CS5285
Information Security for eCommerce

Lecture 8

Dr. Gerhard Hancke

CS Department
City University of Hong Kong

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

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

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**)

Privacy and security is your responsibility

GET CAUGHT!

Using a unique password
(Not your pet's name)

Secure our role as a leader in e-Health. Do your part by using a strong password to defend against unauthorized access. Passwords must have eight or more characters and include at least one uppercase, one lowercase, one digit and one special character. Don't share your password or write it down.

Contact Privacy and Security
privacyandsecurity@sshs.on.ca
416 946 4767

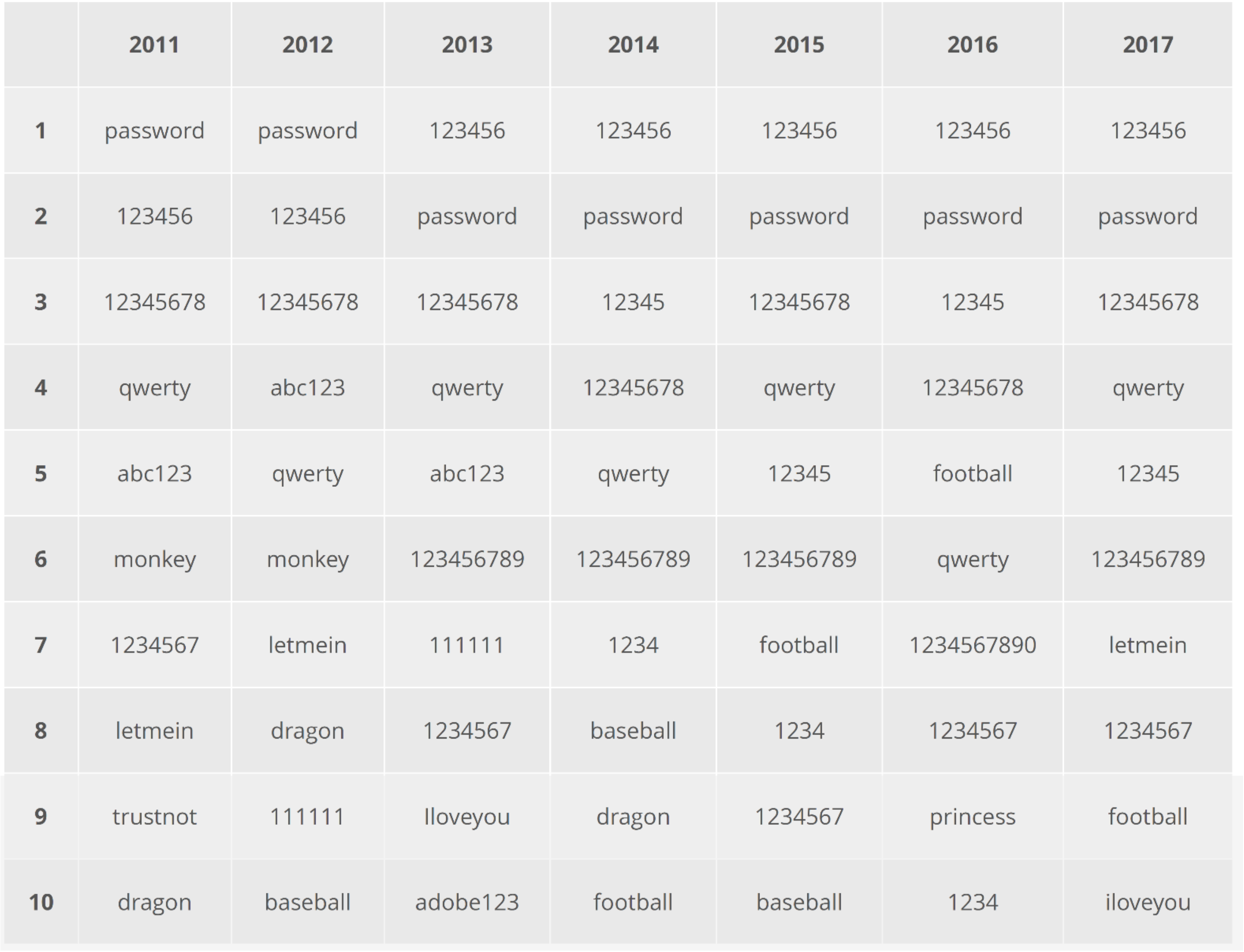
Get caught doing the right thing

Ontario
Smart Systems
for Health Agency

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!

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	Iloveyou	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
  - winner → **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

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

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

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/

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!

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

hashcat
advanced
password
recovery

Password File

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

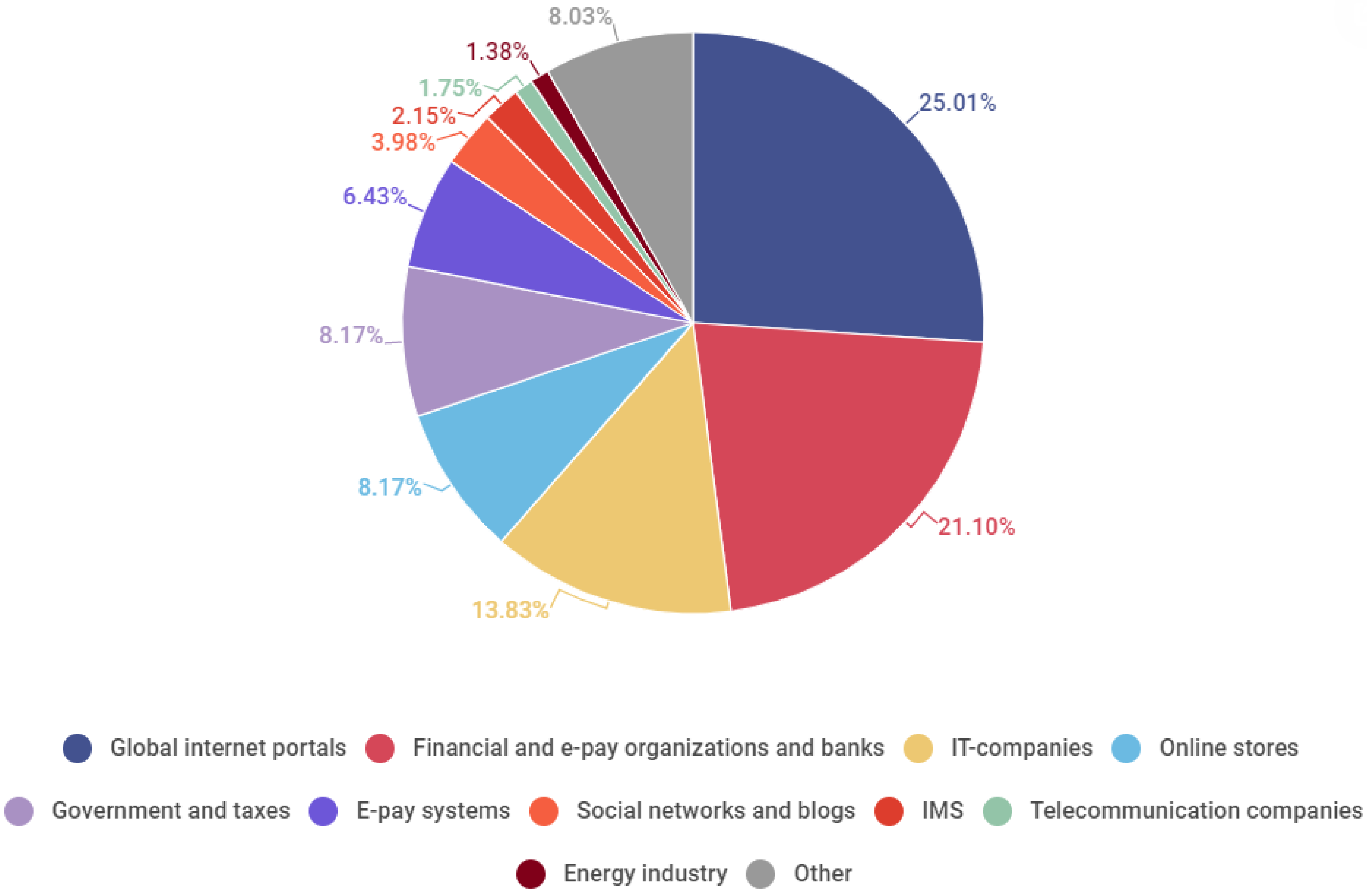
  $$y = h(\text{password}, s)$$

  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!

