SWINBURNE UNIVERSITY OF TECHNOLOGY

Network Security and Resilience

Access Control

Lecture eleven

Outline of Lecture

- Identification, Authentication and Authorisation
- Passwords and pass-phrases
- Explain the role of Hash Functions in authentication
- PPP authentication
  - PAP and CHAP
- RADIUS and DIAMETER

Learning objectives

- You should be able to
  - Explain
    - Identification, Authentication and Authorisation
  - Describe the strengths and weaknesses of password and passphrase based authentication
  - Explain the operation of RADIUS
  - Explain how DIAMETER differs from RADIUS

Access

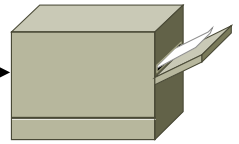
- Key concepts of Access Control
  - Subject
    - Some entity such as a process, user or program who wants access to some resource
  - Identification
    - A method of linking a subject to an identity. Identification may include user ids, account numbers. Needs to be distinguished from authentication
  - Authentication
    - Additional information validating the identification. Examples might be a password, biometric, PIN, anatomical attribute, token
  - Authorization
    - A method of ensuring the authenticated entity accesses only those resources it is entitled to

Access control

Identification

Authentication

Authorization



Access control good practices

- Deny access to anonymous accounts
- Limit and monitor usage of administrator and super-user accounts
- Suspend accounts after a number of failed log in attempts
- Remove obsolete accounts
- Suspect inactive accounts after 30 or 60 days
- Disable unneeded services
- Replace default passwords on accounts
- Enforce password change (controversial)
- Audit system and user events and actions
- Protect audit logs

Access control models

- Three commonly used models
- Discretionary Access Control (DAC)
  - Owner of object (file, database etc) specified who can access it
- Mandatory Access Control (MAC)
  - Object is labelled according to security level and for a user to access it, they must have sufficiently high security level
  - Unix file permissions an example
    - Three groups Owner / Group / All
    - Each group can Read/Write/eXecute
- Role Base Access Control (RBAC)
  - Access to objects governed by role within organisation

Identity management

- Whole area of who is allowed to do what is described by the general term ‘identity management’
- Essentially concerned with who has access to what information assets
- Identity management needs to deal with
  - Different types of users who need access to different levels of access
  - Information resources have different security levels
  - Lots of different identity information that needs to be kept secure
    - Passwords, biometric data etc
  - Continual changes in roles within the organisation

Authentication

- Purpose of authentication
  - Enables high degree of certainty as to the identity of the other party
- Authentication ties an identity to a secret
  - Sometimes the system to whom the individual is attempting to gain access knows the secret
  - Sometimes the system to whom the individual is attempting to gain access knows something derived from the secret
- We need authentication to prove our identity when we want to use some resource or another party wants to be sure we are who we claim to be

Multifactor authentication

- Usually two out of three factors necessary for satisfactory level of authentication
  - Something one knows
    - Password, pass-phrase, PIN number
  - Something one has
    - Credit card, Driver's license, Smart card, USB security dongle, one-time-password generator
  - Something one is
    - Biometrics
- Biometrics has been poorly accepted
  - Some acceptance of fingerprint systems on laptops
  - Strong resistance to retinal scans, DNA scans and similar
  - Usually a pass-phrase and an authentication token

Level of authentication

- Specified in the security policy
  - Importance of the asset protected
  - Cost of the method
  - Convenience to the user
- Most applications use single factor authentication
  - Poorly chosen passwords
- Strong authentication uses Biometrics and one of the two other factors

Question

- What security factors are used in the following scenarios? Which scenario is an example of Strong Authentication?
  - An ATM where a debit card and PIN must be entered in order to withdraw cash
  - A laptop with a fingerprint system and password
  - A network login that requires a smart card to be swiped and a password to be entered

Authentication tokens

- Not necessarily physical tokens
- Exchange of information based on shared secret
- Token performs a computation based on the shared secret and some variable data which is sent to the authentication server
- The authentication server compares the result with the value it has
- If the same then authenticated

Passwords and pass-phrases

- User passwords are usually poorly chosen
  - Date of birth, daughter's name, friend's name
  - Can be broken easily with a dictionary attack or through social engineering
- Machine generated passwords
  - Much more difficult to attack
  - BUT much more difficult to remember
- An interesting comment on passwords
  - http://xkcd.com/936
- And a counterview
  - http://www.wired.co.uk/news/archive/2013-05/28/password-cracking

Passwords and pass-phrases

- Good password practice is
  - Use a different password for different accounts
  - Use a random, meaningless string of characters
  - Change passwords frequently
  - Don't write them down
- BUT most of us have around 40 or 50 passwords that we need to remember
  - Cannot remember all of them
  - Should not write them all down
  - Should not reuse passwords
- Most of us reuse passwords
  - If we reuse passwords we should do so in a structured way
    - Password for sensitive accounts, another for moderately sensitive, etc.

