Computer and Operating System History

Lecture 1

Instructor : Joohan Lee
jlee@cs.ucf.edu

http://www.cs.ucf.edu/~jlee

School of Computer Science
University of Central Florida

Relevant History of Computer

- 1949: Claude Shannon
  - Lead to the development of modern block cipher
  - Diffusion to dissipate statistical structure of plaintext over bulk of ciphertext confusion and confusion to hide the relationship between ciphertext and key
- Late 1950's: Memory Protection Hardware
  - Partition based system uses special registers to define partitions of memory and provides protection against illegal accesses to them
- 1960: DEC introduces the PDP-1, the first commercial computer with a monitor and keyboard input
- 1960: Virtual Memory
  - Protect each virtual memory object separately

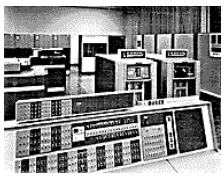
Relevant History of Computer

- 1962: File Access Control in Time-sharing System
  - MIT's Compatible Time Sharing System
  - The University of Cambridge's Multiple Access System

- 1964: Douglas Engelbart invents the mouse
- Mid 1960s: System Calls
  - The first operating system to introduce system calls was University of Machester's Atlas I Supervisor

Relevant History of Computer

- Mid 1960's: IBM 7094 & CTSS
  One of the biggest, fastest computers available, able to add floating numbers at a speed of about 0.35 MIPS. It had 32K 36-bit words of memory. They cost about $3.5 million.



- 1961: Compatible Time Sharing System (CTSS) was developed at the MIT Computation Center by a team led by Fernando J. Corbato. CTSS was first demonstrated in 1961 on the IBM 709, swapping to tape. In its mature form, CTSS ran on a modified IBM 7094 with a second 32K-word bank of memory, using two IBM 2301 drums for swapping and provided remote access to up to 30 users via an IBM 7750 communications controller connected to dialup modems.

Relevant History of Computer

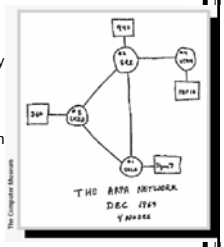
- 1962: Project Multiple Access Computer (MAC) at MIT started
  Led to the development of Multics OS funded by ARPA.
  Idea of virtual memory segmentation. IBM wasn't interested in the idea of segmentation and paging. GE supported the project that would become GE-645.
- 1964: PL/1 is chosen as a programming language
- 1965: Bell Lab, GE, and MIT started development of Multics together
- Mid 1968: Multics Security Kernel
  - Identified a small kernel of system calls which, if correct, would guarantee that all security policies of the system would be followed.
  - Mandatory access control and avoid buffer overflow
- 1969: Multics Project canceled

Relevant History of Computer

- 1973: Commercial Multics OS
  - Honeywell (who bought GE computer business) 6180 processors were about 1 MIPS each. A two-CPU system with 768KB of memory, 8MB of bulk store, 1.6GB of disk, 8 tape drives, and two DN355s, had a purchase price of about $7 million.
- 1970's and early 1980's:
  - Multics used by Ford, General Motors, Air Force, and in Europ
- 1985
  - Multics development was canceled by Honeywell in July 1985

Relevant History of Computer

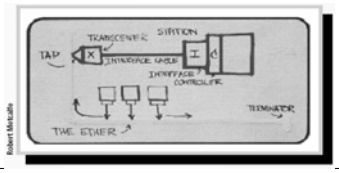
- 1969: The US department of Defense commissions APANET for research networking, and the first four nodes become operational at UCLA, UC Santa Barbara, SRI, and the University of Utha.
- 1970: Unix is developed at Bell Labs by Dennis Ritchie and Kenneth Thomson. First, it was run on DEC's PDP-7



- 1971: The first UNIX Programmer's Manual published by Bell Lab

Relevant History of Computer

- 1971: Ray Tomlinson of Bolt Beranek and Newman sends the first network e-mail message.
- 1972: Dennish Ritchie develops C at Bell Labs.
- 1973: Robert Metcalfe writes a memo on "Ether Acquisition" which describes the Ethernet as a modified Alohanet.



