

Computer System Security and Management

D0004E

Lecture 12: Recap
Paweł Pietrzak



1

The course

- Maintenance
 - mostly labs
 - some lectures
- Security
 - lectures

2

D0004E, 2011-12

Exam

- Approximately
 - maintenance 50%
 - security 50%

3

D0004E, 2011-12

Maintenance

- Basic Unix
- DNS
- Mail
- Storage and backup

4

D0004E, 2011-12

Security

- General security and computer security definitions
- Principles of designing computer security
- Implementing computer security
- Cryptography
- Keys
- Communication and network security
- Software security

5

D0004E, 2011-12

Maintenance

6

Filesystem Hierarchy

```

/
├── bin/
│   └── ls
├── dev/
├── etc/
│   └── passwd
├── tmp/
├── usr/
│   └── lib/

```

File Basics

- Long listing of all files:

```

> ls -la /etc/hosts
lrwxrwxrwx    ... /etc/hosts -> ./inet/hosts

> ls -la ...
crw-----    ... /devices/pseudo/conskbd@0:kbd
prw-----    ... /etc/initpipe1
brw-r-----    ... /devices/pci@1f,0/ide@sd@1,0:a
drwxr-xr-x    ... /usr/bin/

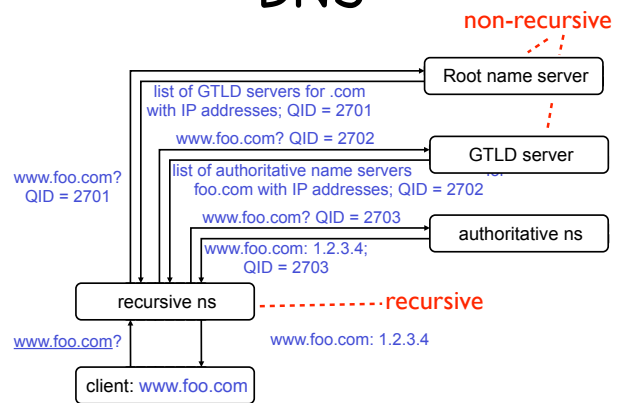
```

File permissions

Flags	Owner	Group	World
d	rwX	rwX	---

- r = Read; w = Write; x = eXecute
- Owner - permissions for the owner of the file
- Group - permissions for the group of the file
- World - permissions for the world

DNS



Record types in DNS

- **SOA**: Start of Authority
- **NS**: Name Server definition
- **A**: Host name to IP address mapping
- **CNAME**: Canonical name, host alias
- **MX**: Mail server definition

More Record Types

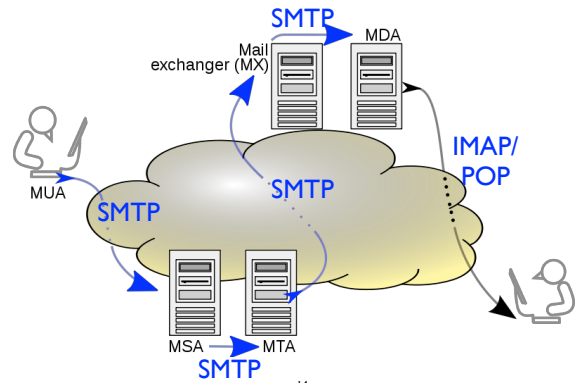
- **PTR**: IP address to host name mapping
- **SRV**: Service record
- **AAAA**: IPv6 host name to address mapping

DNS security issues

- Cache poisoning
- DNS Rebinding attacks

D0004E, 2011-12

E-mail



Source: Wikipedia

14

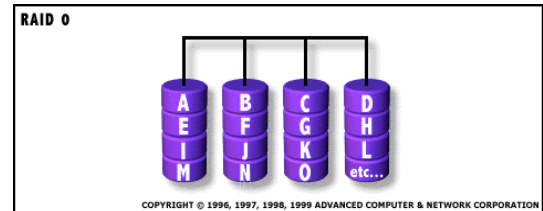
Storage-RAID

- Redundant Array of Inexpensive Disks
- Developed to replace expensive disk solutions with cheap SCSI drives, retaining performance and error tolerance

