தகவல் பாதுகாப்பு மேலாண்மை - அறிவோம் வாரீகளா?

- **சுப. இரத்தினகிரி**

தகவல் தொழில்நுட்ப யுகமான இப்போதைய காலகட்டத்தில் தகவல் ஒரு சொத்தாகும். (Information Resource/Asset) அந்தத் தகவலைப் பாதுகாத்துக் கொள்வது என்பது மிக மிக அவசியமான ஒன்றாகும்.

கணினி மூலம் தகவல் பயன்படுத்தும்/பரிமாறிக்கொள்ளும் அனைவருமே தகவல் பாதுகாப்பு மேலாண்மை (Information Security Management) பற்றி அறிந்து கொள்ள வேண்டியது தேவையாகும்.

தகவல் பாதுகாப்பு மேலாண்மை என்பது என்ன?

முதலில் தகவலை ஏன் பாதுகாக்க வேண்டும்? என்று பார்ப்போம். தகவல் எப்போது சொத்தாகும்? அந்தத் தகவலின் மூலம் நமக்கு வணிக லாபம் கிடைக்குமாயின் அது சொத்தாகும் தானே? உதாரணமாக பெப்சி நிறுவனத்தில் என்னென்ன மூலப் பொருட்களை என்ன விகிதத்தில் கலந்தால் என்ன குளிர்பானம் வரும் என்பது ஒரு தகவல் ஆகும். அந்தத் தகவல் ஒரு பெரிய சொத்து தானே அந்த நிறுவனத்தைப் பொருத்தவரை?

சரி. தகவலைப் பாதுகாக்கிறேன் பேர்வழி என்று யாருக்கும் கிடைக்காமல் செய்து விட்டால் என்ன செய்வது?

எனவே நல்லதொரு தகவல் பாதுகாப்பு மேலாண்மையானது மூன்று பின்னப்பட்ட அடிப்படைத் தேவை/விஷயங்களைப் பூர்த்தி செய்வதாய் இருக்க வேண்டும்.

அவை யாவன:

1. சரியான தகவல்
2. சரியான நபர்
3. சரியான நேரம்

அதாவது சரியான தகவல், சரியான நபருக்குச் சரியான நேரத்தில் கிடைக்குமாறு செய்யவேண்டும். (Right Data to the Right Person at the Right Time)

இதில் ஏதேனும் ஒன்று மாறினால் கூட பெரும்பாதகம் விளையக் கூடும். உதாரணமாக சரியான நேரத்தில் சரியான தகவல் தவறான நபருக்குப் போய்ச் சேர்ந்தால் என்னாகும் யோசித்துப் பாருங்க!

"20 நபர்களால் 20 ஆண்டுகளாய்ச் செய்ய முடியாத தவறைக் கூட கணினியால் 2 விநாடிகளில் செய்து விட முடியும்" என்று மர்பி ஓரிடத்தில் சொல்வார்.

எனவே, கணினியில் நம் தகவல்களைப் பாதுகாக்க எத்தனை அரும்பாடு படவேண்டும் என்பது உங்களுக்கு விளங்கக் கூடும்.

இந்தக் கட்டுரையில் ஏதோ எனக்குத் தெரிந்தவரையில் தகவல் பாதுகாப்பு மேலாண்மை பற்றி பரிமாறிக் கொள்ள விழைகின்றேன்.

உங்களுக்கு நமது பாடத்திட்டத்தைச் சொல்லி விடுகின்றேன்.

முதலில் கள்ளர்களைப் பற்றித் தெரிந்து கொள்வோம். பின்னர் ஒவ்வொருவரையும் எப்படி எதிர்கொள்வது என்றும் அறிந்து கொள்வோம்.

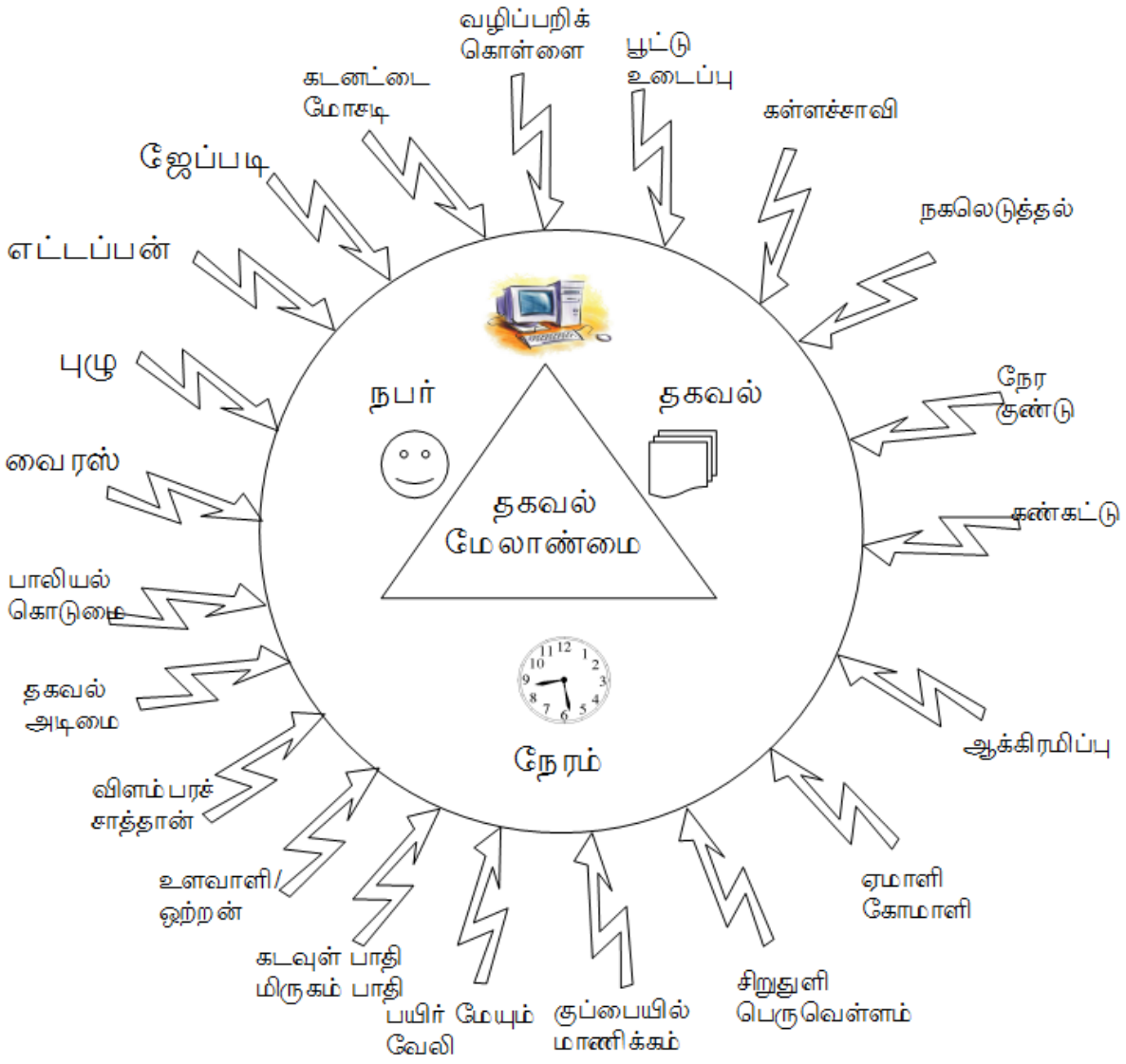
முதல் பாகத்திலேயே சொல்லக் கடமைப்பட்டிருப்பது இது தான்:

நான் ஒன்றும் கணினிப் பொறியாளன் அல்லன். நான் சொல்வதில் பல தவறுகள் இருக்கக் கூடும். அவற்றைப் பொறுத்தும் திருத்தியும் வழி நடத்துமாறு பெருந்தகைகளைப் பணிந்து கேட்டு இணைந்து கற்போம் என்றே இக்கட்டுரையை ஆரம்பிக்கின்றேன்.

சுப. இரத்தினகிரி

22-10-2007

கீழே இருக்கும் படத்தைப் பாருங்கள். உஸ்ஸ்ஸ்ஸ்ஸ். அப்பா, இப்பவே கண்ணைக் கட்டுதே என்கின்றீர்களா?



ஒவ்வொன்றாய்க் காண்போம்!

நான் மேலே கொடுத்துள்ள படம் முழுமையான பட்டியல் கொண்டது அல்ல. ஒரு மிகப் பெரிய பனிப்பாறையின் முனையினைப் பார்ப்பது போல் தான். நாம் எத்தனை பெரிய டைட்டானிக் கப்பலாய் இருந்தாலும் உடைக்கும் வல்லமையுடன் பனிப்பாறை வலிமையாய் இருக்கின்றது. எனவே நாம் ஒதுங்கிப் போவது தான் சாமர்த்தியம்.

இனி ஒவ்வொரு கள்ளர்களையும் வரிசையாய் நிறுத்தி அவர்கள் பண்பு என்ன, சாமர்த்தியம் என்ன என்று பார்ப்போம்.

மேலே கண்ட படத்தினை முதலில் எட்டப்பனில் ஆரம்பித்து கடிகார சுற்றில் முடிப்போம்!

1. எட்டப்பன் (Social Engineering)

முதலில் ஒரு உண்மைக்கதை:

சில ஆண்டுகளுக்கு முன் அடையாளம் தெரியாத சில நபர்கள், ஒரு மிகப் பெரிய கப்பல் நிறுவனத்தின் உள்ளே புகுந்து அந்த நிறுவனக் கணினியின் மொத்தத் தகவல்களையும் அபேஸ் செய்து விட்டுத் தப்பி விட்டனர். எப்படி முடிந்தது அவர்களால்?

சின்னச் சின்னச் செயல்களால் அந்த நிறுவனத்தில் இருக்கும் தொழிலாளிகளின் நம்பிக்கையைப் பெற்று அவர்களால் அலுவலகத்துள் நுழைய முடிந்தது. இரண்டு நாட்களாய் அவர்கள் அந்த நிறுவனத்தை முற்றிலுமாக வெளியிருந்தே கண்காணித்தனர். தொலைபேசியின் மூலம் பல்வேறு முறைகள் அழைத்து அங்கிருப்போரின் பெயர்களைக் கிரகித்துக் கொண்டனர். முன்வாசலின் முன் சாவியைத் தொலைத்தது போல் தேடி காவலாளிகளின் கவனத்தை ஈர்த்தனர். உள்ளிருப்பவரின் பெயரைச் சொன்னதும் காவலாளி உள்ளே விட்டார்.

மூன்றாவது மாடிக்குச் செல்கையில் தங்கள் அடையாள அட்டையை மறந்து வைத்து விட்டதாகச் சொன்னதுடன் பல அலுவலக ஊழியர்களின் பெயரையும் சர்வ சாதாரணமாக உச்சரித்தனர்.

சிறிது நேரத்திலேயே அந்த நிறுவனத்தின் நிதி நிர்வாக அதிகாரி (CFO) ஊரில் இல்லை என்று அறிந்து கொண்டனர். அங்கு சென்றால்

அவர்களுக்குக் கிடைத்தது லக்கி பிரைஸ். ஆம், அந்த அதிகாரியின் கணினிக்கு கடவுச்சொல் வைத்துப் பூட்ட வில்லை. அவர் கணினியில் தேவையான விபரங்கள் சிடியில் நகலெடுத்தனர். மேஜையைத் திறந்து பல நிர்வாகம் சம்பந்தப்பட்ட கோப்புக்களில் இருந்து காகிதங்களை எடுத்து கையோடு வெளியே வந்து இதைக் குப்பைத் தொட்டியில் போட வேண்டும் என்று ஊழியர் ஒருவருக்குத் தெரியும்படி அவர்களின் மேற்பார்வையுடனே காகிதங்களை வெளியேயும் கொண்டு வந்து விட்டனர்.

சிறிது நேரம் கழித்து கணினித் தொழில்நுட்பத் துறையில் அவர்களின் பிணையக் கடவுச்சொல்லை மறந்தது போல் அவசர அவசரமாய் CFO குரலில் பேசுவது போல் பேசி கடவுச்சொல்லை வாங்கிவிட்டனர். அவ்வளவு தான், அதன் பின் அவர்களிடம் இருந்த கணினி மென்பொருட்களின் மூலம் அந்த நிறுவனத்தின் மொத்தக் கணினித் தகவல் பரப்பையும் அவர்கள் கைக்குக் கொண்டு வந்தனர்.

இவர்கள் வேறு யாருமல்லர். அந்த CFO வே பணிக்கமர்த்திய பாதுகாப்பு தணிக்கையாளர்கள். அவர்கள் நியமிக்கப் பட்டது CFO தவிர வேறு யாருக்குமே தெரியாது. எத்தனை பாதுகாப்பாய் இருப்பினும் ஓட்டை எங்கிருக்கின்றது என்று கண்டுபிடிக்க அமர்த்தப்பட்டவர்கள்.

இனி, இது போன்றவர்கள் தவறான எண்ணத்துடன் வந்திருந்தால் என்ன ஆகியிருக்கும்?

இதைத் தான் எட்டப்பன் என்னும் பெயரில் அழைக்கின்றேன் நான்!

அதாவது நம்மிடம் நைச்சியமாகப் பேசி, தகவல்களை/கடவுச்சொல்லைக் கறந்து நமக்கு பெருந்தீங்கு விளைவிக்கும் நோக்கத்தோடு செயல்புரிவார்கள்.

இதில் பல வகை உண்டு. நம்பிக்கை தானே முக்கியம். நம்பிக்கை கொண்டு நம்மவர்களே ஏதேனும் வெளியாட்களுக்குச் சொல்லிவிட்டால் போதும்! நமக்குத் தேவையில்லாததாக இருக்கும் விஷயம் கூட எதிராளிக்குச் சாதகமாகிவிடும். சும்மா உணவகத்தில் சாப்பிடும் போது கூட

யாரேனும் எதையேனும் உளறி விடக் கூடும். எனவே தான் பெரிய நிறுவனங்களில் வெளியே கூட விட அனுமதிக்க மாட்டேன் என்கின்றனர்.

ஆங்கிலத்தில் FTD என்று சுருக்கமாக அழைப்பார்கள். Fear, Truxt, Desire. அதாவது பயம், நம்பிக்கை, ஆசை இவற்றில் ஏதேனும் ஒன்றைப் பயன்படுத்தியே மனிதர்களிடம் இருந்து தகவல்களைக் கறக்க முடியுமாம்!

இந்த எட்டப்பன் வேலைகள் தொலைபேசி வழி, நம் நிறுவனத்தின் விலைப்பட்டியல், தகவல் பட்டியலிலிருந்தே தகவல் எடுத்தல் (Dumpster Driving), மின்னஞ்சல்/இணையத்தளம் மூலம், ஏதேனும் ஒரு ஊழியரைக் குறி வைத்து அவரின் பலவீனங்களின் மூலம் நம்பிக்கை உருவாக்குதல் (Persuasion) போன்றவைகள் மூலம் எளிதில் சாதிக்கப்படுகின்றன.

இன்னும் சாமர்த்தியமான வழிமுறை ஒன்று உண்டு. அதன் பெயர் **முதுகில் குத்தும் எட்டப்பன் முறை (அதாவது Reverse Social Engineering).** இந்த முறையில் யார் எட்டப்பனோ அவர் ஏதோ ஒரு பெரிய அதிகாரி போலும், அவரிடம் எல்லா தகவல்களையும் பெற்றுக் கொள்ளலாம் என்றும் முதலில் ஒரு நம்பிக்கையை உருவாக்குவார். அதாவது அவர் தகவல் சேகரிக்காமல், அவரிடம் நிறுவனம் பற்றிய தகவல் யார் வேண்டுமானாலும் தெரிந்து கொள்ளலாம் என்றும் ஒரு மாயையை உருவாக்குவார். எப்போது அவருக்கு வேண்டிய மீன் தூண்டிலில் சிக்குகின்றதோ அன்று தான் அவரின் சுயரூபம் தெரியவரும்.

இப்போது பிரபலமாகி வரும் ஒரு முறை **Phishing** (இரட்டை வேடம்) ஆகும். இதைப் பற்றி இன்னும் விரிவாகப் பின்னால் காணலாம். இதில் கடனட்டை வழங்குபவர்கள் போலவும் அதில் ஏதோ பிரச்னை இருப்பதாகவும், நீங்கள் தகவல் தந்தால் உடனே சரி செய்வதாகவும் மின்னஞ்சல் மூலம் சொல்லப்பட்டிருக்கும். தெரியாத் தனமாக நம்பிக் கொடுத்து விட்டால் அதோ கதி தான்!

இது போதாதென்று Vishing, Vishing... என்று ஒன்று வந்திருக்கின்றது (நன்றி: தமிழ்நிதி)

*"Phishing" என்ற பெயரில் சிலர் நம் உயிரை எடுத்தார்கள். இப்போது "**Vishing**" என்ற டெக்னிக்கை பயன்படுத்தி சிலர் கிளம்பியிருக்கிறார்கள். உங்கள் வங்கியிலிருந்து உங்களுக்கு ஒரு மின்னஞ்சல் வரும். "உங்கள் கணக்கில் சில பிரச்னைகள் உள்ளது. 1800-123-4567 என்ற எண்ணை உடனடியாக தொடர்பு கொள்ளவும்" என்று அவசரமான அழைப்பு இருக்கும். அந்த நம்பரை நீங்கள் தொடர்பு கொண்டால் automated voice system உங்களது வங்கி கணக்கு நம்பரை தொலைபேசியில் அழுத்த சொல்லும். அப்புறம் உங்கள் Pin numbers-ஐ கேட்கும். வெகுளியாக அதையும் நீங்கள் கொடுத்து விட்டால் அடுத்த சில நாட்களில் உங்கள் வங்கி கணக்கின் இருப்பு குறைந்து விடும். நீங்கள் டயல் செய்த எண்ணை வைத்திருப்பவர்கள் ரஷ்யாவிலோ பிரேசிலிலோ உட்கார்ந்து கொண்டு நம்மை சுத்தமாக மொட்டை அடித்து விடுகிறார்கள்.*

இந்த மாதிரி பிராடு மின்னஞ்சல்களுக்கு "Vishing" என்று பெயர் வைத்திருக்கிறார்கள். Phishing + Voice system = Vishing. உங்கள் வங்கியிலிருந்தோ அல்லது Paypal, Ebay போன்ற நிறுவனங்களிலிருந்தோ இது போன்ற மின்னஞ்சல்கள் வந்தால் உங்கள் வங்கியின் கிரடிட் கார்டு அல்லது ஸ்டேட்மென்ட்டில் உள்ள எண்களை டயல் செய்து விசாரிக்கவும். மின்னஞ்சல்களில் உள்ள எண்களை நம்ப வேண்டாம். VOIP டெக்னிக்கை பயன்படுத்தி சில நேரங்களில் உங்கள் ஏரியா கோடு உள்ள நம்பர்கள் கூட இந்த மின்னஞ்சல்களில் வரலாம். ஆனால் அந்த நம்பர்களை மானிட்டர் செய்யும் ஆட்கள் பல ஆயிரம் மைல்கள் தள்ளி இருக்கலாம்! Skype, Vonage போன்ற நிறுவனங்களின் சேவைகளை உபயோகித்து இது போல செய்வது மிக சுலபம்!

எத்தனை மிகக் கடினமான கட்டுப்பாடுகள், பாதுகாப்பு முறைகள் கொண்டு வந்தாலும், மிகப் பழைய முறையான இந்த எட்டப்பன் வேலை மிக எளிதில் அனைத்தையும் தகர்த்தெறிந்து விடுவதால் இதுவே தகவல் பாதுகாப்பு மேலாண்மைக்கு முதல் எதிரியாகும்! ஏனென்றால் நட்பின் முன் அனைவரும் மண்டியிட்டே ஆவார்கள்! அதை வேண்டியவர்கள் வேண்டிய மாதிரி சாதித்துக் கொள்ள வாய்ப்பாகி விடுகின்றது.

