Appendix

CYBER TIMELINE

When anyone thinks about a recent event or tries to remember a historical incident in context, it is very difficult. We have provided this timeline of some of the significant events that have shaped or impacted cybersecurity to help you understand the relationship of what has happened.

- 1912 Radio Act Regulates private communications
- 1945 Rear Admiral Grace Murray Hopper discovers a moth trapped between relays in a Navy computer. She calls it a "bug," a term used since the late nineteenth century to refer to problems with electrical devices.
- 1946 ENIAC was the first general-purpose computer
- 1960 AT&T introduces its Dataphone, the first commercial modem
- 1962 First computer game invented—Spacewar Computer Game
- 1965 Established NIST responsibility for IT standards and technical assistance
- 1969 Department of Defense (DOD) Advanced Research Projects Agency (DARPA) established Advanced Research Projects Agency Network (ARPANET)
- 1970 Creeper worm and reaper virus are seen on ARPANET. (Reaper is created to delete creeper)
- 1971 The Floppy disk is created. This is the first instance of removable media
- 1972 Draper discovers a toy whistle from Cap'n Crunch could emit a 2600-Hz tone to get free phone calls from pay phones
- 1973 First encrypted message sent over ARPANET
- 1974 Institute of Electrical and Electronic Engineers (IEEE) proposed TCP/IP
- 1974 Rabbit virus was seen outside of the closed ARPANET
- 1977 PC Modem developed
- 1977 Data Encryption Standard (DES) encryption program is approved by National Bureau of Standards
- 1978 First SPAM e-mail sent (sent to 393 recipients on ARPANET)—becomes rampant by mid-1990s
- 1981 Chaos Computer Club (CCC) founded. It was the first hacker organization, striving for "freedom of information"
- 1981 First IBM PCs sold
- 1982 The 414 group broke into 60 computer systems and the incident appeared as the cover story of Newsweek with the title "Beware, Hackers at play"
- 1982 Movie TRON came out
- 1983 Internet Protocol Suite (TCP/IP) became standardized, and became the only approved protocol on ARPANET. The U.S. Military portion of ARPANET broke off to

become MILNET (later known as NIPRNET). ARPANET with MILNET was foundation for what became the Internet.

- 1983 The movie WarGames introduces the wider public to the phenomenon of hacking
- 1983 The FBI busts the "414s," a group of young hackers who break into several U.S. government networks, in some cases using only an Apple II+ computer and a modem.
- 1984 Computer Fraud and Abuse Act passed
- 1984 Domain Name System (DNS) was initiated
- 1984 The hacker magazine 2600 begins regular publication
- 1985 Elk Cloner was the first large-scale virus outbreak
- 1986 The first PC virus, "The Brain," is released by programmers in Pakistan
- 1986 Electronic Communications Privacy Act passed
- 1987 The number of network hosts reaches 10,000
- 1987 Computer Security Act passed
- 1988 Robert Morris created the first "worm"
- 1989 The number of network hosts surpasses 100,000
- 1989 Clifford Stoll discovers USSR cyber spies on Berkeley mainframe—becomes book "The Cuckoo's Egg"
- 1990 Secret Service launches Operation Sun Devil to hunt down hackers
- 1991 First digital cell phones sold
- 1992 The number of network hosts surpasses 1,000,000
- 1992 The first SMS (text message) is sent. It uses the control channel of a cellular connection
- 1992 Movie Sneakers came out
- 1993 The first DEFCON hacking conference takes place in Las Vegas
- 1994 First publicly known major cybercrime—Russian Vladimir Levin leads a group of hackers that steals millions of dollars from Citibank though its dial-up wire transfer service
- 1995 Time magazine has cover on "Cyber War"
- 1995 Hacker with handle "Hobbit" released Netcat (army knife of hacker tools)
- 1995 Kevin Mitnick arrested and eventually gets a five-and-a-half-year prison term
- 1996 The number of network hosts surpasses 10,000,000
- 1996 President Clinton Executive Order 13010, President's Commission on Critical Infrastructure Protection (PCCIP). "Examine physical and cyber threats to the critical infrastructures"
- 1996 Term Phishing Attacks becomes common as identity theft becomes bigger issue
- 1996 Health Insurance Portability and Accountability Act passed
- 1997 Nmap published as an article in Phrack magazine with source-code
- 1997 Eligible Receiver exercise tests the government's readiness for cyber attacks, results immediately classified
- 1998 Google search engine established
- 1998 Solar Sunrise incident hits the news as Pentagon gets hacked, ends up being two kids from California mentored by Israel hacker
- 1998 Martin Roesch starts open source called Snort—free Intrusion Detection System
- Wireshark (formally Ethereal) open source project starts—free sniffer/protocol analyzer

