Digital Identity & Machine Security

Announcement

- HW 04 Explained
- Please come to the TA office hours!

Hw 4 Explained

```
#USING CADE SERVERS
ssh username@lab1-10.eng.utah.edu
mkdir CS1060-HW4
cd CS1060-HW4
wget http://www.sci.utah.edu/~beiwang/teaching/cs1060/hw4.zip
unzip hw4.zip
cd hw4

# To edit a file
nano hw4.py

# To run a file
python3.5 wordcount.py
python3.5 streaming.py
```

MAC OS:

```
sudo pip install twitter
sudo pip install oauth

$ python wordcount.py
$ python streaming.py
```

The game of secret exchange:

Diffie-Hellman key exchange

Blue means public, Red means private/secret.

1. Alice and Bob agree to use a modulus $p = 23$ and base $g = 5$ (which is a primitive root modulo 23).
2. Alice chooses a secret integer $a = 6$, then sends Bob $A = g^a \bmod p$
   - $A = 5^6 \bmod 23 = 8$
3. Bob chooses a secret integer $b = 15$, then sends Alice $B = g^b \bmod p$
   - $B = 5^{15} \bmod 23 = 19$
4. Alice computes $s = B^a \bmod p$
   - $s = 19^6 \bmod 23 = 2$
5. Bob computes $s = A^b \bmod p$
   - $s = 8^{15} \bmod 23 = 2$
6. Alice and Bob now share a secret (the number 2).

Credit and further reading:
https://en.wikipedia.org/wiki/Diffie–Hellman_key_exchange
http://web2.0calc.com/

Rule of the Game

Need 2 teams, each with 2 members (preferably 1 member with a laptop).

1 team acts like Alice, 1 team acts like Bob.

Use modulus $p = 23$, base $g = 5$.

Follow the instruction on the previous page, compute A and B and send it each other...

Validate their shared secret!

Bonus point: 1 point for participation, 1 point for correctness + speed

The team then write down their computation on the board...

Review

Review

- Encryption
  - Plaintext: original message
  - Ciphertext: encrypted message
  - Key: a # used to encrypt/decrypt a message
- Key exchange
  - Share public info and private-public mix to generate a unique key private to 2 parties
- But…

Who are you exchanging keys with?

Attacks on Communication

Man-in-the-middle (MITM) attacks

- Intercept communications
- Can work against key exchange
- MITM maintains communication with each side

Attacks on Communication

Man-in-the-middle (MITM) attacks

- Intercept communications
- Can work against key exchange
- MITM maintains communication with each side

Attacks on Communication

Man-in-the-middle (MITM) attacks

- Intercept communications
- Can work against key exchange
- MITM maintains communication with each side

Attacks on Communication

Man-in-the-middle (MITM) attacks

- Intercept communications
- Can work against key exchange
- MITM maintains communication with each side

Digital Identity

Digital Identity

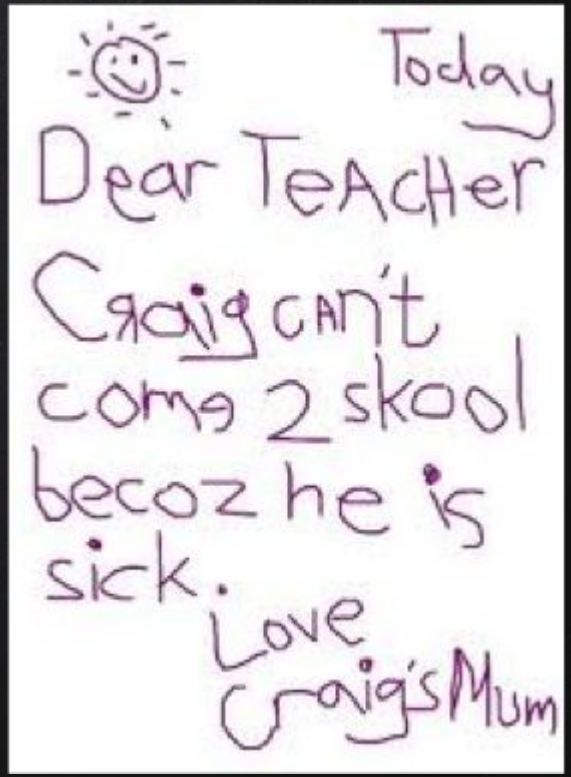
- Need to have a mechanism for authenticating identity
- How does this work in real life?
  - Letters from someone
  - Checks
  - Driving a car

Signatures

Written signatures

- Stored in a trusted institution (bank)
- Verified at time of signing by a notary
- Uses additional ID to determine your identity

Difficult to forge identity? Not really



Digital Signatures

- Digital things can be easily copied
  - If I see an image of a signature, I can make an exact copy
- Another mechanism is needed
- Need an action that only I can do but others can undo
  - Then others can tell something was sent by me

