allow inheritable permissions from parent to propagate to this object

- User can change permissions on files
- User can remove administrative accounts
- User can allow others to access file, printer and network share via the GUI

Single Sign On (SSO)

- User has one password for all enterprise systems and applications
- That way, one strong password can be remembered and used
- All of a users accounts can be quickly created on hire, deleted on dismissal
- Hard to implement and get working
- Kerberos, CA-Unicenter, Memco Proxima, IntelliSoft SnareWorks, Tivoli Global Sign-On, x.509

Kerberos V5 Example



Initial Logon

KDC

1

Ticket-Granting Ticket

TGT

2

3

TGT Cached Locally

Windows 2000–based Computer

Service Request

KDC

1

TGT

ST

2

Service Ticket

3

ST

4

Session Established

Windows 2000–based Computer

Target Server

Security And Auditing: Practical Examples

- Web Server log files
  - IIS log files in IIS, W3C format or ODBC
- Windows event logging
  - Application, Security, System, ADS, DNS
  - Most features must be enabled
- Logging does not affect performance

  (under normal conditions)
- Benefits of logging and auditing
  - Intruder Detection; Permissions abuse
  - Problem Resolution
  - Detect Misconfiiguration

What is an “Intrusion”?

- An intrusion can be defined as:
  - Any set of actions that attempts to compromise the integrity, confidentiality or availability of a resource
- All intrusions are defined relative to a security policy
  - A security policy defines what is permitted and what is denied on the system
  - Without a set of normal behavior defined, it is useless to catch intrusions

What are Common Intrusions?

- Most simple
  - Remote scanning
  - Exploit exploration and reconnaissance
- Most sophisticated
  - Multi-stage attacks by a group of intruders
- External penetrations
  - Internet connected systems
  - Dial-up access points and modems
- Internal penetrations
  - Unprivileged accounts

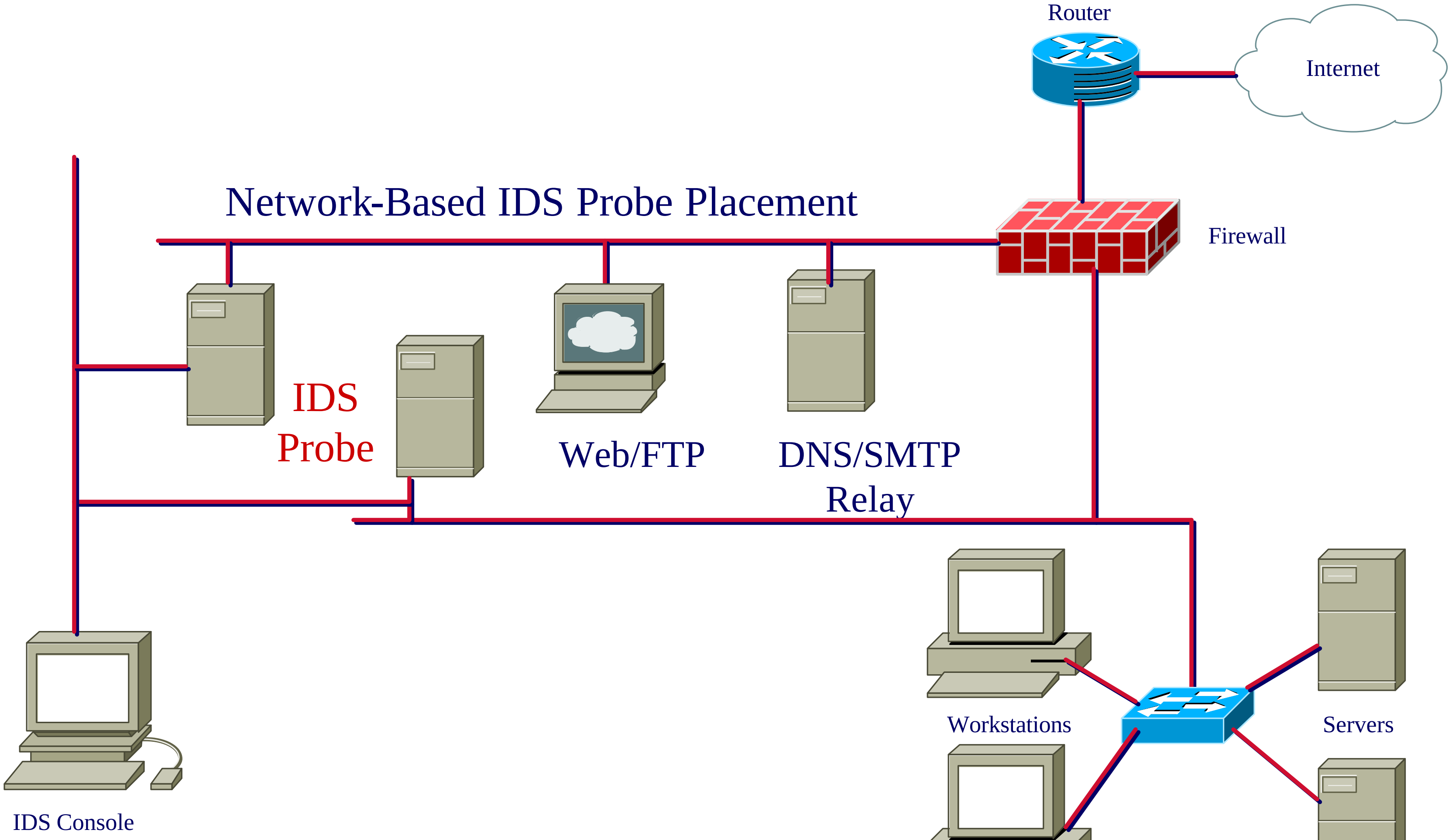
What is an IDS?

- An intrusion detection system monitors computer systems and networks, looking for signs of intrusion (unauthorized access) or misuse (authorized users).

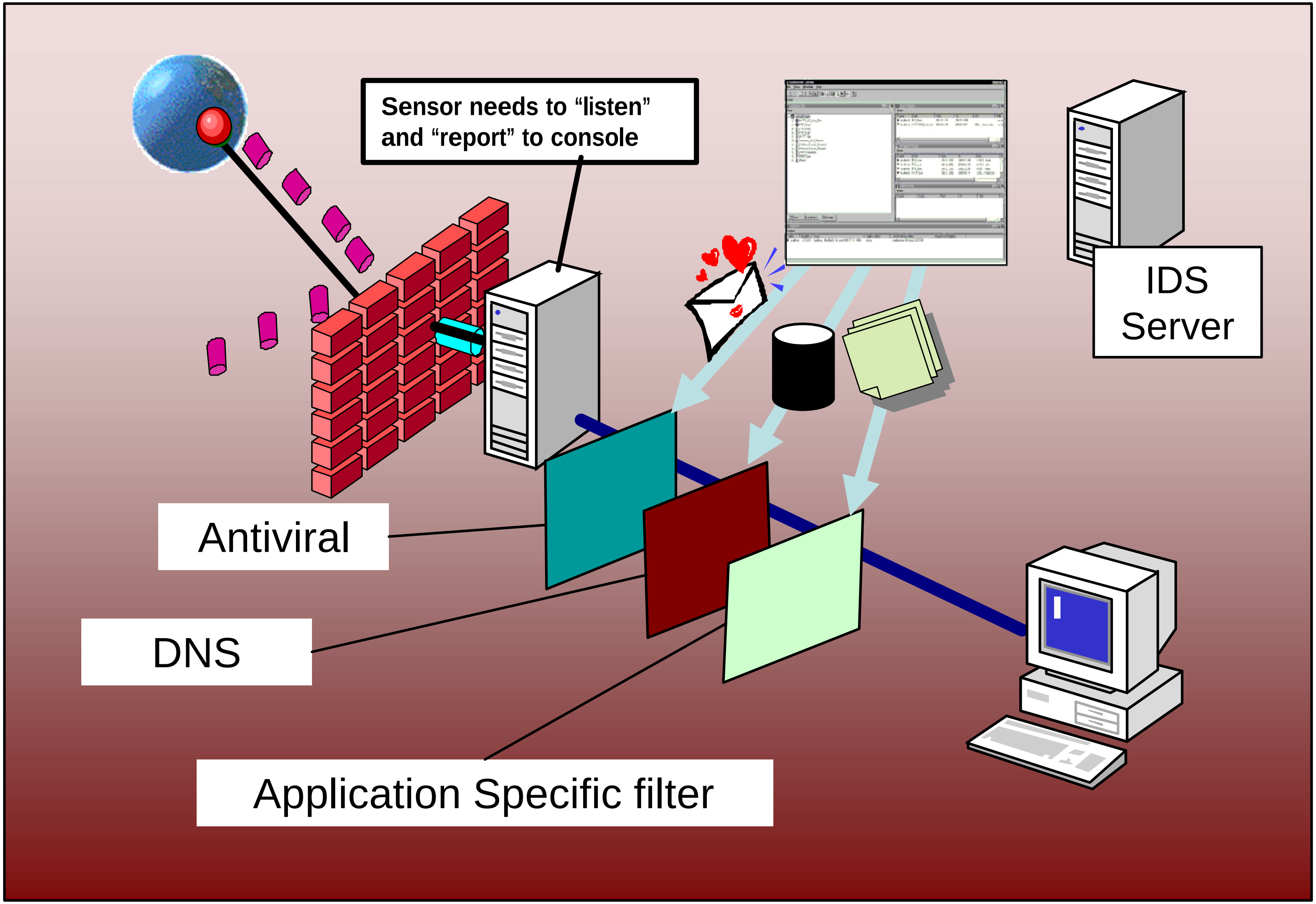
Types of IDS

- Host-based
  - Detection agents collect information reflecting the activity that occurs on a particular system
  - Example: BlackICE Defender
- Network-based
  - Collects information from the network itself through sniffing
- Combination products appearing for the desktop user
  - Example: Norton Internet Security 2003

Example IDS Placement Diagram



Other candidate locations for IDS placement



Sensor needs to "listen" and "report" to console

IDS Server

Antiviral

DNS

Application Specific filter

Host-Based IDS

- Advantages
  - Can map problem activities to a specific user
  - Can operate in encrypted network environments if it knows private keys
  - Can track behavioral changes
  - Can operate in switched network environments
  - Verifies the success or failure of an attack
  - Can monitor the file system and processes
- Product Examples
  - TCP wrappers, tripwire, antiviral software
  - Microsoft Operations Manager 2000

Host-Based IDS

- Disadvantages
  - Cannot monitor network activity
  - May cause performance degradation of monitored system
  - Agents are more platform-specific, which adds to the deployment costs
  - Myopic

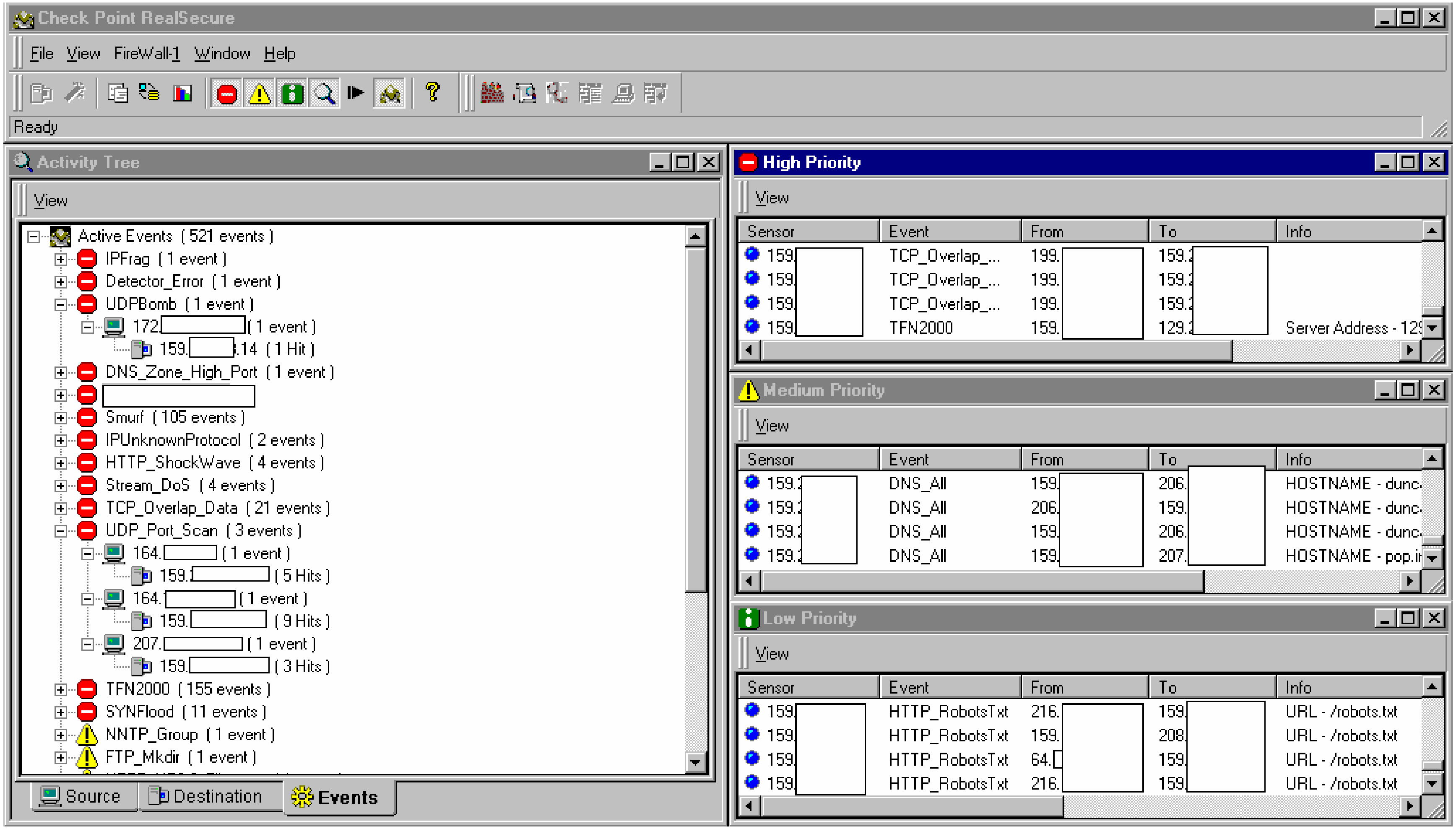
Network-Based IDS

- Advantages
  - Can detect and monitor network attacks (i.e. packet storm attacks and SYN floods)
  - Does not require logging or auditing to be enabled
  - Are not Operating System specific
    by their very nature
- Examples
  - Snort, ISS, NFR, Symantec, Cisco (embedded)

