CITI Fault Report Classification and Encoding for Vulnerability and Risk Assessment of Interconnected Infrastructures

Hafiz Abdur Rahman and Konstantin Beznosov
{rahmanha,beznosov}@ece.ubc.ca

LERSSE Technical report LERSSE-TR-2005-03

October 4, 2005

Abstract

Effective functionalities of many of the critical infrastructures depend on Communication and Information Technology Infrastructure (CITI). As such, any fault in CITI can disrupt the operation of these infrastructures. Understanding the origin of these faults, their propagation pattern and their impact on other infrastructures can be very valuable for secure and reliable infrastructures design and operation. However, up to now there is no well-defined technique to comprehend these inter-infrastructure fault scenarios. Public domain CITI fault reports can serve as a useful source to identify vulnerability patterns and impact of those vulnerabilities on other infrastructures. But, as most of these reports are unstructured description of fault events, this make their use limited and ineffective for formal research. Until now, not much work was done to methodically classify and interpret these reports. However, such classification could give infrastructure research community huge benefit to explore this massive amount of open source information. In this paper, we propose a classification method and a report layout format, which will enable meaningful analysis of these fault reports and will enable selective query and filtering when kept in a database. We have demonstrated our method by classifying and analyzing some of those reports and have explained the results in the context of interdependency research.

Contents

1 Introduction

Modern data communication and information technology infrastructure (CITI) provides key links and services to many other critical infrastructures, such as important government and corporate offices, manufacturing facilities, water supply, interstate road communications, gas and petroleum distribution networks, etc. Over many years, couplings and dependencies of these infrastructures on CITI have become pervasive, extensive and complex. As such, any fault or failure in CITI, either due to an accident or caused by a malicious attack can propagate to other infrastructures and can degrade or disrupt their functionality. Conversely, fault in other infrastructure can also propagate to CITI and hence disrupt the operation of these interconnected systems. Traditional approaches of such CITI fault and vulnerability analysis are based on different types of traffic and protocol analysis [1]. These approaches give progressive picture of fault sequences, such as, how fault is originated, aggravated and eventually led to network or system failure. However, results obtained through this approach are mostly applicable to CITI domain and does not give much idea how such faults affect the functionality of other infrastructures. Besides, most of these CITI fault and vulnerability data are not available to research community due to conservative attitude of government and corporations [2].

Another possible way to get fault information is through public domain security and vulnerability reports, mostly from newspapers and private individuals. Even though, these reports do not give exact progressive picture of fault sequences, they give a higher-level detail (panoramic view) of the fault scenarios. Systematic classification and analysis of each of these reports can give us valuable information about CITI vulnerabilities; and how those vulnerabilities affect other infrastructures. Such understanding from real life failure information can be valuable for secure, reliable and fault tolerant infrastructure design. However, biggest problems of using these reports in research are, they are unstructured and in many cases do not clearly describe the fault scenarios. Besides, sometime it is difficult to validate the original sources as well. Based on this observation, in this paper, we propose a method to classify these reports into different categories based on their fault type. We also propose a report-encoding structure that will allow selective search and query for meaningful analysis; and considering the completeness of fault description and integrity of the source, we are assigning a report accuracy rating. We present few analytical results using our techniques at the end of this paper. In Section 2, we discuss some of the previous works on CITI fault reports and their limitations, and then develop rationale for our own classification methodology. In Section 3, we give a brief overview of our own methodology. In Section 4, we classify and interpret some of the public domain fault reports using our methodology in the context of infrastructure interdependency analysis. In Section 5, we discuss some of the possible implications and use of these faults reports in the study of infrastructure safety and security analysis. Section 6 concludes this report discussing its contribution and then giving some future research directions.

2 Related Work

Until now, little attention was given on CITI fault reports for infrastructure related research. As such, only handful numbers of works were done to classify and interpret CITI fault reports. One of the earliest attempt was made by Peter G. Neumann, who started Association for Computing Machinery (ACM) RISKS forum in 1985 to compile computer related fault and vulnerability reports and their implication in public life. Later he published a book (1994) named "Computer-Related Risks" [3]. In this book, he qualitatively analyzed some of the reports from RISKS forum. He did not use any formal taxonomy or did not do any quantitative analysis. Even then, his discussions are very useful to get an understanding on different aspects of fault cases and show that, origin of many of those faults are due to system design error, improper runtime conditions, human mistakes, natural causes or due to deliberate malicious attacks. He also draws attention to the implication of safety and security risks associated with those faults in public life. He also discusses ideas about how to mitigate some of those problems by using better hardware, software design techniques and other preventive mechanisms.

John D. Howard proposes a taxonomy based on attack types (1997) and using that taxonomy he has done frequency analysis of more than 4000 security related incidents reported to Computer Emergency Readiness Team Coordination Center (CERT/CC) [4]. From the results of that analysis, he proposes a set of recommendation for government, vendors, CERT/CC and individual users to improve some of the security practices. Howard and Longstaff [5] extend this taxonomy to incorporate additional terms to include additional objects and attributes, such as site name, attack date and reporting time, etc.

Another taxonomy is proposed by Chakrabarti and Manimaran (2002) to classify Internet infrastructure security faults [6]. Their classification is based on a survey of research works in different areas of intrusion detection and prevention techniques. They classify Internet infrastructure faults into four broad categories; DNS hacking, routing table poisoning, packet mistreatment, and denial of service attack. They also discuss consequences of these attacks and possible detection and prevention techniques.

Even though these taxonomies [5][6] are useful in their own context, they are not very useful for CITI fault and vulnerability classification. This is because these classifications are primarily based on intentional cyber attacks. However, in CITI infrastructure, many of the faults are accidental and related to the reliability and survivability aspect of the infrastructure. A recent study by Nicol et al [7] shows the differences between reliability paradigm and security paradigm. Computational modeling of reliability of large computer system is a well-developed paradigm and many of these modeling techniques are useful to model security of lager computer network with some modification. However, there are some concepts like data confidentiality, integrity and non-repudiation, which do not have reliability counterpart [7]. Our study, which is targeted towards the development a comprehensive analytical framework for modeling interdependencies of CITI and other interconnected infrastructures, needs to capture both reliability and security aspects of the infrastructure.

As such, taxonomies developed in [5][6] for network fault classification are not adequate. In this report, we propose a layered approach, which divides Chakrabarti and Manimaran's classifications [6] into three layers, and then add an additional layer for physical devices and links. This approach will enable us to model and simulate CITI infrastructure in a layer-by-layer basis. Hagin's [8] used one such approach for reliability and survivability analysis of X.25/X.75 switching network. Our approach has some similarity with ISO/OSI reference model [9] and is discussed in the following section.

