

Computer Security: Attacks and Threats



Human Factors and Malicious Software

What we know



- Attacks can be
 - Intentional\Unintentional
 - Insider\Outsider
 - Passive\Active
- Attacks exploits vulnerabilities, and tries to evade (or go around) policies.
- Attacks may results in lost of
 - Confidentiality
 - Integrity
 - Availability
- You will need appropriate countermeasures

Ponder this for a minute

- What is computer security?

Computer security is the security of any automated information system— preserving CIA on the resources

- What is the biggest threat to computer security?

Human

Computer Security: Attacks and Threats



Human Factors

The Human Factor



- Human comes in many different behaviour and emotional frame.
- Computer security violations usually relates to
 - error or misuse of human apart
 - malicious activities by the human itself.
- Security violations from:
 - Outsiders
 - Insiders

The Human Factor



Outsiders

- Prompted by
 - money, fame, emotion (anger, hate, jealousy, etc)
- Countermeasures
 - security services and applications (firewalls, IDS, awareness, etc)

Insiders

- Prompted by
 - money, emotion (anger, dissatisfaction, etc)
- Countermeasures
 - security and management services (access control, awareness, hiring policies, etc)

Human Factors: Minimizing impact



- This is an important and broad area.
- Minimizing impact can be done through
 - **Understanding** - Security awareness, training, and education
 - **Control** – Policies
 - ✦ Organizational security policy
 - ✦ Hiring or Personnel security policy
 - ✦ Usage (e.g. E-mail and Internet usage) policy

Security Awareness, Training, and Education



- Prominent topic in various standards (*check out ISO, NIST etc*)
- Provides benefits in:
 - Improving employee behavior
 - Increasing the ability to hold employees accountable for their actions
 - Mitigating liability of organization for employee behavior
 - Complying with regulations and contractual obligations

Benefits of SA-T-E

⤴ Better employees
means ⤵ of errors,
fraud, bad actions

Knowing of accountability and
penalties – will deter employees
from doing bad things

improving
employee
behavior

increasing the
ability to hold
employees
accountable for
their actions

Mitigating liability
of organization for
employee behavior

complying with
regulations and
contractual
obligations

Due care is taken – we
cannot be held responsible
for what they did

It's the law.

Awareness



- Seeks to inform and focus an employee's attention on security issues related to security within the organization
 - To recognize - threats, vulnerabilities, impacts, responsibility
- Must be tailored to organization's needs
- Must use a variety of means
 - events, promo materials, briefings, employee policy document

Training



- Seeks to teach the skills to perform IS-related task more securely.
 - Knowing WHAT to do and HOW to do it
- Tailored to the role of the user:
 - General users : good computer security practices
 - Programmers, developers, maintainers : security mindset, secure code development
 - Managers: making tradeoffs involving security risks, costs, benefits
 - Executives : risk management goals, measurement, leadership

Education



- Most in depth
- Targeted at security professionals whose jobs require expertise in security
- Fitted more to employee career development
- Often provided by outside sources
 - college courses
 - specialized training programs

