OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

INF FAKULTÄT FÜR INFORMATIK

Distributed and Operating Systems Group

Advanced Operating System Issues (AOSI)

Excercise Sheet 7

Due date: 17.01.2013

1 Security in Operating Systems

Describe the basic security mechanisms in Windows 2K and Unix. People often regard Windows NT operating systems as insecure. Do you agree with that? Explain your opinion.

2 Access control methods

There are two major forms of access control models:

- Access control List(ACL)
- Capability Lists(C-Lists)

Describe both concepts and discuss benefits and drawbacks. Compare the usage of these concepts in Linux and Windows 2K.

3 Cryptographic Hash functions

Consider the following hash algorithm:

```
procedure ExampleHash($x$)
    $hash \leftarrow 0$
    for all $char$ in $x$ do
        $hash \leftarrow hash \otimes char$
    end for
    return $hash$
end procedure
```

Do you consider it to be a cryptographic-hash function? Justify your decision!

4 Secret key exchange

The Diffie-Hellman-Merkle-System created a means to transfer keys through an unsecure channel. What major problem of symmetric encryption systems was solved by it and how did it work?
The RSA asymmetric encryption system provides the possibility to communicate through an unsecured channel, without the need of a common secret key. Why is it seldom used for the communication itself, but only for the exchange of the secret keys?

5 Secure programming

Consider the following function, that copys a string in reverse order.

```
char* strncpy_R( char* dest, const char* src, size_t len){
    char buffer[1024];
    char* bufPtr = buffer;
    while ( *src && len-- )
        *bufPtr++ = *src++;
    while ( bufPtr != buffer )
        *dest++ = *--bufPtr;
    return dest;
}
```

Are there any security related problems within the function? If there are, explain them and give examples for their exploitation.

6 Authentication

One-time Pad is proven to be perfectly secure, if it is used correctly. If one uses Lamport's Algorithm to derive the individual keys by applying one-way functions to a secret does the perfect security property still hold? Justify your answer!