Cyber Security:

Game of Threats

Presented by:

Dawood Sajjadi

Ph.D. Candidate in Computer Science, University of Victoria, BC

February 28th 2017, Victoria Computer Club, Victoria, BC

sajjadi@uvic.ca

UVic Speakers Bureau

The culture of the original Internet was **one of trust**.

- Leonard Kleinrock

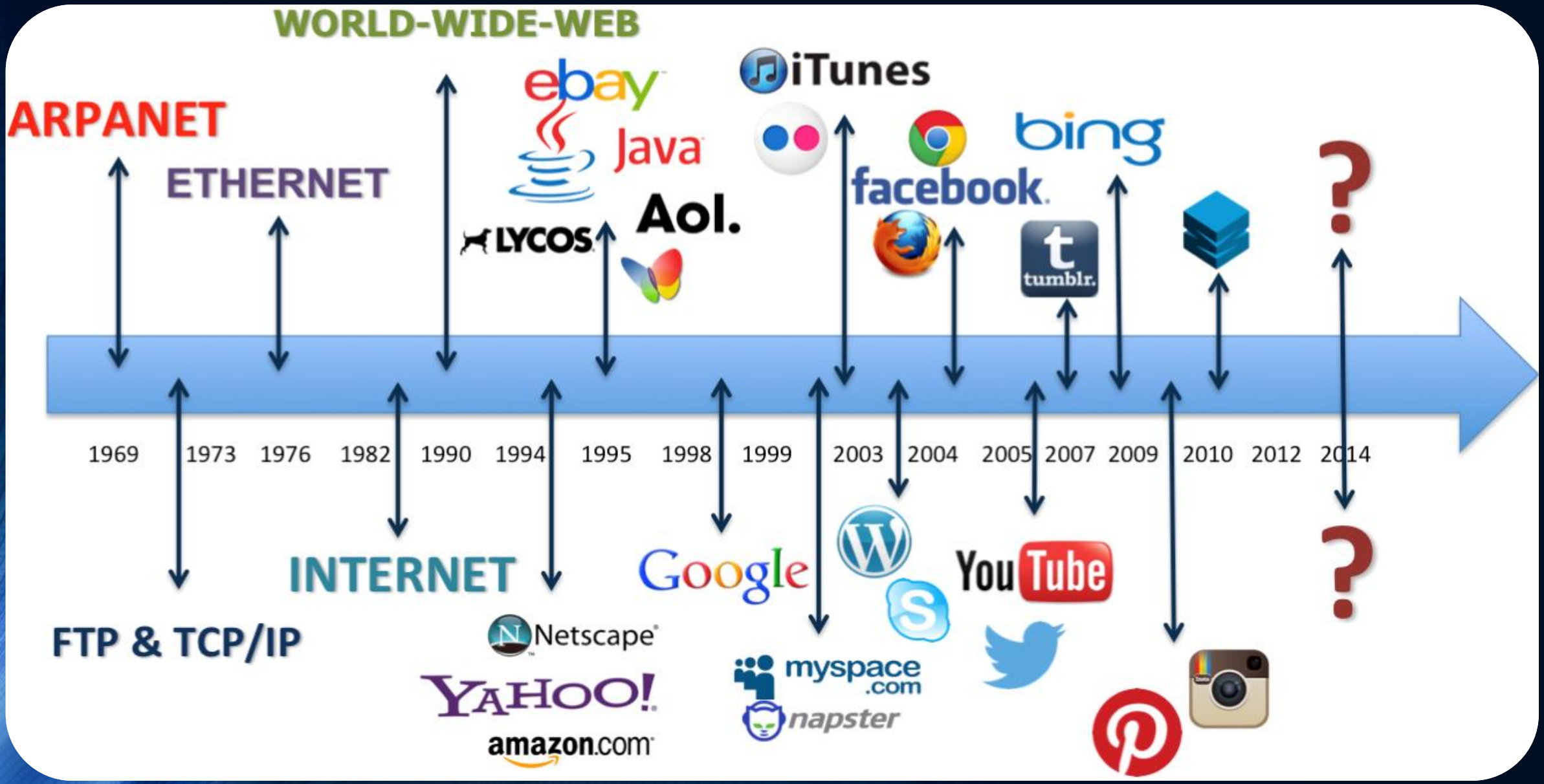
ACM Mobicom 2016, NYC

October 29th, **1969,** 10:30 pm

The first message transferred over the **ARPANET**

UCLA → Stanford

A Brief History of Internet



How the Internet Looks Like?

Public Internet

Private Internet

TorProject.org

SURFACE WEB

Google

Bing

Wikipedia

DEEP WEB

Academic Information

Medical Records

Legal Documents

Scientific Reports

Subscription Information

Contains 90% of the information on the Internet, but is not accessible by Surface Web crawlers.

