Introduction to Network Security

Dr. Usha Rani
Vice President, NMSWorks Software Limited

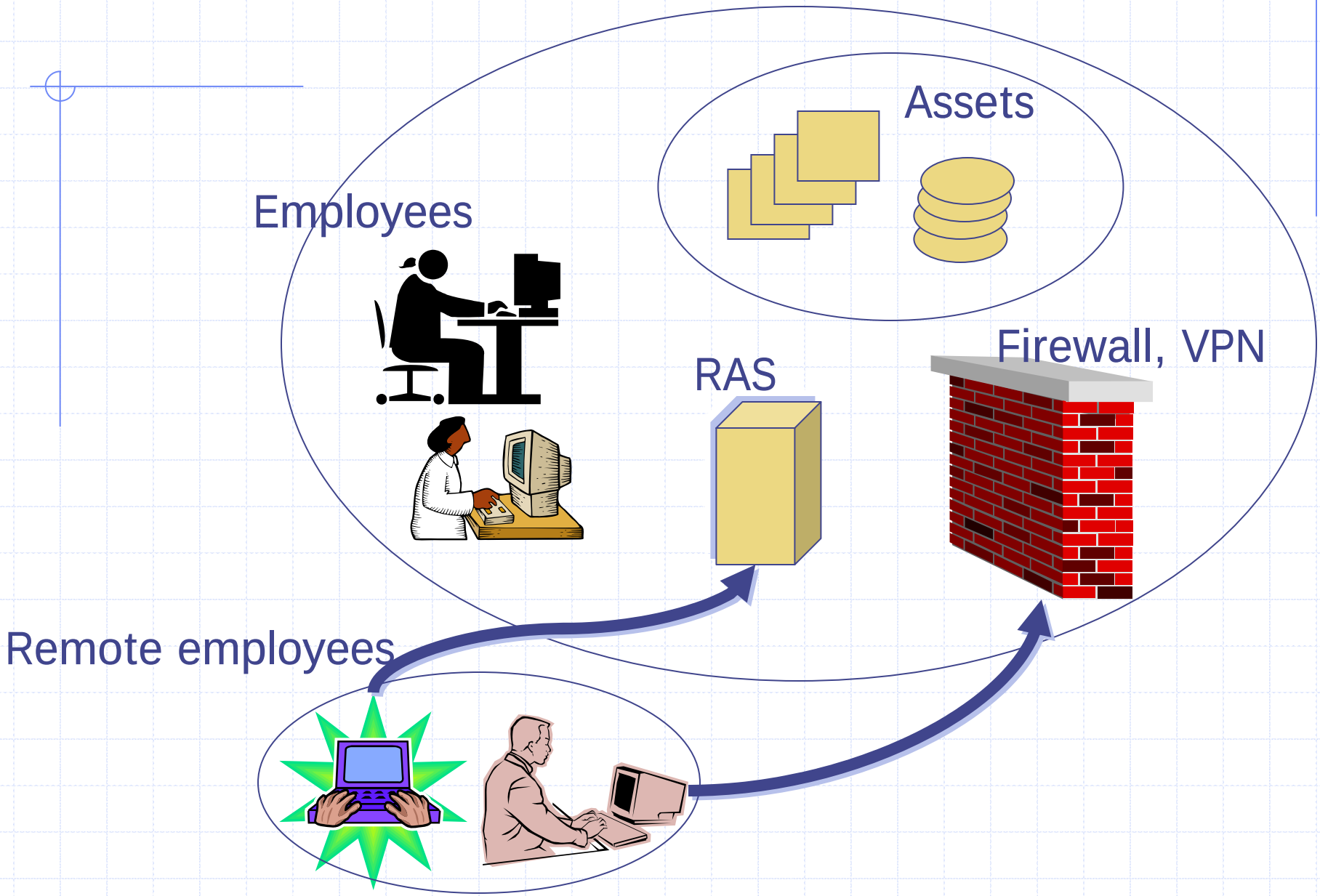
Network security threats are real!

- Basic technologies have evolved from collaborative computing requirements where security was not much of a concern

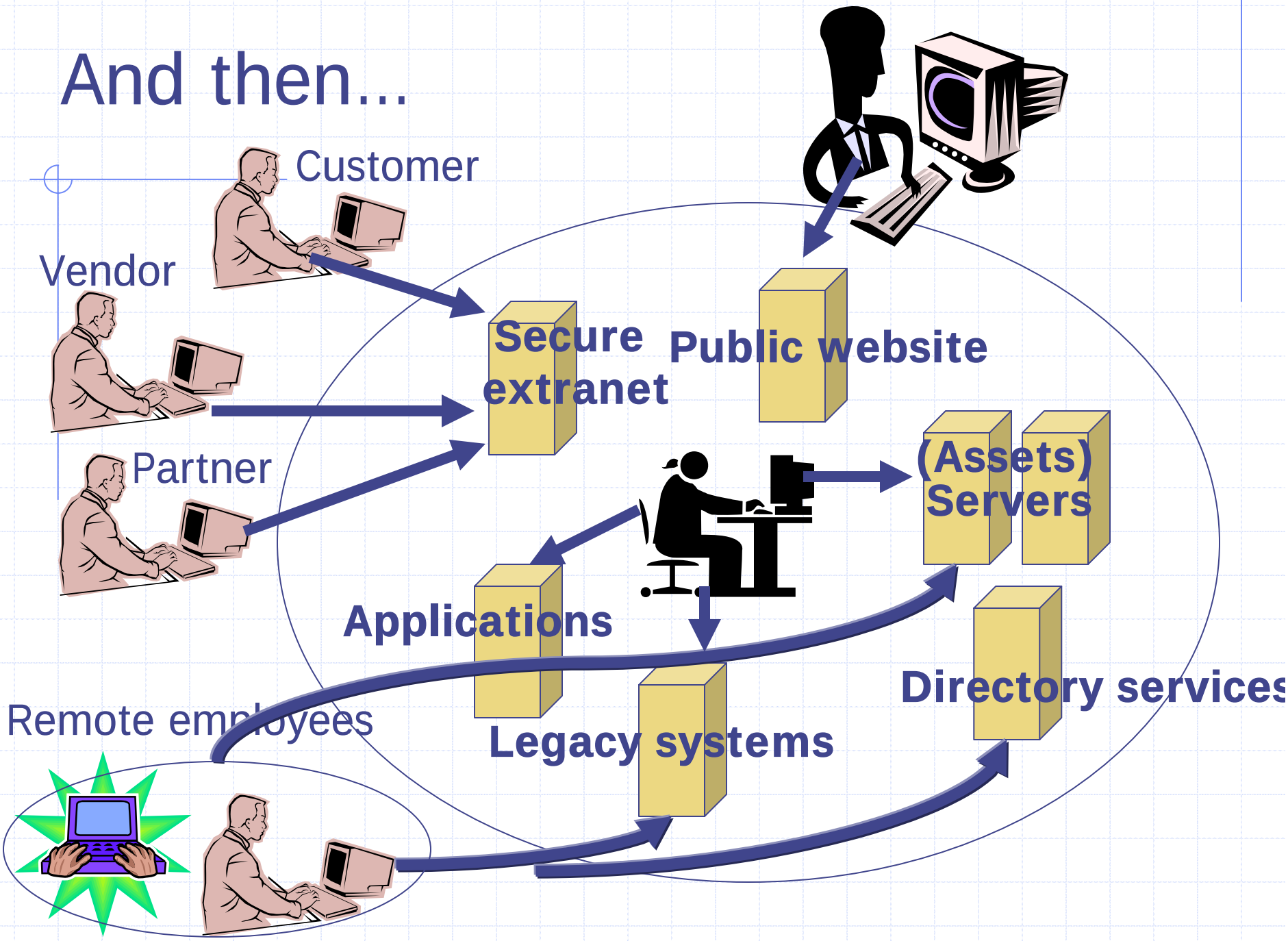
Trends

- Connectivity is no longer an option, it is a necessity to organizations
- Along with the undeniable benefits, there are threats that arise

The way it was ...

