Risks to the Public in Computers and Related Systems

Peter G. Neumann plus contributors as indicated
SRI International EL-243,
333 Ravenswood Ave.,
Menlo Park CA 94025-3493
(1-650-859-2375; neumann@csl.sri.com)

Opinions expressed are individual rather than organizational, and all of the usual disclaimers apply. To economize on space despite the enormously increasing volume of cases, we tersify many items and include on-line pointers to other items in the on-line Risks Forum, where (S i j:p) denotes *SEN* vol i no j page p (1997 = volume 22), and (R i j) denotes RISKS vol i number j. The RISKS archives are available on ftp.sri.com, cd risks. *SEN* archives are summarized at ftp://ftp.CSL.sri.com/illustrative.PS. Please send RISKS-related items to risks@CSL.sri.com. Read RISKS as a newsgroup (comp.risks), or subscribe via the automated listserv at risks-request@CSL.sri.com. Peter G. Neumann, http://www.csl.sri.com/neumann/).

Internet nameserver problem affects .com and .net

Around 11:30pm EDT on 16 Jul 1997, Network Solutions Inc attempted to run the autogeneration of the top-level domain zone files, which resulted from the failure of a program converting Ingres data into the DNS tables, corrupting the .COM and .NET files. Quality-assurance alarms were evidently ignored and the corrupted files were released at 2:30am EDT on 17 Jul – with widespread effects. Other servers copied the corrupted files from the NSI version. Corrected files were issued four hours later, although there were various lingering problems after that.

Programmed tunnel-digging robot runs a-muck (Robert J. Sandler)

Anthony Catania got suspicious when his floor started to shake. For weeks, sewer diggers had been tearing up the street in front of his restaurant-supply store in Seattle. Among the deployed tools was a tunnel-digging robot "mole," a $475,000, 18-foot-long device that can chew through 70 feet of soil a day using programmed directional coordinates. The machine has been doing solid yeoman's work for years, but this time somebody programmed it incorrectly. Catania realized this when he saw 11 hard hats peering expectantly into a 30-foot-deep hole in the street, one muttering, "Our mole is supposed to come out here but we haven't seen it." Eventually recovered without damaging Catania's property, the wayward mole left behind a 700-foot hole that will have to be filled with concrete. Cost: $600,000. [Source: *The New York Times Magazine*, 1 Jun 1997, p. 25] [Apparently for only $475,000 you don't get any tracking! RJS]

Washington D.C. air traffic slowed

Air-traffic control around the eastern United States was seriously slowed down for nearly eight hours on 11 Jun 1997 because of a wiring error that occurred two months before when new communications equipment had been installed. The main system at National Airport for communication with aircraft in flight broke down.

Smith Barney customers become momentary millionaires (Jim Griffith)

CNNfn reported on 5 Jun 1997 that a computer glitch at Smith Barney caused half a million customer accounts to be credited with $19 million each for a brief period Wednesday night. Company representatives claim that customers did not have access to the money, and that the balances were only visible to Smith Barney brokers and any customers who happened to look at their account balances via the Internet during the brief period that the problem exists. The problem was reportedly quickly noticed and fixed. $19 million times 525,000 accounts = $9,975,000,000,000. That's $9.975 trillion, folks. Methinks someone misplaced the national debt by mistake...

Malfunction causes motor melee (Scott Lucero)

The United States Auto Club (USAC) declared a new winner in the True Value 500 on 8 June 1997 when an electronic device in five of the cars failed to record the laps where cars pull into the pit stop. Although there are two forms of manual backup, neither were used until hours after the race was complete even though the officials received notice of the malfunction during the race. USAC officials are considering fining A.J. Foyt and Arie Luyendyk, who turned out to be the winner following the audit, after they got into a victory circle scuffle. The malfunction came with 19 laps remaining, not leaving much time to change over manual methods. Race officials counted on the malfunction not affecting the outcome of the race. The USAC Chief Stewart said this is the first major malfunction since the devices were introduced in 1990. The risk is believing that, just because it hasn't happened in the past, doesn't mean that it isn't happening now.