Network-Based IDS

- Disadvantages
  - Can show what is happening on a network, but cannot tell the outcome of commands executed on a host
  - Cannot be used on encrypted networks
  - Can be difficult to implement in modern switched networks
  - Cannot keep up with today's high speed networks
  - Are not application aware unless programmed to be so – which requires skill and time

Network-Based IDS
An Example with RealSecure



Active Events (521 events)
- IPFrag (1 event)
- Detector_Error (1 event)
- UDPBomb (1 event)
  - 172.[redacted] (1 event)
    - 159.[redacted].14 (1 Hit)
- DNS_Zone_High_Port (1 event)
- [redacted]
- Smurf (105 events)
- IPUnknownProtocol (2 events)
- HTTP_ShockWave (4 events)
- Stream_DoS (4 events)
- TCP_Overlap_Data (21 events)
- UDP_Port_Scan (3 events)
  - 164.[redacted] (1 event)
    - 159.1[redacted] (5 Hits)
  - 164.[redacted] (1 event)
    - 159.[redacted] (9 Hits)
  - 207.[redacted] (1 event)
    - 159.[redacted] (3 Hits)
- TFN2000 (155 events)
- SYNFlood (11 events)
- NNTP_Group (1 event)
- FTP_Mkdir (1 event)

High Priority

Sensor	Event	From	To	Info
159.[redacted]	TCP_Overlap_...	199.[redacted]	159.2[redacted]	
159.[redacted]	TCP_Overlap_...	199.[redacted]	159.2[redacted]	
159.[redacted]	TCP_Overlap_...	199.[redacted]	159.2[redacted]	
159.[redacted]	TFN2000	159.[redacted]	129.2[redacted]	Server Address - 12

Medium Priority

Sensor	Event	From	To	Info
159.2[redacted]	DNS_All	159.[redacted]	206.[redacted]	HOSTNAME - dunc
159.2[redacted]	DNS_All	206.[redacted]	159.[redacted]	HOSTNAME - dunc
159.2[redacted]	DNS_All	159.[redacted]	206.[redacted]	HOSTNAME - dunc
159.2[redacted]	DNS_All	159.[redacted]	207.[redacted]	HOSTNAME - pop.i

Low Priority

Sensor	Event	From	To	Info
159.[redacted]	HTTP_RobotsTxt	216.[redacted]	159.[redacted]	URL - /robots.txt
159.[redacted]	HTTP_RobotsTxt	159.[redacted]	208.[redacted]	URL - /robots.txt
159.[redacted]	HTTP_RobotsTxt	64.[redacted]	159.[redacted]	URL - /robots.txt
159.[redacted]	HTTP_RobotsTxt	216.[redacted]	159.[redacted]	URL - /robots.txt

Remote Control / Access
Practical Thoughts

- Prevent remote control to critical resources where possible
- User a different password for remote control when possible
- Enable security audit logging for success and failures
- Dial in authentication code independent of userid if possible

Banners – Lay the Groundwork

- Banners display at login or connection stating that the system is for the exclusive use of authorized users and that their activity may be monitored
- Not foolproof, but a good start, especially from a legal perspective
- Make sure that the banner does not reveal system information, i.e., OS, version, hardware, etc.

Banner Example

This University system may be used only for authorized purposes. Unauthorized access or modification of information stored on this system may result in criminal prosecution. Accessing this system implies consent to possible monitoring or auditing.

Application and System Development

Information Security meets the modern programmer

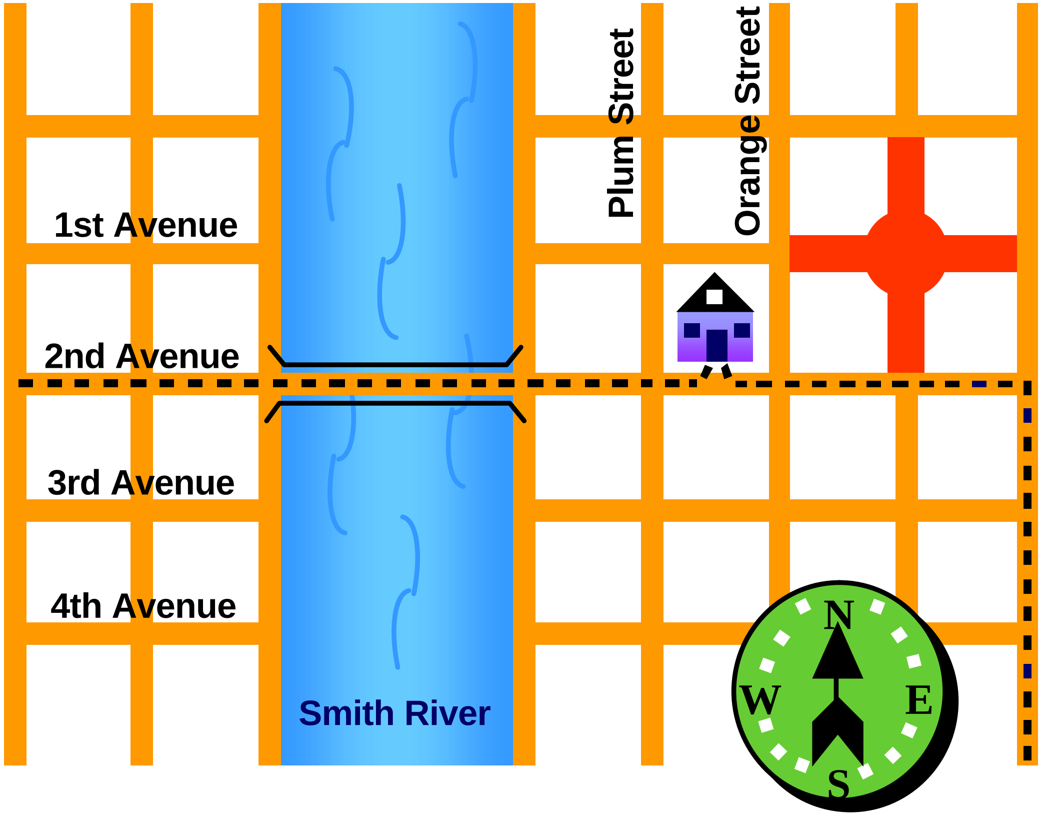
Applications & Systems Development – controls within software itself to ensure the application is used properly.

Key Issues in Application Development

- Application Issues
  - Distributed Environment
  - Databases and Data Warehousing
  - Data/Information Storage
  - Knowledge-based Systems
- Systems Development Controls
- Malicious Code
- Methods of attack
- How many software developers start with Security in mind?
- Device or Software security?
- Application risks and mitigation
  - COM/DCOM
  - Java and Applets

Applying Structure to Application Development

- A ***methodology*** applies specific directions to a known destination
- A ***framework***, like a compass, verifies progress and provides directional guidance when directions for your type of project have not been documented yet



MSF

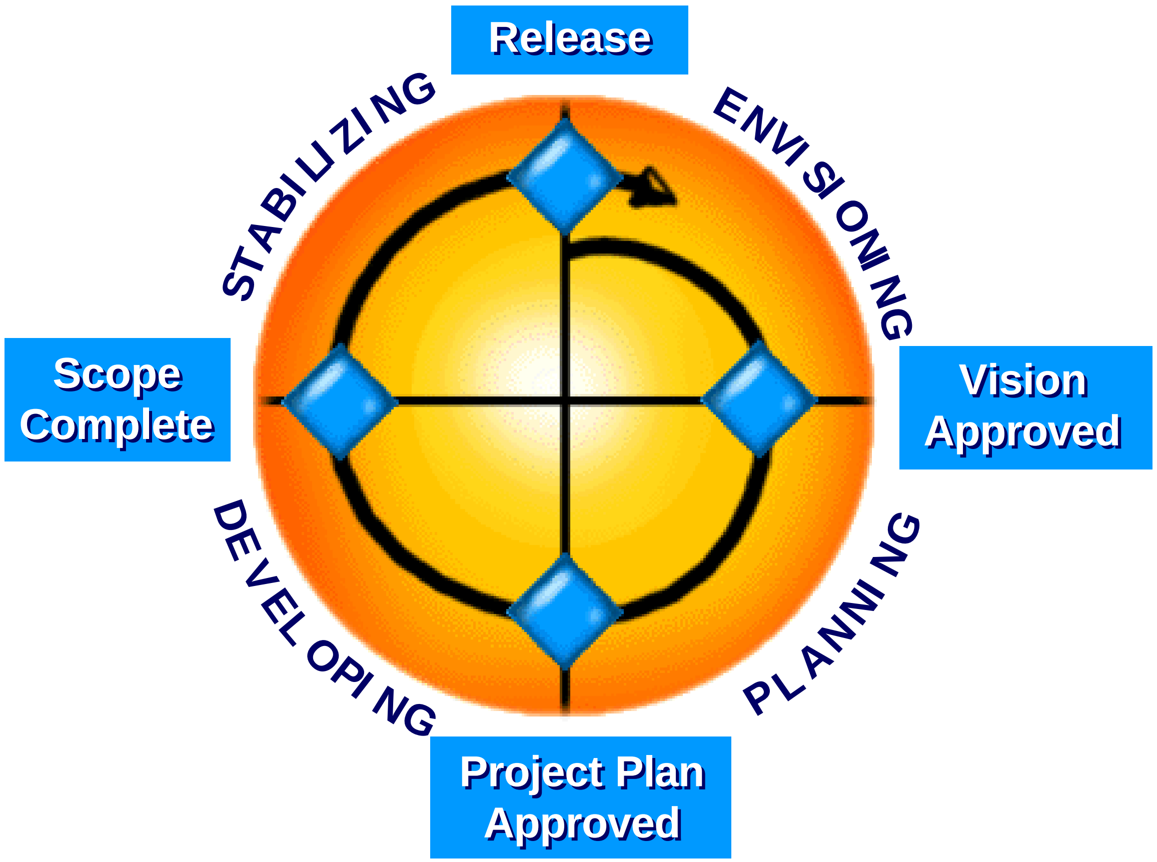
Specifics on Web Application Security

- Building secure Web apps is very difficult
  - Complex technologies
  - Difficult to implement
  - Difficult to hide complexity from users
  - Often “pasted” on after the fact
  - Lack of skills in the market
- Building secure Web apps means
  - Analyzing your threats
  - Designing a system to cope with the threats
  - Choosing the appropriate technologies
  - Building the system
  - Testing the system
  - Monitoring for product exploits that appear

Software Change Control Process

- Request control
  - Establishing the priorities of requests
  - Estimating the cost of the changes requested
  - Determining the interface that is presented to the user
- Change control
  - Recreating and analyzing the problem
  - Developing the changes and corresponding tests
  - Performing quality control
- In addition, there are also other considerations such as the following:
  - The tool types to be used in implementing the changes
  - The documentation of the changes
  - The restriction of the changes' effects on other parts of the code
  - Recertification and accreditation, if necessary
- Release control

