SWINBURNE UNIVERSITY OF TECHNOLOGY

Secure and Resilient Networks

Access Control

Lecture twelve

Outline of Lecture

- Kerberos
- One-time passwords
- Biometrics

Learning goals

- You should be able to
  - Describe the operation of Kerberos
  - Describe one-time passwords
  - Describe the main forms of biometric measures along with their strengths and weaknesses

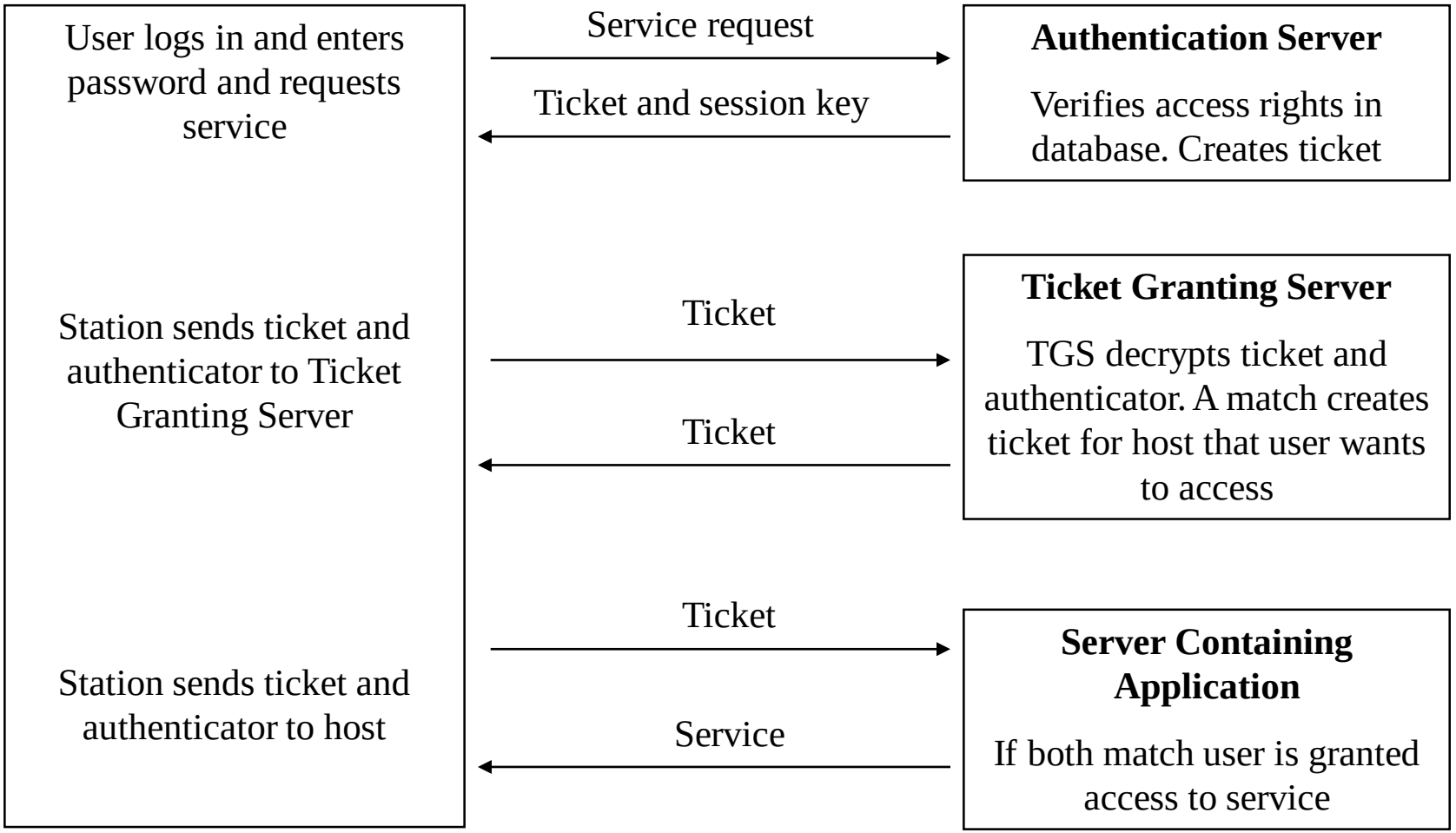
Kerberos

- Single Signon System
- Enables user to prove identity once and then be able to access all authorised resources without subsequent authentication
- Users sign into the Kerberos server, and are issued a ticket, which their client software presents to servers that they attempt to access
- Integral part of Windows Server

