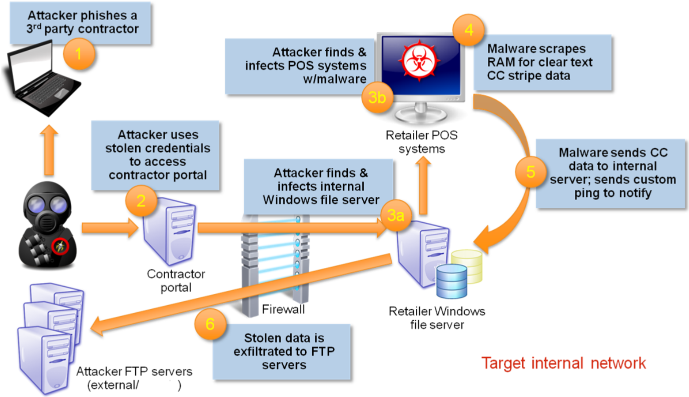
Overview

CS 363 Computer Security

Cyber-attack is complicated

Anatomy of the Target Retailer Breach



1 Attacker phishes a 3rd party contractor

2 Attacker uses stolen credentials to access contractor portal

3a Attacker finds & infects internal Windows file server

3b Attacker finds & infects POS systems w/malware

4 Malware scrapes RAM for clear text CC stripe data

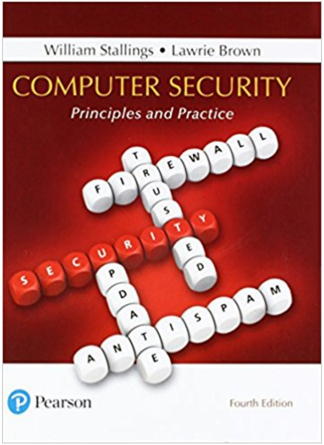
5 Malware sends CC data to internal server; sends custom ping to notify

6 Stolen data is exfiltrated to FTP servers

Computer Security

- Goal: to provide an up-to-date survey of developments in cyber-security through study of the theoretical foundation and hands-on practical implementation.
- Topics: basic security technology, cryptography, security management, risk assessment, operations and physical security, software and network security, as well as ethical and legal issues.

Textbook



William Stallings • Lawrie Brown

COMPUTER SECURITY

Principles and Practice

Pearson

Fourth Edition

Policy

- Material dissemination
  - Project assignments and lecture notes on Canvas
- Grade
  - 5% - one individual presentation
  - 75% - five individual projects
  - 20% - final exam
- Etown college's code of student conduct strictly enforced

Computer Security

"The protection afforded to an automated information system in order to attain the applicable objectives of preserving the Confidentiality, Integrity, and Availability of information system resources"

- NIST computer Security Handbook

Key Security Concepts

Confidentiality

- preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Key Security Concepts

Integrity

- guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity

Key Security Concepts

Availability

- ensuring timely and reliable access to and use of information

Practice: CIA?

- Hardware: Equipment is stolen or disabled, thus denying service?
- Software: Programs are deleted, denying access to users?An unauthorized copy of software is made?A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task?

Practice: CIA?

- Data: Files are deleted, denying access to users? An unauthorized read of data is performed. An analysis of statistical data reveals underlying data? Existing files are modified or new files are fabricated?
- Communication Lines: Messages are destroyed or deleted? Communication lines or networks are rendered unavailable? Messages are read? The traffic pattern of messages is observed? Messages are modified, delayed, reordered, or duplicated? False messages are fabricated?

Vulnerabilities

- categories of vulnerabilities
  - corrupted (loss of integrity)
  - leaky (loss of confidentiality)
  - unavailable or very slow (loss of availability)

Threats

- capable of exploiting vulnerabilities
- represent potential security harm to an asset

Attacks

- passive - does not affect system resources
- active - attempt to alter system resources or affect their operation
- insider - initiated by an entity inside the security perimeter
- outsider - initiated from outside the perimeter

Examples - Passive attacks

- Passive attacks attempt to learn or make use of information from the system but does not affect system resources
  - eavesdropping/monitoring transmissions
  - difficult to detect
  - emphasis is on prevention rather than detection
  - two types:
    - release of message contents (ex. WikiLeaks)
    - traffic analysis

Examples - Active attacks

- Active attacks involve modification of the data stream
    - Goal: recovery and deterrence
    - four categories:
        - masquerade
        - replay
        - modification of messages
        - denial of service

Categorization of countermeasures

- functional areas that primarily require computer security technical measures include:
  - access control
  - identification & authentication
  - system & communication protection
  - system & information integrity

Categorization of countermeasures

- functional areas that primarily require management controls and procedures include:
  - awareness & training
  - audit & accountability
  - certification, accreditation, & security assessments
  - contingency planning; maintenance
  - physical & environmental protection
  - personnel security
  - risk assessment
  - systems & services acquisition

Categorization of countermeasures

- functional areas that overlap computer security technical measures and management controls include:
  - configuration management
  - media protection

Practice

Consider the following general code for allowing access to a resource:

```
DWORD dwRet = IsAccessAllowed(...);
if (dwRet == ERROR_ACESS_DENIED){
   // Security check failed
   // Inform user that access is denied.
 }
else
{
   // Security check OK.
}
```

- Explain the security flaw in this program.
- Rewrite the code to avoid the flaw.

Discussion

Security news of 2017?

- WannaCry?
- Wikileaks CIA Vault 7?
- Cloudbleed?
- 198 million voter records exposed?

Next ...

- Legal and Ethical Aspects