ONE-LINERS:

- Russian nuclear warheads armed by computer malfunction (R 19 14)
- Ontario toll-road system six months late at twice the cost (R 19 24)
- Software problems with NATS new-generation air-traffic control center (R 19 18,23)
- Flaw discovered in Swedish rail control system after near miss (R 19 22)
- U.S. national EFTPOS system crashed on 2 Jun 1997 for two hours, 100K transactions were "lost". One CPU failed, backup procedures to redistribute the load also failed. (R 19 21)
- Washington D.C. Metro Blue Line delay 6 Jun 1997; system + backup failed (R 19 22)
- New GAO report says Pentagon overpaid contractors by $millions because different accounting systems do not interoperate (R 19 14)
- Time-bomb ticks in noncompliant no-name Pentium motherboards (R 19 13); further flaw detected in Pentium II and Pro – approximately 140,739,635,839,000 floating-point numbers affected (R 19 14); (R 19 18)

- DEC Alpha bug: pow(1.234567, 7.654321) may not give 5.017... (R 19 24,25)
- Telehouse 'reliable' backup center in London downed by internal power switch, downing most of the UK Internet (R 19 13,14)
- Norwegian brothel surveillance camera broadcasts live on WorldWideWeb (R 19 13)
- More on Y2K: sliding window approach, year-2069 problem (R 19 13); (R 19 14); year 2106 and 2038 problems in Unix (R 19 15); year 65,536, leap seconds, UTC vs TAI (R 19 16); DEC OpenVMS expired on 19 May 1997 (R 19 18); clock synchronization (R 19 18); Java Y2K problem arises in the year 292271023 (R 19 21)
- European Community study of fraud on the Internet (R 19 13)
- Texas prisoner convicted of rape employed to enter Metromail survey results, harasses respondents (R 19 13)
- Some speculative discussion on the downing of TWA 800 (R 19 13)
- Judge overturns all but smallest verdict in Digital keyboard case (R 19 14) noted earlier (R 18 66)
- ACM's ISP cuts off service for late payment of fees (R 19 15)
- Bank of America loses 1529 ATMs after maintenance goof (R 19 16)
- $98,002 refund check based on zip code, not correct amount $1.99 (R 19 16)
- Risks of leading zeros in Netscape and MSIE (R 19 21,22)
- MS Outlook e-mail Word problem (R 19 23)
- Cracker exploits flaw in MS Internet server software (R 19 23)
- Appropriateness of Confutatis Maledictis in MSIE advertisment? (R 19 23)
- Fire ants enjoy the comfort of electrical equipment (R 19 17-19)
- Effects of Leonid meteor shower in 1998-99 on satellites? (R 19 23)
- Faulty car alarm jams S-band downlink for Lewis satellite (R 19 24)
- More on EMI from passenger devices in aircraft systems (Ladkin) (R 19 24)
- Counseling available for deaths of Tamagotchi virtual pets (R 19 20)
- Train-ticket vending machine issues bogus tickets; victim harassed (R 19 20)

SECURITY, INTEGRITY, PRIVACY

U.S. Supreme Court rules on Communications Decency Act (PGN)

All nine Justices declared the CDA unconstitutional on 26 Jun 1997. In the majority opinion written by Justice Stevens, 7 of them ruled that the CDA violated free-speech rights in attempting to protect children from sexually explicit material on the Internet. The remaining two Justices (in an opinion written by Justice O'Connor, with Chief Justice Rehnquist concurring) wrote that they would invalidate the law only insofar as it interferes with the First Amendment rights of adults.

