12 ஆம் வகுப்பு – கணினி பயன்பாடுகள்

பாடம் 17.

மின்-வணிக பாதுகாப்பு அமைப்புகள்

Prepared by,

J. Kavitha, B.Sc,B.Ed, M.C.A,M.Phil.,

Computer Instructor Gr - I,

GHSS, S.S.KULAM,

Coimbatore.

கற்றலின் நோக்கங்கள்

- மின்-வணிக பாதுகாப்பு அமைப்புகளின் அடிப்படைகளைத் தெரிந்து கொள்ளுதல்
- பல்வேறு வகையான மின்-வணிக அச்சுறுத்தல்களை புரிந்து கொள்ளுதல்
- மின்-வணிக பாதுகாப்பின் பரிமாணங்கள் பற்றி அறிந்து கொள்ளுதல்
- மின்-வணிக பரிமாற்றத்தில் பாதுகாப்பு தொழில்நுட்பங்கள் பற்றி அறிந்து கொள்ளுதல்

அறிமுகம்

- இணையத்தின் வேகமான வளர்ச்சியுடன், இணையதள பரிவர்த்தனைகள் முக்கிய வர்த்தக மாதிரியாக மாறிவிட்டன. இணைய வளங்களை அடிப்படையாக கொண்ட மின்-வணிக பரிவர்த்தனைகளை பொதுமக்கள் ஏற்றுக் கொள்ளத் தொடங்கியுள்ளனர்.
- இணைய பரிவர்த்தனைகளால் ஏற்படும் வசதியைப் பயன்படுத்தும் போது, பரிமாற்றங்களின் பாதுகாப்பு மிகவும் கவனத்தை ஈர்த்துள்ளது. எந்த ஒரு வளர்ந்துவரும் மின் வணிகத்திற்கும் பாதுகாப்பு முக்கியக் காரணியாக உள்ளது.

மின்-வணிக பாதுகாப்பு

- மின்-வணிக பாதுகாப்பு என்பது இணையம் மூலம் மின்-வணிக பரிவர்த்தவனைகளை பாதுகாப்பாக வழிநடத்தும் நெறிமுறைகளைக் கொண்ட ஒரு தொகுப்பு ஆகும்.

மின்-வணிக அச்சுறுத்தல்கள்

நச்சுநிரல்:

- நச்சுநிரல், கணினிகளுக்கு தீங்கு விளைவிக்கிறது. அதன்மூலம், மின்-வணிகத்தின் செயல்திறன் மற்றும் சீரான செயல்பாட்டில் பாதிப்பை ஏற்படுத்துகிறது.
- சில நச்சுநிரல்கள் கணினியில் சேமித்து வைக்கப்பட்டுள்ள அனைத்து தகவல்களையும் அழித்து, பெரிய அளவில் வருவாய் மற்றும் நேர விரயத்தை ஏற்படுத்துகின்றன.

மின்-வணிக பாதுகாப்பு அச்சுறுத்தல் வகைகள்

தகவல் கசிவு (Information Leakage):

- மின்-வணிகத்தில் வர்த்தக ஆவண இரகசியங்கள்,
  - விற்பனையாளர் மற்றும் வாடிக்கையாளருக்கு இடையிலான பரிமாற்றத்தின் உள்ளடக்கம் மூன்றாம் தரப்பினரால் திருடப்படுவது,
  - வணிகர் அல்லது வாடிக்கையாளரால் வழங்கப்பட்ட ஆவணங்கள் மற்றவரால் சட்ட விரோதமாக பயன்படுத்துவது.
- இவ்வாறு மின் ஆவணங்களை இடைமறித்து திருடுதல் தகவல்கசிவு என அழைக்கப்படுகிறது.

மின்-வணிக பாதுகாப்பு அச்சுறுத்தல் வகைகள்

தரவு சிதைப்பு (Tampering):

- தரவுகளின் நம்பகத்தன்மை மற்றும் நேர்மை தொடர்பான பிரச்சினை மின்-வணிகத்தின் முக்கிய சிக்கலாக உள்ளது.
- இணையத்தின் வழியாக தரவுகளைப் பரிமாறும் போது ஹேக்கர்களால் அத்தரவுகள் பல்வேறு தொழில்நுட்பங்கள் வாயிலாக தவறானதாக மாற்றி இலக்கு கணிப்பொறிக்கு அனுப்பப்படுகிறது. இதன் மூலம் தரவுகளின் நம்பகத்தன்மை சிதைக்கப்படுகிறது.