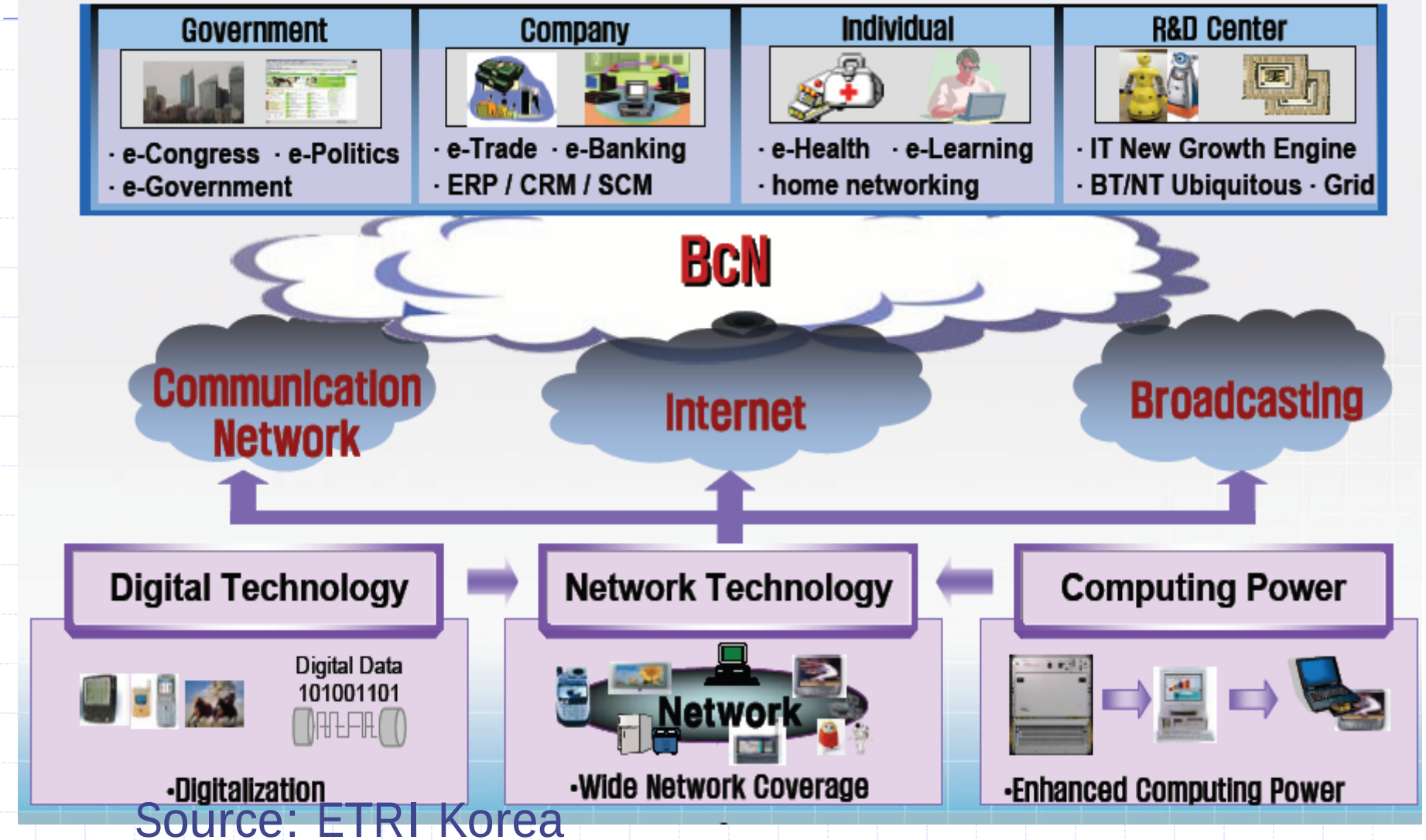


And then...


Customer
Vendor
Partner
Secure extranet
Public website
(Assets) Servers
Applications
Legacy systems
Directory services
Remote employees

The way it is today

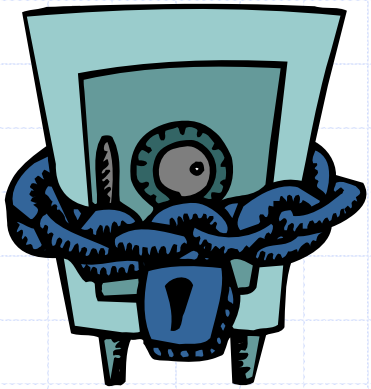
- Next generation network which provides seamless converged services from communication, broadcasting and Internet at anytime and anywhere.



Source: ETRI Korea

The need for security

- Prior to this “computer era”, information felt to be valuable was protected by physical and administrative means



Hacking no longer esoteric

- Hackers develop tools that are freely available and easy to use
- Anyone with browser access can download them from common sites like rootshell.com, securityfocus.com, insecure.org
- Leading search strings from any search engine give overwhelming responses

What makes cyber crime easy

- Not easy to introduce legislation to punish malfeasors
- However, in the last few years, awareness of the painful reality has been hammered in
- Escalation from term “hacktivism” to “cyberterrorism” to “information warfare”
- In India, the first cyber-crime-only police station has been set up in Bangalore

Security incidents

- BARC network was successfully attacked
- Ministry of External Affairs (MEA) website defaced
- Done by GForce, a Pakistan based hacker group
- GForce has admitted to repeatedly hacking the Indira Gandhi Centre for Atomic research and 13 other Indian websites over a month
- In addition, there are....

Acknowledged and known surveillance systems

- Echelon is a global surveillance system built and operated by the US, UK, Canada, Australia and New Zealand
  - Can eavesdrop and spy on any telephone, email and telex communication around the world
  - Satellite communications, land based communications and radio communications impartially monitored
  - Indiscriminately spies on all the communications and then extracts ones of interest

Acknowledged and known surveillance systems

- Carnivore is a network traffic interceptor
- Is deployed at ISPs
- The traffic of interest can be filtered out from the mainstream traffic intercepted

Acknowledged and known surveillance systems

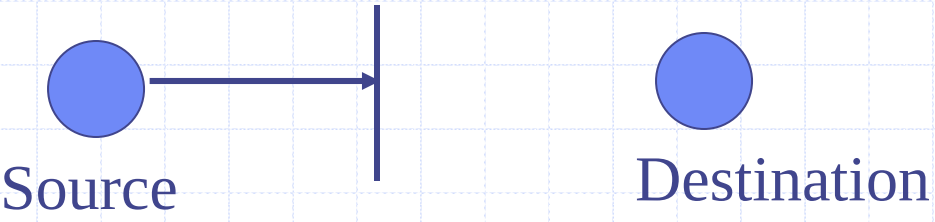
- Magic lantern is a key stroke logger
- The implications are obvious
- Self proclaimed FBI motto

In God we trust, the rest we monitor…….

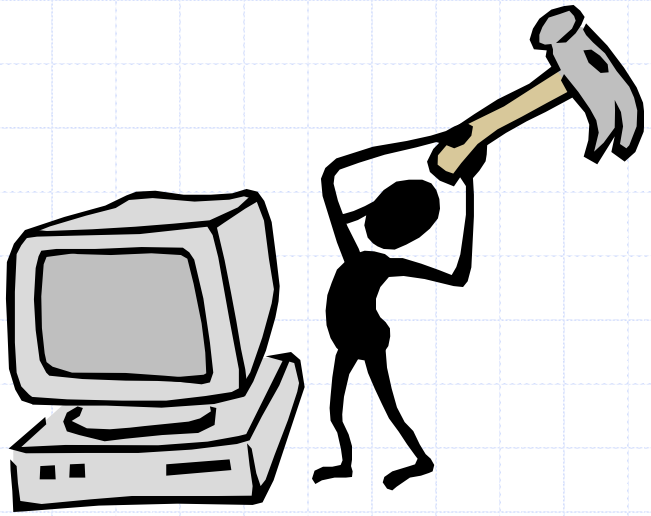
A classification of attacks

- Most security attacks can be classified into one of the following generic types
  - Interruption
  - Interception
  - Modification
  - Fabrication

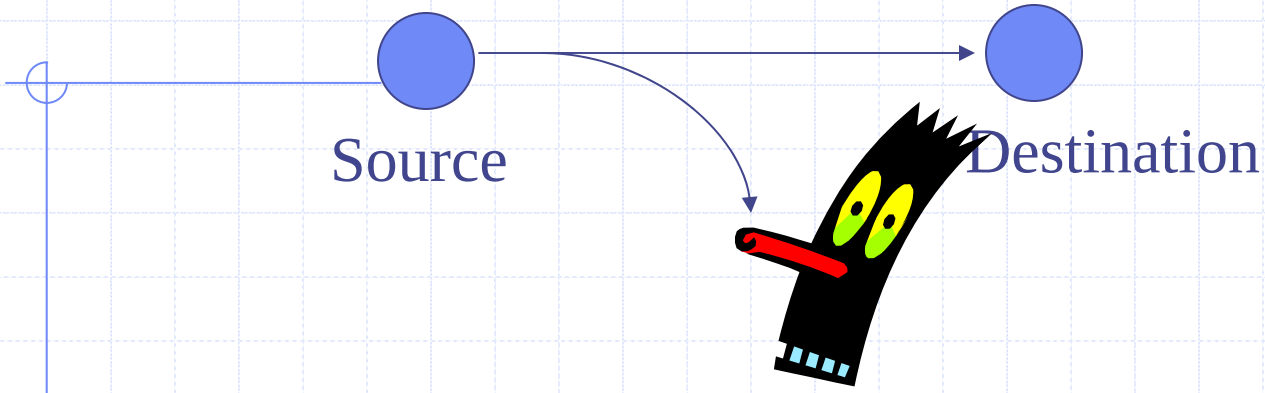
Interruption



- Attack on availability
- Denial of service attacks
- Malicious code such as viruses, worms, Trojans
- Destruction of hardware or communication lines



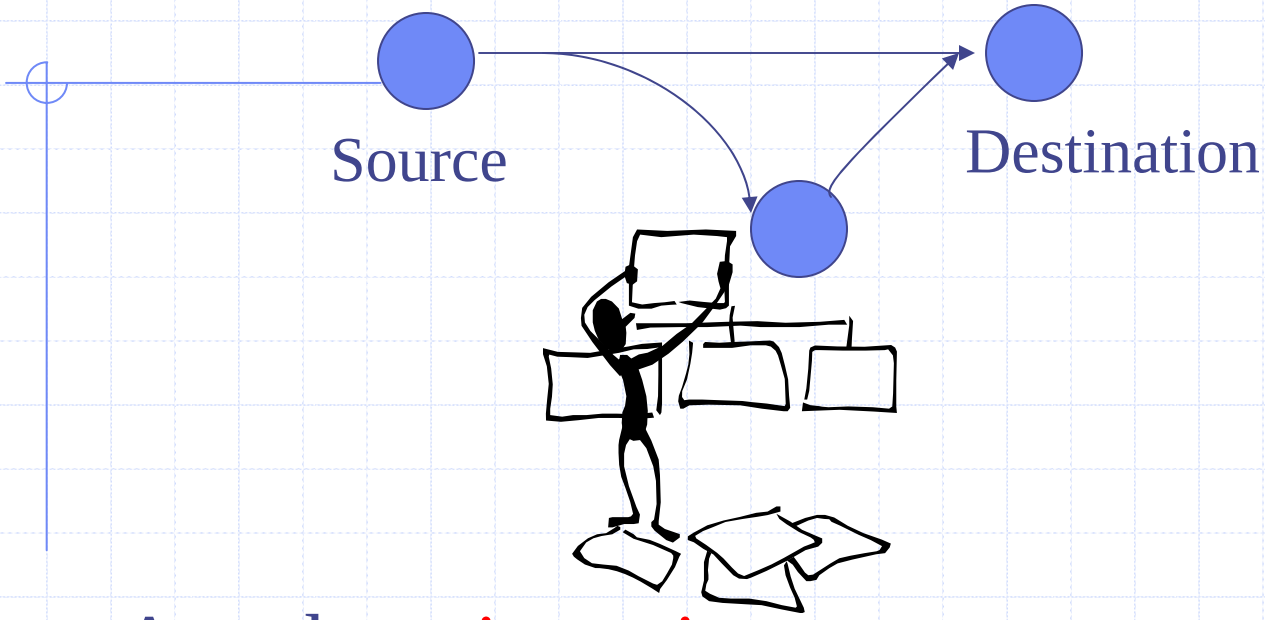
Interception



- Attack on confidentiality

- Eavesdropping, wiretapping, keystroke logging
  - Physical layer by tapping the communication medium
- At network layer, use packet sniffers and protocol analysers