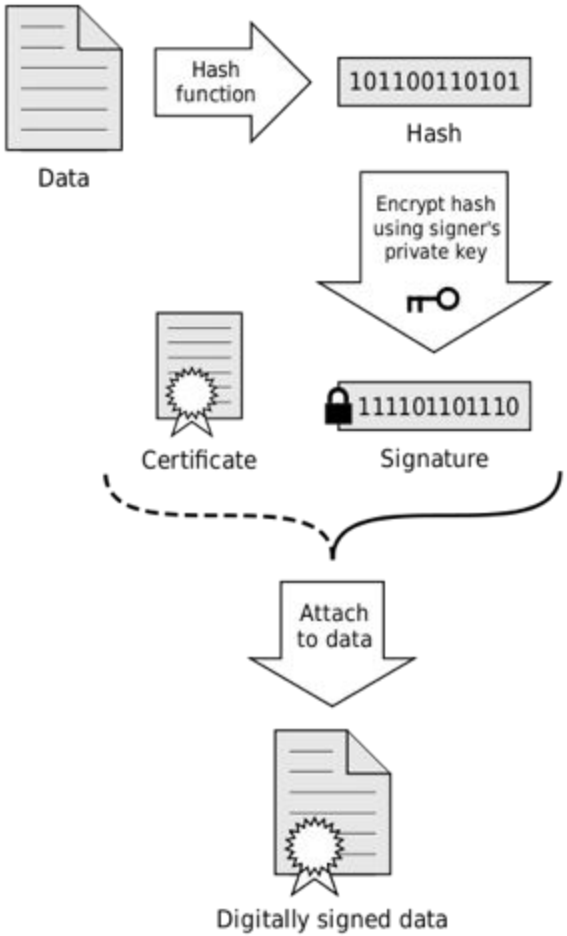
Public/Private Key

- I create a cipher which 2 keys
  - Public and private key
    - Mathematically related
  - Encrypt with 1 key
  - Decrypt with another key
- Public key stored in a trusted location

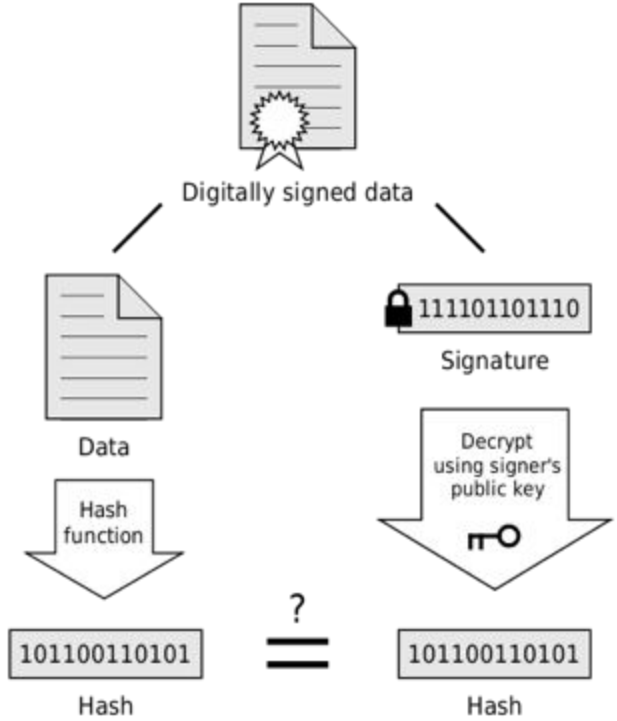
Private/Public Key Applications

- If someone wants to verify a document comes from me
  - I make a checksum (hash) of the document
  - Encrypt the checksum with my private key
  - Send the document
  - The receiver decrypts the checksum with the public key from me
    - Compares the real checksum of the document with the decrypted one I sent