3 Approach and Methods

Layer based abstraction of network functionality has made OSI reference model a powerful conceptual tool to partition communication related entities in different layers and then define logical relationship among these layers. As such, OSI model has influenced different types of communication and software engineering architectures for many years. For instance, White [10] proposes a seven-layer reference model for military's Global Communication; Hightower et al [11] proposes a seven-layer software engineering model for location in ubiquitous computing; and Ciarletta and Dima [12] proposes a four-layer pervasive computing conceptual model. Likewise, we propose a CITI fault classification framework with the following four layers. Existing techniques to model reliability and security issues related to these layers can be found in [7].

a. Physical Devices and Link Layer (Class A)
b. Data Packet Layer (Class B)
c. Network Connectivity Layer (Class C)
d. Subscriber Systems Layer (Class D)

Physical Devices and Link Layer (Class A): This layer is similar to physical layer of OSI model. All faults of this layer are related to infrastructure devices and physical communication links, such as device failure, physical communication channel disruption or inadequate link capacity. Unlike other three layers, faults in this layer are mostly due to improper design, accident, natural causes or intentional subversive activity such as terrorist attack. Reliability and performance are the most frequent concerns for this layer. Redundant devices, backup physical channels and sufficient bandwidth are some common ways to deal with these problems. [13]

Data Packet Layer (Class B): This layer is associated with the faults related to the raw data packets flowing through the network and as such, it has some similarity with the Data Link layer of OSI protocol model. We consider any packet mistreatment attack belongs to this class [6]. For example, adversaries capture actual data packets and then drop, modify or replicate those packets. Decryption of captured packets is also falls in this category. Use of secure protocol such as IPSec can take care of some of the concerns for this layer.

Network Connectivity Layer (Class C): This layer is similar to Network layer of OSI protocol model. For TCP/IP network, all router and DNS server attacks fall into this category. Possible solutions include use of digital signature, DNSSEC protocol, etc. [6]

Subscriber Systems Layer (Class D): All host systems and services belong to this layer. All subscriber level faults, which are not in class A, B and C, belong to this category. Although, all end system faults which do not directly effect infrastructure operation (e.g., website hacking) are also belong to this category; we ignored them in our case studies. This is because we are only focused on those faults, which disrupt the operation of the infrastructure network Denial of Service attacks, Worm attacks and other similar attacks and vulnerabilities are considered in our case studies. Different kinds of intrusion detection techniques and packet filtering mechanisms are used as a preventive technique for these kinds of vulnerabilities. [5]

4 Case Studies

In this section, we have compiled materials from the RISKS Forum [14] and Hobbes' Internet Timeline [15]. Many of these cases are also mentioned in Peter Neumann's book [3]. Intuitively we define fault as a single event of vulnerability that leads to undesirable consequences. Failure is a collapsed state of a system caused by single or multiple faults. Each report has a code number and a title. Code number is a sequential number coupled with its fault type (Class A, B, C or D). Title is a more descriptive form of report name and can be used for selective query or grouping. Most often, case title is the same as the title of the original report. For each of the following events, we have added few classification attributes for our own interpretation. These are Fault Type, Severity, Network Trace, Simulation, Date, Country, Duration, Affected Sites, Public Safety, Fault Origin, Source Infrastructure, Affected Infrastructures and Affected Industry Sectors. In Fault Type, we have used three attributes based on their primary causes. These are natural, unintentional and intentional causes. Natural faults are mainly due to climatic or environmental reasons, such as earthquake, hurricane or tornado. Unintentional faults are those, which occur due to system design flaw or run-time malfunctioning, such as unexpected device failure. On the other hand, intentional faults are those, which occur due to deliberate and malicious attempts by any individual or groups. Besides, based on severity we have divided these faults into high, moderate and low impact categories. "High" are those events, which affect large segment of the CITI infrastructure, "Moderate" are those, which affect small number of systems, and "Low" is for a single device or a system failure. Network Trace shows availability of TCP/IP protocol trace or other supporting information related to a particular fault. Simulation attribute indicates if the fault conditions can be simulated within a lab environment using NS2 [16] or similar network simulator. Date is the timeline when the fault incident happened. In the absence of such information, it is the date of the original fault report. Country is location where the fault incident had vital impact. Duration is the time from the fault start time up to its full recovery. Affected Sites is the number of sites or locations affected by a particular fault incident. Public Safety attribute implies any public risk associated with a particular fault incident, such as loss of human life or failure of lifeline services (e.g., 911-directory service).

Most of the events are collected from "The Risks Digest" and are referred in the form RISKS (i, j) where i is the volume number and j is the issue within the volume. RISKS forum has online version of these digests. For each of these reports, information source is mentioned. Based on the source type we assign an accuracy rating on a scale of 10. If the information is released from an official source and has other supporting references for validation, we assign it 9 or 10 points. If it is from an official source, but no further detail is given, it has 7 or 8 points. All newspaper reports have 5 or 6 points. Reports from individuals, which have difficulty to verify, are normally given less than 5 points. Higher rating is given to a report of a particular class, if the report fulfills most of our additional attribute criteria. For instance, if a newspaper report has most of the information like severity, duration, financial impact, description of fault origin, etc. then it is given 6 points. Otherwise, it is given 5. Next, we make an assessment about origin of fault, affected infrastructures and affected industries from the fault description. Finally, we add comments to specify some interesting aspects of these faults.

4.1 Physical Devices and Link Layer (Class A):

All faults of this layer are related to infrastructure devices and physical communication links, such as device failure, physical communication channel disruption or inadequate link capacity.

A.1	**Ground-cable removal blows Iowa City phone system upgrade**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
11/19/1994	USA	High	No	Unsure
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	6 hours	Unknown	Yes	Unknown

On November 19, 1994, Iowa City's US West telephone system shut down at about 3:30 p.m., local time, and service was gradually restored between 7:30 and 9:30 p.m, affecting about 60,000 people. Analysis showed that a new switching system had been installed in July 1994. In removing the old system, an electrical grounding cable had been inadvertently removed.

Report Source	*Iowa City Press Citizen, November 22, 1994; see discussion by Douglas W. Jones, RISKS (16, 58)*
Report Accuracy	6
Fault Origin	Fault in electrical system due to human error.
Source Infrastructure	Electrical Power System
Affected Infrastructures	Telephone infrastructure
Affected Industry Sectors	All kinds of industries of Iowa City
Comment	Lack of detailed planning

A.2	**MFS Communications switch fails, with widespread effects**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
9/8/1997	UK	High	No	No
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	Unknown	Unknown	No	Unknown

Around 7 p.m. on the evening of 8 Sep 1997, the main MFS Communications switch (MFS Switch One) failed, downing UK telecommunications links provided by MFS, Worldcom, and First Telecom. The outage also affected most of CompuServe's UK customers, whose access is typically via an MFS phone number. [Evening usage is not necessarily off-peak, because it is an excellent time to access computers in the U.S. No one has yet reported how long it took to restore service.]

