


**Author(s):** Arreymbi, Johnnes.
**Article title:** Modelling to Enhance GSM Network Security
**Year of publication:** 2006
**Citation:** Arreymbi, J. (2006) 'Modelling to enhance GSM Network Security.' Proceedings of the International Conference on Security and Management (SAM'06), Las Vegas, USA, CSREA Press pp. 252-260
**Link to published version:**
http://ww1.ucmss.com/books/LFS/CSREA2006/SAM5086.pdf

# Modelling to Enhance GSM Network Security

Johnnes Arreymbi
School of Computing and Technology
University of East London
Essex, RM8 2AS
Email: j.arreymbi@uel.ac.uk

## Abstract

*With the rapid development in global communication networks, the threat of security and in particular that of cellular telecommunication system is real and highly dangerous. Mobile phone and other wireless device usage is increasing daily with ground breaking technological developments – in design, style, content and micro-chips performance. The contents of the multimedia packages – conversation (audio), text, graphics, colour, and video messages - delivered may be very important and confidential. Such confidentiality needs to be protected. Any interference and interceptions in the communication process would bring about reduced system usage and development benefits. This paper discusses the several aspects of security of GSM and takes into consideration the fact that World-wide GSM usage is very high. It will also look at how GSM protects the data from interception by authentication, encryption, and ciphering. Some likely flaws in these security methods will be explored and possible measures suggested to curb the security flaws.*

***Keywords:*** *GSM, Network Security, Authentication, Encryption, Ciphering, Multimedia, Mobile devices*

## 1. Introduction

Nowadays, millions of people use mobile phones over radio links for communication any time any where, for business and /or convenience [18]. The Global System for Mobile communication or Group Special Mobile (GSM) platform which was formed in 1982 [1] is a hugely successful wireless technology and an unprecedented invention of global achievement. Research has shown that at the end of Jan 2004 [2] there were over 1 billion GSM subscribers across more than 200 countries World-wide and the figures are increasing even more, especially in Africa and other advancing economies where mobile communication uptake has increased by 65% [17].

The passage of time has moved wireless tele-communication some steps further. In the older analog-based cellular telephone systems such as the Advanced Mobile Phone System (AMPS) and the Total Access Communication System (TACS) [3], cellular drop rate, interference/interception rate and general fraud on such systems was extensive. It was very simple and easy for a radio hobbyist to tune in and hear mobile telephone conversations. Mostly, without any encryption [4], the voice and user data of the subscriber was in raw form sent to the network. SIM card cloning too was very easy and they together posed dangerous threat to the users. Such fatal flaws in the mobile phone technologies were all prevalent [5]. To prevent such flaws in mobile communication and to make mobile phone traffic more

secure, GSM became an apparent and relevant solution. GSM operates in the 900MHz, 1800MHz, or 1900 MHz frequency bands which in essence provide a secure and confidential method of communication.

The prevalence of GSM technologies, together with the introduction of multimedia content delivery, provided means for users to begin to enjoy some of the benefits of having stable, continuous, private and secure environments for conversations or text messages through GSM network systems [18]. But how safe and secure is the GSM technology? Can it really protect vitally important information? The first section would review the security and encryption in GSM systems. Section two tends to deal with designing a security model for GSM optimization and giving some descriptions of the model. Some of the flaws and possible measures of the GSM technologies would be covered in section three. Section four would give an evaluative critique and conclusion to this paper.

## 2. Security and Encryption in GSM system

All cellular communication operates using air waves which can easily be intercepted with easily available suitable eavesdropping receivers. Taking account of this, GSM integrated some security controls [6] in order to make the cellular system as secure as a fixed line phone, which offers some level of physical security such that physical access is needed to the phone line for listening in. This kind of control measures keeps the conversation between two mobile phone users from being insecure. According to GSM specification 02.09 [6], the security functions put in place are authentication of a user, data and signaling confidentiality and Confidentiality of a user. Authentication of a user means that mobile phone can prove that it has access to a particular account with the operator. In other words, a person is not allowed to personate certain subscriber to use that person's account. This function proves very important in protecting all subscribers' cellular air-time fee and other benefits.

Data and signaling confidentiality can be more appropriately understood. This function is to make sure that all signaling and user data such as text messaging and speech are protected against interception by means of ciphering. Confidentiality of a user function keeps the unique IMSI, - International Mobile Subscriber Identity – and prevents it from being disclosed and displayed in plaintext to avoid leaving track of the user. It means that intruders cannot easily track certain subscriber of the GSM system.