Kerberos

- Based purely on symmetric keys
  - Shared secret keys
  - Session keys
- Makes use of multiple layers of encryption
  - Session keys will be encrypted and transmitted within shared secret keys
- Kerberos is very cleverly designed to ensure that users do not give themselves privileges that they are not entitled to
- Main entities are
  - Authentication server
  - Ticket granting server
  - Kerberos enabled application or server

Kerberos


User logs in and enters password and requests service
Service request
Ticket and session key
Authentication Server
Verifies access rights in database. Creates ticket
Station sends ticket and authenticator to Ticket Granting Server
Ticket
Ticket
Ticket Granting Server
TGS decrypts ticket and authenticator. A match creates ticket for host that user wants to access
Station sends ticket and authenticator to host
Ticket
Service
Server Containing Application
If both match user is granted access to service

Kerberos animation

kerberos07.swf

Question

- Why in Kerberos is the TGT encrypted with the TGS' secret key and then encrypted with the user's secret key?

Some weaknesses of Kerberos

- KDC can be a single point of failure
- KDC needs to be scalable
- Secret keys stored user's workstations
  - Possibly compromised
- Session keys stored on workstations
  - Possibly compromised
- Relies on passwords
  - Could be subject to dictionary attack

One-time passwords

- A one-time password is used exactly once, after which it is no longer valid.
  - Very strong defence against eavesdroppers, and replay attacks
- Usual technique is built around a handheld device that generates the password
  - The password is valid only once
    - prevents replay attack
  - The password is valid for only a short period of time
    - typically one to two minutes
  - Only one login per minute (or so) is permitted
  - SecurID most commonly used

One-time passwords

- Typically generate passwords based on a hash function
  - Reminder as to what hash functions are
    - A hash function takes a number as an input and generates an output
    - It is impossible to generate the input from the output even if the algorithm is known
    - MD5, SHA-1, SHA-256, SHA-3 examples of hash algorithms
    - Sometimes ‘trap-door’ functions
- One time password will usually generate the hash based on a PIN number and the current time
  - The device generates the hash function value based on its inputs
  - This is transmitted to the authentication server
  - It uses the same information to generate the hash
    - If equal then authenticated.

One-time passwords

- Some difficulties with One-time passwords
  - device needs to be kept secure
  - PIN used on it needs to be kept secure
  - Time skew between the host and the authentication server
    - usually dealt with by the server keeping track of several candidate hash values
- The database on the authentication server needs to be fast, available and secure

One-time passwords using Lamport's Method

- One-time password schemes can be implemented without special hardware (Lamport, 1981)
  - Construct a sequence of hashes of hashes starting with some starting password
- Calculated values are used progressively
  - Need to keep a track of number of times the password sequence has been used
- Creates a virtual list of passwords
  - Need to use from the bottom up

One-time passwords (Lamport) example

- The user has some password ‘x’ and a password sequence number
- The password sequence generated from ‘x’ can be used 1000 times before being reset.
- First time through the password sequence number is set to 10000
- The user system calculates F(F(F(….(F(x))))..) = $F^{1000}(x)$
- The first password used is $F^{1000}(x)$
- The user calculates this and submits it during authentication
- The authentication system also knows ‘x’ and does the same calculation
- If the value it calculates matches then the user is authenticated
- Both the user and authentication system decrement the password sequence number to 999.
- The next password expected is $F^{999}(x)$

Question

- Why do we work backwards from $F^{1000}(x)$? Why don't we start from $F^{1}(x)$ and work forwards?