Signing



Verification

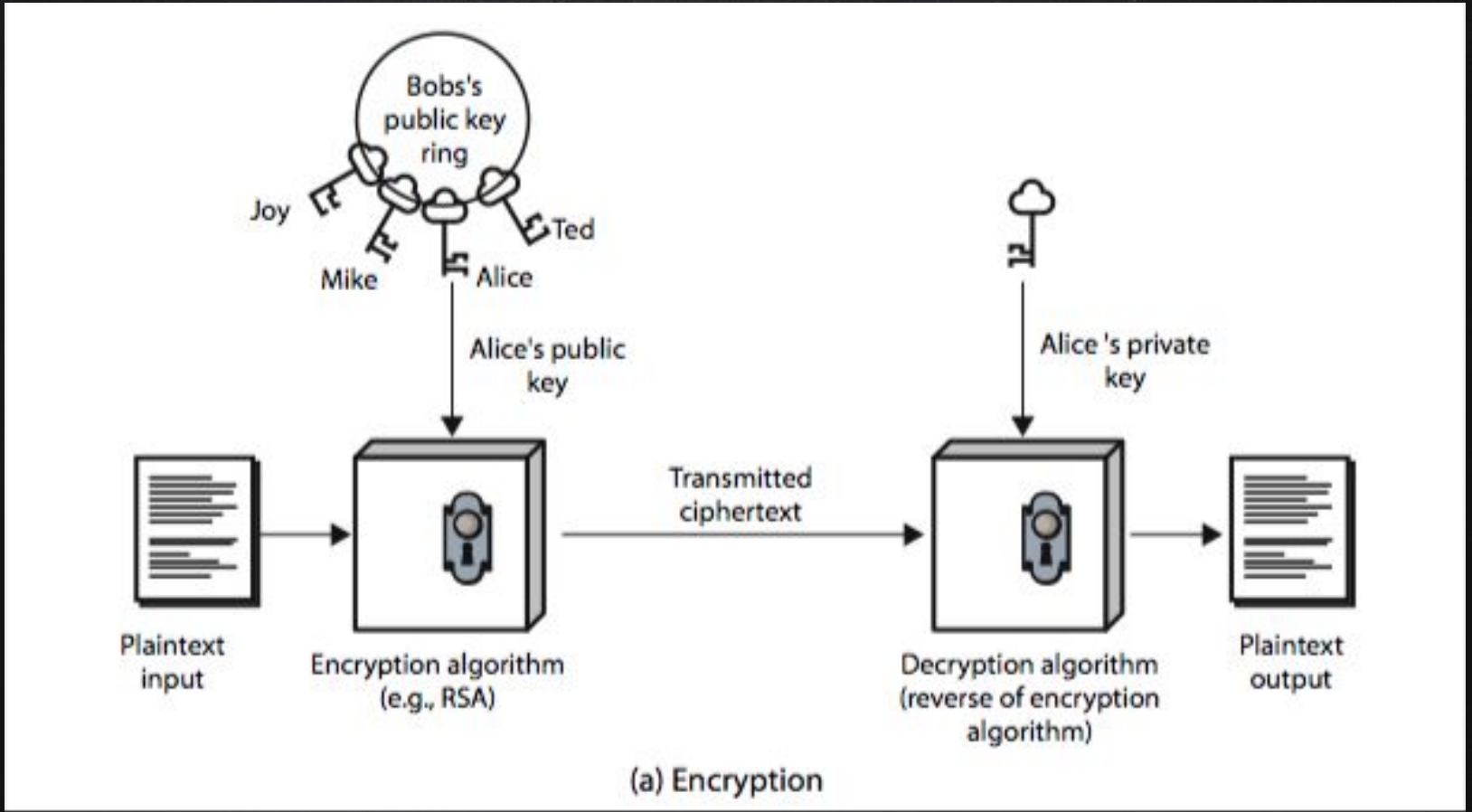


If the hashes are equal, the signature is valid.

Private/Public Key Applications

- Send me a private message
  - Encrypt with public key
  - The holder of the private key is the only one who can decrypt it
- This is computationally more difficult for big messages than doing a Diffie-Hellman key exchange followed by encrypting using a different cipher

Sending Using Public Key



RSA public/private cipher

- Named for inventors
- Similar to math for Diffie-Hellman key exchange
  - Raise to a power modulo some #
- Based on a big #
  - Difficult to factor: bignumber = A x B
  - A and B help make the public and private keys
    - A and B are primes
    - Would take billions of years to guess the private key from the public

RSA EXPLAINED

1. Choose two different large random prime numbers p and q
2. Calculate $n = pq$
   - n is the modulus for the public key and the private keys
3. Calculate the totient: $\phi(n) = (p-1)(q-1)$.
4. Choose an integer e such that $1 < e < \phi(n)$, and e is coprime to $\phi(n)$ **ie:** e and $\phi(n)$ share no factors other than 1; gcd(e,$\phi(n)$) = 1.
   - e is released as the public key exponent
5. Compute d to satisfy the congruence relation $de \equiv 1 \pmod{\phi(n)}$ **ie:** $de = 1 + k\phi(n)$ for some integer k.
   - d is kept as the private key exponent

https://simple.wikipedia.org/wiki/RSA_(algorithm)

https://www.youtube.com/watch?v=zsjZ2r9Ygzw

A group of Johns Hopkins University researchers found a bug in Apple's encryption that would let a skilled attacker decrypt photos and videos that were sent as secure instant messages. (Matthias Schrader/AP)

https://www.washingtonpost.com/world/national-security/johns-hopkins-researchers-discovered-encryption-flaw-in-apples-imessage/2016/03/20/a323f9a0-eca7-11e5-a6f3-21ccdbc5f74e_story.html

Summary

Public/private keys are an incredibly useful tool

- Often just used to establish identity and a shared secret key
- Shared key is then used for further private communication

Machine Security

Machine Security

- All of this network security depends on having a secure local machine
- Computer data is valuable: identity theft
- Computer resources are valuable
  - Botnets use processing and internet connections

A botnet (zombie army) is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet.

http://searchsecurity.techtarget.com/definition/botnet

https://en.wikipedia.org/wiki/Botnet

http://searchsecurity.techtarget.com/definition/botnet

Botnets explained

Compromised machines:

- Users download a malicious file
- It exploits errors in the system code
- Makes a zombie PC
- A bot master can send commands without logging in

Botnets of up to 12 million machines discovered

- Hired out to send spam
- Denial of service attacks: millions of machines all trying to access a web page
- Extortion against such threats (before it looks too appealing as a future career: prices have fallen dramatically)
- New value as bitcoin miners

Basics of System Security

- Something you know: password
- Something you have:
  - Not often used
  - A card/key
  - Fingerprints (for PC and USB drives)

Passwords

- Passwords allow access to machines or system settings
- Passwords are encrypted and stored in a computer file
- When you log in, your typed-in password is encrypted, compared against encrypted stored password
- Nobody knows your plaintext password

Set password: ChangeMe

Encrypted: Edr4^7dW

Login: ChangeMe

OS compares Edr4^7dW

to the stored Edr4^7dW

Only you know your plaintext

The 25 Most Popular Passwords of 2015: We're All Such Idiots

http://gizmodo.com/the-25-most-popular-passwords-of-2015-were-all-such-id-1753591514

The 25 Most Popular Passwords of 2015: We're All Such Idiots

1. **123456** (Unchanged)
2. **password** (Unchanged)
3. **12345678** (Up 1)
4. **qwerty** (Up 1)
5. **12345** (Down 2)
6. **123456789** (Unchanged)
7. **football** (Up 3)
8. **1234** (Down 1)
9. **1234567** (Up 2)
10. **baseball** (Down 2)
11. **welcome** (New)
12. **1234567890** (New)
13. **abc123** (Up 1)
14. **111111** (Up 1)
15. **1qaz2wsx** (New)
16. **dragon** (Down 7)
17. **master** (Up 2)
18. **monkey** (Down 6)
19. **letmein** (Down 6)
20. **login** (New)
21. **princess** (New)
22. **qwertyuiop** (New)
23. **solo** (New)
24. **password** (New)
25. **starwars** (New)

http://gizmodo.com/the-25-most-popular-passwords-of-2015-were-all-such-id-1753591514