D0004E, 2011-12

RAID 0 - Striping

- No redundancy
 - No fault tolerance
- High I/O performance
 - Parallel I/O



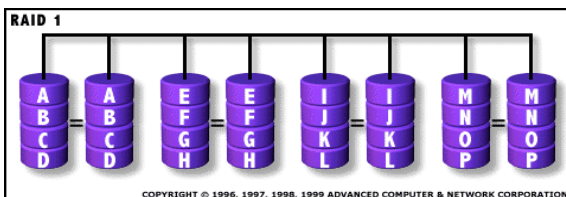
COPYRIGHT © 1996, 1997, 1998, 1999 ADVANCED COMPUTER & NETWORK CORPORATION

16

D0004E, 2011-12

RAID 1 - Mirroring

- Provide good fault tolerance
 - Works ok if one disk in a pair is down
- One write = a physical write on each disk
- One read = either read both or read the less busy one
 - Could double the read rate



COPYRIGHT © 1996, 1997, 1998, 1999 ADVANCED COMPUTER & NETWORK CORPORATION

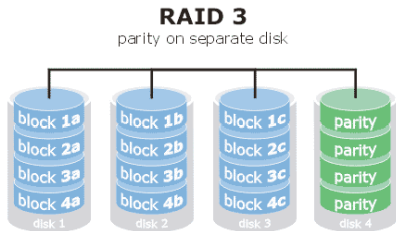
17

D0004E, 2011-12

Which is which: RAID 0 provides 0 help if a disk dies!

RAID 3 - Parallel Array with Parity

- Fast read/write
- All disk arms are synchronized
- Speed is limited by the slowest disk



D0004E, 2011-12

Parity Check - Classical

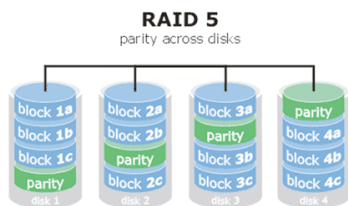
- An extra bit added to a byte to detect errors in storage or transmission
- Even (odd) parity means that the parity bit is set so that there are an even (odd) number of one bits in the word
- A single parity bit can only detect single bit errors since if an even number of bits are wrong then the parity bit will not change
- It is not possible to tell which bit is wrong

20

D0004E, 2011-12

RAID 5 - Parity Checking

- For error detection, rather than full redundancy
- Each stripe unit has an extra parity stripe
 - Parity stripes are distributed

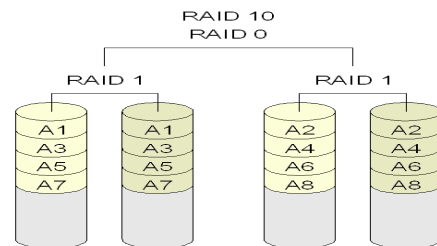


21

D0004E, 2011-12

RAID 10 - Striped Mirroring

- Nickname for RAID 1+0
- Performance of striping, security of mirroring
- Stripe over mirrors



22

D0004E, 2011-12

Comparing RAID Levels

	RAID 0	RAID 1	RAID 5	RAID 10
Read	High	2X	High	High
Write	High	1X	Medium	High
Fault tolerance	No	Yes	Yes	Yes
Disk utilization	High	Low	High	Low
Key problems	Data lost when any disk fails	Use double the disk space	Lower throughput with disk failure	Very expensive, not scalable
Key advantages	High I/O performance	Very high I/O performance	A good overall balance	High reliability with good performance

23

Backup & restore

- Why do we need backups?
 - Data gets lost.
 - Equipment fails.
 - Humans delete data by mistake and on purpose.
 - Judges impound all documents related to a lawsuit that were stored on your computers on a certain date.
 - Data gets corrupted, either by mistake, on purpose, or by gamma rays from space.
- You need reliable backups.

D0004E, 2011-12

Points to consider

- What files need to be backed up?
- Where are these files?
- Who will back up the files?
- When, where, and under what conditions should backups be performed?
- How often do these files change?
- How quickly does the file need to be restored?
- How long do we need to retain the data?
- Where should the backup media be stored?
- Where will the data be restored?