Report Source	*RISKS (19, 39)*
Report Accuracy	4
Fault Origin	Hardware fault in telephone switching system.
Source Infrastructure	Telecommunication Infrastructure.
Affected Infrastructures	Home users.
Affected Industry Sectors	Not known.
Comment	Device failure. No backup system was available

A.3	**Indian satellite failure**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
10/6/1997	India	High	No	No
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	Unknown	Unknown	No	Unknown

According to the 6 Oct 1997 Daily Brief, officials in India say the country's most advanced communications satellite was abandoned on 5 Oct 1997 due to a power failure aboard the craft. The loss of the satellite reportedly affected communications to remote parts of the nation and the operation of satellite-dependent functioning of India's stock exchange. This appears to be an example of the familiar RISK of having a single point of failure, or, more colloquially, putting all your eggs in one basket.

Report Source	*RISKS (19, 41)*
Report Accuracy	4
Fault Origin	Electrical failure.
Source Infrastructure	Telecommunication Infrastructure.
Affected Infrastructures	Telecommunication and Data networks.
Affected Industry Sectors	Financial sector, public and private telecom users.
Comment	Device failure.

A.4	**Blown fuse takes out 911 system**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
11/25/1996	USA	High	No	No
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	3 hours	Unknown	Yes	Unknown

A blown fuse took out a large portion of Iowa's 911 emergency phone system for three hours over the 1996 Thanksgiving weekend. U.S. West could not say how many 911 calls went unanswered. A spokesperson said that the problem came from the complexity of the system.

Report Source	*National Public Radio, noted by Scott Lucero, RISKS (18, 65).*
Report Accuracy	5
Fault Origin	Hardware failure in telephone switching hardware.
Source Infrastructure	Telecommunication Infrastructure.
Affected Infrastructures	Home users.
Affected Industry Sectors	Unknown.
Comment	Device failure. No backup system was available.

A.5	**Garbage-truck worker wipes out telephone service**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
2/20/1996	USA	High	No	No
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	Unknown	Unknown	Yes	Unknown

A cowboy garbage-truck driver in Oregon playing the game of "swing the cables" with his fork lift accidentally severed a cable that disrupted service for a wide area of subscribers.

Report Source	*Andrew J. Klossner, RISKS (17, 77).*
Report Accuracy	4
Fault Origin	Telephone infrastructure.
Source Infrastructure	Telephone infrastructure.
Affected Infrastructures	Telephone infrastructure.
Affected Industry Sectors	All kinds of telephone subscribers of Oregon, US.
Comment	Human error.

A.6	Rough days on the stock markets			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
10/28/1997	USA	High	No Information	No
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	2 days	Unknown	No	Unknown

With the huge fluctuations in stock prices on 27-28 Oct 1997, the NYSE and NASDAQ each handled over a billion shares for the first time ever on 28 October 1997, with the NYSE at 175% of the previous blockbuster day. The bad news is that those folks who relied on the Internet to do their panic trading were in for a rough time. There were huge numbers of e-trades already queued up before opening, causing an early traffic jam. Joseph Konen of AmeriTrade Holding blamed some of the delays on limitations of its firewall technology. Many would-be Internet buyers and sellers simply could not get access, in part because their Internet service providers were saturated. Many customers were blocked out because others were tying up lines just to monitor the market. (Illustrating the extent to which Internet trading has become a part of the markets, Schwab normally does 35 percent of its trading on-line; previous day's trading of more than 300,000 on-line transactions more than doubled their Monday load and tripled their typical day.) Conventional trades were also affected. [Steve Bellovin, Frank Carey, and Nick Bender gave lots of details, including Nick noting the effects on NASDAQ of a sequence-number overflow from 999,999 to 000,000 (R 19 44).] .

Report Source	*RISKS (19, 43).*
Report Accuracy	
Fault Origin	Network service request exceed ISPs' system capacity.
Source Infrastructure	Data network.
Affected Infrastructures	Data network.
Affected Industry Sectors	Financial sector.
Comment	Network congestion. Inadequate bandwidth.

A.7	**Redundant virtual circuits lead to single point of failure**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
1/14/1997	Finland	High	No Information	Yes
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	Unknown	Unknown	No	Unknown

A report from Finland indicated that the main and reserve lines between Oulu and Kajaani went through the same physical circuit, despite an agreement with Finnnet that they should be separate

Report Source	*Sidney Markowitz, RISKS (18, 76).*
Report Accuracy	
Fault Origin	Physical link failure due to incorrect planning.
Source Infrastructure	Telecommunication Infrastructure.
Affected Infrastructures	Significant part of Finnnet (Finland's Internet).
Affected Industry Sectors	Exact detail not known.
Comment	Human error.

A.8	**Microsoft, AT&T, AOL netwoes**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
6/23/1996	USA	High	No Information	Unsure
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	10 hours	Unknown	No	Unknown

Microsoft shut down its nationwide network on June 23, 1996, for 10 hours as part of an intended backup power-supply upgrade, but the upgrade failed and they had to try again.

AT&T had to shut down its Internet access for up to 8 hours each week, for maintenance.

America Online was out of service for an hour on June 19, 1996, when a planned system software upgrade backfired.

Report Source	*Peter H. Lewis, The New York Times, June 24, 1996, p. D1; RISKS (18, 23)*
Report Accuracy	6
Fault Origin	Electrical power system.
Source Infrastructure	Data Communication Network.
Affected Infrastructures	A significant part of US Internet.
Affected Industry Sectors	Significant part of commercial and non-commercial Internet users of US.
Comment	Lack of detail planning.

A.9	Explosion causes Internet blackout in New England			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
8/7/1997	USA	High	No	Yes
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	4 hours	Unknown	Yes	Unknown

More than 200 New England businesses experienced a four-hour Internet blackout on 7 Aug 1997 after an explosion knocked out electrical power in the Boston area. One person was killed in the blast, which overloaded a panel switch at MIT, causing a fire and cutting off Internet access to BBN Planet customers. Access resumed around 10:00. The speed with which the incident happened made it impossible to reroute traffic, said a BBN spokesman.

Report Source	*TechWire, 8 Aug 1997; Edupage, 10 Aug 1997, RISKS (19, 29-30)*
Report Accuracy	5
Fault Origin	Physical link failure due to an accident.
Source Infrastructure	Electrical Power Network.
Affected Infrastructures	A significant part of US Internet.
Affected Industry Sectors	Almost all commercial and non commercial Internet users of eastern US.
Comment	Exact reason for power failure not known.

A.10	**Swedish telephone outage**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
3/15/1999	Sweden	High	No	No
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unknown	8 hours	Unknown	Yes	Millions

After a number of ISDN outages last year and some this year in the country, our nationally owned Telco Telia had two big outages in the capital of Stockholm. It happened the first time 15 Mar 1999, when millions of phone lines including the police headquarters' PBX were unusable for 8 hours! The outage was repeated exactly a week later between 10:25am and 11:05am, when incoming calls to the police PBX and to another 250 business PBXs where blocked.

The second outage is explained as an intermittent error that disturbed the communication between PBXs and the Telco equipment. In addition, the software that would localize the problem had a bug so that the error would not display.

Coming to mind is that Telco exchanges are often purchased in international competition. A telco operator cannot see through the software. However, given the complexity neither can the producer; we might not have bugs if they did. Therefore, if an intruder paid by some nearby country wanted to, he could program some code "detonating" as a part of war attack.