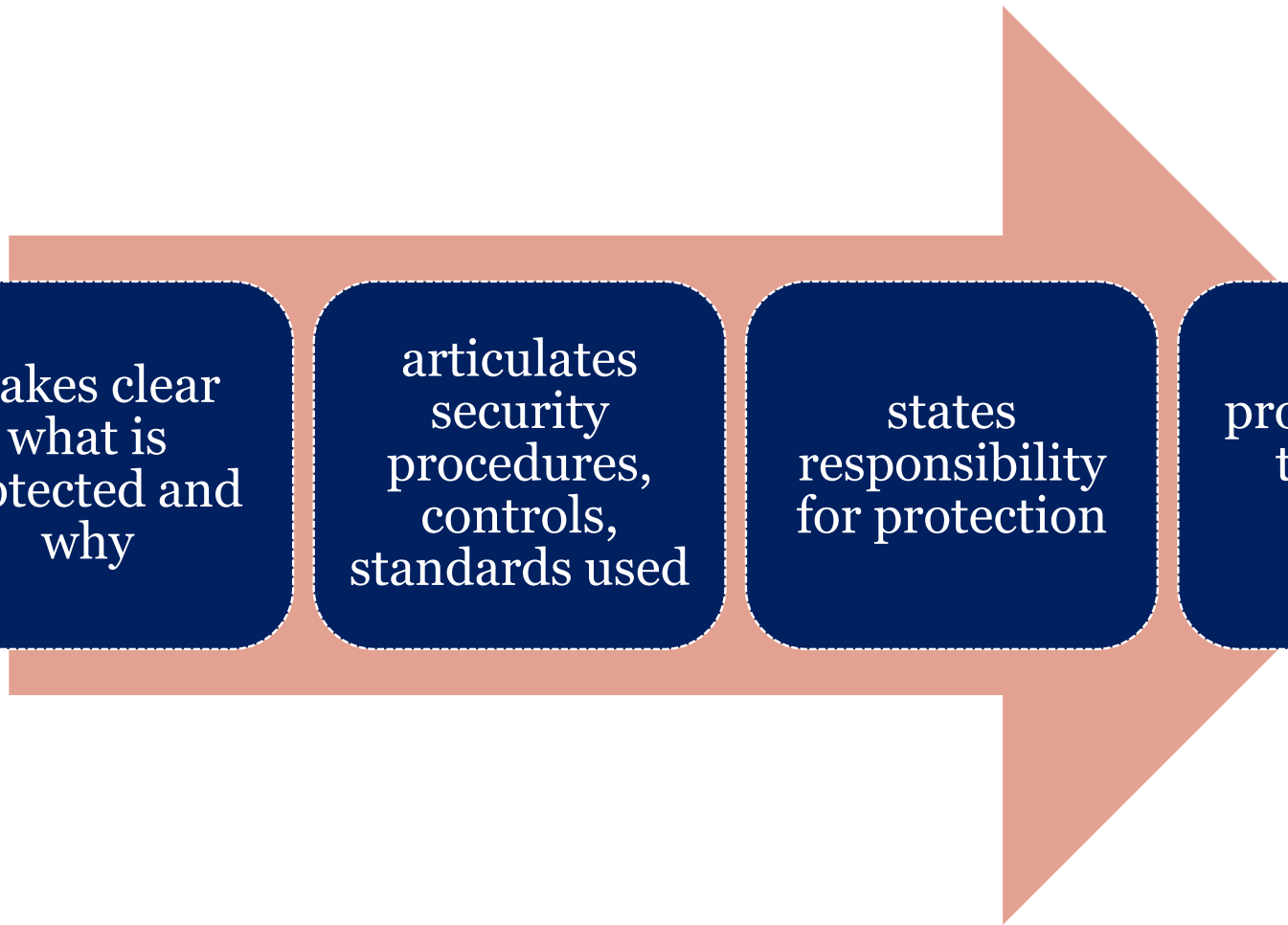
	Awareness	Training	Education
Attribute	What	How	Why
Level	Information	Knowledge	Insight
Objective	Recognition	Skill	Understanding
Method	<ul style="list-style-type: none"> •Videos •Newsletter •Posters, etc 	<ul style="list-style-type: none"> •Lecture •Workshops •Hands-on practice 	<ul style="list-style-type: none"> •Seminar •Background reading
Impact timeframe	Short term	Intermediate	Long term

Organizational Security Policy



- “Formal statement of rules by which people given access to organization's technology and information assets must abide”
- A written security policy document is fundamental.
- It must reflect security decisions made by executive management