FBI sting nabs man trying to sell 100,000 credit-card data items (PGN)

Carlos Felipe Salgado Jr. ("Smak", 36, Daly City, CA) was arrested at San Francisco Airport on 21 May 1997 after he sold an encrypted diskette with personal data on more than 100,000 credit-card accounts to undercover FBI agents, who paid him $260,000, checked out the validity of the data, and then nabbed him. He reportedly had obtained the information by hacking into various company databases on the Internet or by packet-sniffing an unidentified SanDiego-based ISP. He faces up to 15 years in prison and $500,000 in fines. [Source: *San Francisco Chronicle,* 22 May 1997, A25; 23 May 1997, D1-2]

Add this case to the burgeoning file of cases related to Risks of Identity Theft, including recent cases involving thefts of a Visa International database of 300,000 credit cards (R 18 62), Caltrain's ticket-by-mail commuter database (R 19 02), and Levi Strauss' 40,000 employees and retirees (R 19 12).

DA computer chief almost loses all to clever sabotage (James H. Haynes)

Ralph Minow runs a family support computer system for the San Mateo County District Attorney. Their system crashed in March 1996. His assistant Paul Schmidt wanted his job, rigged the evidence to show that Minow deliberately caused the crash. Minow nearly lost his job because of the sabotage; but the perpetrator made enough mistakes that he was detected. Schmidt was fired in February, and will be prosecuted if his firing is upheld after a final hearing. His lawyer says Schmidt is being prosecuted for whistle-blowing. [Source: an Associated Press item datelined San Francisco in an unidentified paper published in Arkansas, 8 Jul 1997.]

ONE-LINERS:

- Cyber Promotions spamming restrained by Earthlink injunction; CP agrees to pay CompuServe $65,000; CP hit by 20-hour retaliatory spam attack (R 19 13); CompuServe blocks some multiple-address mailings? (R 19 21)
- Spammer Craig Nowak used Tracey LeQuey Parker's *from:* address; she received 5,000 bounces, and sued – along with EFF and Texas ISPs Assoc. (R 19 19,20)
- Spammer retaliates against Beth Arnold at NJ ISP for blocking him, using her e-mail address and 800 number; she was ping stormed and flooded with calls (R 19 21)
- More spamming: Newmediagroup anti-spam measures draw retaliation (R 19 16,17,21); Anti-spam bills in U.S. Congress and Senate (R 19 18,21);
- Spam filtering (R 19 24)
- Oregon DMV lost $15K photo licensing equipment (R 19 16)
- Report that "hackers get into Ramsay case computer" (R 19 23) is false; it was a dead CMOS battery!! (R 19 24)
- Swedish teen-aged hacker fined for U.S. telephone phreaking etc. (R 19 13)