D0004E, 2011-12

Security

26

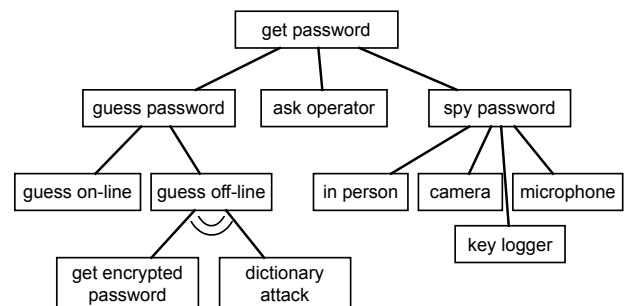
Basic definitions

- Vulnerabilities
- Threats
- Attacks

27

D0004E, 2011-12

Attack Tree - example



D0004E, 2011-12

Security Strategies

- **Prevention:** take measures that prevent your assets from being damaged.
- **Detection:** take measures so that you can detect when, how, and by whom an asset has been damaged.
- **Reaction:** take measures so that you can recover your assets or to recover from a damage to your assets.
- **The more you invest into prevention, the more you have to invest into detection to make sure prevention is working.**

D0004E, 2011-12

Security Objectives

- **Confidentiality:** prevent unauthorised disclosure of information
- **Integrity:** prevent unauthorised modification of information
- **Availability:** prevent unauthorised withholding of information or resources
- **Authenticity:** "know whom you are talking to"
- **Accountability (non-repudiation):** prove that an entity was involved in some event

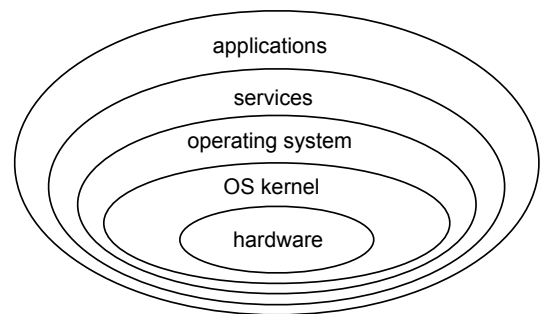
D0004E, 2011-12

Reliability & Safety

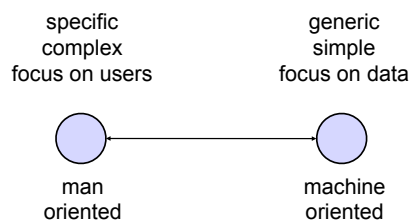
- Reliability and safety are related to security:
 - Similar engineering methods,
 - Similar efforts in standardisation,
 - Possible requirement conflicts.
- **Reliability** addresses the consequences of accidental errors.
- Is security part of reliability or vice versa?
- **Safety**: measure of the absence of catastrophic influences on the environment, in particular on human life.

D0004E, 2011-12

Onion Model of Protection



Man-Machine Scale



Authentication

- A secure system might have to track the identities of the users requesting its services.
- **Authentication**: process of verifying a user's identity.
- Two reasons for authenticating a user:
 - access control decisions (integrity, confidentiality)
 - logging security relevant events (accounting, non-repudiation)
- Attacks.

D0004E, 2011-12

Passwords in Unix

- Passwords stored in `/etc/passwd` "encrypted" with the algorithm `crypt(3)`.
- `crypt(3)` is really a one-way function: slightly modified DES* algorithm repeated 25 times with all-zero block as start value and the password as key.
- **Salting**: password encrypted together with a 12-bit random "salt" that is stored in the clear.

* An encryption/decryption algorithm we shall take up later

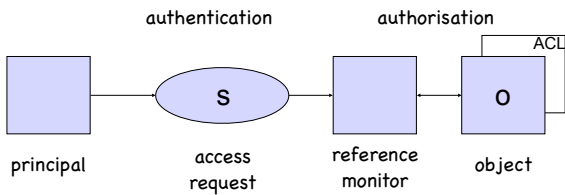
D0004E, 2011-12

Access Control

- Access control: who is allowed to do what?
- Traditionally, "who" is a person.
- Traditionally, "what" consists of an operation (read, write, execute, ...) performed on a resource (file, directory, network port, ...)
- The type of access control found in Unix, Windows.
- Today, access control is a more general task.
 - Java sandbox: "who" is code running on a machine.