Roles of a Security Policy



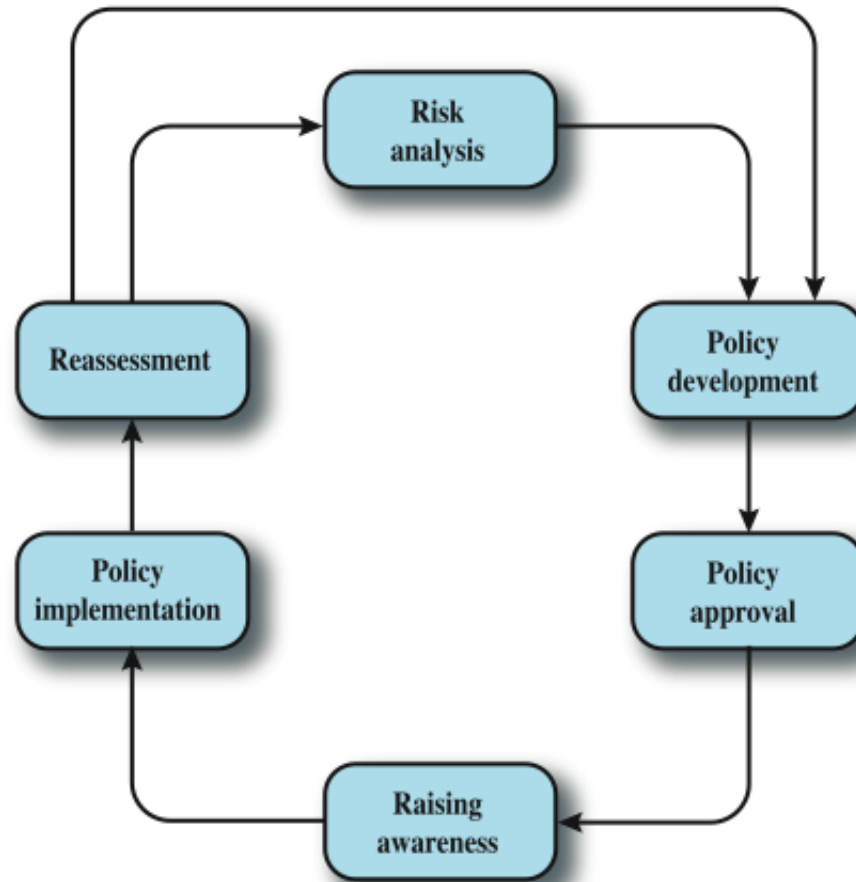
makes clear
what is
protected and
why

articulates
security
procedures,
controls,
standards used

states
responsibility
for protection

provides basis
to resolve
conflicts

Security Policy Lifecycle



Policy Document Responsibility



- Security policy needs broad support
- Support from top management is essential
- The “policy development team” should include:
 - site security administrator, IT technical staff, user groups admins, security incident response team, user groups representatives, responsible management, legal counsel

Document Content



- what is the reason for the policy?
- who developed the policy?
- who approved the policy?
- whose authority sustains the policy?
- which laws / regulations is it based on?
- who will enforce the policy?
- how will the policy be enforced?
- whom does the policy affect?
- what information assets must be protected?
- what are users actually required to do?
- how should security breaches be reported?
- what is the effective date / expiration date of it?

Policy Example: Hiring or Personnel Security



- Handles hiring, training, monitoring behavior, and departure
- Employees may involve in security violations:
 - unwittingly aiding commission of violation
 - knowingly violating controls or procedures
- threats include:
 - gaining unauthorized access, altering data, deleting production and back up data, crashing systems, destroying systems, misusing systems , holding data hostage, stealing strategic or customer data for corporate espionage or fraud schemes

Policy Example: Hiring or Personnel Security



- **Hiring process:**
 - Background checks and screening
 - Employment contracts and agreement – employees must agree to sign
- **During employment:**
 - Security and policy - awareness and training
 - Least privilege
 - Separation of duties
 - Limited reliance on key employees
- **Termination:**
 - Return all access and authorization elements – e.g. cards, keys
 - Remove personal access codes
 - Change locks, keys, passwords, key combinations where necessary

Policy Example: Email & Internet Use Policies



- Increasingly, E-mail & Internet access for employees is common in some organizations (e.g. offices and some factories)
- Employed due to concerns regarding
 - Lost of work time doing non-work activities
 - Consuming computer and communications resources
 - Risk of importing malware
 - Possible liability to company - possibility of harm, harassment, bad conduct
 - Risk of industrial espionage
- Policy includes: business use only, reasonable personal use, prohibition of unlawful activities, etc.

Summary



- introduced some important topics relating to human factors
- security awareness, training & education
- policies

Class Exercise



- Write a security policy (mind map style) for the following:
 - Cyber café
 - Faculty computer lab
 - Faculty academic management centre
 - Apple Computer research Lab
 - Pharmaceutical company research lab

Computer Security: Attacks and Threats



Malicious Software

Malicious Software (Malware)



- Malwares are programs exploiting system vulnerabilities
- There many different types of malware
 - refer Table 7.1 - William Stallings .“Computer Security Principles and Practice”
- Malwares do a lot of harm
- It can get into action straight away or lay dormant for a while until triggered by something
 - Time/date
 - Event
 - Conditions
 - Count
 - Combination of these
- Malwares are old veterans with newer, nastier sidekicks in the new age.
- The newer Malwares are copies of the old with distinct instances and better ‘zing’!