Passwords and pass-phrases

- Proliferation is the problem with passwords
  - Too many
- Some solutions
  - Password vault
  - Single signon system
  - Passwords based on images, algorithms, word associations
- Bruce Schneir says either use a software password vault or simply write them down and put the list in your wallet
  - Controversial

Passwords and pass-phrases

- Single sign on systems
  - Kerberos, RADIUS etc
  - Use a single password for access to all systems at a site
  - Uses an authentication server
  - Identification information is passed to the server in some encrypted form which then responds with ‘authenticated’ or ‘not authenticated’
  - Reduces but doesn’t fully solve proliferation problem
  - More on this topic later

Passwords and pass-phrases

- Using images for authentication instead of passwords
  - Users remember pictures rather than character strings
- Secret knowledge is of an algorithm rather than a password
  - Given a challenge sequence of numbers the user knows an algorithm that enables him/her to respond
  - A simple (and not very secure) example might be ‘Return the numbers divisible by 5’ from the challenge list:
  - >Your challenge list is 100, 23, 402, 50, 60
  - >100, 50, 60

Passwords and pass-phrases

- Pass sentences and word association
  - When your account is set up you supply a number of questions and their associated answers to the authentication system
  - When you wish to log on the system randomly selects a question for you to answer
  - Examples of questions
    - Where were you born?
    - What was your favourite toy when you were a child?
    - etc
  - Idea is to use trivia that is not readily available elsewhere that only you know
- BUT social networks (like FaceBook) make this much less secure than it used to be

Passwords and pass-phrases

- Password susceptible to Rainbow Table attacks
  - Usually the password is stored as a hash
  - When creating a password the operating system hashes the password and stores the hash
  - When validating the password the OS hashes the password entered, and compares the resulting hash with the stored hash
- Rainbow tables can be used to break passwords quickly if the password file can be obtained
  - Rainbow tables map a password to a fixed number sequence of hashes and plausible passwords (generated by a Reduction function)
  - Store the start and end of sequence
  - The Reduction and hash function are alternately applied until either a match is found or the number of transforms in the sequence is exceeded
  - Some available rainbow tables reported 1.5 Tbytes

Passwords and pass-phrases

- ‘Salting’ is a technique to defend against rainbow attacks
  - Add a prefix or suffix to every password before hashing
    - Doesn’t need to be secret
  - As well as the user having a secret password the organisation has a (potentially much longer) string called a ‘salt’
  - Eg. User’s password is ‘password’. Organisation’s salt is hash of the password
  - When storing the password the two are concatenated and then hashed.
  - When validating the password the two are concatenated and then hashed

Passwords and pass-phrases

- Salting can be made more complex by interspersing parts of organisation's salt throughout user's password and by having multiple passes
- Advantage of salting is that it makes the number of combinations an attacker must try much larger
- Another defense against rainbow attacks is to use multiple hashing.
  - Hash the password, then hash that result, then hash it again and so on
  - Example: SHA512crypt (used in most Unix implementations) passes the result through 5000 hashing iterations
- An example implementation is at https://quickhash.com/

Smart cards

- A smart card is a portable device that has a CPU, some input/output ports, and a few thousand bytes of nonvolatile memory that is accessible only through the card's CPU.
- Can be used to store passwords and calculate hash functions
- An example of "something you have" authentication but usually augmented by "something you know," a PIN.
- Some smart cards have handheld portable readers. Some readers are now available in the PC card format.
- Smartcards mostly tamper proof but some nondestructive techniques for reading them
  - subject cards to abnormal voltages or radiation;
  - monitor power consumption
  - monitor the precise time to do public key calculations.

PPP Authentication

- Number of different authentication protocols
  - Password Authentication Protocol (PAP)
  - Challenge-handshake authentication protocol (CHAP)
  - Extensible Authentication Protocol (EAP)
  - Lightweight Extensible Authentication Protocol (LEAP)

PPP Authentication

- Point-to-Point Protocol (PPP)
  - Used for most remote access
- PPP is capable of operating across any DTE/DCE (serial) interface
- The only requirement imposed by PPP is the provision of a duplex circuit, either dedicated or switched, that can operate in either an asynchronous or synchronous bit-serial mode, transparent to PPP link layer frames
- No PPP imposed transmission rate other than those imposed by the particular DTE/DCE interface in use.