Relevant History of Computer

- 1973: UNIX version 4
  - First several versions were internal to Bell Lab
  - Included C compiler and the OS was rewritten in C
  - Bell Lab started providing UNIX to universities (UC Berkeley) for educational and research purpose. It did not advertise or market the system and did not support its release.
- 1978: VAX and UNIX/32V
  - UNIX was ported to the DEC VAX machine (first port to 32 bit machine)
  - Evolved to 3BDS
- 1978: Commercial Berkeley Software Distribution (BSD)
  - BSD was developed by a group of graduate students (Bill Joy and Chuck Harley)
  - BSD version 2 sold at $50 per license
- 1979: UNIX version 7
  - First truly portable UNIX and ran on PDP-11
- 1979: 3BSD
  - Supports page based virtual memory system for VAX

Relevant History of Computer

- 1975: The first PC, an Altair 8800, available as a kit, appears on the cover of Popular Electronics in January.

Relevant History of Computer

- 1975: UUCP (Unix-Unix Copy Protocol)
  - A computer program and protocol allowing remote execution of commands and transfer of files, emails, and between UNIX computers.
  - It also enabled attackers to erase or overwrite configuration files if the software were not correctly configured.
- 1976: First public-key type scheme proposed by Diffie & Hellman
  - Enabled two users to exchange a key securely that can then be used for subsequent encryption of messages
  - Also provided the first technical mechanism for digital signatures that cannot be repudiated.
- 1977: RSA public cryptography system
  - By Rivest, Shamir & Adleman of MIT

Relevant History of Computer

- 1976: Steve Jobs and Steve Wozniak build the Apple I, which consists mostly of a circuit board.
- 1977: Bill Gates and Paul Allen found Microsoft setting up shop first in Albuquerque, New Mexico.

Relevant History of Computer

- 1977: Data Encryption Standards (DES)
  - A symmetric block cipher adopted by NIST
  - 64bit block and 56 bit key
- 1978: First Vulnerability Study of Passwords
  - Password guessing is far more effective than deciphering password images
- 1980: The Osborn 1 "portable" computer weighs 24 pounds and is the size of a small suit case
- 1983: Domain Naming Service of the Internet
  - Vulnerable to spoofing
- 1983: Completion of the TCP/IP switchover marks the creation of the global Internet.

Relevant History of Computer

- System V by AT&T UNIX System Laboratories
  - System V in 1983
  - System V Release 2 in 1984
  - System V Release 3 in 1987
- 1982: Sun founded
  - Bill Joy left Berkeley to cofound Sun Microsystems
  - Released SunOS, a variant based on 4.2 BSD
  - SVR4-based variant called Solaris
- 1980's : a number of UNIX commercial offerings
  - AIX from IBM, HP-UX from HP, ULTRIX/Digital UNIX from DEC
- Mid 1980's : Mach
  - UNIX was popular because it's simple and small
  - Carnegie Mellon Univ. began working on the a new OS called Mach based on microkernel architecture

Relevant History of Computer

- 1987 : SVR4 – System V Release 4
  - AT&T and SUN collaborated to develop SVR4
- 1988 : Open Software Foundation (OSF) vs Unix International (UI)
  - Alliance of Digital, IBM, HP, Apollo, and other, OSF, was formed against SUN and AT&T trying to develop UNIX that is free of AT&T licenses
  - AT&T, SUN, and other vendors form UI
- 1989 : OSF
  - OSF released a graphical user interface called Motif and the initial version of its OS, called OSF/1
  - OSF/1 was based on Mach 2.5 and compatible with 4.3 BSD
- 1989 : SVR4 – System V Release 4
  - SVR4 released (Solaris)
- 1991 : Novell (Netware)
  - Novell purchased part of Unix System Laboratories from AT&T and formed a joint venture called Univel
  - Developed PC version of SVR4 integrated with UnixWare

