CS5285
Information Security for eCommerce

Lecture 8

Dr. Gerhard Hancke
CS Department
City University of Hong Kong

1

Reminder of previous lecture

- Key Management
  - For all crypto we need keys (most important)
  - Symmetric key management
    - Looked at protocols for key establishment
    - Key control (agreement or transport?)
    - Explicit key authentication?
  - Asymmetric key management (Certificates)
    - We considered PKI architecture
    - CAs, and Certificates chains

Today's Lecture

- Aspects of Computer/Network Security
  - Authentication (passwords)
  - Access control
  - Firewall
  - Malware
- CILO1,CILO2 and CILO4

  (Organisational requirements, impact on security and regulations)

Credit to Keith Martin RHUL (borrowing few slides from his lecture notes)

Computer Security

Access Control

- Two parts to access control
- **Authentication:** Who goes there?
  - Determine who can access a system
  - Authenticate human to machine
  - Authenticate machine to machine
- **Authorization:** Are you allowed to do that?
  - Once you have access, determine how much you can access
  - Enforces limits on actions

5

You should know the difference and relationship between authentication (who are you) and authorisation (what are you allowed to do).

Authentication+authorisation = Access Control

Who Goes There?

- How to authenticate a human to a machine?
- Can be based on…
  - Something you **know**
    - For example, a password
  - Something you **have**
    - For example, a smartcard
  - Something you **are**
    - For example, your fingerprint

6

You should know the three factors of human authentication and be able to give an example.

Remember that we cannot authenticate a person the same way we authenticate a machine (using protocols/shared keys – where the person is expected to compute a response based on a key. The person can get help to calculate a response if he has a PC, but first you need to make sure the person is who you think via one of these methods).

Keys vs Passwords

- **Crypto keys**
- Suppose keys are 64 bits long
- Then 2^{64} keys
- Choose key at random
- Then attacker must try about 2^{63} keys

- **Passwords**
- Suppose passwords are 8 characters, and 256 different characters
- Then $256^8 = 2^{64}$ pwds
- Users do **not** select passwords at random
- Attacker has far less than 2^{63} pwds to try (**dictionary attack**)

7

Only important aspects from slide 7-10 is that people choose passwords – so not truly random! This make them less secure than keys.

The problem with passwords is that we choose them…

Personal details used to be ok for passwords…dog, anniversary, child birthday…

What changed? Social network data.

For interest

How good are users at pwds?

- RockYou – classic social media games
- Hacked in 2010 and all user password compromised.
- 32 million user passwords made public
- Top 10 are ?
  1. 123456
  2. 12345
  3. 123456789
  4. Password
  5. iloveyou
  6. princess
  7. rockyou
  8. 1234567
  9. 12345678
  10. Abc123
- Users are not good at choosing strong passwords!

Hey look at the last one – that follows all the good rules lower case, upper case, letters and numbers….

Historically bad…

	2011	2012	2013	2014	2015	2016	2017
1	password	password	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password
3	12345678	12345678	12345678	12345	12345678	12345	12345678
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty
5	abc123	qwerty	abc123	qwerty	12345	football	12345
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789
7	1234567	letmein	111111	1234	football	1234567890	letmein
8	letmein	dragon	1234567	baseball	1234	1234567	1234567
9	trustnot	111111	lloveyou	dragon	1234567	princess	football
10	dragon	baseball	adobe123	football	baseball	1234	iloveyou

SplashID/SplashData

Password Experiment

- Three groups of users — each group advised to select passwords as follows
  - **Group A:** At least 6 chars, 1 non-letter
  - **Group B:** Password based on passphrase
  - **Group C:** 8 random characters
- Results
  - **Group A:** About 30% of pwds easy to crack
  - **Group B:** About 10% cracked
    - Passwords easy to remember
  - **Group C:** About 10% cracked
    - Passwords hard to remember

winner →

11

Design an awareness…

Which one you think is best?

Its not only about the pwd

- Remember system view of security
- Even if password is strong think about entry and storage….
- Software vulnerable to timing attack?
  - Software exhibits input-dependent timings
  - We tend to forget the attacker can interact with our system
  - We tend to think only about the part we are developing and how well it works rather than the system as a whole

12

We tend to only think about the user? Are there other weak points?

Attacker Strategy

PwdCheck(RealPwd, CandidatePwd) should:
- Return TRUE if RealPwd matches CandidatePwd
- Return FALSE otherwise

```
PwdCheck(RealPwd, CandidatePwd) // both 8 chars
for i = 1 to 8 do
  if (RealPwd[i] != CandidatePwd[i]) then Return FALSE
  else Return TRUE
```

- Attacker can guess CandidatePwds through some standard interface
- Naive: Try all 256^8 = 18,446,744,073,709,551,616 possibilities
- Better: Time how long it takes to reject a CandidatePasswd.
- Then try all possibilities for first character, then second, then third,....total tries: 256*8 = 2048

13

Interest

Comment: Passwords

- We discussed password entry issues
  - Anyone have a Mac?
- macOS High Sierra 'hack'
  - At login - type 'root' as username
  - Leave password empty
  - Click 'unlock' twice…(or a few more times)
  - Now you have root access

  https://www.wired.com/story/macos-high-sierra-hack-root/

14

In 2017, root as username, unlock twice.

Password File

- Bad idea to store passwords in a file
- But need a way to verify passwords
- Cryptographic solution: **hash** the passwords
  - Store y = h(password)
  - Can verify entered password by hashing
  - If attacker obtains password file, he does not obtain passwords
  - But attacker with password file can guess x and check whether y = h(x)
  - If so, attacker has found password!

15

Slides 15-17 are important.

Why do we need to store passwords? Otherwise we cannot authenticate users….

Why do we not store plaintext passwords? What if it is stolen? What if someone within organisation looks at it?

This means we store the hash of the password.

Why a hash? It is one way, once we store the hash we cannot work back and get the input.

Why not encryption? Who has the key?

If the password is hashed client side, you still need to compare the hashes in "length-constant" time. If you compare the first 8 bits, next 8 bits, etc. and fail as soon as wrong then you basically have the same problem as slide 13. Ensure all checks take same amount of time whether correct or incorrect.

Dictionary Attack

- Attacker pre-computes h(x) for all x in a **dictionary** of common passwords
- Suppose attacker gets access to password file containing hashed passwords
  - Attacker only needs to compare hashes to his pre-computed dictionary
  - Same attack will work each time
- Can we prevent this attack? Or at least make attacker's job more difficult?
- Off the shelf tools
  - Hashcat 86,000,000 hash c/s

16

The easiest way for an attacker to try and find a password is to choose a number of passwords and then calculate the hash of these passwords.

