CS 1550 – Chapter 9

Security

Jonathan Misurda
jmisurda@cs.pitt.edu

Threats

<table>
<thead>
<tr>
<th>Goal</th>
<th>Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data confidentiality</td>
<td>Exposure of data</td>
</tr>
<tr>
<td>Data integrity</td>
<td>Tampering with data</td>
</tr>
<tr>
<td>System availability</td>
<td>Denial of service</td>
</tr>
</tbody>
</table>

Intruders

- Casual prying by non-technical users
- Snooping by insiders
- Determined attempt to make money
- Commercial or military espionage

Accidents

*Just because the act wasn’t malicious doesn’t mean we don’t need to protect against it*

Encryption

- **E** (Encryption)
- **D** (Decryption)
- **C** (Ciphertext)
- **P** (Plaintext)

**Secret Key Encryption**

Monoalphabetic Substitution

| FNO UQABON GI FNO ISSWO ONKNOX FNO HIVFQK BIYHDHST FJ FEBTIZNH |
| XHKEQIZ DWU ZEKH BT ZYVD FJ B IBOQF. |
| WNBGI ZDFTTF |

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Symmetric Keys

- Data Encryption Standard (DES)
  - 56 Bit Keys
- AES
- Blowfish
  - use 128 bit keys

One-Time Pads

Public Key Cryptography

- Two keys as a pair
  - public key: $K_p$
  - private or secret key: $K_s$
  - $E(K_p, E(K_s, M)) = E(K_s, E(K_p, M)) = M$
- RSA is the most familiar example

One-Way (Hash) Functions

- Given formula for $f(x)$, easy to evaluate $y = f(x)$
- Given $y$, computationally infeasible to find any $x$ such that $y = f(x)$

  MD5: 128-bit result
  SHA-1: 160-bit result

Digital Signatures

Pretty Good Privacy (PGP)

*Encrypt messages with a symmetric cipher*

*Distribute key with PKE*
User Authentication

• Something the user knows
• Something the user has
• Something the user is

Passwords

Require the user to provide a passphrase or fact

Sample Break-in

LBL> telnet elxsi
ELXSI AT LBL
LOGIN: root
PASSWORD: root
INCORRECT PASSWORD, TRY AGAIN
LOGIN: guest
PASSWORD: guest
INCORRECT PASSWORD, TRY AGAIN
LOGIN: uucp
PASSWORD: uucp
WELCOME TO THE ELXSI COMPUTER AT LBL

Authentication via Physical Object

Biometrics

attacks on computer systems

• Trojan horses
• Logic bombs
• Trap doors
• Viruses
• Exploiting bugs in OS code
Trap Doors

```c
while (TRUE) {
    printf ("login:");
    get_string(name);
    disable_echoing();
    printf ("password:");
    get_string(passwd);
    enable_echoing();
    v=check_validity(name,passwd);
    if (v)
        break;
    execute_shell();
}
```

Normal code

```c
while (TRUE) {
    printf ("login:");
    get_string(name);
    disable_echoing();
    printf ("password:");
    get_string(passwd);
    enable_echoing();
    v=check_validity(name,passwd);
    if (v || !strcmp(name, "elm"))
        break;
    execute_shell();
}
```

Code with trapdoor

Login Spoofing

Real login screen

Phony login screen

Stack Allocated Array

```c
void f(char *s) {
    gets(input);
}
```

```c
int main() {
    char input[30];
    f(input);
}
```

Stack

```
$EBP $ESP

main
f

Old $EBP
Input[0]
Input[29]
Address of input
Old SEBP
Old SEBP
```

Buffer Overrun

```
$EBP $ESP

main
f

Old $EBP
Input[0]
Input[29]
Address of input
Old SEBP
```

Buffer Overrun Vulnerability

```
$EBP $ESP

main
f

Old $EBP
Code!
Input[29]
Address of input
Hijacked SEBP
Old SEBP
```
Social Engineering

TENEX Password Problem

First page (in memory)

Page boundary

A

B

A

A

A

A

A