நாம் கற்றுக்கொள்ள வேண்டியது:

ரகசியம் ஒருவரிடம் மட்டும் இருந்தால் அது கடவுளின் ரகசியம்.

ரகசியம் இருவரிடம் மட்டும் இருந்தால் அது மானிட ரகசியம்.

ரகசியம் மூவரிடம் போய்விட்டால் அது பரரகசியம் ஆகி விடும்.

என்பது தான்!

2. ஜேப்படி: (Electronic pickpockets)

அமெரிக்காவில் 35 முதல் 40 சதம் வரை நிதிப்பட்டுவாடாக்கள் கணினி மூலம் நிகழ்நிலையில் (Online) நடைபெறுகின்றன.

பணம் மின்மயமாய் ஆனதால் ஜேப்படிக் காரர்களும் மின்மயமாகிவிட்டனர்! அதாவது நம்முடைய கணினியில் இருந்து தகவல்களை நமக்குத் தெரியாமலேயே நகலெடுத்து விடுகின்றனர். அதற்கு மிக முக்கியக் காரணங்கள்:

1. நம் கணினியில் தகுந்த இணைய பாதுகாப்புக்கள் செய்யாமலிருத்தல். (Network Security)

2. நம் கணினியில் இருந்து இன்னொரு கணினிக்குத் தகவல் அனுப்புகையில் பாதுகாப்பின்றி அனுப்புதல்.

உதாரணத்திற்கு உங்கள் செல்பேசியில் ப்ளூடூத் தொழில்நுட்பம் இருக்கின்றது என்று வைத்துக் கொள்வோம். உங்கள் செல்பேசிக்கும், உங்கள் ஹெட் செட்டில் பாடல் கேட்பதற்கும் ப்ளூடூத் இயக்கத்தில் இருக்குமாறு வைத்திருக்கின்றீர்கள் என்று வைத்துக் கொள்வோம். இது ஒரு விமான நிலையத்தில் என்று வைத்துக் கொண்டால், பக்கத்தில் இருக்கும் ப்ளூடூத் வசதி உள்ள ஒரு மடிக்கணினி மூலம் உங்கள் செல்பேசியில் இருக்கும் அனைத்து தகவல்களும் (உங்களின் தொடர்பு எண்கள் உட்பட) நகலெடுக்க முடியும். அதில் உங்கள் கடனட்டை எண்ணோ, பாதுகாப்பு கடவுச்சொல் எண்ணோ பதிந்து வைத்திருந்தால் பணம் அம்பேல்!

அத்தனை பாதுகாப்பில்லாதது ப்ளூடூத் வசதி என்று அங்கலாய்க்கிறார் ஆதம் லாரி (Adam Laurie of security firm AL Digital).

எனவே நம் கருவிகளைப் பாதுகாப்பாய் வைத்திருப்பதுடன், அதைப் பாதுகாப்பாய் உபயோகிப்பதும் நம் கையில் தான் இருக்கின்றது!

3. கடனட்டை மோசடி: (Credit Card Fraud)

இந்தக் கடனட்டை மோசடி என்பது மிகப்பெரிய அச்சுறுத்தலாக இருந்து வருகின்றது என்றால் அது மிகையாகாது!

கடனட்டை மோசடி என்பது, கடனட்டை மூலமாகவோ, அல்லது மற்ற நிகழ்நிலை பணம் செலுத்தும் வசதிகளின் மூலமாகவோ பணத்தைத் திருடுவது அல்லது மோசடி செய்வது என்பதைக் குறிக்கும். இதன் மூலம், பணத்தை எடுத்துக் கொள்வதோ அல்லது பணம் செலுத்தாமலேயே பொருட்களை வாங்கிக் கொள்வதோ நடக்கக் கூடும்.

அடையாளப் பறிமுதலும் இதனை ஒத்ததாகும். (Identity Theft)

2006ம் ஆண்டில், இங்கிலாந்தில் மட்டும் நடைபெற்ற கடனட்டை மோசடிகளின் மொத்த மதிப்பு 750-800 மில்லியன் அமெரிக்க டாலர்களாகும்! உலகம் முழுதும் கணக்கிட்டால் அது பில்லியன்களில் போய் நிற்கின்றது.

கடனட்டை மோசடி நடப்பது எவ்வாறு?

1. கடனட்டையைத் திருடுவதன் மூலம்.

2. கடனட்டை எண்ணைத் தெரிந்து கொள்வதன் மூலம். (இதற்கு எத்தனை வழியிருக்கின்றது என்று யோசித்துப் பார்த்தால் தலை சுற்றுகின்றது! சாதரணமாக நாம் கடையில் வாங்கும் பொருளுக்குக் கட்டும் பில்லிலேயே நம் கடனட்டை எண்ணும் விழுகின்றது. எளிதில் மற்றவர்கள் (கடைச்சிப்பந்தி) அதை உபயோகிக்க முடியும்)

மாதம் ஒரு முறை வரும் கணக்கு அறிக்கை மூலம் குற்றம் நடந்திருக்கின்றது என்று கண்டறிவதற்குள்ளேயே தாவு தீர்ந்து விடும்.

கடனட்டையில் பின்புறம் இருக்கும் காந்தப்புலத்தில் இருக்கும் தகவல்கள் என்னென்ன?

* கடனட்டை தாரரின் பெயர் (Name of card holder)

* அவரது கணக்கு எண் (Account number)

* காலாவதி தேதி (Expiration date)

* கடவுச்சொல் (Verification/CVV code)

இவைகளை எளிதில் இணைய தளத்தில் இருக்கும் தரவுகளின் மூலம் கண்டறிய முடியும்.

இன்னும் கொஞ்சம் ஆராய்ந்தால், மொத்தம் நான்கு வகைகளாய் இந்தக் கள்ளர்களைத் தரம்பிரிக்கலாம்:

1. மின்னஞ்சல்/இணைய தள மோசடி:

இதன் மூலம் தான் மிக அதிகமாக கடனட்டை மோசடிகள் நடக்கின்றன. அதாவது மேலே கண்ட தகவல்களை அறிந்து கொண்ட ஒருவர் மின்னஞ்சல்/இணையதளங்களில் இந்தக் கடனட்டை தகவல்களை உபயோகித்துப் பணத்தின் மதிப்பைப் பெறுவது ஆகும்.

2. வங்கிக் கணக்கு அடையாள மோசடி: (Identity Theft/Account Take Over)

இந்த வகைக்காரர்கள், நம்மிடம் இருந்து ஏதேனும் ஒரு முக்கியத் தகவல் கொண்ட ஆவணங்களைக் கையாடுவர். (உதாரனம் தொலைபேசி பில், குடியுரிமை அட்டை) நம் வங்கிக் கணக்கு எண்ணையும் தெரிந்து கொள்வார்கள். ஏதோ அவர் தான் அந்தக் கணக்கின் சொந்தக் காரர் போல் நடித்து, அந்த முக்கிய ஆவணங்களைச் சாட்சியாய்ப் பயன்படுத்தி வங்கியை நம்ப வைப்பார்கள். பின், கடனட்டை தொலைந்து போனதாய் ஒரு புகார் தருவார்கள். புதுக் கடனட்டை வந்ததும், அதை வைத்து பணத்தைச் சுருட்டிக் கொள்வார்கள். உங்களிடம் இருக்கும் கடனட்டை மட்டும் வேலை செய்யாமல் போய்விடும்!

3. நம்பிக்கைத் துரோகம்: (Skimming)

இந்த முறையில், நமக்குக் கீழ் இருப்பவர்களே அல்லது நாம் யாரை நம்பி ஒப்படைக்கிறோமோ அவர்களே கடனட்டை தகவல்களை அறிந்து கொண்டு பின்னர் உபயோகித்துக் கொள்வது ஆகும். உதாரணமாக, ஒரு ஒட்டலில் சாப்பிட்டு விட்டு கடனட்டையை பணம் கட்டச் சிப்பந்தி கையில் தருகின்றோம். அவர் ஒரு சிறிய காந்தப் புலக் கருவி மூலம் நம் கடனட்டை விபரங்களை நகல் எடுத்துக் கொண்டு திருப்பித் தந்து விட்டு, பின் அத் தகவல்களைப் பயன்படுத்தி அடிக்கடி பணம் எடுத்துக் கொள்வது ஆகும்.

இது அடிக்கடி ATM இயந்திரங்களில் மூலம் நடைபெறுகின்றது.

இதனைப் பயனர்களை விட வங்கிகள் எளிதில் கண்டறிய முடியும். ஒரே எண்ணிலிருந்து ஒரே விதமாக அடிக்கடிப் பணம் பெற்றுக் கொண்டே இருந்தால் அல்லது ஒரே கடையில் வாங்கிக் கொண்டே இருந்தால் அது உண்மையானது தானா என்று வாடிக்கையாளர்களைக் கவனமாக இருக்கச் சொல்லலாம்.

4. குருட்டாம் போக்குத் தத்துவம்: (Carding) இந்த முறையில் மோசடிக்காரரிடம் எந்தத் தகவலுமே இருக்காது. ஆனால், மென்பொருளின் மூலம் ஏதேனும் ஒரு இணையத் தளத்தில் குருட்டாம்போக்காகப் பல எண்களைக் கொடுத்து ஏதேனும் ஒரு கடனட்டை எண் செயல்படுத்த முடிகின்றதா என்று கண்டறிவது ஆகும்! இத்தகைய இணைய தளங்களை Cardable Website) என்கின்றனர்.!

இனி, கடனட்டை உபயோகிப்பவர்கள், அதைப் பாதுகாப்பாய் உபயோகிக்கும் சில வழிமுறைகளைப் பார்க்கலாம்:

1. உங்கள் கடனட்டையை ஒவ்வொரு முறை உபயோகிக்கும் போதும் உங்கள் கண் மிக விழிப்பாய் இருக்க வேண்டும். வெளியாளிடம் தரும் போது அவர் எங்கெங்கு செல்கின்றாரோ, நீங்களும் அங்கெல்லாம் செல்ல வேண்டும். எவ்வளவு சீக்கிரம் அது மீண்டும் உங்கள் கைக்கு வருகின்றதோ அத்தனை சீக்கிரம் திரும்ப வாங்கிக் கொள்ள வேண்டும்.

2. யாரிடம் உங்கள் கடனட்டை தருகின்றோம் என்பதில் கவனமாயிருங்கள். நீங்களாக அழைக்காத தொலைபேசி அழைப்பில் கடனட்டை எண்ணை எக்காரணம் கொண்டும் தராதீர்கள்.

3. மின்னஞ்சல் மூலம் கடனட்டைத் தகவல்களைத் தரவே கூடாது.

4. https:// என்று ஆரம்பிக்காத எந்த முகவரி இருக்கும் இணையப் பக்கத்திற்கும் உங்கள் கடனட்டை விபரங்களைத் தரவே கூடாது. தருமுன் ஒருமுறைக்கு இருமுறை சரி பார்த்துக் கொள்ளுங்கள்.

5. கடனட்டை வந்த மறுநிமிடமே பின்பக்கம் உங்கள் கையெழுத்தை இட்டு விடுங்கள்.

6. உங்கள் கடனட்டை வாங்க உபயோகித்த ஆவணங்களை அப்படியே பத்திரப்படுத்தி வைத்திருங்கள்.

7. உங்கள் பின் கடவுச்சொல்லை எங்கும் எழுதி வைக்காதீர்கள். மனதில் பதிந்து கொள்ளுங்கள்!

8. உங்கள் கடனட்டையையோ அல்லது அதை உபயோகித்த பில்களையோ வெளியே விட்டு விடாதீர்கள். பாதுகாப்பாய் வைத்திருங்கள்.

9. கடனட்டை எண் வெளியே தெரியாதவாறு வைத்திருங்கள். யாரேனும் கேமிரா மூலம் புகைப்படம் எடுக்கா வண்ணம் இருக்கட்டும்.

10. மிகப் பத்திரமான இடத்தில் உங்கள் கடனட்டை எண், காலாவதி தேதி, வங்கி தொலைபேசி எண் ஆகியவற்றைக் குறித்து வைத்திருங்கள்.

11. அடிக்கடி உபயோகிக்காத கடனட்டையைத் தேவையில்லாமல் தூக்கிக் கொண்டு திரியாதீர்கள்!

12. மாத மாதம் வரும் கடனட்டைக் கணக்குப் பட்டியலை வரி விடாமல் சரி பாருங்கள். பணம் கட்டிய ரசீதையும் அதனுடன் சேர்த்துப் பத்திரப் படுத்தி வையுங்கள்.

13. மிகக் குறைந்த தொகையானாலும், உங்களால் கண்டுபிடிக்க முடியாத நிகழ்வுகளை உடனே புகார் செய்யுங்கள்.

14. காலியாக நிரப்பப்படாத எந்த ஆவணத்திலும் கையொப்பமிடாதீர்கள். அத்தகைய பகுதிகளைக் குறுக்கு கோடு வைத்து அடித்து விடுங்கள்.

15. கார்பன் தாள்கள் உபயோகித்தால், அந்தக் கார்பன் தாள்கள் உடனடியாக அழிக்கப்பட வேண்டும்.

16. பொது இடங்களில் கடனட்டை எடுத்துப் பார்க்காதீர்கள். (பந்தாவுக்குப் பலர் செய்வார்கள்!)

17. பொதுவாக உங்களின் மணிபர்ஸில் கடனட்டை வைக்காமல் தனியாக வைத்திருத்தல் நல்லது.

18. உங்கள் கடனட்டையை வேறு யாருக்கும் உபயோகப்படுத்தத் தராதீர்கள்.

19. வேறு முகவரிக்குச் செல்லும் போது வங்கிகளுக்கு முன்கூட்டியே தகவல் தந்து விட்டுச் செல்லவும்.

20. இவை எல்லாவற்றிற்கும் மேலாக, ரொக்கம் கட்டி பொருட்களைக் கடைகளில் வாங்குங்கள்!

4. வழிப்பறிக் கொள்ளை:

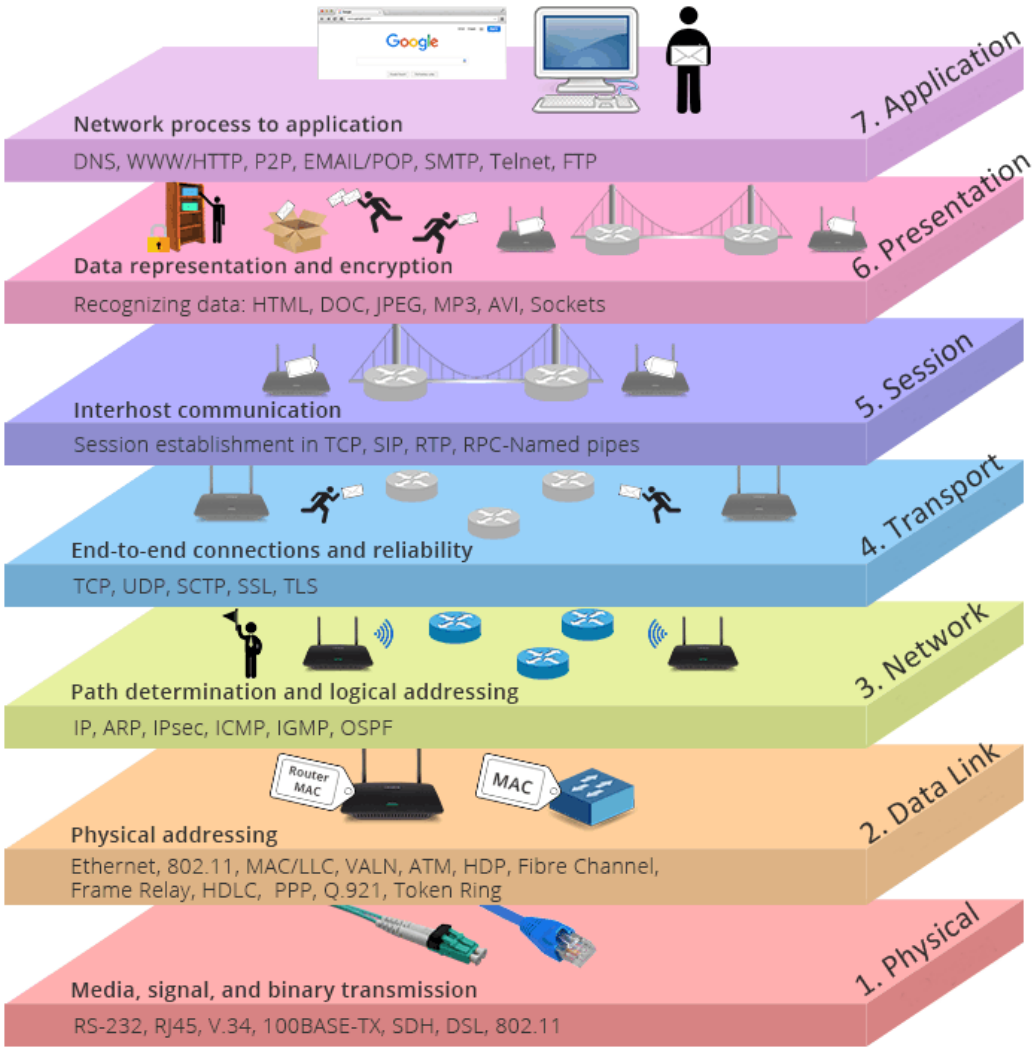
வழிப்பறிக் கொள்ளை என்று இங்கு நான் குறிப்பிடுவது, இணையம் அல்லது பிணையத்தில் தகவல்களைப் பகிர்ந்து கொள்ளும் போது அதை வழிமறித்து தகவல்களைக் கறந்து கொண்டு அதன் மூலம் பாதிப்பு ஏற்படுத்துவது ஆகும்.

இது அனுப்புபவர்/பெறுபவருக்குத் தெரிந்தும் நடக்கலாம், தெரியாமலும் வழியிலேயே நடந்திருக்கலாம்.

முதலில் இணையத்தில் எவ்வாறு தகவல் அனுப்பப் படுகின்றது என்று பார்ப்போம்.

கீழ்க்கண்ட படத்தைப் பாருங்கள். இது TCP/IP எனப்படும் நாம் அடிக்கடி உபயோகிக்கும் முறைமை மூலமாகப் பகிர்ந்து கொள்வதைக் காண்கின்றோம். இது போக ftp,smtp, udp, pop3,imap போன்ற பல முறைமைகள் இருக்கின்றன. இவை அனைத்தையும் தரப்படுத்த ISO நிறுவனம் தகவல் தொடர்பை எவ்வாறு நிகழ்த்த வேண்டும் என்று பல்வேறு

நிலைகளில்/அடுக்குகளில் பிரித்து விளக்குகின்றது. இதை அனைவரும் ஏற்றுக் கொண்டதாலேயே அனைவரும் எளிதில் இணையம் மூலம் உலகம் முழுமையும் தகவல் பரிமாற்றம் செய்ய இயல்கின்றது.



நாங்கள் பாடமாய் இதைப் படிக்கையில் APSTNDP என்று சுருக்கமாய் சொல்லிக் கொள்வோம். ஒவ்வொன்றும் ஒவ்வொரு அடுக்குகள். உதாரணம் காண்போமா?

இது அனுப்பும் போது!

1. பயன்பாடு அடுக்கு (Application Layer) - ஒரு கடிதம் வரைதல்

2. முகப்பு அடுக்கு (Presentation Layer) - கடிதத்திற்கு முகவரி இட்டு உறையிடுதல்

3. தொகுப்பு அடுக்கு (Session Layer) - பல கடிதங்களை முகவரியிட்டு ஒன்றாக்கி அதைத் தபால் பெட்டியில் இடத் தயார் செய்தல். (ஒவ்வொரு கடிதம் எழுதியதும் ஓடிப் போய் தபால் பெட்டியில் போடாமல், ஒரு நாள் முடியும் வரை காத்திருப்போம் அல்லவா? அது தான்!