This selections of passwords is his 'dictionary' – a password along with the hash is stored. If he then gets a password file the can see if any of his hash results matches the content of password file. If so he knows the password.

Password File

- Store hashed passwords
- Better to hash with **salt**
- Given password, choose random s, compute

  y = h(password, s)

  and store the pair (s,y) in the password file
- Note: The salt s is **not secret**
- Easy to verify password
- Attacker must recompute dictionary hashes for each user — lots more work!

17

We can prevent his by storing a salt (random number) with each password hash (we stored username, salt and h(password, salt)).

Example: If the total number of possible passwords is 1000, then the dictionary size for attack on slide 14 is 1000. If we now add a salt to each value it is still easy for legitimate system to verify but it means that a standard dictionary no longer works – the attackers needs one for each possible salt value.

So for any given password he needs the hash of the combination of every password and every single salt value. So if our salt has 100 possible value he now need 100*1000 dictionary entries.

What goes wrong with passwords? Example: Email phishing

- Attacker masquerades as a trustworthy entity
  - Attempts to fraudulently acquire sensitive information (usernames, passwords and credit card details)
  - Convince user to perform some other actions
- Social engineering attack
  - Phishing email makes an effort to look legitimate
  - Possibly redirects to web site that looks legitimate
- Phisher uses information in further attacks
- Difficult to prevent – most effective countermeasure is user education!

18

For Phishing (18-24) you do not need to know all the details and stats but you must be able to explain what a phishing attack is and what the important aspects of successfully executing this attack is.

Failure of authentication in itself…

Spam is also an ideal vehicle for phishing attacks, but only a very very small percentage of spam is actually phishing attempts - about 0.05%

Phishing is a combination of fishing and phreaking (old school telephone network experimentation) – play on the fact that you lure or bait the victim.

Earliest occurrences were attackers trying to get AOL login credentials in the 90s.

Asks to send details by email, more commonly directs to a website.

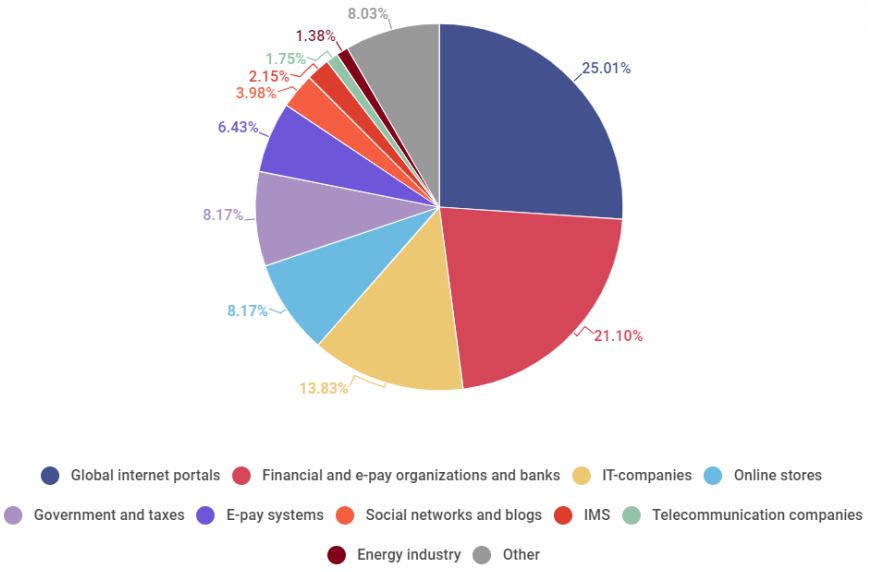
Phishing can also convince the user to install a program or open attachment.

Social engineering

Phishing emails might even come form a legitimate source whose email account has been compromised.

Phisher used this information for committing further crimes

Phishing targets



Source: Kasperksy Labs

19

Targets of phishing – according to Kaspersky labs the top phishing targets fall under several categories. Some recent stats released by them shown on the right – there are some clear winners.

Global internet portals = gmail/qq/yahoo. Large internet companies/providers - this category included search engines where services were affected by registered phishing attacks. This is any service offered by search engines, including email.

Financial and e-pay organizations, banks. As the name suggests, this category includes banks whose clients have become victims of phishing attacks. It also includes e-pay systems such as Visa, MasterCard, PayPal.

E-pay systems. Independent of banks – e.g. cryptocurrency…Ethereum most popular

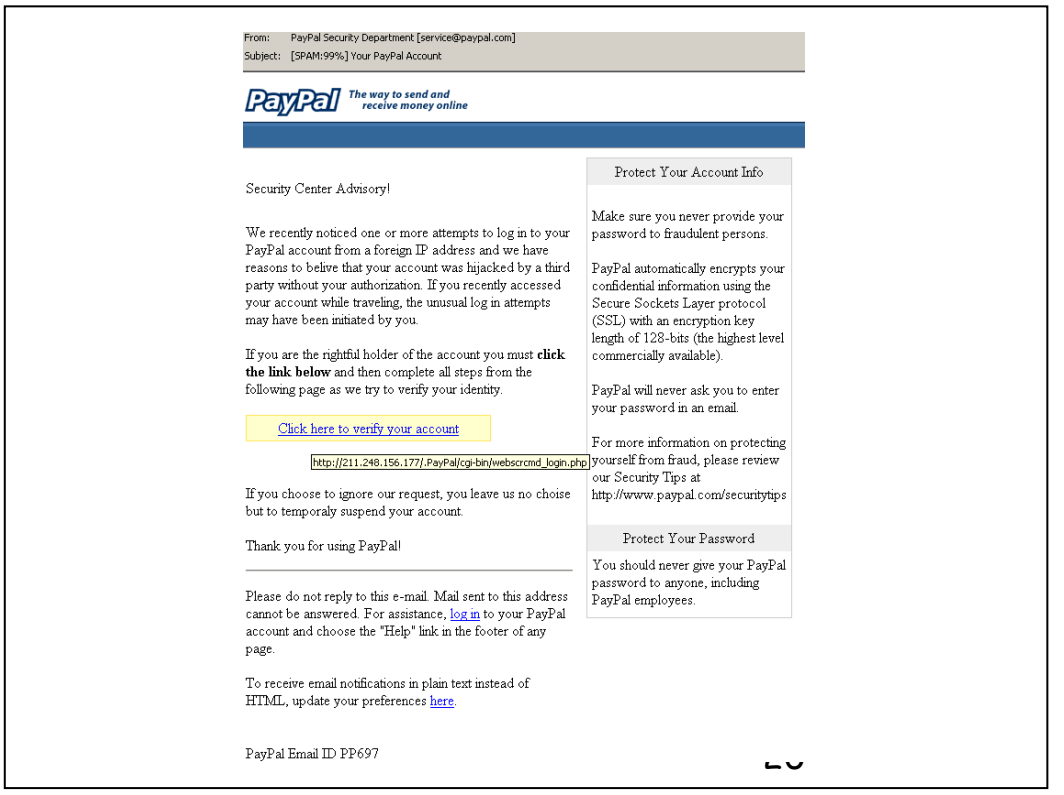
Online stores and e-auctions. User accounts in many online stores are aligned with their credit cards and contain personal information.