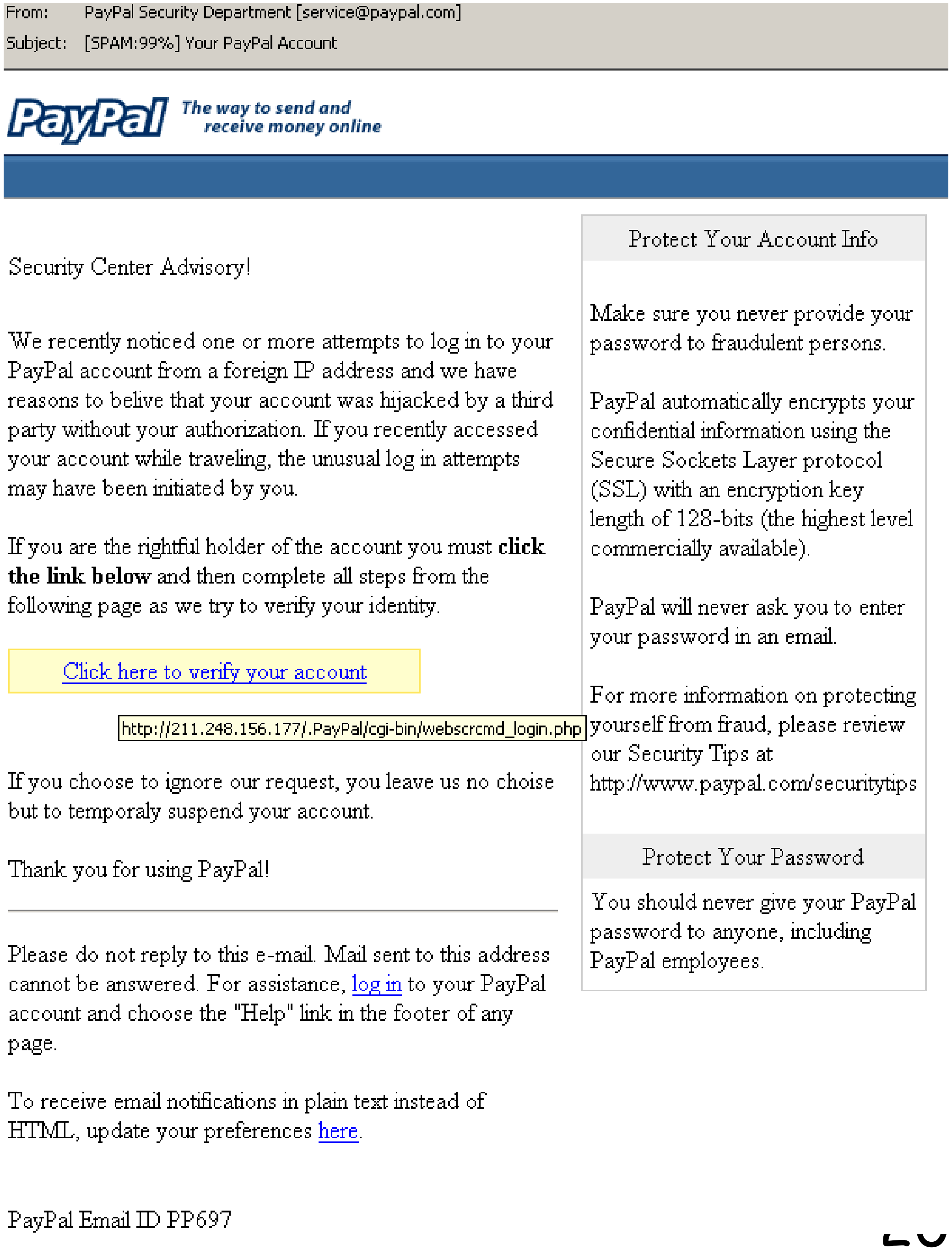
What goes wrong with passwords? Example: Email phishing

- 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!

Phishing targets



Source: Kasperksy Labs



From: PayPal Security Department [service@paypal.com]

Subject: [SPAM:99%] Your PayPal Account

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).

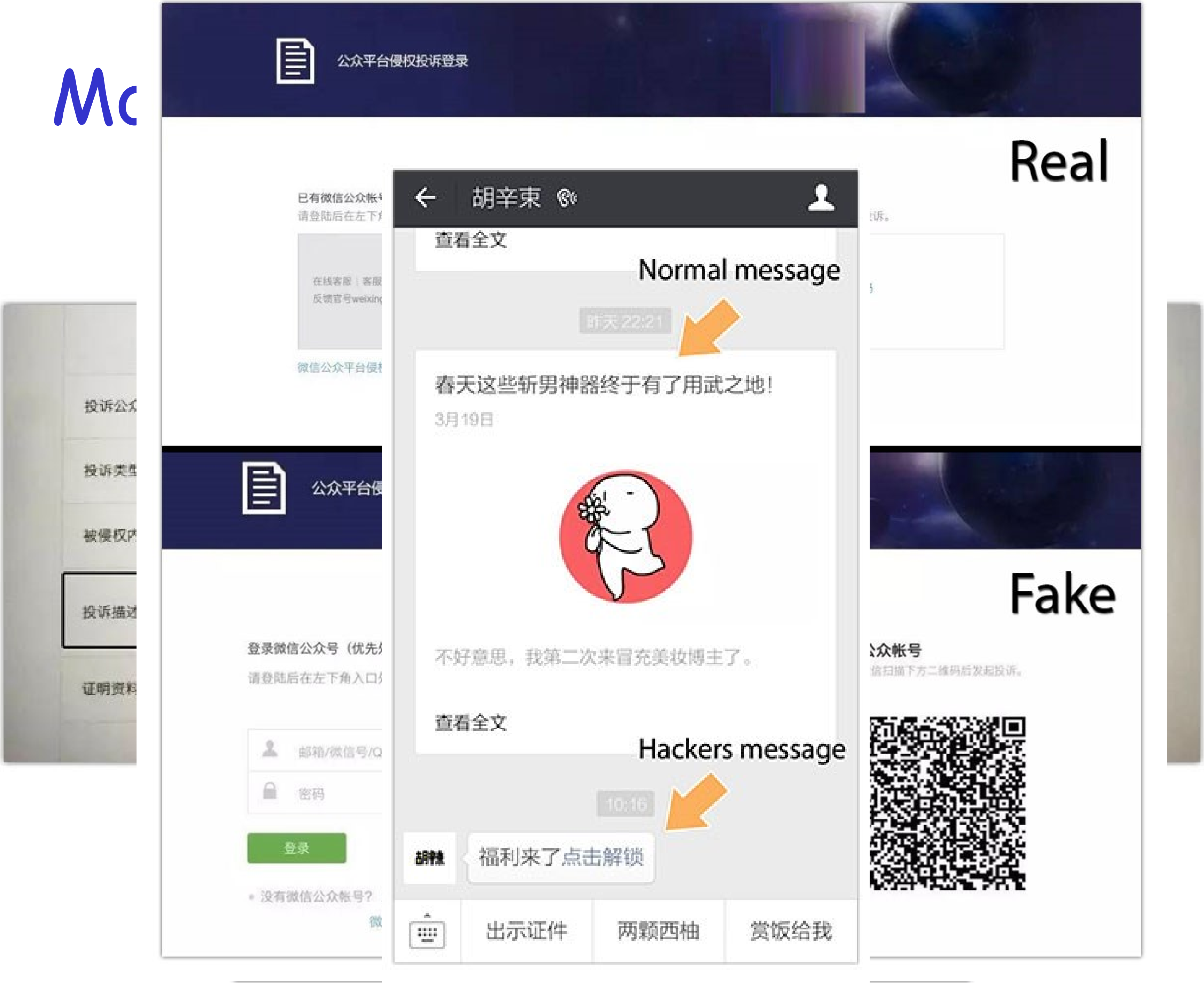
PayPal will never ask you to enter your password in an email.

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.

Mc



查看全文

昨天 22:21

春天这些斩男神器终于有了用武之地!