4. போக்குவரத்து அடுக்கு (Transport Layer) - தபால்பெட்டியில் போட்டதும் தபால் நிலையத்தில் ஒரே இடத்துக்குப் போகும் கடிதங்களாகப் பிரித்துக் கட்டப்படுதல்.

5. பிணைய அடுக்கு (Network Layer) - எந்த ஊருக்கு எந்த வண்டியில் எந்த வழியில் அனுப்பினால் விரைவாகச் செல்லும் என்று கண்டறிந்து அனுப்பப் படுதல்.

6. தரவு அடுக்கு (Data Layer) - சிறு சிறு பொட்டலங்களாகப் பிரித்து வண்டியில் ஏற்றுதல்

7. நிகழ்வு அடுக்கு (Physical Layer) - வண்டியில் பொட்டலங்கள் செல்தல்.

இதைப் பெறும் போது, கீழிருந்து மேலாக நிகழ்ச்சிகள் நடைபெறும்:

7. நிகழ்வு அடுக்கு (Physical Layer) - வண்டி வந்து சேர்தல்

6. தரவு அடுக்கு (Data Layer) - சிறு சிறு பொட்டலங்கள் சரியாக வந்திருக்கின்றதா என்று சரி பார்த்தல்

5. பிணைய அடுக்கு (Network Layer) - சேரும் ஊருக்குத் தகுந்தாற் போல் பொட்டலங்களைச் சேர்த்தல்.

4. போக்குவரத்து அடுக்கு (Transport Layer) - முகவரிக்குத் தகுந்தாற் போல் ஒரே பொட்டலமாக மாற்றி சேருமிடத்துக்கு எடுத்துச் செல்லல்.

3. தொகுப்பு அடுக்கு (Session Layer) - அப்படி வந்த கடிதங்களை ஒருவர் வந்து சேருமிடத்தில் வழங்குதல் (தபால்காரர் ஒரு நாளைக்கு ஒரே முறை வந்து பல கடிதங்களைத் தருவதை ஞாபகம் செய்து கொள்ளுங்கள்)

2. முகப்பு அடுக்கு (Presentation Layer) - உறையில் இருக்கும் முகவரிக்காரர் மேசைக்குக் கடிதம் சென்றடைதல்.

1. பயன்பாடு அடுக்கு (Application Layer) - அவர் அக்கடிதத்தைப் பார்வையிடல்.

இது தான் கணினியிலும் நடக்கின்றது. இங்கு ஒரே ஒரு வித்தியாசம் என்னவெனில், மொத்தக் கடிதமும் பிரிக்கப்பட்டு சிறு சிறு பொட்டலங்களாய் ஆக்கப் படுவது தான். தபால் துறையில் கடிதத்தைப் பிரிப்பதில்லை.

இவ்வாறு ஒவ்வொரு அனுப்பப்படும் ஒவ்வொரு பொட்டலத்திலும் அனுப்ப/பெறப்படும் ஐபி முகவரி போன்ற சில முக்கியத் தகவல்கள் தலை மற்றும் வால் (Header and Footer) சேர்க்கப் பட்டு இணையத்தில் தூவி விடப் படுகின்றன. சிறந்த வழியைக் கண்டறிந்து (Router) அவை சேரும் ஐபி கண்டு சேர்கின்றன.

இனி நம் கதைக்கு வருவோம். அவ்வாறு வரும் பொட்டலங்களை முகர்வதற்கென்றே (Packet Sniffers) மென்பொருட்கள் இருக்கின்றன. எனவே அவை மூலம் உங்கள் ஐபி முகவரியிலிருந்து செல்லும் அனைத்துப் பொட்டலங்களையும் படிவம் எடுத்துக் கொண்டு, பின் ஒட்டிப் பார்க்கத் தெரிந்திருந்தால் உங்கள் தகவல்கள் அனைத்தும் அம்பேல் தான்.

சரி இந்த வழிப்பறிக் கொள்ளையிலிருந்து எவ்வாறு தப்பிப்பது?

இந்தத் தகவல் வழிப்பறிக் கொள்ளையிலிருந்து நம்மால் தப்பிப்பது சற்றுக் கடினமான காரியம் தான். அதுவும் நம் தளம் மிக முக்கியமானதாக இருந்து, அங்கிருந்து செல்லும் தகவல்கள் அனைத்துமே முக்கியமானவை என்றும் அறிந்திருந்தால் அத்தகவல்களைப் பாதுகாக்க நிறைய முயற்சிகள் மேற்கொள்ள வேண்டும் என்பதில் சிறிதும் ஐயமில்லை தானே?

இது இன்று நேற்றுள்ள பிரச்னை அல்ல. என்று தகவல் அனுப்பப் பட ஆரம்பித்ததோ அப்போதே ஏற்பட்ட பிரச்னை தான். தகவல்களை புறாக்களின் காலில் கட்டி விடும் போதே அவைகளை வழிமறித்துத் தகவல்களைப் பிடுங்கும் சம்பவங்கள் உண்டாம்.

எனவே ராணுவ ரகசியங்களை அனுப்புகையில் தகவல்களை நேரடியாக அனுப்பாமல் குறியீடு செய்து அனுப்புவது இன்றும் கூட வழக்கத்தில் உண்டு. இதற்குத் தேவை மூன்று விஷயங்கள் ஆகும்.

1. தகவல். (information)

2. சாவி. (Key)

3. முறைமை. (Logic)

உதாரணமாக 'apple' என்ற வார்த்தையைக் குறியீடு செய்ய வேண்டும் என்று வைத்துக் கொள்வோம். ஒவ்வொரு எழுத்திற்கும் மூன்று எழுத்துக்கள் தள்ளிக் குறியீடு செய்து அனுப்புவதாய் வைத்துக் கொண்டால்

a - f

p - t

p - t

l - p

e - i

என்று மூன்று எழுத்துக்களை நடுவில் விட்டு fttpi என்று மட்டும் அனுப்பி வைக்கலாம். அங்கு சென்றதும் ஒவ்வொரு எழுத்தையும் மூன்று எழுத்துக்கள் குறைத்து மீண்டும் apple என்று மீட்டுக் கொள்ளலாம். இப்படிச் செய்வதற்கு குறியிடுதல் (Encryption), மீளப் பெறுதல்(Decryption) என்று பெயரிட்டிருக்கின்றனர்.

இந்த முறையில் எழுத்துக்களைக் கூட்டுதல் என்பது முறைமை (logic) என்றும், மூன்று என்பதைச் சாவி (key) என்றும் குறிப்பிடலாம்.

அடுத்த முறை தகவலை அனுப்புகையில் மூன்றெழுத்துக்களைக் கூட்டாமல் 4 எழுத்துக்களைக் கூட்டலாம்! இப்படி ஒவ்வொரு முறையும் 3,4 என சாவியை மட்டும் மாற்றுவதன் மூலம் தகவல்களைப் பாதுகாக்க முடியும். சில சமயங்களில் முறைமையையும் மாற்ற வேண்டியதிருக்கும்.

இப்போது கணினி மூலம் அனுப்புகையில் சாவியாக கடவுச்சொல்லையும், முறைமையாக அனுப்பப் படும் கோப்பினைச் சுருக்கியும் (zip) செய்து அனுப்பினால் போதும் தான்!

ஆனால் இந்தக் குறியீட்டு முறை 100% பாதுகாப்பளிக்கும் என்று சொல்ல முடியாது. ஏனெனில் இந்த முறையில் இரண்டு பிரச்னைகள் இருக்கின்றன.

1. பூட்டப்பட்ட சாவியை தகவலைப் பெறுபவர் எப்படித் தெரிந்து கொள்வது? அவருக்கு அதை எப்படியாவது தெரிவிக்க வேண்டும் தானே? அப்போது அது தவறான நபருக்குச் சென்று சேர்ந்து விட்டால்?

2. கணினியின் அதிவேக வளர்ச்சியின் காரணமாக, சாவியை ஊகிப்பது (Cracking) ஒரு சிறு மென்பொருள் மூலம் எளிதில் முடியும். அத்தகைய எத்தர்கள் அதிகம் நிறைந்தது தகவல் தொழில்நுட்ப உலகம். அதற்கு தகவல் எந்த முறைமையின் படி குறியீடு செய்யப் பட்டிருக்கின்றது என்பதை அறிந்திருந்தால் போதுமானது ஆகும்.

அப்படியானால் இதை எப்படித் தான் சரி செய்வது?

மேற்சொன்ன இரண்டு பிரச்னைகளையும் தீர்க்கும் தீர்வு கண்ட உடன் தான் தகவல் தொடர்பு இத்தனை பரவலாயிற்று என்பது என் எண்ணம்.

வந்தார்கள் மூவர் Ron Rivest, Adi Shamir மற்றும் Len Adleman.

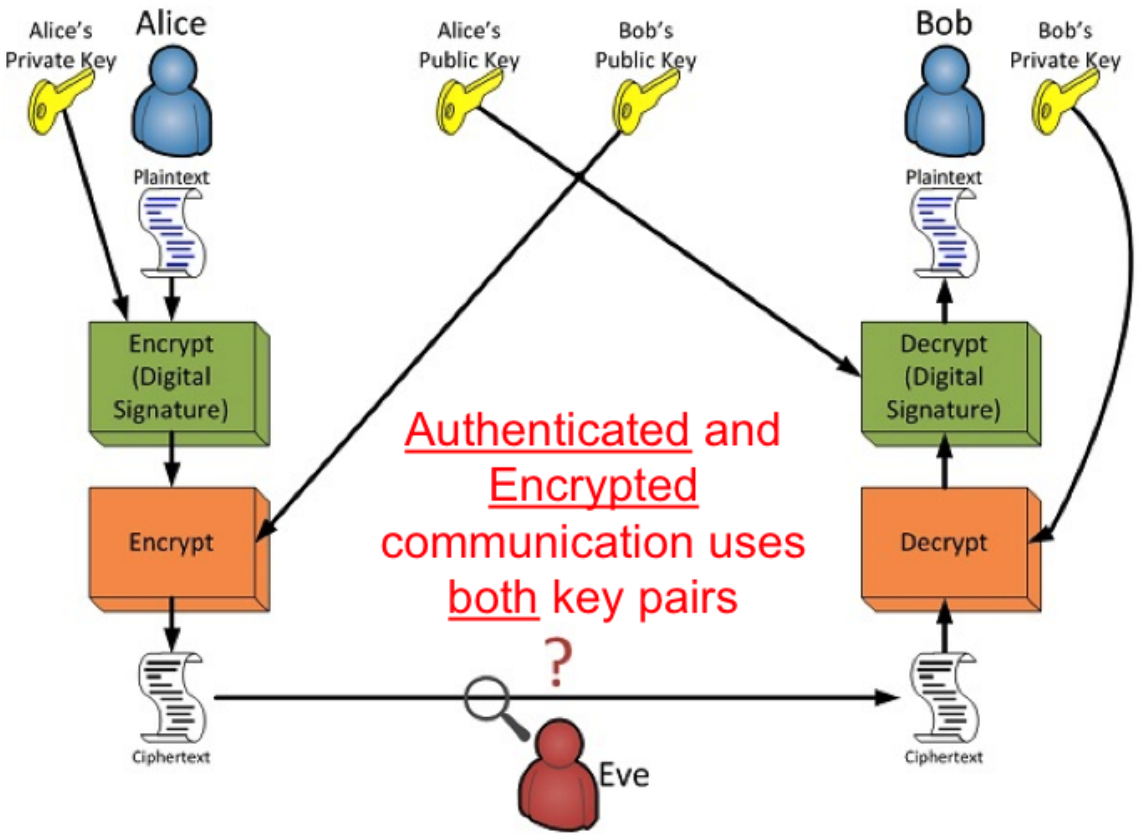
இவர்கள் ஒரு முறைமை கண்டறிந்தனர். ஒன்றும் புதுமையெல்லாம் இல்லை. காலங்காலமாய்த்தெரிந்தது தான். ஆனால் கணிணிக்குத் தக்கவாறு மாற்றியமைத்தனர்.

பழைய கால புதையல் கண்டுபிடிக்கும் படங்கள் பார்த்திருப்பீர்கள். அதில் புதையல் இருக்கும் வரைபடம் ஒரு இடத்தில் இருக்காது. ஒரே வரைபடத்தின் பல பாகங்களைப் பல கொள்ளைக்காரர்கள் ஒருவரை ஒருவர் நம்பாமல் கிழித்துக் கையில் வைத்திருப்பார்கள்.

அதே போல், இப்போது நாம் உபயோகிக்கும் வங்கி பாதுகாப்புப் பெட்டக வசதிக்கு ஒரு சாவி கிடையாது. இரண்டு சாவிகள் உண்டு. முதலில் மேலாளர் சென்று கதவைத் திறப்பார், பின் நாம் சென்று திறக்க வேண்டும். அப்புறம் நாம் பூட்டி விட்டு வந்து விட வேண்டும். அப்புறம் மேலாளர் பூட்டி விடுவார். அவர் பூட்டிய பின் நம் சாவி உபயோகிக்க இயலாது. அவரும் திறக்க இயலாது.

இது போன்று இரண்டு சாவிகளை உபயோகித்து (ஒன்றை வைத்துத் திறக்கவும், இன்னொன்றை வைத்துப் பூட்டவும்) கடவுச்சொல்லை அனுப்பாமலேயே பெறுபவர் குறியீட்டை மீளப் பெற முடியும் என்று கண்டறிந்தார்கள்.

இப்போது இந்தக் கீழ்க்கண்ட படத்தைப் பாருங்கள்.



இந்த முறையின் படியே தான் இலக்கச் சான்றிதழ் (Digital Certificate), பாதுகாப்பான இணைய தள அணுகுமுறை (https - secured) போன்றவை செயல்படுகின்றன.

இந்தப் படத்தில் காட்டியுள்ள படி, மொத்தம் நான்கு சாவிகள் இருக்கின்றன.

அதாவது

1. அனுப்புபவரின் தனிச்சாவி (Sender's Private Key)

2. அனுப்புபவரின் பொதுச்சாவி (Sender's Public Key)

3. பெறுநரின் தனிச்சாவி (Receiver's Private Key)

4. பெறுநரின் பொதுச்சாவி (Receiver's Public Key)

இங்கு சாவி என்பது ஒரு குறிப்பிட்ட வரிசையில் அடுக்கப்பட்ட கடவுச்சொல் அல்லது எண்கள் என்று சொல்லலாம்.

பெயரைப் போலவே தனிச்சாவி அவரவர்களிடம் ரகசியமாக இருக்கும், பொதுச்சாவி உலகில் யாவரும் பெற்றுக் கொள்ளுமாறு திறந்த நிலையில் இருக்கும். இன்னாருக்கு இது தான் பொதுச்சாவி என்று சான்றிதழ் அதிகாரியால் (Certifying Authority) முத்திரை இடப்பட்டு இலக்கச் சான்றிதழில் குறிப்பிடப் பட்டிருக்கும். அதன் மூலம் அவர்களின் பொதுச்சாவியை யார் வேண்டுமானாலும் அறிந்து கொள்ளலாம்.

உதாரணமாக மைக்ரோசாப்டின் Microsoft Windows Hardware Compatibility க்கான பொதுச்சாவி இதோ கீழே இருக்கின்றது. இது 1024 பிட் சாவியாகும்.

30 81 89 02 81 81 00 e0 4e 10 0e b8 a7 ef 21 ca 60 5a dc 9f 1e 3e 83 77 5a 29 2e f9 4e e5 08 5d de e1 cf 09 c0 1f 44 b7 07 a8 4b a4 22 30 3b 19 06 83 ee f3 ac 27 78 ae ca d6 40 2b ce 79 01 e1 9d 56 8b 36 72 b1 63 90 5f a0 b2 c0 66 a6 49 c5 3c fa 26 a2 62 c3 d3 b5 cc 61 15 4c f2 3f b4 e7 45 08 43 89 7f 6a 8d d5 66 fb d7 ff 64 00 c4 11 fd 2c a3 0b 75 b0 fb e5 ac 26 65 a3 81 e6 66 49 3d 1d 73 7a 9b 71 d7 02 03 01 00 01

இதை எளிதில் Internet Options -> Content -> Certificates -> Intermediate Certifying Authorities என்ற பகுதிக்குச் சென்று நீங்களும் காணலாம்.

நாமும் தகவலைப் பாதுகாப்பாக அனுப்புவது எவ்வாறு?

நாமும் நமக்கென முதலில் இரு சாவிகள் உருவாக்க வேண்டும். அதாவது தனிச்சாவியும் பொதுச்சாவியும். அதற்கான மென்பொருட்கள் பலவுண்டு.

இந்தத் தனிச்சாவியும் பொதுச்சாவியும் என்ன? எப்படிக் கண்டறியப்படுகின்றன?

ஒரு கடவுச்சொல்லையும் (Keyphrase) குறிப்பிட்ட முறைமையையும் வைத்து உருவாக்கப் படுவதே இந்த தனிச்சாவியும் பொதுச்சாவியும் ஆகும்.

இந்த முறைமையைக் கண்டறிந்தவர்களின் பெயர்களிலேயே இந்த

முறைமை (Algorithm) குறிப்பிடப்படுகின்றது. இதைச் சுருக்கமாக RSA Algorithm என்பார்கள். (Ron Rivest, Adi Shamir மற்றும் Len Adleman ஆகிய மூவரின் பெயர்ச்சுருக்கமே RSA)

RSA அல்காரிதம் என்று உலகம் பெயர் சொல்லி அழைக்கும் முறைமையில் மொத்தம் ஐந்து படிகளில் தனிச்சாவியும் பொதுச்சாவியும் பெறப்படுகின்றன. பகா எண்கள் என்று கேள்விப்பட்டிருப்பீர்கள். அவற்றை உபயோகித்துத் தான் இன்று தகவல் தொழில்நுட்ப உலகமே சுற்றிக் கொண்டிருக்கின்றது என்றால் அது மிகையாகாது.

அனுப்புநர் தன் தனிச்சாவியைப் பத்திரமாக வைத்துக் கொள்வார். அவருக்குத் தெரிந்தது மூன்று சாவிகள்.

அதாவது,

1. அவருடைய தனிச்சாவி

2. அவருடைய பொதுச்சாவி (அவருக்கும் உலகத்துக்கும் தெரிந்தது!)

3. பெறுநருடைய பொதுச்சாவி (உலகத்துக்கே தெரிந்தது!)

அதே போல், பெறுநரும் மூன்று சாவி பற்றி அறிந்திருப்பார்.

அதாவது,

1. அவருடைய தனிச்சாவி

2. அவருடைய பொதுச்சாவி (அவருக்கும் உலகத்துக்கும் தெரிந்தது!)

3. அனுப்புநருடைய பொதுச்சாவி (உலகத்துக்கே தெரிந்தது!)

இப்போது, அனுப்புநர் தன்னுடைய கடனட்டை எண்ணை பெறுநருக்கு பாதுக்காப்பாய் அனுப்ப முடிவு செய்கின்றார் என்று வைத்துக் கொள்வோம்.

1. முதலில் தன்னுடைய மின்னஞ்சல் மென்பொருளின் மூலம் மின்னஞ்சல் தயார் செய்வார். அதில் தன் கடனட்டை எண்ணை இடுவார்.

2. அதன் பின் தன்னுடைய **தனிச்சாவி** மூலம் அந்த மின்னஞ்சலைக் **கையொப்பமிடுவார்**.