- Swedish meat packer Website penetrated and replaced (R 19 14)
- WorldNet security flaw (R 19 19, correction in R 19 20)
- Internet Explorer runs arbitrary code: MIME type overridden (R 19 14)
- More on Web browser risks (R 19 18)
- Netscape flaw allows reading of entire hard drive (R 19 22,23)
- Macro virus lists from Klaus Brunnstein, ftp://agn-www.informatik.uni-hamburg.de/pub/texts/macro/ and ftp.informatik.uni-hamburg.de/pub/virus/macro/macrolst.* (R 19 24)
- 17 in Asian syndicate indicted for May 1995 theft of $10M in Pentium chips (R 19 21)
- Russian harvests 60 meters of cable in Ulan-Ude, disableing external phone service in Russia [19 Jun 1997]. Previously, 2 thieves in eastern Kazakhstan were electrocuted trying to steal high-voltage copper wires. (R 19 23)
- Backup system failure: cable had been stolen at Korat Royal Thai AFB, 1973 (R 19 24)
- 2,300 credit-card numbers stolen from ESPN Sportszone, NBA.com (R 19 24)
- Armed theft of $800K in chips thwarted (R 19 23)
- Theft of entire ATM bungled in British Columbia (R 19 20)
- Calif. PG&E power substation attacked, linked to McVeigh verdict (R 19 21)
- *Lost World* Website hacked into Duck World: Jurassic Pond (R 19 20,21)
- UK's MI5 phone recruitment hotline spoofed by KGB impersonator (R 19 20)
- Database misuse by 11 prison guards in Brooklyn (leaking names of informants to prisoners, warning about searches, etc.) (R 19 20)
- More on Social Security Administration PEBES database problems (R 19 16)
- Texas driver database on the Internet (R 19 22)
- Kansas sex-offender database full of incorrect entries (R 19 14); Also true in California DB: 2/3 of entires incorrect (R 19 24)
- Spreadsheet Research documents enormous operational error rates (R 19 24)
- Screening SW blocks access to *sex-y New Jersey counties (Sus*sex*, Es*sex*, etc.) (R 19 24)
- Abelson et al., report on key-recovery cryptography (http://www.crypto.com/key_study, ftp://research.att.com/dist/mab/key_study.ps or key_study.txt) (R 19 17); discussion (R 19 18)
- McCain-Kerrey bill in U.S. Senate seeks crypto key-recovery infrastructure (R 19 23)
- Draconian controls on Chinese Internet usage (R 19 23)
- RSA's DES challenge broken after 4 months (http://www.rsa.com) (R 19 23)
- Sun exploits loophole in crypto ban for SunScreen SKIP E+ (R 19 17)
- MD5 weakness and possible consequences (R 19 14,16,24)

Report from SEKE'97

Oh Cheon Kwon
Centre for Software Maintenance
Department of Computer Science
University of Durham
email:O.C.Kwon@durham.ac.uk

The Ninth International Conference on Software Engineering & Knowledge Engineering (SEKE'97), was held June 17-20, 1997 at the Husa Princesa Hotel in Madrid, Spain. The objective of SEKE'97 is to bring together two disciplines, i.e., Software Engineering(SE) & Knowledge Engineering(KE), in order to find solutions to most problems associated with both areas, as well as to identify interactions between Software Engineering & Knowledge Engineering. In the SEKE'97 conference, there were two main areas where the intersections of SE and KE were discussed: Software Process and Reuse. There have been around 120 delegates from more than 23 countries, and about 70% of these were from academia and 30% from industry. The SEKE'97 program committee received more than 150 contributions and chose about 70 papers.

The programme of SEKE'97 consisted of 5 tutorials, 4 keynote speaker talks, 5 presentations, 5 speakers' discussions focused on "Perspectives on Software Development," 16 sessions to present the authors' research.

The tutorials of the SEKE'97 Tutorials were composed of 5 topics: "Reuse Strategies" that presented a practical guide to the evaluation and implementation of the reuse of the application level in an organisation; "Analysis and Verification of real-time Rule-based Systems" which presented the basis of the technology for building the next generation of real-time expert systems capable of performing complex monitoring and control functions in a real time environment while meeting all specified time constraints; "Systematic Evaluation and Certification of Software Products and Processes" that addressed international software process standards (e.g., ISO9000 series, IEEE, CMM, Trillium, SPICE, Vorgehensmodell) and national process standards(e.g., IDEFx, V-Model, MERISE, SSADM and EUROMETHOD); "Agent Based Modelling" that covered the basic concepts that support the modelling of agent architectures to solve real world problems related to natural and socio-economic systems.

About 70 papers were presented in 16 sessions that were devided into 8 two parallel sessions, but I attended only sessions associated with software reuse that is one of my research areas. In this report, it is difficult to review all the talks that I listened to since many talks were given during the conference. Thus, I will be discussing specific talks which are related to my research and which I was interested in. The program of the SEKE'97 conference is available at http://www.ls.fi.upm.es/SEKE97/.

Vasconcelos who came from COPPE/UFRJ in Brazil, gave a talk titled "Software Development Process Reuse Based on Patterns." He presented a discussion about the use of patterns as a representation of a process knowledge. He also