Social networking sites. User accounts on social networks remain a nice target for fraudsters because they are in great demand on the black market.

IT companies. Many software and hardware vendors have web services which can be accessed (to pay for the services or grocery orders or to download updates) only after registration. In order to make the purchasing process easier for the user, financial information such as bank card details are often stored on the service account. For example, Office 365.

IMS. IMS accounts are also among phishers' targets due to their popularity on the black market.

Government organizations. Accounts of users registered on the sites of government organizations. These attacks have a seasonal character. For example, most of them are launched when tax returns are due to be filed



From: PayPal Security Department [service@paypal.com]
Subject: [SPAM:99%] Your PayPal Account

PayPal The way to send and receive money online

Security Center Advisory!

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to belive that your account was hijacked by a third party without your authorization. If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you.

If you are the rightful holder of the account you must **click the link below** and then complete all steps from the following page as we try to verify your identity.

Click here to verify your account

http://211.248.156.177/.PayPal/cgi-bin/webscrcmd_login.php

If you choose to ignore our request, you leave us no choise but to temporaly suspend your account.

Thank you for using PayPal!

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

PayPal Email ID PP697

Protect Your Account Info

Make sure you never provide your password to fraudulent persons.

PayPal automatically encrypts your confidential information using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available).

PayPal will never ask you to enter your password in an email.

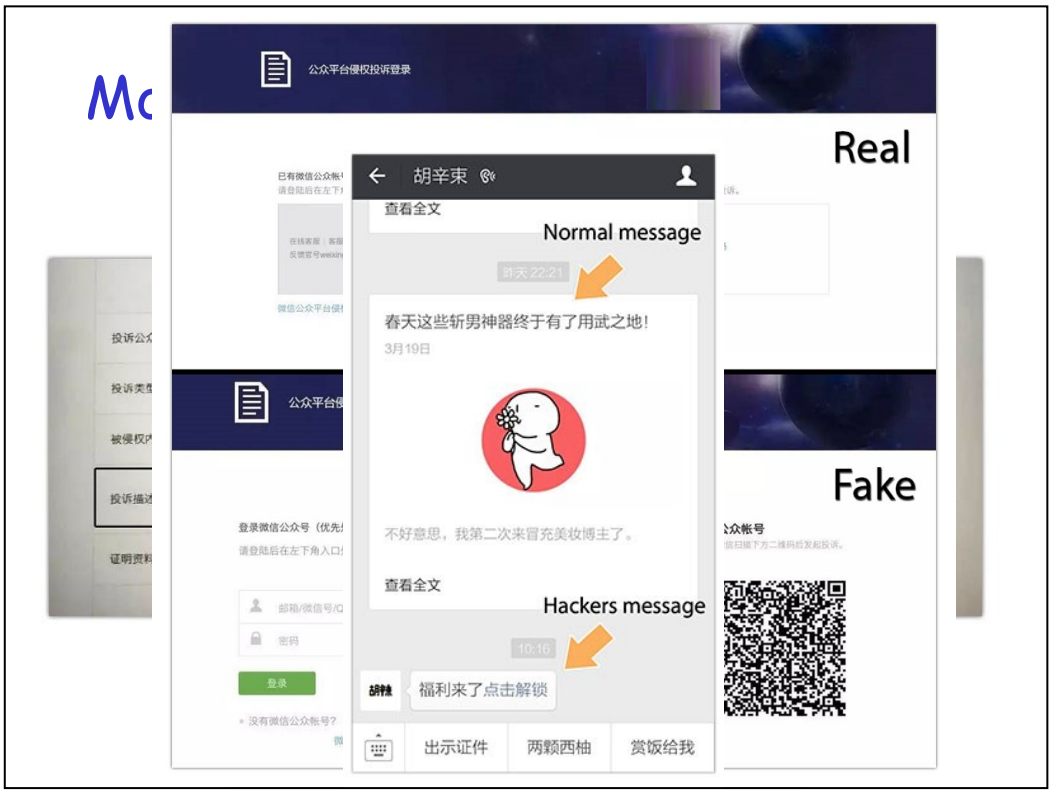
For more information on protecting yourself from fraud, please review our Security Tips at http://www.paypal.com/securitytips

Protect Your Password

You should never give your PayPal password to anyone, including PayPal employees.

Example of a phishing email. Obviously more thought goes into this – logo, styling and cover story (warns you to be secure, wary of schemes – evil phishers will of course not do that). Put some pressure on the victim (closing your account), usually important part of social engineering.

Really the email is key – recent study with online banking has shown that very few people follow the email link (about 1%), but then half of those that do click end up entering their details.



Use social media, IM. Use the system options.

Make fake complaint again popular user (many friends/followers)

Gave option to type complaint (text entered by attacker) (notice comes from valid source!)

Hijack account – phish

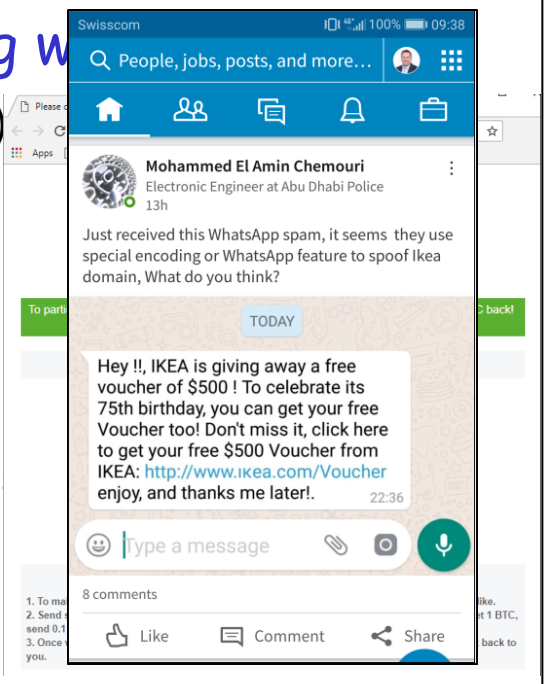
Hacker's message: A reward is here, click her to unlock

Phishing w

- The payoff (e.g. get paid)
- Needs to look like a legitimate site
  - Spoof the brand "hsbcbankupdate.co.hk"
  - Visual spoofing/URL obfuscation
  - For example, previous Punycode (allows Unicode characters in domain) bugs

"xn–pple-43d.com" displays a "apple.com"

uses Cyrillic "a"not ASCII "a"



Source: X.Zheng (Phisphing with Unicode Domains),I. Butler Visual Phsihng with Whatsapp;Kasperky Labs

22

The purpose of the email is to get the user to click through to a phishing website….this gathers the data. It should also look like a legitimate site.