3. அதன் பின்னர் தனக்குத் தெரிந்த **பெறுநரின் பொதுச்சாவி** மூலம் அந்த மின்னஞ்சலைப் **பூட்டுவார்**. இதன் மூலம் வெறும் குறியீடுகளாக யாரும் அறியா வண்ணம் அவரது மின்னஞ்சல் மாற்றப்படும். அதன் பின் அந்த மின்னஞ்சலை அவர் நினைத்தாலும் திறக்க முடியாது!

4. தைரியமாக இணைய இணைப்பின் மூலம் மின்னஞ்சலை அனுப்பி வைப்பார்.

5. பெறுநர், மின்னஞ்சலைப் பெற்றவுடன், தன்னிடமிருக்கும் **தன்னுடைய தனிச்சாவி** மூலம் பூட்டைத் **திறப்பார்**. அவரது பொதுச்சாவியால் பூட்டப்பட்ட பூட்டை உலகத்தில் அவரது தனிச்சாவி மூலம் மட்டுமே திறக்க இயலும்.

6. அதன் பின், அனைவருக்கும் தெரிந்த **அனுப்புநரின் பொதுச்சாவி** மூலம் அவர் அனுப்பியது தானா என்று கையெழுத்தைச் **சரிபார்ப்பார்**.

இதன் மூலம் பத்திரமாக மின்னஞ்சல் சென்று சேர்ந்து விடும்.

கையெழுத்திடுதல், பூட்டுதல், திறத்தல், சரிபார்த்தல் ஆகிய நான்கு நிகழ்வுகள் நிகழ்கின்றன. கையெழுத்திட்டாலும் கடிதத்தின் விஷயங்களைப் பார்வையிட முடியும். உறையில் போட்டு பூட்டி விட்டால் அறிய முடியாது. சரி தானே?

பூட்டுதல், திறத்தல் தவிர ஏன் கையெழுத்திடுதலும், சரிபார்த்தலும் நிகழ்கின்றன என்ற ஒரு கேள்வி உங்களுள் எழும். மேலும், அனுப்புநர், பெறுநர் தவிர மூன்றாமவராய் சான்றிதழ் அதிகாரி எங்கிருந்து முளைத்தார்? போன்ற கேள்விகளுக்கான பதில்களைத் தேடுவோம்!

அனுப்புனரின் தனிச்சாவி கொண்டு கையெழுத்திடுதலும், பெறுநரின் பொதுச்சாவி கொண்டு பூட்டுதலும் நிகழ்கின்றது என்று பார்த்தோம்.

இதில் ஏன் கையெழுத்திடுதல் அவசியம்?

சமீபத்தில் அதிகம் பொதுத்துறையில் கேள்விப்பட்ட ஒரு வார்த்தை இ-கவர்னன்ஸ் (e-Governance) அதாவது மின்னியல் அரசு நிர்வாகம் என்று கொள்ளலாம். நியாய விலை அட்டையிலிருந்து, வெளிநாட்டுக்குச் செல்ல உதவும் பாஸ்போர்ட் வரை கணினி கொண்டு தான் நிர்வகிக்கப் படுகின்றது. அதுமட்டுமல்ல, ஒவ்வொரு மாதமும் விற்பனை வரிக் கணக்கு

சமர்ப்பிப்பதிலிருந்து ஆண்டு தோறும் வருமான வரி கணக்கு சமர்ப்பிப்பது வரை கணினி மூலமே செய்ய முடிகின்றது.

பணமும் நமது வங்கிக் கணக்கிலிருந்து நிகழ்நிலையிலேயே மாற்ற முடிகின்றது.

இதையெல்லாம் செய்யும் ஒருவர், நாளைக்கு எனக்குத் தெரியாது, நான் செய்ய வில்லை என்று கையை விரித்து விடாமல் இருக்கவும், இன்னார் தான் இதைச் செய்தார் என்று நிரூபிப்பதற்காகவும் கையெழுத்து இடப்படுகின்றது தானே?

அதே நோக்கம் தான் இங்கும். எண்ணியல் கையொப்பம் இடுவதும் இதே காரணத்திற்காகத் தான். சரி, என்னுடைய கையெழுத்தைப் போன்றே இன்னொருவர் போட்டு விட்டார் என்றோ அல்லது எனது தனிச்சாவியை யாரோ கண்டுபிடித்து விட்டார்கள் என்றோ அல்லது தனிச்சாவி இணையத்தில் எப்படியோ வெளியிடப்பட்டு விட்டது. எனவே இதை நான் செய்ய வில்லை என்று ஒருவர் சொன்னால் என்ன செய்வது?

அதே போல், பெறுநரும், என் தனிச்சாவி அனைவருக்கும் தெரிந்து விட்டது. எனவே எனக்கு மட்டும் வர வேண்டிய தகவல்கள் அனைவரும் காணும் படி ஆகிவிட்டது என்று சொன்னால் என்ன செய்வது?

ஆக மொத்தத்தில், தனிச்சாவியை இணையத்தில் இவர்களே பரப்பி விட்டோ அல்லது இவர்களின் தனிச்சாவியை யாரோ நிஜமாகவே திருடியோ இணையத்தில் போட்டுவிட்டால் என்ன செய்வது?

இக்கேள்விகளின் தீர்வே நடுநிலையாய் செயல்படும் சான்றிதழ் அதிகாரி (Certifying Authority - CA - இது வேற சிஏ).

இந்தச் சான்றிதழ் வழங்கும் அதிகாரிகளைக் கண்காணிப்பதற்கென்றே அரசாங்கம் பல விதிமுறைகளை வகுத்திருக்கின்றது. இதற்கென்று தனித்துறையே இருக்கின்றது. இத்துறை மேலிடத்திடம், சான்றிதழ் அதிகாரியாக இருக்க விருப்பம் தெரிவிப்பவர்கள் அதற்கென்று அனுமதி வாங்கி இப்பணியை மேற்கொள்ளலாம். உதாரணமாக: டாட்டா நிறுவனம் நம் நாட்டில் அதற்கென்று அனுமதி வாங்கி செயல்படுகின்றது. http://www.tcs-ca.tcs.co.in/

இவ்வதிகாரிகளின் பணி என்னவென்றால், தன்னிடம் கையொப்பத்தைப் பதிந்து கொண்டு சான்றிதழ் பெறும் நபர்களின் பொதுச்சாவியை வெளியிடுவதும், அவற்றைச் சரி பார்ப்பதும், இவரது பொதுச்சாவி இது தான் என்று நிரூபணம் செய்வதும் ஆகும்.

நீங்களாகவே இது என் தனிச்சாவி, இது என் பொதுச்சாவி என்று சொல்லி விட முடியாது! இது போன்ற சான்றிதழ் அதிகாரியிடம் உங்களின் பொதுச்சாவியை அனுப்பி வைக்க வேண்டும். பின்னர், ஏதேனும் ஒரு மின்னஞ்சலை உங்களின் தனிச்சாவி கொண்டு கையொப்பமிட்டு அவர்களுக்கு அனுப்பி வைக்க வேண்டும். அவர்கள், நீங்கள் அனுப்பிய பொதுச்சாவி கொண்டு அக்கையொப்பத்தைச் சரிபார்த்த பின்னர், உங்களுக்குச் எண்ணியல் சான்றிதழ் (Digital Certificate) வழங்கப்படும். அதில் உங்களின் பொதுச்சாவி பற்றிய முழுவிபரமும் இருக்கும். அச்சான்றிதழில் குறிப்பிட்டிருக்கும் நாள் வரை, சான்றிதழ் அதிகாரி தனது சான்றிதழைத் திரும்பப் பெறாத வரை அப்பொதுச்சாவிக்குரிய தனிச்சாவி உங்களிடம் தான் இருக்கின்றது என்பதன் நிரூபணமே அச்சான்றிதழ் ஆகும்.

தனிச்சாவியைப் பத்திரமாக வைத்திருத்தல் வேண்டும். எப்படியோ திருட்டுப் போய்விட்டால், உடனே சான்றிதழ் அதிகாரியிடம் தெரியப்படுத்தி அதை உடனே முடக்க வேண்டும். அதுவரை வேறு யாரும் உங்களின் தனிச்சாவி கொண்டு கையொப்பம் இட்டால், அது நீங்கள் செய்ததாகவே கருதப்படும். எனவே மிகவும் கவனமாக இருத்தல் வேண்டும்.

இந்தச் சான்றிதழ்கள் மூன்று வகைப்படும்.

நிலை - 1, நிலை - 2, நிலை - 3 Class -1,2,3 என்று அவற்றை அழைக்கின்றார்கள்

நிலை 1 இலக்கச் சான்றிதழ்களுக்கு ஒரு மின்னஞ்சல் முகவரி மட்டும் இருந்தாலே போதுமானதாகும். அதை வைத்து அதிகம் சரி பார்க்க இயலாது. ஆனால், மென்பொருட்களை அனுப்புவோர் மற்றும் பெறுவோர் தம்மைச் சரிபார்த்துக் கொள்ள இந்த நிலை இலக்கச் சான்றிதழ்கள் போதுமானது.

நிலை 2 இலக்கச் சான்றிதழ்கள் யாருக்குத் தரப்பட்டிருக்கின்றன என்பதைச் சரி பார்த்துக் கொண்டு தரப்படும் இலக்கச் சான்றிதழ்கள். இவை தனிநபர்களுக்குத் தரப்படுகின்றன. தங்கள் அடையாளத்தை இவர்கள்

சான்றிதழ் வழங்குவோரிடம் நிரூபித்தல் அவசியம் ஆகும். பல அரசு சார் மின் ஆவணங்களில் இலக்கக் கையொப்பமிட இவ்வகைச் சான்றிதழ்கள் உபயோகமாக இருக்கின்றன.

நிலை 3 இலக்கச் சான்றிதழ்கள் இன்னும் ஒரு படி மேலே சென்று நிறுவனங்களுக்கும் தனிப்பட்ட நபர்களுக்கும் தரப்படுகின்றன. புகைப்பட அடையாளத்துடன், முழு முகவரி அனைத்தும் சரி பார்க்கப்பட்டே பின்னர் வழங்கப்படுகின்றன. இச்சான்றிதழ் பெற வேறு சில உரிமங்களையும் (எடுத்துக்காட்டாக ஏற்றுமதி/இறக்குமதி உரிமம்) சில சான்றிதழ்களையும் (எடுத்துக்காட்டாக பட்டயக் கணக்காளர்கள் சான்றிதழ்) தரவேண்டியிருக்கும்.

நிலை அதிகமாக அதிகமாக பாதுகாப்பு இன்னும் அதிகம் என்பதைத் தெரிந்து கொள்ளலாம். மேலும் தனிச்சாவியை மிகவும் பாதுகாப்பாக வைத்திருத்தல் அவசியம் என்பதையும் தெரிந்து கொள்ளலாம். அவ்வாறு தனிச்சாவி திருடு போய் விட்டால் உடனடியாக சான்றிதழ் வழங்குவோரிடம் தெரிவித்தால் உடனடியாக அதன் பொதுச்சாவி முடக்கப்பட்டு புதியதாக இரு சாவிகளும் தரப்படும்.

இலக்கச் சான்றிதழ்களைப் பின்னர் மறுதலிக்காமல் இருக்கவும் இத்தனை முன்னேற்பாடுகள் அவசியமாகின்றன.

இப்போதைக்கு இலக்கச் சான்றிதழ்கள் மூலம் நடைபெறும் பணத் தொடர்புகள் பாதுகாப்பானதாகவே நிகழ்ந்திருக்கின்றன. எனவே இதுபற்றி நன்கு அறிந்து சான்றிதழ்களைத் தகுந்த முறையில் உபயோகிப்பதன் மூலம் நம் தகவல் பாதுகாப்பை உறுதி செய்து கொள்ளலாம்.

வழிப்பறிக் கொள்ளையில் இருந்து அப்படியே இலக்கச் சான்றிதழ்கள் பற்றி ஆராய ஆரம்பித்ததால் நமது பட்டியலை அம்போவென விட்டு விட்டோம்! இப்போது அதைத் தொடரலாம்!

5. பூட்டு உடைப்பு:

பூட்டு உடைத்தல் என்பது அதிகாரபூர்வமற்ற வகையில் கணினியின் வன்பொருளையோ, மென்பொருளையோ, தகவலையோ உட்புகுந்து திருடுதல் என்ற பொருளில் கூறப்படுகின்றது. இதன் மூலம், உலகின் ஒரு மூலையில் எங்கோ இருந்து கொண்டு இன்னொரு மூலையில் இருக்கும் கணினியின் நிர்வாகக் கடவுச்சொல்லை ஒருவர் அறிந்திருந்தால்

தகவல்களைத் திருடுதல் எத்தனை சுலபமானது என்பது அறிந்து கொள்ள இயலும்.

திருடக் கூடிய தகவல்கள் பலப் பல! வியாபார ரகசியங்கள், பொருட்களின் விலைப்பட்டியல்கள், கடனட்டை எண்கள், சாதாரண எழுத்தில் (Plain Text) சேமிக்கப்பட்ட கடவுச்சொற்கள், தனிப்பட்ட தகவல்கள், படங்கள் என்று இந்தப் பட்டியல் நீண்டு கொண்டே செல்கின்றது.

இதைத் தடுக்க தனிப்பட்ட முறையில் ஒவ்வொரு கணினியைப் பாதுகாப்பதும், தீச்சுவர் மூலமாக பிணையத்தையும் இணையத்தையும் பிரித்து மிகுந்த சோதனைக்குப் பின்னரே இணையத்தை அனுமதிப்பதும் தேவையாகின்றது. எக்காரணத்தைக் கொண்டும் நிர்வாகி (Administrator) கணக்கு கடவுச்சொல்லின்றி இருத்தலே கூடாது.

6. கள்ளச்சாவி:

கணினித் துறையைப் பொருத்தவரை ஒரு சாவி அல்லது கடவுச்சொல் எப்போது கெடுதலான எண்ணமுடையவர் கரங்களில் சென்று சேர்கின்றதோ அப்போது அது கள்ளச் சாவி ஆகின்றது. பூட்டை உடைப்பதற்கும் கள்ளச் சாவிக்கும் இருக்கும் ஒரு மெல்லிய வித்தியாசம் என்னவெனில், பூட்டுடைப்பில், பூட்டு சேதாரமாகின்றது. அதாவது அடுத்து வருபவர் உடனே தனது பூட்டு உடைபட்டிருப்பதை அறிந்து கொண்டு ஏதேனும் தவறு நேர்ந்திருப்பதை ஊகிக்க இயலும்.

ஆனால், கள்ளச் சாவியிலோ பூட்டு உடைபடாமல் இருப்பதால், திருடன் எதை எப்போது எடுத்துச் சென்றிருக்கின்றான் என்பதைக் கூட அறிந்து கொள்ள முடியாது.

பொருட்களுக்கும் தகவலுக்கும் இருக்கும் வித்தியாசம், பொருளை எடுத்துச் சென்று விட்டால் அது இருக்காது. அதை வைத்து திருடு போயிருப்பதை அறிந்து கொள்ளலாம். தகவலை நகலெடுத்துச் சென்றால்? நகலெடுத்துச் சென்றவர் மோசமான விளைவை ஏற்படுத்தும் போது தான் அறிந்து கொள்ள முடியும். சில சமயங்களில் அதைக் கூட நம்மால் யூகிக்க இயலாமல் போய்விடும்.

அதே சமயத்தில் கணினித்துறையில் கள்ளச்சாவி தயாரிப்பது சற்றுக் கடினமானது. எத்தனை கடினமானது என்றால், நமது சாவியின் கடினத்

தன்மையைப் பொருத்தது. நமது கடவுச்சொல் எத்தனை கடினமானதாக, யூகிக்க முடியாததாக, அடிக்கடி மாற்றக் கூடியதாக இருக்கின்றதோ, எங்கும் சேமிக்கப்படாமல் மனதில் மட்டும் இருத்தப்பட்டிருக்கின்றதோ அத்தனை பாதுகாப்பானது என்று அறிந்து கொள்ளலாம்.

முற்றிலும் இலவசமான, திறவு மூல (Open source) கடவுச்சொல் மேலாளர்கள் (Password Managers) இப்போது நிறைய புழக்கத்தில் உள்ளன. அவற்றில் நமது கடவுச்சொற்களைப் பதிந்து வைத்துக் கொண்டு ஒரே ஒரு கடவுச்சொல் மூலம் அனைத்துக் கடவுச்சொற்களையும் சேமித்துக் கொள்ளலாம். ஒரே கடவுச்சொல்லைப் பல தளங்கள், மென்பொருட்களில் பயன்படுத்துவது தவறாகும். ஏதேனும் ஒரு தளத்தில் நமது கடவுச்சொல் திருடு போனாலும் நமக்குத் தான் அதில் நட்டமாகும்.

7. நகலெடுத்தல்:

இது கணினித் துறையில் மிகவும் பிரபலமானது மட்டுமின்றி நம்மில் பலரும் தெரிந்தோ தெரியாமலோ செய்திருக்கக் கூடிய விஷய(ம)மாகும்.

ஒரு நிறுவனம் அல்லது ஒரு தனிப்பட்ட நபர் தனது நேரத்தையும், சிந்தனையையும், உழைப்பையும் செலவளித்து ஒன்றை உருவாக்கி அதற்கு விலையொன்று வைத்திருக்க, அதை அவரிடம் இருந்து பிடுங்கிக் கொண்டு சென்று விடுவதே பைரசி எனப்படும் நகலெடுத்தல் ஆகும்.

ஒரு பொருள் விலை அதிகம் இருக்கின்றது என்பதற்காக அதைத் திருடுவது முறையாகாது. ஒவ்வொருவருக்கும் தான் உருவாக்கிய பொருளுக்கு விலை வைக்கும் உரிமை இருக்கின்றது தானே?

நகலெடுப்பது தவறென்று அறிந்தே ருசி கண்ட பூனையாக, திருட்டு மாங்காய் சுவையென தொடர்ந்து செய்வதால் தனிப்பட்ட நபர்களுக்கு அதிக பாதிப்பில்லை என்றாலும், பெரு நிறுவனங்கள் தங்கள் தகவலைப் பாதுகாப்பாய் நிர்வகிக்க அதிகார பூர்வ மென்பொருட்களையே உபயோகித்தல் நலம் பயக்கும். இதனால் அவ்வப்போது மென்பொருள் மேம்பாடு (Up gradation) , புதுப்பித்தல் (Update), புதிய பதிப்பை நிறுவுதல் மற்றும் மென்பொருள் சார்

பிரச்னைகளைத் தீர்க்க உதவும் சேவைகள் (Support) ஆகியவற்றைப் பெற ஏதுவாக இருக்கும்.

மேலும், நகலெடுக்கத் தேவையில்லாத அளவுக்குத் தற்போது இலவச மென்பொருட்களும் உலா வருகின்றன. அவற்றையும் உபயோகப்படுத்தலாம்.

8. நேர குண்டு:

ஒரு குறிப்பிட்ட நேரம் வரை ஒழுங்காக வேலை செய்யுமாறு அமைக்கப்பட்டு, அந்நேரம் முடிவடைந்தவுடன், செயலிழக்குமாறோ அல்லது மென்பொருட்களையும் தகவல்களையும் அழிக்குமாறோ உருவாக்கப்பட்டிருக்கும் மென்பொருட்களை இப்பெயரிட்டு அழைக்கின்றனர்.

எடுத்துக்காட்டாக வெள்ளிக்கிழமை 13ம் தேதி நேரகுண்டு என்று சொல்லலாம். மாதத்தின் 13ம் தேதி வெள்ளிக்கிழமையாக இருந்தால் இக்குண்டு வெடித்து (?!) தகவல்களுக்கு நாசம் விளைவிக்குமாறு எழுதப்பட முடியும்.

சில ஷேர்வேர் எனப்படும் பங்கு மென்பொருட்களிலும் இது போன்ற நேர குண்டுகள் இருக்கக்கூடும்.