3月19日

不好意思，我第二次来冒充美妆博主了。

查看全文

10:16

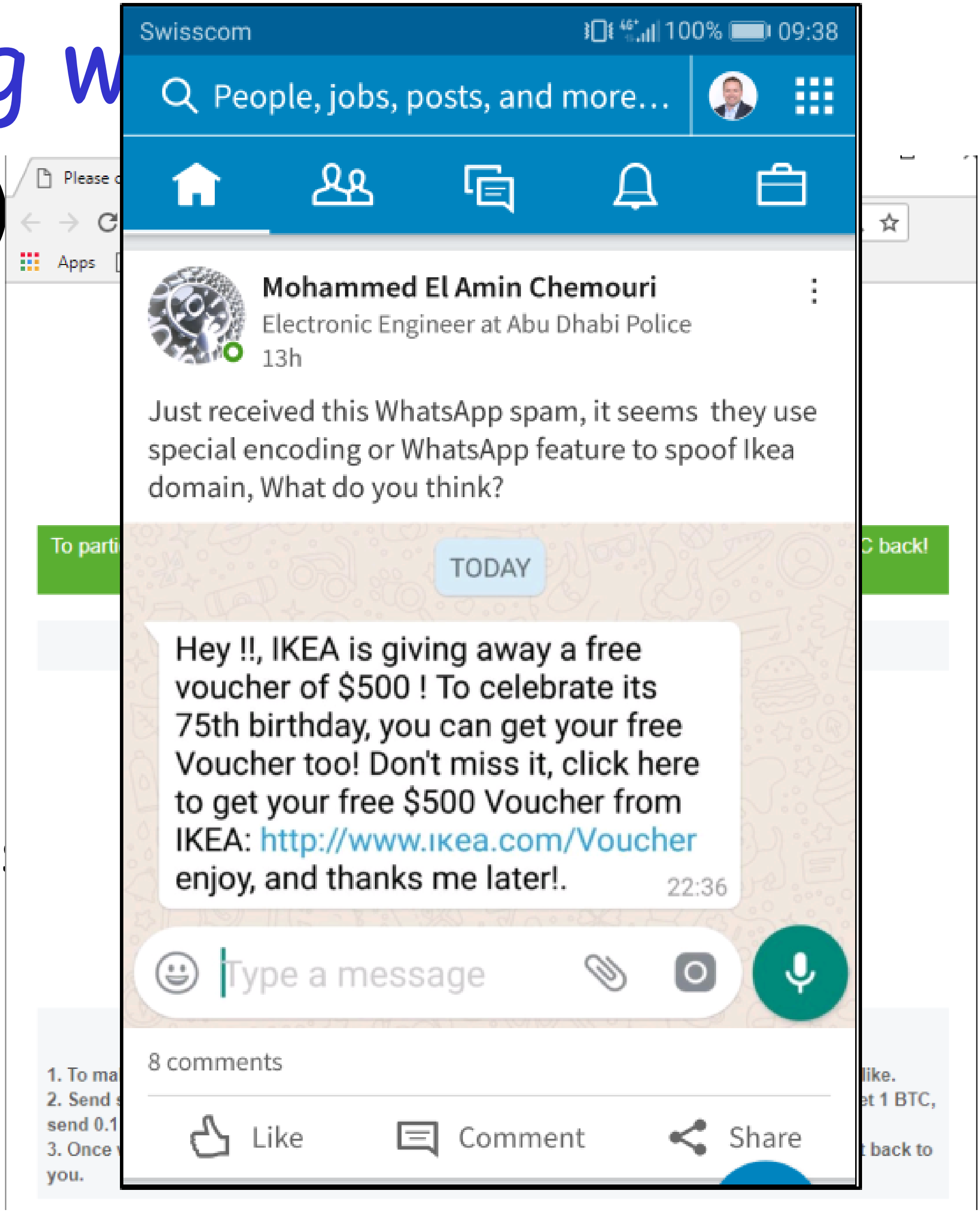
福利来了点击解锁

Phishing w

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

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

uses Cyrillic "a"not ASCII "a"



Mohammed El Amin Chemouri
Electronic Engineer at Abu Dhabi Police
13h

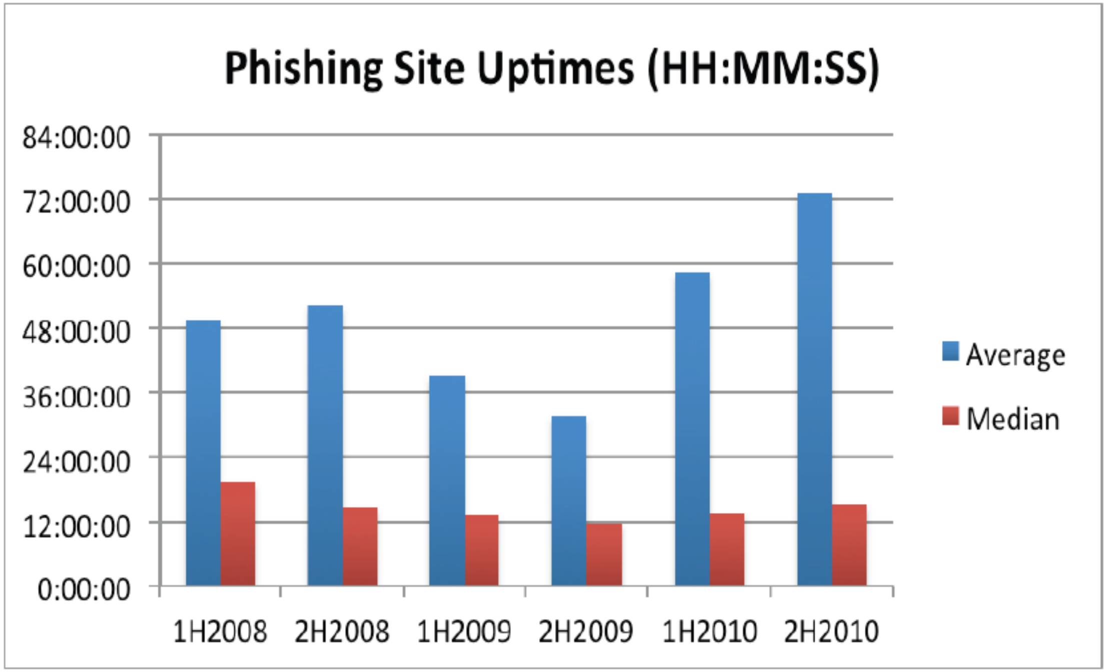
Just received this WhatsApp spam, it seems they use special encoding or WhatsApp feature to spoof Ikea domain, What do you think?

TODAY

Hey !!, IKEA is giving away a free voucher of $500 ! To celebrate its 75th birthday, you can get your free Voucher too! Don't miss it, click here to get your free $500 Voucher from IKEA: http://www.ıкea.com/Voucher enjoy, and thanks me later!. 22:36

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

Phishing websites (2)



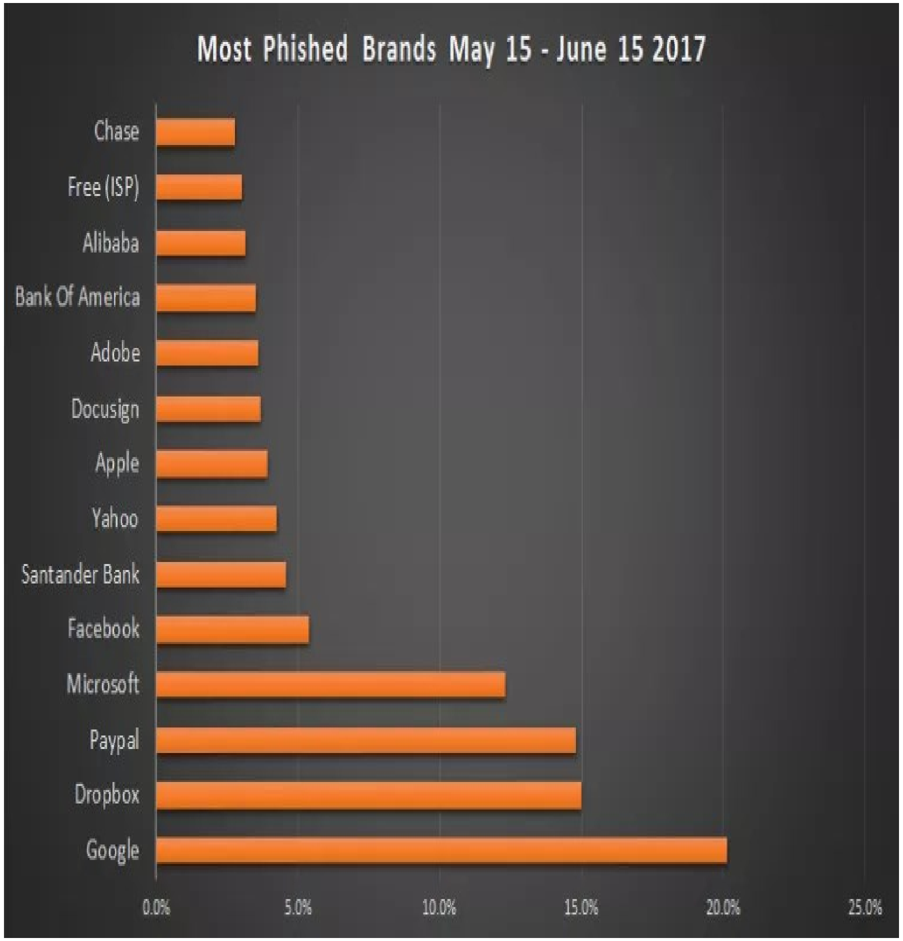
APWG

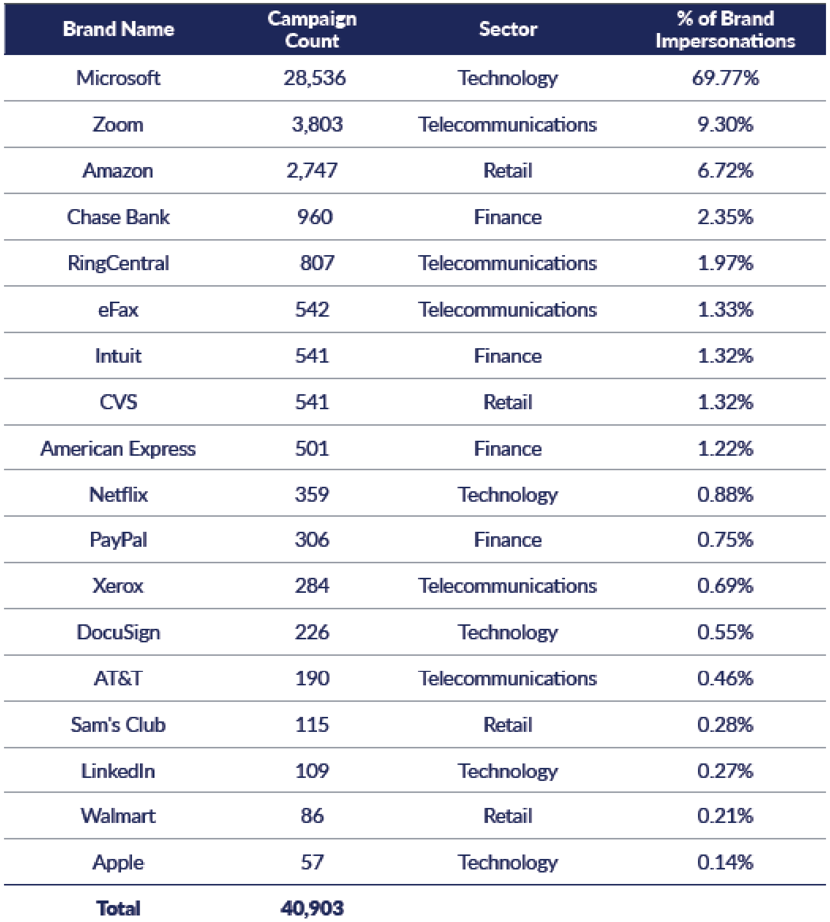
- Phishing sites are difficult to find and take down
  - Redirected through a collection of proxies
  - Scam sites are often hosted on compromised servers
  - Usually in poorly regulated countries
  - There is no direct connection between the phisher and the server
  - Sites are only live for a very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