Modification



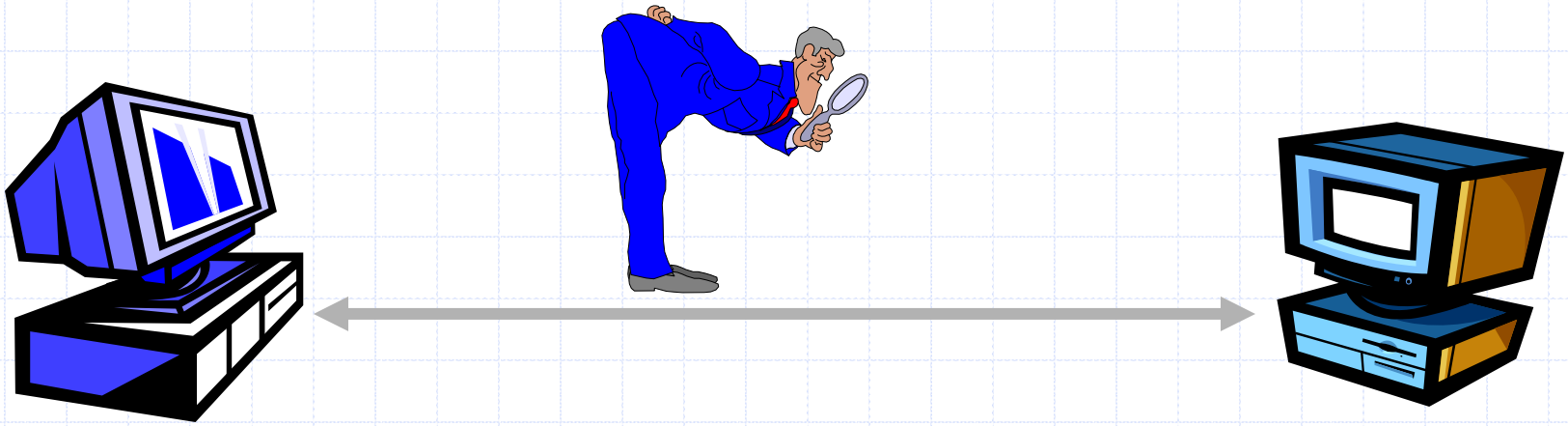
- Attack on integrity
- Attacker could modify
  - Data
  - Programs
  - Authentication data

Fabrication

- Happens due to weak authentication of entities
- Results in spurious records or false message in a network

Passive attacks

- Passive attacks
  - Eavesdropping to enable adversary to get message contents
  - Traffic analysis



Active attacks

- Masquerade - Impersonation of some other entity
  - Results as a result of authentication or access control violation
- Replay – passive capture of some data and its subsequent retransmission
- Data modification – Data which is captured by unauthorized means is modified
- Denial of service – render normal facilities unfit for use

Goals of security

- Provide confidentiality of sensitive information – only intended persons can see the information
- Authenticate legitimate entities – make sure they are who they claim to be
- Provide access control - prevent unauthorized entry to information systems

Goals of security

- Enforce non-repudiation of transactions – an entity cannot later disavow a transaction
- Ensure freshness of transactions
  - a message, or a portion of a message, is recorded and replayed later
- Ensure availability of systems and services to legitimate users

Electronic security services and mechanisms

- Most mechanisms that provide the services of confidentiality, integrity, authentication, access control and non-repudiation are cryptography based
- Availability of systems and services requires other mechanisms as well
  - Firewalls, Intrusion Detection / Prevention Systems

Authentication

- Password based is the most familiar technique
  - Based on something a user “knows”
- Smart cards / tokens
  - Based on what the user “has”
- Biometric systems – finger print, retina, palm geometry
  - Based on what the user “is”
- Multi-factor authentication systems combine several of the above
- Cryptographic techniques – digital signatures

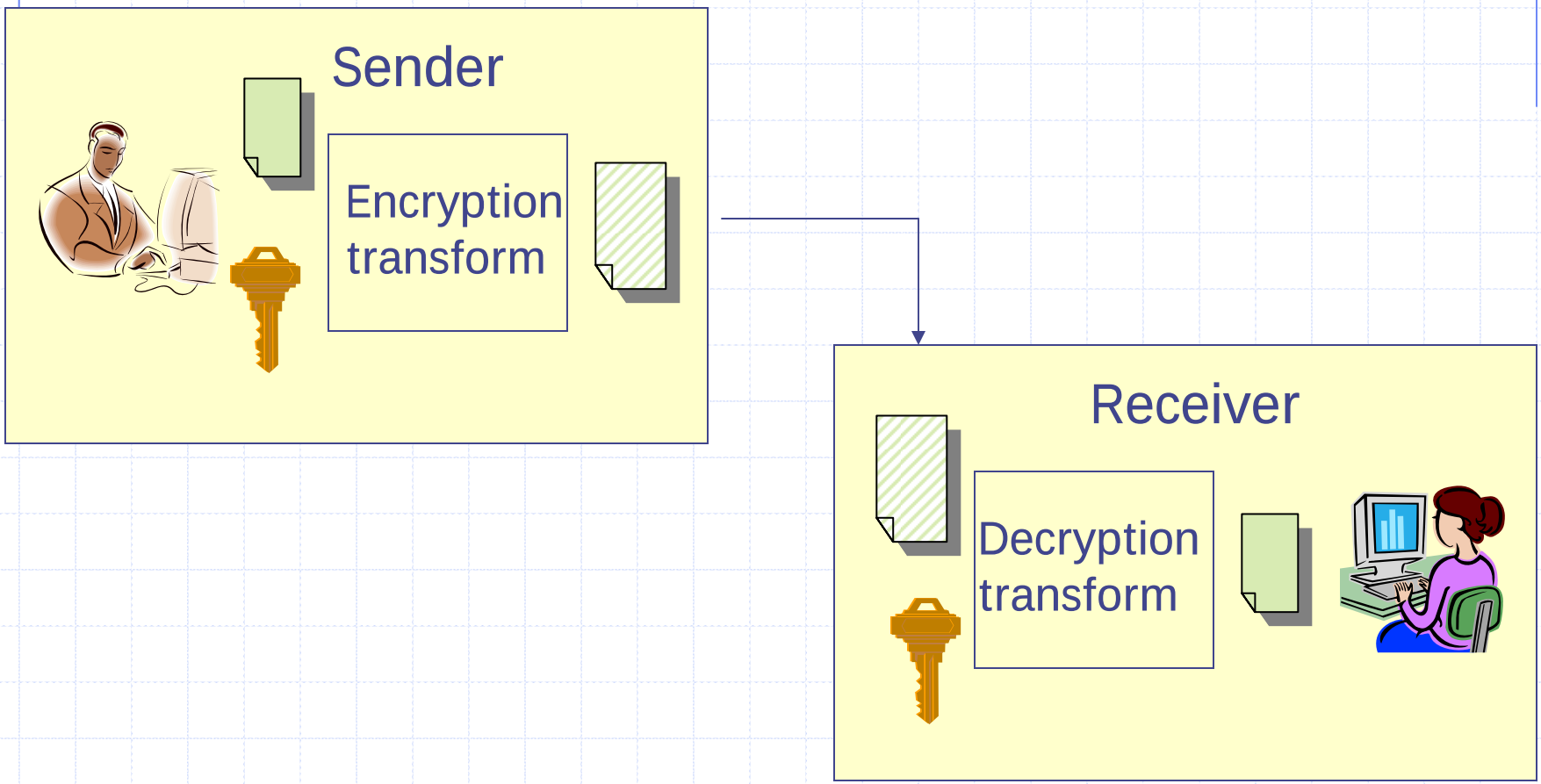
Confidentiality

- Two kinds of crypto systems
  - Symmetric key cryptosystems
    - Classical and familiar method
    - Sender and receiver share a key (secret)
    - Egs. DES, 3-DES, AES, Blowfish
  - Asymmetric or public key cryptosystems
    - Sender and receiver have no shared secret
    - RSA, El Gamal, Diffie Hellman, elliptic curve based systems