9. கண்கட்டு: (Data Diddling)

கண்கட்டு என்னும் இந்த வகைக் குற்றம் உண்மையிலேயே சற்றுச் சுவாரசியமானது தான். தகவலை உள்ளீடு செய்பவருக்கும் தகவல் சேமிப்புக்கும் இடையே புகுந்து கொண்டு, உள்ளீடு செய்யும் தகவலை மென்பொருளொன்று மாற்றி மாற்றிச் சேமிப்பதால் ஏற்படும் பாதகங்களே கண்கட்டு என்று அழைக்கப்படுகின்றன.

1000 என்று உள்ளீடு செய்வதெல்லாம் 10000 என்று உள்ளீடு செய்வதாகக் கணினி சேமித்தால் எப்படி இருக்கும் என்று யோசித்துப் பாருங்கள்!

இதில் கைதேர்ந்த இன்னொரு விஷயம் என்னவென்றால், உள்ளீடு செய்யும் போது 1000 எனவும் தகவல்களைக் கணக்கிடும் போது (Processing) 10000 எனவும் மீண்டும் சேமிக்கும் போது 1000 எனவும் சேமிப்பது ஆகும்!

இதற்கெல்லாம் நம் நிறுவனத்திலேயே பணி புரியும் ஒருவரே காரணமாக இருக்கக் கூடும்.

10. ஆக்கிரமிப்பு: (Denial of Service - DoS Attack)

ஒரு அறைக்குள் செல்ல ஒரு வழி இருக்கின்றதென்றும், ஒரே நேரத்தில் அந்தப் பாதை வழியே பத்துப் பேர் செல்லலாம் என்றும் வைத்துக் கொள்வோம். அந்த வழியில் குண்டர்கள் பத்துப் பேர் அமர்ந்து கொண்டு நகர மறுத்தால் என்ன விளைவு ஏற்படுமோ அதே விளைவு தான் ஆக்கிரமித்தலிலும் நிகழ்கின்றது.

தேவையான தகவல் தேவையான சமயத்தில் **தேவையான நபருக்கு**க் கிடைக்க விடாமல் செய்வது இது. பத்தாம் வகுப்புத் தேர்வு முடிவுகளைக் காலையில் பார்ப்பதற்கும் மாலையில் பார்ப்பதற்கும் இருக்கும் வித்தியாசத்தை எடுத்துக்காட்டாகச் சொல்லலாம்.

இணைய வழங்கிகள், தனிப்பட்ட வழங்கிகள் மேல் இது போன்ற தாக்குதல் அடிக்கடி நடைபெறுகின்றன.

ஒரே ஒரு கணினியை வைத்துக் கொண்டு, ஒரு இணைய தளத்தை 1000 பேர் ஒரே நேரத்தில் பார்க்க விரும்புவது போல் மென்பொருட்கள் மூலம் வழங்கியை முற்றுகையிட்டு வேறு யாருமே அந்த இணைய தளத்தைக் காண இயலாதவாறு செய்து விடுவது ஆக்கிரமிப்பு இல்லாமல் வேறென்ன?!

ஆயினும், இது போன்ற தாக்குதல்களை முறியடிக்க வழங்கிகளிலேயே பல வசதிகள் தற்போது வந்திருப்பது சற்று ஆறுதல் அளிக்கின்றது.

இப்போது விநியோகமுறை ஆக்கிரமிப்பு (Distributed Denial of Service - DDoS) கூட வந்து பல இணைய முகவரிகளிலிருந்து ஒரே நேரத்தில் ஆக்கிரமிப்பு செய்வதும் நிகழ்கின்றது. இணைய வழங்கியாளர்கள் மிகவும் விழிப்புடன் இருக்க வேண்டிய தருணம் இது.

11. ஏமாளி, கோமாளி: Piggybacking

இந்த வகைக் குற்றத்தில் ஏமாளியாக இருப்பவர் கோமாளியாக முகத்தில் கரிபூசப்படுகின்றார். அதாவது தனது கணினியிலிருந்து சரியான முறையில் வெளியேறாமல் அப்படியே வைத்து விட்டுச் சென்று விடுகின்றார் என்று வைத்துக் கொள்வோம், அவர் சென்ற சில

நிமிடங்களில் அடுத்து வருபவர் அவரது தகவல்களை உபயோகிப்பதால் பல கெடுதல்கள் நிகழக் கூடும்.

பொது இணைய மையங்களில் வாடகைக்கு ஒரு இருக்கையைத் தேர்ந்தெடுத்துக் கொண்டு தனது சொந்தத் தகவல்களைப் பகிர்ந்து கொள்ளும் பலர் தனது பயனர் பெயர், கடவுச்சொல் ஆகியவற்றை அழிப்பது மட்டுமின்றித் தகுந்த முறையில் அனைத்து இணையதளங்களில் இருந்தும் வெளியேறி இருத்தல் அவசியமாகும். இல்லாவிடில் ஏமாளியாகிக் கோமாளியாக வேண்டியது தான்.

12. சிறுதுளி பெருவெள்ளம்: Salami attack

சிறுதுளி பெருவெள்ளம் என்பது சேமிப்புக்கு உகந்தது தான். ஆனால், அதுவே மென்பொருள் குற்றம் என்று வரும் போது அது மிகப்பெரிய தவறாகவும் ஆகிவிடும்.

இது பொதுவாக மென்பொருள் தயாரிப்பில் விடப்படும் கோளாறாகும்.

ஒரு வங்கியில் ஒவ்வொரு நிகழ்வில் இருந்தும் மிகக் குறைவான (1 ரூபாய்க்கும் கீழ்) தொகையை ஒருவர் தன் கணக்குக்கு மாற்றியமைப்பது போன்று மென்பொருள் எழுதியிருந்தால், அது சில நாட்களில் கோடியைத் தொட்டு விடும் வாய்ப்பு ஏற்பட்டு விடும். இது ஊகமல்ல. இது போன்ற மோசடிகள் உண்மையிலேயே நிகழ்ந்திருக்கின்றன என்பது குறிப்பிடத் தக்கது. மேலும் இது சிற்சில மாறுதல்கள் கொண்டு கண்டுபிடிக்க இயலாதவாறு அமையக் கூடும். சில சமயங்களில் நாம் மென்பொருள் உருவாக்கத்தில் தெரியாமல் விட்ட தவறால் அதிகமான தொகையை இழக்கக் கூடியதாகவும் இருக்கலாம்.

எடுத்துக்காட்டாக, ஒரு வங்கியில் லீப் ஆண்டிலும் 365 நாட்களுக்கே வட்டி போடுவதாக மென்பொருள் எழுதியிருந்தால், அந்த வங்கியின் மொத்தக் கடன் தொகையில் ஒரு நாளைக்கான வட்டி சில கோடிகளை இழக்க நேரிடலாம்!

அதாவது காண்பதற்குச் சிறிதாகத் தோன்றினாலும் பெரிய அளவில் பாதிப்பை ஏற்படுத்துவதே சிறுதுளி பெருவெள்ளம் எனப்படுகின்றது.

சிறு உளியும் பெருமலையை நகர்த்தி விடும் அல்லவா? எனவே மென்பொருள் உருவாக்கத்தின் போது மிகுந்த கவனத்துடன், ஒவ்வொரு விஷயத்தையும் பல்வேறு கோணங்களில் அலசி ஆராய்ந்து செயல்படவேண்டும் என்பதை அறிந்து கொள்ளலாம்.

13. குப்பையில் மாணிக்கம். Scavenging

அப்பாடி! பல கெடுதல்களுக்கிடையிலும் நன்மை கிடைக்க இருக்கின்றது போல என்று நிம்மதிப் பெருமூச்சு விடுகின்றீர்களா?! அது தான் இல்லை!

நாம் குப்பை என்று ஒதுக்கி வைக்கும், அழித்து விட்ட தகவல்களில் இருந்து அதை மீண்டும் யாரேனும் கெட்ட எண்ணம் உடையவர்கள் கிளறிப் பெறுவதை இவ்வாறு சொல்லியிருக்கின்றேன்!

எனவே முக்கியமான கோப்புக்களை அழிக்கும் போது கூட மிகுந்த கவனம் தேவை. அதை மீளப் பெற முடியாதவாறு அழிக்க நிறைய மென்பொருட்கள் இருக்கின்றன.

தகவல்கள் குப்பையில் இருந்தாலும் அவை மாணிக்கங்களே என்பதைப் புரிந்து கொண்டு அதைப் பாதுகாத்தல் அவசியமாகும்.

14. பயிர் மேயும் வேலி:

வேலியே பயிரை மேய்கின்றது என்ற சொற்றொடரைக் கேட்டிருப்போம். கணினித் துறையில் இது எவ்வாறு குற்றங்கள் செய்ய ஏதுவாக இருக்கின்றது என்று காண்போம்.

ஒரு குறிப்பிட்ட மென்பொருளை நம்பிக்கையான ஒருவரிடம் இருந்து வாங்குகின்றீர்கள். அந்த நம்பிக்கையானவர் அம்மென்பொருளில் ஒரு குறுக்கு வழி அல்லது கள்ள வழி (Trap door/back door) வைத்து அதன் மூலமாக எப்போது வேண்டுமானாலும் அவர் நுழையவும் தகவல்களைத் திருடிக் கொண்டும் இருந்தால் அது பயிர் மேயும் வேலி எனலாம்.

நம்பகமான மென்பொருளினூடே பாதுகாப்பற்ற மென்பொருளும் இணைந்து வந்து தகவலுக்கு ஊறு விளைவிப்பதைத் தவிர்க்க தீச்சுவர்,

பதிவேடு (Log) ஆகியவற்றின் மூலம் பாதுகாப்பை பலப்படுத்த வேண்டும். மேலும், வெளிநபர்கள் கணினியின் பிணையத்துக்குள் அதிகாரமில்லாமல் நுழைவது அனுமதிக்கவே படக் கூடாது, அவர் மென்பொருள் உருவாக்கியவராக இருப்பினும் கூட. அப்போது தான் வேலி பயிரை மேயாமல் பார்த்துக் கொள்ள இயலும். அதாவது வேலிக்கும் பயிருக்கும் இடையில் இன்னொருவருடைய மின்வேலி இடுவதைப் போன்றது இது.

14. கடவுள் பாதி மிருகம் பாதி. (Trojan horse)

நன்மை செய்வது போல் உள் நுழைந்து தீமையும் செய்யும் மென்பொருட்களை இவ்வாறு அழைக்கலாம்.

அதிகாரபூர்வமான மென்பொருளினூடே அதிகாரபூர்வமற்ற தகவல்களை அழிக்கின்ற மென்பொருளும் இணைந்தே இருப்பதை இவ்வகையில் சேர்க்கலாம். மேலே குறிப்பிட்ட வேலி பயிரை மேய்வதற்கும், இதற்கும் இருக்கும் வேறுபாடு என்னவெனில், வேலி பயிரை மேய்வதில் மென்பொருள் உருவாக்குபவருக்கும் பங்கிருக்கும், இந்தத் தாக்குதலுக்கு அவ்வாறு இருக்க வேண்டிய அவசியம் இல்லை. நாம் அறிந்திராத மூன்றாம் நபரும் இதில் சம்பந்தப்பட்டிருக்கக் கூடும்.

அதிக அளவில் நகலெடுக்கும் மென்பொருட்களில் இவையும் சேர்ந்தே பரவுகின்றன என்பது குறிப்பிடத் தக்கது.

ட்ராஜன் எனப்படும் பெரிய குதிரைச் சிலைக்குள் பல வீரர்கள் பதுங்கி இருந்து, பரிசு போல கோட்டைக்கு உள்ளே நுழைந்து கோட்டையைத் தகர்த்த கதையைப் போன்றிருப்பதால் இதற்கு இப்பெயர் வந்தது.

15. உளவாளி/ஒற்றன்:

ஒரு கணினியின் அனைத்துப் பாதுகாப்புச் செயல்பாடுகளையும் தாண்டி அதில் ஊடுருவி வெற்றி காண்பவரை இவ்வாறு அழைக்கின்றோம். ஹேக்கர் என்ற பெயரில் சாதாரணமாக இவரை அறிந்திருப்போம். இவரது நோக்கம் தகவலை அழிக்க என்றில்லாது பொழுது போக்காக என்றும் இருக்கக் கூடும். அவ்வாறில்லாது தகவலை அழிப்பாரேயானால் அவரை க்ராக்கர் (Cracker) என்றழைக்கின்றனர்.

இதற்கென்று பல மென்பொருட்கள் இணையத்தில் உலா வருகின்றன.

கடவுச்சொல்லைக் கண்டறிவதிலிருந்து தீச்சுவரை உடைப்பது என்று பல கருவிகள் இவர்களிடம் இருக்கின்றன.

சில சமயங்களில் தமது பாதுகாப்பை உறுதிப்படுத்திக் கொள்வதற்காக சில நிறுவனங்கள் சம்பளம் தந்தே இது போன்ற ஒற்றர்களைப் பணியில் அமர்த்தி இருக்கின்றன என்பது குறிப்பிடத்தக்கது.

16. விளம்பரச் சாத்தான்:

இணையத்தில் வலம் வரும் போதும் சரி, நமக்கு வந்த மின்னஞ்சலைப் பார்வையிடும் போதும் சரி, தவறான இணைய முகவரியைச் சில சமயங்களில் கொடுக்கும் போதும் சரி எத்தனையோ விளம்பரங்கள் நம் கண்முன்னே வந்து செல்கின்றன. அவற்றில் எத்தனை நமக்கு உண்மையிலேயே பயனுள்ளதாக இருந்தன என்பதை யோசித்துப் பார்த்திருக்கின்றோமா?

அவற்றில் பலவற்றைக் குப்பைகள் தான் என்பதை நாம் இனங்கண்டு அதை ஸ்பாம் மின்னஞ்சல்கள், விளம்பரங்கள் என்று ஒதுக்கி விடுகின்றோம் தானே? அப்படியான மின்னஞ்சல்கள் எப்படி நம் முகவரியைச் சரியாக வந்தடைகின்றன? நாம் எப்போதாவது எங்கேனும் இணையத்தில் நம் மின்னஞ்சல் முகவரியைக் கொடுத்துச் சில தகவல்களைப் பெற்றிருப்போம். இத்தகைய மின்னஞ்சல் முகவரிப் பட்டியல்களை விற்பதே ஒரு பெரிய வணிக நோக்கமாக இருக்கின்றது என்பதை நாம் தெரிந்து கொள்ள வேண்டும். சரியாக மின்னஞ்சல் சென்றடைந்து விட்டது என்பதை நிரூபிக்கும் மின்னஞ்சல்களை அனுப்புவதற்கென்று பணம் தர நிறுவனங்கள் தயாராக இருக்கின்றன. சமீபத்தில் கூட வேலூரில் இது போன்று மின்னஞ்சல்களை அனுப்புவதற்கு ஒப்பந்தத்திற்கு என்று ஒருவர் ஏமாற்றி இருப்பதைக் கேள்விப்பட்டிருப்போம்.

பத்து மின்னஞ்சல்களில் ஒரு மின்னஞ்சல் குப்பை என்றால் பரவாயில்லை. ஆனால் ஆயிரம் குப்பை மின்னஞ்சல்களுக்கிடையே ஒரு உருப்படியான மின்னஞ்சல் வந்தால் என்ன ஆகும் என்று யோசித்துப் பாருங்கள்! நமக்குத் தேவையான மின்னஞ்சலும் சேர்த்தே அழித்து விடும்

தவறு நிகழ வாய்ப்பிருக்கின்றது. இத்தனை குப்பைகளைக் கிளறி நமக்கான மின்னஞ்சலைக் கண்டறிவது மிகவும் கடினமே என்பதை அனுபவித்தவர்களிடம் கேட்டுப் பார்த்தால் அறியலாம்.

சில விளம்பரங்களில் இருக்கும் தொடுப்புக்களைச் சொடுக்கினால் சில வைரஸ் மென்பொருட்களைக் கூட தரவிறக்குமாறு மின்னஞ்சல்கள் வருகின்றன. சில மின்னஞ்சல்களிலேயே வைரஸ்களும் வருகின்றன.

இது தவிர, நமது வங்கிகளில் இருந்தே வருவது போன்ற தோரணையில் கடனட்டை எண்ணைப் பெற முயற்சிக்கும் மின்னஞ்சல்களும் அதிகம். எனவே மிகவும் கவனமாக இருத்தல் அவசியமாகும்.

17. தகவல் அடிமை:

நமது கணினியிலிருந்து மிக முக்கியமான ஆவணங்கள்/தகவல்களை எடுத்துச் சென்று கொண்டு, அது மீண்டும் கிடைக்க வேண்டுமென்றால் ஒரு குறிப்பிட்ட எண்ணுக்கு குறுந்தகவல் அனுப்பி வைக்க வேண்டும் என்ற மிரட்டல் விடும் கும்பல் களமிறங்கி இருப்பதைக் கண்டறிந்திருக்கின்றனர்.

நாம் ஒருவருக்குக் குறுஞ்செய்தி அனுப்புவதால் அவருக்கு என்ன லாபம் என்று நீங்கள் கேட்கலாம். குறுஞ்செய்தி பெறுவதற்கென்று பணம் வாங்கவும் இப்போது வசதி இருக்கின்றது. மேலும், உங்களின் மொபைல் எண் குறிப்பிட்ட நபரிடம் சிக்கிக் கொள்கின்றது. அதை வைத்து உங்கள் எண்ணுக்கு விளம்பரங்கள்/ஸ்பாம் அஞ்சல்கள் அனுப்பி அவர் பணம் சம்பாதிக்க இயலும்.

பத்து நொடிக்கொரு முறை ஒரு குறுஞ்செய்தி வந்து கொண்டிருந்தால் உங்கள் அலைபேசியின் நிலை என்ன என்பதை யோசித்துப் பார்க்கவும்!

தகவல்கள் நமக்கு அடிமையாக இருக்கலாமே அன்றி, தகவலுக்கு நாம் அடிமையாகும் அளவுக்கு இருத்தல் கூடாது. எந்த நேரத்திலும் தகவலை நம்

கைக்கட்டுப்பாட்டுக்குள் வைத்திருக்க வேண்டும் என்பதையுமே இது உணர்த்துகின்றது.

18. பாலியல் கொடுமை:

இணையத்தில் 50 சதவீதத்துக்கும் மேல் ஆபாச தளங்கள், பாலியல் தளங்கள் விரவிக் கிடக்கின்றன. இவற்றில் பல தளங்களில் தளத்தில் நுழைவதற்கு இலவசம் என்றும், தங்கள் வயதைச் சரிபார்க்க மட்டும் கடனட்டை எண் தரவேண்டும் என்றும் விளம்பரம் செய்திருப்பார்கள். இன்னும் சில தளங்களில் சோதனை முறையில் தளத்திற்குள் நுழைய ஓரிரு நாட்களுக்குக் குறைந்த கட்டணம் என்றும் வைத்திருப்பார்கள். இவை அனைத்துமே மீன்களுக்கு இடப்படும் தூண்டில்களே!

தூண்டிலில் மீன் சிக்கி விட்டால் அம்பேல் தான். தெரியாமல் தவறி கடனட்டை எண்ணை வழங்கி விட்டால், மாதா மாதம் சந்தா தாரராக்கி குறைந்த பட்சம் 1000 ரூபாய்க்கு மேல் கடனட்டை எண்ணிலிருந்து கறந்து கொண்டே இருப்பார்கள். நமக்கு வரும் கடனட்டை அறிக்கையில் இது எந்தத் தளத்திற்காக என்று இருக்காது. யாருக்கும் தெரிந்து விடக் கூடாது என்பதில் கடனட்டை தாரர் வேறு வழியின்றி அந்தப் பணத்தைக் கட்ட வேண்டிய சூழ்நிலைக்கு ஆளாவார்.