The Microsoft Solution Framework



Release

ENVISIONING

Vision Approved

PLANNING

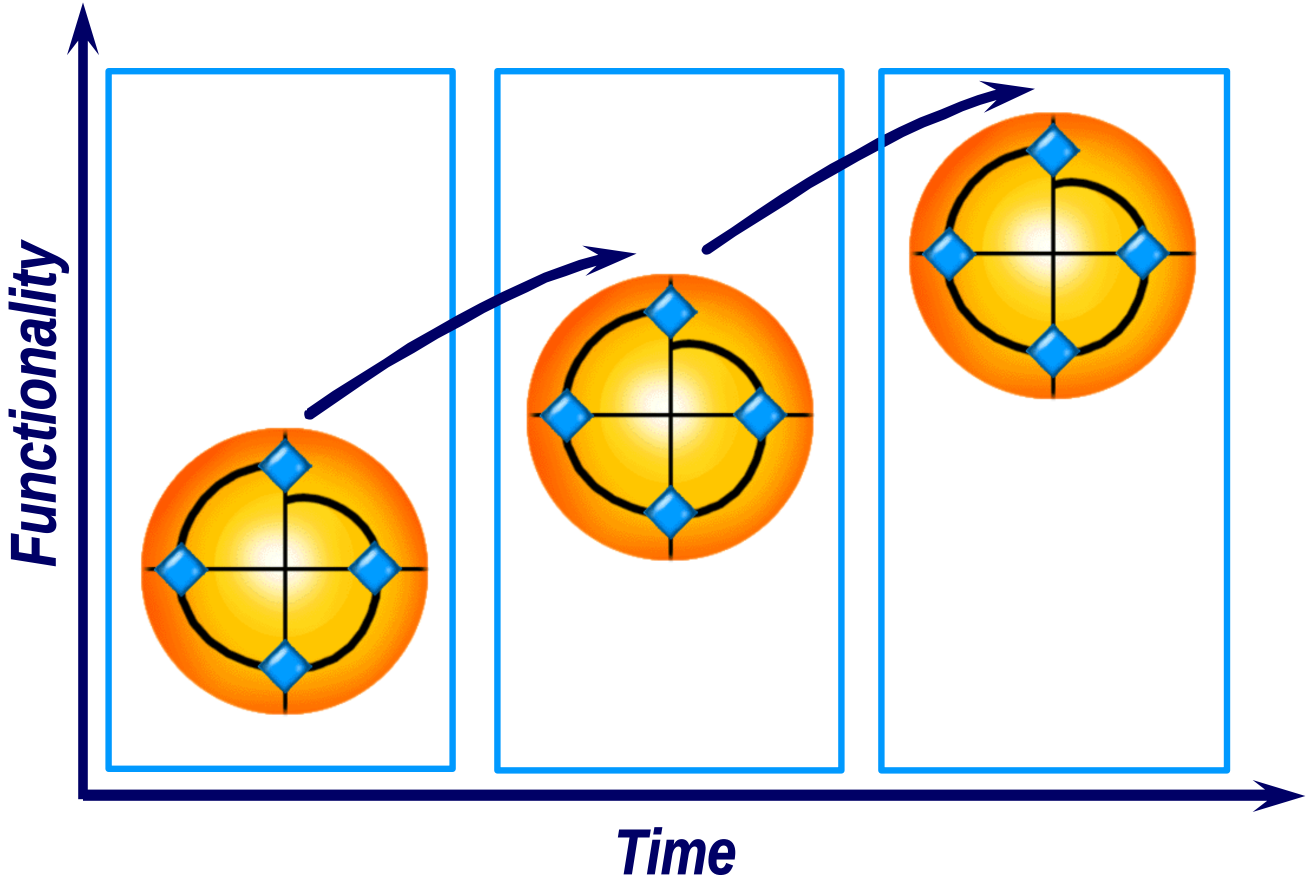
Project Plan Approved

DEVELOPING

Scope Complete

STABILIZING

MSF – Versioned releases – Baseline Early and Freeze Late on a 4 month schedule

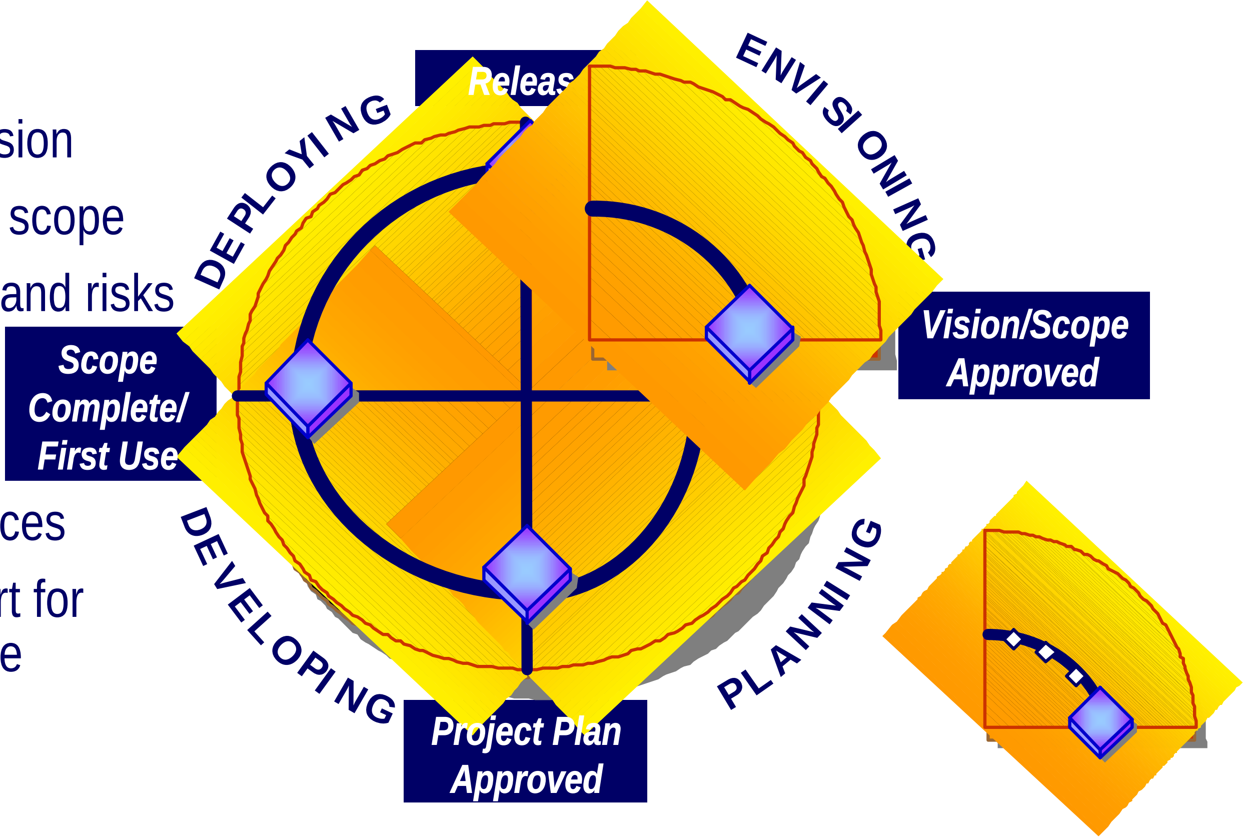


Envisioning Culminates in the Vision/Scope Approved Milestone

Vision/Scope Approved

Agreement on:

- Long-range vision
- Shorter-range scope
- Opportunities and risks
- Assumptions
- Constraints
- Project resources
- Time and effort for planning phase

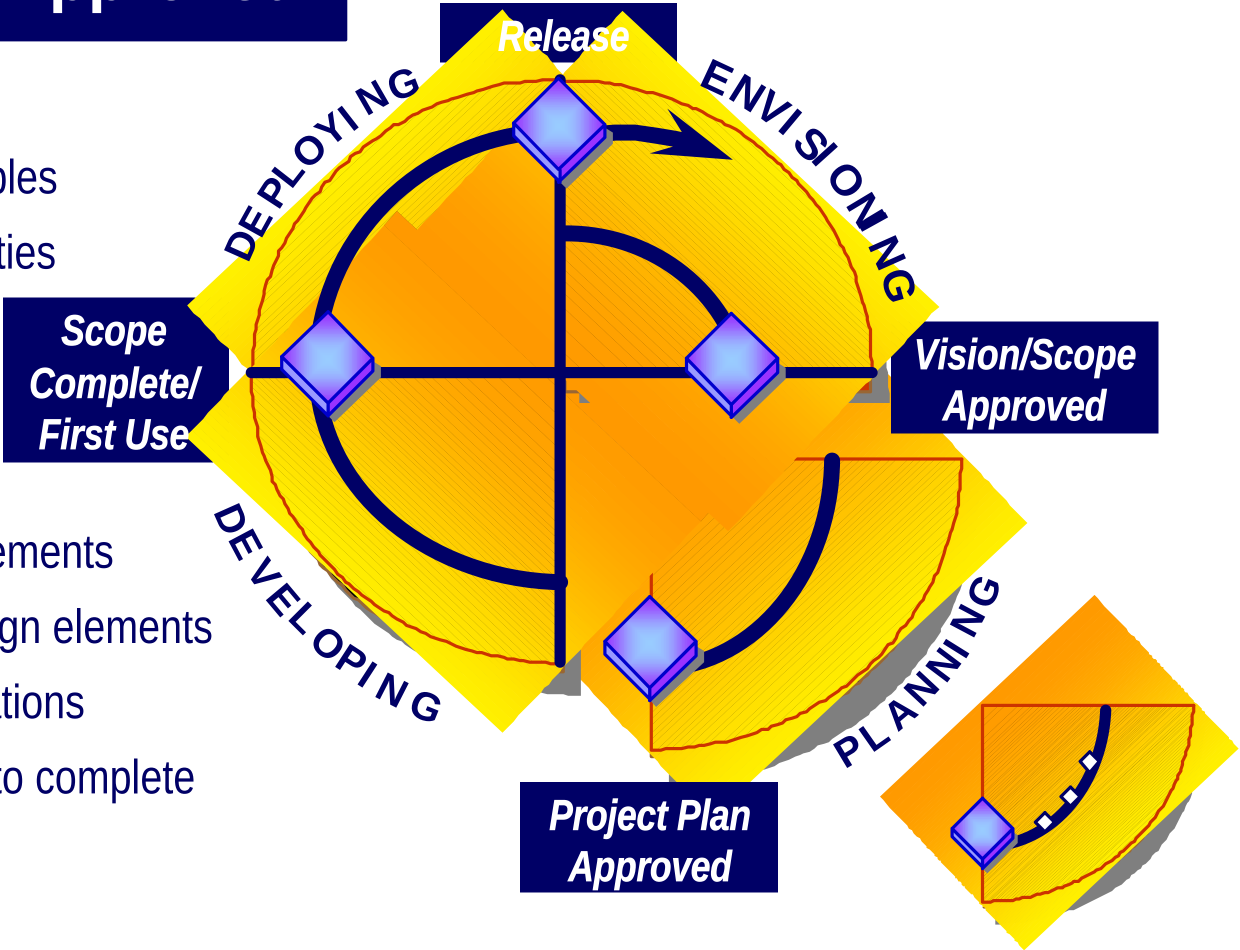


Planning Culminates in the Project Plan Approved Milestone

Project Plan Approved

Agreement on:

- Project deliverables
- Functional priorities
- Risks
- Ship date
- Project plan
- Business requirements
- Conceptual design elements
- Design specifications
- Time and effort to complete the project

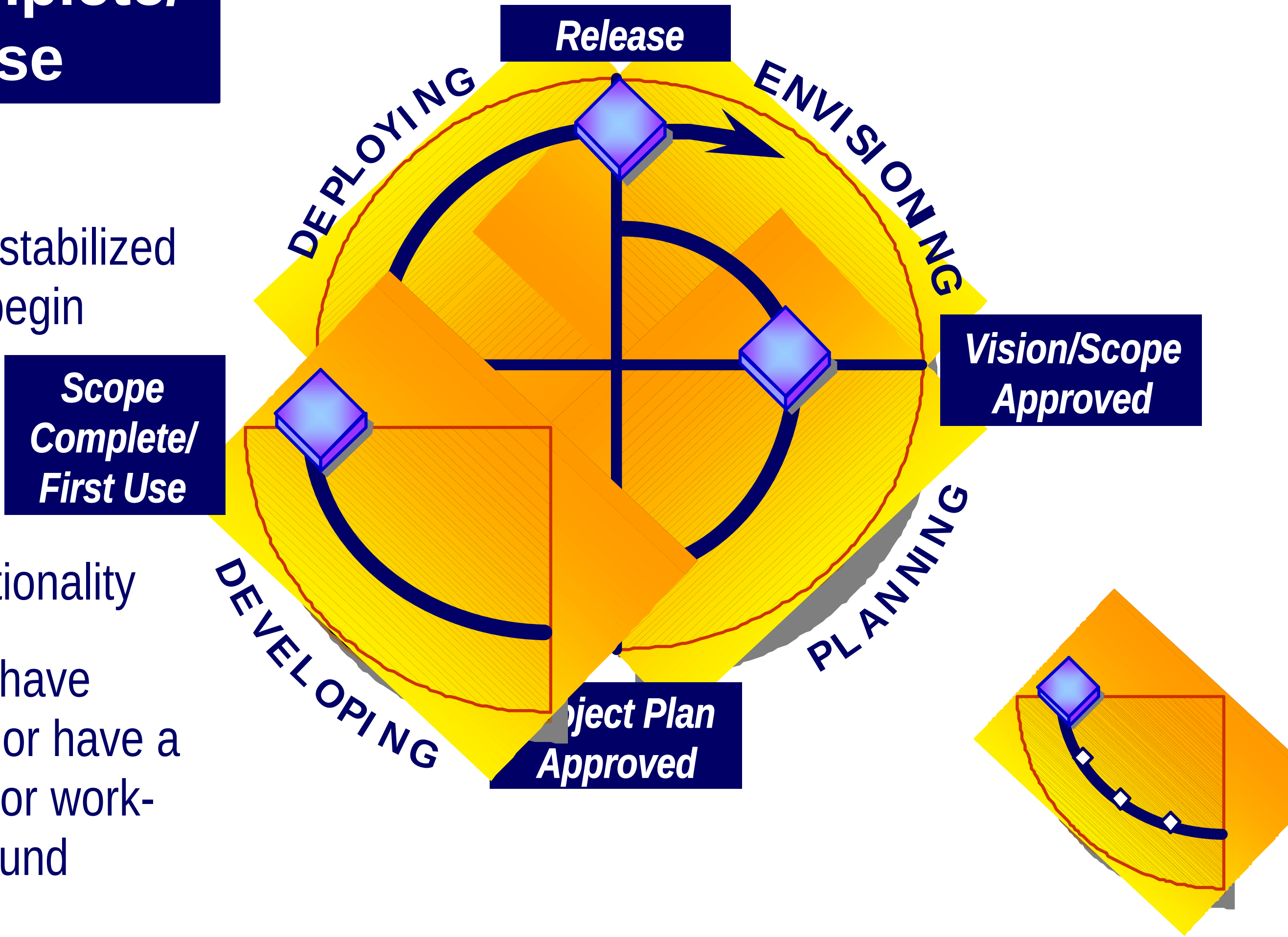


Developing Culminates in the Scope Complete/First Use Milestone

Scope Complete/ First Use

Agreement on:

- Technology is stabilized sufficiently to begin loading users
- A test group of users are using the functionality
- Known issues have been resolved or have a practical plan for work-off or work-around

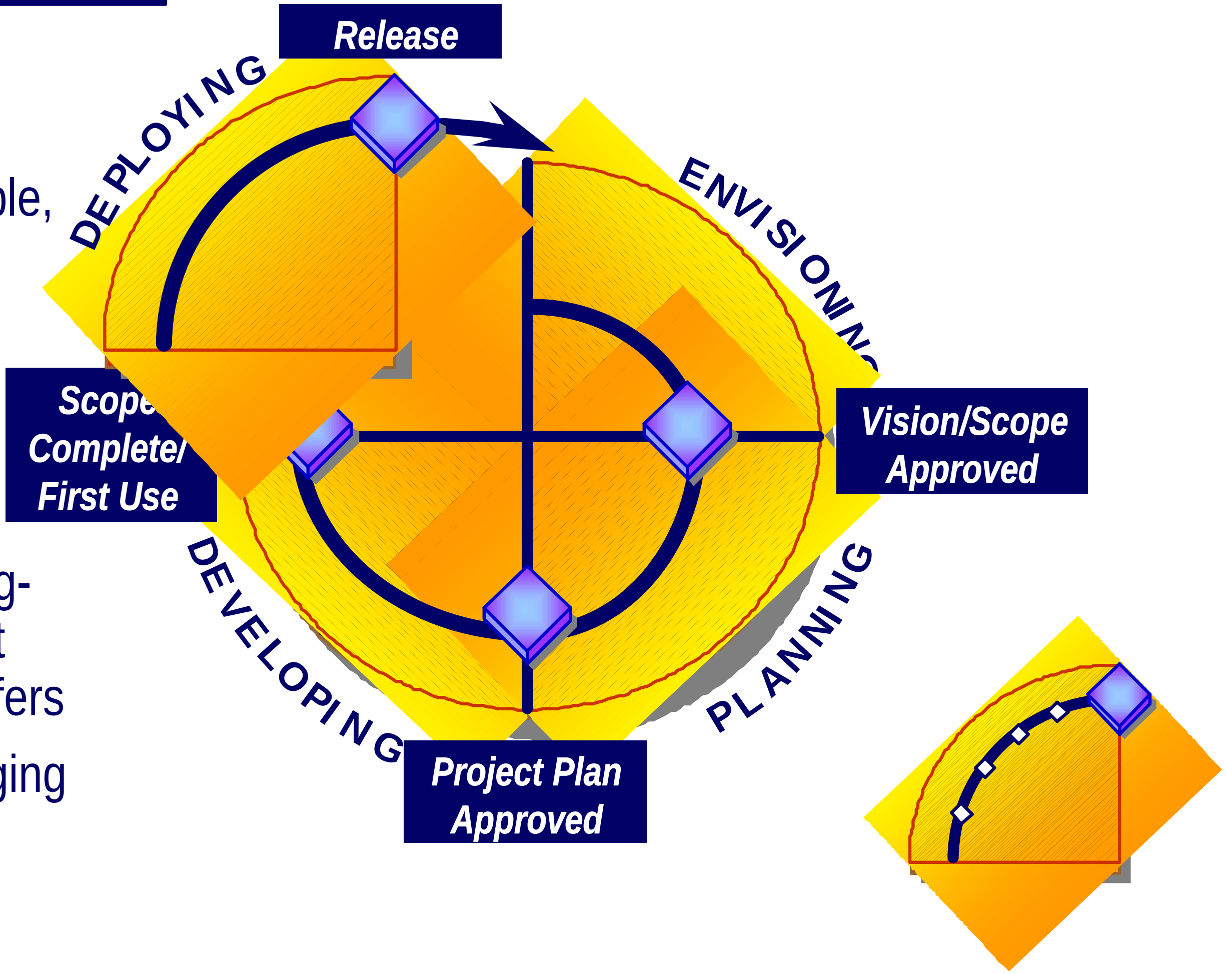


Deploying Culminates in the Release Milestone

Release

Agreement on:

- Solution that is deployed and stable, with all issues addressed
- Customer acceptance of the solution
- Ownership for long-term management and support transfers
- Team focus changing to the next project



General Security Principles relating to Application Development

- Identification, Authenticating, Authorization, and Accountability
  - Who accessed the system? Identification
  - Did we interrogate them? Authenticate
  - Can we track their permissions usage? Authorization
  - Do we know what they did? Accountability
- Separation of duties
- Least privilege
- Risk reduction
- Layered defense

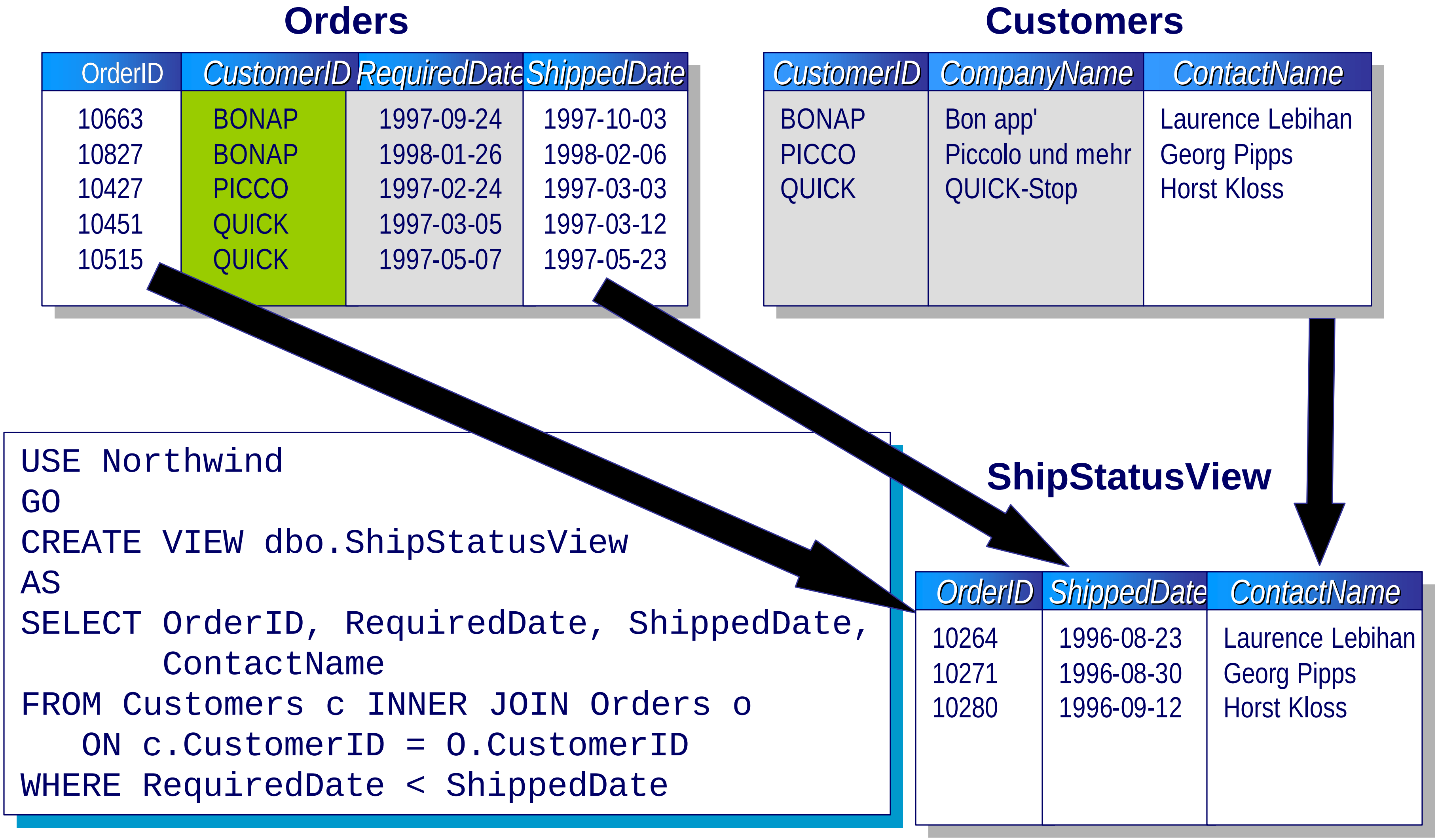
General Issues in RDBMS Development

- Various RDBMS items can have “permissions”
- Tables
  - “Relation” (Table or set of columns in table)
  - With “Attributes” (Columns)
  - Having “Permissible values”
  - Specific Attribute is “Key” with unique values
  - Occurring in “Instances” (Rows)
  - “Tuple” of a Relation Instance

General Issues in RDBMS Development (2/2)

- Views
  - “Virtual” Relations (tables)
  - With selected “Attributes”
  - Linked by Key attributes
- Stored Procedures
  - DB specific units of execution that access / update data for the user
  - Abstracts functionality from actual database access

Example: View of Joined Tables



Orders

OrderID	CustomerID	RequiredDate	ShippedDate
10663	BONAP	1997-09-24	1997-10-03
10827	BONAP	1998-01-26	1998-02-06
10427	PICCO	1997-02-24	1997-03-03
10451	QUICK	1997-03-05	1997-03-12
10515	QUICK	1997-05-07	1997-05-23

Customers

CustomerID	CompanyName	ContactName
BONAP	Bon app'	Laurence Lebihan
PICCO	Piccolo und mehr	Georg Pipps
QUICK	QUICK-Stop	Horst Kloss

```
USE Northwind
GO
CREATE VIEW dbo.ShipStatusView
AS
SELECT OrderID, RequiredDate, ShippedDate,
       ContactName
FROM Customers c INNER JOIN Orders o
   ON c.CustomerID = O.CustomerID
WHERE RequiredDate < ShippedDate
```

ShipStatusView

OrderID	ShippedDate	ContactName
10264	1996-08-23	Laurence Lebihan
10271	1996-08-30	Georg Pipps
10280	1996-09-12	Horst Kloss

RDBMS Information Issues

- Aggregation
  - When a user does not have the clearance or permission to access specific information, but she does have the permission to access components of this information. She can then figure out the rest and obtain restricted information.
- Inference
  - Happens when a subject deduces information that is restricted from data he has access to. This is seen when data at a lower security level indirectly portrays data at a higher level.

Methods of Attack

- Brute force or exhaustive attack
- Denial Of Service
- Dictionary Attacks
- Spoofing
- Pseudo flaw
- Alteration of authorized code
- Hidden code
- Logic bomb
- Trap door
- Interrupts
- Remote maintenance
- Browsing
- Inference
- Traffic analysis
- Flooding
- Cramming
- Time of Check/Time of User (TOC/TOU)

Examples of Common Exploits

- Web server attacks
  - – Weak configuration
- CGI scripts
  - – Samples installed
- Web browser exploits
- SMTP attacks
  - – Relaying
- Buffer Overflows
  - – Poorly written code
- Default passwords
  - – No change since install

AppDev Definitions Commonly Misused

- Acceptance
  - Verification that performance and security requirements have been met
- Accreditation
  - Formal acceptance of security adequacy, authorization for operation and acceptance of existing risk (QC)
- Certification
  - Formal testing of security safeguards
- Operational Assurance
  - Verification that a system is operating according to its security requirements
- Assurance
  - Degree of confidence that the implemented security measures work as intended

Cryptography

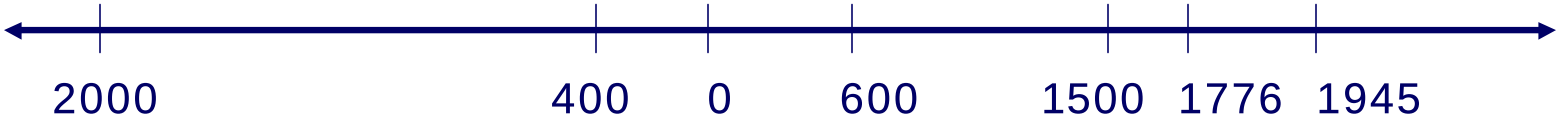
Cryptography – data encryption and digital signatures which are required to support nonrepudiation.