மின்-வணிக பாதுகாப்பு அச்சுறுத்தல் வகைகள்

ஃபிஷிங் (Phishing):

- ஃபிஷிங் என்பது ஒரு வகை மின் - வணிக அச்சுறுத்தலாகும். தனிநபர் நம்பற்குரியவர் போல் வேடமிட்டு உள்நுழைவு சான்றுகளை போன்ற முக்கியமான தரவை தொலைபேசி, எஸ்எம்எஸ், மின்னஞ்சல் அல்லது சமூக ஊடகங்கள் மூலம் அடைவது ஆகும்.

மின்-வணிக பாதுகாப்பு அச்சுறுத்தல் வகைகள்

சைபர் squatting (Cyber Squatting):

- இது புகழ்பெற்ற வர்த்தக முத்திரைகள் மற்றும் வணிகப் பெயர்களை குறிப்பிட்ட நிறுவனம் தங்களது களப்பெயர்களாக பதிவு செய்யும் சட்டவிரோத நடைமுறையாகும். மேலும் சைபர் squatting என்பது ஒரு புகழ் பெற்ற / நற்பெயர் பெற்ற நிறுவனத்தின் பெயரில் போலி வலைப்பக்கத்தை உருவாக்கி நிறுவனத்தின் அதிகாரபூர்வ வலைப்பக்கம் என நம்பச் செய்து வாடிக்கையாளரை ஏமாற்றும் செயல் ஆகும்.

மின்-வணிக பாதுகாப்பு அச்சுறுத்தல் வகைகள்

டைபோபைரஸி:

- டைபோபைரஸி என்பது சைபர் squatting ன் ஒரு வகையாகும். சில போலி வலைத்தளங்கள் பயனர்களின் பொதுவான தட்டச்சு பிழைகளை பயன்படுத்தி அவர்களை தங்கள் வலைத்தளத்திற்கு திசை திருப்ப பிரபலமான களப்பெயர் போன்றே தங்கள் வலைத்தளத்திற்கு பெயரிடுகின்றனர்.

  எ.கா: www.goggle. com, www.faceblook.com

மின்-வணிக பாதுகாப்பு அச்சுறுத்தல் வகைகள்

ஹேக்கிங்:

- ஹேக்கிங் என்பது கணிப்பொறி அல்லது வலையமைப்பிற்குள் அங்கீகரிக்கப்படாத ஊடுருவலை குறிக்கிறது.
- அதாவது சட்டவிரோதமாக கணிப்பொறியின் பாதுகாப்பு அரணை உடைத்து, இணையதளத்தில் உள்புகுதல் மற்றும் இரகசிய தகவலை இடைமறித்தல் செயல் ஆகும்.

மின்-வணிக பாதுகாப்பின் பரிமாணங்கள்

- அங்கீகாரம்: தரவு மூலத்தை அங்கிகரித்தல் மற்றும் பங்கேற்பாளர்களின் அடையாளத்தை சரிபார்த்தல்.
- இருப்பு: தரவு தாமதம் அல்லது நீக்கத்தை தடுத்தல்.
- முழுமை: அனைத்து வர்த்தகத் தகவல்களையும் ஒன்றிணைத்தல்.
- இரகசியத்தன்மை: அங்கீகரிக்கப்படாத நபர்களிடமிருந்து தரவை பாதுகாத்தல்
- திறனுடைமை: வன்பொருள், மென்பொருள் மற்றும் தரவை முழுமையாகவும் திறம்படவும் கையாளுதல்.

மின்-வணிக பாதுகாப்பின் பரிமாணங்கள்

- நேர்மை: அங்கீகரிக்கப்படாத தரவு மாற்றத்தை தடுத்தல்.
- மறுதலிக்கப்படாதிருத்தல்: உடன்படிக்கை மீறாதிருத்தல்.
- தனியுரிமை: வாடிக்கையாளர்களின் தனிப்பட்ட தரவுகளை பிறர் பயன்படுத்தாமல் தடுத்தல்.
- நம்பகத்தன்மை: தனிநபர்கள் அல்லது நிறுவனங்களின் நம்பகத்தன்மையை அடையாளங்காணல்.
- மீளாய்வு திறன்: தணிக்கை நடவடிக்கைகள் மற்றும் வணிகச் செயல்பாடுகளை கண்காணிக்கும் திறன்.