D0004E, 2011-12

Authentication & Authorisation



B. Lampson, M. Abadi, M. Burrows, E. Wobber: Authentication in Distributed Systems: Theory and Practice, ACM Transactions on Computer Systems, 10(4), pages 265-310, 1992

D0004E, 2011-12

Elementary Access Operations

- Bell-LaPadula model has four **access rights**:

- > [execute](#)
- > [read](#)
- > [append](#), also called [blind write](#)
- > [write](#)

- Mapping between **access rights** and **access modes**:

	execute	append	read	write
observe			X	X
alter		X		X

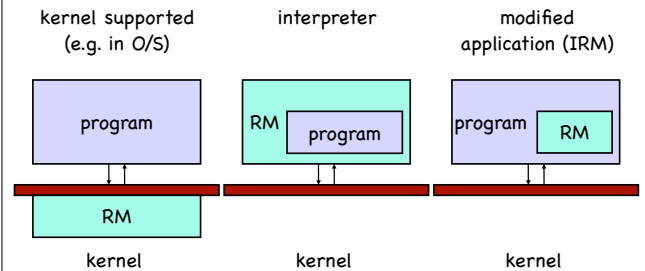
D0004E, 2011-12

Reference Monitor (RM)

- **Reference monitor**: access control concept that refers to an abstract machine that mediates all accesses to objects by subjects.
- **Security Kernel**: hardware firmware, and software elements of a TCB that implement the reference monitor concept. It must mediate all accesses, be protected from modification, and be verifiable as correct.

D0004E, 2011-12

Reference monitors – Design Choices



D0004E, 2011-12

Controlled Invocation

- Example: A user wants to write to memory (requires supervisor mode).
- The system has now to switch between modes, but how should this switch be performed?
- Simply changing the status bit to supervisor mode would give all supervisor privileges to the user without any control on what the user actually does.
- Thus, the system should only perform a predefined set of operations in supervisor mode and then return to user mode before handing control back to the user.
- Let's refer to this process as **controlled invocation**.

D0004E, 2011-12

Principle of Least Privilege

- Give the user/program only the privilege it needs to get its task done
 - One of the most important principles in systems security
- Why?
 - Limit the damage when program misbehaves or is compromised
- What privileges should you give to your
 - ssh server
 - Video game program

D0004E, 2011-12

Cryptography

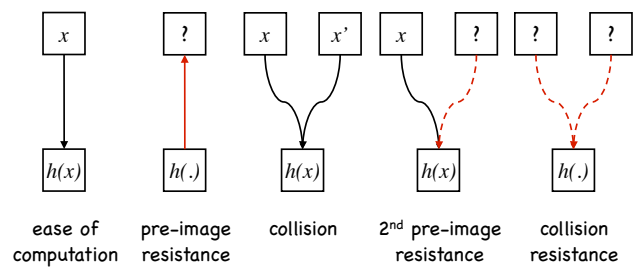
Cryptography

- from Latin, stands for "secret writing"
- purpose
 - **data confidentiality:** encryption algorithms hide the content of messages;
 - **data integrity:** integrity check functions provide the means to detect whether a document has been changed;
 - **data origin authentication:** message authentication codes or digital signature algorithms provide the means to verify the source and integrity of a message.

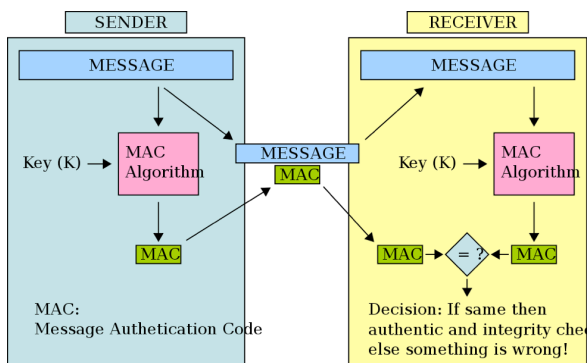
One-way Functions

- Requirements on a one-way function h :
- **Ease of computation:** given x , it is easy to compute $h(x)$.
- **Compression:** h maps inputs x of arbitrary bitlength to outputs $h(x)$ of a fixed bitlength n .
- **Pre-image resistance (one-way):** given a value y , it is computationally infeasible to find an input x so that $h(x) = y$.