Malware division

- Malware can be divided into 2 categories:

- program fragments that need a host program
 - ✦ e.g. viruses, logic bombs, and backdoors
- independent self-contained programs
 - ✦ e.g. worms, bots

- Malware can also be differentiated between:

- Programs that do not replicate themselves
 - ✦ e.g. bots, logic bombs, and backdoors
- Programs that replicate themselves
 - ✦ e.g. worms, virus

Malware Terminology



- Virus
- Worm
- Logic bomb
- Trojan horse
- Backdoor (trapdoor)
- Mobile code
- Auto-rooter Kit (virus generator)
- Spammer and Flooder programs
- Keyloggers
- Rootkit
- Zombie, bot

Caution:
This list is NOT
exhaustive.
Please explore for
more.

Backdoor (a.k.a Trapdoor)



- Secret entry point into a program
- Allows someone to gain access of the program without going through access control procedures
- Started out for testing and debugging purposes (a **maintenance hook**)
- Continued on by unethical programmers to do bad things.

Viruses



- A piece of software that infects other programs
 - modifying them to include a copy of the virus
 - so it executes secretly when host program is run
- specific to operating system and hardware
 - taking advantage of their details and weaknesses
- a typical virus goes through phases of:
 - dormant
 - propagation
 - triggering
 - execution

Viruses



- **Dormant phase:**
 - The virus is idle, waits for a trigger to be activated
 - Triggers can be some event - such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit.
 - Not all viruses have this stage.
- **Propagation phase:**
 - The virus places a copy of itself into other programs or into certain system areas on the disk.
 - Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.

Viruses



- **Triggering phase:**
 - The virus is activated to perform the function for which it was intended.
 - As with the dormant phase, the triggering phase can be caused by a variety of system events, including a count of the number of times that this copy of the virus has made copies of itself.
- **Execution phase:**
 - The function is performed, which may be harmless (e.g. a message on the screen), or damaging (e.g. the destruction of programs and data files).

Virus Structure



- Has 3 components:
 - infection mechanism - enables replication
 - trigger - event that makes payload activate
 - payload - what it does, malicious or benign
- Can be either prepended / postpended / embedded
- Viral infection can be completely prevented by preventing virus from gaining entry – easier said than done!
 - Virus can be part of ANY program
 - Re-used codes
 - Creativity of virus creators – e.g. different platforms, compression virus

Virus Classification

encrypted virus – a portion of the virus creates a random key, and encrypts the other portion. When it replicates, it changes the key.