மின்-வணிகத்தின் பல்வேறு வகையான பாதுகாப்புத் தொழில்நுட்பங்கள்

- மின்-வணிக பரிவர்த்தனைகளில் பாதுகாப்பை உறுதிப்படுத்த அதிநவீன பாதுகாப்பு தொழில்நுட்பங்கள் தேவைப்படுகின்றன.
- தற்சமயம் மின்-வணிக பரிவர்த்தனையில் உள்ள பாதுகாப்பு தொழில்நுட்பங்கள் பின்வருமாறு வகைப்படுத்தப்பட்டுள்ளன. அவை,
  - குறியாக்கத் தொழில்நுட்பம் (Encryption technology)
  - அங்கீகார தொழில்நுட்பம் (Authentication technology)
  - பாதுகாப்பு அங்கீகார நெறிமுறைகள் (Authentication protocols)

குறியாக்கத் தொழில்நுட்பம்
(ENCRYPTION TECHNOLOGY)

- குறியாக்கத் தொழில்நுட்பம் என்பது ஒரு செயல்திறன் மிக்க தகவல் பாதுகாப்பு அமைப்பாகும்.
- குறியாக்க வழிமுறைகளைப் பயன்படுத்தி ஒரு மூல உரையை அர்த்தமற்ற மறை எழுத்து உரையாக மாற்றுவது குறியாக்கம் என்று வரையறுக்கப்படுகிறது.
- இரண்டு குறியாக்க தொழில்நுட்பங்கள் பரவலாகப் பயன்படுத்தப்படுகின்றன. அவை,

  1. சமச்சீர் குறியீடு குறியாக்கம்,
  2. சமச்சீரற்ற குறியீடு குறியாக்கம்.

குறியாக்கத் தொழில்நுட்பம்
(ENCRYPTION TECHNOLOGY)

சமச்சீர் குறியீடு குறியாக்கம்:

- தரவு குறியாக்க தர நிலை (Data Encryption Standard - DES) ஒரு சமச்சீர் குறியீடு குறியாக்க நெறிமுறை ஆகும். சமச்சீர் குறியீடு குறியாக்கம், மறைகுறியாக்கம் மற்றும் குறியாக்கம் இரண்டிற்கும் ஒரே குறியீடு பயன்படுத்தப்படுகிறது
- சமச்சீர் குறியீடு குறியாக்கம் வழிமுறைகள் ஒரு குறியீட்டை மட்டுமே பயன்படுத்துவதால், கோட்பாட்டின் படி, குறியாக்கம் செய்வதற்கு பயன்படுத்தப்பட்ட துல்லியமான குறியீட்டை அறிந்தவர்கள் மட்டுமே மறை குறியாக்கம் செய்ய முடியும்.

குறியாக்கத் தொழில்நுட்பம்
(ENCRYPTION TECHNOLOGY)

சமச்சீரற்ற குறியீடு குறியாக்கம்:

- சமச்சீரற்ற குறியீடு குறியாக்கம் பொது குறியீடு குறியாக்கம் என்றும் அழைக்கப்படுகிறது.
- இது பொது குறியீடு மற்றும் எண்முறைச் சான்றிதழ்களை பயன்படுத்துகிறது.
- சமச்சீர் குறியாக்கம் போலில்லாமல், சீரற்ற குறியாக்கத்தில் தகவல் பரிமாற்றம் செய்யும் நபர்களுக்கு மற்றவரின் தனிப்பட்ட குறியீடு தெரிந்திருக்க வேண்டியதில்லை.
- RSA, DSS போன்ற நெறிமுறைகள் சமச்சீரற்ற குறியீடு குறியாக்க தொழில்நுட்பங்களை பயன்படுத்துகின்றன.