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

Targets change



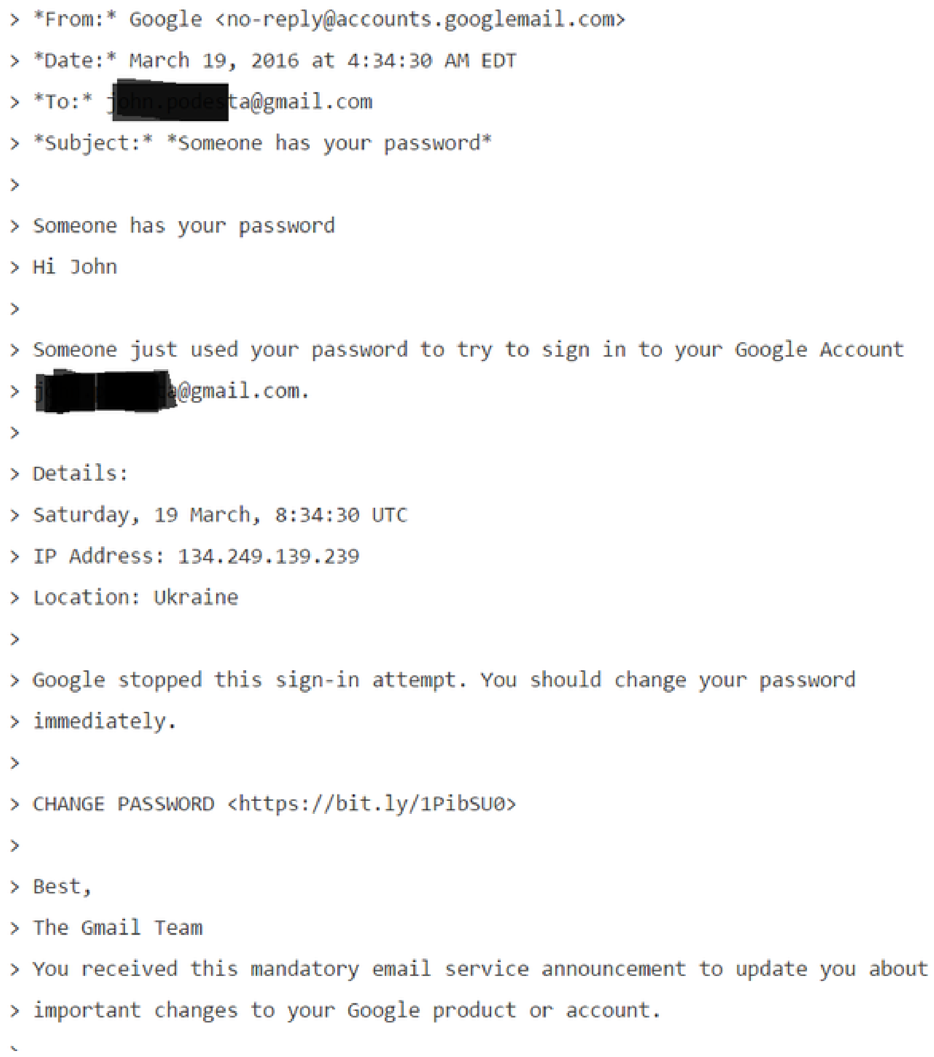


Brand Name	Campaign Count	Sector	% of Brand Impersonations
Microsoft	28,536	Technology	69.77%
Zoom	3,803	Telecommunications	9.30%
Amazon	2,747	Retail	6.72%
Chase Bank	960	Finance	2.35%
RingCentral	807	Telecommunications	1.97%
eFax	542	Telecommunications	1.33%
Intuit	541	Finance	1.32%
CVS	541	Retail	1.32%
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

Final example



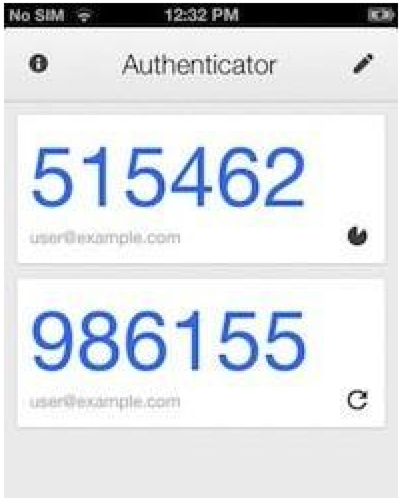
```
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* [redacted]ta@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [redacted]@gmail.com.
>
> 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.
>
```

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)

Something You Have and Know

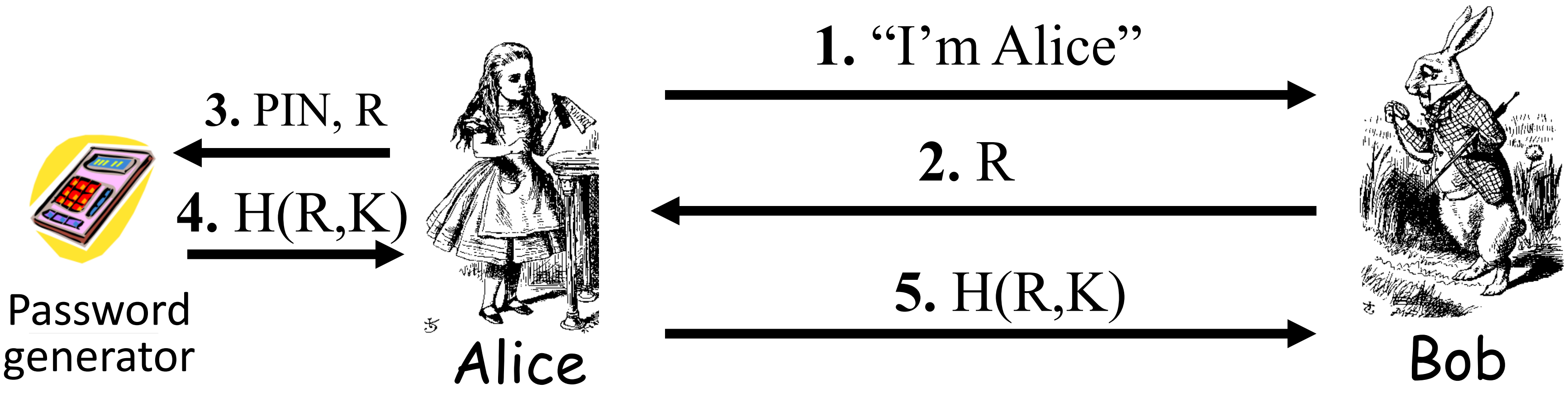
- Most common 2FA
  - Password + something in your possession
- Online and remote connection
  - Increasingly for corporate login/remote work
  - Password and one-time password/mobile app
  - Google/Microsoft Authenticator
  - Company-specific apps



515462
user@example.com

986155
user@example.com

Password Generator



1. "I'm Alice"

2. R

3. PIN, R

4. H(R,K)

5. H(R,K)

Password generator

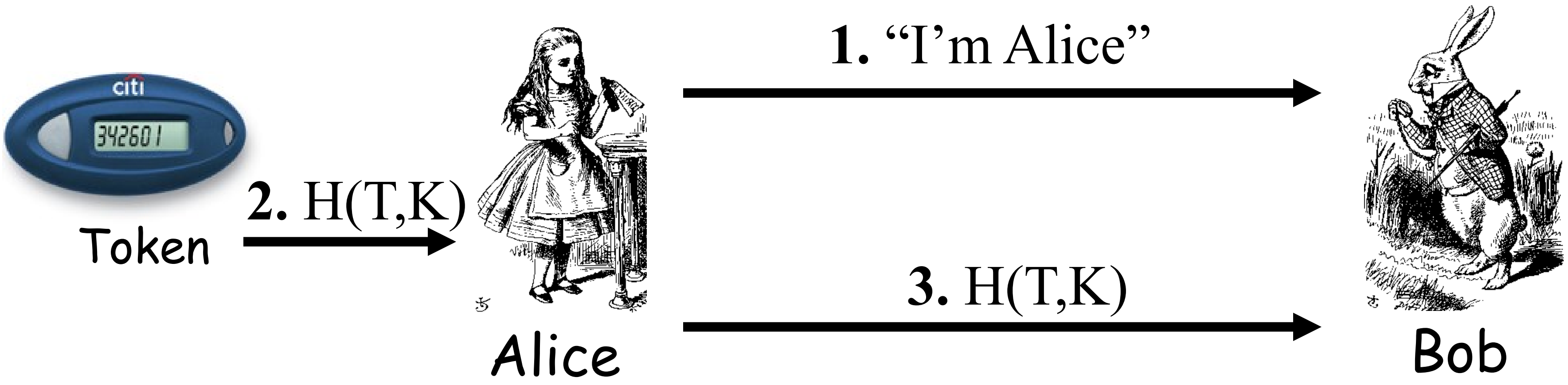
Alice

Bob

- 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!