Password Cracking

Sometimes, people gain access to encrypted password file

- Can spend days/weeks trying out passwords to see if they match
  - Modern systems can try 3.5 billion passwords/sec
- Use dictionaries of common passwords to speed search
- How many possibilities if random?
  - 4 letters (26 x 26 x 26 x 26) = 456, 976
  - 8 letters = 200 billion
- Adding uppercase and numbers increases possibilities
  - 4 characters (80^4) = 40,960,000
  - 8 (80^8) = 1.6 quadrillion

Social Engineering

Gaining access to secure areas/passwords through social means

- Physical access is often enough to gain admin privileges to machines
- Pretexting: learn enough about someone to gain initial access, learn more, repeat
- Baiting: leave malicious software in a location where it might be picked up and installed
- Quid Pro Quo: randomly call offering tech support. Have users type commands that install malware.

Phishing

Attempt to gain sensitive info

- Pretend to be from trusted site: use logos, obscure web page locations
- Use panic to push people to act: account is compromised/suspended, etc.
- Works because:
  - Will match some small percentage of people who use the site/service
  - People with ongoing problem so the need appears legitimate

Web Server Hiding

Many ways of hiding malicious web servers:

- Incorrect link in a message
- Use close approximations

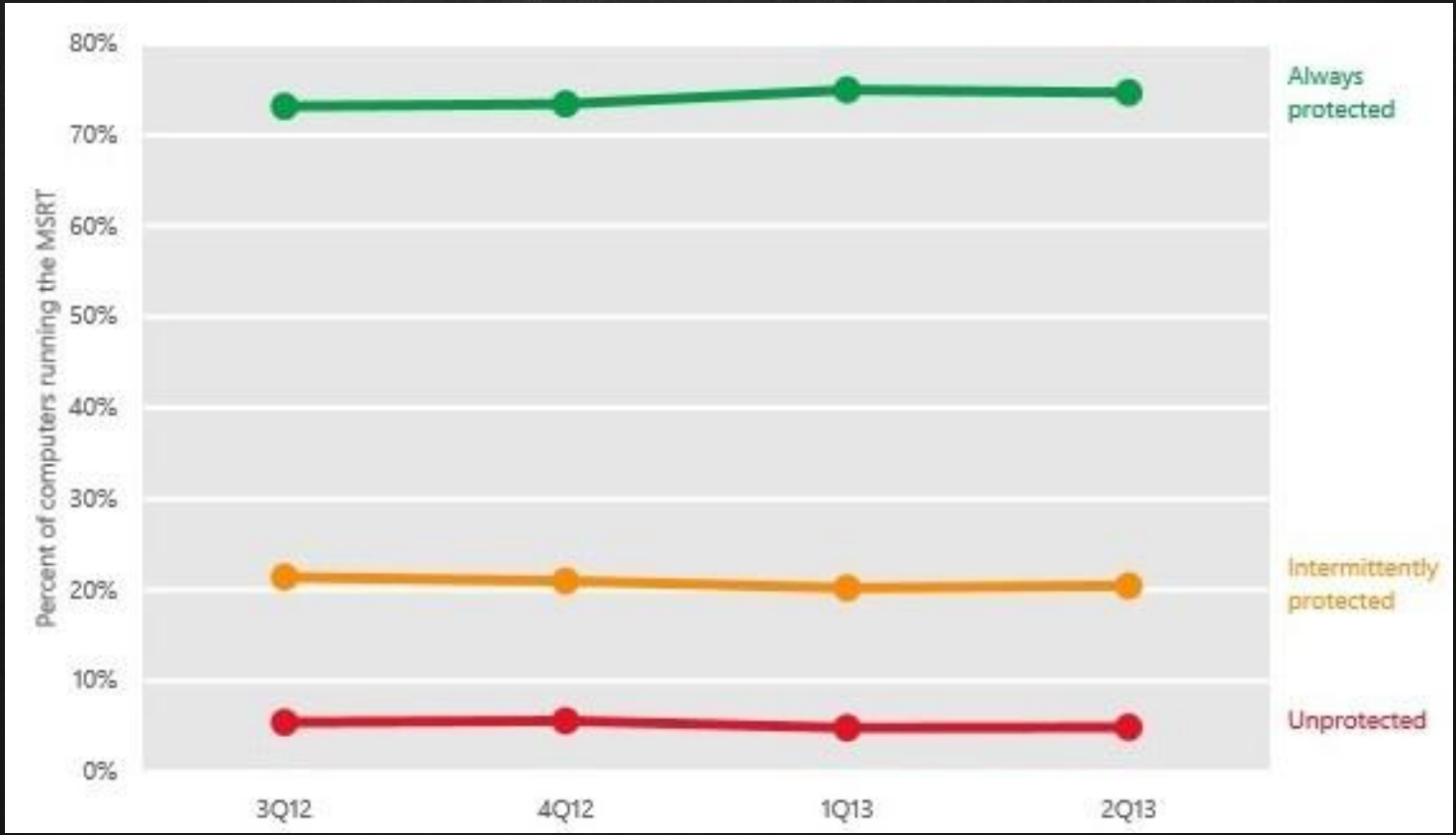
- http://privatebanking.mybank.com.**ch**
- http://mybank.**privatebanking**.com
- http://privatebanking.**mybonk**.com or even http://privatebanking.**mybánk.**com
- http://privatebanking.mybank.**hackproof.com**

