Intrusion Detection and Malware Analysis

Introduction to Malware

Pavel Laskov
Wilhelm Schickard Institute for Computer Science
The term malicious software denotes program code executed without a user’s consent and carrying out harmful functionality.
The term **malicious software** denotes program code executed without a user’s consent and carrying out harmful functionality.

*Why is malware such a serious problem?*
Malware: definitions and root causes

The term malicious software denotes program code executed without a user’s consent and carrying out harmful functionality.

Why is malware such a serious problem?

Technical reasons:
- Difficulty to separate code and data
- Homogeneity of “computing base” (Windows, iPhone, Facebook)
- Unprecedented connectivity
Malware: definitions and root causes

The term malicious software denotes program code executed without a user’s consent and carrying out harmful functionality.

Why is malware such a serious problem?

Technical reasons:
- Difficulty to separate code and data
- Homogeneity of “computing base” (Windows, iPhone, Facebook)
- Unprecedented connectivity

Non-technical reasons:
- Recklessness and ignorance of users
- Profitability of security violations (spam, DoS extortion, stealing of personal information)
An example from last semester

You have just received a virtual postcard from a friend!

From: "received@postcard.org" <received@postcard.org>
To: taskov@first.fhg.de
Date: Yesterday 16:27:23

You have just received a virtual postcard from a friend!

You can pick up your postcard at the following web address:

Click here to pick up your postcard

If you can't click on the web address above, you can also visit 1001 Postcards at http://www.postcards.org/postcards/ and enter your pickup code, which is: d21-sea-sunset

(Your postcard will be available for 60 days.)
An example from last semester

You can pick up your postcard at the following web address:

Click here to pick up your postcard

If you can't click on the web address above, you can also:

Visit 1001 Postcards at http://www.postcards.org/postcards/ and enter your pickup code, which is: d21-sea-sunset

(Your postcard will be available for 60 days.)

Oh -- and if you'd like to reply with a postcard,

you can do so by visiting this web address:

http://www2.postcards.org

(Or you can simply click the "reply to this postcard" button beneath your postcard!)
“Theoretical foundations” of malware

- Von Neumann’s model (1948, 1953)
  - universal machine
  - universal constructor
  - information on the tape
- Darwin/Core Wars: fighting programs (1966)
  - a special assembly language with 10 instructions (“Redcode”)  
  - two programs simultaneously running in the same memory  
  - a program dies if it executes division by 0 or a null instruction  
  - to increase their survival chances, programs can replicate themselves
  - definition of a virus
  - mathematical description of virus propagation
Elk Cloner (1982)
- an Apple-II program written by a student Rich Skrenta
- a program spread via boot sector infection
- on every 50-th reset a short poem was displayed by hooking the reset handler

Brain Virus (1986)
- first virus to spread in the wild
- written by Ashar brothers to prevent illegal copying of software
- included in a boot sector of distributed software diskettes

Morris worm (1988)
- used a debugging feature of sendmail (remote execution)
- propagated in the Arpanet
- penetrated ca. 6,000 computers (10% of Arpanet)
First generation of malware

**Definition**

A virus is a program that infects other programs by modifying them to include a possibly modified copy of itself.

- **Boot sector viruses**
  - stored in disk boot sectors, executed automatically at boot
- **Executable viruses**
  - stored in executable data, hijack flow control
- **Macro viruses**
  - stored in non-executable data, started by opening a document
Definition

A **worm** is a program that actively propagates over computer networks, with or without human interaction.

- **Mass-mailers** (e.g. Melissa, LoveLetter, Nimda)
  - use SMTP protocol for propagation
  - usually (but not necessarily) require manual interaction
- **In-memory worms** (e.g. Slammer, CodeRed)
  - proliferation over TCP/HTTP
  - automatic execution on vulnerable systems (very fast!)
Definition

A trojan horse is a program carrying a hidden functionality behind a seemingly useful one.