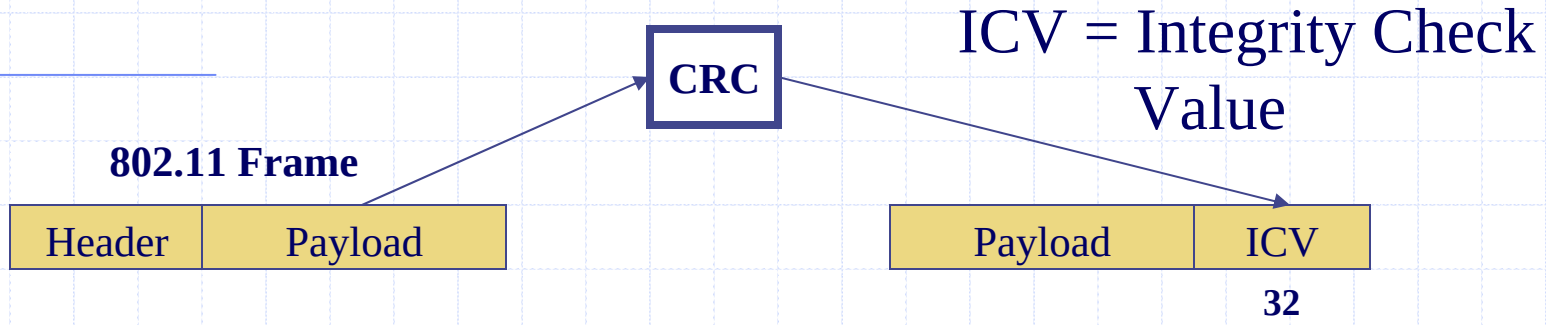
Symmetric key ciphers

- Block ciphers
  - Message is broken up into equal sized blocks and encryption transformation is applied to each block
  - Eg. DES, AES, Blowfish, Twofish etc.
- Stream ciphers
  - Message is operated on a bit at a time
  - Eg. RC4 used in WEP

Symmetric key systems

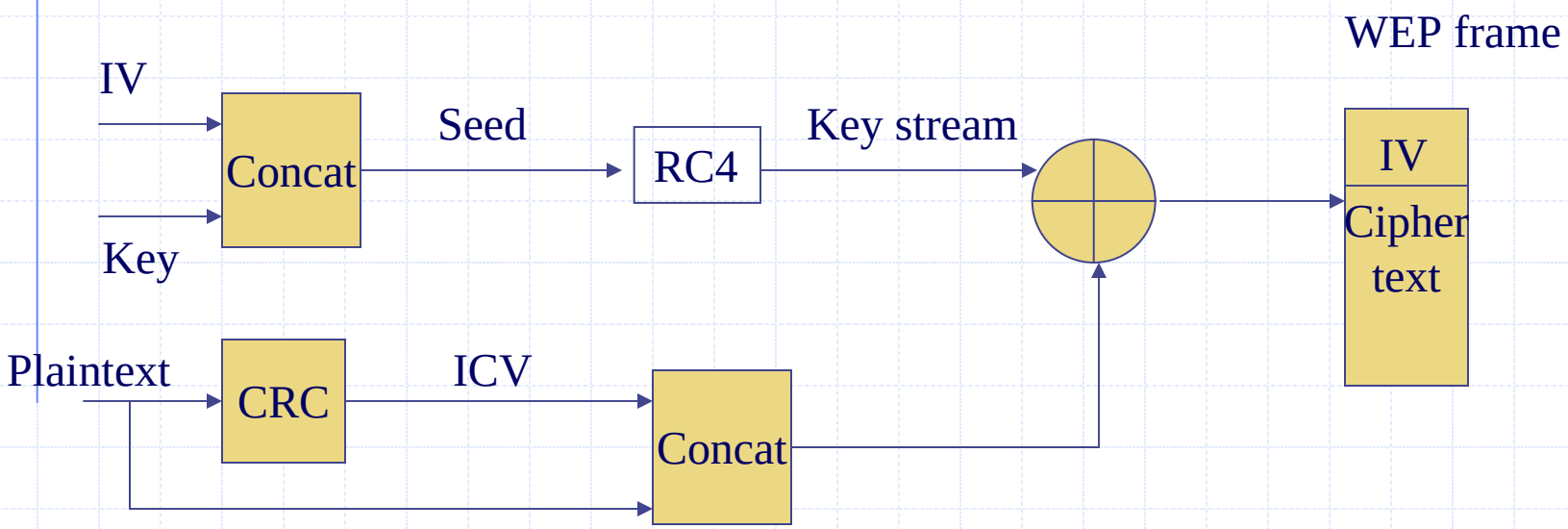


WEP



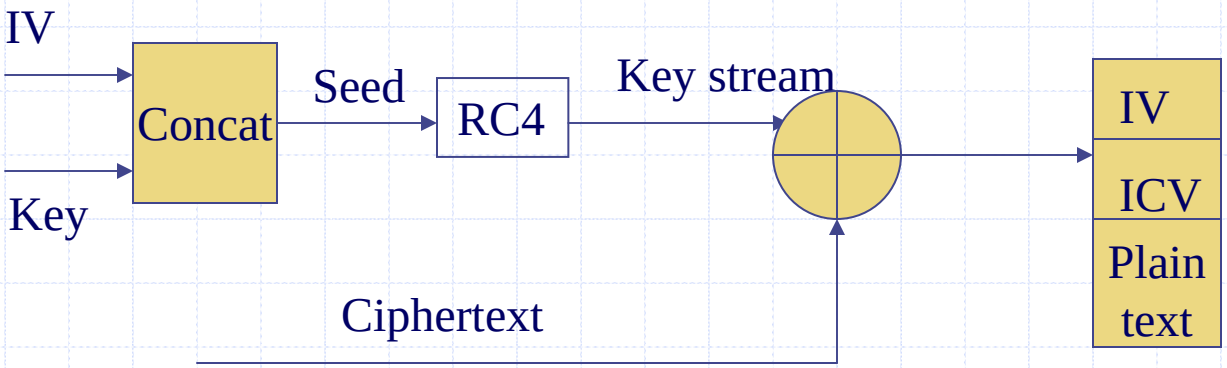
- ICV computed – 32-bit CRC of payload
- RC4, a stream cipher is applied on this payload
  - This is a well-known cipher, and the designers were wise to choose it

WEP encryption

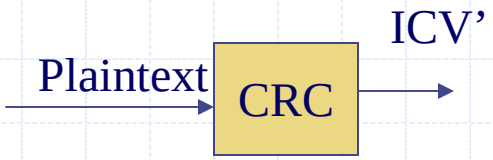


IV – Initialization Vector, one per packet
Key – Shared secret key
ICV – Integrity check value

WEP decryption



IV – Initialization Vector, one per packet
Key – Shared secret key
ICV – Integrity check value



If ICV' = ICV, integrity preserved

Stream ciphers – some pitfalls

- $C = P \oplus KS$
- Key streams must never be reused
  - $C1 \oplus C2 = (P1 \oplus KS) \oplus (P2 \oplus KS) = P1 \oplus P2$
    - => if a part of one plaintext is known, corresponding part of the other can be obtained
- Forgery is easy – Bit flip attack
  - If $P2 = P1 \oplus X$
  - Then $C2 = C1 \oplus X$

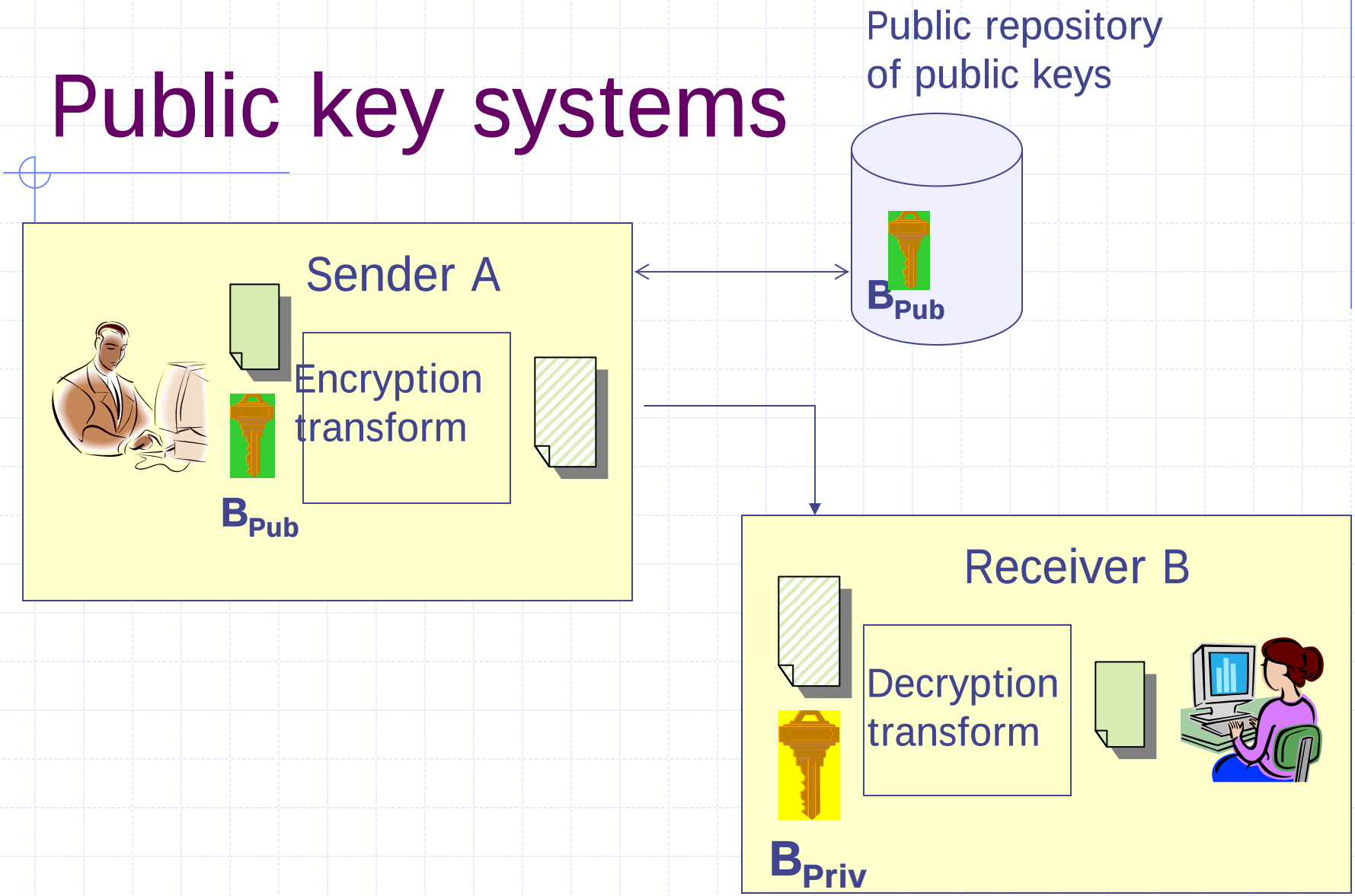
WEP solution

- ICV – Prevents forgery
  - Checksum on the data prevents bit flipping
- IV – Prevents key reuse
  - Each packet a new key that starts a new stream is used
- Practically however
- The keystream for WEP is RC4(IV,K), which depends only on IV and K
  - k is a fixed shared secret - every user in WLAN shares the same k
- So the keystream depends only on IV
  - If two packets ever get transmitted with the same value of IV means keystream reuse
- Since IV gets transmitted in the clear for each packet, the adversary can even easily tell when a value of IV is reused (a "collision")