Malware: malicious software

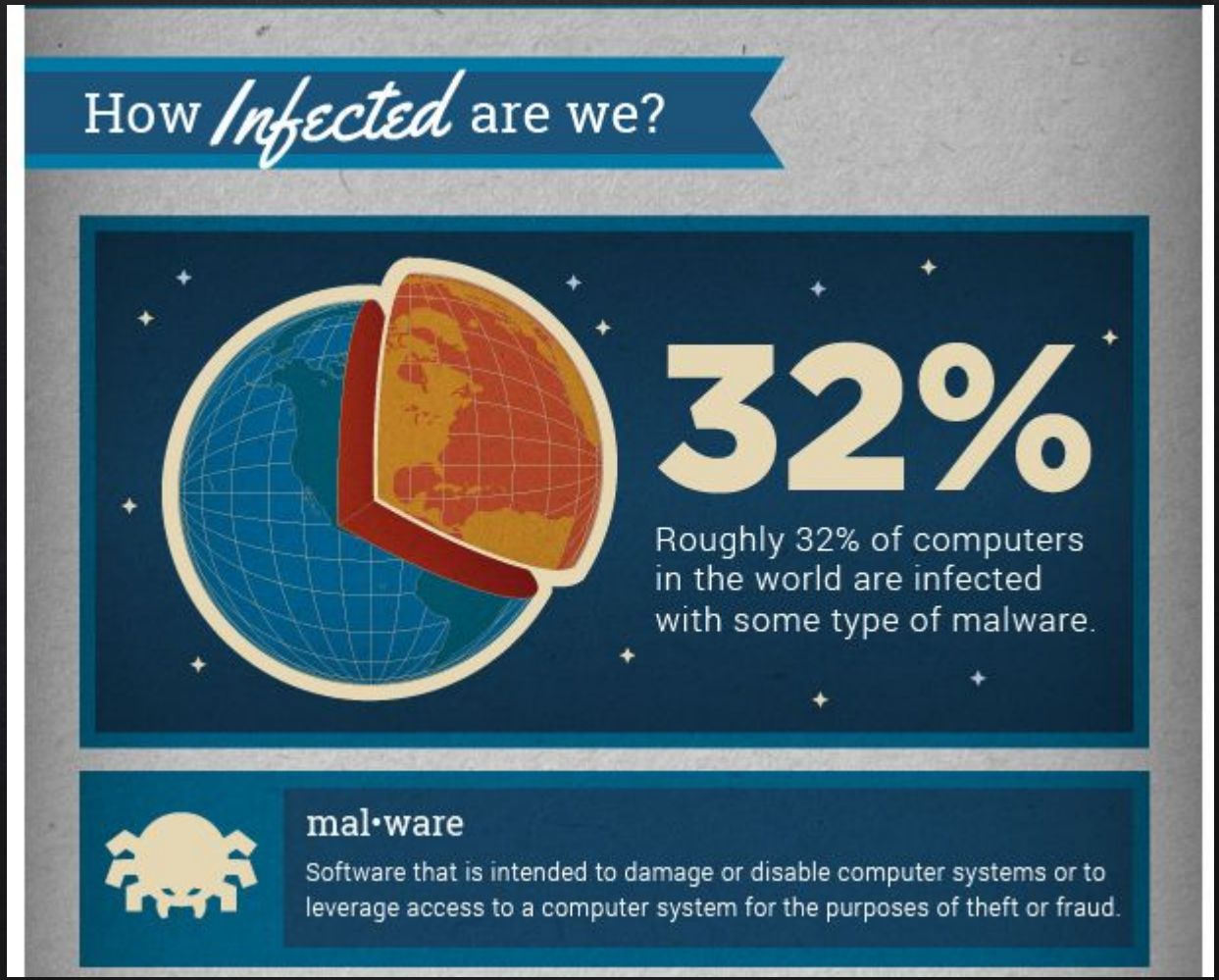
Mal – Latin for bad or evil

Malware is any program that is designed to harm a computer

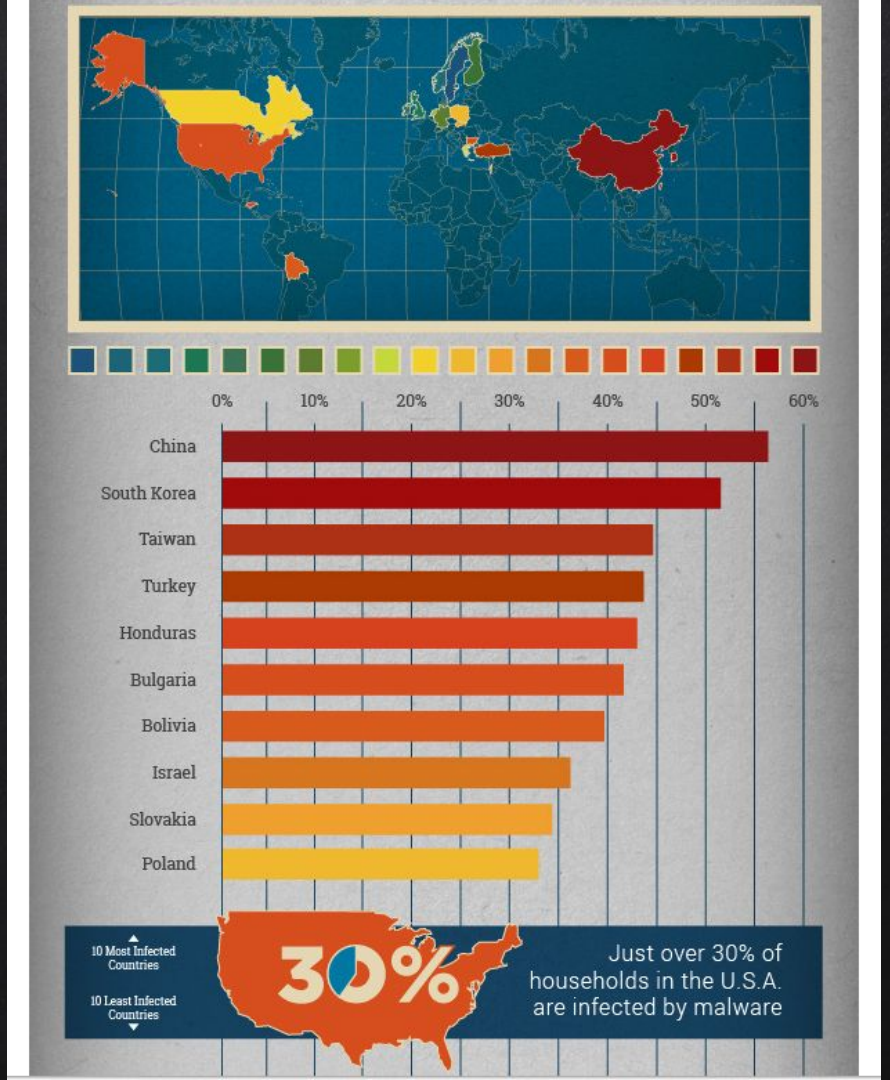
2004: average time for a new computer to get infected was 4 minutes