- focus on stealthy operation
- anti-detection mechanisms (obfuscation, encryption and polymorphism)
- combination of various malware types and techniques
- increasing commercialization
Further malware types (1)

- **Backdoor**: remote access to compromised computers (especially used in botnets)
- **Downloader**: installation of malicious content (used to overcome filtering of executables and update of already installed malware)
- **Rootkit**: modification of system behavior, either at a user level (e.g. user settings) or a root level (e.g. system tools or registry entries)
- **Dialer**: calling premium services, re-surfacing in mobile malware
Further malware types (2)

- **Spyware**: monitoring of user behavior (e.g. during web browsing)
- **Adware**: unsolicited presentation of advertisement
- **Keylogger**: capturing of keystrokes, especially for typed in passwords or financial credentials
- **Sniffer**: capturing of network traffic, especially for passwords send in clear text
- Save the original MBR in a safe location
- Overwrite the MBR with an infected one
- Bootstrap a system using the new MBR
Malware carriers: COM executables

- Append a virus body to a program
- Save an entry point to a program in a virus body
- Replace a program entry point with a jump to a virus body
- Virus code restores the original entry point and jumps to it after its own execution
Malware carriers: EXE executables

- Append a virus body to a program
- Overwrite a program header to switch the entry point to a virus
- Jump to the original entry point during execution
Malware carriers: PE executables

- Virus is split into parts that are parcelled together by a defragmentation routine.
- Defragmentation routine is inserted between the PE header and the first section.
- Entry point in the PE header is switched to the defragmentation routine.
- Additional viral sections are stored in unused parts of sections.
Malware carriers: companion viruses

- MS-DOS feature: if a command is typed without an extension, first a .COM file is searched for and then an .EXE
Malware carriers: companion viruses

- MS-DOS feature: if a command is typed without an extension, first a .COM file is searched for and then an .EXE
- **Exploitation**: Inject a malicious program `<program>.COM` which calls `<program.EXE>` besides doing its dirty job.
Malware carriers: companion viruses

- MS-DOS feature: if a command is typed without an extension, first a .COM file is searched for and then an .EXE.

- Exploitation: Inject a malicious program `<program>.COM` which calls `<program.EXE>` besides doing its dirty job.

- Variations on a theme:
  - Renaming legitimate files
  - Placing a new earlier in the search path
Malware carriers: macros

- Malicious functionality is implemented in Visual Basic for Applications (VBA).
- If a document template are infected, so will be every document on a system.
Malware carriers: Visual Basic (VB) script

- Similar functionality to macro viruses implemented in “pure” VB.
- A script is executed by a user by clicking at the email attachment (LoveLetter mass-mailer).
- Why does the user execute a VB script? The attachment name LOVE-LETTER-FOR-YOU.TXT.vbs is shown in Outlook as LOVE-LETTER-FOR-YOU.TXT (without extension!).
- Further functionality is possible via access to ActiveX objects.
Malware carriers: SuperLogo

- A set of “turtle-control” commands is provided in the Logo language (e.g. HIDETURTLE, FORWARD, PENUP, PENDOWN, WAIT).
- Sets of commands can be saved in LGP file.
- A command PRINTTO “XYZ” can be used to write directly to files (with a complete path to a file).
Malware carriers: SuperLogo

- A set of “turtle-control” commands is provided in the Logo language (e.g. HIDETURTLE, FORWARD, PENUP, PENDOWN, WAIT).
- Sets of commands can be saved in LGP file.
- A command PRINTTO “XYZ” can be used to write directly to files (with a complete path to a file).
- Overwrite winstart.bat with any functionality and it will be run!
Malware carriers: JavaScript

- Similar functionality to VB scripts:
  - Read, write and overwrite files
  - Access to ActiveX communication objects: send emails
  - ...

- Automatic invocation during web browsing: infection is possible via opening of malicious web pages.
Malware carriers: other script languages

- Potential carriers: shell scripts, PHP, Perl, Python, Emacs, Tcl, VIM
- Infection strategies:
  - file overwriting
  - “exec” functionality
Covering the tracks

- Erasing data
- Manipulation of registry entries
- Changing time stamps
- Changing checksums
- Memory-resident operation
- API hooking
- ...

...
A run-time executable packer is a program for compressing a program code and data.

Primary goal: reduction of the program size

Side effect: signature detection is heavily impeded!

Main idea:

- Compress the original executable program and store it in a data segment
- Put a decompression routine in some program segment.
- Decompression routine unpacks malicious code into memory and transfers control to it.

Further development: compression can be implemented using cryptographic primitives of varying strength.
Oligomorphism: a set of decryptors is carried along; a new decryptor is chosen at random for each new replication.

Polymorphism: insert junk or semantically equivalent code into a decryptor to increase its variability.

Metamorphism: instead of decryption, the malware body is mutated during each replication using equivalent program transformations.
The key challenge in fighting malware is its rapid evolution due to an underlying monetary interest.

The main technical cause of malware is poor separation between code and data.

Malware exemplifies a fundamental tradeoff between security and usability: advanced programming language features facilitate operation of malware.
John Aycock.  
*Computer Viruses and Malware.*  

Peter Szor.  
*The art of computer virus research and defense.*  