Public key systems

- Each communicating entity has a key pair – one public and one private
- The public key is made available to others in some fashion, private key is kept secret

Public key systems



Integrity

- Simplest technique – XOR
- Checksums, CRC systems
- Hash functions
  - Message digests
  - Condense an arbitrary length message to constant length output
  - Egs: SHA-1, MD5
- Message Authentication Code (MAC)
  - Keyed hash

Hybrid systems

- A chooses a secret symmetric key that will be used as a session key.
- A uses the session key to encrypt message to B
- A uses B’s public key to encrypt the session key
- A sends the encrypted message and the encrypted session key to B
- On receipt, B the session key using his own private key.
- B uses the session key to decrypt A's message.

Digital signature

- A digital signature has to bind the message with sender's identity
- Signature
  - Compute hash of message M to be signed
  - Encrypt hash using sender's private key
  - Attach to message M
- Verification
  - Receiver retrieves sender's public key
  - Decrypts signature block using this
  - Computes hash of message and compares it with decrypted value

Ensuring freshness

- Digital timestamp
  - Message and timestamp must be tied together and encrypted
- Sequence numbers
  - Not effective in connectionless network
- Nonces
- Challenge response protocols

Ensuring availability

- Provision for alternate network paths
- Provision for redundancy of critical servers and services
  - Computing power
  - Storage
- Provision for redundancy of data and within data
- Firewalls, intrusion detection systems

Denial of service attacks

- Intention
  - Prevent legitimate users from accessing resources
- Common resources targetted
  - Bandwidth, processing power, memory
  - Abundance of these resources can only raise the bar, not eliminate impact
- Defence against DoS attacks
  - Rate limiting, packet filtering etc.
  - Far from an exact or complete science
- Interdependency of security on the Internet
  - The exposure to DoS attack of SiteA depends on the security of SiteB
  - There are huge numbers of SiteB's

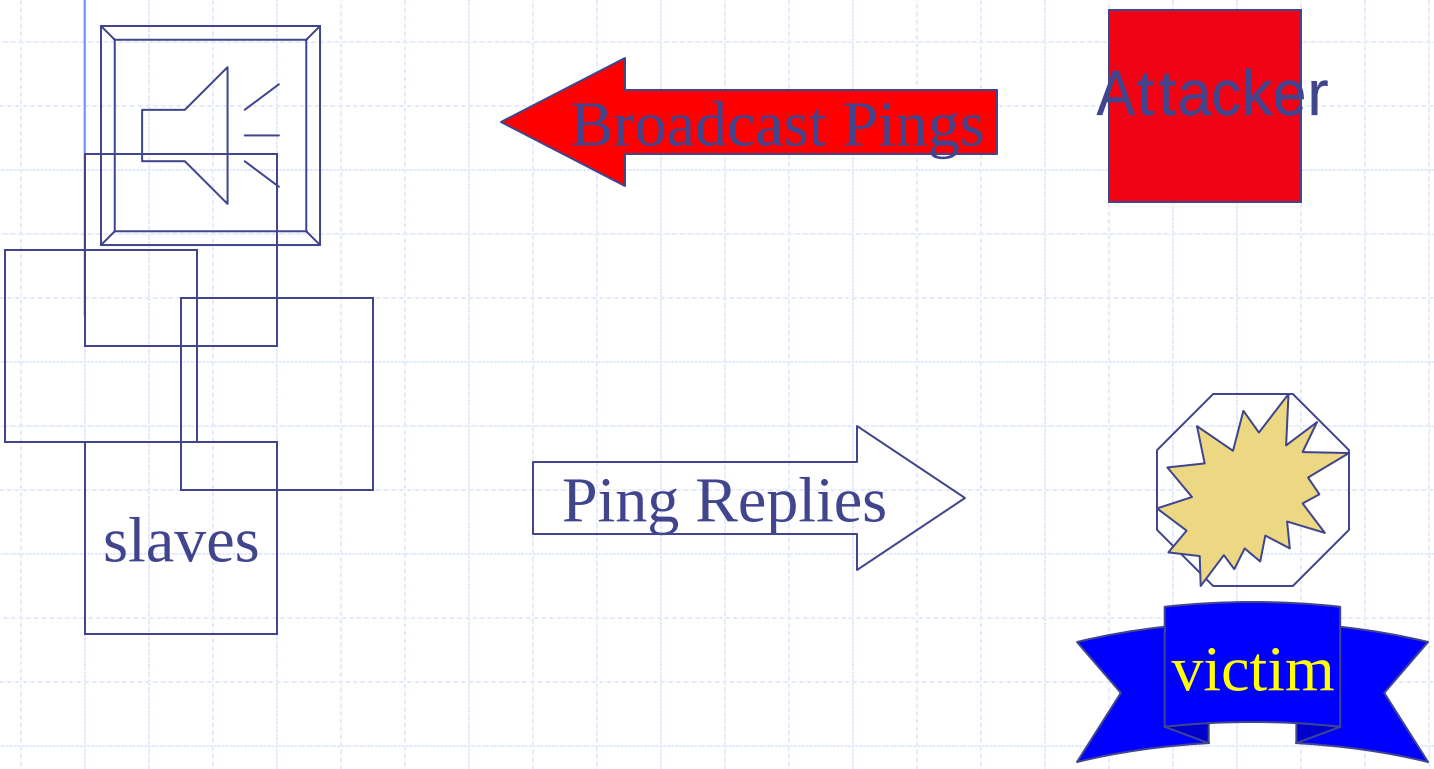
Early DoS attacks

- Packet floods to consume bandwidth
  - UDP flood
  - ICMP echo request/reply flood
  - Amplification attacks
- TCP SYN flood to consume memory
- Finger bomb to consume CPU
  - finger xyz@victim.com@differ.com - fingers user xyz at victim.com and makes it appear as if the request is from differ.com
  - finger xyz@victim.com@victim.com@victim.com@victim.com..
- IP fragmentation attacks
  - Based on limits to packet sizes

Pre-1999 DoS attacks

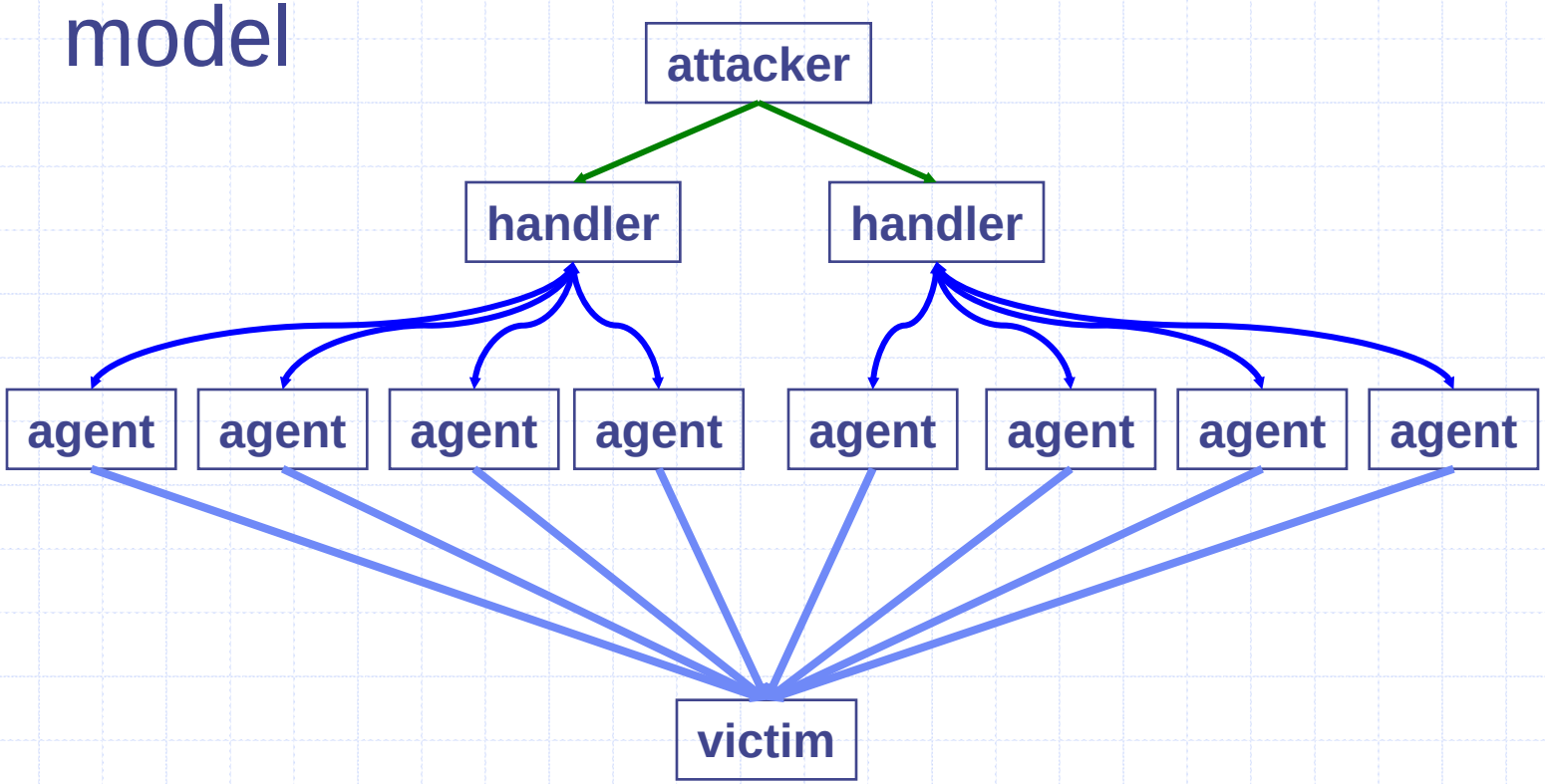
- DoS Tools:
  - Single-source, single target tools
  - IP source address spoofing
  - Packet amplification (e.g., smurf)
- Deployment:
  - Widespread scanning and exploitation via scripted tools
  - Hand-installed tools and toolkits on compromised hosts
- Use:
  - Hand executed on source host