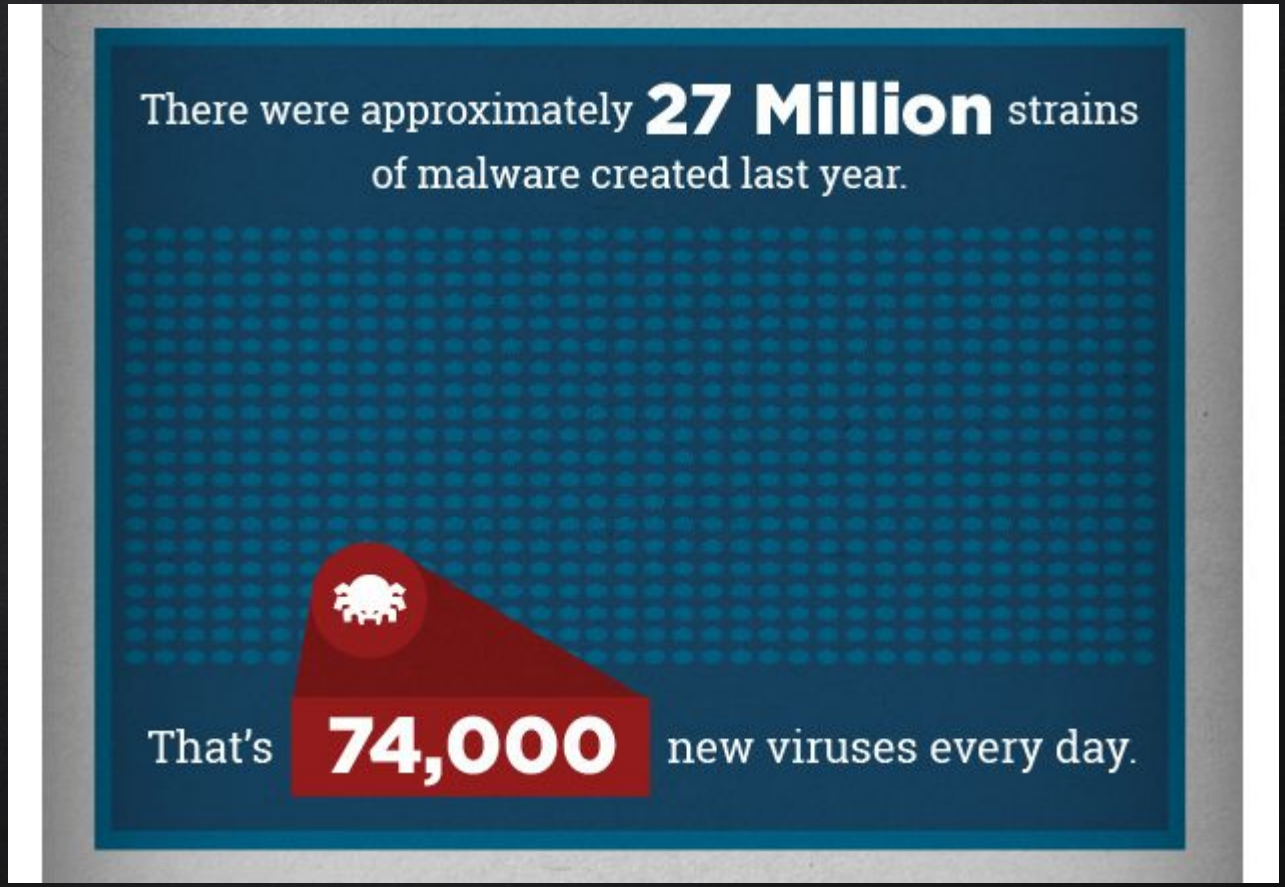
https://blogs.technet.microsoft.com/mmpc/2013/10/29/new-infection-rate-data-for-unprotected-computers/