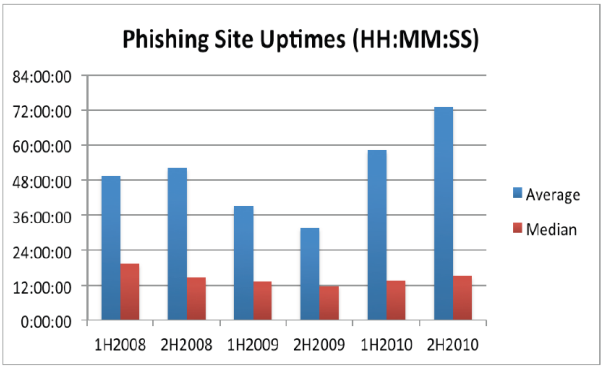
Once again made up to look like a real site. Once again there are tools available that help you set up sites.

Strong brand- register copycat brand name at domain provider, for example "hsbcbankupdate.co.hk"

Visual spoofing – replace certain components of a user's browser with fake copies in the form of images, for example, the address and status bars

URL obfuscation – disguise true URL bar content

Phishing websites (2)



APWG

- Phishing sites are difficult to find and take down
  - Redirected through a collection of proxies
  - Scam sites are often hosted on compromised servers
  - Usually in poorly regulated countries
  - There is no direct connection between the phisher and the server
  - Sites are only live for a very short time

Kasperksy Labs

23

Despite industry efforts phishing sites are difficult to find and take down.

The link goes through many proxies, once you get through that the site in then most likely not an a machine belonging to the phisher, but a compromised server.

Usually located in poorly regulated countries, difficult to get authorities involved.

You have the server – no strong link to the phisher.

Phisher can turn up once, collect data and disappear.

Once you have done all this the site is possibly gone anyway already.

Look at the picture, essentially half the sites are live for less than 12 hours. This is a combination of phishers moving sites (really it has maximum impact soon after email sent), and take down

measures becoming more effective.

Phishing techniques

- Conventional Phishing
  - Discussed up to now….
- Spear Phishing
  - Targeted phishing
  - Email tailored to specific person
  - Whaling
- Clone Phishing
  - Constructs phishing messages from previous email
  - Pretends to be from same sender, similar topic

24

There are some variations on this attack –

Phishing – generic email sent out, hope recipient is a customer of the site you are targeting.

Spear phishing – targeted email at single person (or small group of people). Personal references, believable story. Take time to get to know the victim, possible background information from previous phishing attempts (i.e. social networking – facebook, linked in).

Example,

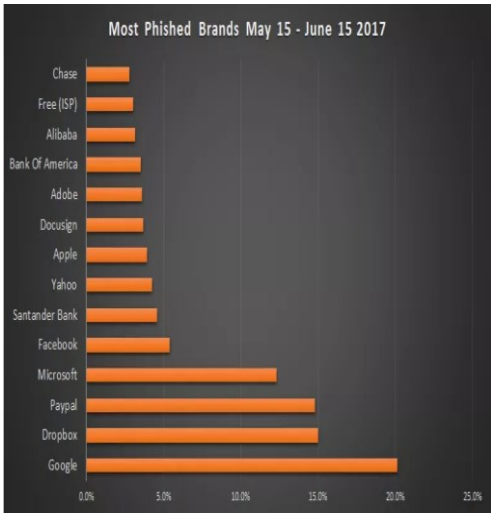
Someone might send an email around after class saying – this is an assignment based on the cybercrime class this morning please open attachment and then click here to log into moodle to submit answer.

Whaling – subset of this where phishing targets senior executives, high profile, VIP people.

Clone phishing works on observing email, possibly a compromised

mail server. If Alice sends Bob an email with an attachment, an attacker might then immediately send another email from Alice with a malicious attachment saying ' oops, attached the wrong file please open this one). 'Bob' might respond – Hi, Alice here is an attachment for you.

Targets change



Brand Name	Campaign Count	Sector	% of Brand Impersonations
Microsoft	28,536	Technology	69.77%
Zoom	3,803	Telecommunications	9.30%
Amazon	2,747	Retail	6.72%
Chase Bank	960	Finance	2.35%
RingCentral	807	Telecommunications	1.97%
eFax	542	Telecommunications	1.33%
Intuit	541	Finance	1.32%
CVS	541	Retail	1.32%
American Express	501	Finance	1.22%
Netflix	359	Technology	0.88%
PayPal	306	Finance	0.75%
Xerox	284	Telecommunications	0.69%
DocuSign	226	Technology	0.55%
AT&T	190	Telecommunications	0.46%
Sam's Club	115	Retail	0.28%
LinkedIn	109	Technology	0.27%
Walmart	86	Retail	0.21%
Apple	57	Technology	0.14%
Total	**40,903**		

- Phishing brands/topics change with time
- Attackers keep things up to date and relevant.

Redmarlin Labs/INKY

25

2020 right.

Difficult to judge (depends on where data is collected.

Use hot topics like FIFA 2018 World Cup, bitcoin

What is currently the most phished brand? Difficult to say – gather data more in certain countries

2019 *North America*

Microsoft (365,Outlook,Skype, Xbox Live)

Netflix

PayPal

In some places, better ways than phishing…

Lottery scams…

Final example

> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* [redacted]ta@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [redacted]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.
`

Example of phishing email.

Its from weird accounts.googlemail.com account….

2-factor Authentication

- Requires 2 out of 3 of
  1. Something you know
  2. Something you have
  3. Something you are
- Examples
  - Password + Security Token
  - ATM: Card and PIN
  - Password + Cellphone (e.g. SMS)

27

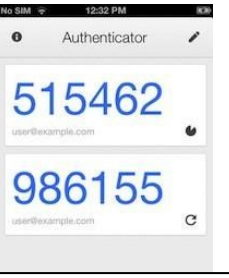
Why is two-factor better than single factor? If one fails then there is another measure in place.

Can you think if a real example?