நமது சந்தாவை நிறுத்த நாம் யாரைத் தொடர்பு கொண்டாலும் சரியான பதில் கிடைக்காது. தவிர, அவ்வாறு சந்தாவை நிறுத்தியே ஆக வேண்டும் என்று மின்னஞ்சல் மூலம் மிரட்டினால் அடுத்த மாதத்திலிருந்து வேறொரு தளத்திலிருந்து கடனட்டை எண்ணைப் பயன்படுத்திப் பணம் சுருட்டப்படுமாம்.

இதை வெளியிலும் சொல்ல முடியாமல், திருடனுக்குத் தேள் கொட்டியது போல் தாங்கிக் கொண்டு இருக்க வேண்டியது தான் என்கின்றனர்.

19. வைரஸ்:

வைரஸ். இதைப் பற்றிச் சொல்லித் தான் நமக்குத் தெரிய வேண்டுமா என்ன? கணினித் துறையில் தகவல்களுக்கும், மென்பொருட்களைச் சிறந்த முறையில் உபயோகப்படுத்துவதற்கும் கண் முன்னே நிற்கும் எதிரியாகப் பல வடிவங்களில், பல தினுசுகளில் வைரஸுகள் இருக்கின்றன.

இன்றைய தேதியில் கோடிக்கும் மேலான வைரஸ்கள் இனங்காணப் பட்டுள்ளன! ரூம் போட்டு உக்கார்ந்து யோசிப்பாய்ங்களோ என்று திரைப்படத்தில் வசனம் வருவது போல, இதையும் வேலை மெனக்கெட்டு எழுதுவதற்கு ஆட்கள் இருக்கின்றார்களே என்று தான் நினைக்கத் தோன்றுகின்றது.

முதலில் வைரஸ் என்றால் என்ன என்று பார்க்கலாம். இதைக் கண்டறிந்தவர்கள் மிகச் சரியான பெயரிட்டிருக்கின்றனர். வைரஸுக்கு என்று உயிர் கிடையாது. ஆனால் அது ஒரு செல்லுடன் ஒட்டிக் கொண்டால் உயிர் பெறுகின்றது. இயக்கம் பெறுகின்றது. வைரஸ் மட்டும் தனித்திருந்தால் அதனால் எதுவும் நடத்த இயலாது. வைரஸ் என்பது ஒரு கெட்ட நோக்கமுடைய மென்பொருளாகும். இந்த மென்பொருள் தனித்திருந்தால் இயங்காது. ஆனால், இதை இன்னொரு இயங்கக் கூடிய (Executable) மென்பொருளுடன் சேர்த்து அனுப்பப்படுகின்றது.

இதன் தன்மை இரண்டு ஆகும். ஒன்று, எப்போதெல்லாம் இந்த இயங்கும் மென்பொருள் இயக்கப்படுகின்றதோ அப்போதெல்லாம் மற்ற இயங்கும் மென்பொருட்களில் நகலெடுத்துக் கொண்டு ஒட்டிக் கொள்வது. அதன் மூலமும், மேலும் அந்த இயங்கும் மென்பொருள் எங்கெல்லாம் நகலெடுத்து மற்ற கணினிகளில் இயக்கப்படுகின்றதோ அங்கும் நகலெடுத்துக் கொண்டு பரவுவதும் ஆகும். இரண்டாவதாக, இந்த வைரஸ் இணைந்திருக்கும் மென்பொருள் இயங்க ஆரம்பிக்கும் போது, இந்த வைரஸில் குறிப்பிடப் பட்டிருக்கும் கட்டளைகளும் உயிர் பெற்று தகவல்கள் அழிப்பு, மற்ற மென்பொருட்களை ஏன் சில சமயங்களில் வன் தட்டுக்களையே இயங்க விடாமை போன்ற மோசமான நாசகார விளைவுகளை ஏற்படுத்த வல்லவையாக இருக்கின்றன.

வைரஸுகளால் எரிச்சலும், கணினியின் செயலாதாரங்கள் (resources) நிலைகுலைக்கப்படுவதும் மேலும் பிரச்னையைச் சிக்கலாக்குகின்றது. இது போதாதென்று வைரஸுகளைக் கண்காணிக்கும், நீக்கும் மென்பொருட்களுக்கென்று செலவளிக்க வேண்டிய கட்டாயம் ஏற்படுகின்றது. மேலும் அவைகளும் கணினியின் நினைவகத்தில் அமர்ந்து கொண்டு நமது கணினியின் செயலாதாரங்களைச் சிறந்த முறையில் உபயோகிப்பதில் இருந்து நமக்குத் தடையாக இருக்கின்றன.

ஆக மொத்தத்தில் வைரஸ்களால் எத்தனை பிரச்னைகள் என்பதை வெறும் வார்த்தைகளால் சொல்லி விட முடியாது என்பது தான் உண்மை.

20. புழுக்கள்: (Worms)

வைரஸும் புழுக்களும் ஒன்று என்றல்லவா இத்தனை காலம் நினைத்திருந்தோம்? இரண்டும் வெவ்வேறா? என்று கேட்கத் தோன்றுகின்றதல்லவா?

வைரஸ்கள் போலல்லாமல் புழுக்களுக்கென்று உயிர் உண்டு! தானே இயங்கி நெளிந்து கலக்கும் வல்லமை உடையது புழு ஆகும்! இவை இணையத்தில் கணினிகளுக்கிடையேயான தகவல் போக்குவரத்தில் பரிமாறிக் கொள்ளப் படுகின்றன. அதிக அளவில் பாட்டை அகலத்தை (Bandwidth) ஏப்பமிடும் புழுக்கள் தானாகவே இயங்குவதுடன், தன்னைத் தானே நகலெடுத்துக் கொண்டு பிணையத்திலும் இணையத்திலும் வலம் வருகின்றன!

தானாகவே இயங்க முடிவதால், வைரஸ்களைக் காட்டிலும் புழுக்கள் பயங்கரமானவையே!

புழுக்கள் பெரும்பாலும் இயங்குதள மென்பொருட்களில் இருக்கும் ஊடுருவ முடிகின்ற (Vulnerability) பி(இ)ழைகளின் வழியாக உள்நுழைகின்றன. எனவே அடிக்கடி மென்பொருள் வழங்குபவர் தரும் துளை மூடிகள் அல்லது ஒட்டுப் போடும் மென்பொருட்களைத் (Security Patches) தரவிறக்கி நிறுவிக் கொள்தல் வேண்டும்.

மென்பொருட்கள் எழுதப்படும் போது பிழைகள் நேர வாய்ப்புண்டு. எடுத்துக்காட்டாக,

```
dim a(10)
dim max,i = 0
for i = 1 to 10
input a(i)
if a(i) > max then
max = a(i)
endif
next
print "Maximum is",max
end
```

மேலே கண்ட சிறு மென்பொருள் கொடுக்கப்படும் பத்து எண்களில் எது பெரியது என்பதைக் கண்டறிய எழுதப்பட்டது ஆகும். மேலோட்டமாகக் காண்பதற்குச் சரியானதாகவே தெரியும் இந்த மென்பொருளில் ஒரு பிழை இருக்கின்றது. அதாவது அனைத்து எண்களுமே பூஜ்ஜியத்துக்கும் குறைவானதாக இருக்கின்றது என்று வைத்துக் கொள்வோம். எடுத்துக்காட்டாக -2,-3,-4 ... என்று இருந்தால் இந்த மென்பொருள் 0 தான் மிகப்பெரிய எண் என்று பத்து எண்களில் இல்லாத ஒரு எண்ணை வழங்கக் கூடும்! ஆக, இது ஒரு மென்பொருள் பிழை.

இதையே,

```
dim a(10)
dim max,i = 0
input a(1)
max = a(1)
for i = 2 to 10
input a(i)
if a(i) > max then
```

```
max = a(i)

endif

next

print "Maximum is",max

end
```

என்று மாற்றிவிட்டால் சரியாகி விடும்.

எந்த ஒரு புது மென்பொருள் வந்தாலும் அதிலிருக்கும் பாதுகாப்புத் துளைகளைத் தேடுவதே பலரின் பொழுதுபோக்காகும்!

புழுக்களைக் கண்டறியும் ஒரு எளிய வழி, நாம் இணையத்தை உபயோகிக்கவே செய்யாவிட்டால் கூட, நமது கணினி இணையத்தைத் தொடர்பு கொண்டே இருக்குமானால், அது நிச்சயமாகப் புழுவின் கைங்கரியம் தான் என்று அறிந்து கொள்ளலாம். ஏனெனில், புழுக்கள் அடிக்கடி இணையத்தில் இன்னொரு கணினியைத் தாக்குவதற்காகத் தேடிக் கொண்டே இருக்கும்.

இனிச் சில சமீபத்திய தாக்குதல்களைப் பற்றியும் அறிந்து கொள்ளலாம்.

இதில் முதலில் வருவது Phishing எனப்படும் இரட்டை வேடம்!

திரைப்படங்களில் இரட்டை வேடத்தில் வருபவர்கள் ஒருவருக்கொருவர் உருவ ஒற்றுமையைப் பயன்படுத்தி நிச்சயம் இடம் மாறி சாதனை செய்வார்கள். இல்லாவிடில் இரட்டை வேடம் என்பதே தேவையில்லை தானே?

அதே போல் இங்கேயும் நமக்கு மிகவும் நம்பகமான, நாம் அடிக்கடி செல்லும் தளத்தைப் போன்றே தளத்தை உருவாக்கி நம்மை ஏமாற்றிக் கடனட்டை எண்கள், தகவல்கள், மின்னஞ்சல் முகவரிகள் ஆகியவற்றைப் பெறும் மோசடிகள் பல நடைபெறுகின்றன.

இந்த இரட்டை வேடத்தில் நாம் கண்டறிய மிகவும் கஷ்டப்படும் விஷயம் என்னவென்றால் Spoofing. அதாவது உருவ ஒற்றுமை. (நன்றி விக்கிபீடியா)

1. இரண்டு URLகள் பார்க்க ஒன்றே போல் தோற்றமளித்தாலும், இரண்டும் வெவ்வேறு தளங்களுக்குச் செல்லக் கூடும்! எடுத்துக்காட்டாக http://www.paypal.com முகவரியும், http://www.paypal.com/ என்ற முகவரியும் ஒன்றல்ல! என்ன? ஆச்சரியமாக இருக்கின்றதா? உண்மை தான். இரண்டும் ஒன்றல்ல. இதை IDN_homograph_attack என்றழைக்கின்றனர். முதலில் இருக்கும் 'a' வில் ஒன்று ஆங்கிலம், மற்றொன்றில் இருக்கும் 'a' Cyrillic என்னும் மொழியில் இருக்கும் எழுத்தாகும்! பார்க்கத் தான் இரண்டும் ஒன்று!

2. இது தவிர 'o'க்குப் பதிலாக '0' போடுதல், 'i'க்குப் பதிலாக '1' போடுதல், 'm' க்குப் பதிலாக 'rn' போடுதல், 'w' க்குப் பதிலாக 'vv' போடுதல் என்று ஏமாற்றுவதும் நடக்கின்றது.

3. இன்னொரு விதம் http://www.yourbank.example.com இந்த முகவரி காண்பதற்கு yourbankன் இணைய தளத்தின் example என்ற பக்கத்துக்குச் செல்வதாகத் தோன்றினாலும் உண்மையில் செல்வதோ example.com என்னும் இணைய தளத்தின் yourbank என்னும் பக்கத்துக்கு!

4. அப்புறம் சொல்வதொன்று செய்வதொன்று! எடுத்துக்காட்டாக http://muthamilmantram.com/viewforum.php?f=147 இப்படி ஒரு முகவரி இருக்கக் கூடும். அதாவது காண்பதற்கு ஒரு பக்கத்துக்குப் போவது போல் தோற்றமளித்தாலும் போவதென்னவோ மற்றொரு பக்கத்துக்கு.

இப்படி ஏதாவது ஒரு விதத்தில் நம்மை மயக்கி வேறொரு தளத்துக்கு நம்மை இட்டுச் சென்று நம்மிடம் இருக்கும் தகவல்களை நம் வாயிலிருந்தே வரவைப்பது மிகவும் சாதாரணமாக நடந்து கொண்டிருக்கின்றது.

இணையத் தீவிரவாதம்:

இப்போது பரவி இருக்கும் மற்றொரு கொடுமை இணையத்தின் மூலம் நடைபெறும் தீவிரவாதம் ஆகும். தீவிரவாதிகள் கையிலும் இணையமும் தகவல் புரட்சியும் சிக்கி இருக்கின்றது. அவர்களும் இதையெல்லாம் தங்கள் அழிவு மற்றும் நாசகாரத் திட்டங்களுக்கு இவற்றைப் பயன்படுத்திக் கொள்ள இயலும்.

முக்கியமாக, நம் இல்லங்களில் பயன்படுத்தும் கம்பியில்லா இணைய வழிகாட்டி (WiFil Router) தகுந்த படி பாதுகாப்பு செய்யப்படவில்லையெனில், நமது இணைய இணைப்பு மூலமே யார் வேண்டுமானாலும் இணையத்தில் தொடர்பு ஏற்படுத்தித் தகவல் அனுப்ப முடியும். இதை நம் வீட்டுக்கு அருகில் இருந்து ஒரு தீவிரவாதி செய்தால், நமது ஐபி முகவரி தான் முதலில் பதிவாகும். இப்படிப் பல முறை அப்பாவிகள் மாட்டிக் கொள்ளும் நிகழ்வு நடந்திருக்கின்றது.

இணையம், கைபேசி, மின்னஞ்சல் ஆகியவற்றை மிக நவீன முறையில் நூதனமாகவும் சாதுரியமாகவும் பயன்படுத்துகின்றனர் தீவிரவாதிகள் என்று கண்டறிந்திருக்கின்றனர்.

சரி. இப்போது ஒரு அதிர்ச்சியான விஷயமும் சொல்லப் போகின்றேன்.

2007ல் ஒரு நிறுவனம் எடுத்த ஆய்வின் படி, 120 நாடுகளே இணையத்தை ஆயுதமாகப் பயன்படுத்தி இன்னொரு நாட்டின் நிதி ஆதாரத்தை முடக்கவும், அந்நாட்டு அரசின் கணினிகளை முடக்கவும், தகவல்களைச் சேகரிக்கவும் செய்து இணையப் போர் நடந்து கொண்டிருக்கின்றது என்பது தான் அந்த அதிர்ச்சி விஷயம்.

சீனா தான் இதில் முதலிடத்தில் இருக்கின்றது என்பது குறிப்பிடத் தக்கது. சீனாவுக்கு இந்தியா, ஜெர்மனி மற்றும் அமெரிக்கா ஆகிய நாடுகளின் கணினிகள் மீது தான் கண்ணாம். மேலும், உலகிலேயே அதிகக் கணினிகளை வசப்படுத்தி அவற்றில் இருந்து தகவல்களைச் சேகரிக்கும் வலிமை கொண்ட புழுக்களைப் (botnet/Zombie computers) பரவ விட்டிருக்கின்றது சீனா என்றும் கண்டறிந்திருக்கின்றனர். ஆனால், இதையெல்லாம் சீனா மறுத்து வருகின்றது.

எடுத்துக்காட்டாக, 28, மார்ச், 2009 அன்று ஒரு இணைய ஒற்று அமைப்பு, சீனாவில் இருந்து இயங்கும் வழங்கிகளின் மூலமாக, 103 நாடுகளின் முக்கிய ஆவணங்களை நகலெடுத்தது. அவற்றில் திபெத் சம்பந்தப்பட்ட ஆவணங்களும் அடக்கம். ஆனால் இதைச் சீனா மறுத்து வருகின்றது.

அதன் தொடர்ச்சியாக ஏப்ரல், 2009ல் அமெரிக்கா, 100 மில்லியன் அமெரிக்க டாலர்களைக் கடந்த ஆறு மாத காலங்களாக, இணையப்

போரினால் ஏற்பட்ட அழிவிலிருந்து மீள செலவளித்திருப்பது குறிப்பிடத் தக்கது!

சமூகத் தளங்கள் மூலம் முற்றுகை:

ஆர்குட், பேஸ்புக் போன்ற தளங்களை அறியாத இளைஞர்களைத் தற்போது காண்பது அரிதாக இருக்கின்றது. இத்தளங்களில் உறுப்பினர்களாக இருப்பவர்களுக்கு, அந்தத் தளங்களில் இருந்தே இன்னொருவர் மூலமாக, நண்பர் அனுப்புவது போன்று குறிப்பிட்ட யூடியூப் படம் அருமையாக இருக்கின்றதென்றும், அதைக் காணும் தொடுப்பு இது என்றும் மின்னஞ்சல் அல்லது தகவல் அனுப்பப்படும்.

நண்பர், அதன் நோக்கத்தை அறியாமல், அந்தத் தொடுப்பைச் சொடுக்கினால், கணினியின் ஃப்ளாஷ் தொழில்நுட்ப மென்பொருளை மேம்பாடு செய்யவா என்று கேள்வி கேட்கப்படும். அவர், ஆம் என்றதும், ஃப்ளாஷ் தொழில்நுட்ப மென்பொருள் என்ற போர்வையில் புழுக்கள் இறக்குமதி செய்யப்படும். பின்னர் தொடுப்பிலுள்ள அசைபடம் காட்டப்படும். நண்பர் மகிழ்ச்சியாகப் படம் பார்த்து விட்டு பாதிக்கப்பட்ட கணினியைக் கொண்டவராக மாறிவிடுவார்!

Web 2.0 எனப்படும் சமீபத்திய இணைய மொழி மேம்பாட்டினாலேயே யூ டியூபிலிருந்து, ஆர்குட் வரை பல தளங்கள் இயங்க முடிகின்றது. எனவே அவற்றின் மூலமும் தாக்குதல் இப்போது தொடர ஆரம்பித்திருக்கின்றது.

இதுமட்டுமல்ல, உலாவியின் முகவரிப் பட்டையையே மாற்றிக் காட்டக் கூடிய எத்தனான ஜாவா வரிவடிவங்கள் இருக்கின்றன. மேலும் உண்மையாகவே ஒரு வங்கியின் தளத்தில் இயங்கிக் கொண்டிருக்கும் போது அந்த வங்கியின் தகவல் சேமிப்புப் படிவம் போன்றே பாப்-அப் எனப்படும் முன் காட்டும் சட்டத்தின் மூலமாகத் தகவலைத் திருடும் ஜாவா வரிவடிவங்களும் கண்டறியப்பட்டிருக்கின்றன!

இணைய இயந்திர மனிதன்: Botnets

இணைய இயந்திர மனிதன் முதன் முதலாக நல்ல விஷயங்களைச் செய்வதற்கு மட்டுமே பழக்கப்படுத்தப்பட்டிருந்தான். நமது மன்றத்தின் முகப்பில் கூட எப்போதாவது GoogleBot என்னும் இயந்திர மனிதனும் நம்முடன் உலாவிக் கொண்டிருப்பதை நீங்கள் கண்டிருக்கக் கூடும்!

கூகுளில் எதைத் தட்டினாலும் தேட முடியும் என்றால் அதற்குக் காரணம் இந்த இணைய இயந்திர மனிதன் தான். இதை இணைய உறிஞ்சி (Web Crawler) என்றும் செல்லமாக அழைக்கின்றனர்! இணையத்தை வலைப்பின்னல் என்றழைத்தால், இவனை அதில் மேயும் இணைய எட்டுக்கால் பூச்சி (Web Spider) என்கின்றனர்!

இவன் வேலை அடிக்கடி இணைய தளங்களில் புதுப்பிக்கப்படும் செய்திகளைத் தன் தேடுபொறியில் சேமித்துக் கொள்வது தான். இதனால் தான் கூகுளில் தேடும் போது உடனே நமக்கு புதுப்பிக்கப்பட்ட செய்தியும் சேர்ந்தே காணக் கிடைக்கின்றது.