Biometrics

- Useful for where strong authentication needed
- 3rd factor
  - Something you have
    - Token
    - Smart card with private key
  - Something you know
    - Password
    - PIN
  - Something you are
    - Biometrics

Biometrics

- Mechanism
  - Takes a measure of some physical characteristic
  - Compares it with a stored version of the characteristic
  - If a good enough match then access will be granted
- An analogue measure
  - Usually scope for false positives
    - Identify a recorded and physical measure as being the same when they are not
  - False negatives
    - Reject a recorded and physical as being the same when they are

Biometric false negatives

- Types of errors
  - Type I error
    - False positive
  - Type II error
    - False negative
- Cross over error rate
  - Percentage at which false rejection rate equals false accepance rate
  - Typically used to measure the effectiveness of a Biometric system

Biometrics

- A good biometric is
  - Universal
    - It can be measured for everyone
  - Unique
    - It is different for every person
  - Permanent
    - It doesn't change as you grow older, fatter, thinner, balder, hairier
  - Collectable
    - It can be measured by a machine
  - Is easily measured
    - It is collected and can be compared with the stored measure quickly

Biometrics

- A good biometric is
  - Acceptable
    - No use if people refuse to use it
  - Difficult to circumvent
    - Can't be faked
  - Portable
    - Equipment is low cost and easy to move and install

Biometric techniques

- Signature
  - Well accepted
  - Can be forged
- Face geometry
  - Measure some key aspects of face
    - Distance between eyes
    - Location of mouth, eyes, ears
- Facial thermogram
  - Uses an infrared camera to measure heat dispersion on the face
  - Very accurate method
  - Good acceptance
  - Can't be forged or tampered
  - Expensive equipment

Biometric techniques

- Fingerprint
  - Unique
  - Unchanging
  - Well understood and accepted
  - Cheap and portable equipment
- Hand geometry
  - Takes a number of measures of the hand
    - Length of fingers
    - Area of palm
  - Simple to use
  - But fairly low accuracy and hardware is bulky and expensive

Biometric techniques

- Retina and Iris scans
  - Scans blood vessel pattern at back of eye (retina)
  - Scans patterns, shapes, colours of coloured part of eye (iris)
  - Very reliable technology
  - Difficult to circumvent
  - Expensive
  - Lots of public resistance
- Voice
  - Not fully unique
    - Can be circumvented fairly easily
  - Low cost hardware

Biometric techniques

- DNA
  - Entirely unique
  - Expensive and slow
  - Lots of public resistance
- Signature dynamics
  - Signatures usually signed in the same way and speed every time
  - Physical motions captured as signals
  - Very reliable
- Keyboard dynamics
  - Characteristic way in which a person types a certain phrase
  - Surprisingly reliable
    - Very difficult to repeat a person's typing style
- Palm scans

Difficulties with Biometrics

- Where does biometric data get stored and how do you protect it?
- Biometrics do not work for some part of the population
  - Construction workers and elderly people often have fingerprints that are worn down and cannot be read (3-7% of the population)
  - Voice doesn't work for someone who through surgery can no longer talk
  - Signatures don't work for people who are illiterate

Difficulties with Biometrics

- Some biometrics are poorly accepted
  - Laser based retinal scanning
  - Laser based iris scanning
  - DNA testing
- Biometrics cannot be changed
  - General principle is that authentication data should change periodically
  - Cannot change fingerprints
- Biometrics can be obtained easily and possibly spoofed
  - Fingerprints on glass
  - Voice can be recorded
- Can be easy to spoof some biometrics
  - Fake fingerprints made out of gelatin
  - Face recognition software fooled by life-sized photographs

Conclusion

- Kerberos
  - Multiple layers of encryption
- One time passwords
  - Based on hash functions
- Biometrics
  - Biometrics a third factor in authentication
  - Used in ‘strong authentication’
  - Many possible biometrics but lots of resistance
  - Can be faked
  - Can’t be changed