Social Media

Multilingual Databases

Financial Records

Government Resources

Competitor Websites

Organization-specific Repositories

(DARK WEB)

A part of the Deep Web accessible only through certain browsers such as Tor designed to ensure anonymity. ***Deep Web Technologies has zero involvement with the Dark Web.***

Illegal Information

TOR-Encrypted sites

Political Protests

Drug Trafficking sites

Private Communications

Social Engineering Fraud (SEF)

Pretexting **Phishing**

IVR or phone phishing

Baiting **Tailgating**

Scams **Diversion theft**

$2.3 billion from **17,642** victims in at least **79** countries

through Business Email Compromise (BEC)

from **October 2013** through **February 2016**.

Source: FBI, http://www.securityweek.ca/

Playing Video 1

Phishing

How it works?

It looks like the real website!

2. The link in the email re-directs the victim to a **fake** website.

3. All login information will be sent to the hacker.

1. Hacker sends a fake email to the victim

Over **Half a Billion** Personal Information Records Stolen or Lost in **2015**

Phishing

Email Phishing Rate

2013	1 in 392
2014	1 in 965
2015	1 in 1,846

FBI: **$2.3 Billion** Lost to CEO Email Scams

Don’t get caught by phishers

Playing Video 2

Credit Card Security

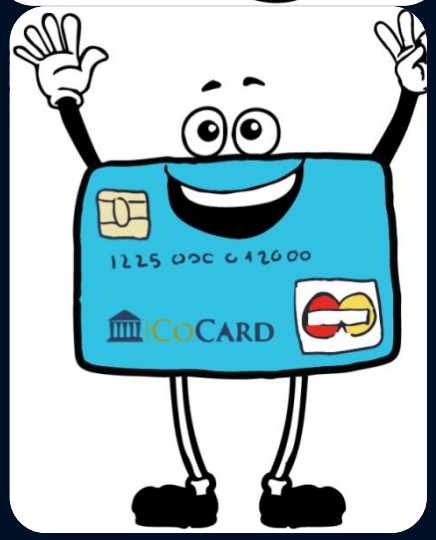
PacSafe RFID Anti-Theft

Playing Video 3

ATM Skimming

Playing Video 4

PIN Code Theft



Playing Video 5

Online Shopping

1. Harden your computer.
2. Do not shop while using public PCs.
3. Do not shop while using public Wi-Fi.
4. Avoid clicking on links from email ads.
5. Shop on secure websites & connections.
6. Use credit instead of debit cards.
7. Enable fraud notifications and other alerts.