Topics in Cryptography

- History relating to cryptography
- Cryptography Uses (CIA)
- Cryptographic Concepts, Methodologies, and Practices
- Private Key Algorithms
- Public Key Algorithms
- Public Key Infrastructure (PKI)
- System Architecture for Implementing Cryptographic Functions
- Methods of Attack

History Highlights

- B.C.
  - 2000 – Egypt - Hieroglyphics
  - 400 – Spartans – Message cylinder
- A.D.
  - 600 – Rome, Julius Caesar – K letters to the right (ROT 13)
  - 1000-1600 - Europe Middle Ages, Mary Queen of Scots
  - 1776 - Revolutionary War, Benedict Arnold
  - 1945 – WW II Germany, Enigma



Cryptography Starting Points

- Why Encrypt?
  - Protect stored information
  - Support the C and I the CIA Triad
- Encryption - process by which plaintext is converted to cipher text using a key
- Decryption - process by which ciphertext is converted to plaintext (using the appropriate key)

The Basic Definition List

- Block Cipher
- Cipher
- Cipher text / Cryptogram
- Clustering
- Codes
- Cryptanalysis
- Cryptographic Algorithm
- Cryptography
- Cryptology
- Cryptosystem
- Decipher
- Encipher
- End-to-End Encryption
- Exclusive Or
- Key or Crypto variable
- Link Encryption
- One Time Pad
- Plaintext
- Steganography
- Work Function (Factor)

Some Terms Expanded On

- Cryptography:
  - art/science relating to encrypting, decrypting information
- Cryptanalysis:
  - art/science relating to converting ciphertext to plaintext without knowing the (secret) key
- Strength:
  - how the algorithm, the key length, initialization vectors and how the parts work together.
- Repudiation:
  - In communication between parties, Denial by one party of having participated in communication. (commonly heard as non

Requirements of a Crypto System

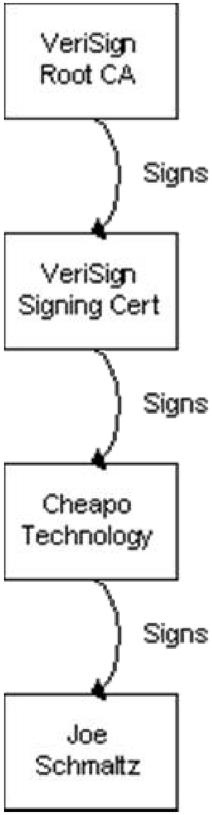
- If ciphertext and plaintext are known, it should be computationally infeasible to determine the deciphering algorithm
- It should be computationally infeasible to systematically determine plaintext from intercepted ciphertext (Even if you decrypt ciphertext once, it should require the same amount of work to do it again.)
- Encryption/decryption transformations must be efficient for all keys
- The security of the system should depend ONLY on the secrecy of the keys and not on the secrecy of the encryption/decryption transformations

Public vs. Private Cryptography

- Private key encryption uses the same key for both encryption and decryption (faster) (DES)
  - Private key encryption known as symmetric
- Public key encryption uses two different keys, one to decrypt and one to encrypt (RSA)
  - Thus, one key can be "public", because the other key is still necessary for decryption
  - More complex, key management is an issue
  - Public key encryption known as asymmetric

Public Key Infrastructure (PKI)

- PKI is a structured application of …
  - Public/Private Keys
  - Digital certificates
  - Certificate Authority (CA)
  - Registration authorities
  - Policies and procedures
  - Certificate revocation
  - Non-repudiation support
  - Timestamping
  - Lightweight Directory Access Protocol (LDAP)
  - Security-enabled applications
  - Cross certification



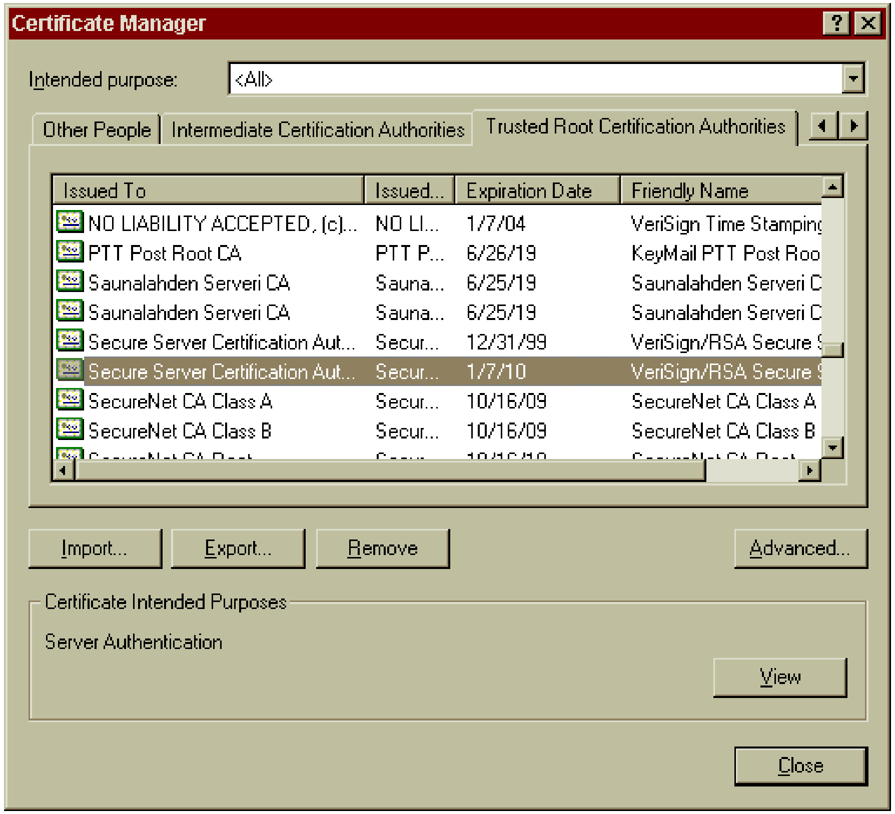
Practical Examples of Cryptography

- Secure file system – Win2K EFS
  - Implement on a Win2K Pro PC after knowing how to recover keys!
- IPSec on the network
- SSL on web servers – Server Cert’s
- Hardware based encryption devices
  - GemPlus, Schlumberger, Aladdin
  - Notebook encryption in IBM Thinkpads
  - Variety of link and end to end devices in use by the military and some commercial

Internet Centric Examples of Cryptography

- Secure Electronic Transaction (MC/Visa, 1997)
- IPass – authentication payload using RADIUS
- Secure Sockets Layer
  - (SSL)/Transaction Layer Security (TLS)
- HTTP/S and SSL Session keys
- Internet Open Trading Protocol (IOTP)
- S/MIME, PGP, Signed/encrypted messages
- IPSec – both AH and ESP
- Key based TCP/IP services
  - Secure Shell (SSH-2) with Fsecure/PuTTy as a Win32 client and SSH as a Unix client

Microsoft Windows Certificate Examples



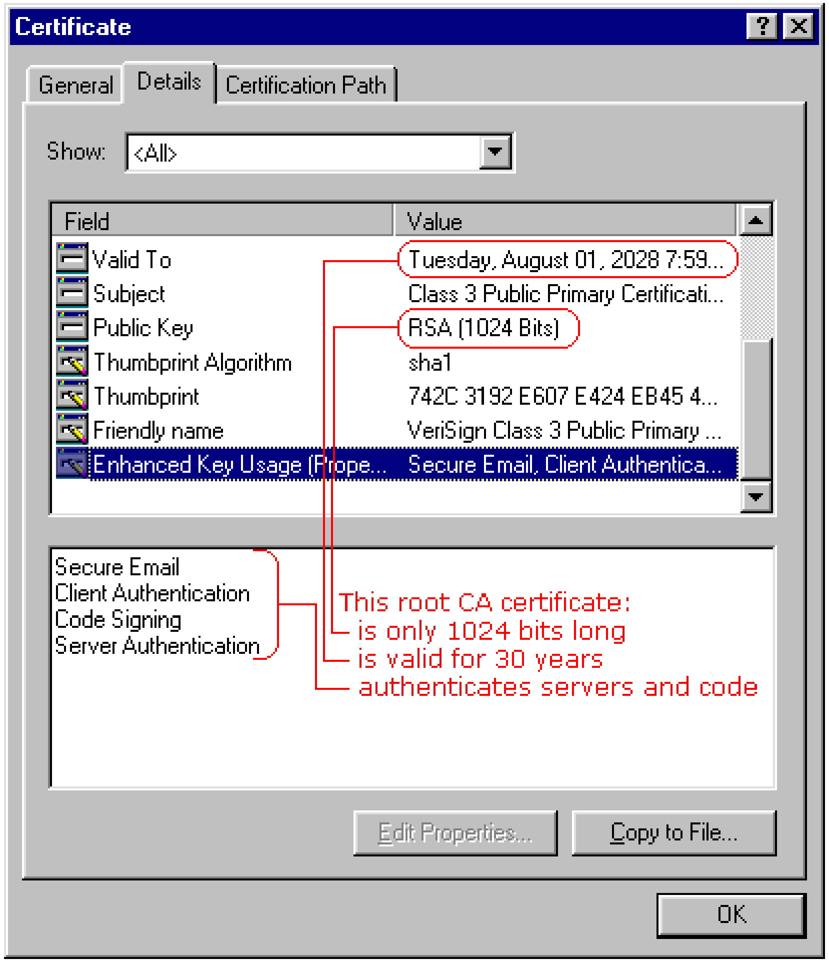
Certificate Manager
Other People
Intermediate Certification Authorities
Trusted Root Certification Authorities
Import...
Export...
Remove
Advanced...
View
Close

Intended purpose: <All>

Issued To	Issued...	Expiration Date	Friendly Name
NO LIABILITY ACCEPTED, (c)...	NO LI...	1/7/04	VeriSign Time Stamping
PTT Post Root CA	PTT P...	6/26/19	KeyMail PTT Post Roo
Saunalahden Serveri CA	Sauna...	6/25/19	Saunalahden Serveri C
Saunalahden Serveri CA	Sauna...	6/25/19	Saunalahden Serveri C
Secure Server Certification Aut...	Secur...	12/31/99	VeriSign/RSA Secure S
Secure Server Certification Aut...	Secur...	1/7/10	VeriSign/RSA Secure S
SecureNet CA Class A	Secur...	10/16/09	SecureNet CA Class A
SecureNet CA Class B	Secur...	10/16/09	SecureNet CA Class B
SecureNet CA Root	Secur...	10/16/10	SecureNet CA Root

Certificate Intended Purposes

Server Authentication



Show: <All>

Field	Value
Valid To	Tuesday, August 01, 2028 7:59...
Subject	Class 3 Public Primary Certificati...
Public Key	RSA (1024 Bits)
Thumbprint Algorithm	sha1
Thumbprint	742C 3192 E607 E424 EB45 4...
Friendly name	VeriSign Class 3 Public Primary ...
Enhanced Key Usage (Prope...	Secure Email, Client Authentica...

Secure Email
Client Authentication
Code Signing
Server Authentication

This root CA certificate:
- is only 1024 bits long
- is valid for 30 years
- authenticates servers and code

Disaster Recovery and Business Continuity

Business Continuity Planning (Disaster Recovery Planning) – how the business will respond from interruption of service.

DRP and BCP

- Basic Definition: A contingency plan is:

  "A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation…"

  (National Computer Security Center 1988)
- DRP – covers everything from a failed disk to the data center burning down – oh, and the servers melted after the lightning storm.
- BCP – keeping the business or mission afloat while you restore and return to normal operations.

Threats to a Business / Mission

- Unauthorized access
- Hardware failure
- Utility failure
- Natural disasters
- Loss of key personnel
- Human errors
- Neighborhood hazards
- Tampering
- Disgruntled employees
- Emanations
- Safety
- Improper use of technology
- Repetition of errors
- Cascading of errors

- Illogical processing
- Translation of user needs (technical requirements)
- Inability to control technology
- Equipment failure
- Incorrect entry of data
- Concentration of data
- Inability to react quickly
- Inability to substantiate processing
- Concentration of responsibilities
- Erroneous/falsified data
- Misuse

Business Continuity Definitions

- The goal is to assist the organization/business to continue functioning even though normal operations are disrupted
  - Disaster Recovery
  - Business Continuity Planning
  - End-user Recovery Planning
  - Contingency Planning
  - Emergency Response
  - Crisis Management
- Business Continuity Covers
  - The steps to take
    - Before a disruption
    - During a disruption
    - After a disruption

BCP and DRP Motivation (1/2)

- It is better to plan activities ahead of time rather than to react when the time comes
  - “Proactive” rather than “Reactive”
  - Take the correct actions when needed
  - Allow for experienced personnel to be absent
- Maintain business operations
  - Saves time, mistakes, stress and $$
  - Short and long term loss of business
  - Have necessary materials, equipment, information

BCP and DRP Motivation (1/2)

- Legal requirements
  - ‘77 Foreign Corrupt Practices Act/protection of stockholders
  - Federal Financial Institutions Examination Council
  - FCPA SAS30 Audit Standards
  - Defense Investigative Service
  - Legal and Regulatory sanctions, civil suits

Some More Important Definitions

- Due Care
  - Minimum and customary practice of responsible protection of assets that reflects a community or societal norm
- Due Diligence
  - Prudent management and execution of due care
- From Data Pro reports (late 90’s)
  - Errors & omissions 50%
  - Fire, water, electrical 25%
  - Dishonest employees 10%
  - Disgruntled employees 10%
  - Outsider threats 5%

Macro Steps in BCP and DRP

- Initiation
- Current state assessment including Risk Assessment and Information Valuation
- Develop support processes
- Training
- Impact Assessment
- Alternative selection
- Recovery Plan development
- Support services continuity plan development
- Master plan consolidation
- Testing strategy development
- Post transition transition plan development

Risk Analysis Steps (1/2)

- 1 - Identify essential business functions
  - Dollar losses or added expense
  - Contract/legal/regulatory requirements
  - Competitive advantage/market share
  - Interviews, questionnaires, workshops
- 2 - Establish recovery plan parameters
  - Prioritize business functions
- 3 - Gather impact data/Threat analysis
  - Probability of occurrence, source of help
  - Document business functions
  - Define support requirements
  - Document effects of disruption
  - Determine maximum acceptable outage period
  - Create outage scenarios

Risk Analysis Steps (2/2)

- 4 - Analyze and summarize
  - Estimate potential losses
    - Destruction/theft of assets
    - Loss of data
    - Theft of information
    - Indirect theft of assets
    - Delayed processing
    - Consider periodicity
  - Combine potential loss & probability
  - Magnitude of risk is the ALE (Annual Loss Expectancy)
  - Guide to security measures and how much to spend

Risk Analysis Results

- Significant threats & probabilities
- Critical tasks & loss potential by threat
- Remedial measures
  - Greatest net reduction in losses
  - Annual cost
- Understanding of the situation
  - Can we recover?
  - Where are weaknesses?
  - Can we succeed?
  - How do we build up staff to support DR/BC?