http://anti-virus-software-review.toptenreviews.com/how-infected-are-we.html



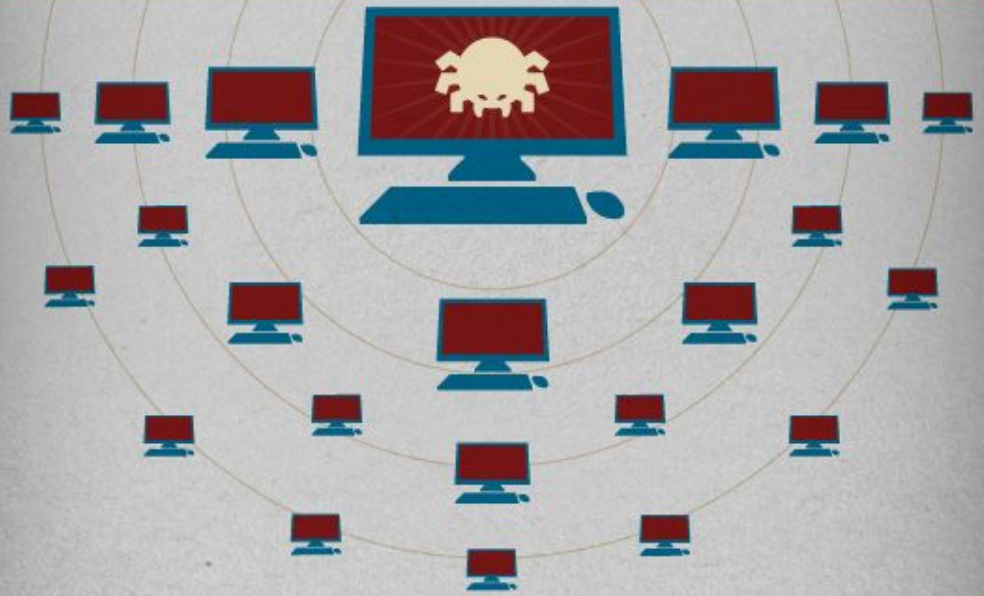
http://anti-virus-software-review.toptenreviews.com/how-infected-are-we.html



http://anti-virus-software-review.toptenreviews.com/how-infected-are-we.html

The most *Prolific* virus of all time

Conficker (also known as Downup, Downadup and Kido) is a computer worm that targets flaws in the Windows operating system to spread across system networks while forming its own network of auto-acting malware. It is known to be unusually difficult to counter. The Conficker infected millions of computers across 200 countries including everything from home personal computers to business and government networks. It is the largest known computer worm infection on record.



http://anti-virus-software-review.toptenreviews.com/how-infected-are-we.html

Computer Virus

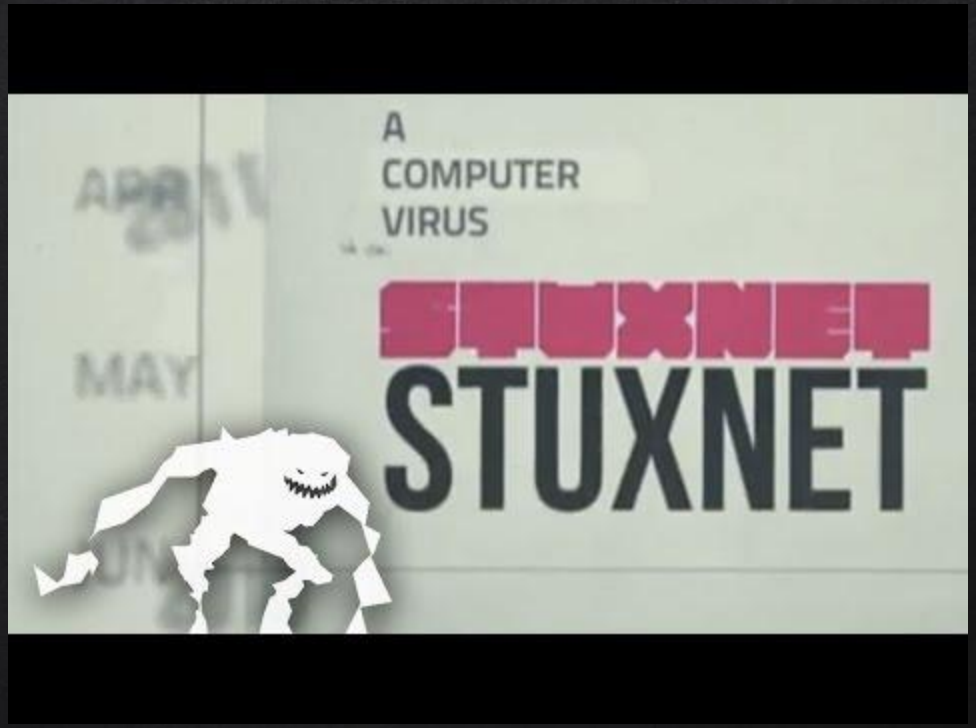
Sometimes used as a term for any malware.

A virus is a computer program that can copy itself to infect another machine:

- Often copied along with a host file
- Modern viruses often use macro languages in Excel and Word

Trojan Horse

- A trojan horse is a software program that appears useful but contains malware: some look like anti-virus programs
- Does not replicate itself: depends on users