Online Shopping

Use **Secure** Wi-Fi

Playing Video 6

Ransomwares

Damages caused by Ransomware in **2015**

$ 325 million

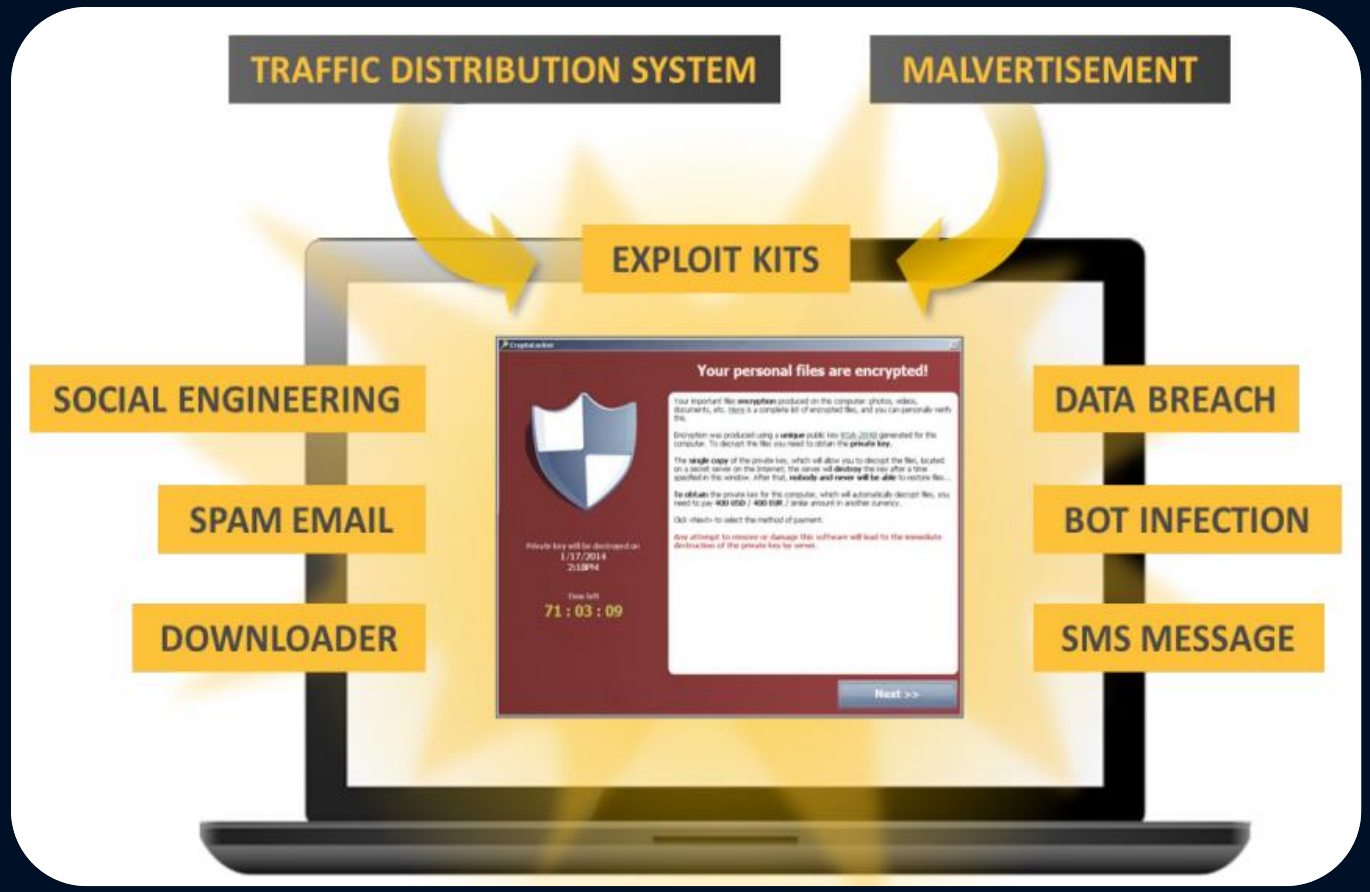
In a one-month study

68,000

Computer were infected

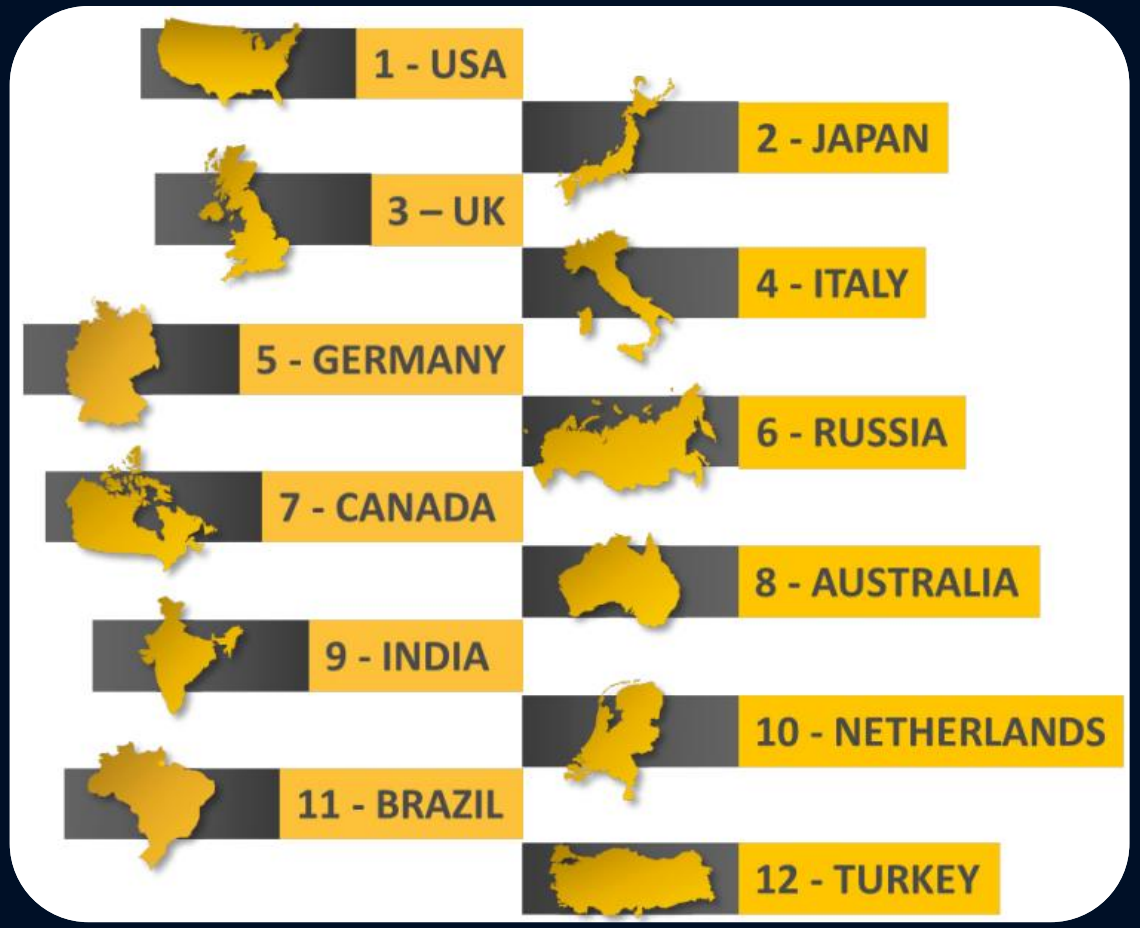
Source: http://www.netcetera.ca/

Ransomwares



Routes for ransomware to arrive on a computer

Top countries impacted by binary-based ransomware

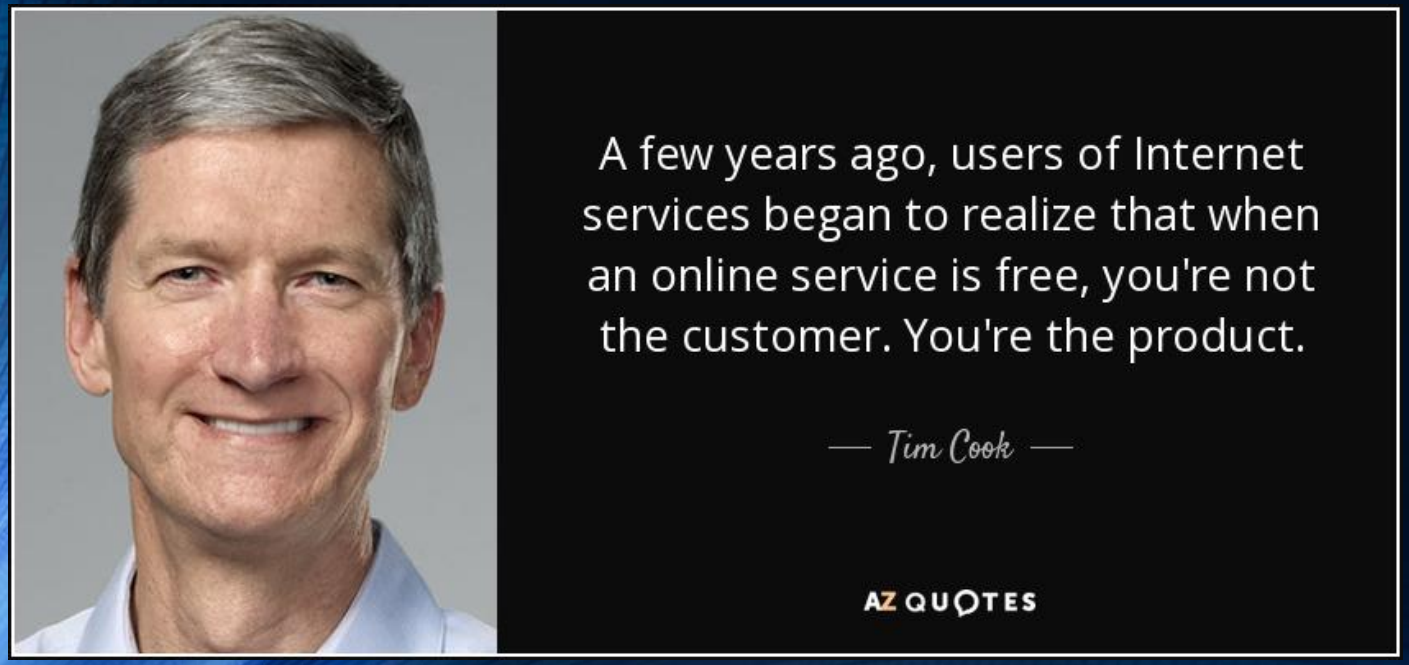


Social Networks

Think, before you Post.

Watch, before click any Link.

Don’t accept the friendship request of the people that you don’t know



Social Networks

Playing Video 7

Security on Home/Mobile Devices

Use Security Software.

Keep updating your
Anti-virus, **Software** & **Applications**

Security on Home/Mobile Devices

Look for **Legitimate** Apps

Strong Password Protection

Never Share your passwords

Be Smart about passwords

In a Nutshell

Nobody is Completely Safe on **the Internet**.

BUT

We can make it harder for the intruders to get what they want…

& take it serious…

Thank You

Q & A

Web Security

Dark Web

Malwares

Social Engineering

Social Networks

ATM Skimmers

Ransomwares

Phishing

Credit Card Security

Pin Code Theft

Mobile Security