For example, if I lose my payment card it cannot be used to withdraw money without the PIN. If someone sees my PIN they still need my card.

Something You Have and Know

- Most common 2FA
  - Password + something in your possession
- Online and remote connection
  - Increasingly for corporate login/remote work
  - Password and one-time password/mobile app
  - Google/Microsoft Authenticator
  - Company-specific apps



28

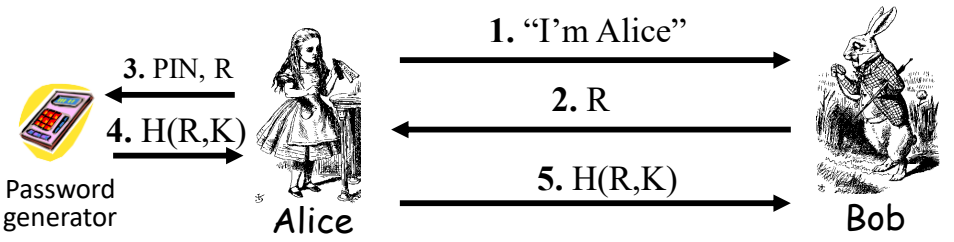
What can we do more than passwords?

Study

You must be able to explain both challenge-response and time based OTP generation.

You must also be able to explain why OTP are a good security measure if compared to standard password…(used only once, even if compromised a new password is used next time so does not matter).

Password Generator



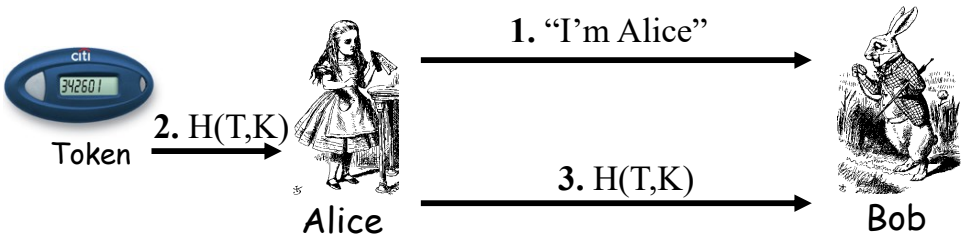
- Alice gets "challenge" R from Bob
- Alice enters R into password generator
- Alice sends "response" back to Bob
- Alice **has** pwd generator and **knows** the PIN
- K is only known to Bob and Password Generator, but not to Alice!

29

Does this protocol authenticate Alice? Yes, with the PIN.

Dynamic Password Token

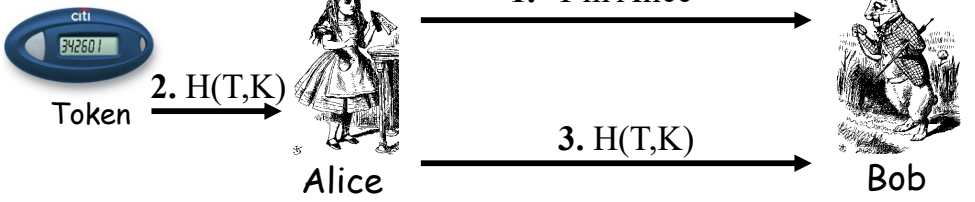
(a.k.a. Time-Based One-Time Password or **T-OTP**)



- Timestamp T is the "challenge" (*yes, the Token has an internal clock*)
- K is only known to Bob and the Token, but not to Alice, or we say "*not necessary for Alice to know*"
- Alice sends "response" H(T,K) back to Bob
- Alice **has** the Token
- Time synchronization between the token and Bob is required.

30

Does this protocol authenticate Alice? No, only that 'Alice' has control of the token.



In practice, how a Dynamic Password Token is implemented?

RFC 6238: TOTP: Time-Based One-Time Password Algorithm

https://tools.ietf.org/html/rfc6238

•contains reference code in Java

further reference

Google Authenticator

https://code.google.com/p/google-authenticator/

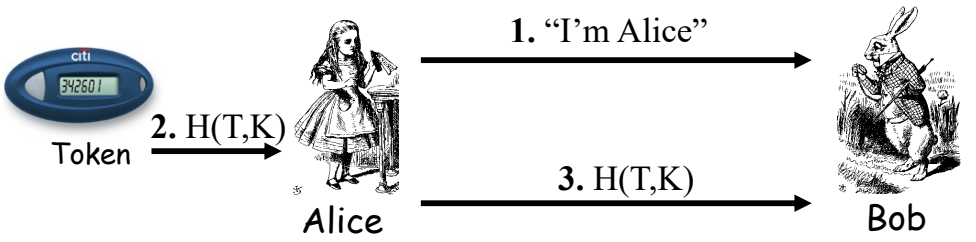
•based on RFC 6238 and more

•contains implementations, e.g. Android, iOS

More details about RFC 6238: *P.T.O.*

31

For interest only, enough detail for you on previous two slides.



Timestamp T:

•T is an integer and represents the number of **time steps** from a **time reference**.

•**time step** X = 30 seconds (by default)

•**time reference** R is the midnight UTC of January 1, 1970

•T = (Current Unix Time – R) / X where the default floor function is used in the computation.

•**Current Unix Time** is the number of seconds elapsed since R.

•For example, if (Current Unix Time -R)= 59 seconds, then T = 1; and if Current Unix Time = 60 seconds, then T = 2.

32

For interest.

Potential generation of timestamp. the

Authorization
(brief note on Access Control)

33

No need to study Authorisation – for interest only.

Authentication vs Authorization

- Authentication — Who goes there?
  - Restrictions on who (or what) can access system
- **Authorization** — Are you allowed to do that?
  - Restrictions on actions of authenticated users
- Authorization is a form of **access control**
- Authorization enforced by
  - Access Control Lists
  - Capabilities Lists
- Mandatory vs Discretionary Access Control

34

Mandatory is set by central authority, users do not control their own data.

Discretionary means users can set/control access to their data.

Lampson's Access Control Matrix

- **Subjects** (users) index the rows
- **Objects** (resources) index the columns

	OS	Accounting program	Accounting data	Insurance data	Payroll data
Bob	rx	rx	r	---	---
Alice	rx	rx	r	rw	rw
Sam	rwx	rwx	r	rw	rw
Accounting program	rx	rx	rw	rw	rw

35

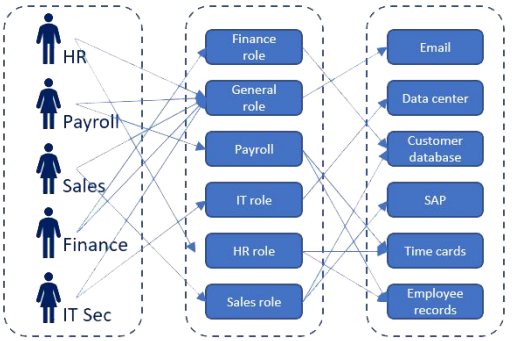
You can have an Access Control List or a Capability List

-One is stored with the resource and specifies rights of users. Each time a user wants access to the resource we see if the user is on the resource's list.