Properties of One-way Functions



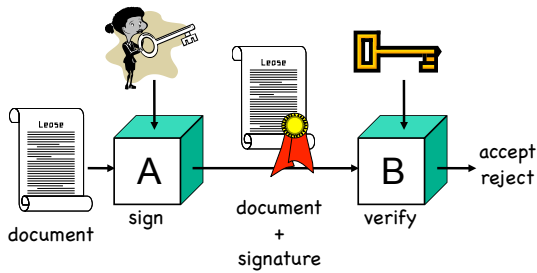
MAC overview



Frequently Used Hash Functions

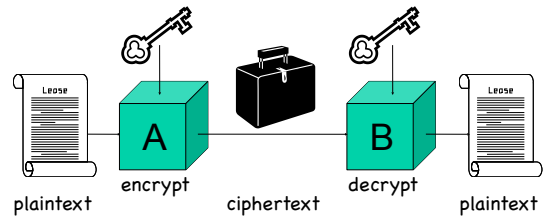
- **MD4:** weak, it is computationally feasible to find meaningful collisions.
- **MD5:** standard choice in Internet protocols, so broken and no longer recommended.
- **Secure Hash Algorithm (SHA-1):** designed to operate with the US Digital Signature Standard (DSA); 160-bit hash value; collision attacks reported.
- **RIPMD-160:** hash function frequently used by European cryptographic service providers.
- **SHA-256:** when longer hash values are advisable.

Digital Signatures



D0004E, 2011-12

Symmetric Key Encryption



D0004E, 2011-12

Symmetric Key Cryptography

- Protects documents on the way from *A* to *B*.
- A* and *B* need to share a key.
- A* and *B* have to keep their keys secret (secret key cryptography).
- There has to be a procedure whereby *A* and *B* can obtain their shared key.
- For *n* parties to communicate directly, about n^2 keys are needed.

D0004E, 2011-12

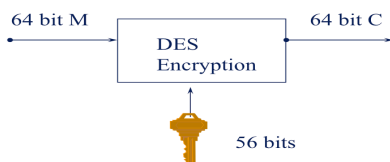
Block Ciphers & Stream Ciphers

- Block ciphers:** encrypt sequences of "long" data blocks without changing the key.
 - Security relies on design of encryption function.
 - Typical block length: 64 bits, 128 bits.
- Stream ciphers:** encrypt sequences of "short" data blocks under a changing key stream.
 - Security relies on design of key stream generator.
 - Encryption can be quite simple, e.g. XOR.
 - Typical block length: 1 bit, 1 byte.

D0004E, 2011-12

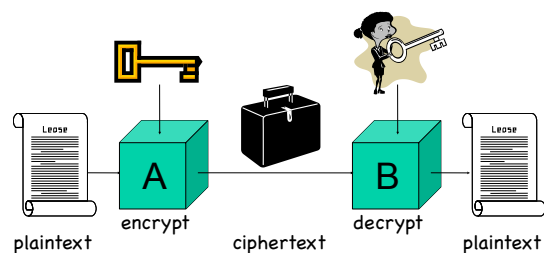
DES - an instance of a block cipher

- Data Encryption Standard (DES) -
 - Designed by IBM in 1974 responding to NIST request
 - Standardized in 1979
- Designed for fast VLSI implementation
- Key length 56, block length 64



D0004E, 2011-12

Encryption with Public Keys



D0004E, 2011-12

Public key Encryption

- Protects documents on the way from *A* to *B*.
- B* has a **public encryption key** and a **private decryption key**.
- A procedure is required for *A* to get an authentic copy of *B*'s public key (**need not be easier than getting a shared secret key**).
- For *n* parties to communicate, *n* key pairs are needed.

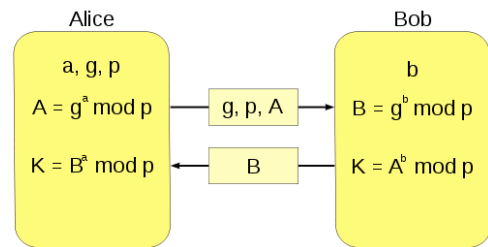
Keys

AKEP2

- Let n_A and n_B be random numbers (nonces) picked by *A* and *B* respectively.
- AKEP2 is a three-pass protocol:
 - $A \rightarrow B: n_A$
 - $B \rightarrow A: B, A, n_A, n_B, h_K(B, A, n_A, n_B)$
 - $A \rightarrow B: A, n_B, h_K(A, n_B)$

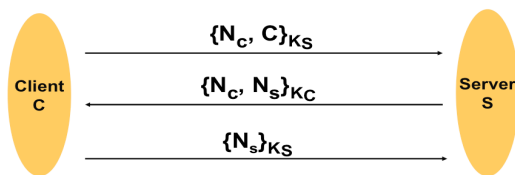
The shared key is $k = h'_K(n_B)$
- AKEP2 provides mutual entity authentication and (implicit) key authentication.