Report Source	*RISKS (20, 29)*
Report Accuracy	
Fault Origin	Telephone switching circuit malfunction and also software bug.
Source Infrastructure	Telecommunication Infrastructure.
Affected Infrastructures	Telephone infrastructure.
Affected Industry Sectors	All kinds of subscribers of Swedish telecom (Telia).
Comment	Human error or could be intentional.

A.11	Software bug cripples Singapore phone lines			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
10/12/1994	Singapore	High	No	No
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	5 hours	Unknown	Yes	26

A bug in newly installed computer software corrupted one of the two common channel signaling systems, affecting 26 out of 28 exchanges, and knocking out two-thirds of Singapore's telephone lines on October 12, 1994. Hand phones, fax machines, pagers and credit cards were all hit by the disruption, which began at 11:31 a.m. in the City Exchange. It took Singapore Telecom's engineers about five hours to get services back to normal again. Fortunately the old backup system was still running side by side with the new system.

Report Source	*The Straits Times, October 13, 1994; Lee Lup Yuen, RISKS (16, 46).*
Report Accuracy	6
Fault Origin	Software bug in telephone switching devices.
Source Infrastructure	Telecommunication Infrastructure.
Affected Infrastructures	Telephone, pager and credit cards.
Affected Industry Sectors	Financial, public and private users.
Comment	Software bug.

A.12	**SpaceCom technician disables millions of pagers**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
9/26/1995	USA	High	No	No
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	1 day	Unknown	Unknown	Millions

At the SpaceCom uplink facility in Tulsa, Oklahoma, an operator accidentally sent out a command shutting down the satellite receivers used by pager systems throughout the country, affecting millions of pagers. SpaceCom supports 5 of the largest 10 paging outfits. This happened at 1 a.m. on September 26, 1995, and each receiver had to be manually reprogrammed – which took all day until most of the service could be restored. Apparently, the operator omitted a carriage return at the end of a line, which is sort of the inverse of intending to type rm *.log but accidentally fat-fingering the carriage return just after the asterisk

Report Source	*AP report, seen in the San Francisco Chronicle, 27 Sep 1995, p. A2; RISKS (17, 37).*
Report Accuracy	6
Fault Origin	Human error to enter correct command. More subtle reason seems that there was no safeguard or warning mechanism before the start of a destructive command sequence.
Source Infrastructure	Telecommunication Infrastructure.
Affected Infrastructures	Telephone (pager) infrastructure.
Affected Industry Sectors	Wide range of government, non-government organizations and private individuals.
Comment	Human error.

A.13	**NASDAQ Computers Crash**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
7/25/1994	USA	High	No	No
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	3 hours	Unknown	Unknown	1

The U.S. automated over-the-counter NASDAQ marketplace went down for 2.5 hours on the morning of July 15, 1994, when the computer system died. (It was finally restored just before N.Y. lunchtime.) The problem was traced to an upgrading to new communications software. One new feature was added each morning, beginning on Monday. Thursday's fourth new feature resulted in some glitches, but the systems folks decided to go ahead with the fifth feature on Friday morning anyway – which overloaded the mainframes (in Connecticut). Unfortunately, the backup system (in Rockville, MD) was also being upgraded, in order to ensure real-time compatibility. The backup died as well. The backup system is "really for natural disasters, power failures, hardware problems that sort of thing," said Joseph R. Hardiman, Pres and CEO of Nasdaq. "When you're dealing with operating software or communication software, it really doesn't help you." Volume on the day was cut by about one third, down from a typical 300 million shares. The effects were noted elsewhere as well, including several stock indexes, spreading to the Chicago options pits, trading desks, and the media. That in turn affected the large stock-index mutual funds.

Report Source	*Diana B. Henriques, NASDAQ Computers Crash, Halting Trading for More Than Two Hours, The New York Times, July 16, 1994; RISKS (16, 25).*
Report Accuracy	6
Fault Origin	Updated communication software malfunction.
Source Infrastructure	Data Network Infrastructure.
Affected Infrastructures	Data network and connected systems.
Affected Industry Sectors	Financial sector.
Comment	Network problem, detail not known. Possibly software configuration problem.

A.14	**Fire damages fiber-optic cable at Maryland**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
7/18/2001	USA	High	No Information	Yes
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	Unknown	Unknown	Unknown	Unknown
A fire in a train tunnel running through Baltimore, Maryland seriously damages various fiber-optic cable bundles used by backbone providers, disrupting Internet traffic in the Mid-Atlantic states and creating a ripple effect across the US (18 Jul).				

Report Source	*Hobbes' Internet Timeline.*
Report Accuracy	7
Fault Origin	Origin of the fire might be an accident or a natural phenomenon.
Source Infrastructure	Physical Infrastructure.
Affected Infrastructures	Data network.
Affected Industry Sectors	Wide range of industries connected to Internet.
Comment	

A.15	**Attack on fiber-optic cables causes Lufthansa delays**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
2/1/1995	Germany	Medium	No	Yes
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Intentional	Unknown	Unknown	Yes	15000
On February 1, 1995, unknown attackers severed 7 fiber-optic cables near the Frankfurt/Main airport. About 15,000 telephone lines were interrupted. The cables also carried data for Lufthansa's booking computers; consequently, new reservations had to be made manually. As Lufthansa's main computers (at Frankfurt airport) were cut off for some time, delays of up to 30 minutes were caused.				

Report Source	*Klaus Brunnstein, RISKS (16, 78).*
Report Accuracy	
Fault Origin	Fault in CITI infrastructure due to malicious attack.
Source Infrastructure	Data Communication Network.
Affected Infrastructures	Data and telephone network.
Affected Industry Sectors	Airline industry.
Comment	Lack of physical infrastructure security.

A.16	**Disruption from stolen cables**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
6/19/1997	Russia	High (assumed)	No	No
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unknown	Unknown	Unknown	Yes	Unknown

In Ulan-Ude, Russia, a man harvested 60 meters of cable, disabling external phone service on June 19, 1997. Previously, 2 thieves in eastern Kazakhstan were electrocuted trying to steal high-voltage copper wires. In a much older case recalled by Cliff Krieger, a computer backup system failed when it was needed because a cable had been stolen at the Korat Royal Thai Air Force Base in 1973.

Report Source	*RISKS (19, 23 and 24).*
Report Accuracy	
Fault Origin	Telephone infrastructure.
Source Infrastructure	Telecommunication infrastructure.
Affected Infrastructures	Telephone infrastructure.
Affected Industry Sectors	All kinds of telephone subscriber of Ulan-Ude, Russia (assumed).
Comment	Lack of physical infrastructure security.

4.2 Data Packet Layer (Class B):

All faults related to the raw data packets flowing through the network belong to this category. Any packet mistreatment attack such as, adversaries capture actual data packets and then drop, modify or replicate those packets. Decryption of captured packets is also falls in this category.