சமச்சீர் குறியீடு குறியாக்கம் மற்றும் சமச்சீரற்ற குறியீடு குறியாக்கம் - வேறுபாடு

சமச்சீர் குறியீடு குறியாக்கம்	சமச்சீரற்ற குறியீடு குறியாக்கம்
மறைகுறியாக்கம் மற்றும் குறியாக்கம் இரண்டிற்கும் ஒரே குறியீடு பயன்படுத்தப்படுகிறது	மறைகுறியாக்கம் மற்றும் குறியாக்க இரண்டிற்கும் வெவ்வேறு குறியீடுகள் பயன்படுத்தப்படுகிறது.
மறைகுறியாக்கம் அல்லது குறியாக்கத்தின் வேகம் மிக அதிகம்	மறைகுறியாக்கம் அல்லது குறியாக்கத்தின் வேகம் குறைவு.
தெளி உரை மற்றும் மறைக்குறியீட்டு உரை இரண்டும் ஒரே அளவானதாக இருக்கும்	தெளி உரை மற்றும் மறைக்குறியீட்டு உரையின் அளவு வெவ்வேறானதாக இருக்கும்
DES, AES, RC4 போன்ற நெறிமுறைகள் சமச்சீர் குறியீடு குறியாக்க தொழிநுட்டபத்தை பயன்படுத்துகின்றன.	RSA, ECC, DSA போன்றநெறிமுறைகள் சமச்சீரற்றகுறியீடு குறியாக்க தொழிநுட்டபத்தை பயன்படுத்துகின்றன.
இது தரவுகளுக்கு இரகசியத்தன்மையை வழங்குகிறது	இது இரகசியத்தன்மை, அங்கீகாரம் மற்றும் மறுதலிக்கப்படாதிருத்தல் போன்ற நன்மைகளை வழங்குகிறது
பயனரின் எண்ணிக்கையை பொருத்து பயன்படுத்தப்படும் குறியீடுகளின் எண்ணிக்கை அடுக்குகளில் அதிகரிக்கிறது	பயனரின் எண்ணிக்கையை பொருத்து பயன்படுத்தப்படும் குறியீடுகளின் எண்ணிக்கை நேர்கோட்டில் அதிகரிக்கிறது

அங்கீகார தொழில்நுட்பம்
(AUTHENTICATION TECHNOLOGY):

- நம்ப கத்தன்மை, நேர்மை மற்றும் மறுதலிக்கப்படாதிருத்தல் ஆகியவற்றை உறுதி செய்வது அங்கீகார தொழில்நுட்பத்தின் முக்கிய பணியாகும். இதனை

  1. எண்முறைச் சான்றிதழ்கள் மற்றும்
  2. எண்முறைக் கையொப்பம் மூலம் அடையலாம்.

அங்கீகார தொழில்நுட்பம்
(AUTHENTICATION TECHNOLOGY):

எண்முறைச் சான்றிதழ்:

- ஒரு எண்முறைச் சான்றிதழ் என்பது ஒருவரது பொது குறியீட்டின் உரிமையை நிரூபிக்க பயன்படுத்தப்படும் ஒரு மின்னணு ஆவணம் ஆகும்.
- இந்த சான்றிதழில் அனுப்புநரின் அடையாளம் பற்றிய தகவல்கள், அனுப்புநரின் எண்முறைக் கையொப்பம் மற்றும் அவரின் பொது குறியீடு போன்ற தகவல்கள் அடங்கியிருக்கும்.
- எண்முறை சான்றிதழ் அங்கீகரிக்கப்பட்ட சான்றளிப்பு அதிகாரிகளால் (Certification Authorities - CA) வழங்கப்படுகின்றது. Pretty Good Privacy (PGP) மற்றும் X.509 ஆகியவை புகழ்பெற்ற எண்முறைச் சான்றிதழ் வகைகள் ஆகும்.

அங்கீகார தொழில்நுட்பம்
(AUTHENTICATION TECHNOLOGY):

எண்முறைக் கையொப்பம்:

- எண்முறைக் கையொப்பம் என்பது ஒரு குறிப்பிட்ட மின்னணு ஆவணம், செய்தி அல்லது பரிவர்த்தனை உண்மையானதா என சரிபார்க்கப் பயன்படும் ஒரு அமைப்பு ஆகும்.
- இது ஒரு பெறுநருக்கு தகவல், குறிப்பிட்ட அனுப்புநரால் தான் உருவாக்கப்பட்டது என்பதற்கான உத்தரவாதம் அளிக்கிறது.