- 1998 Renaud Deraison started open source project called Nessus—free security scanner
- 1998 Digital Millennium Copyright Act (DMCA)
- 1998 Internet Corporation for Assigned Names and Numbers (ICANN) stood up
- 1998 Moonlight Maze incident DoD found intrusion from systems in Soviet Union but the sponsor of the attacks is unknown and Russia denies any involvement
- 1999 60 Minutes starts regular stories covering "Waging War With Computers"
- 1999 DES encryption broken due to small 56-bit key size
- 1999 Melissa virus unleashed; the first self-replicating worm
- 1999 Hackers in Serbia attack NATO systems in retaliation for NATO's military intervention in Kosovo
- 1999 Gramm Leach Bliley Act passed
- 1999 NATO accidentally bombs the Chinese embassy in Belgrade, spawning a wave of cyber attacks from China against U.S. government Web sites
- 2000 The number of network hosts surpasses 100,000,000
- 2000 Y2K bug hype ends up with little impact
- 2000 Mafiaboy shuts down major commercial Web sites
- 2000 First Top Officials (TOPOFF) exercise
- 2001 NIMDA (Admin spelled backward) hit
- 2001 USA Patriot Act passed
- 2001 Code Red worm hit—designed to conduct DDoS against White House
- 2001 Kournikova virus hit, malware embedded in an image
- 2001 AES, Advanced Encryption Standard, is published, and the standard becomes effective in 2002. Its key sizes range from 128-bits up.
- 2002 Bill Gates decrees that Microsoft will secure its products and services, and kicks off a massive internal training and quality control campaign
- 2002 Federal Information Security Management Act passed
- 2002 Solo (Gary McKinnon) hacked into government computers looking for UFOs
- 2002 Sarbanes–Oxley Act passed
- 2003 Titan Rain attacks identified, believed to be from China; it spawns new term "Advance Persistent Threat"
- 2003 SQL Slammer worm reached its peak within three minutes
- 2003 Metasploit Framework project started
- 2004 ILOVEYOU, aka LoveLetter, e-mail attack hit
- 2006 MySpace becomes main social networking site
- 2006 First Cyber Storm Exercise
- 2006 BackTrack, a forensics/penetration-testing-focused Knoppix build was released based on WHAX/Whoppix and Auditor Security Collection
- 2007 The number of network hosts surpasses 500,000,000
- 2007 Hackers believed to be linked to the Russian government bring down the Web sites of Estonia's parliament, banks, ministries, newspapers, and broadcasters— NATO reacts
- 2007 Storm Worm (one of the first BotNets) began infecting thousands of (mostly private) computers in Europe and the United States
- 2007 British Security Service, French Prime Minister's Office, and Office of German Chancellor all complained to China about intrusion on their government networks

- 2008 Facebook takes over from MySpace as main social networking site
- 2008 Operation Buckshot Yankee in reaction to Agent.btz forcing U.S. military to stop using thumb drives
- 2008 Databases of both the Republican and Democratic presidential campaigns were hacked and downloaded by unknown foreign intruders
- 2008 The networks of several Congressional offices were hacked by unknown foreign intruders (some incidents involved offices with an interest in human rights or Tibet)
- 2008 Cyber attackers hijack government and commercial Web sites in Georgia during a military conflict with Russia
- 2008 FBI conducts Dark Market sting on cyber identity theft ring
- 2009 Twitter Revolution occurs in Iran over election unrest
- 2009 FAA computer systems were hacked
- 2009 Ghost Net report released by Canadian researchers who found espionage tools they attributed to China implanted on government networks of 103 countries
- 2009 Reports in the press suggest that the plans for Marine Corps 1, the new presidential helicopter, were found on a file-sharing network in Iran
- 2009 Conficker worm infiltrated millions of PCs worldwide including many government-level top-security computer networks
- 2009 Reports reveal that hackers downloaded data about the F-35 Joint Strike Fighter, a multibillion-dollar high-tech fighter jet
- 2009 Zeus banking Trojan Horse released
- 2010 TRON Legacy hits theaters (28 years after original movie)
- 2010 First Cyber Shockwave exercise
- 2010 Operation Aurora in which Google publicly reveals being hacked (China blamed)
- 2010 October U.S. Cyber Command begins overseeing the protection of military networks from cyber threats
- 2010 WikiLeaks released U.S. embassy cables, Anonymous attacks MasterCard for stopping accepting donations for them
- 2010 Stuxnet worm attacks SCADA devices in Iran causing physical damage, eventually reveled as part of operation code-named Olympic Games by the United States and Israel in the book "Confront and Conceal Obama's Secret Wars and Surprising Use of American Power"
- 2010 China Redirect of 15% of internet traffic through its country (claimed it was an accident), this showed the DNS weaknesses
- 2011 The number of network hosts surpasses 883,000,000
- 2011 RSA attack allowed their security tokens to be compromised (used by Gov, DoD contractors, and financial organizations to name a few), China suspected
- 2011 Duqu (son of Stuxnet) released
- 2011 Tehran Bomb—Comodo Certificate Authority (CA) compromised allowing access to e-mail accounts of Iranian citizens and showing weakness of CAs
- 2011 saw an spike of Android threats as the phones started to outsell the iPhone
- 2011 Global Energy Cyberattacks "Night Dragon" report released showing systematic economic espionage against energy sector companies, China suspected
- 2011 Operation Shady RAT Report
- 2012 Anonymous attacks Sony multiple times causing impact on gamers
- 2012 Stop Online Piracy Act (SOPA) defeated when major vendors held webpage blackout

- 2012 Mac Defender and Flashback malware attacks Apple systems
- 2012 Flame and Gauss state-sponsored cyber exploit discovered—tied to Stuxtnet
- 2012 Thunderstruck Atomic Energy Organization of Iran was attacked. The attackers played the AC/DC Thunderstruck song
- 2012 LinkedIn password leaks impact over 6 million users
- 2012 Shamoon attack against Saudi Aramco, one of the world's largest oil conglomerates, resulted in more than 30,000 computer systems wiped of all data
- 2013 President Obama signed Executive Order for Improving Critical Infrastructure Cybersecurity
- 2013 The Spamhaus Project—CyberBunker feud
- 2013 Mandiant Intelligence Center Report—APT1 Exposing One of China's Cyber Espionage Units
- 2013 South Korean banks and media report large number of computer network crashes causing speculation of North Korea cyberattack
- 2013 Kaspersky Lab releases reports on "Operation Red October" and "Operation NetTraveler"