Information Valuation

- Information has cost/value
  - Acquire/develop/maintain
  - Owner/Custodian/User/Adversary
- Do a cost/value estimate for
  - Cost/benefit analysis
  - Integrate security in systems
  - Avoid penalties
  - Preserve proprietary information
  - Business continuity
- Circumstances effect valuation timing
- Ethical obligation to use justifiable tools/techniques

Next Steps in BCP

- Strategy Development (Alternative Selection)
  - Management support
  - Team structure
  - Strategy selection should be Cost effective/Workable
- Implementation (Plan Development)
  - Specify resources needed for recovery
  - Make necessary advance arrangements
  - Mitigate exposures

Risk Mitigation

- Risk Prevention/Mitigation
  - Risk management program
  - Security - physical and information (access)
  - Environmental controls
  - Redundancy - Backups/Recoverability
    - Journaling, Mirroring, Shadowing
    - On-line/near-line/off-line
  - Insurance
  - Emergency response plans
  - Procedures
  - Training

Steps in DRP

- Goals and objectives
  - Protect organization from IT / IS failures
  - Minimize risks for IT / IS Services
  - Reliable standby systems that can take over
  - Minimize decision making
- Data processing continuance
  - Ways to provide backup services
    - Mutual Aid
    - Subscription Services – HP, IBM, Sun Guard
    - Multiple Centers
  - Drill into subscription services
    - Hot Site – Processing can resume in short order, usually with the most recent data restore
    - Warm Site – enough to get you going.
    - Cold Site – a room with HVAC and electricity we own

Law, Investigation, and Ethics

Having a response that will
stand up in court
(criminal or civil) with
supporting evidence.

Topics

- Laws – Criminal and Civil
- Major categories and types of laws
- Investigations
    - Evidence, processes, interrogation, confidentiality
- Major categories of computer crime
- Incident Handling
- Ethics

Federal (USA) Computer Crime Law

- Computer Fraud and Abuse Act (Title 18, U.S. Code, 1030)
  - Accessing Federal Interest Computer (FIC) to acquire national defense information
  - Accessing an FIC to obtain financial information
  - Accessing an FIC to deny the use of the computer
  - Accessing an FIC to affect a fraud
  - Damaging or denying use of an FIC thru transmission of code, program, information or command
  - Furthering a fraud by trafficking in passwords

Federal (USA) Computer Crime Law

- Economic Espionage Act of 1996:
  - Obtaining trade secrets to benefit a foreign entity
- Electronic Funds Transfer Act:
  - Covers use, transport, sell, receive or furnish counterfeit, altered, lost, stolen, or fraudulently obtained debit instruments in interstate or foreign commerce.

Federal (USA) Computer Crime Law

- Computer Security Act of 1987: Requires Federal Executive agencies to Establish Computer Security Programs.
- Electronic Communications Privacy Act (ECPA): Prohibits unauthorized interception or retrieval of electronic communications
- Fair Credit Reporting Act: Governs types of data that companies may be collected on private citizens & how it may be used.
- Foreign Corrupt Practices Act: Covers improper foreign operations, but applies to all companies registered with the SEC, and requires companies to institute security programs.
- Freedom of Information Act: Permits public access to information collected by the Federal Executive Branch.

Civil or Tort Law

- Damage/Loss to an Individual or Business
- Type of Punishment Different: No Incarceration
- Primary Purpose is Financial Restitution
- Compensatory Damages: Actual Damages, Attorney Fees, Lost Profits, Investigation Costs
- Punitive Damages: Set by Jury to Punish Offender
- Statutory Damages: Established by Law
- Easier to Obtain Conviction: Preponderance of Evidence

Issues in International Law

- Lack of Universal Cooperation
- Lack of cultural support
- Differences in Interpretations of Laws
- Outdated Laws Against Fraud
- Problems with Evidence Admissibility
- Extradition
- Low Priority

Proprietary Rights and Obligations

- Legal Forms of Protection
  - Trade Secrets: Information that Provides a Competitive Advantage. Protect Ideas.
  - Copyrights: Right of an Author to Prevent Use or Copying Works of the Author. Protect Expression of Ideas.
  - Patents: Protect Results of Science, Technology & Engineering
- Business Needs
  - Protect Developed Software
  - Contractual Agreements
  - Define Trade Secrets for Employees

Computer Crime Types

- Denial of Service (DoS) and Distributed Denial of Service
- Theft of passwords.
- Network Intrusions
- Emanation Eavesdropping
- Social Engineering
- Illegal Content of Material
- Fraud
- Software Piracy
- Dumpster Diving
- Malicious Code
- Spoofing of IP Addresses
- Information Warfare
- Espionage
- Destruction/Alteration of Information
- Use of Readily Available Attack
- Masquerading
- Embezzlement
- Terrorism
- Data-Diddling

Computer Crime Examples

- Distributed Denial of Service (DoS) attacks against Yahoo, Amazon-com, and ZDNet in February of 2000.
- Love Letter (Love Bug) worm released by Onel de Guzman in the Philippines that spread worldwide in May of 2000.
- Inadvertent transmission of emails containing personal client information to 19 unintended recipients by Kaiser Permanente HMO in August of 2000.

What are “business records”?

- “…all books, papers, maps…regardless of physical form or characteristics, made or received by an agency …as evidence of the organization, functions, policies, decisions…” -36 CFR Part 1220
- Also affected by Federal Rules of Evidence, Sec 803.

Actual Rules of Evidence

http://www.usdoj.gov/criminal/cybercrime/usamarch2001_4.htm

- Most federal courts that have evaluated the admissibility of computer records have focused on computer records as **potential hearsay**. The courts generally have admitted computer records upon a showing that the records fall within the business records exception, Fed. R. Evid. 803(6):
- **Records of regularly conducted activity**. A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term "business" as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

Computer Crime Investigation

- Detection and Containment
- Report to management/responsible arties
- Conduct preliminary investigation
- Disclosure determination
- Perform corrective action
- After action analysis

The evidence lifecycle
Chain of Custody must be Preserved

- Discovery and recognition
- Protection
- Recording
- Collection
- Collect all relevant storage media
- Make image of hard disk before removing power
- Print out screen
- Avoid degaussing

- Identification (tagging and marking)
- Preservation
- Protect magnetic media from erasure
- Store in proper environment
- Transportation
- Presentation in a court of law
- Return of evidence to owner

Types and Rules of Evidence

- Types
  - Direct: Oral Testimony by Witness
  - Real: Tangible Objects/Physical Evidence
  - Documentary: Printed Business Records, Manuals, Printouts
  - Demonstrative: Used to Aid the Jury (Models, Illustrations, Charts
- Rules
  - Best Evidence Rule: To Limit Potential for Alteration
  - Exclusionary Rule: Evidence Must be Gathered Legally or it Can't Be Used
  - Hearsay Rule: Key for Computer Generated Evidence
  - Exceptions: Rule 803 of Federal Rules of Evidence (Business Documents created at the time by person with knowledge, part of regular business, routinely kept, supported by testimony)

Sources of Information on Ethics

- National Computer Ethics and Responsibilities Campaign (NCERC)
- ISC2 Ethics Computer Ethics Resource Guide
- Generally Accepted Systems Security Principles (GASSP)
- National Computer Security Association (NCSA)
- Computer Ethics Institute
  - 1991 – Ten Commandments of Computer Ethics
  - End User's Basic Tenants of Responsible Computing

Operations Security

Operations Security – controls over the environment of the system, or what to do after everything is installed.

Operations Security

- OpSec is the day to day application of every topic in this presentation
  - What are you doing on a day to day basis?
  - Accountability – checks and balances
  - Anti Virus
  - Policies – technical and administrative
  - Intrusion detection
  - Patches, updates, service packs

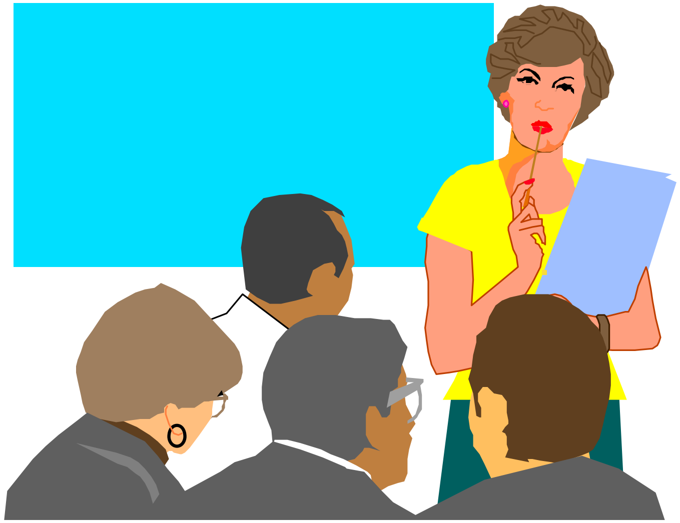
Virus Issues

- They will keep coming, and coming, and coming …
- Delivery
- Media
- Higher degree of "being connected" increases the threat plane

- Costs:
  - Initial software
  - Deployment
  - Maintenance
  - False alarms
- Cost of nonconformance
  - Productivity loss
  - System downtime
  - Damage (many forms)
  - Public image

Spreading The Word

- How do you get security information to your employees?
  - Awareness programs
  - Distribute translated excerpts from main security policy
  - New employee orientation.
  - Webcast / Streaming
  - PowerPoint and Producer
  - Repeat annually



Testing

- When to test
  - – Changes in policy
  - – Changes in staffing
  - – Network architectural changes
  - – System updates (software, firmware, hardware)
- How often?
  - – DAILY – test or review something

Physical Security

Physical Security – threats, threat agents, vulnerabilities, and their countermeasures to a system.

Physical Security

- Protecting facilities
  - Building, Location, Computer room, offices ...
- Providing ample and proper computer facilities
- Environmental issues
  - HVAC, Power
  - Fire detection/prevention
  - Facility access
- The perimeter may be larger than you think

Examples of Physical Access Controls

- Guards
- Fences
- Barriers
- Lighting
- Keys and Locks
- Badges
- Escorts
- Property Controls
- Monitoring/Detection Systems

Physical Environment Protection

- Power Protection
- HVAC
- Water Protection
- Fire Detection
- Fire Suppression
- Evacuation
- Environmental Monitoring/Detection

- Factors in site selection
  - Local Crime
  - Visibility
  - Emergency Access
  - Natural Hazards
  - Air and Surface Traffic
  - Joint Tenants
  - Stable Power Supply
  - Existing Boundary Protection

Security Management Practices

Security Management Practices – asset identification and policy implementation along with risk management and mitigation.

Security Management Practices

- CIA Triad
  - Confidential, Accessible, Integrity
- Risk Analysis
  - Asset Identification and Classification
  - Threat analysis and threat agent/contagion
  - End Goal: Does the cost of the mitigation outweigh the cost of the asset?
- Security Policies
- Layers of Responsibility

Data Classification

- Classification ensures that sensitive data is properly controlled and secured
- Classification Roles
- Owner, Custodian, User
- Repeat as needed over time on value and age

- Governmental Data
  - Unclassified
  - Sensitive but Unclassified
  - Confidential
  - Secret
  - Top Secret
- Private Sector
  - Public
  - Sensitive
  - Private
  - Confidential

Separation of Duties

- The principle of separating of duties is that an organization should carefully separate duties, so that people involved in checking for inappropriate use are not also capable of make such inappropriate use
- No person should be responsible for completing a task involving sensitive, valuable or critical information from beginning to end. Likewise, a single person must not be responsible for approving their own work

Principle of Least Privilege

- Subject
  - A user of a computer resource, such as data, printer, connectivity method, etc.
- Object
  - Data and/or devices within a computer system or a computer network
- Principle
  - each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks

Why Use A Policy?

- The function of a security policy is to preserve the availability, integrity, and confidentiality of information resources.
- Company’s current and past activities become the *de facto* policy in the absence of an established policy.

Components of an Effective Policy

- Title
- Purpose
- Authorizing individual
- Author/sponsor
- Reference to other policies
- Scope
- Measurement expectations
- Exception process
- Accountability
- Effective/expiration dates
- Definitions

Successful Policies

- Clear up confusion, not generate new problems
- Have management support
- Written for a general audience (not “techies”)
- Aim for shorter; longer indicates policy may be to broad or have procedural contents
- Available to everyone
- Your written policy will drive how you can investigate and respond to possible intrusion.

Internet Security Policy

- Authentication
- Virus Detection
- Remote Access
- Intrusion Detection
- Appropriate Use (HTTP Access, Email)

Telecommunications and Network Security

Telecommunications, Network & Internet Security – the measures taken to safely transmit data “over the wire”.

Telecommunications and Network Security

- Technologies involved
- Common threats
- Firewall Configuration and management
- Security Tools

Technology ….

- Protocols
- The Layered Architecture Concept
- Open Systems Interconnect (OSI) Model
- Transmission Control Protocol/Internet Protocol (TCP/IP) Model
- Security-Enhanced and Security-Focused Protocols
- Firewall Types and Architectures
- Virtual Private Networks (VPN)
- VPN Protocol Standards
- VPN Devices
- Data Networking Basics
- Data Network Types
- Common Data Network Services
- Data Networking Technologies
- LAN Technologies
- WAN Technologies
- Remote Access Technologies
- Remote Identification and Authentication Technologies

Common Threats and Countermeasures (1/2)

- Denial of Service (DoS/DDoS) Attacks –
  - CM: CIR, Stateful firewall system
- IP Spoofing (“borrowing” someone’s IP)
  - CM RFC 2827 and RFC 1918 filtering and egress routing configured.
- Unauthorized Access
  - CM: ACL for protocol and users
- Trust Exploitation
  - CM: Private VLANs.
- Application Layer Attacks
  - CM: OS, devices and applications kept up to date with latest security fixes & Host Intrusion Detection System (HIDS).