Dynamic Password Token

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



1. "I'm Alice"

Token

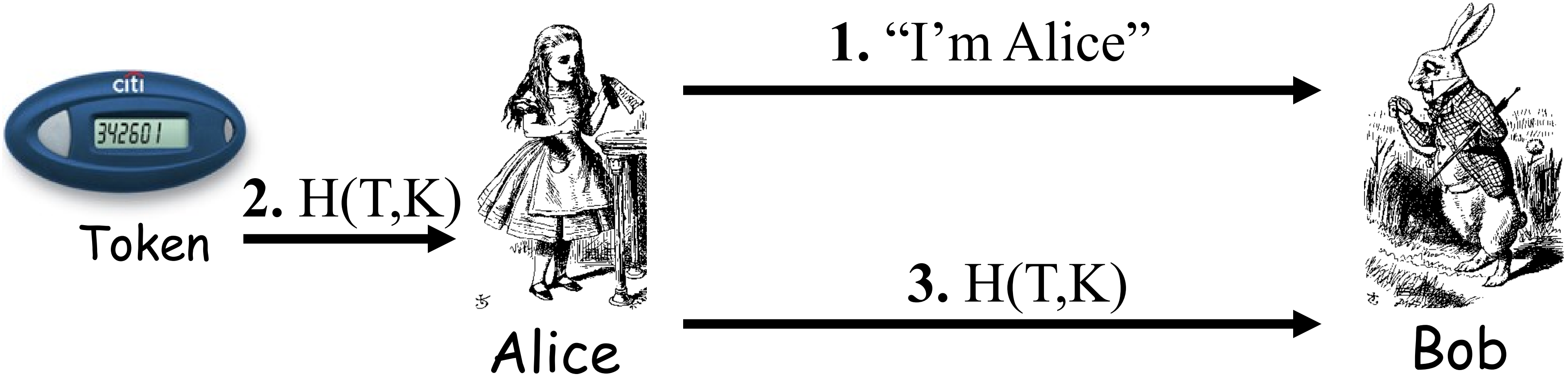
2. H(T,K)

Alice

3. H(T,K)

Bob

- 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.



1. "I'm Alice"

Token

2. H(T,K)

Alice

3. H(T,K)

Bob

<u>In practice, how a Dynamic Password Token is implemented?</u>

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

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

•contains reference code in Java

<u>further reference</u>

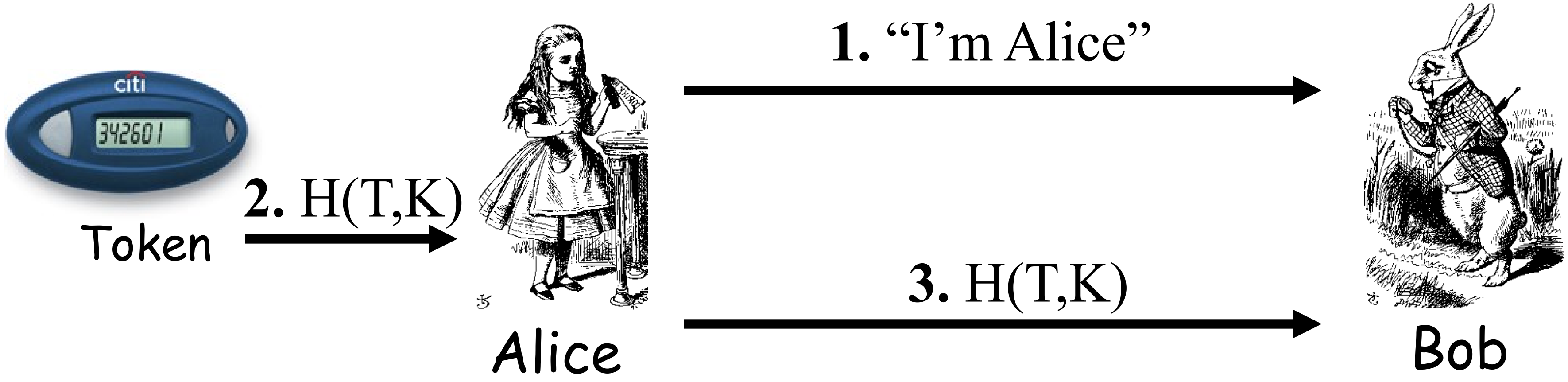
Google Authenticator

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.*



1. "I'm Alice"

2. H(T,K)

Token

3. H(T,K)

Alice

Bob

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.

Authorization
(brief note on Access Control)

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

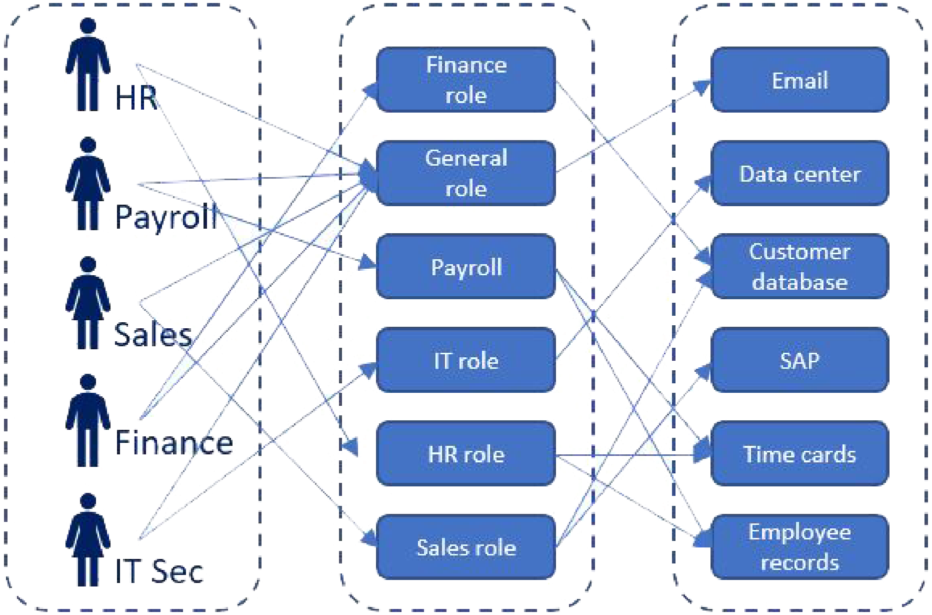
Lampson's Access Control Matrix

- **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

Role-Based Access Control

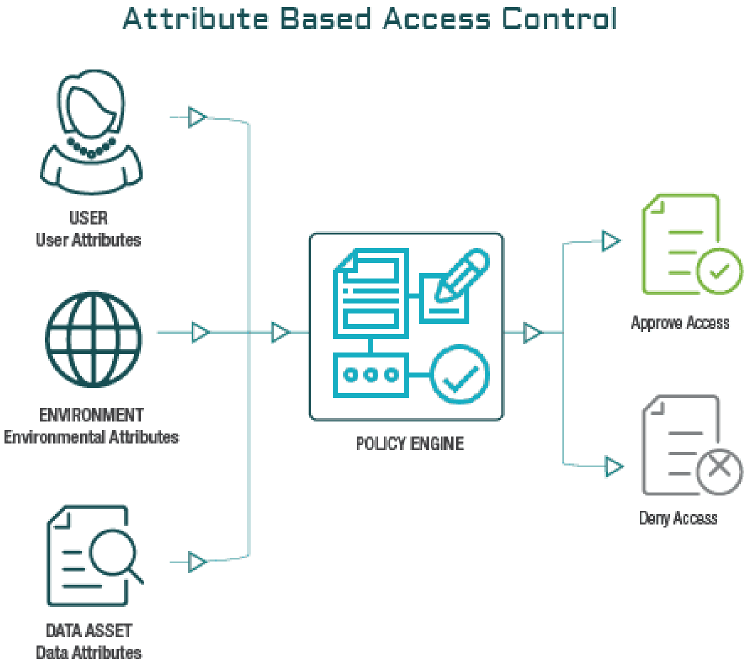
- No longer just linking subjects and objects
- Roles assigned access rights to objects
- Subjects are assigned roles