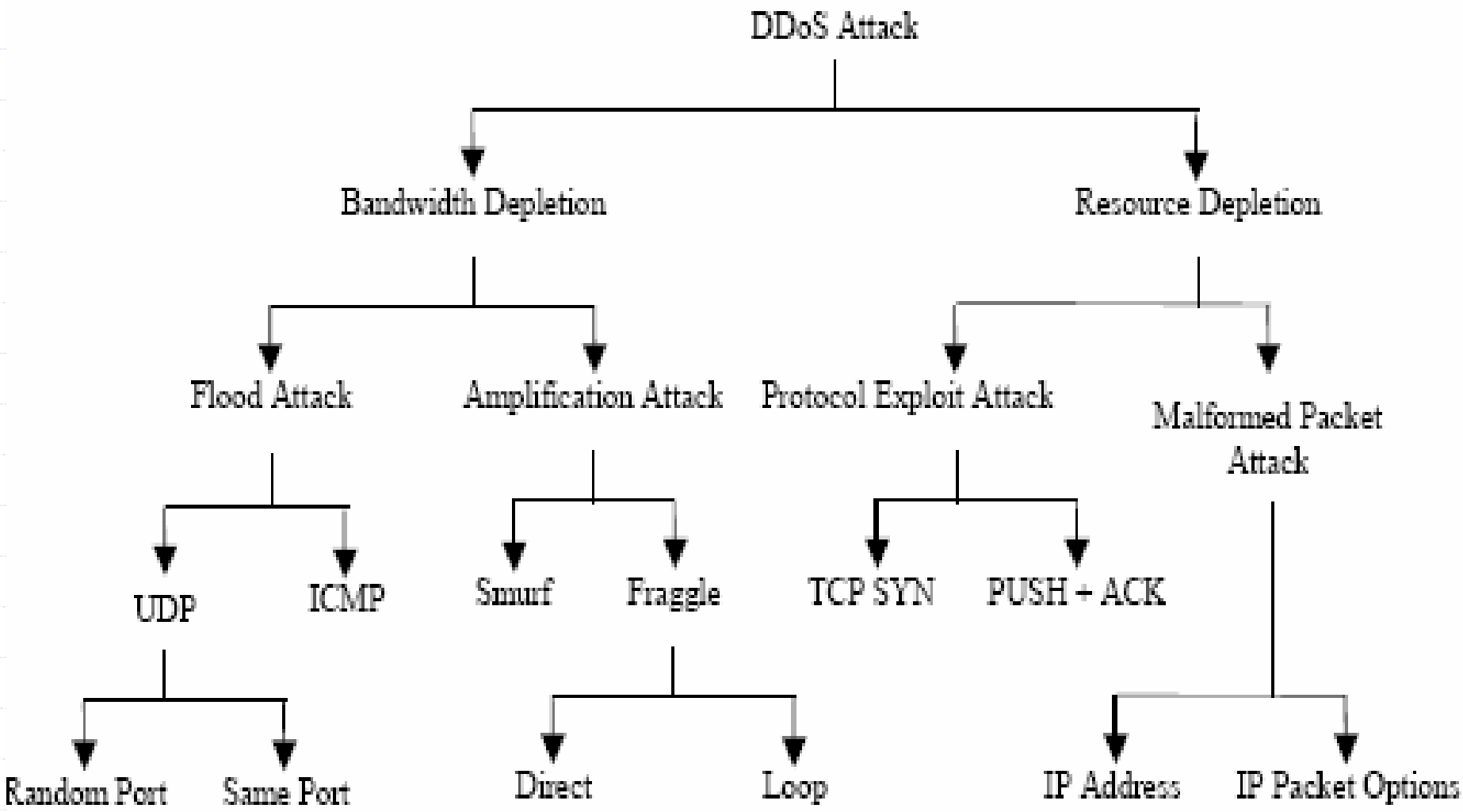
Smurf Attack (2-tier)



Distributed Denial of Service

Control Infrastructure – The classic DDoS model




DDoS Attack
Bandwidth Depletion
Resource Depletion
Flood Attack
Amplification Attack
Protocol Exploit Attack
Malformed Packet Attack
UDP
ICMP
Smurf
Fraggle
TCP SYN
PUSH + ACK
Random Port
Same Port
Direct
Loop
IP Address
IP Packet Options

Degree of Automation

- Manual
  - attacker manually scans, breaks in, installs attack code, then directs the attack
  - Used by early DDoS attacks only
- Fully Automated
  - exploit/recruitment phase and attack phase both automated
    - everything is preprogrammed in advance
    - no need for further communication between master & agent
    - minimal exposure for attacker
    - inflexible - attack specification is hard coded
    - hybrid of auto/semi-auto

Overview of DoS/DDoS

- DDoS
  - entities: attacker, [masters], agents, target
  - stages:
    - recruit - scan potentially vulnerable hosts
    - exploit - compromise a vulnerable host using some exploitable vulnerability
    - infect - propagate the attack code to the new agent
    - attack – use attack code to inflict denial of service

Degree of Automation

- Semi-Automated
  - recruitment phase automated, attack phase manually initiated
  - requires communication between master & agents to initiate attack:
    - direct communication
      - network packets exchanged between master & agent
      - need to know each other's IP address
    - indirect communication
      - use some pre-existing legitimate communication channel
      - IRC commonly used
      - discovery of agent may only tell us IRC server & channel
      - channel hopping used to further disguise

Agent Recruitment - vulnerability scanning

- Horizontal
  - Looks for specific port/vulnerability
- Vertical
  - Look for multiple ports/vulnerabilities on the same host
- Coordinated
  - Scan multiple machines on the same subnet for a specific vulnerability
- Stealthy
  - Any of the above, but do it slowly to avoid detection
- Attack code propagation
  - Central server
  - From machine that was used to exploit system

Exploited Weakness

- Semantic (TCP SYN, NAPTHA)
  - Exploits a specific feature or bug of a protocol or application on the victim in order to consume excessive amounts of its resources
  - Can potentially be mitigated by deploying modified protocols/applications
- Brute Force
  - Intermediate network has more resources than victim - can deliver higher volume of packets than victim can handle
  - Overwhelms victim resources using seemingly legitimate packets
    - hard to filter without also harming legitimate traffic
  - Requires higher volume of attack packets
    - modifying protocols to counter semantic attacks raises the bar somewhat for the attacker

Source Address Validity

- Spoofed Address
  - Avoids accountability, helps avoid detection
  - Required for reflector attacks
- Valid Address
  - Some attacks (NAPTHA) require a valid source address, since the attack mechanism requires several request/reply exchanges between agent & victim

Reflector Attacks

- Attacker sends packets to some (non-hostile) intermediate entity
  - spoofed source address of the packets is the victim's IP address
  - response from the intermediate entities overwhelms the victim
- SMURF (1998)
  - ICMP echo requests sent to various IP broadcast addresses
  - amplifier effect: many responses from a single packet
  - Feb. 2000 attack against Yahoo was based on SMURF
- DNS Reflector Flood (2000)
  - agents generate a large number of DNS requests, with the spoofed source address of the victim
  - amplifier effect: DNS responses can be significantly larger than the DNS request

CERT: Advisory CA-1998-01, Incident Note IN-2000-04

Attack Rate Dynamics

- Constant Rate (most)
  - agents send packets as fast as they can after attack is started
  - large traffic stream may aid detection
- Variable Rate
  - used in an attempt to avoid or delay detection
  - Increasing Rate
    - start slow, gradually increase, perhaps over long period of time
    - harder to distinguish from a legitimate increase in traffic
  - Fluctuating Rate
    - could respond to victim behavior or preprogrammed timing
    - could be used to pulse the attack intensity
    - agents could coordinate pulsing, so attack intensity is steady, but set of agents attacking at any one time varies
      - makes it harder to detect & mitigate at the source network of the agent

Possibility of Characterization

- Characterizable
  - Filterable vs. Non-Filterable
    - Filterable:
      - packets may be malformed
      - protocol or application may not be needed by target
        - ex: UDP flood against a web server, http flood against an SMTP server
        - traffic can be filtered by a firewall
    - Non-Filterable:
      - well formed packets that request legitimate/critical services
        - no way to distinguish attack packets from legitimate service requests
        - ex: http flooding a web server