-Second is attached to the user – specified his rights to resources. So each time a user want a resource we see if the resource is on his list.

Role-Based Access Control

- No longer just linking subjects and objects
- Roles assigned access rights to objects
- Subjects are assigned roles



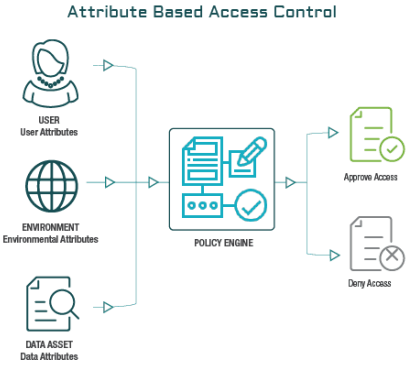
Credit:https://thorteaches.com/cissp-certification-rbac/

36

In practice we do not define access control like this anymore. We use other models that makes it easier such as role-based access control. Instead of Bob, Alice and Sam we have engineering, administration, finance we then assign these roles to Alice and Bob as needed (For example if bob is an engineering responsible for department admin he gets two role's rights.

Attribute-Based Access Control

- User: ID, clearance, group
- Environment: Location, device, network
- Data: Type, security classification



Credit:https://www.archtis.com/attribute-based-access-control-security-model/

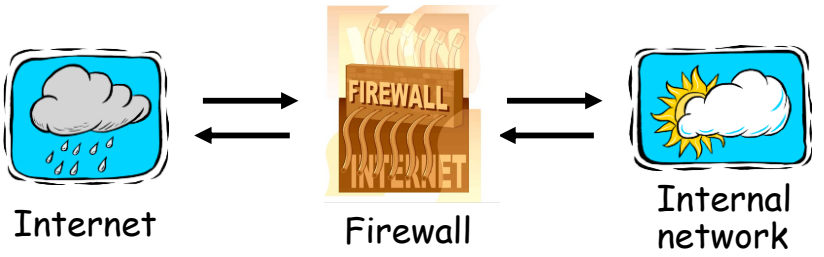
37

Where RBAC divided people based on role, ABAC allows for finer grained control. Taking into account the user, the environment and the resource.

This allows right people to access right data at say the right time.

Firewalls

Firewalls



- Firewall must determine what to let in to internal network and/or what to let out
- **Access control** for the network

39

Recognise where a Firewall is usefull

Firewall as Secretary

- A firewall is like a **secretary**
- To meet with an executive
  - First contact the secretary
  - Secretary decides if meeting is reasonable
  - Secretary filters out many requests
- You want to meet chair of CS department?
  - Secretary does some filtering
- You want to meet President of *country*?
  - Secretary does lots of filtering!

40

Interest only

Firewall Terminology

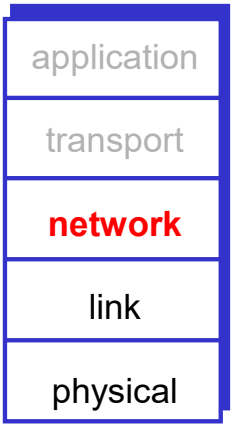
- No standard terminology
- Types of firewalls
  - **Packet filter** — works at network layer
  - **Stateful packet filter** — transport layer
  - **Application proxy** — application layer
  - Personal firewall — for single user, home network, etc.

41

You must know each of the firewall types – be able to give basic description, know what they can and cannot do and be able to give an advantage and disadvantage of each approach.

Packet Filter

- Operates at network layer
- Can filters based on
  - Source IP address
  - Destination IP address
  - Source Port
  - Destination Port
  - Flag bits (SYN, ACK, etc.)

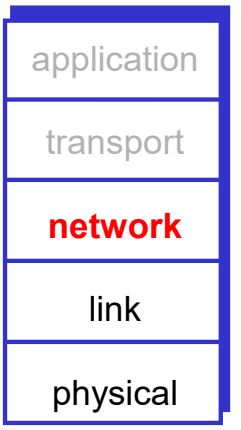


42

Remember that although there is Transport Layer info here SYN,ACK etc. the decision making is still at network layer – the firewall can look at these flags but it does not understand what they mean.

Packet Filter

- Advantage
  - Speed
- Disadvantages
  - No state
  - Cannot see TCP connections
  - Blind to application data



Packet Filter

- Configured via Access Control Lists (ACLs)
  - Different meaning of ACL than previously

Action	Source IP	Dest IP	Source Port	Dest Port	Protocol	Flag Bits
Allow	Inside	Outside	Any	80	HTTP	Any
Allow	Outside	Inside	80	> 1023	HTTP	ACK
Deny	All	All	All	All	All	All

- Intention is to restrict incoming packets to Web responses

44

What does this allow? What is the importance of the 'ACK' bit in the flag field?

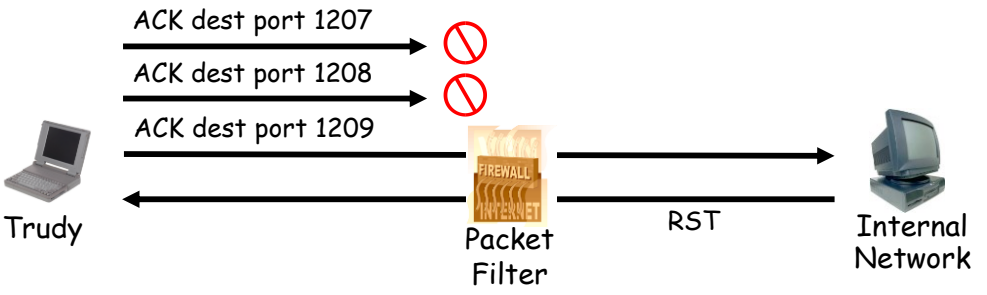
TCP ACK Scan

- Attacker sends packet with ACK bit set, **without** prior 3-way handshake
- Violates TCP/IP protocol
- ACK packet pass thru packet filter firewall
  - Appears to be part of an ongoing connection
- RST sent by recipient of such packet
- Attacker scans for open ports thru firewall

45

44 and 45 interest only.