B.1	**The Eagle (the President) and the Eagle Beagle**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
9/13/1997	USA	High	No Information	Unsure
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Intentional	1 day	Unknown	Yes	1

An unidentified hacker announced on 19 Sep 1997 the interception of President Clinton's pager messages (along with pager messages destined for staff, Secret Service agents, and other members of his entourage) during his April 1997 trip to Philadelphia. The lengthy transcript of pager messagers was published on the Internet to demonstrate that the pager infrastructure is highly unsecured.

(Apparently, the President's entourage relies a lot on pagers for communications. There are messages from Hillary and Chelsea; a Secret Service scare; late-breaking basketball scores for the President; staffers exchanging romantic notes; and other amusements.)

This comes at quite an embarrassing time for the administration, given their policy on encryption. Strong encryption is the one technology that could have protected the private pager messages, but the administration has been fighting against strong encryption. Top FBI officials have been giving many classified briefings to House members, asking them to ban all strong encryption in the US.

An anonymous White House staffer was quoted as saying that it would be "an expensive and complicated proposition" to put encryption into pagers and cell phones. This quote is interesting, because it is the White House's crypto policies that have made it so complicated and expensive to add strong encryption - the cell phone and pager industries have wanted to add strong encryption for privacy and security, but the administration has forcefully dissuaded them from doing so. [See RISKS-19.39 and 40 for more]

Report Source	*RISKS (19, 39).*
Report Accuracy	
Fault Origin	Weak or no encryption used in pager communication.
Source Infrastructure	Data network (pager).
Affected Infrastructures	Data network (pager).
Affected Industry Sectors	Government sector. May have large impact on for non-government sectors and private individuals.
Comment	Weak encryption. May lead to packet mistreatment.

4.3 Network Connectivity Layer (Class C):

All router and DNS server related faults fall into this category.

C.1	**MCI Internet gateways choked**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
8/1/1994	USA	Medium	No	Yes
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	30+ day	Unknown	Yes	Unknown

MCI's inbound Internet gateways were saturated during July 1994, resulting in days of delay in delivering e-mail to MCI customers. A fix was considered to be months in the offing

Report Source	*The Washington Post, August 1, 1994, noted by Mich Kabay , RISKS (16, 30).*
Report Accuracy	5
Fault Origin	Insufficient gateway capacity.
Source Infrastructure	Data network.
Affected Infrastructures	ISP subscribers.
Affected Industry Sectors	All subscribers of MCI, which might include commercial, non-commercial and domestic end users.
Comment	Design flaw. Internet gateway capacity is less than actual requirement.

C.2	**Internet routing black hole**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
4/23/1997	USA	High	No information	Yes
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	3 hours	Unknown	No	Unknown

On April 23, 1997, at 11:14 a.m. EDT, Internet service providers lost contact with nearly all of the U.S. Internet backbone operators. As a result, much of the Internet was disconnected, some parts for 20 minutes, some for up to 3 hours. The problem was attributed to MAI Network Services in McLean, Virginia (www.mai.net), which provided Sprint and other backbone providers with incorrect routing tables, the result of which was that MAI was flooded with traffic. In addition, the InterNIC directory incorrectly listed Florida Internet Exchange as the owner of the routing tables. A "technical bug" was also blamed for causing one of MAI's Bay Networks routers not to detect the erroneous data. Furthermore, the routing tables Sprint received were designated as optimal, which gave them higher credibility than otherwise. Some thing like 50,000 routing addresses pointed to MAI

Report Source	*Randy Barrett, Steven Vonder Haar, and Randy Whitestone, Inter@ctive Week Online, April 25, 1997, RISKS (19, 12).*
Report Accuracy	5
Fault Origin	Routing problem due to a technical bug might be a human error.
Source Infrastructure	Data network.
Affected Infrastructures	Significant part of US Internet backbone.
Affected Industry Sectors	Almost all industry sectors connected to Internet.
Comment	Routing protocol problem. A similar intentional fault can be due to routing table poisoning.

C.3	Partial failure of Internet root name servers			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
7/16/1997	USA	High	No information	Yes
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	4+ hours	Unknown	No	Unknown

Around 11:30 p.m. EDT on July 16, 1997, Network Solutions Inc. attempted to run the autogeneration of the top-level domain zone files, which resulted in the failure of a program converting Ingres data into the DNS tables, corrupting the .com and .net domains in the top-level domain name server (DNS), maintained by NSI. Quality-assurance alarms were evidently ignored and the corrupted files were released at 2:30 a.m. EDT on July 17 – 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

Report Source	*Peter Wayner in Cybertimes, July 18, 1997, see also RISKS (19, 25).*
Report Accuracy	5
Fault Origin	DNS server update problem due to incorrect operation of a data conversion program.
Source Infrastructure	Data communication network.
Affected Infrastructures	Part of Internet infrastructure. Effect on other infrastructure is not known.
Affected Industry Sectors	Not known.
Comment	DNS server problem. A similar intentional fault can be due to DNS hacking.

C.4	Netcom crash.			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
7/17/1996	USA	Medium	No	Yes
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	14 hours	Unknown	No	100+

Netcom, Inc. (now part of ICG Communications Inc.) went down for more than 14 hours during the week of June 17, 1996, because of an extra ”&” in the border gateway protocol code in the MAE-East router in the Washington, D.C., area. Recovery required that all of the more than 100 routers be brought down

Report Source	*David Leshe, RISKS (18, 23).*
Report Accuracy	
Fault Origin	Software bug in the gateway routers.
Source Infrastructure	Data communication network.
Affected Infrastructures	A small but important part of US Internet.
Affected Industry Sectors	Subscriber of Netcom and others in that region.
Comment	Software bug.

C.5	**Satellite transmission snafu leads to diplomatic incident**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
7/19/1997	France	Low	No	No
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	Unknown	Unknown	No	Unknown

On 19 Jul 1997, a "technical error" caused the contents of a channel on a satellite (operated by France Telecom) to be transmitted on another channel, for about twenty minutes. Normally this would have been merely annoying for the viewers. However, these viewers were in (among other places) Saudi Arabia, the channel they expected to be watching was the French government-run, general interest and news station, Canal France International (CFI), and the program which replaced it was a hard-core pornographic movie that should have been shown on the subscription-only, encrypted French domestic station, Canal Plus. As a result, Arabsat cancelled its contract with France Telecom, claiming that France Telecom had not "honored its commitment to respect Arabic and Islamic values." The French Foreign Ministry and the French Ambassador in Riyadh was trying to calm what has become a diplomatic incident.

Report Source	*RISKS (19, 26).*
Report Accuracy	
Fault Origin	Scheduling error of a satellite operator.
Source Infrastructure	Telecommunication network.
Affected Infrastructures	Telecommunication and Broadcasting Infrastructure.
Affected Industry Sectors	Home TV viewers.
Comment	Human error.