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

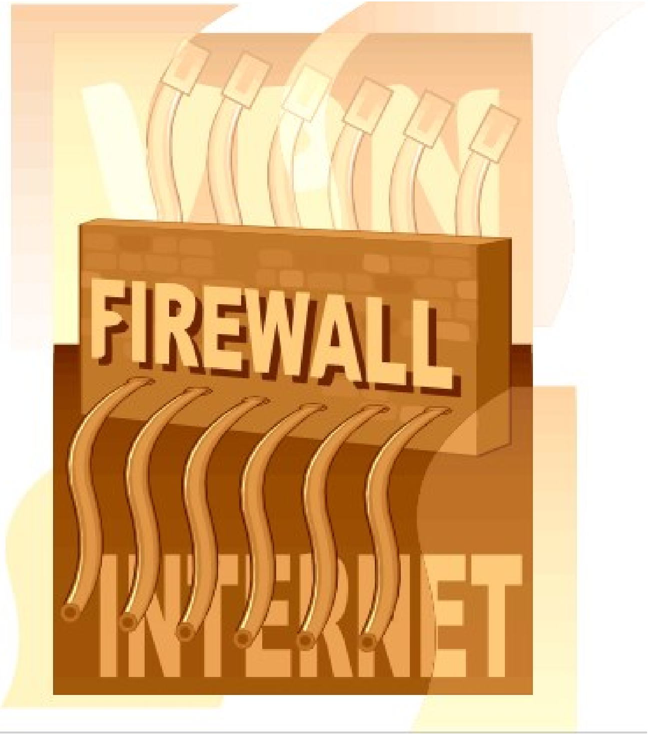
Attribute-Based Access Control

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

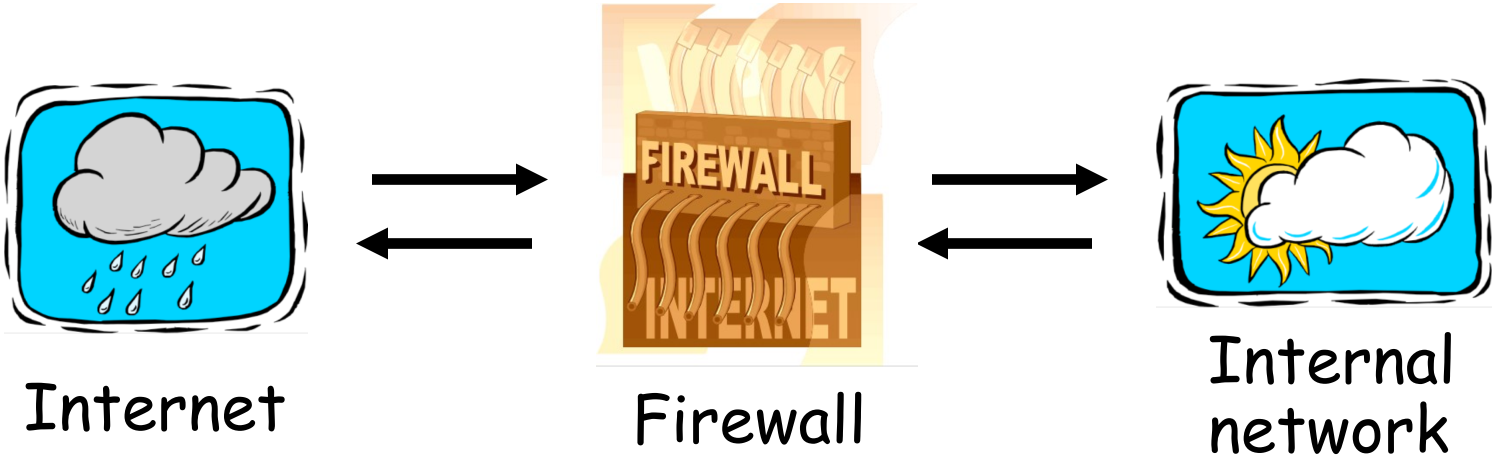


Credit:https://www.archtis.com/attribute-based-access-control-security-model/

Firewalls



Firewalls



Internet

Firewall

Internal network

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

Firewall as Secretary

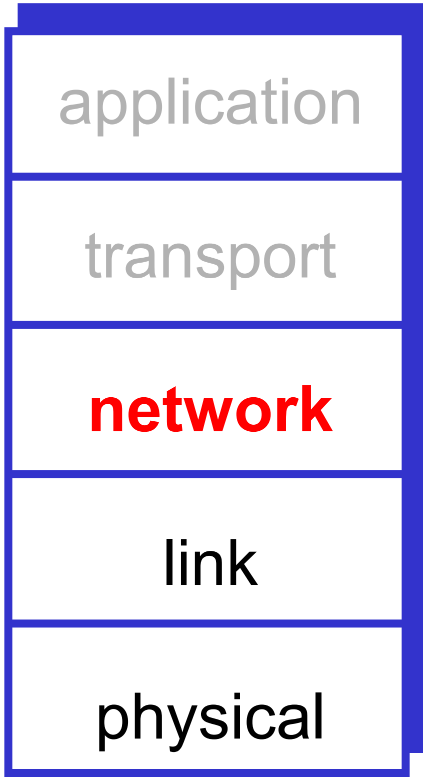
- A firewall is like a **secretary**
- To meet with an executive
  - First contact the secretary
  - Secretary decides if meeting is reasonable
  - Secretary filters out many requests
- You want to meet chair of CS department?
  - Secretary does some filtering
- You want to meet President of *country*?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

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.

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.)



application

transport

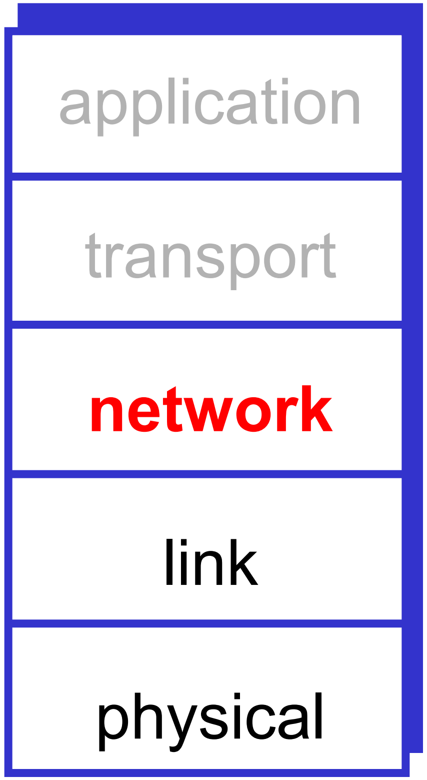
network

link

physical

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

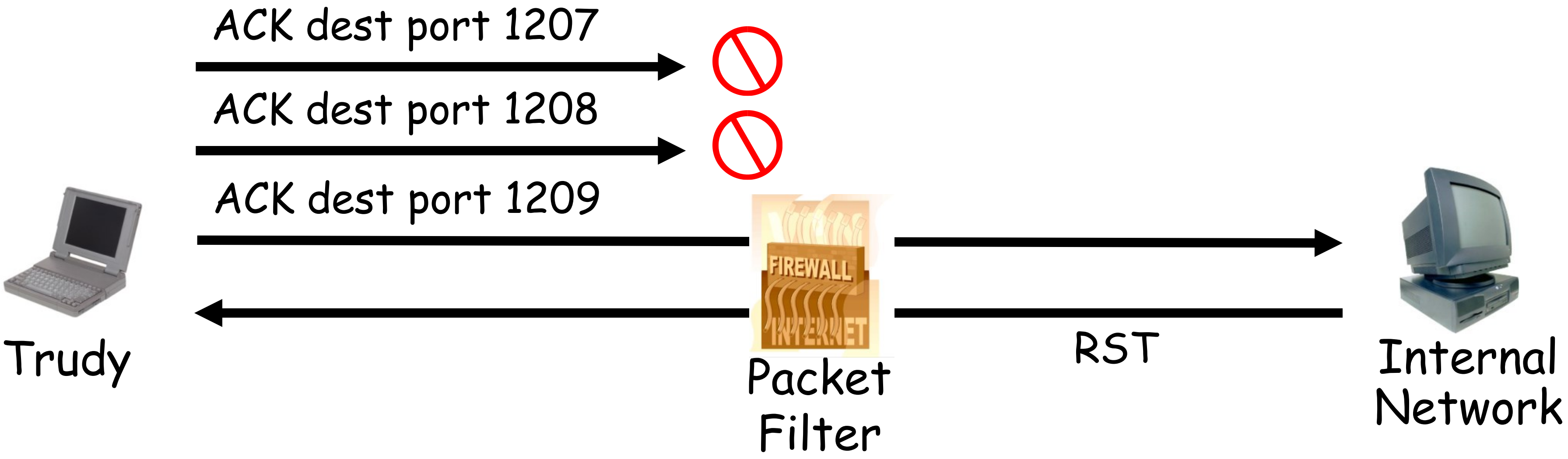
Action	Source IP	Dest IP	Source Port	Dest Port	Protocol	Flag Bits
Allow	Inside	Outside	Any	80	HTTP	Any
Allow	Outside	Inside	80	> 1023	HTTP	ACK
Deny	All	All	All	All	All	All