By concealment strategy

By target

Macro virus

Encrypted virus

Stealth virus

stealth virus – the entire virus is hidden from antivirus software detection

File infector

Polymorphic virus

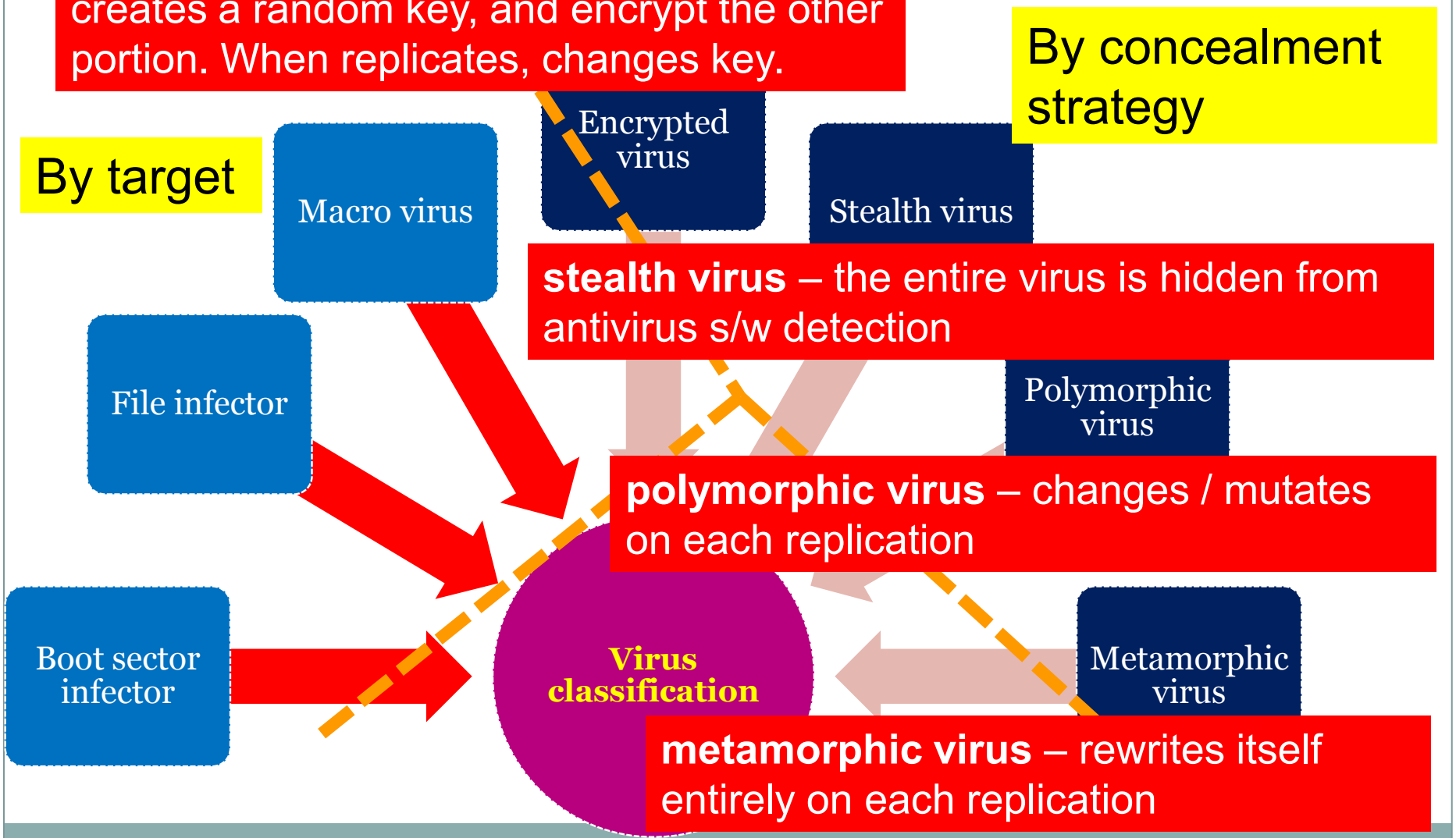
polymorphic virus – changes / mutates on each replication

Boot sector infector

Virus classification

Metamorphic virus

metamorphic virus – rewrites itself entirely on each replication



Macro Virus



- became very common in mid-1990s since
 - platform independent
 - infect documents
 - easily spread
- exploit macro capability of office apps
 - executable program embedded in office doc
 - often a form of Basic
- more recent releases include protection
- recognized by many anti-virus programs

E-Mail Viruses



- more recent development
- e.g. Melissa
 - exploits MS Word macro in attached doc
 - if attachment opened, macro activates
 - sends email to all on users address list
 - and does local damage
- then saw virus versions that triggered by only reading email
- hence much faster propagation

Virus Countermeasures



- Prevention - ideal solution but difficult
- Realistically need:
 - Detection
 - Identification
 - Removal
- If detected but can't identify or remove, must discard and replace infected program