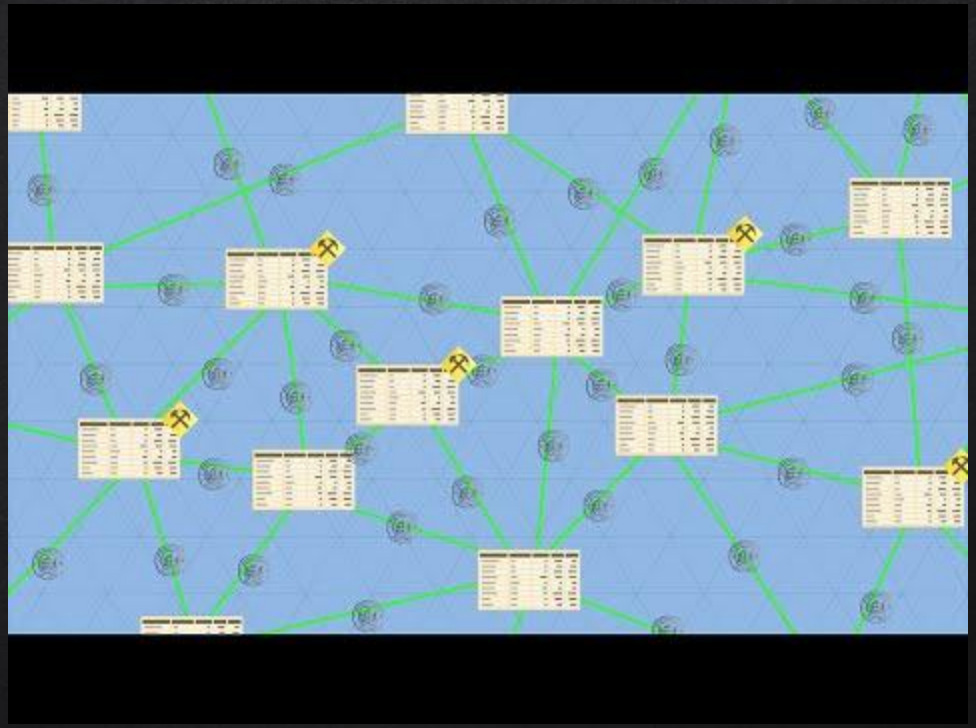
https://www.youtube.com/watch?v=7g0pi4J8auQ

Worm

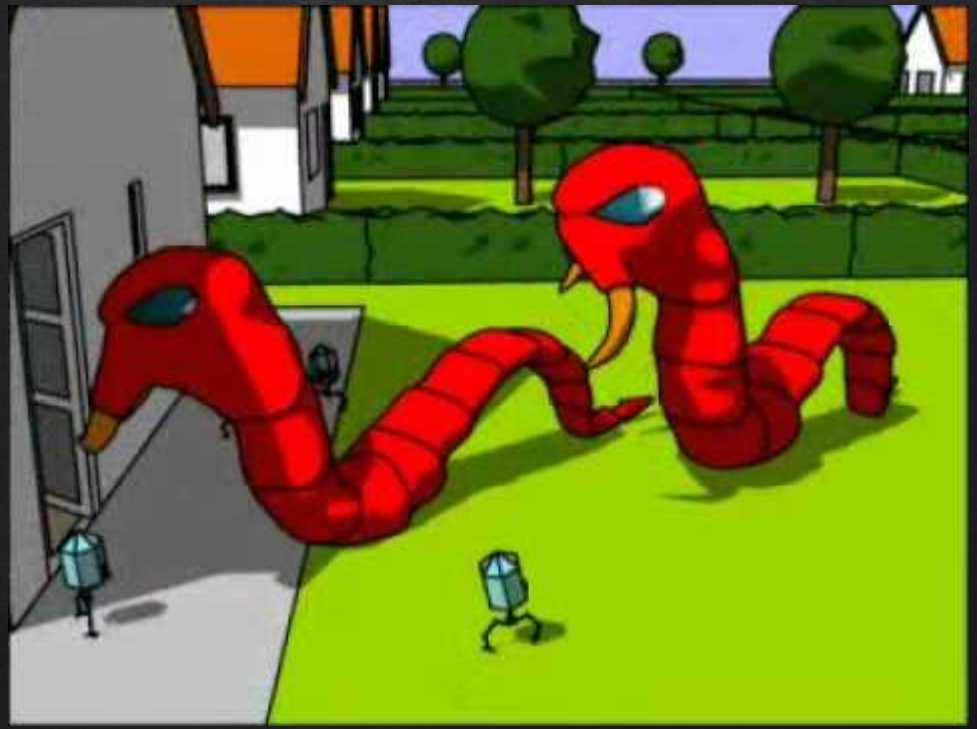
- A worm is a type of virus capable of replicating w/o human help or host file
- Might carry more dangerous programs
  - Crypto extortion: encrypt your hard drive and extort money to decrypt it
- Stuxnet
  - Computer worm found in 2010
  - Attacks industrial equipment
    - Some believe it was written to target Iranian nuclear enrichment capabilities

Rootkits and backdoors

- Backdoors compromise computer to allow further access
  - Bypasses normal authentication
  - Some large-systems have backdoors installed by original programmers
  - Speculations that compilers could install backdoors by recognizing code
- Rootkits bypass normal login and also hide malicious activities
  - Sony music installed rootkits on computers in an effort to thwart piracy (2005)



https://www.youtube.com/watch?v=YIVAIuSL9SU&feature=youtu.be



https://www.youtube.com/watch?v=c34QwtYI40g&ebc=ANyPxKrQcDOYHVwXUsY8vxWe26XxmUcREmLRlWPiU24nVe6341B7q_jVcxTopAjRrMbW_rsDCf7vDp79sxJLR5yVvuVvIP__nw

Protection

- Firewall
  - Prevents unauthorized communications
  - Keeps viruses from spreading
- Anti-virus
  - Searches files, messages from known viruses
- Web browsers
  - Maintain lists of phishing and malware sites
- Spam filters
  - Look for word patterns

Ongoing Battle

- Attacks and protection get more sophisticated
- Keeping a machine updated is important
  - Other programs have vulnerabilities as well: Acrobat, browsers
- Use strong passwords
- Don't use a personal machine password for some shopping site
- Backup data
  - Do a clean OS install

THANKS!

Any questions?

You can find me at
beiwang@sci.utah.edu

http://www.sci.utah.edu/~beiwang/teaching/cs1060.html

Credits

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival
- Photographs by Unsplash