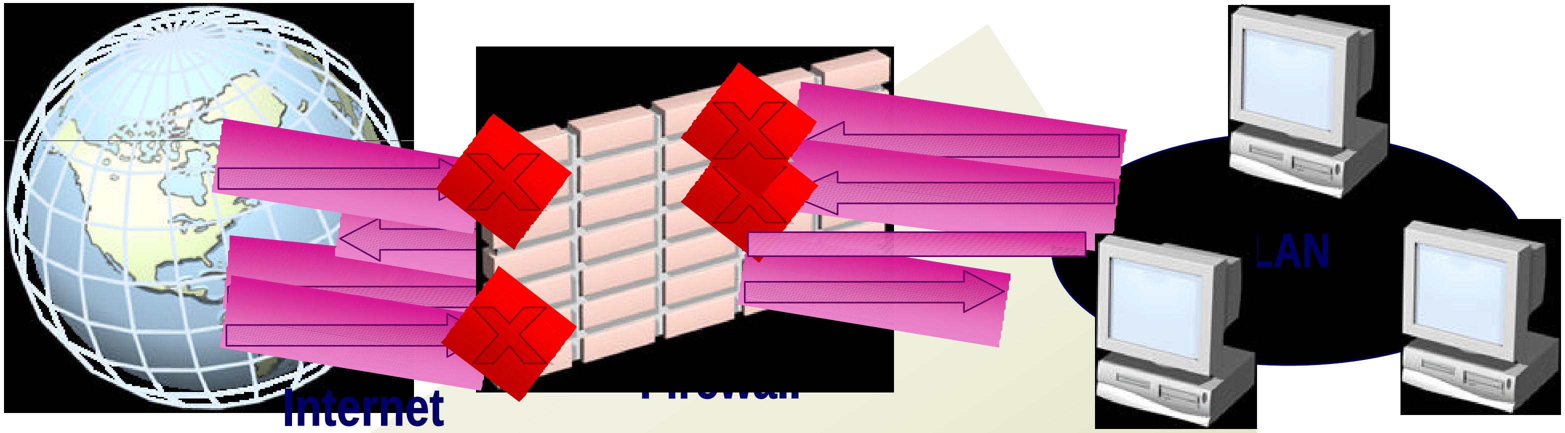
Common Threats and Counter Measures (2/2)

- SMURF – collusion based ICMP ECHO‘s send to multiple systems via amplifying network
  - – CM: Control ICMP traffic at the border/edge
- Fraggle – like a SMURF, using UDP
  - – CM: Control inbound UDP traffic
- SYN – attacker sends spoofed SYNch packets – attacker won’t get the SYN/ACK
  - – CM: modify connection timeout, increase TCP port size

A Few More Common Attacks ...

- Denial of Service (DoS)
  - Blocks service ports on servers, keeps them busy
- Vulnerability scanning
  - Searching for weak security policy
  - Weak encryption schemes
  - Security software may have Trojans
- DNS Attacks
  - Security holes in DNS servers, buffer overflows, attempted zone transfers
- IMAP Attacks
  - Security holes in IMAP protocol

How Firewalls Protect Networks and Computers
(Microsoft Security Clinic)



Firewalls protect networks and computers by providing such services as:

- Network address translation (NAT)
- Packet filters
- Server publishing
- Stateful packet inspection
- Packet content inspection
- Intrusion detection software

Firewalls (a place to start)

- Firewalls cannot protect against inside attacks
  - Most loss due to computer security incidents is caused by insider abuse
- Various firewalls are subject to a variety of well-known port attacks with frequent updates
- Firewalls do not protect against attacks that bypass it (i.e. tunneling or application based attacks)

Firewall Pitfalls

- Common to only install a firewall to protect the internal network from the external network
  - Traffic should be controlled outbound as well
- Assume that the firewall will protect against current and future threats
- Pitfalls
  - The firewall is not complimented with additional security measures
  - Organizational security policy is not reviewed regularly
  - Firewalls are not updated and logs not checked thoroughly because of the volume involved, lack of trained personnel, and lack of time – or management will power

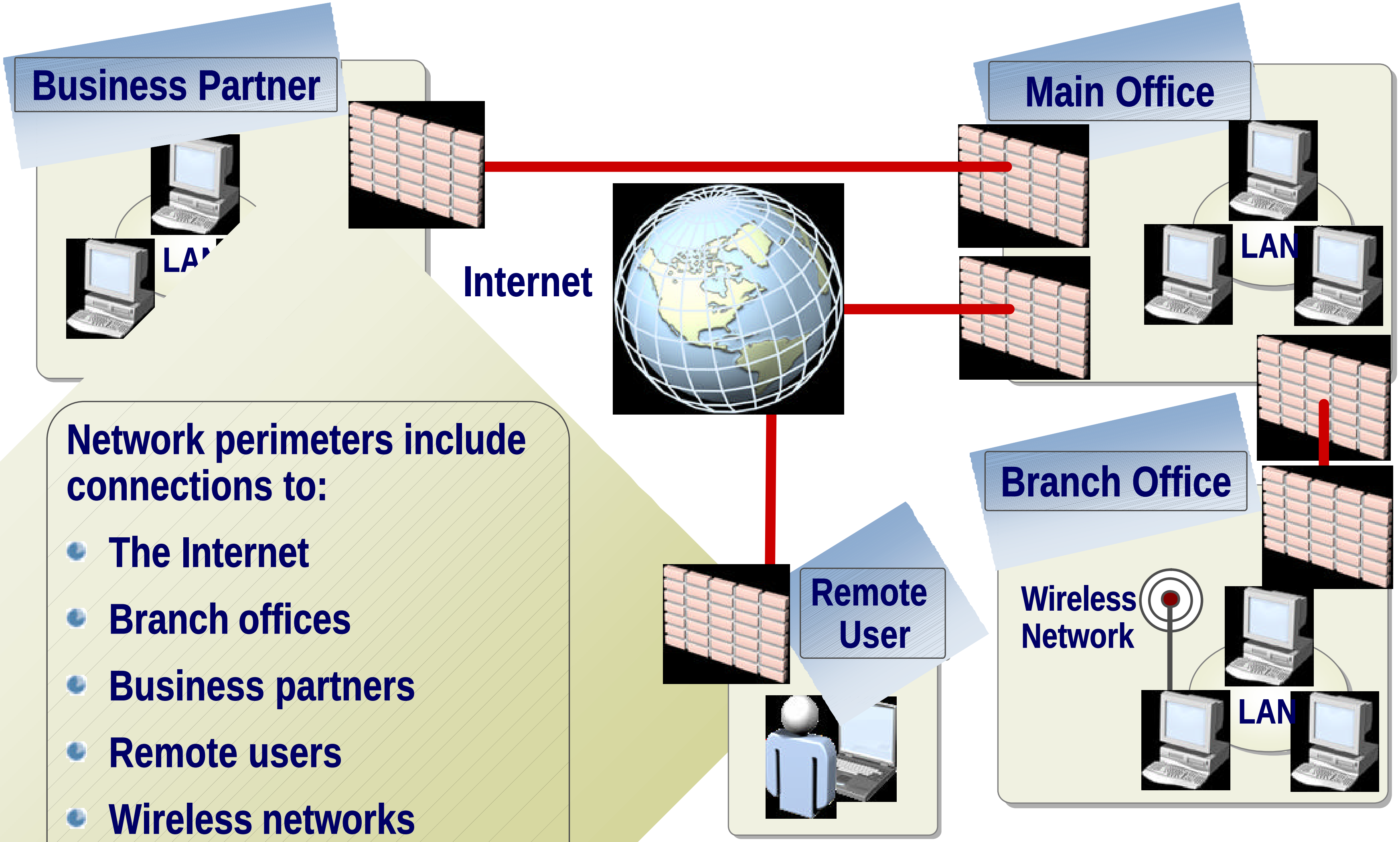
Types of Firewalls?

- Personal Firewalls (sub $100)
  - ZoneAlarm
  - Ontrack SystemSuite
  - BlackICE Defender
  - Norton Internet Security / Personal Firewall
- Firewall Appliances
  - Cisco Secure PIX Firewall, Nokia Firewall, SonicWall
- OS server based
  - Microsoft ISA Server
  - Check Point FireWall-1
  - Linux based systems (ipcains or iptables)

Firewall Features

- Network Configuration
  - Inside, Outside, Perimeter, Traffic flow
- Security Policy Rule Base
  - Zones
  - Time of day
  - Content management, allowed content
- Network Address Translation
  - Dynamic, fixed, many to many
- Virtual private networks (VPNs)
  - PPTP
  - L2TP/IPSec

Identifying a Network Perimeter
(Microsoft Security Clinic)

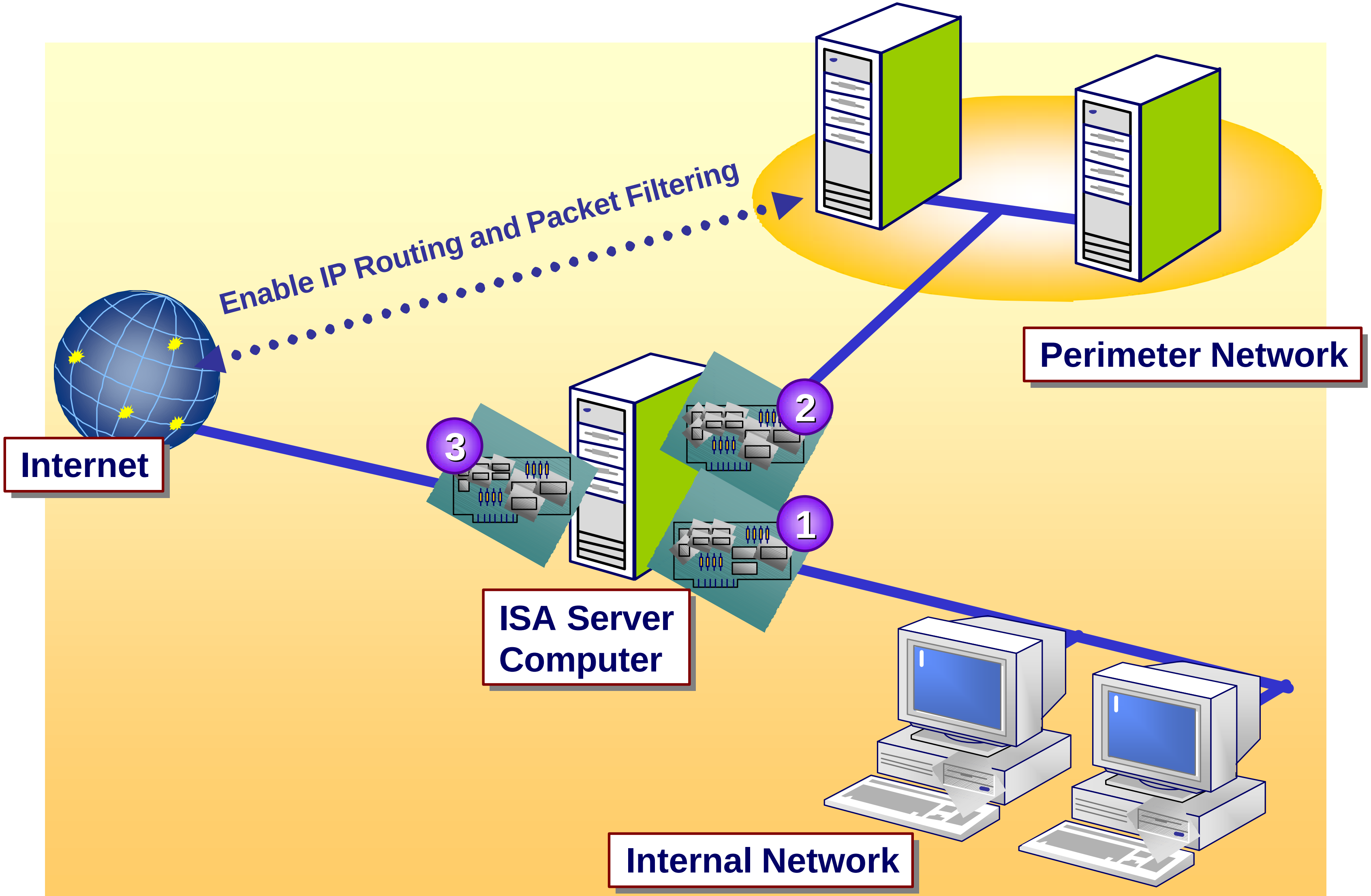


Network perimeters include connections to:

- The Internet
- Branch offices
- Business partners
- Remote users
- Wireless networks
- Internet applications