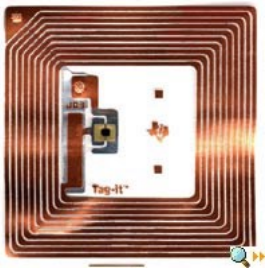
இதுவரை கேட்பதற்கு நன்றாகத் தான் இருந்தது! ஆனால், இதே இயந்திர மனிதன் கெட்டவர்கள் கையில் சிக்கி விட்டால் பூதமாக மாறி விடுகின்றான். இணைய வலையில் நட்டநடுவில் அமர்ந்து கொண்டு அனைத்துக் கணினிகளையும் ஆட்டிப் படைத்து அவற்றிலிருந்து தகவல்களையும் கோப்புக்களையும் கடத்தும் பணியினை அசராமல் செய்து கொண்டிருக்கின்றான். இவன் கண்களில் இருந்து தப்புவது சற்றுக் கடினமே என்று பெருமூச்செறிகின்றனர் கணினிக்காரர்கள்.

ஒரு இணைய இயந்திரத்தின் மூலம் நமது கணினி வைரஸால் பாதிக்கப்பட்டது போன்றும், இலவச வைரஸ் கண்டுபிடிப்பான் மூலம் கண்டறியலாம் என்றும் தரவிறக்க ஒரு தொடுப்பு வழங்கப்படும். அங்கே உண்மையிலேயே இலவசமாக வைரஸ் கண்டுபிடிப்பான் இருக்கும். அதைத் தரவிறக்கி நம் கணினியில் சோதித்தால், "ஆம்! வைரஸ் இருக்கின்றது. அதை நீக்க 49.95 டாலர் பணம் கட்டினால் வைரஸ் நீக்குவான் கிடைக்கும்" என்ற விளம்பரம் வரும். அது குறிப்பிடும் வைரஸ் பெயர் பற்றி நீங்கள் இணையத்தில் தேடினால் கிடைக்காது! ஏனெனில் ஒவ்வொரு முறையும் புதிய பெயர் வைத்துக் கொள்கின்றது அந்த வைரஸ்! ஆக, அந்த வைரஸை நீக்க நீங்கள் மென்பொருளை வாங்கும் நோக்கத்துடன் கடனட்டை எண்ணை வழங்கி விட்டால் போச்சு! இது எப்படி இருக்கு?!

RFID திகில்: நன்றி: http://www.rfidvirus.org/

ஆம். உண்மையிலேயே திகில் தான். Radio Frequency Identification என்ற பொருளில் வழங்கப்படும் RFID எனப்படுவது உண்மையில் ஒரு மைக்ரோ

சிப்பம் ஆகும். அதில் 1024 பிட் நினைவகமும் மிகச் சிறிய செயலியும் இருக்கின்றது. படத்தில் அதைக் காணலாம்.



இந்தச் சிப்பத்தின் அருமை என்னவென்றால், இதற்கென்று மின்கலம் தேவையில்லை. ஆனால், இதன் நினைவகத்தில் இருக்கும் தகவல்களை ஒரு வருடியின் மூலம் (Scanner) தொலைவிலிருந்தே வானொலி அலைகளின் மூலம் பெற இயலும். இவை தற்போது பல இடங்களில் உபயோகத்துக்கு வந்திருக்கின்றன.

இவற்றின் உபயோகங்கள் பலப்பல. பார் கோட் எனப்படும் பலவகைப்பட்ட தடிமனான கருப்புக் கோடுகளை உபயோகப்படுத்துவதைப் பார்த்திருப்போம். இப்போது அதற்குப் பதிலாகச் சாதாரண ஊறுகாய் பாட்டிலில் இருந்து அதிநவீன பொருட்கள் வரை இந்த அட்டைகளைப் பயன்படுத்த ஆரம்பித்து விட்டார்கள். இதன் உபயோகம், இதை நாம் எடுத்துக் கொண்டு பணம் தராமல் அதாவது பில் போடப்படாமல் கடையிலிருந்து வெளியேறினால் உடனே சத்தம் போட்டு ஊரைக் கூட்டிக் காட்டிக் கொடுத்து விடும்! அதுமட்டுமின்றி, ஒருவரின் வாங்கும் திறன், வழக்கங்கள் ஆகியவற்றையும் சேர்த்துத் தனது தரவுகளில் சேமித்துக் கொண்டு அதன் பிறகு அது சம்பந்தமாக அவர்களுக்கு மின்னஞ்சலில் விளம்பரம் தரும் அளவுக்கு இது போய்விட்டது!

இனி இதைக் கெட்ட காரியத்துக்கு எப்படிப் பயன்படுத்துகின்றார்கள் என்று காண்போம்.

அதே ஊறுகாய் பாட்டிலை எடுத்துக்காட்டாக எடுத்துக் கொள்வோம். வைரஸைப் பரப்பும் நோக்கத்தில் இருக்கும் நம்மவர், இந்த ஊறுகாய்ப் பாட்டிலைக் கடையில் ஒழுங்காகப் பணம் கொடுத்து வாங்குவார். வீட்டுக்கு வந்ததும் அந்த அடையாள அட்டையை நீக்கிவிட்டுப் புதியதாக அதே போன்ற அட்டையை உருவாக்குவார். அந்த அட்டையை மீண்டும் ஊறுகாய் பாட்டிலில் ஒட்டுவார். மீண்டும் கடைக்கு வந்து நல்ல பிள்ளை போல, அந்த ஊறுகாய்ப் பாட்டிலுக்கும் சேர்த்து மீண்டும் ஒரு முறை பணம் கட்டுவார். அப்போது கடைக்காரர் இந்த அடையாள அட்டையிலிருந்து வருடி மூலம் தகவல் பெறுவார் தானே? அப்போது ஆரம்பிக்கின்றது வினை! அந்தத்

தகவலுடன் சிறிய வைரஸும் சேர்ந்து கொள்ளும். மொத்தத் தரவையும் நம்மவர் கட்டுப்பாட்டுக்குக் கொண்டு வந்துவிடும். இனி இஷ்டம் போல அவர் பொருட்களின் விலையை மாற்றி அமைத்துக் கொள்ள முடியும்!

படத்தில் அவ்வாறு உருவாக்கப்பட்ட வைரஸ் பற்றி விளக்கிக் காட்டுகின்றார் ஒரு நிபுணர்.

இது சின்ன அளவிலான தாக்குதல்.

தீவிரவாதிகள் கையில் சிக்கினால் என்னாகும் என்று காண்போம்.

இன்றைய தினம், விமான நிலையங்களில் மூட்டை முடிச்சுகளுக்கு இந்த அடையாள அட்டையைப் பயன்படுத்துகின்றனர். இதன் மூலம் தூரத்திலிருந்தே அடையாள அட்டையின் மூலம் யாருடைய பெட்டி என்பதைக் கண்டறிய முடியும். ஆனால், ஒரு தீவிரவாதி தனது சாமர்த்தியமான அடையாள அட்டையின் மூலம் இன்னொருவருடைய அடையாள அட்டையின் தகவலைப் பிரதிபலிக்க முடியும். வைரஸைப் பரப்ப முடியும். இந்த வைரஸ் விமானநிலையங்களின் கணினிகளை முடக்கக் கூடும். வெடிகுண்டு இருக்கும் பெட்டியைப் பற்றி அறிந்து கொள்ள முடியாமலே போய்விடக் கூடும்.

ஆக, தொழில்நுட்பம் வளர வளர அதனால் ஏற்படும் அவதியும் பெருத்துக் கொண்டே வருகின்றது. நாம் தான் கவனமாக இருத்தல் வேண்டும்.

இன்னும் இன்னும் எந்த வழிகளிலெல்லாம் தகவல்கள் திருடப்படுகின்றன என்று சொல்லிக் கொண்டே போனால் அது உண்மையில் ஒரு பெரிய பட்டியலாகி விடும். முக்கியமான, குறிப்பிட்ட சில வழிமுறைகளை இங்கே கண்டோம்.

இவற்றைப் பற்றிய பட்டியல்கள், அகராதிகள் இணையத்திலேயே காணக் கிடைக்கின்றன.

எடுத்துக்காட்டாக இந்தத் தளத்தைச் சொல்லலாம். இதைக்

கையடக்கக் குட்டி அகராதி என்று சொன்னால் அது மிகையாகாது.

http://www.h-spot.net/threat_glossary.htm

எல்லாம் சரி, தகவலை அழிப்பதற்கு ஆயிரம் வழிகள் இருக்கின்றன. அதைக் காப்பதற்கு எத்தனை வழிகள் இருக்கின்றன என்ற கேள்வி எழுகின்றது தானே?

சில சமயங்களில் போராக இருக்கின்றது. சில சமயங்களில் விளையாட்டாக இருக்கின்றது. போரோ, விளையாட்டோ பாதிக்கப்படப் போவது நாம் மட்டுமே என்று சிந்தித்தால், நாம் எவ்வளவு கவனமாக இருத்தல் அவசியம் என்பது புரிபடும்.

ஆக, விழிப்புணர்ச்சி (vigilance) மற்றும் எச்சரிக்கை உணர்வு (Alert) ஆகியவை எப்போதும் உளப்பூர்வமாக இருத்தல் தான் முதல் படி என்று உணர்ந்து என்னென்ன வழிகளில் எல்லாம் தகவல்களைத் திருடுவதில் இருந்து பாதுகாக்கலாம் என்பதைச் சற்று விரிவாகக் காணலாம்.

தகவல் என்பது ஒரு சொத்து. அதைக் காப்பாற்ற வேண்டியது தகவல் பாதுகாப்பு மேலாண்மையின் கடமை என்பதை இது காறும் அறிந்தோம். அதை எவ்வாறு செய்வது?

தகவல் பாதுகாப்பு என்பது அறிவியல் (Science) என்றாலும் கூட பாதுகாப்பு மேலாண்மை என்பது ஒரு கலையே (Art) ஆகும். எந்த ஒரு கலையும் ஆர்வத்துடன் விடாது முயற்சித்தால் மட்டுமே கை கூடும். புத்தகத்தில் எந்த ஒரு கலையையும் கற்றுக் கொள்ள முடியாது. புத்தகத்தில் படித்து நீச்சலை எவ்வாறு கற்றுக் கொள்ள இயலாதோ அதே போன்று எந்த ஒரு முயற்சியும் பயிற்சியும் இன்றி தகவல் பாதுகாப்பு மேலாண்மையும் கற்றுக் கொள்ள இயலாது.

எந்த ஒரு பூட்டு பூட்டினாலும் அதைத் திறப்பதற்கான சாவியை உருவாக்க வழிகள் இருக்கின்றன.

இருப்பினும், தகவல் பாதுகாப்பு மேலாண்மையில் இருக்கும் நடைமுறைகள் பற்றியும் அதில் இயைந்திருக்கும் தொழில்நுட்பம் பற்றியும், பயன்படுத்தும் வெவ்வேறு கருவிகள் பற்றியும்

அறிந்திருத்தல் அடிப்படைத் தேவையாகும். அவைகளையே நாம் இங்கு காண இருக்கின்றோம்.

தகவல் (Information), தொழில்நுட்பம் (மென்பொருள்+வன்பொருள்) (Technology), தகவல் தேவைப்படுபவர், தகவல் உருவாக்குபவர், தகவலை நிர்வகிப்பவர் (Persons) இவைகள்/இவர்களே தகவல் பாதுகாப்பில் அங்கம் வகிக்கும் முக்கிய பொறுப்பாளிகள் ஆகின்றனர்.

தகவலைப் பாதுகாக்க இயலும். தொழில்நுட்பங்களும் அவ்வாறே! ஆனால், இந்த மனிதர்களைக் கண்காணிப்பது இருக்கின்றதே? அது தான் மிகக் கடினமான ஒன்றாகும். ஆக, தகவல் பாதுகாப்பில் முதல் படியாக வந்து நிற்பது, தகவல் தொழில்நுட்பப் பயனர்கள் தான்.

பயனர்கள் மூலம் தெரிந்தோ தெரியாமலோ தகவல் பாதுகாப்பு உடைக்கப்படாமல் எவ்வாறு பாதுகாப்பது என்று அறிந்து கொள்வோம்.

முதலில் தகவல் பாதுகாப்பு மேலாண்மை குறித்த அனைத்து விவரங்களும் அடங்கிய ஒரு கையேடு தயாரிக்கப்படவேண்டும். அதை நிறுவனத்தின் தொழிலாளர்களுக்கு அறிமுகப்படுத்தி, அவர்கள் அதில் பயிற்சி பெற நடவடிக்கை எடுக்கப்படவேண்டும். இப்பயிற்சிகள் அடிக்கடி தொடர்ந்து நடைமுறைப்படுத்தப் பட வேண்டும்.

எடுத்துக்காட்டாக, ஒரு நிறுவனத்தில் தொழிலாளர்களின் கடவுச்சொற்கள் பதினைந்து நாட்களுக்கொருமுறை மாற்ற வேண்டும் என்ற நடைமுறை இருப்பின், அதைத் தொடர்ந்து அனைத்துத் தொழிலாளர்களும் செயல்படுத்துகின்றனரா என்று கண்காணிப்பது முக்கியமாகும்.

தகவல் பயனர்கள் கடவுச்சொல்லைப் பத்திரமாகப் பாதுகாப்பது தான் மிக முக்கியமான விஷயம் ஆகும்.

நல்லதொரு கடவுச்சொல்லின் பண்புகள்:

1. கடவுச்சொல் எளிதில் யூகிக்க முடியாததாக இருக்க வேண்டும். (பயனரின் பிறந்த நாள், பெயர், நெருங்கிய உறவினர்களின் பெயர், திருமண நாள், ஊர்ப் பெயர், எளிதில் ஞாபகம் வைத்துக் கொள்ளக் கூடிய சொற்கள் (எ.கா. 12345, password) ஆகியவற்றைக் கடவுச்சொல்லாக வைத்திருத்தல் கூடாது)

2. கடவுச் சொல்லைத் தகுந்த கால இடைவெளியில் மாற்றிக் கொள்தல் வேண்டும். கடவுச்சொல் பாதுகாக்கும் தகவலின் முக்கியத்துவம் அதிகமாக இருந்தால் அதை மாற்றும் கால இடைவெளி குறைவாக இருத்தல் அவசியமாகும்.

3. கடவுச்சொற்கள் குறைந்த பட்சம் 8 எழுத்துக்களாவது கொண்டிருத்தல் அவசியமாகும். அதில் எண்ணும், எழுத்தும், பெரிய எழுத்தும், சிறிய எழுத்துகளும் கலந்து இருத்தல் அவசியம்.

4. கடவுச்சொல் குறித்துக் கொள்ளப்படக் கூடிய ஒரே இடம் பயனரின் மனம் மட்டுமே. வேறெங்கும் கடவுச்சொல் குறித்து வைக்கப்படலாகாது.

5. ஒரே கடவுச்சொல் நாம் செல்லும் அனைத்து இணையப்பக்கங்களுக்கும், கணினிக்கும், தகவல் சேமிப்புக்கும் வைத்திருத்தல் கூடாது. ஏனெனில், ஏதேனும் ஒரு இடத்தில் கடவுச்சொல் கண்டுபிடிக்கப்பட்டு விட்டால், அத்தனை தகவலும் அம்பேல் ஆகி விடும்.

இப்படி முன்னுக்குப் பின் முரணான நிபந்தனைகள் கொண்ட கடவுச்சொல்லைக் கவனத்துடன் கட்டிக் காப்பது என்பது தான் தகவல் பயனரின் முன் நிற்கும் மிகப் பெரிய தடைக்கல்லாகும். ஆயினும், நமக்கு நாமே ஏதேனும் ஒரு முறைமைப்பாட்டுடன் புதிய புதிய கடவுச்சொற்களை உருவாக்கிக் கொண்டால், எளிதில் ஞாபகம் வைத்துக் கொள்ள ஏதுவாக இருக்கும்.

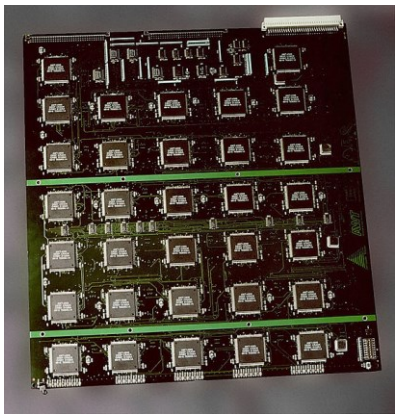
மேலும், நிறைய கடவுச்சொற்களை ஞாபகம் வைத்திருக்க முடியாததால், கடவுச்சொற்களைப் பாதுகாப்பதற்கென்றே மென்பொருட்கள் இருக்கின்றன (எடுத்துக்காட்டு: http://keepass.info/). இம்மென்பொருட்களில் கடவுச்சொற்கள் பலவற்றை இட்டு, அவையனைத்தையும் ஒரே ஒரு கடவுச்சொல் மூலம் பூட்டி வைத்து விட இயலும். அந்தக் கடவுச்சொல் மேலே குறிப்பிட்டவாறு கவனமாக இருத்தல் அவசியமாகும்.

இதே போல், புதிய புதிய கடவுச்சொற்களை உருவாக்கவும் சில மென்பொருட்கள் இருக்கின்றன. அவற்றையும் உபயோகப்படுத்திக் கொள்ளலாம். சில மென்பொருட்கள் அவற்றை நாம் நினைவில் வைத்துக் கொள்ள உதவியாக சொற்களையும் உருவாக்கித் தருகின்றன. (எ.கா. https://sourceforge.net/projects/pwdstr/)

தகவல் பாதுகாப்பில் முக்கியத்துவம் வகிப்பது கடவுச்சொல்லே என்றாலும் கூட, காலப்போக்கில் கடவுச்சொல் மட்டுமே நிறைவான பாதுகாப்பு தரும் என்று சொல்லிவிட முடியாது. இன்றைய அதிவேகச்

சிப்பங்களின் மூலம், எத்தனை பெரிய கடவுச்சொல் என்றாலும் கூட அதை ஒவ்வொரு எழுத்தாகவேனும் யூகித்தறிந்து (Brute Force Attack) பாதுகாப்பை உடைத்தெறிய சாத்தியக்கூறுகள் இருக்கின்றன.

எடுத்துக்காட்டாக 250000 டாலர்கள் மதிப்புள்ள, 1800 சிப்பங்களைக் கொண்ட இந்த கடவுச்சொல் உடைப்பான் சில நாட்களிலேயே மிகக் கடினமான DES கடவுச்சொல்லையே உடைத்தெறியும் பலம் கொண்டதாகும்!



எனவே கடவுச்சொல் பாதுகாப்பு மட்டுமே தகவல் பாதுகாப்பாகி விடாது. அப்படியானால் என்ன தான் செய்வது?

பாதுகாப்பினை இறுக்கவும், தகவலின் பயனர் மட்டுமே தகவலை அணுகவும் வழி வகை செய்ய மொத்தம் நான்கு விதங்களில் நடவடிக்கை மேற்கொள்ளப்படுகின்றன.

அவையாவன:

1. உங்களிடம் இருப்பதென்ன? (What do you have?)
   - சாவி, அடையாள அட்டை, நுழைவுச்சீட்டு, கடனட்டை, பற்று அட்டை
2. உங்களுக்கு என்ன தெரியும்? (What do you know?)
   - கடவுச்சொல், PIN எண்கள், இரண்டும் இணைந்தது.
3. நீங்கள் செய்வதென்ன? (What do you do?)
   - கையெழுத்துச் சோதனை
4. உங்களின் தனித்தன்மை என்ன? (What you are?)
   - பயோமெட்ரிக்ஸ் எனப்படும் உடலமைப்புச் சோதனை, கைரேகை சோதனை, குரல் சோதனை, முகவமைப்பு சோதனை, விழிச் சோதனை

இந்தக் கேள்விகளுக்கான விடைகளில் தான் இன்றைய தேதியில் தகவல் பாதுகாப்பு தொக்கி நிற்கின்றது! நமது தகவலின் முக்கியத்துவத்துக்கேற்ப, மேற்கண்ட சோதனைகள், கட்டுப்பாடுகளை விதித்து தகவல் பாதுகாப்பை மேம்படுத்தலாம்.