பாதுகாப்பு அங்கீகார நெறிமுறைகள் (AUTHENTICATION PROTOCOLS)

- தற்போது மின்-வணிகத்தில்,

  1. பாதுகாப்பான மின்னணு பரிவர்த்தனை மற்றும்

  2. பாதுகாப்பான சாக்கெட் அடுக்கு

- ஆகிய இரண்டு வகையான பாதுகாப்பு அங்கீகார நெறிமுறைகள் பயன்படுத்தப்படுகின்றன.

பாதுகாப்பு அங்கீகார நெறிமுறைகள் (AUTHENTICATION PROTOCOLS)

பாதுகாப்பான மின்னணு பரிவர்த்தனை (Secure Electronic Transaction - SET):

- பாதுகாப்பான மின்னணு பரிவர்த்தனை என்பது, இணையம் வழியாக கடன் அட்டை மூலம் மின்னணு பணம் செலுத்தல்களுக்கான பாதுகாப்பு நெறிமுறை ஆகும்.
- SET இன் செயலாக்கம் எண்முறைக் கையொப்பம் மற்றும் பரிமாற்ற தரவின் குறியாக்கம் ஆகியவற்றின் அடிப்படையில் செயலாக்கப்படுகிறது. மேலும் தனியுரிமையை உறுதிப்படுத்த, இரட்டைக் கையொப்பங்களையும் பயன்படுத்துகிறது.
- இது GTE, IBM, மைக்ரோ சாப்ட் மற்றும் நெட்ஸ்கேப்பின் பங்களிப்புடன், 1996 ல் விசா மற்றும் மாஸ்டர்கார்டு நிறுவனங்களால் உருவாக்கப்பட்டது.

பாதுகாப்பு அங்கீகார நெறிமுறைகள் (AUTHENTICATION PROTOCOLS)

பாதுகாப்பான சாக்கெட் அடுக்குகள் (Secure Sockets Layers - SSL):

- மிகவும் பொதுவான மறைகுறியீட்டியல் நெறிமுறை பாதுகாப்பான சாக்கெட் அடுக்குகள் (Secure Sockets Layers - SSL) ஆகும்.
- SSL என்பது இணைய பரிமாற்றங்களைப் பாதுகாப்பதற்காகன ஒரு கலப்பு குறியாக்க நெறிமுறை ஆகும்.
- இது இணையத்தில் தரவு பரிமாற்றத்தின் பாதுகாப்பை உறுதிப்படுத்துவதற்கான பொது குறியீடு குறியாக்கவியல் செயல்முறையின் அடிப்படையில் அமைந்துள்ளது.
- இதன் நோக்கம் ஒரு அங்கீகார நடவடிக்கைக்கு பிறகு முனையம் மற்றும் சேவையகம் இடையே ஒரு பாதுகாப்பான தகவல் தொடர்பு தடத்தை நிறுவுவது ஆகும்.

பாதுகாப்பு அங்கீகார நெறிமுறைகள்
(AUTHENTICATION PROTOCOLS)

பாதுகாப்பான சாக்கெட் அடுக்குகள் (Secure Sockets Layers - SSL):

- இன்று, சந்தையில் உள்ள அனைத்து உலாவிகளும் SSL நெறிமுறையை ஆதரிக்கின்றன.
- மேலும் பெரும்பாலான பாதுகாப்பான தகவல்தொடர்புகள் இந்த நெறிமுறை மூலமே தொடர்கின்றன.
- பயனர் செய்ய வேண்டிய ஒரே செயல் http:// க்கு பதிலாக https:// உடன் தொடங்குவது மட்டுமே. “s” (secured) என்பது, பாதுகாக்கப்பட்ட என்று பொருள்படுகிறது.