Relevant History of Computer

- 1993:
  - AT&T sold the rest of its interest in USL to Novell
- 1993: with 4.4 BSD, UC Berkeley stopped UNIX development
  - Berkeley Software Design Inc. (BSDI) was formed to commercialize and market BSD 4.4
  - BSDI claimed that the source code had replaced with new code developed at Berkeley and free of AT&T licenses
  - Lawsuit against BSDI by AT&T and counter lawsuit by BSDI. In 1994, all parties dropped their claims.
- 1994:
  - Sun Microsystems bought the right to use SVR4 code from Novell freeing themselves of royalty
  - Sun's SVR4 based release is called Solaris

Relevant History of Computer

- 1988: Graduate student Robert Morris Jr. reveals the need for greater network security by releasing a worm program into the Internet on November 2
- 1988: Kerberos
  - Centralized private-key third-party authentication in a distributed network
- 1989: Pretty Good Privacy (PGP)
  - Digital certificates without a central authority

Relevant History of Computer

- 1989: Tim Berners-Lee proposes the World Wide Web project to CERN (European Council for Nuclear Research)
- 1990: Berners-Lee writes the initial prototype for the World Wide Web, which uses his other creations: URLs, HTML, and HTTP.
- 1992: After generating great concern in early March, the Michelangelo virus results in little actual damage.

From: torvalds@klaava.Helsinki.FI (Linus Benedict Torvalds)
Newsgroups: comp.os.minix
Subject: What would you like to see most in minix?
Summary: small poll for my new operating system
Message-ID: <1991Aug25.205708.9541@klaava.Helsinki.FI>
Date: 25 Aug 91 20:57:08 GMT
Organization: University of Helsinki

Hello everybody out there using minix -
I'm doing a (free) operating system (just a hobby, won't be big and professional like gnu) for 386(486) AT clones. This has been brewing since april, and is starting to get ready. I'd like any feedback on things people like/dislike in minix, as my OS resembles it somewhat (same physical layout of the file-system (due to practical reasons) among other things).
I've currently ported bash(1.08) and gcc(1.40), and things seem to work. This implies that I'll get something practical within a few months, and I'd like to know what features most people would want. Any suggestions are welcome, but I won't promise I'll implement them :-)
Linus (torvalds@kruuna.helsinki.fi)
PS. Yes - it's free of any minix code, and it has a multi-threaded fs. It is NOT portable (uses 386 task switching etc), and it probably never will support anything other than AT-harddisks, as that's all I have :-(.

1991: Linus Torvalds posted an article in comp.os.minix saying his new experimental kernel (Linux)was running bash and gcc, and he was going to post the source code soon. Though it's impossible to pick a given day that Linux started, this is generally accepted as when the project reached critical mass. This was also the message that got others besides Linus interested in the project.

Relevant History of Computer

1993: Students and staff at the University of Illinois' National Center for Supercomputing Applications create a graphical user interface for Internet navigation called NCSA Mosaic.

1994: In April, Jim Clark and Marc Andreesen found Netscape Communications

1995: The Java programming language, unveiled in May, enables platform independent application development. "Duke" is the first applet.