Password Authentication Protocol (PAP)

- PAP can authenticate an identity and password for a peer resulting in success or failure.
  - RFC 1334, pages 2, 3 and 4:
- After the PPP link has been established there is an optional authentication phase
  - The authentication mechanism is specified during the connection phase
- PAP provides a simple method for the peer to establish its identity using a 2-way handshake.
- Done only upon initial link establishment.

Password Authentication Protocol (PAP)

- After the Link Establishment phase is complete, an Id/Password pair is repeatedly sent by the peer to the authenticator until authentication is acknowledged or the connection is terminated.
  - very simple but not particularly secure mechanism
- PAP is not a strong authentication method.
  - Passwords are sent over the circuit "in the clear",
  - No protection from playback or repeated trial and error attacks.
  - The peer is in control of the frequency and timing of the attempts.
- A requirement for most authentication systems is that PAP is a last resort
  - If a stronger authentication method (such as CHAP) is supported the system MUST offer to negotiate that method prior to PAP.

Challenge-Handshake Authentication Protocol (CHAP)

- CHAP is used to periodically verify the identity of the peer using a 3-way handshake.
- This is done upon initial link establishment,
- MAY be repeated anytime after the link has been established.

CHAP

1. After the Link Establishment phase is complete, the authenticator sends a "challenge" message to the peer.
2. The peer responds with a value calculated using a "one-way hash" function.
3. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged; otherwise the connection SHOULD be terminated.
4. At random intervals, the authenticator sends a new challenge to the peer, and repeats steps 1 to 3.

Hash functions

- A trapdoor function
  - Given a particular value X, a hash system does a one-way transformation to produce the hash f(X)
  - Knowing f(X) it is impossible to determine X
  - A small change in X leads to a big change in f(X)
    - On average, a single bit change in X should change 50% of the bits in f(X)
- MD5, SHA-1 and SHA-2 are well known and commonly used hash functions
  - 128 bits for MD5; 160 bits for SHA-1.
  - SHA-2 is a family of functions able to generate hashes of 224, 256, 384 or 512 bits

SHA-1

Philip	d9acbb0d8ec837efe80c92fc791abd04ea27d57a
Philip (space appended)	25dbd5be5294338381feb46d4f9f56accbd66cf7
Philip.	cd4e7cf17d3327ef9d05ac67c9bdc082c5c90c32
Phillip	95021406637b46dbf42b5b83a5dcf5ba4f1137f1

Network Access Server (NAS)

- For most networks, access beyond the PPP termination point is controlled by a NAS
- The NAS is a gateway to guard access to the Internet
- The client connects to the NAS (typically by PPP). The NAS then connects to another resource asking whether the client's supplied credentials are valid. Based on that answer the NAS then allows or disallows access to the Internet or whatever service is being requested.
- The NAS usually contains no information about what clients can connect to or what credentials are valid. All the NAS does is send the credentials the client supplied to a resource which does know how to process the credentials.
  - Usually a RADIUS server