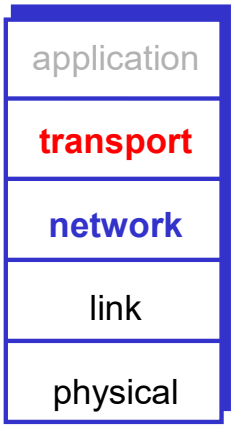
TCP ACK Scan



- Attacker knows port 1209 open thru firewall
- A **stateful packet filter** can prevent this (next)
  - Since ACK scans not part of established connections

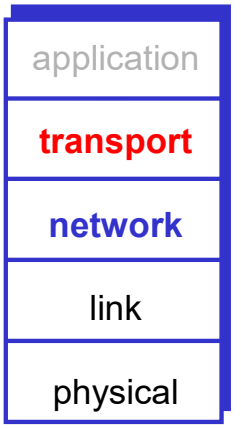
Stateful Packet Filter

- Adds **state** to packet filter
- Operates at transport layer
- Remembers TCP connections and flag bits
- Can even remember UDP packets (e.g., DNS requests)



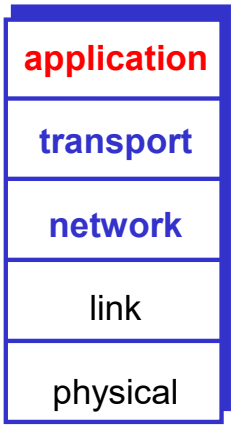
Stateful Packet Filter

- Advantages
  - Can do everything a packet filter can do plus...
  - Keep track of ongoing connections
- Disadvantages
  - Cannot see application data
  - Slower than packet filtering



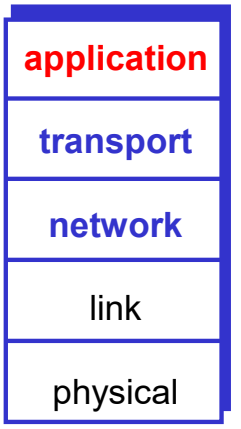
Application Proxy

- A **proxy** is something that acts on your behalf
- Application proxy looks at incoming application data
- Verifies that data is safe before letting it in



Application Proxy

- Advantages
  - Complete view of connections and applications data
  - Filter bad data at application layer (viruses, Word macros)
- Disadvantage
  - Speed



Application Proxy

- Creates a new packet before sending it thru to internal network
- Attacker must talk to **proxy** and convince it to forward message
- Proxy has complete view of connection
- Prevents some attacks stateful packet filter cannot

Firewalk

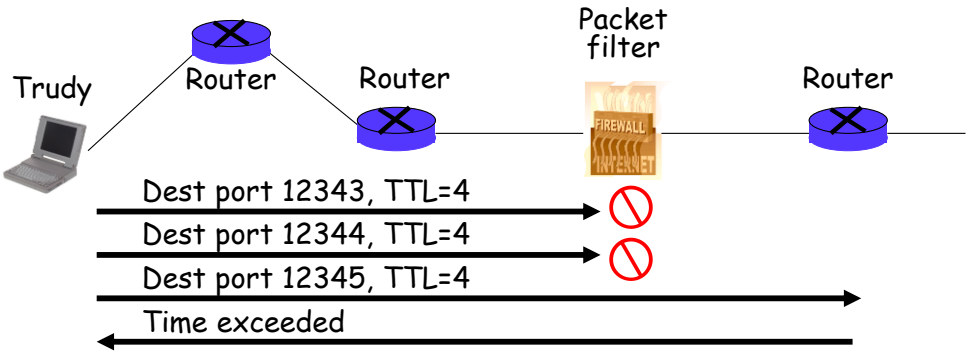
- Tool to scan for open ports thru firewall
- Known: IP address of firewall and IP address of one system inside firewall
  - TTL set to 1 more than number of hops to firewall and set destination port to N
  - If firewall does not let thru data on port N, no response
  - If firewall allows data on port N thru firewall, get time exceeded error message

52

50 and 51 for interest only

It's a node that does not use TCP (like a router).

Firewalk and Proxy Firewall



- This will **not** work thru an application proxy
- The proxy creates a new packet, destroys old TTL

53

We might not know a specific address, so we guess an address in the right range.

Personal Firewall

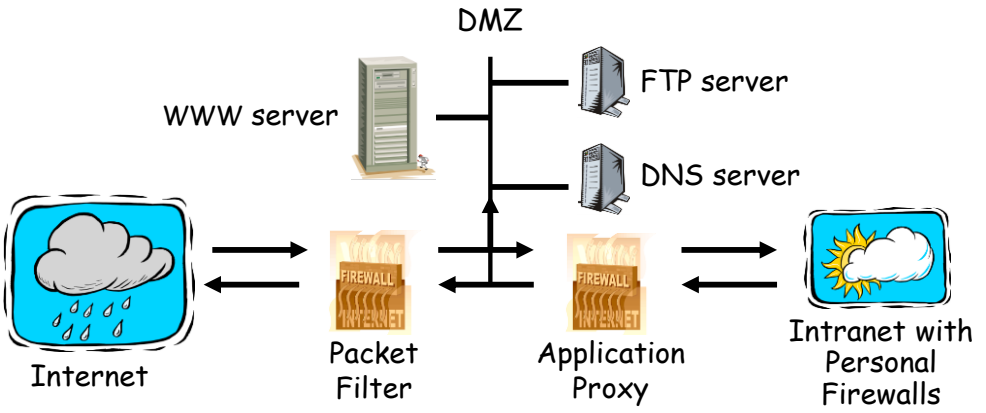
- To protect one user or home network
- Can use any of the methods
  - Packet filter
  - Stateful packet filter
  - Application proxy

54

The only difference is that personal firewall usually only protect one host or very small network.

Firewalls and Defense in Depth

- Example security architecture



55

This picture is important for you to think about what type of firewall is useful where – if you are going to have lots of traffic then maybe application proxy is not the best approach and basic packet filter is OK (all this traffic is going to carefully controlled server you configure).

However all traffic going to personal machines goes through a secondary firewall (application proxy).

Malicious Programs

Requires A Host Program
- Trapdoor/Backdoor
- Logic bombs
- Trojan horses
- **Viruses**

Independent of Host Programs
- Bacteria
- **Worms**

56

Viruses and Worms are the most well known.

You must be able to name and briefly describe and also identify each type of malware if given a description of its behaviour.

Make it simple for yourself by working out a scheme for yourself stating what the main differences are…

- Is it trying to replicate?

If yes – could be worm, virus, bacteria

If no, it could be backdoor, logic bomb, trojan horse

How is it trying to replicate? Over network (worm), spread to other files (virus), or just launching more instances(bacteria)?

