


Bringing British
Education to You
www.nccedu.com

Network Security and
Cryptography

Topic 7:
Authentication

V1.0

© NCC Education Limited



Bringing British
Education to You
www.nccedu.com

Network Security and
Cryptography

Topic 7 – Lecture 1:
An Overview of Authentication and Passwords

V1.0

© NCC Education Limited

Authentication Topic 7 - 7.3

Scope and Coverage

This topic will cover:

- Overview of Authentication
- Passwords
- Multi-factor Authentication
- Biometrics



Bringing British
Education to You
www.nccedu.com

V1.0


© NCC Education Limited

Authentication Topic 7 - 7.4

Learning Outcomes

By the end of this unit students will be able to:

- Explain the different authentication mechanisms;
- Describe multifactor authentication;
- Describe biometrics and their issues.


 Bringing British Education to You
www.nccedu.com

V1.0 © NCC Education Limited

Authentication Topic 7 - 7.5

Authentication Overview

- We are taking a network-based view of user authentication
- User authentication is the first line of defence of a network
- It aims to prevent unauthorised access to a network
- It is the basis of setting access controls
- It is used to provide user accountability


 Bringing British Education to You
www.nccedu.com

V1.0 © NCC Education Limited

Authentication Topic 7 - 7.6

Verifying User Identity

- User authentication has two steps:
 - **Identification** – presenting the user to the security system
 - **Verification** – providing information that binds the entity to the identity
- Identification is the means by which a user claims to be a specific identity
- Verification is the method used to prove that claim

 Bringing British Education to You
www.nccedu.com

V1.0 © NCC Education Limited

Authentication Topic 7 - 7.7

Means of Authentication

- Something the individual knows
 - E.g. password, PIN
- Something the individual possesses (tokens)
 - E.g. cryptographic key, smartcard
- Something the individual is
 - E.g. fingerprint, retina
- Something the individual does
 - E.g. handwriting pattern, speech pattern

V1.0 NCC Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.8

Authentication Problems

- Guess or steal passwords, PIN, etc
- Forget passwords, PIN
- Steal or forge smartcards
- Lose smartcard
- False positives in biometrics
- False negatives in biometrics
- The most common method of network authentication uses passwords and cryptographic keys

V1.0 NCC Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.9

Smartcards


- Tamper-resistant devices
- Have a small amount of memory
- Have a small processor
 - Simple computations, e.g. encryption/decryption, digital signatures
- Difficult to duplicate
- Easily transferable
- Can be used with PIN/password

V1.0 NCC Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.10

Smartcard Examples


- Bank/ATM cards
- Credit cards
- Travel cards
- Pass cards for a workplace

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.11

Passwords


- Most common means of authentication
- Require no special hardware
- Typical authentication by password
 1. User supplies a username and password
 2. System looks up the username in the relevant database table
 3. Checks that username, password pair exists
 4. Provides system access to the user

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.12

Password Strength

- Users tend to pick weak passwords if allowed
- Easy to crack via dictionary attack
- Users can be forced to create more complex passwords
- System can supply users with a strong password
- Many users will write down a stronger password and this can be a greater security risk than a weak password

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.13

Attacks on Password Security

- Eavesdropping may allow an attacker to “listen” in and gain password information
 - Encrypting messages will prevent this
- A direct attack on the database storing passwords can be used to discover or change passwords
- Sessions can be hijacked the attacker disconnects the user but remains connected themselves
- ***Never use the same password for different applications***

V1.0 NCC Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.14

Losing Passwords

- Not uncommon for a user to lose or forget a password
- Can be dealt with by regularly changing passwords
- Password generators can be used to change passwords
 - Automatically generate new passwords based upon a master secret

V1.0 NCC Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.15

Challenge - Response

- Systems are used that request specific characters in a password rather than the whole password.
- Commonly used in online banking
- Example
 - The password is “MyPassword”
 - The system asks for the 2nd, 3rd and 8th characters
 - The user enters “y”, “P” and “o”
- The idea is that it would take an eavesdropper many sessions to determine the whole password

V1.0 NCC Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.16

Hash Functions

- A database of plaintext passwords makes stealing all passwords more likely
 - Sony!!
- A level of protection is supplied by using a one-way hashing function on the passwords
 - Public function
 - Easy to compute
 - Hard to invert
- All passwords stored in the database are encrypted

V1.0 NCC Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.17

Hashing Passwords

- MD5 and SHA-1 are commonly used hashing algorithms
- User sends a username, password pair to the system
- The system hashes the password
- The database stores a username, $h(\text{password})$ pair
 - $h(\text{password})$ is the result of applying the hashing function to the password


V1.0 NCC Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.18

Cracking Hashed Passwords

- Hashing works on the principal that it would take a very long time to crack the hashed password via trial and error
- If users use short and simple passwords this is not the case
- Strong passwords are still required for the hashing function to provide a good level of security

V1.0 NCC Bringing British Education to You www.nccedu.com © NCC Education Limited



Bringing British
Education to You
www.nccedu.com

Network Security and Cryptography

Topic 7 – Lecture 2:
Multifactor Authentication and Biometrics

V1.0 © NCC Education Limited

Authentication Topic 7 - 7.20

Multi-Factor Authentication

- An identity is verified and authenticated using more than one verification method
- User/password authentication is single factor authentication
 - Only one verification method, the password
- A stronger form of identity verification
- Used for applications where security is more important
 - E.g. bank ATM – card and PIN

V1.0 © NCC Education Limited

Authentication Topic 7 - 7.21

Multi-Factor Systems

- This does not mean using two or three different passwords but two or three different methods
- ATM – Two-factor authentication
 - Something you possess – bank card
 - Something you know – PIN
- Three-factor systems exist for financial transactions via mobile phone
 - Something you possess – mobile phone
 - Something you know – PIN
 - Something you do – voice recognition