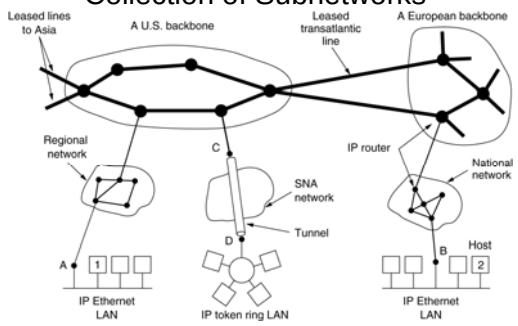
Relevant History of Computer

- 1995: SHA-1 Secure Hash Function by NIST
  - Input message : maximum 2^{64} bits
  - Output hash code : 160 bits
  - The input is processed in 512-bit blocks
- DES crackers
  - In 1997, RSA Data Security Inc. issued its first "DES challenge"
  - Jan. 1997: 96 days to crack by Rocke Verser
  - Feb. 1998: 56 hours using a machine valued less than $250,000 by Distributed.net and ETF(Electronic Frontier Foundation)
  - Jan. 1999: less than 24 hours by the same team
- 2000: Advanced Encryption Standard (AES)
  - NIST selected Rijndael for AES
  - 128 bit block size and 128, 196, and 256 bit key sizes

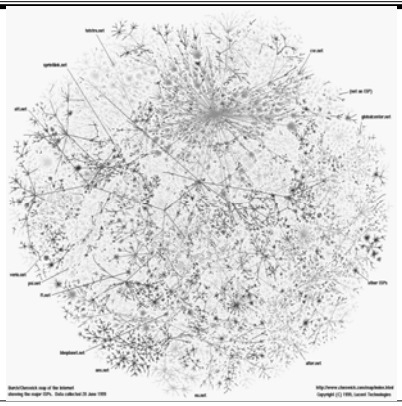
Basic Infrastructure

- 15 years ago there was no commercial use of the net
  - 14 years ago, fewer than 100,000 systems
  - 231 systems in 1981
- The Internet Today
  - Millions of systems on all seven continents
  - In excess of 400 million users have access
  - 220 countries around the world have registered for access
  - Population doubling in approximately 10 months for last 11 years
  - Volume of traffic doubling approximately every 90 days
- Explosion of Storage

Collection of Subnetworks



The Internet is an interconnected collection of many networks.



June 28 1999

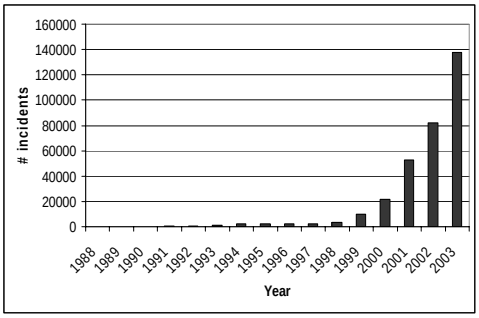
Future Environment

- World-wide
- High speed networking
- Cheap, ubiquitous computing
- Widely-deployed encryption
- Truly mobile computing
- Many embedded systems connected
- Billions of users

State of Security: Poor

- Examples abound:
  - Feb 2000, Denial of Service against eBay, Yahoo, Amazon, etc.
  - CERT reporting 82094 incidents in 2002 (833% increase from 1999)
  - In 2003, first three quarter statistics already outnumbered last year's number of incidents by CERT
- FBI figures
  - Fewer than 20% sites report no unauthorized use

State of Security: Poor



1988: 6, 1995: 2412, 2003: 137,529

Real Losses

- **The Morris Worm**
  - About 6000 computers were victimized. At the time, this was about ten percent of the Internet.
  - Estimated damage was $98 million
  - This was the first conviction violating the 1986 US Federal Law Computer Fraud and Abuse Act (Title 18). After all of the appeals he was sentenced to three years probation, 400 hours of community service, a fine of $10,050 and the costs of his supervision.
  - Resulted in establishing Computer Emergency Response Team (CERT)

Real Losses

- Brain
  - Took 5 years to do $50 million damage
- Melissa, March 1999
  - Word 97, Word 2000: $300 million in damages
  - Approximately 4 days, 150,000 systems infected
- ILOVEYOU, May 2000
  - Outlook: As much as $10 billion in damages
  - Approximately 24 hours, 500,000 systems infected
- Code Red I
  - IIS flaws, with fixes published months earlier
  - 360,000 systems in 14 hours, several billion in damages
- Sapphire Worm
  - Saturday, January 25 2003
  - Exploit: UDP Buffer Overflow, Microsoft SQL Server (Not malicious)
  - Due to large numbers of scans, large sections of backbone providers shut down
  - Time to 90% infection of vulnerable hosts: 10 Minutes