- Intention is to restrict incoming packets to Web responses

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

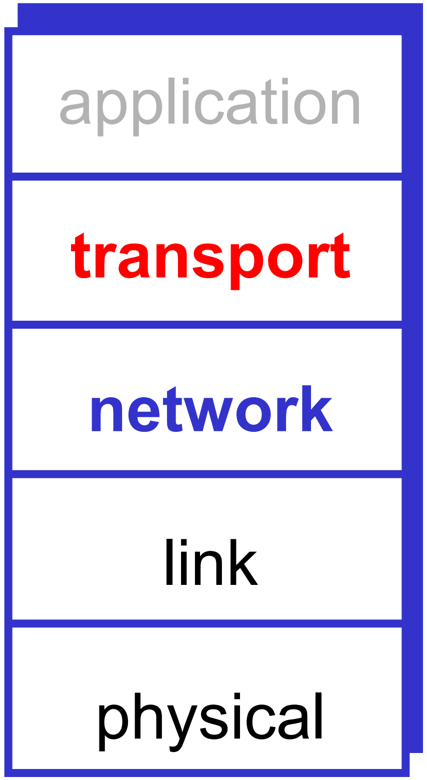
TCP ACK Scan



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

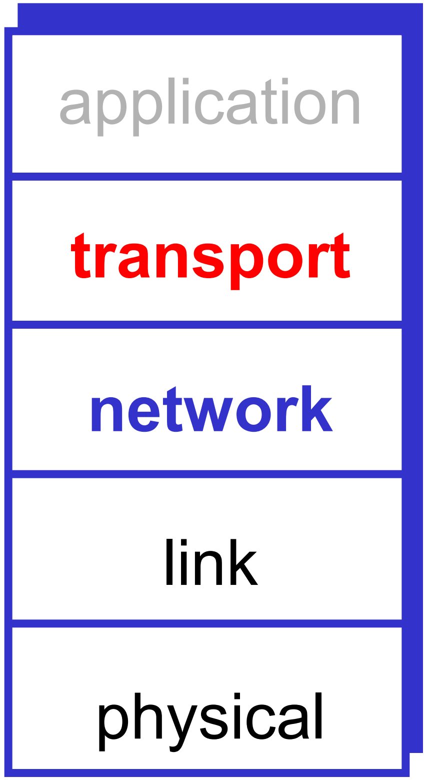
Stateful Packet Filter

- 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

transport

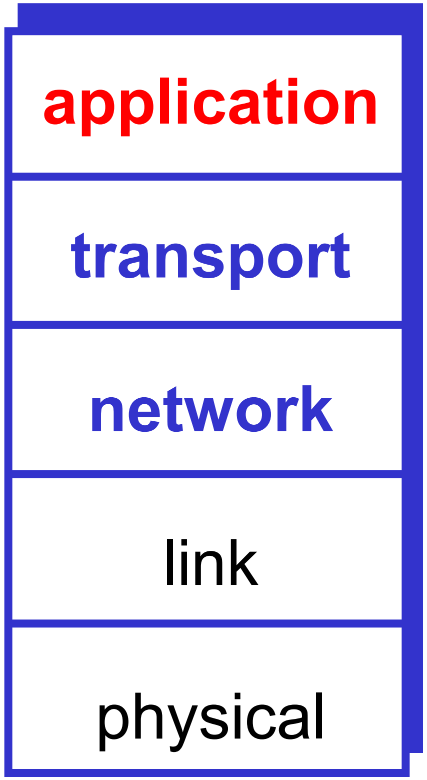
network

link

physical

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

transport

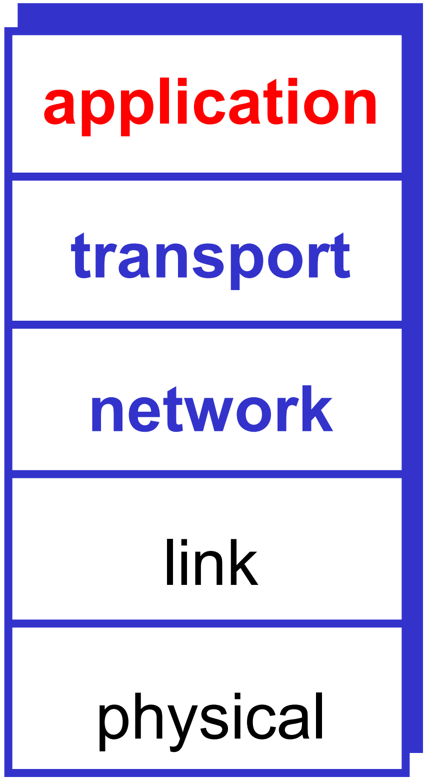
network

link

physical

Application Proxy

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



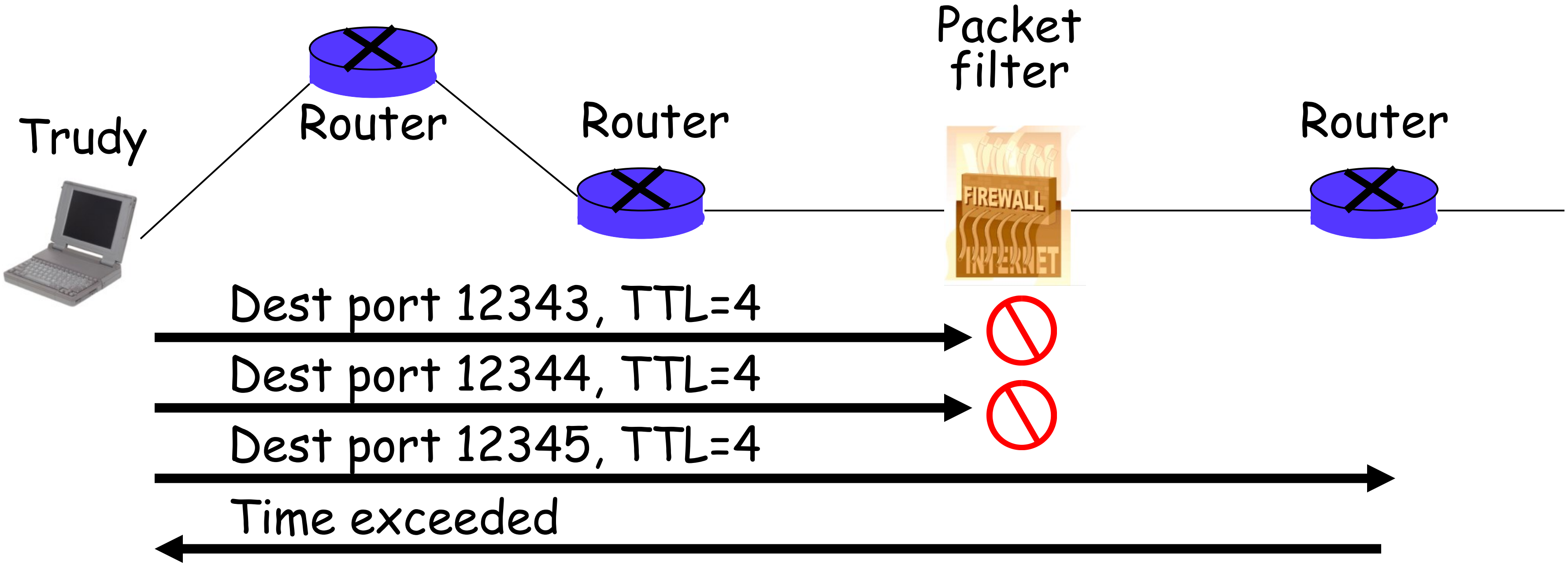
Application Proxy

- 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

Firewalk and Proxy Firewall



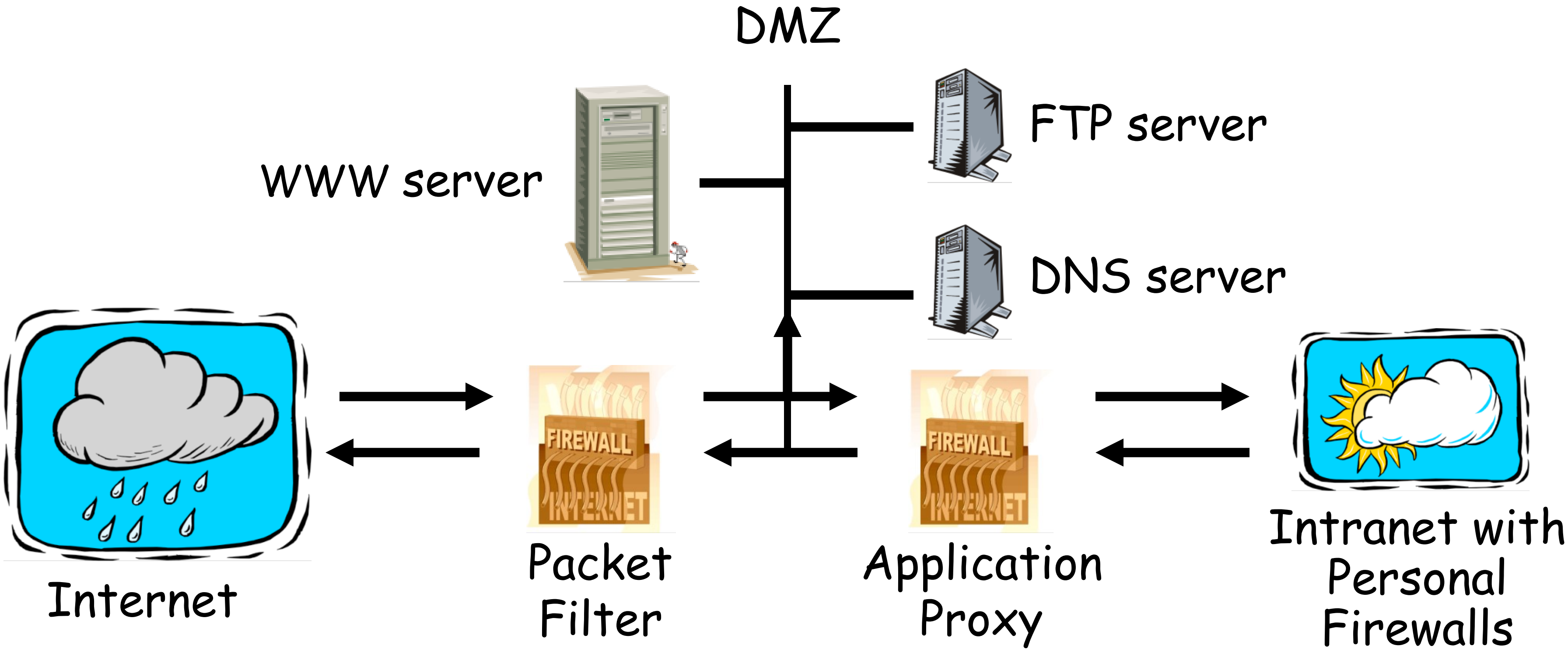
- This will **not** work thru an application proxy
- The proxy creates a new packet, destroys old TTL