V1.0 © NCC Education Limited

Authentication Topic 7 - 7.22

Disadvantages

- Cost
 - Cost of supplying smartcards, USB tokens, etc.
 - Cost of hardware/software to read the tokens
- Inconvenience
 - Users may not like the inconvenience of having to carry around a token
- A balance has to be made between the cost and inconvenience of security and the sensitivity of the data and transactions being protected

Bringing British Education to You
www.nccedu.com


V1.0

© NCC Education Limited

Authentication Topic 7 - 7.23

Increased Security - Probability

- Combining two or more verification methods greatly decreases the probability of randomly producing the correct verification information
- Voiceprint
 - There is around a 1 in 10000 chance of matching
- PIN
 - There is a 1 in 10000 chance of guessing a PIN
- Combined
 - There is a 1 in 100,000,000 chance of matching both

Bringing British Education to You
www.nccedu.com


V1.0

© NCC Education Limited

Authentication Topic 7 - 7.24

Biometrics

- Automated methods used to recognise the unique characteristics of humans
- Uses one or more traits:
 - Physical traits (static biometrics)
 - Behavioural traits (dynamic biometrics)
- Biometric authentication aims to provide a non-transferable authentication method
 - Someone else could use your ATM card
 - Can someone else use your finger?

Bringing British Education to You
www.nccedu.com

V1.0

© NCC Education Limited

Authentication Topic 7 - 7.25

Biometric Types

- Physical characteristics:
 - Fingerprints
 - Retinas
 - Irises
 - Facial patterns
 - Hand measurements
- Behavioural characteristics
 - Signature
 - Typing patterns
 - Voice recognition

V1.0 NCC Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.26

Registering Biometric Data

- User registers with the biometric system
- Measurements of biometric data are taken
- Can take several measurements of biometric data if required
- Algorithm is applied to the measurement to obtain a template
- Template is stored in a database

V1.0 NCC Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.27

Authenticating Biometric Data


- User identifies themselves to the system (e.g. username)
- Biometric data measurement of the user is taken
- Again processed into a digital template
- This template is compared to template in database
- See if there is a match
- Matching process is approximate
- If biometric data matches the stored template the user is authenticated

V1.0 NCC Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.28

Matching Biometric Data


- Not an exact science
 - No two measurements of biometric data will match exactly
- Multiple measurements are taken when a user first enrolls in the system
- Matching with template is a success
- Tolerances are built into the algorithm that matches the templates

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.29

Fingerprints


- Fingertips have ridges and valleys that are unique to that fingertip
 - Used by police for a long time
- Most common biometric method
- Available for laptops and PCs
- Access to systems provided via touch technology

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.30

Face Recognition

- Capture facial image in the visible spectrum
 - Use a standard camera
 - Use central portion of face
 - Extract features that remain constant over time
 - Avoid changing features, e.g. hair
- An alternative version captures an infra-red image of the heat emitted by a face
- Most users accept use of such systems
- Problems caused by lighting, masks, etc.

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.31

Speech Recognition

- Some features of speech differ between individuals
- These patterns produced reflect the anatomy of the speaker
- These patterns reflect the patterns of speech learned as a result of:
 - Location
 - Peers
 - Language

V1.0 NCC Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.32

Iris Recognition

- Iris is the coloured area around the pupil
- Iris patterns are thought to be unique
- Video systems are used to capture an image of the iris
- Becoming economically viable as equipment prices have lowered
- Works with glasses and contact lenses

V1.0 NCC Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.33

Hand Geometry


- Can utilise measures of fingers or whole hands
 - Length
 - Width
 - Thickness
 - Surface area
- Used for access control in commercial and residential premises

V1.0 NCC Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.34

Written Signatures


- Uses measurement of the way the signature is written not just the final signature
- Can measure a range of parameters:
 - Speed
 - Pressure
 - Angle of writing
- Used in business applications where a signature is commonly used to identify a user

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.35

Typing Patterns


- Similar to the recognition of written signatures
- Uses a standard keyboard
- Recognises the password that is typed
- Recognises the way the password is typed:
 - Intervals between characters
 - Speed of typing

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.36

Errors in Biometric Systems

- Has a **false accept rate** (FAR): measures the rate at which an invalid user is accepted by the system
- Has a **false rejection rate** (FRR): measures the rate at which a valid user is rejected by the system
- In many systems it is possible to adjust both rates by changing some variables
- In modern systems both rates are low

V1.0  Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.37

Concerns with Biometric Systems

- **Privacy**
 - All transactions in different systems are linked to a real identity
 - For passwords etc. different identities can be presented to different systems
- **Injury**
 - Hygiene concerns about equipment
 - Criminals chopping off fingers to use!!
- **Exclusion**
 - An amputee may have no fingers

V1.0 NCC Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.38

The Market Leader

- Fingerprint authentication is widely used
- Laptops and computer peripherals come with built-in fingerprint readers
- They are relatively inexpensive
- Allow user to authenticate by putting finger on the reader
- May be used with a password or PIN for two-factor authentication.

V1.0 NCC Bringing British Education to You www.nccedu.com © NCC Education Limited

Authentication Topic 7 - 7.39

References


- Stallings, W. (2010). *Cryptography and Network Security: Principles and Practice*. Pearson Education.
- Scambrey, J., McClure, S. and Kurtz, J. (2001). *Hacking Exposed: Network Security Secrets & Solutions, 2nd Edition*. McGraw Hill.

V1.0 NCC Bringing British Education to You www.nccedu.com © NCC Education Limited


Authentication Topic 7 – 7.40

Topic 7 – Authentication

Any Questions?



Bringing British
Education to You
www.nccedu.com



V1.0

© NCC Education Limited