தீச்சுவர்:

இந்தப் பேருலகம் ஒரு கிராமமாய்ச் சுருங்கியதற்கு கணினியும் ஒரு முக்கியக் காரணம் ஆகும். எண்ணிக்கையில் கணினிகள் பெருகி வந்தாலும் அவற்றின் இடையே இருக்கும் இடைவெளியைக் குறைக்க உதவுவது **இணையம்** என்றொரு பெருங்கடல் என்றால் அது மிகையாகாது.

நல்லது எதிலெல்லாம் இருக்கின்றதோ அதிலெல்லாம் தீமையைக் கலப்பது மனிதனின் மூளையல்லவா?

இணையத்திலும் தீமைகள் விரவிக் கிடக்கின்றன. இணையம் என்பது மின்கடத்தி போல் தகவல் கடத்தி என்று வைத்துக் கொள்ளலாம். கடத்தியில் பிரச்னை இல்லை. ஆனால் அது எதைக் கடத்துகின்றது என்பதில் தான் பிரச்னையே.

திரு. பாலச்சந்தர் அவர்களின் ரயில் சிநேகம் என்றொரு தொலைக்காட்சித் தொடர் வெளிவந்தது அநேகம் பேருக்குத் தெரிந்திருக்க நியாயமில்லை! அந்தத் தொடரின் தலைப்புப் பாடலாக வைரமுத்துவின் வைர வரிகளில்,

"இந்த வீணைக்குத் தெரியாது அதைச் செய்தவன் யாரென்று,
இந்தப் பிள்ளையும் அறியாது இதைத் தந்தவன் யாரென்று,
வீணையில் படிக்கும் ராகங்கள் வீணை அறியாது..."

என்று செல்லும் வரிகளில் குறிப்பிடுவது போல், இணையம் அறியாது தான் எதைத் தருகின்றோம் என்று!

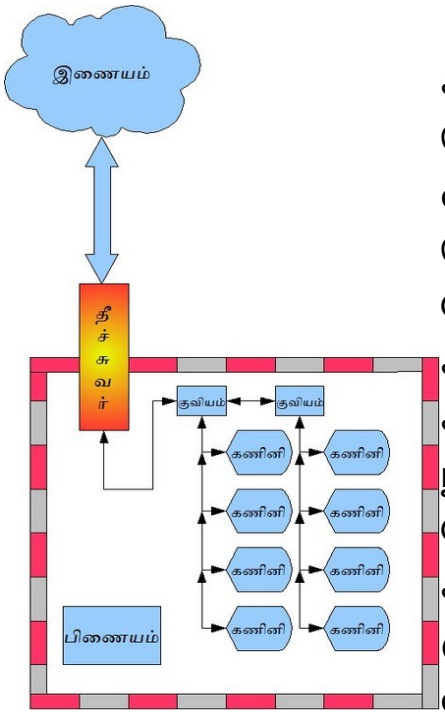
அதில் நமக்குத் தேவையான தகவல்களும் இருக்கலாம். அல்லது வைரசுகள், நச்சுப் புழுக்கள், ஒற்று மென்பொருட்கள், குப்பை கூளங்கள் வரும் மின்னஞ்சல்கள், தகாத விளம்பரங்கள், 108 பேருக்கு அனுப்பு என்ற கட்டளைகள், 10000 கோடி ரூபாய் கொஞ்ச நாள் வைத்திருக்கின்றீர்களா என்று கேள்விகள் என்று பல்வேறு பிரச்னைகள் இணையத்தில் தொடர்பு கொள்வதால் நமக்கு இலவசமாய் கிடைக்கின்றன. அதற்காக இணையமே நான் உபயோகிக்கப் போவதில்லை என்றால், மூட்டைப்பூச்சிக்காக வீட்டைக் கொளுத்திய கதை தான்.

எனவே பாதுகாப்பாய் இணையத்தை உபயோகித்து நமக்குத் தேவையான தகவல்களை மட்டும் பெறுவது என்பது ஒரு கலை. அந்தக் கலைக்கு உபயோகமாய் இருக்கும் ஆயுதமே **தீச்சுவர்** (Firewall) ஆகும்.

தீச்சுவர் என்பது இணையத்திலிருந்து (WWW) தனியாகச் செயல்படும் ஒரு பிணையத்தைப் (Private Network) பிரித்து உள்ளே வரும் தகவலையோ, வெளிச் செல்லும் தகவலையோ சரி பார்க்கும் ஒரு காவலாளி ஆகும். தீச்சுவர் ஒரு மென்பொருளாகவோ வன்பொருளாகவோ இருக்கலாம்.

நம் இல்லத்தில் நான்கு புறமும் சுவர் கட்டி வைத்திருப்பது எதற்காக? நாம் பாதுகாப்பாய் இருப்பதற்கும், அடுத்தவர் உள்ளே வந்து விடாதிருக்கவும் தானே? அதற்கு உதவுவது கதவு. இங்கே தீச்சுவரும் கதவின் பணியே செய்கின்றது. எனவே **தீச்சுவர் வைத்திருப்பதன் மூலம் நம் தகவல் பரப்பை ஓரிடத்தில் குவித்துச் சரி பார்த்துப் பின் வெளியே அனுப்புவது அல்லது உள்ளே விடுவது ஆகிய பணியைச் செய்கின்றோம்.**

இந்தப் படத்தைப் பாருங்கள். இணையத்திலிருந்து வரும் தகவலை தீச்சுவர் வழியே பிணையத்திற்கு அனுப்பி அங்கிருக்கும் கணினிகள் பகிர்ந்து கொள்கின்றன.



தீச்சுவர் வைத்திருந்தால் போதுமா? என் கணினியை இணையத்தில் எந்த ஒரு நச்சுப் பொருளும் பாதிக்காதா? என்று கேட்டீர்களானால் விடை இல்லை என்றே வரும்! ஏற்கனவே நான் சொன்னது போல தீச்சுவர் என்பது ஒரு கதவு போன்றது. எனவே திருடன் (நச்சுப் பொருள்) சரியான சாவி கொண்டு வந்தாலோ அல்லது கதவை உடைத்து உட்புகுந்தாலோ உள்ளே நுழைந்து விட வாய்ப்பிருக்கின்றது. நல்ல வேளையாக இங்கே கதவை உடைப்பது என்பது சாத்தியமில்லை. எனவே சாவி தான் மிக முக்கியமானது. எந்தச் சாவியைக் கொண்டு வந்தாலும் திறக்க முடியாத பூட்டு எப்படி தயாரிப்பது?

இணையம் வேலை செய்வது எப்படி?

இணையத்தில் நீங்கள் மின்னஞ்சல் அனுப்பினாலும் சரி, கோப்பு அனுப்பினாலும் சரி, அல்லது ஒரு வலைப்பக்கத்தில் உலவினாலும் சரி, இணையத்தைப் பொருத்த வரை அது ஒன்று தான். எதுவானாலும் இணையத்தைப் பொருத்தவரை இருமைத் (binary) தகவல்கள் ஒரு புறமிருந்து இன்னொரு புறம் செல்கின்றது அவ்வளவே!

இதில் எங்கிருந்து எங்கே செல்கின்றது என்று தபால் நிலையத்தில் போல் குறித்து வைத்து இணையம் அனுப்புகின்றது. அதைப் பொட்டலம் (Packets) என்பார்கள். ஆம், நம் தகவல்களும் சிறு சிறு பொட்டலங்களாகக் (65535 பைட்டுக்கள் அளவில் - IPV4) கட்டப்பட்டு இணையத்தில் அனுப்பப்படுகின்றன. ஒவ்வொரு பொட்டலத்திலும் அதை அனுப்பும் இணைய முகவரி (ஐபி), சேரும் இணைய முகவரி, நெறிமுறை என பல தலைப்புத் தகவல்களுடன் (Header information) நம் தகவல்களும் இருக்கும்.

முதல் தலைமுறை தீச்சுவர்கள் வெறுமனே இந்தப் பொட்டலத்தினைப் பிரித்துப் பார்த்து நமக்குத் தேவையானது தானா என்று வடிகட்டி (Packet Filters) சரி பார்ப்பதாகவே இருந்தன. பின்னால் பல வசதிகள் சேர்க்கப்பட்டு தற்போது கள்ளனைப் போல் காப்பானும் வளர்ந்து கொண்டே வருகின்றது!

இனி தீச்சுவரை எப்படி அமைப்பது? என்னென்ன செய்து கணினியைக் காக்கலாம் என்று கண்டறிவோம்.

சில கலைச்சொற்களை அறிந்து கொள்வோம்.

1. Port - துறைமுகம். நம் நாட்டிலுள்ள துறைமுகம் போல தான். நாட்டில் பல துறைமுகங்கள் இருப்பது போல ஒரு கணினியிலும் பல துறைமுகங்கள் இருக்கின்றன. நாட்டுத் துறைமுகத்துக்குப் பெயர் இருப்பது போல், இந்தத் துறைமுகத்துக்கும் எண்களால் பெயருண்டு. உதாரணமாக 80, 110, 25, 3306, 8080,21 போன்றவை நம் தூத்துக்குடி போல மிகப் புகழ் பெற்ற துறைமுகங்களாகும்!

2. Protocol - நெறி. ஒரு அரசியல் கூட்டம் நடக்கையில் இந்த வார்த்தையைக் கேட்டிருப்போம். அங்கே சரியான நெறிப் - protocol படி நடத்த வேண்டும். முதலில் தலைவர் தான் மேடையேற வேண்டும். அப்புறம் மற்றவர்கள். யார் முதலில் பேசுவது. அப்புறம் கடைசி முடிப்பது எப்படி என்று. அது போலவே இங்கும் பல நெறிகள் உண்டு. உதாரணமாக (http, pop3, smtp, ftp, udp போன்றவை)

3. Application Software - பயன்பாட்டு மென்பொருள். இவை பற்றி அதிகம் சொல்லவேண்டியதில்லை. உங்களுக்கே தெரிந்து இருக்கும். எடுத்துக்காட்டாக (வலை உலாவி, அலுவல் தொகுப்புக்கள், கணக்கீட்டு மென்பொருட்கள்)

4. IP Address - இணைய அடையாள முகவரி - சுருக்கமாக ஐபி முகவரி. இவற்றை எட்டெண்கள் (Octet) ஆகப் பிரித்திருக்கின்றார்கள். ஒரு எட்டெண் என்பது 2^8 ஆகும். அதாவது 0 முதல் 255. இது போல் 4 எட்டெண்கள் கொண்டது ஐபி முகவரி. உதாரணம்: 59.112.34.35 இதன் மூலம் 256 x 256 x 256 x 256 தனிப்பட்ட கணினிகளைச் சுட்ட முடியும்! இதில் நிலை முகவரி (Static IP Address) மாறும் முகவரி (Dynamic IP Address) என்று இரு வகை உண்டு. இது போக முகமூடி வழங்கிகளும் (Proxy Servers) உண்டு!

5. Deny - மறு/ தடை செய்தல்.

6. Allow - அனுமதி

இணையத்தில் ஒரு தகவல் பரிமாற்றம் நடக்கையில் இவை யனைத்தும் சம்பந்தப் படுகின்றன! எனவே தான் தீச்சுவரில் இத்தகவல்களனைத்தும் உபயோகிக்கப் படுகின்றன!

உதாரணமாக நீங்கள் வலையில் உலாவுகின்றீர்கள் என்று வைத்துக் கொள்வோம்: Internet Explorer என்ற பயன்பாட்டு மென்பொருளின் மூலம் http (hypertext transfer protocol) என்ற நெறிப்படி 80 என்ற துறைமுகம் வழியாக யுக்தி முறைமை முகவரியில் இருந்து (logical address எ.கா. http://www.yahoo.com) DNS என்னும் பெயர்க்கள வழங்கி மூலம் அடிப்படை ஐபி முகவரியாக மாற்றப்பட்டு தகவல் பரிமாற்றம் செய்யப்படும்.

எனவே ஒரு தகவல் பரிமாற்றத்தில் துறைமுகம், நெறி, பயன்பாட்டு மென்பொருள், இணைய முகவரிகள் (துவக்கமும் சேருமிடமும்)

ஆகியவையும் தகவலுடன் சேர்ந்து செல்கின்றன. இவற்றில் சில தொடர்புடையவையும் ஆகும்! உதாரணமாக http சாதாரணமாக 80 அல்லது 8080 என்ற துறைமுகம் மூலமாகவே அனுப்பப்படும். அதற்காக மற்ற துறைமுகங்களில் அனுப்பப்படக் கூடாது என்று அர்த்தம் இல்லை. மற்ற துறைமுகங்கள் மூலமும் அனுப்பலாம். அப்படி அனுப்பும் போது அவற்றை உலாவி எடுத்துக் கொள்ளாது. இதுவே நச்சுப் பொருட்கள் அனுப்புவோர் உபயோகித்துக் கொள்கின்றனர். மொத்தம் 65535 துறைமுகங்கள் இருக்கின்றன!

தீச்சுவரில் எவ்வாறு தடுப்பது?

இந்த நான்கின் மூலமாகவோ, இவற்றை இணைப்பதன் மூலமோ சில விதிகளைச் செய்வதன் மூலம் நச்சுப் பொருட்கள் வருவதைத் தவிர்க்க இயலும்.

1. **ஐபி முகவரி முறை:** இந்த முறையில் ஐபி முகவரியைக் கொண்டு தடை செய்யவோ, அனுமதிக்கவோ செய்யலாம். உதாரணமாக 59.* என்று வரும் ஐபி முகவரியைத் தடை செய்க எனலாம். அல்லது 59.* இது மட்டுமே அனுமதிக்கப்பட்ட ஐபி எனலாம்! அப்படிச் சொல்லி விட்டால் அந்த முகவரி தவிர வேறெங்கிருந்து வந்தாலும் தீச்சுவர் உள்ளே விடாது!

2. **பயன்பாட்டு மென்பொருள் முறை:** இந்த முறையில் ஒரு குறிப்பிட்ட மென்பொருள் இணையத்தைத் தொடர்பு கொள்வதைத் தவிர்க்கவோ அல்லது அனுமதிக்கவோ செய்யலாம். உதாரணமாக, உங்கள் பிணையத்திலிருந்து மின்னஞ்சலே அனுப்பக் கூடாது என்றால் மின்னஞ்சல் அனுப்பும் மென்பொருட்களைத் தடை செய்யலாம். அல்லது உலாவி மென்பொருட்களை மட்டுமே அனுமதிக்கலாம்!

3. **துறைமுக முறை:** இதன் மூலம் நீங்கள் குறிப்பிட்ட துறைமுகத்திலிருந்து வரும் தகவல்களை அனுமதிக்கவோ அல்லது மறுக்கவோ முடியும். உதாரணமாக 21 என்ற துறைமுகத்தை அடைத்து விட்டால் ftp மூலம் வரும் கோப்புக்களைப் பகிர்ந்து கொள்ள முடியாது.

4. **நெறி முறை:** இந்த முறை மூலம் குறிப்பிட்ட நெறி மூலம் வரும்

தகவலை அனுமதிக்கவோ மறுக்கவோ முடியும். உதாரணமாக http நெறியை அடைத்து விட்டால் யாருமே உலாவியில் உலாவ முடியாது. அது எந்த மென்பொருளாய் இருந்தாலும் சரி.

இவையனைத்தும் உட்புகும் தகவல்கள் அல்லது வெளிச்செல்லும் (Inward/outward) என்று இரண்டு வகையாய் விதிகளை அமைக்கலாம்.

அனுமதித்தல் மறுத்தல் இரண்டினையும் அறிந்து கொள்தல் அவசியமாகும். ஒன்றினை அனுமதி என்றால் மற்ற அனைத்தும் தடையா? என்பதையும், ஒன்றை மறுத்தால் மற்ற அனைத்துக்கும் அனுமதி உண்டா என்பதையும் ஞாபகம் வைத்துக் கொள்ள வேண்டும்.

கறுப்புப் பட்டியல், வெள்ளைப் பட்டியல் என்றும் இரண்டு வகை உண்டு. கறுப்புப் பட்டியல் என்பது மோசமான தளங்கள்/இணைப்புகளை மட்டும் பட்டியலிட்டு மற்றவர்களை உள்ளே அனுமதிப்பது. வெள்ளைப் பட்டியல் என்பது பாதுகாப்பான இணைப்புகள்/தள முகவரிகளுக்கு மட்டும் அனுமதி வழங்கி விட்டு மற்றபடி யாரையும் தொடர்பு கொள்ள முடியாமல் தடுப்பது. இதில் வெள்ளைப் பட்டியலே மிகவும் பாதுகாப்பானது.

நீங்கள் அடிக்கடி இணையத்தில் உலவுபவர் என்றால் 80 தவிர மற்ற துறைமுகங்களை அடைத்து விடலாம். இனி 80 வழியாக http நெறி மூலம் மட்டுமே தகவல் பரிமாறிக் கொள்ளலாம் என்று விதிக்கலாம். இதையும் தாண்டி வரும் நச்சுக்களை வேறெதுவும் மென்பொருளை உபயோகிக்க முடியாமல் செய்வதன் மூலமும், இணைய முகவரியைக் கண்டறிவதன் மூலமும் அறிந்து கொள்ளலாம்.

தீச்சுவர் சரியான பாதுகாவலனாகவும் இருக்காமல், பதிகை (log) மூலம் அனைத்து நிகழ்வுகளையும் பதிந்து வைத்திருப்பதால் எந்த நேரம் யார் யாரிடம் எந்த மென்பொருள் மூலம், எந்த துறைமுகத்தில் எந்த நெறியின் மூலம் தொடர்பு கொண்டார்கள், எத்தனை பொட்டலங்கள் பகிர்ந்து கொண்டனர் போன்ற தகவல்களைப் பெற முடியும்!

சரி. http மூலமாகவே, 80 என்ற துறைமுகம் மூலமாகவே, internet explorer ஐத் தாக்குவதாகவே, நம்பத்தகுந்த இணைய முகவரியில் இருந்து வந்தால்

என்ன செய்வது? சரியான அடையாள அட்டையைக் கொண்டு வரும் கொலைகாரனை உள்ளே காவலாளி விடும் கதை தான் இங்கேயும்.

அதற்கு விடை இந்த இடத்தில் தான் ஒற்றுக் காணும் மென்பொருட்கள், வைரசு கண்டு பிடிக்கும் ஆண்டி வைரசு மென்பொருட்கள் ஆகியன உபயோகிக்கப்பட வேண்டும். வெறுமனே தீச்சுவர் மட்டுமே போதாது. ஆனால் சரியான தீச்சுவர் விதிகள் செயல்படுத்தப்பட்டு இருந்தாலே மிகப் பெரும்பான்மையான பிரச்னைகள் முளையிலேயே கிள்ளி எறியப்படும்.

மேலும் நிறைய தீச்சுவர்கள் நிறுவுவதால் பயனேதும் இருக்கப் போவதில்லை. இரு தீச்சுவர்களும் சண்டை போட்டு கடைசியில் நச்சுப் பொருள் உள்ளே நுழைந்து விடும் வாய்ப்பு இருக்கின்றது!

எனவே மிகச் சரியான விதிமுறைகளைக் கடைப்பிடித்து தீச்சுவர்களைச் சரியாகப் பயன்படுத்தி பாதுகாப்பாக இணையத்தினை அணுக வேண்டும்.