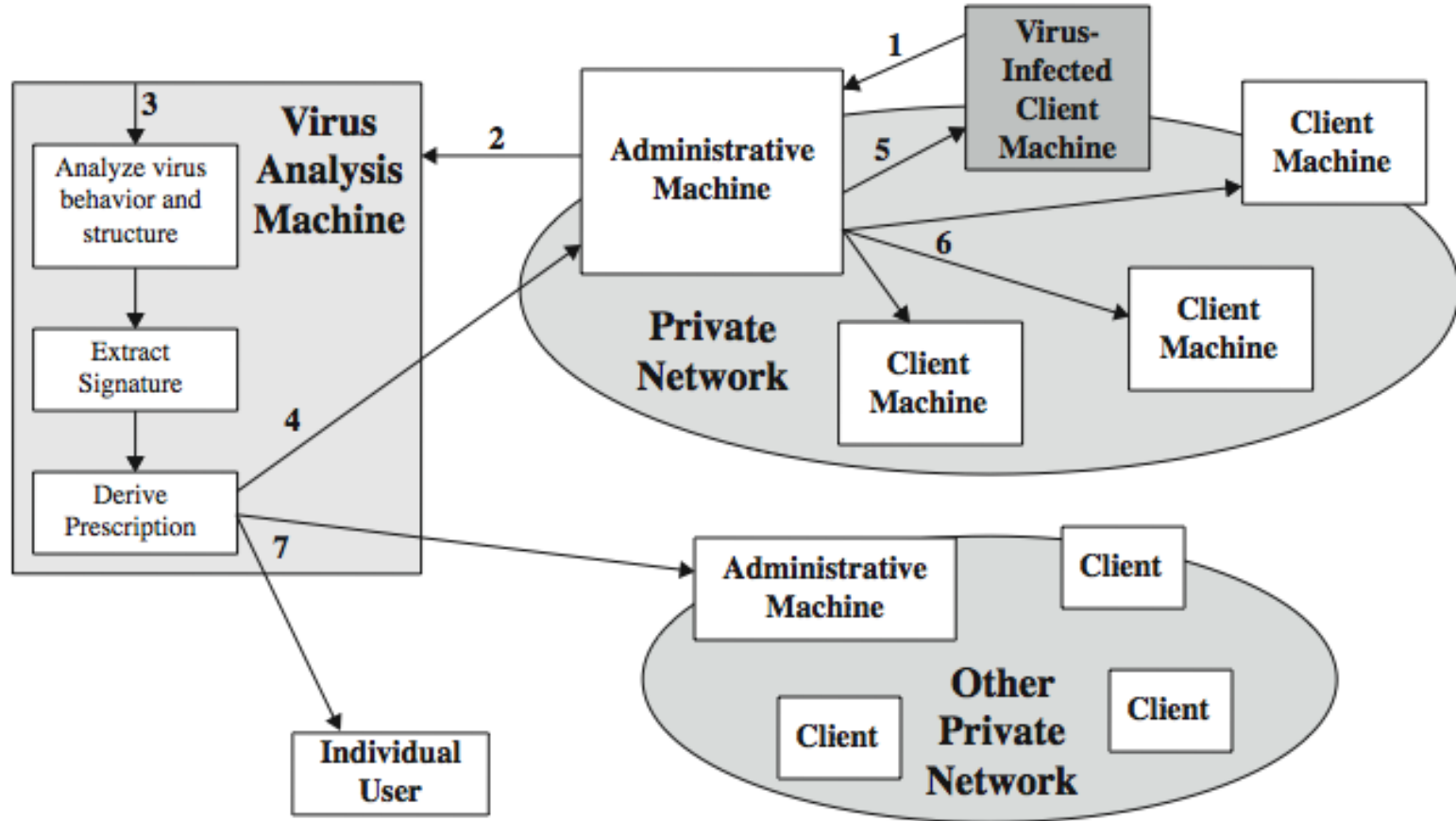
Anti-Virus Evolution



- Virus & antivirus tech have both evolved
- Early viruses simple code, easily removed
- As viruses become more complex, so must the countermeasures
- Generation of anti-virus software
 - First - signature scanners (viruses may look different but have same structure)
 - Second – heuristics (look for virus code fragments or checksums)
 - Third - identify by actions (not signature or heuristics)
 - Fourth - combination packages

Antivirus Architecture

Prototype of digital immune system by IBM
Objective: rapid response time



Worms



- A self-replicating program that propagates over the net
- To travel (propagate), the worm uses
 - email, remote execution capability, remote login
- It has phases like a virus:
 - dormant, propagation, triggering, execution
 - propagation phase: searches for other systems, connects to it, copies self to it and runs
- It may disguise itself as a system process

Worms



- The most significant difference between virus and worm is ...
 - The way they propagates
 - How do worm propagate?
 - What about virus?