Real Losses

- Blaster
  - takes advantage of a DCOM RPC vulnerability in newer Microsoft Windows operating systems. If an unpatched system with an open port 135 is attacked, the worm will attempt to install and run msblast.exe
  - MSBlast does not spread via e-mail. Instead, it scans the Internet on port 135 looking for vulnerable computers. When it finds one, it attempts to exploit the DCOM RPC buffer overflow, create a remote root shell on TCP port 4444, then use FTP to download a file called msblast.exe onto the infected computer. MSBlast contains a denial-of-service (DoS) attack aimed at Microsoft's windowsupdate.com. The attack starts on August 15 and continues throughout the end of the year

Real Losses

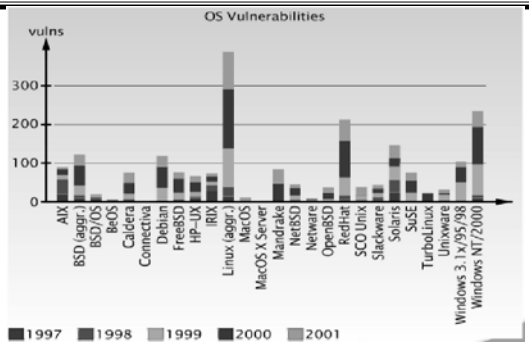
- Sobig.F
  - The fastest virus ever seen
    - Postini (E-mail filtering company) trapped 2.6 million in 24 hours (on average 500,000/day)
    - Clogged corporate e-mail systems on Aug 19 and 20 2003
    - One in every 17 messages contained the Sobig virus--far more then the normal 1-in-275 ratio or 1-in-138 ratio that the previous top threat, Klez.H, had produced (Messagelabs)
  - American Online normally receives about 11 million e-mail messages that bear attachments that need to be checked. On Aug 19 2003, the company took in about 31 million such messages, about 11.5 million of which carried the Sobig.F virus
  - Uses the Network Time Protocol (NTP) to access one of several servers in order to determine the current date and time. If the time returned by the NTP server is between 19:00 and 22:00 UTC+0 on Friday or Sunday, W32/Sobig-F sends a UDP packet to port 8998 of a remote server. This feature could be used to download and run a Trojan or additional worm components. If the date is 10 September 2003 or later the worm stops working

Real Losses

- What's next ?
  - Estimated time for near-total infection: 30 seconds

Magnitude of the Problem

- There is no perfect code
- Assume a conservative rate for serious faults
  - 1 error per 1K LoC in unaudited code (20 pages)
  - 1 error per 5K LoC in examined code (100 pages)
- Kernels
  - OpenBSD 2.6: 1874K lines, implying 375 faults
  - HP/UX: 2341K lines, implying 470 faults
  - Linux 2.2.121: implying 1500 faults
  - Windows 2000: 30million lines, implying 6,000 faults

- About 30% buffer overflows or unchecked data
- Over 90% are coding/design flaws
- Source: Securityfocus.com

More Data

- CERT/CC fielded 21,756 incidents in 2000
  - Growth from 3734 in 1998, 9859 in 1999
  - Doubling annually
- On-going probes (via Intel)
  - 50-60 incidents per day on Internet
  - 10-12 incidents per day on DSL
  - 5-6 incidents per day on dial-up
- Typical User
  - Less than 1 year online
  - No background in computing
  - Has major OS, 1 Ghz machine, but uses only 3 applications
  - Doesn't make backups
  - Online constantly

The world in 2004

- 100,000 computer viruses
  - 99% for one vendor's software
  - New viruses @ more than 1 per hour
- Most common desktop system
  - Almost 100 million LOC, 4 Ghz+
  - 1 security patch announced per day
- Attack over network exceed 10 per hour
- Losses to business and government will exceed $100 billion per year