Diffie-Hellman



$$K = B^a \text{ mod } p = (g^b \text{ mod } p)^a \text{ mod } p = g^{ab} \text{ mod } p = (g^a \text{ mod } p)^b = A^b \text{ mod } p$$

Needham-Schroeder Protocol

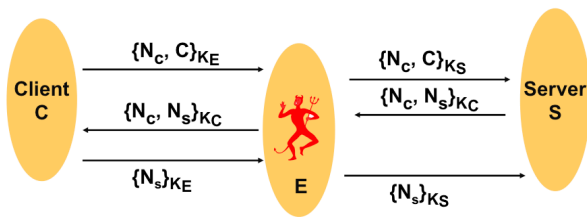


- K_S, K_C are public keys of *S* and *C* respectively
- Goal:
 - Mutual authentication: $C \rightarrow S, S \rightarrow C$
 - Shared secret: N_C, N_S

Active attacker

- An attacker may
 - Eavesdrop on previous protocol runs, even on protocol runs by other principals, replay messages at a later time
 - Inject messages into the network, e.g., fabricated from pieces of previous messages
 - Alter or delete a principal's messages
 - Initiate multiple parallel protocol sessions
 - Run dictionary attack on passwords

Problem with Needham-Schroeder

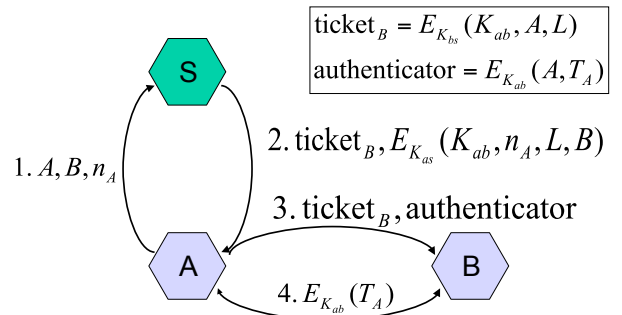


- Flaw (discovered 18 years after publication, with a formal technique called **model checking**):
 - Authentication: $C \rightarrow E$, $S \rightarrow C$
 - Secrecy: E knows N_c , N_s
 - How to fix it? – The second message should be $\{S, N_c, N_s\}_{K_C}$

61

D0004E, 2011-12

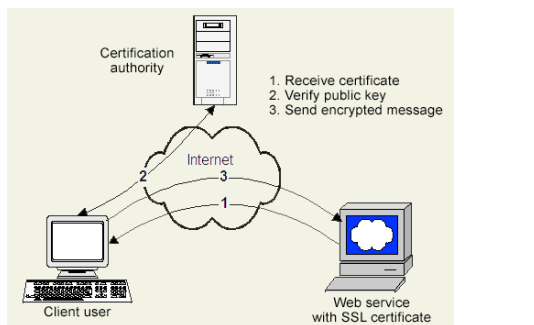
Kerberos (simplified)



62

Public key infrastructure (PKI)

Basic idea:



63

D0004E, 2011-12

Communication and network security

64

SSL/TLS Basic Features

- Security at session layer.
 - 'Thin layer' between TCP and, e.g., HTTP.
 - TCP provides reliable, end-to-end transport.
 - Applications must be **aware** of SSL, need some modification.
- Two layer architecture:
 - SSL Record Protocol: provides secure, reliable channel to second layer.
 - Upper layer carries **SSL Handshake Protocol**, Change Cipher Specification Protocol, Alert Protocol, HTTP, any other application protocols.

65

D0004E, 2011-12

Network security

- Firewalls
- Proxies

66

D0004E, 2011-12

WEB - cross site scripting

67

Conditions

- A Web application accepts user input (well, which Web application doesn't?)
- The input is used to create dynamic content (Again, which Web application doesn't?)
- The input is insufficiently validated (Most Web applications don't validate sufficiently!)

68

D0004E, 2011-12

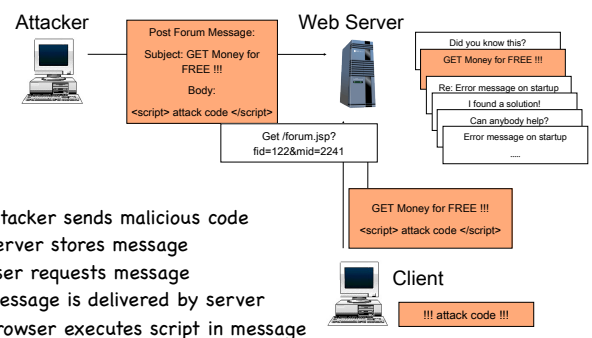
Players

- An Attacker: Anonymous Internet User, Malicious Internal User
- A company's Web server (i.e. Web application)
 - External (e.g.: Shop, Information, CRM, Supplier)
 - Internal (e.g.: Employees Self Service Portal)
- A Client
 - Any type of customer
 - Anonymous user accessing the Web-Server