Possibility of Characterization

- Non-characterizable
  - attack packets use variety of protocols/applications
    - may be randomly generated
  - some attacks characterizable in theory, but not in practice

Victim Type

- Specific Application
  - example: send bogus signature packets to an authentication service
    - other services on the host may be unaffected
  - detection difficult
    - attack volume usually small
    - host operates normally except for targeted application
  - may be able to distinguish legit. from attack packets at application level (or maybe not)
    - even if we can, a defense strategy would need to take into account each application we want to protect

Victim Type

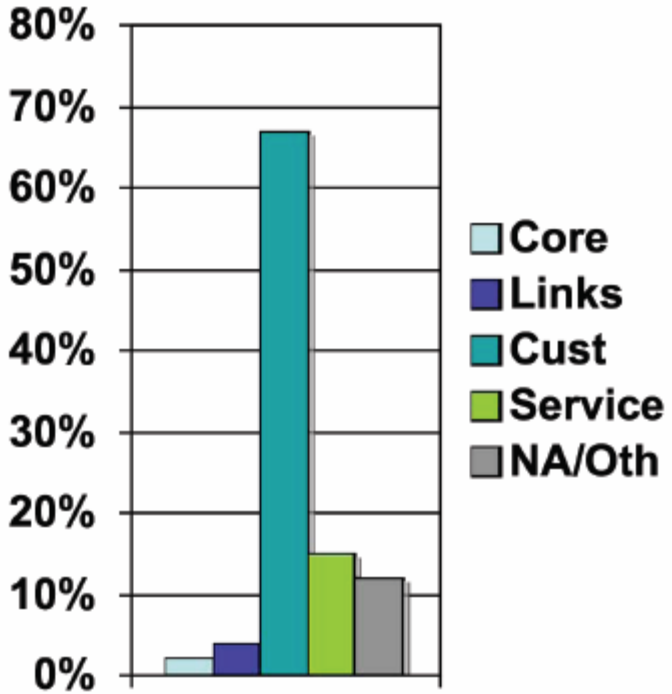
- Host
  - aims to disable all legitimate access to target host
    - overload or disable network communication subsystem
    - otherwise cause host to crash, freeze, or reboot
  - hosts can try to limit their exposure by patching known holes, updating protocols w/DDoS resistant versions
    - however, by themselves cannot defend against attacks that consume all of their network resources
      - need upstream help - i.e., a firewall that can recognize and help filter the attack

Victim Type

- Resource
  - any resource critical to the victim (server, router, bottleneck link)
- Network
  - aims to consume all available incoming bandwidth for target network
    - packet destination can be any host on target network
  - packet volume, not content, is key
  - can be easy to detect due to high traffic volume
  - target network dependant on upstream network for help in defending
    - even if it could detect & filter attack traffic, entire resources of ingress routers may be consumed doing so

Victim Type

- Infrastructure
  - coordinated targeting of distributed services crucial to the global internet
    - attacks on root DNS servers, core routers, etc.
  - from point of view of a single target, may be same as a host-type attack
  - difference in category is due to simultaneous targeting of multiple instances of some critical service
    - coordinated defense may be necessary to counter

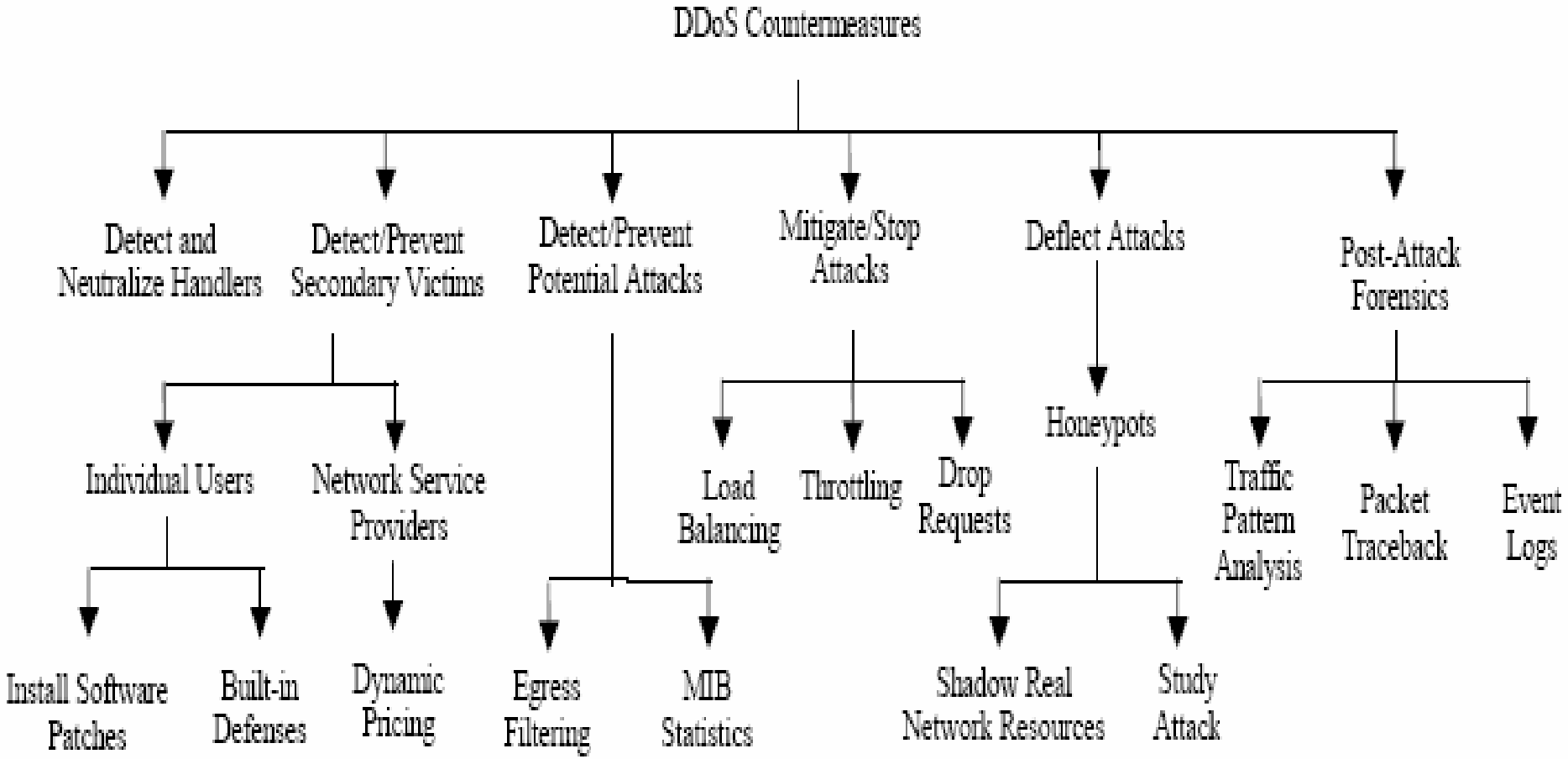


Impact on Victim

- Self-Recoverable
  - after influx of attack packets ends, life returns to normal w/o human intervention
  - a prompt defense (i.e., recognition & filtering) potentially can make these transparent to legit. Clients
- Human-Recoverable
  - after influx of attack packets ends, rebooting or reconfiguration is required
- Non-Recoverable
  - inflict permanent damage to hardware
    - conceivable, but none are known

DDoS countermeasures

- Three categories
  - Preventing the setup of the DDoS attack network, including preventing secondary victims, and detecting and neutralizing handlers.
  - Dealing with a DDoS attack while it is in progress, including detecting or preventing, mitigating or stopping, and deflecting the attack
  - Post-attack category involving network forensics


DDoS Countermeasures
Detect and Neutralize Handlers
Detect/Prevent Secondary Victims
Detect/Prevent Potential Attacks
Mitigate/Stop Attacks
Deflect Attacks
Post-Attack Forensics
Individual Users
Network Service Providers
Load Balancing
Throttling
Drop Requests
Honeypots
Traffic Pattern Analysis
Packet Traceback
Event Logs
Install Software Patches
Built-in Defenses
Dynamic Pricing
Egress Filtering
MIB Statistics
Shadow Real Network Resources
Study Attack

Application security
Spamming, viruses, Trojans, worms, hoaxes....

Spam

- Unsolicited commercial email
- SPAM costs everyone more- in productivity, online fees, bandwidth, etc.
- “Legitimate Spam”
  - Signing up for newsletters, mailing lists, online services opens us to this

Spam

- Spammers can send a piece of e-mail to one, 100, or a distribution list in the millions for roughly the same cost to them.
- Spammers expect only a tiny number of readers will respond to their offer.
- 5 to 7% of email users buy something from a spam message
- Often motive is just to confirm email address

Email address source

- Email lists -- Buying, stealing, renting, trading
- Trickery – e-greeting cards, freeware, and anything else that asks you to enter your email address
- Spambots, Harvesters – search the Internet for email addresses on forums, web pages, newsgroups, blogs, etc.
- Dictionary attacks – sends out emails to guessed/random addresses
- Blanket attacks – “send this to anyone@nmsworks.co.in”

Virus, Trojans, Worms...