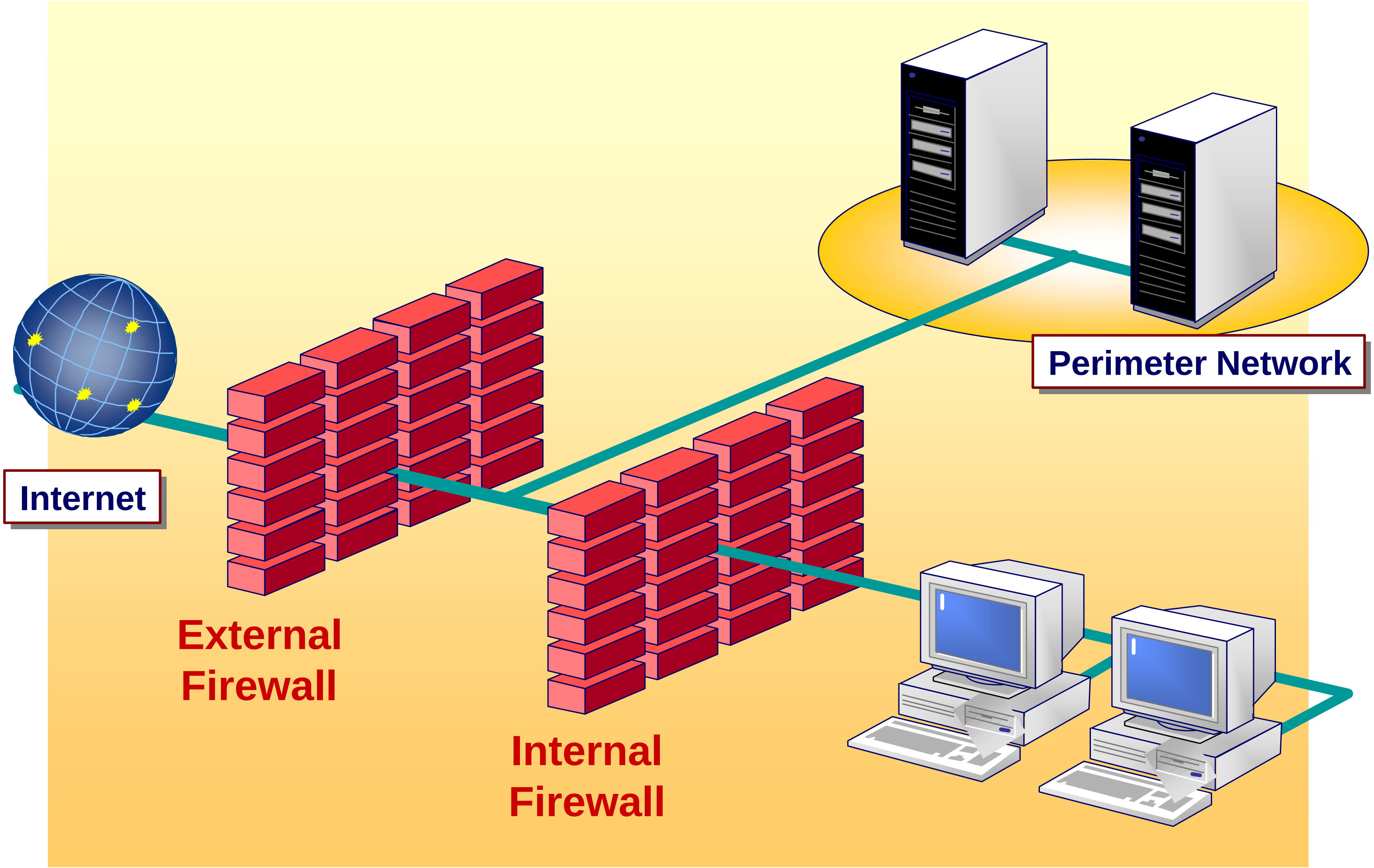
Three-Homed Perimeter Network

(Microsoft Security Clinic)



MOC 2195)

Perimeter Network with Back-to-Back Firewalls (Microsoft security clinic)



MOC 2195)

Best Practices (Microsoft Security Clinic)

- ☑ Stay Informed About Security Issues
- ☑ Install the Latest Service Pack and Security Updates
- ☑ Do Not Run Unnecessary Services or Accept Unnecessary Packets
- ☑ Audit Security-Related Events and Review the Associated Log Files
- ☑ Document All Aspects of Your Network Configuration
- ☑ Understand the Network Protocols that You Use With ISA Server
- ☑ Maintain Physical Security

MOC 2195)

Virtual Private Network

- PPTP - Point to Point Tunneling Protocol
  - Microsoft standard
  - Creates VPN for dial-up users to access intranet
- SSH - Secure Shell
  - Allows encrypted sessions, file transfers
  - Can be used as a VPN
- IPSec + L2TP
  - Set of protocols developed by IETF
  - Two modes
    - Transport Mode: encrypted payload (data), clear text header
    - Tunnel Mode: encrypted payload and header
  - IPSEC requires shared public key

Security Tools

- Security scanners
  - Nessus
- “Honey Pots” – as described in Cheswick
  - Be aware that there is impending legislation that may affect their viability
- Port Scanners
  - NMap for Linux
- Intrusion Detection Systems
- Firewalls
- Scan sites

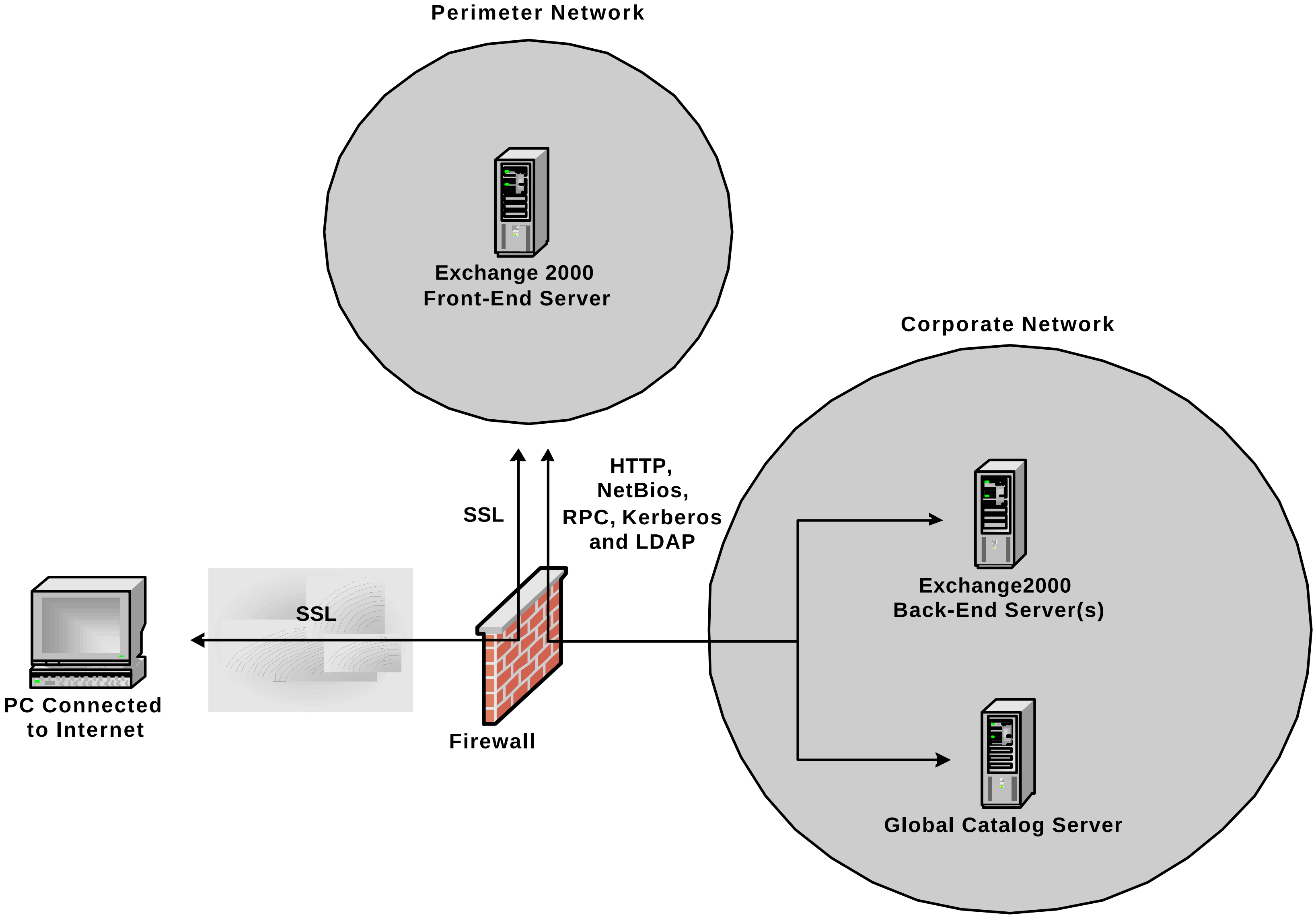
Configuring Email systems

- Messaging and message system availability behind firewall systems
- Middle perimeter / screened subnet system allows access through the firewall for an authenticated user.
- Auto response – yes or no?

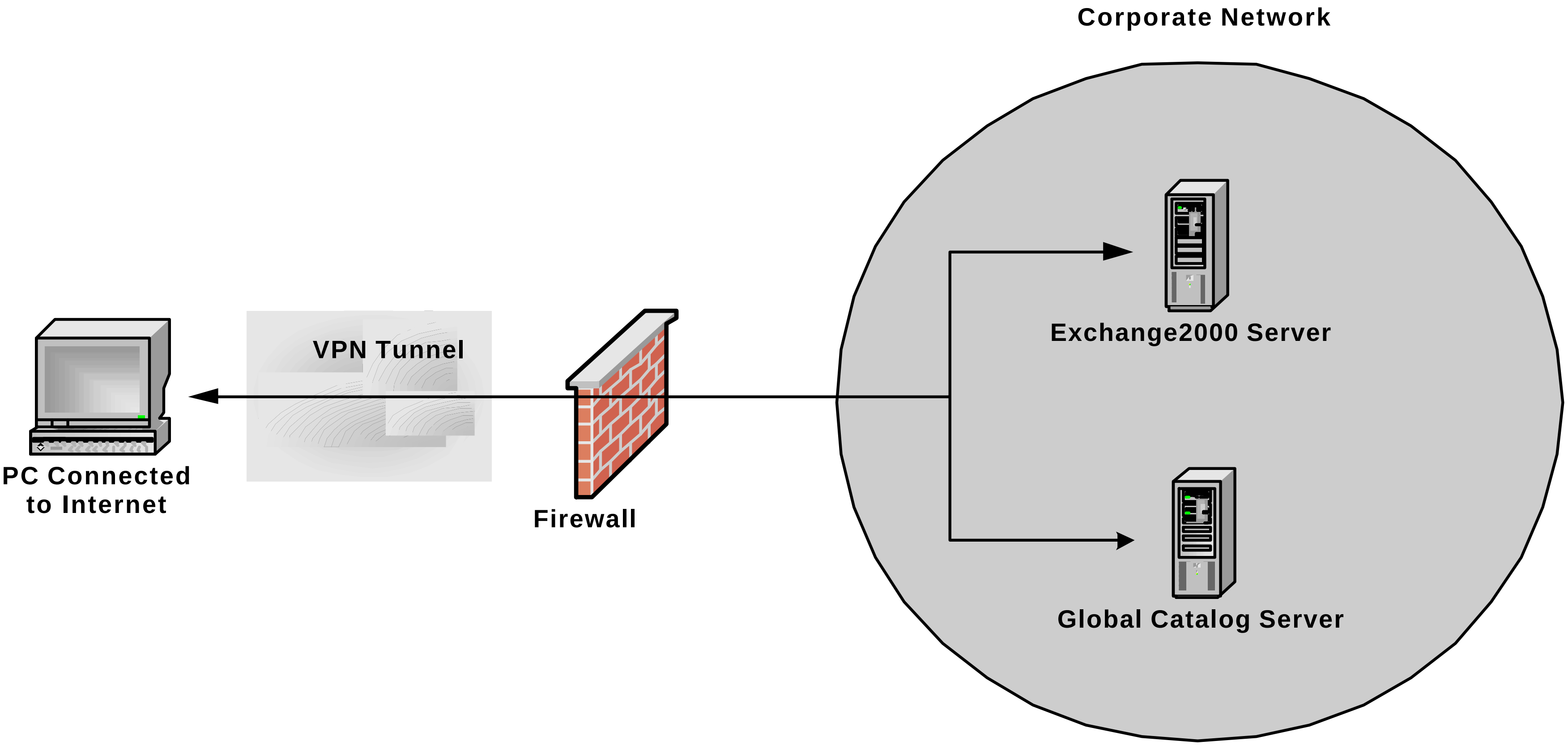
Microsoft Exchange OWA

- OWA - Microsoft Web based Collaboration solution
- Secure access through Digital Certificates and SSL
- Secure access through a VPN tunnel
- Access Microsoft Exchange Server from non-Microsoft Systems

Exchange 2000 OWA via SSL



Exchange 2000 OWA via VPN



TCP/IP Security

- Identify the protocols used
  - HTTP, FTP, NTP, SMTP, HTTPS, NetBIOS, H.323, Streaming, NNTP, POP3, ARP, RARP, SNMP, ….. To name a few.
- Verify the ports required by the protocols and the direction of travel
- TCP/IP security can applied via:
  - IP address and domain name restrictions
  - TCP/IP filtering
  - IP security policy snap in (Windows)
  - Security configuration tool set

Examples of Web Server Authentication

- Anonymous Access
  - Public Web pages
- Basic Access
  - Username/Password cleartext
- Integrated NTLM authentication
- Digest
  - Strong security in a lightweight fashion
- Certificates
  - Code signing, E-commerce, user mapping

Security Models

For this presentation, security models are beyond the scope. There are a variety of formal models to define a system; many are military or government in nature, and often to not find their way into commercial systems.

Examples include ... Clark Wilson, Biba, Take Grant, Orange/Red/Rainbow Series, and the Common Criteria