Trapdoor/Backdoor

- A secret, undocumented entry point into a program
- Usually inserted during code development for testing, debugging and/or for future modification
- Developers forget to remove trapdoor when done
- Developers intentionally keeps the trapdoor for future modification or for accessing unauthorized information

Countermeasures

- Open source
- Develop your own program

57

You can also get hardware backdoors (the idea is the backdoor is built in hardware chips)

See example, search for: Clipper chips

Logic Bombs

- Code embedded in a legitimate program that is set to 'explode' when certain conditions are met
- 'Explosion' = modify files, delete files, shut down the system, etc.

An example of a logic bomb:
- Reported in 2024 in Poland
- Railway operator purchase trains from manufacturer
- Operator has trains serviced by another company
- Trains break down during servicing
  - Do not run
  - Report faulty components
- Software found that would disable trains in specific locations, if there for several days.
  - Locations of workshops of servicing company

58

Note this is in legitimate program – similar behavior could be in virus or worm as payload.

https://badcyber.com/dieselgate-but-for-trains-some-heavyweight-hardware-hacking/

Trojan Horses, Viruses, Bacteria and Worms

Trojan Horses

- A hidden code that performs a hidden function in addition to its stated function.
  - e.g. Collect passwords of a user, collect web browsing information of a user

Viruses

- A program that can 'infect' other programs by modifying them.
  - can cause geometric growth of infection

Bacteria

- A program that does not explicitly destroy any program or file. Its sole purpose is to replicate themselves to create resource starvation – availability attack.

Worms (network extension of viruses)

- It makes use of network management mechanism, identifies a free machine on the net, passes the worm program to other machines.

59

Hardware trojans (sort of like backdoor too).

Virus Stages

1. Dormant Stage
   - Activated by some predetermined condition
   - e.g. date, execution of certain part of a program
2. Propagation Stage
   - Places a copy of itself to another program or system areas
3. Triggering Stage
   - Triggered by some condition in the system and started performing the function it intends to
4. Execution Stage
   - The function performed could be harmless or damaging

In the past, viruses usually infect .exe and .com executable files. Nowadays, more and more viruses make use of macro to distribute and infect computers. Thousands of viruses are embedded inside macros of MsWord and MsExcel because those macros are easy to write. For example, someone can use Visual Basic to code a macro virus easily and email it to others.

60

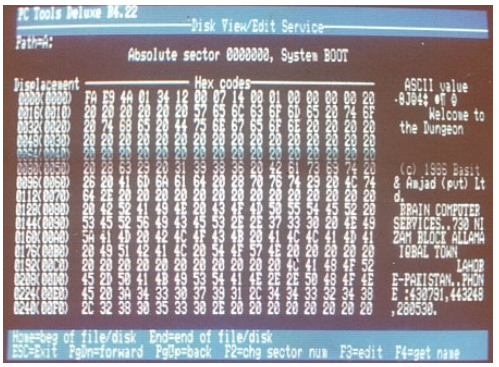
Macro virus is very powerful, think of it as code within another application….

Macro viruses infect documents and use the build in programming routines of document applications (say Word or Excel) to spread and do harm.

See : https://support.microsoft.com/en-hk/help/211607/frequently-asked-questions-about-word-macro-viruses

Viruses and Worms are malware that spreads – but their payloads could be anything ransomware like wannacry,cryptolocker or just delete all your files,

Virus Propagation



Viruses spread as files and storage moves

- Example: First PC virus was Brain 1986
- Overwritten boot sector of floppy disk
- Disk infects PC >> infects other disks…
- Effectively spread worldwide

61

Virus infects the machine and then tries to copy itself to other files/drives…

Two brothers from Pakistan wrote Brain to prevent people from copying their software (they ran a software business). Brain was supposed to track illegal copies.

The design had a flaw in that is ended up propagating much better than expected.

The virus contained and displayed their context details – they only realized what had happened once they started getting calls from worldwide asking them to fix systems.

"Welcome to the Dungeon © 1986 Basit & Amjads (pvt). BRAIN COMPUTER SERVICES 730 NIZAMBLOCK ALLAMA IQBAL TOWN LAHORE-PAKISTAN PHONE: 430791,443248,280530. Beware of this VIRUS.... Contact us for vaccination..."

Worms Stages

1. Dormant stage
2. Propagation stage
   - Search for free systems by examining host tables or remote system addresses (e.g. /etc/hosts)
   - Establish a connection with a remote system (e.g. rsh)
   - Copy itself to the remote system
3. Triggering stage
4. Execution stage

Damages Done

- Usually exploit weaknesses in an operating system or inadequate system management
- Usually results in brief but spectacular outbreaks, resulting in complete network shutdown

Counterattack

- Access control: identification and authentication protocols are needed
- Intrusion detection: statistics of user behavior
- Firewalls

62

So what is different between virus and worm?

Worm Propagation

Worms spread via a network

Propagation via email
- Example: ILOVEYOU (May 2000)
- Infected 10% of all Internet-connects PCs
- Simple email saying I Love You with LOVE-LETTER-FOR-YOU.txt.vbs file
- Only displays as txt file but script executed if opened
- Overwrite files, send to all Outlook contacts in address book

Propagation via other network vulnerabilities
- Vulnerabilities in network software (server OS/web), weak passwords (ssh)
- Example: Slammer (January 2003)
- Single UDP packet, exploits buffer overflow Microsoft's SQL Server
  - Known weakness (6 months old), servers not patched.
- Get server to start sending out attack packet to random IP address
- Started 12:30 am EST, by 12:33 AM slave servers doubles every 8.5 seconds
- Estimated to infect only 75,000 servers but generated so much traffic it disabled most others

63

ILOVEYOU Originated in Philippines – with interesting spread pattern starting in Hong Kong following from East to West as people woke up.

Slammer – the worm that crashed the Internet in 15 minutes

It started with a single packet. Generated so much network traffic it crashed systems worldwide

-5 of 13 root name servers crashed

-PC generally not effected as few had database products – data centres/corporate servers.

- Secondary traffic cause non-vulnerable systems to fail (as links got congested routing updates were so numerous that routers also crashed).

https://www.wired.com/2003/07/slammer/

Ransomware

Encrypts user data an asks for payment to restore original

- Often mentioned with malware
- Strictly not type of malware (it is a payload for malware, e.g. spread by worm)
- Also results of conventional hacking
- Some mitigation by addressing malware as it stops ransomware being delivered

64

Wannacry

May 2017

Unpatched older systems., eg.

Windows XP (2001, end support 2008) (hospitals UK NHS, everyday information systems at train station/airport displays.

The end!

Any questions…