C.6	**Network Solutions goof bumps NASDAQ off the Internet**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
8/19/1997	USA	High	No information	Unsure
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unclear	24+ hours	Unknown	No	5000+

The NASDAQ stock exchange was knocked off much of the Internet for several hours on 19 Aug 1997 as a result of administrative errors at the InterNIC, a centralized Internet address clearinghouse run by Network Solutions Inc. of Herndon, VA. Though the problem was initially invisible to NASDAQ, which maintains its own database of Internet addresses, the temporary suspension of access to the exchange's site blocked users of major computer networks - including those owned by IBM Corp., MCI Communications Corp., PSINet Inc. and UUnet Technologies Inc. As a result, NASDAQ was unreachable to most Internet users for at least several hours Tuesday morning. Problems with the Web site had no effect on the functioning of NASDAQ itself. The snafu was due to a clerical error at NSI, which evidently lost track of Nasdaq's $50 fee, submitted in October 1996. [Abstracting, from article by Will Rodger, in Inter@ctive Week Online, 21 Aug 1997] Will remarked that things like this seem to be occurring more often. The weekend before, more than 5,000 Web sites were blocked for over 24 hours, when Web Communication Inc and other domains were bumped from the Internet after a screw-up in routine InterNIC maintenance.

Report Source	*Sidney Markowitz, RISKS (19, 34).*
Report Accuracy	
Fault Origin	Human error to manage Internet address.
Source Infrastructure	Data communication network.
Affected Infrastructures	Big section of Internet.
Affected Industry Sectors	US Stock market and related financial industries.
Comment	Routing problem. A similar intentional fault can be due to routing table poisoning.

4.4 Subscriber Systems Layer (Class D):

All subscriber level faults, which are not in class A, B and C, belong to this category. Denial of Service attacks, Worm attacks and other similar attacks and vulnerabilities are considered in our case studies.

D.1	**Prodigy misdirects or loses e-mail messages**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
3/10/1995	USA	Low	No	Unsure
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	5 hours	Unknown	No	Unknown
A software glitch on March 10, 1995, caused Prodigy's e-mail system to send 473 e-mail messages to incorrect recipients and to lose 4,901 other messages. The system had to be shut down for five hours				

Report Source	*Atlanta Journal-Constitution, March 11, 1995, B3; Edupage 12 Mar 1995; RISKS (16, 90).*
Report Accuracy	5
Fault Origin	Software bug.
Source Infrastructure	Data network.
Affected Infrastructures	All kinds of subscriber of the ISP. Exact detail not known.
Affected Industry Sectors	Industrial and non-industrial users. Exact detail not known.
Comment	Software bug.

D.2	Online services taking big hits			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
6/29/1994	USA	Low	No	No
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	Unknown	Unknown	No	Unknown

Alan Wexelblat reported seeing a commercial for Prodigy's on-line computer service during Game 6 of the 1994 Stanley Cup finals on ESPN. The ad cut to a live computer screen showing Prodigy. Suddenly, a big window came up on the screen, saying communication error. The ad was talking about how great the hockey game was, but that it did not compare to the excitement available on Prodigy. Apparently, at that time Prodigy users observed that the system locked up for almost a minute, and then their screens went completely blank. ESPN quickly cut away to another commercial. The curse of the live demo

Report Source	*RISKS (16, 21).*
Report Accuracy	
Fault Origin	Improper operation of ISP.
Source Infrastructure	Data network.
Affected Infrastructures	Home users.
Affected Industry Sectors	Home users.
Comment	Result of pushing advertisement into the client machines by the ISP.

D.3	**Bell Atlantic 411 outage.**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
11/25/1996	USA	Medium	No	No
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	Unknown	Unknown	Yes	36

On November 25, 1996, Bell Atlantic had an outage of several hours in its telephone directory-assistance service, due apparently to an errant operating-system upgrade on a database server. For unknown reasons, the backup system also failed. The result was that for several hours 60take callers' requests and telephone numbers, look up the requested information in printed directories, and call the callers back with the information. Apparently, the problem was solved by backing out the software upgrade. This was reportedly the most extensive such failure since operators began using computerized directory assistance

Report Source	*Rich Mintz, RISKS (18, 63) and J. Perillo, RISKS (18, 65).*
Report Accuracy	
Fault Origin	Software updates error.
Source Infrastructure	Information Technology Infrastructure.
Affected Infrastructures	Telephone infrastructure.
Affected Industry Sectors	Home and industrial users of several US cities.
Comment	Software bug.

D.4	**San Francisco 911 system woes.**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
10/12/1995	USA	High	No	No
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	Unknown	Unknown	Yes	1

San Francisco tried for at least three years to upgrade its 911 system, but computer outages and unanswered calls remain rampant. For example, on October 12, 1995, the dispatch system crashed for over 30 minutes in the midst of a search for an armed suspect (who escaped). The dispatch system was installed two months before as a temporary fix to the recurrent problems, and it too suffered unexplained breakdowns. Screens freeze; vital information vanishes; and roughly twice a week the system crashes. Dispatchers are not able to answer between 100 and 200 calls a day. Many non-emergency calls are also being lost. The reported extremely stressful working conditions seem similar to those experienced by air-traffic controllers. The 911 system collapsed again on November 4, 1995, for an hour; the absence of an alarm left the collapse undetected for 20 minutes

Report Source	*Phillip Matier and Andrew Ross, San Francisco Chronicle, October 18, 1995, p.A1; RISKS (17, 40).*
Report Accuracy	
Fault Origin	Hardware and software problem.
Source Infrastructure	Information Technology Infrastructure.
Affected Infrastructures	Telecommunication infrastructure.
Affected Industry Sectors	Wide variety of public and private users.
Comment	Hardware and software configuration problem. Lack of adequate planning.

D.5	**Calling-Number ID ghosts calls**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
3/8/1995	USA	Low	No	No
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	Unknown	Unknown	No	2

In early March 1995, a Detroit area woman looked at her Calling-Number Identification unit (misnamed Caller ID) and was puzzled to notice that it indicated 19 received calls that evening, even though only one person had called. Then she checked the names listed. John F. Kennedy, Thomas Paine, Harry S Truman, John Hancock, Ulysses S. Grant, Samuel Clemens, Ronald Reagan, and many others. Most of the phone numbers were non-working, but a few were. A neighbor had also been plagued with phone calls for Abraham Lincoln. Ameritech believes the Caller ID box was probably a pre-programmed demonstration model, although a telecommunications consultant suspected the work of a phone hacker

Report Source	*Detroit Free Press, March 8, 1995; Jim Huggins, RISKS (16, 88).*
Report Accuracy	5
Fault Origin	Caller ID system in demo mode or was hacked.
Source Infrastructure	Telephone infrastructure.
Affected Infrastructures	Telephone infrastructure..
Affected Industry Sectors	Home users.
Comment	Software configuration problem or system was hacked.

D.6	AOL netwoes			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
8/7/1996	USA	High	No	Unknown
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	Unknown	Unknown	No	Unknown

AOL's computer systems (near the Dulles Airport facility in Virginia) went down at 4 a.m. EDT on August 7, 1996. Service was reportedly restored sporadically 19 hours later, around 11 p.m. EDT. The crash was caused by new software installed during a scheduled maintenance update. Earlier in the same week an AOL representative had said that AOL computers are "virtually immune" to this kind of outage.