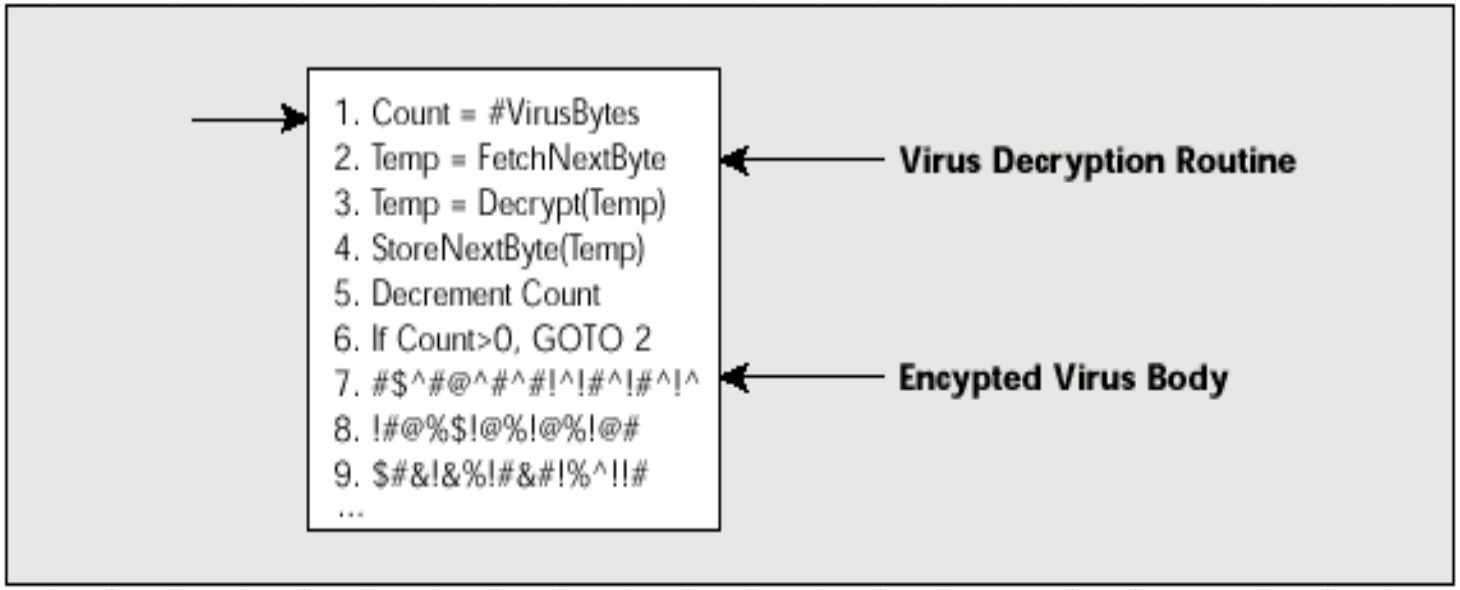
- Virus: Malicious software that causes damage when executed
- Trojan: Malicious code contained in apparently harmless code
- Worm: Self propagating malicious code
- Phishing: Fake but authentic looking messages/websites to trick users into giving up personal information

Simple Viruses

- Replicates itself and is easiest to detect
- Always makes exact replica of itself
- Detection: Scan for a sequence of bytes found in the virus

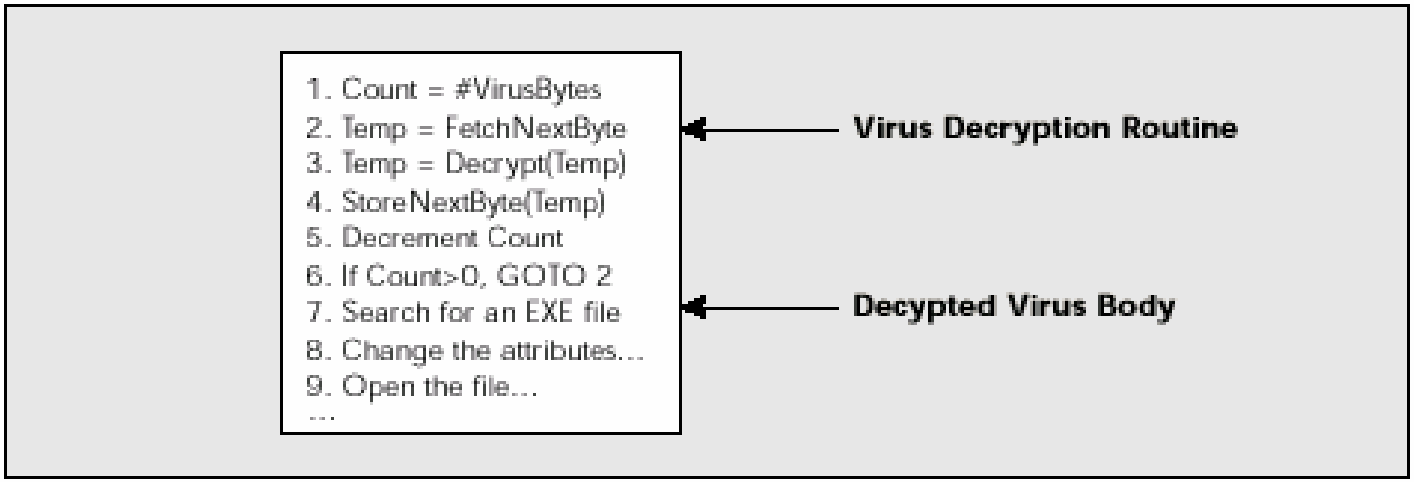
Response

- Encrypting the virus
  - Hide the fixed bytes by encrypting the virus



Detecting encrypted virus

- Decryption remained constant, thus detection was a sequence of bytes of the decryption routine



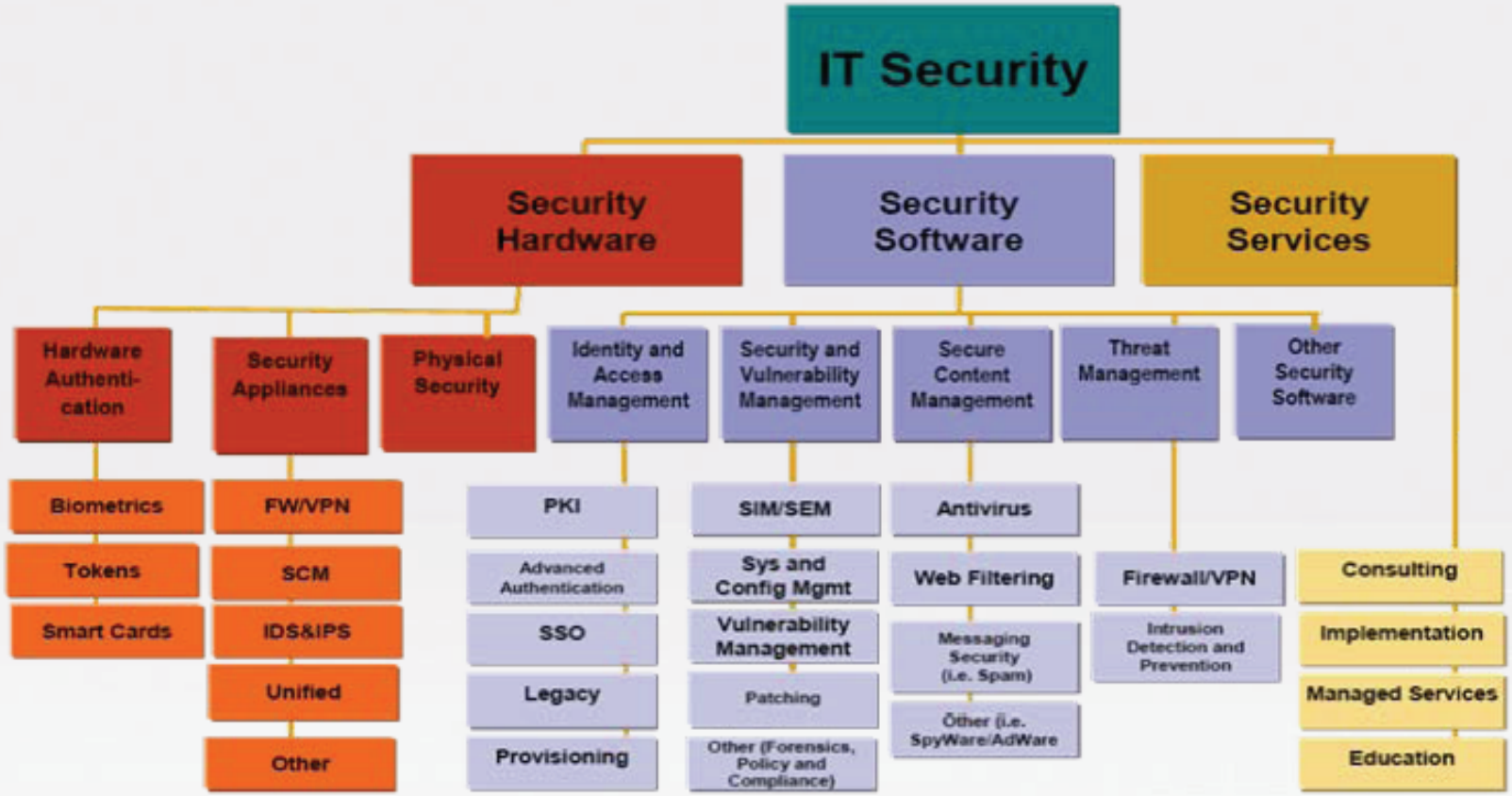
Polymorphism

- Adds a mutation engine that generates randomized decryption routines with each use
- No fixed signature!

Phishing, Phaxing, Vishing ...

- Phishing: Fake but authentic looking messages/websites to trick users into giving up personal information
- Phaxing: fax phishing
- Vishing: use VoIP to build bogus switchboard systems, mimicking thoseof genuine online banks and other organizations

- 3 Parts : Security Hardware, Security Software, Security Services



Acronym Key :
- SCM : Security Contents Monitoring
- SSO : Web & Host Single Sign-On
- SIM/SEM : Security Information Management / Security Event Management
- Unified : Unified threats management appliances
- Managed Services : Managed Security Services

Summary

- Awareness of information security is crucial
- Security has to be achieved at service level, network level, end-point or host level
- Use a combination of technology, processes and people

Thank you!