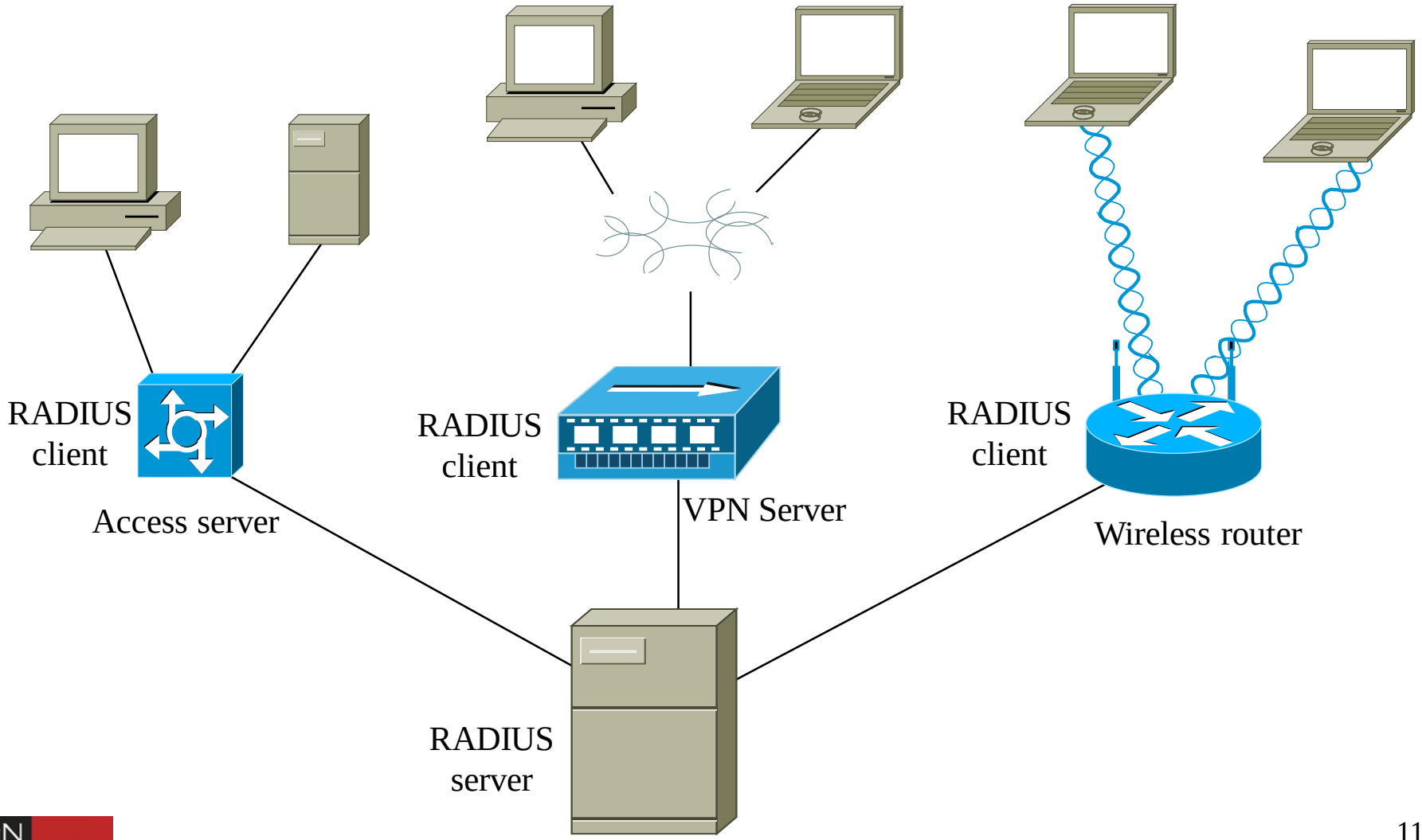
Remote Access Dial-In User Service (RADIUS)

- Used in association with a network access server for authentication of users
- Client server model
  - NAS is a client of the RADIUS server
- Receives user connection requests
  - Authenticates users
- Works with PAP and CHAP
- RFC2865
- RADIUS can be used with a any server requiring authentication including VPN servers or Wireless Access Points

Operation of RADIUS

1. User connects to NAS with PPP and initiates authentication by the NAS
2. NAS communicates with RADIUS for authentication details
3. NAS asks client for ID and Password (PAP) or response to challenge phrase (CHAP)
4. User replies
5. RADIUS client on NAS sends ID and password (PAP) or challenge response (CHAP) to server
6. RADIUS server responds with Accept, Reject or Challenge
7. The RADIUS client on the NAS either accepts or rejects the authentication request from the user based on the RADIUS response

RADIUS and NAS



DIAMETER

- A development of RADIUS
  - Twice as good ☺
- Diameter is not directly backwards compatible to RADIUS but can be upgraded from RADIUS
- The main differences between RADIUS and DIAMETER :
  - it uses reliable transport protocols (TCP or SCTP, not UDP)
  - it uses transport level security (IPSEC or TLS)
  - it has transition support for RADIUS
  - it has larger address space for AVPs (Attribute Value Pairs) and identifiers (32-bit instead of 8-bit)
  - it is a peer-to-peer protocol, not client-server
    - supports server-initiated messages

DIAMETER

- Differences with RADIUS (Cont)
  - both stateful and stateless models can be used
  - it has dynamic discovery of peers (using DNS SRV and NAPTR)
  - it has capability negotiation
  - it supports application layer acknowledgements, defines failover methods and statemachines (RFC3539)
  - it has error notification
  - it has better roaming support
  - it is easier to extend
    - new commands and attributes can be defined
  - basic support for user-sessions with accounting built in

Conclusion

- Authentication
- Passwords and pass-phrases
- PPP authentication
- RADIUS and DIAMETER