Report Source	*San Francisco Chronicle, August 8, 1996, p.A1; RISKS (18, 30).*
Report Accuracy	6
Fault Origin	Software configuration problem.
Source Infrastructure	Data Network.
Affected Infrastructures	Commercial and non commercial subscribers of the ISP (AOL)
Affected Industry Sectors	Almost all commercial and non commercial AOL subscribers.
Comment	Lack of proper planning.

D.7	Does CNID blocking really give you anonymity?			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
1/1/1997	USA	Low	No	No
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	26 days	Unknown	No	Unknown

From the time of an upgrade on Jan 1 1997 until 26 Jan 1997, the mechanisms that are supposed to block the Calling Number ID (misnamed Caller ID) service FAILED in the 510 and 415 areas codes. As many as 516 businesses with PBXs were able to obtain calling numbers despite presumed blocking. (Something on the order of 50subscribers is rumored to have requested blocking.)

Report Source	*San Francisco Chronicle, February 14, 1991; RISKS (18, 82).*
Report Accuracy	6
Fault Origin	Software glitch.
Source Infrastructure	Telephone Infrastructure.
Affected Infrastructures	Telephone infrastructure
Affected Industry Sectors	Financial and Trading Industries.
Comment	Software glitch.

D.8	**NY Stock Exchange halted for one hour**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
12/18/1995	USA	High	No	No
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Unintentional	1 hour	Unknown	No	1

The New York Stock Exchange opened an hour late on December 18, 1995, after a weekend spent upgrading the system software. At 9:15 a.m. on Monday, it was discovered that there were serious communication problems in the software between the central computing facility and the specialists' displays. The problem was diagnosed and fixed by 10:00 a.m., and the market reopened at 10:30 a.m. It was the first time since December 27, 1990, that the exchange had to shut down. The Chicago Mercantile Exchange, Boston Stock Exchange, and Philadelphia Stock Exchange all waited until the NYSE opened as well. (The monster snowstorm on January 8, 1996 subsequently caused a late start and an early close.

Report Source	*RISKS (17, 55).*
Report Accuracy	6
Fault Origin	Software configuration problem..
Source Infrastructure	Information Technology Infrastructure
Affected Infrastructures	Data network
Affected Industry Sectors	Financial and Trading Industries.
Comment	Network problem, detail not known. Possibly software configuration problem.

D.9	**”IP spoofing” SYN flooding attacks**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
12/14/1996	USA	High	No Information	Yes
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Intentional	40 hour	Unknown	No	3000+

Public Access Networks Corporation (Panix) was inundated with a massive attack on its network, flooded with up to 150 bogus ”electronic handshake” SYN requests per second. Network tables overflowed because the SYN transactions were intentionally never completed. A 200-message-per-second SYN-flood attack was launched against WebCom, a large WorldwideWeb service provider in San Francisco Bay Area. The denial of service affected more than 3000 Web sites for 40 hours, during most of what was otherwise a very busy shopping weekend. The attack began on December 14, 1996, shortly after midnight PST.

Report Source	*Elizabeth Weise, High-Tech Attack Shuts Down Web Provider in Santa Cruz, an AP item seen in the San Francisco Chronicle, December 17, 1996, C18; RISKS (18, 45 48 and 69).*
Report Accuracy	6
Fault Origin	Malicious attack on data network infrastructure.
Source Infrastructure	Information Technology Infrastructure
Affected Infrastructures	Data network and connected systems.
Affected Industry Sectors	Wide range of industrial sectors connected to Internet.
Comment	DoS attacks are well known problem for data networks.

D.10	**Denial-of-service attack**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
11/9/1995	USA	Medium	No Information	Yes
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Intentional	44 hour	Unknown	No	1

A student at Monmouth University in New Jersey was charged with disrupting the school's electronic mail system for five hours by bombarding two administrators with 24,000 e-mail messages. The student's computer access had been terminated on November 9, 1995, because of posting advertising and business-venture solicitations to "inappropriate sections of the Internet" (presumably, Usenet groups). It took 44 hours to trace the source of the attack through a service provider in Atlanta, Georgia, and back to an account based in Red Bank, New Jersey, shared by the student. The student is being charged with a federal crime because of using interstate communication to deny service. Carl Stern of the Justice Department is said to have remarked that this was the first time the federal computer-fraud act had been used for an act of this type

Report Source	*Asbury Park Press, James W. Roberts, November 29, 1995, front page; James E. Burns, RISKS (17, 49)*
Report Accuracy	6
Fault Origin	Malicious attack targeted to the email system.
Source Infrastructure	Information Technology Infrastructure
Affected Infrastructures	Data network and connected systems.
Affected Industry Sectors	Educational institution.
Comment	DoS attack from an insider.

D.11	**Internet worm exposed**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
11/2/1988	Worldwide	High	No Information	Unsure
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Intentional	Unknown	Unknown	Yes	60000

2 November - Internet worm burrows through the Net, affecting 6,000 of the 60,000 hosts on the Internet. Computer Emergency Response Team (CERT) formed by DARPA in response to the needs exhibited during the Morris worm incident. The worm is the only advisory issued this year.

Report Source	*Hobbes' Internet Timeline*
Report Accuracy	7
Fault Origin	Vulnerability in the host machines.
Source Infrastructure	Information Technology Infrastructure
Affected Infrastructures	Almost all vulnerable parts of Internet.
Affected Industry Sectors	Wide range of industrial sectors connected to Internet.
Comment	First, know worm attack in the Internet. Worm attack becomes faster and more damaging over time.

D.12	**Denial of service attack against major e-commerce sites**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
2/5/2000	USA	High	No Information	Yes
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Intentional	Unknown	Unknown	No	4+
A massive denial of service attack was launched against major web sites, including Yahoo, Amazon, and eBay in early February.				

Report Source	*Hobbes' Internet Timeline*
Report Accuracy	7
Fault Origin	Malicious attack targeted to major web sites.
Source Infrastructure	Information Technology Infrastructure
Affected Infrastructures	Information Technology Infrastructure.
Affected Industry Sectors	Major e-commerce sites.
Comment	DOS attack remains serious problem in Internet reliability.

D.13	**Code Red worm exposed**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
7/13/2001	Worldwide	High	No Information	Unsure
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Intentional	30+ days	Unknown	Yes	Unknown
Code Red worm and Sircam virus infiltrate thousands of web servers and email accounts, respectively, causing a spike in Internet bandwidth usage and security breaches (July)				

Report Source	*Hobbes' Internet Timeline*
Report Accuracy	7
Fault Origin	Vulnerabilities in the host machines.
Source Infrastructure	Information Technology Infrastructure
Affected Infrastructures	A significant part of the Internet.
Affected Industry Sectors	Wide range of industrial sectors connected to Internet
Comment	Worm attack is a major problem in the Internet.