Morris Worm



- One of best known worms
- Released by Robert Morris in 1988
- Tries these methods to gain access to UNIX systems
 - cracking password file to use login/password to logon to other systems
 - exploiting a bug in UNIX finger protocol
 - exploiting a trapdoor on a debug option of the remote process that get and sends mail
- If succeed have remote shell access
 - sent bootstrap program over to OS, OS run bootstrap, new worm executed

Recent Worm Attacks



- Code Red
 - July 2001 exploiting MS IIS bug
 - probes random IP address, does DDoS attack
 - consumes significant net capacity when active
- Code Red II variant includes backdoor
- SQL Slammer
 - early 2003, attacks MS SQL Server
 - compact and very rapid spread
- Mydoom
 - mass-mailing e-mail worm that appeared in 2004
 - installed remote access backdoor in infected systems

State of the Art Worm Technology

Polymorphic - Each copy of **ultrafast** worm has new code generated advanced to evade detection propagations

Ultrafast

Polymorphic

Metamorphic

multiexploit - Penetrates in a variety of ways – email, web server file sharing, etc.

Multiexploit

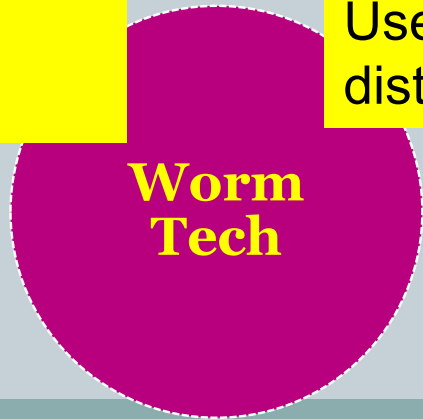
Metamorphic - Changes of behavior patterns at different stages of propagation detection evade

Zero-day exploit – exploit unknown vulnerability when launched distributed attack tools

Transp
Used for
distributed attack tools

Multiplatform - Evolved from platform-dependent to multiplatform

Multiplatform



Zero-day exploit

State of the Art Worm Technology



- Multiplatform - Evolved from platform-dependent to multiplatform
- Multiexploit - Penetrates in a variety of ways – email, web server, file sharing, etc.
- ultrafast spreading -Internet advancements accelerates worm propagations
- Polymorphic - Each copy of worm has new code generated to evade detection
- Metamorphic - Changes of behavior patterns at different stages of propagation to make detection even harder
- Transport vehicles – Used for spreading distributed attack tools
- Zero-day exploit – exploit unknown vulnerability when launched

Worm Countermeasures



- Considerable overlap with anti-virus techniques
- Once worm on a system, antivirus s/w can detect
- Monitoring network activity and usage can help too
 - because worm propagation generates a lot of network activity

Worm Countermeasures



- Worm defense approaches include:
 - Signature-based worm scan filtering
 - ✦ Use signature to block worm scan from entering the network
 - Filter-based worm containment
 - ✦ Focus on the content rather than the scan signature
 - Payload-classification-based worm containment
 - ✦ Examine packet to see if it contains worm using anomaly based detection
 - Rate limiting and rate halting
 - ✦ Limit the rate or block the traffic of infected network/machine

Bots (a.k.a Zombie or Drone)



- A program that secretly takes over another networked computer and then use it to launch attacks
- Difficult to trace attacks back to creator
- A collection of bots acting in a coordinated form is called a botnet.
- Botnets characteristics:
 - The bot functionality – what it is used for
 - remote control facility – has a control module via IRC/HTTP etc
 - spreading mechanism - attack software, identify/scan and exploit vulnerability
- Countermeasures – primary objective is to try to detect and disable botnet during construction

Rootkits



- Set of programs installed for admin access
- Alters host's standard functionality maliciously and secretly
- May hide its existence by changing some aspects of the system
 - Manipulates the processes, files, registry monitoring and reporting mechanisms (cant find it in registry)
- Can be classified as:
 - persistent or memory-based or user mode or kernel mode
- May be installed by user via Trojan horse or via hacker activity
- Countermeasures – very difficult and different range is needed
 - IDS can check known rootkit codes on incoming traffic
 - File integrity check
 - Install all new OS if kernel-level rootkit detected

Summary



- Introduced some important topics relating to human factors
- Security awareness, training & education
- Policies
- Introduced types of malicious software
- Virus types and countermeasures
- Worm types and countermeasures
- Bots and rootkits

<https://www.mandiant.com/threat-landscape/anatomy-of-an-attack/>

<http://www.symantec.com/connect/blogs/francophonied-sophisticated-social-engineering-attack>

Assignment 3



Title: Malware encyclopedia.

Marks %: 5