69

D0004E, 2011-12

XSS-Attack: General Overview



D0004E, 2011-12

Software security

71

Integer wrapping: an example

```
char buf[128];
combine(char *s1, size_t len1,
        char *s2, size_t len2)
{
    if (len1 + len2 + 1 <= sizeof(buf)) {
        strncpy(buf, s1, len1);
        strncat(buf, s2, len2);
    }
}
```

Annotations:

- $len1 < sizeof(buf)$
- $len2 = 0xffffffff$
- $len2 + 1 = 2^{32} - 1 + 1 = 0 \text{ mod } 2^{32}$
- strncat will be executed

72

Buffer overrun

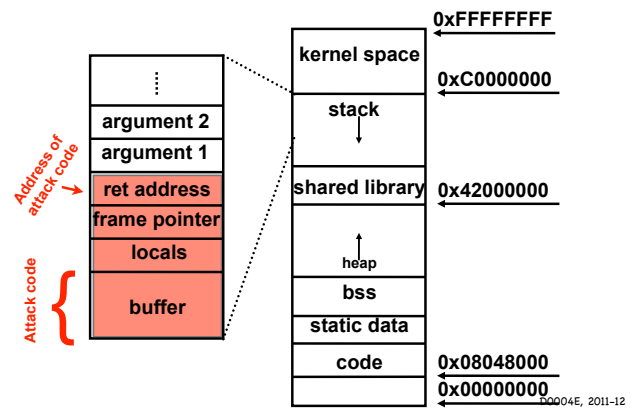
```
char buf[80];
int authenticated = 0;
void vulnerable() {
    gets(buf);
}
```

- A login routine sets authenticated flag only if user proves knowledge of password
- The risks: attacker supplies 81 bytes (81st set non-zero)
 - Makes authenticated flag true!
 - Attacker gains access: security breach!

73

D0004E, 2011-12

Stack smashing



D0004E, 2011-12

SQL Injection

- `statement := "SELECT * FROM users WHERE name = " + userName + "";"`
- Suppose `userName` is:
 - `a' or 't'='t`
- `SELECT * FROM users WHERE name = 'a' or 't'='t';`

75

D0004E, 2011-12

Sample questions

76

DNS

3. DNS

What type of DNS-records have the following functions?

- Name-to-address translation
- Identifies zone servers
- Controls e-mail routing
- Address-to-name translation
- Nicknames or aliases for a host
- What can you expect to find in the zone file of the zone "sm.luth.se"?

(3p)

77

File permissions

4. UNIX File Permissions

- What does it mean to run an application in a chrooted environment?
- What does it mean that a directory has the "sticky" bit set?
- What are the security implications of files that have the "setuid" bit set (2p)?
- Why is it good to check which user accounts that have the `userid 0` on a regular basis?

(5p)

78

Mail

5. Mail

- A mail message has three distinct parts, which three?
- In which part can you find a complete history of the "hops" a message has taken to reach its destination?

(1p)

79

RAID

Describe the different raid levels and their most important characteristics in terms of performance and redundancy (*feel free to draw pictures to illustrate*).

- Raid 0
- Raid 1
- Raid 5

80

Script

Script - Count Disabled Users

Write a shell-script that counts the number of users in `/etc/passwd` that are disabled in such a way that the string `***2007***` is the first part of the password field. An example of the format of passwd:

```
sven:p31TpxCa/..:9993:20:Sven Svensson:/home/sven:/usr/local/bin/tcsh
```

NOTE: *Extracts from the man pages to bash are appended.*

(5p)

81

Script

```
#!/bin/bash
```

```
cat $1 | awk -F: '{print $2}' | grep "***2007***" | wc -l
```

82

Crypto

In this problem, your task is to encrypt a message $M \in \{0,1,2,3,4\}$ using a shared random key $K \in \{0,1,2,3,4\}$. Suppose you do this by representing K and M using three bits (000, 001, 010, 011, 100) each, and then XORing the two representations. Given a ciphertext 101, what can you infer about the corresponding plaintext? Do you think this scheme has the same security guarantees as the **one-time pad**? Explain.

83