http மற்றும் https இடையேயான வேறுபாடு

3D பாதுகாப்பு பணபரிவர்த்தனை நெறிமுறைகள்

- 3D பாதுகாப்பு என்பது இணையத்தில் பாதுகாப்பாக கட்டணம் செலுத்த உதவும் நெறிமுறை ஆகும்.
- இது வலைத்தளம் மூலம் கொள்முதல் செய்யும் போது, கட்டண அட்டை வைத்திருப்பவரின் சிறந்த அங்கீகாரத்தை வழங்குகிறது.
- இந்த நெறிமுறையின் அடிப்படைக்கருத்து, நிதி அதிகாரமளித்தல் செயல்முறையை ஒரு நிகழ்நிலை சான்றளிப்பு அமைப்புடன் இணைப்பதாகும்.
- இந்த சான்றளிப்பு மாதிரி 3 களங்களை உள்ளடக்கியது. அவை:

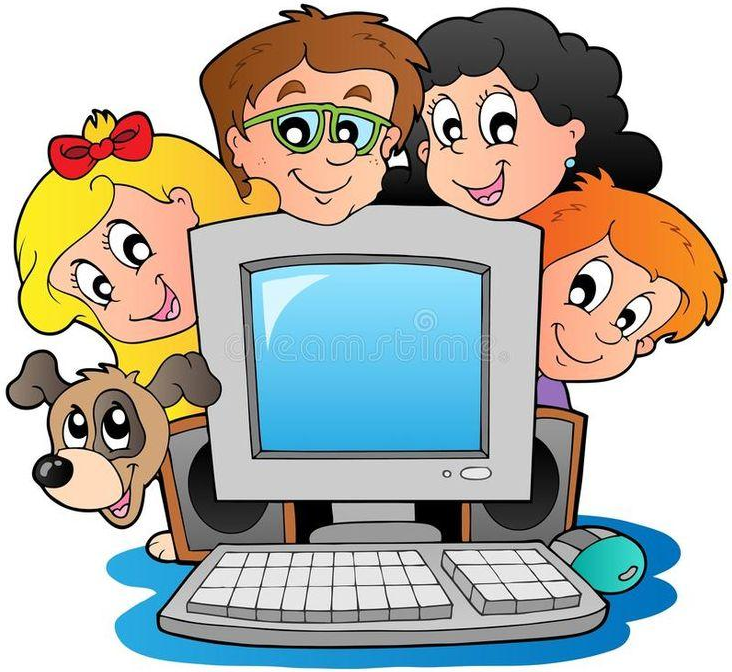
  1. பெறுநர் களம்
  2. வழங்குநர் களம்
  3. இயங்குதன்மை களம் ஆகும்.

முக்கிய வினாக்கள்

1. மின்-வணிக பாதுகாப்பு என்றால் என்ன?
2. ஏதேனும் இரண்டு மின்-வணிக பாதுகாப்பு அச்சுறுத்தல்களை பட்டியலிடுக.
3. மின்-வணிகத்தில் தகவல் கசிவு பற்றி எழுதுக.
4. டைபோபைரஸி பற்றி சிறுகுறிப்பு வரைக.
5. ஃபிஷிங் (Phishing) பற்றி எழுதுக.
6. மின்-வணிகத்தின் பல்வேறு வகையான பாதுகாப்புத் தொழில்நுட்பங்களை பட்டியலிடுக.
7. எண்முறைக் கையொப்பம் பற்றி எழுதுக.
8. எண்முறைச் சான்றிதழ் பற்றி குறிப்பு வரைக.
9. மூல உரை, மறை எழுத்து உரை பற்றி எழுதுக.
10. மின்-வணிக பாதுகாப்பின் பரிமாணங்கள் பற்றி எழுதுக.
11. சமச்சீர் குறியீடு குறியாக்கம் மற்றும் சமச்சீரற்ற குறியீடு குறியாக்கம் வேறுபாடுகளை எழுதுக.
12. பாதுகாப்பு அங்கீகார நெறிமுறைகள் பற்றி விவரி.

நன்றி!

கல்வி கற்பது தவம், அதை
கற்பிப்பது வரம்.
யார் கைவிட்டாலும், கற்றது
கைவிடாது உனை.
அக்கல்வியைப் பெற்று
சிறப்போடு வாழ
வாழ்த்துக்கள்.



ஜெ. கவிதா B.Sc, B.Ed, M.C.A, M.Phil.,
கணினி பயிற்றுநர் நிலை - I
அரசு மேல்நிலைப்பள்ளி,
சர்க்கார்சாமக்குளம்,
கோயம்புத்தூர் – 641107.