D.14	**DDoS against DNS root servers**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
10/23/2002	Worldwide	High	No Information	Yes
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Intentional	Unknown	Unknown	Yes	8
A distributed denial of service (DDoS) attack struck the 13 DNS root servers knocking out all but 5 (21-23 Oct). Amidst national security concerns, VeriSign hastens a planned relocation of one of its two DNS root servers				

Report Source	*Hobbes' Internet Timeline*
Report Accuracy	7
Fault Origin	Malicious attack targeted to core of the Internet infrastructure.
Source Infrastructure	Information Technology Infrastructure
Affected Infrastructures	Wide part of the Internet.
Affected Industry Sectors	No information.
Comment	

D.15	**SQL Slammer worm exposed**			
Date	**Country**	**Severity**	**Network Trace**	**Simulation**
1/25/2003	Worldwide	High	No Information	Unsure
Fault Type	**Duration**	**Financial Impact**	**Public Safety**	**Affected Sites**
Intentional	Unknown	Unknown	Yes	Unknown
The SQL Slammer worm causes one of the largest and fastest spreading DDoS attacks ever. Taking roughly 10 minutes to spread worldwide, the worm took down 5 of the 13 DNS root servers along with tens of thousands of other servers, and impacted a multitude of systems ranging from (bank) ATM systems to air traffic control to emergency (911) systems (25 Jan). This is followed in August by the Sobig.F virus (19 Aug), the fastest spreading virus ever, and the Blaster (MSBlast) worm (11 Aug), another one of the most destructive worms ever				

Report Source	*Hobbes' Internet Timeline*
Report Accuracy	7
Fault Origin	Varieties of worm attack by exploitation of the vulnerabilities of the host machines.
Source Infrastructure	Information Technology Infrastructure
Affected Infrastructures	Significant part of the Internet.
Affected Industry Sectors	Wide range of industrial sectors.
Comment	

4.5 Statistical Results:

In this section, we present simple statistical findings of our reports.

	Physical/Link		**Packets**		**Network Connectivity**		**Subscribers**		**Total**	
Total/category	16	42%	1	3%	6	16%	15	39%	38	100%
Type										
Intentional	1	6%	1	100%	1	17%	8	53%	11	29%
Unintentional	13	81%	0	0%	5	83%	7	47%	25	66%
Unknown	2	13%	0	0%		0%		0%	2	5%
Severity										
High	15	94%	1	100%	3	50%	9	60%	28	74%
Medium	1	6%	0	0%	2	33%	2	13%	5	13%
Low	0	0%	0	0%	1	17%	4	27%	5	13%
Impact										
US/Canada	9	56%	1	100%	5	83%	11	73%	26	68%
Other	7	44%	0	0%	1	17%	4	27%	12	32%
Public Safety										
Concern	8	50%	1	100%	2	33%	6	40%	17	45%
No Concern	6	38%	0	0%	4	67%	9	60%	19	50%
Unknown	2	13%	0	0%	0	0%		0%	2	5%

5 Discussion

The fault cases we have selected are mostly related to CITI failure. As such, this selection process is not purely random. However, while classifying these reports into different categories (layers), we did not have any apriory knowledge of their distribution. As such, this process can be considered unbiased. Given this background, from the results of Section 4.5, we can infer several conclusions. It appears that infrastructure faults have major impacts on all connected systems. Most of the time, faults in the lower layer (e.g., device failure or link failure) are more severe than the upper layer (considering severity and public safety factor). Affected industry sectors, in most cases are the direct subscribers to the respective service(s). Since one infrastructure is related to another infrastructure in a complex way [17], there might have long lasting impact on other infrastructures for each of these faults. A big number of faults belong to unintentional category, which implies lot of reliability issues those need to be taken care of. High number of faults in North America is due to our excessive reliance on CITI infrastructure, than any other region of the world. Many of the faults have public safety implication, which signify CITI faults need to be taken seriously.

6 Conclusions

In this report, we have proposed a systematic approach to study CITI fault cases. We have used this approach to study a number of fault cases and made quantitative findings about CITI fault trends and their impacts. This method will be useful for the infrastructure research community to classify and interpret vast amount of public domain data.

References

1. Juan M. Estevez-Tapiador, Pedro Garcia-Teodoro, Jesus E. Diaz-Verdejo, "Anomaly detection methods in wired networks: A survey and taxonomy", Computer Communications, v 27, n 16, Oct 15, 2004, p 1569-1584
2. Eugene H. Spafford, Congressional Testimony, 10 October 2001, http://www.house.gov/science/full/oct10/spafford.htm
3. Peter G. Neumann, Computer-Related Risks, Addison-Wesley Professional; 1st edition (October 18, 1994), ISBN: 020155805X http://www.csl.sri.com/users/neumann/risks-new.html (2nd Edition - Online)
4. John D. Howard,"An analysis of security incidents on the Internet 1989-1995", Ph.D. Thesis, Carnegie Mellon University, 1997
5. John D. Howard, Thomas A. Longstaff, "A Common Language for Computer Security Incidents", Sandia National Laboratories techinical report SAND98-8997, 1998.
6. Anirban Chakrabarti, G. Manimaran, "Internet infrastructure security: A Taxonomy", IEEE Network, v 16, n 6,November/December, 2002, p 13-21

7. David M. Nicol, William H. Sanders, Kishor S. Trivedi, "Model-based evaluation: From dependability to security", IEEE Transactions on Dependable and Secure Computing, v 1, n 1, January/March, 2004, p 48-64
8. Alexander A.Hagin, "Performability, Reliability, and Survivability of Communication Networks: System of Methods and Models for Evaluation", Proceedings - International Conference on Distributed Computing Systems, 1994, p 562-573
9. Andrew S. Tanenbaum, "Computer Networks", Prentice Hall; 3rd edition, 6 March 1996, ISBN: 0133499456
10. B.E.White,"Layered communications architecture for the Global Grid", Proceedings of IEEE Military Communications Conference MILCOM, v 1, 2001, p 506-511
11. Jeffrey Hightower, Barry Brumitt, Gaetano Borriello. "The Location Stack: A Layered Model for Location in Ubiquitous Computing," Fourth IEEE Workshop on Mobile Computing Systems and Applications, 2002, p. 22
12. Laurent Ciarletta, Alden Dima. "A Conceptual Model for Pervasive Computing," International Conference on Parallel Processing Workshops (ICPPW 2000), p. 9
13. Edward E. Balkovich, Robert H. Anderson, "Critical Infrastructures Will Remain Vulnerable: Neighbourhoods Must Fend for Themselves", International Journal of Critical Infrastructures, 2004 - Vol. 1, No.1 p. 8 - 19
14. The RISKS Forum: http://catless.ncl.ac.uk/Risks
15. Hobbes' Internet Timeline http://www.ietf.org/rfc/rfc2235.txt http://www.zakon.org/robert/internet/timeline/ (current version)
16. NS2 - Network Simulator http://www.isi.edu/nsnam/ns/
17. Steven M. Rinaldi, James P. Peerenboom, Terrence K. Kelly,"Identifying, understanding, and analyzing critical infrastructure interdependencies", IEEE Control Systems Magazine, v 21, n 6, December, 2001, p 11-25