Personal Firewall

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

Firewalls and Defense in Depth

- Example security architecture



Malicious Programs

Requires A Host Program

- Trapdoor/Backdoor
- Logic bombs
- Trojan horses
- **Viruses**

Independent of Host Programs

- Bacteria
- **Worms**

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

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

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)

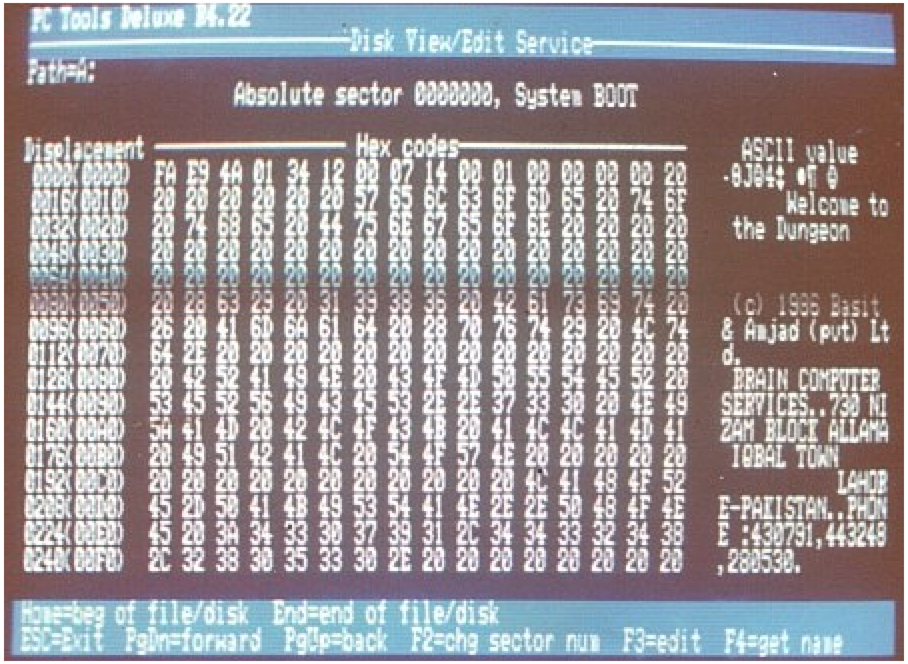
- It makes use of network management mechanism, identifies a free machine on the net, passes the worm program to other machines.

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.

Virus Propagation



```
PC Tools Deluxe R4.22
                              Disk View/Edit Service
Path=A:
                    Absolute sector 0000000, System BOOT

Displacement  ─────────── Hex codes ───────────────────────────     ASCII value
 0000(0000)  FA E9 4A 01 34 12 00 07 14 00 01 00 00 00 00 20   ·éJ☺4↕ •¶ ☺
 0016(0010)  20 20 20 20 20 20 57 65 6C 63 6F 6D 65 20 74 6F         Welcome to
 0032(0020)  20 74 68 65 20 44 75 6E 67 65 6F 6E 20 20 20 20    the Dungeon
 0048(0030)  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
 0064(0040)  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
 0080(0050)  20 28 63 29 20 31 39 38 36 20 42 61 73 69 74 20    (c) 1986 Basit
 0096(0060)  26 20 41 6D 6A 61 64 20 28 70 76 74 29 20 4C 74   & Amjad (pvt) Lt
 0112(0070)  64 2E 20 20 20 20 20 20 20 20 20 20 20 20 20 20   d.
 0128(0080)  20 42 52 41 49 4E 20 43 4F 4D 50 55 54 45 52 20    BRAIN COMPUTER
 0144(0090)  53 45 52 56 49 43 45 53 2E 2E 37 33 30 20 4E 49   SERVICES..730 NI
 0160(00A0)  5A 41 4D 20 42 4C 4F 43 4B 20 41 4C 4C 41 4D 41   ZAM BLOCK ALLAMA
 0176(00B0)  20 49 51 42 41 4C 20 54 4F 57 4E 20 20 20 20 20    IQBAL TOWN
 0192(00C0)  20 20 20 20 20 20 20 20 20 20 20 4C 41 48 4F 52              LAHOR
 0208(00D0)  45 2D 50 41 4B 49 53 54 41 4E 2E 2E 50 48 4F 4E   E-PAKISTAN..PHON
 0224(00E0)  45 20 3A 34 33 30 37 39 31 2C 34 34 33 32 34 38   E :430791,443248
 0240(00F0)  2C 32 38 30 35 33 30 2E 20 20 20 20 20 20 20 20   ,280530.

Home=beg of file/disk  End=end of file/disk
ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name
```

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

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

Worm Propagation

Worms spread via a network

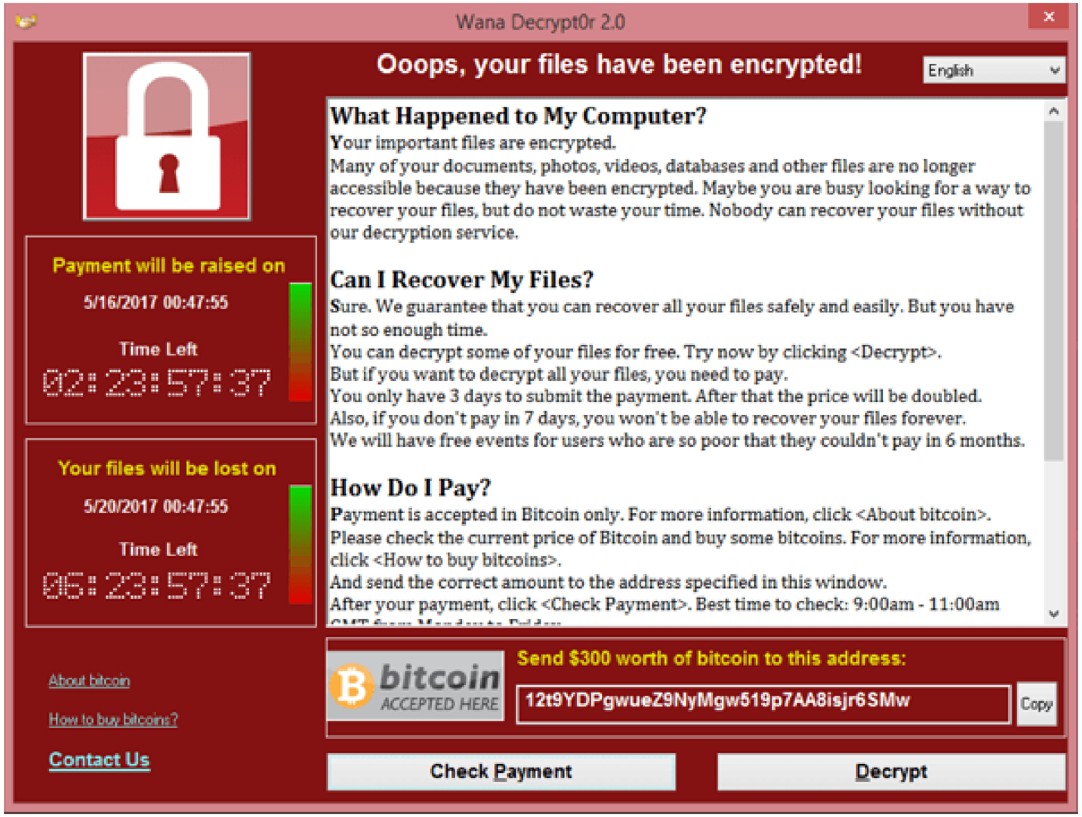
Propagation via email

- 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

Ransomware



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

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

The end!

?

Any questions…