Besides the above security functions, there are other functions that proves to make the mobile phone secure. The most commonly known protective system is that of the PIN which GSM system provides. In this is a kind of security method, if a user fails to provide a valid PIN number, the system would not allow the user to continue to perform any other authentication functions. And, in order to distribute the authentication and ciphering information throughout the network, the root key of all ciphering key generation and authentication, Ki [4] have to be distributed by another form known as vectors. This too adds another security level in our proposed security model as would be highlighted below. These two functions have been added to our designed security model for improved GSM security.

Proposed Model for improve GSM Security.

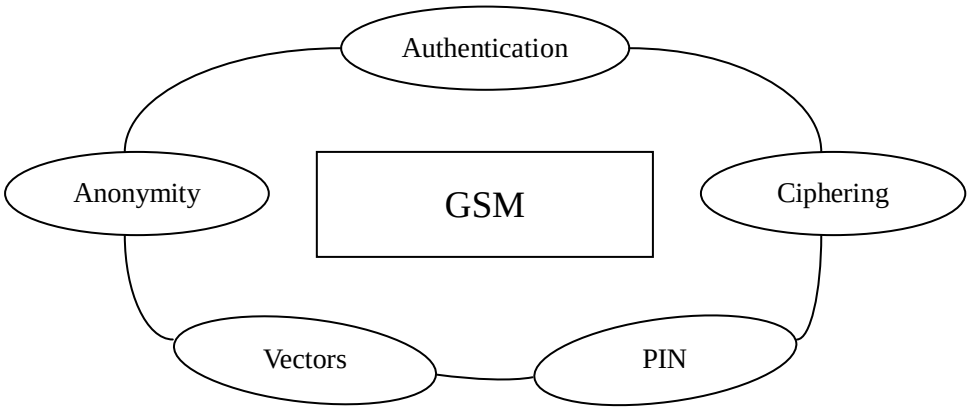


Figure 1. Security model

GSM networks utilize Encryption for three purposes [7]: authentication, encryption and key generation, which would be discussed later.

## 2.1 Authentication

Like the authentication in network security, this service is concerned with assuring that a communication is authentic. It can prohibit an unauthorized user logging into the network claiming to be a bonafide mobile subscriber [6]. In order to ascertain the position, some kind of challenge needs to be issued by the network and which the mobile station (MS), such as mobile phone, must respond to correctly. And if all fails, the unauthorized user therefore fails to personate the bonafide subscriber because of the challenge in order to connect to the network. Others such as the SIM card, A3 Algorithm IMSI and Ki provide certain levels of security as would be discussed.

The SIM (Subscriber Identity Module) card is a small smartcard with embedded micro- chip which is inserted into the GSM phone and provides the appropriate details of an account. The SIM card includes the information which is necessary to get access to a particular account. Some of which are: IMSI (International Mobile Subscriber Identity), and Ki (Individual Subscriber Authentication Key) etc. The IMSI is a sequence of 15-digit code, used to identify an individual GSM MS to a GSM network. It seems like an ID card of a person. The format of IMEI is AABBBB--CC-DDDDDD-E and it denotes basic coded identifier information as shown in the table 1 below.

| | |
|---|---|
| AA | Country Code |
| BBBB | Final Assembly Code |
| CC | Manufacturer Code |
| DDDDDD | Serial Number |
| E | Unused |

Table 1. The format of IMEI [9]

Ki is utilised as a highly protected secret key shared between the MS and the HLR (Home Location Register) of the subscriber's home network [10]. It is a randomly generated 128-bit number and all keys and challenges used in the GSM system are generated according to Ki. Also used in authentication is the A3 algorithm. The figure below shows the A3 algorithm procedure.

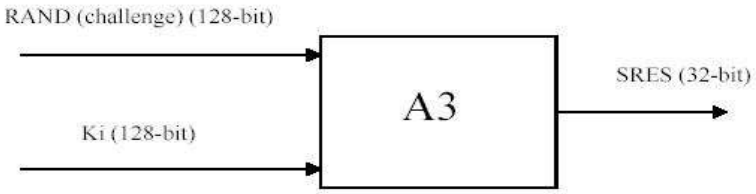


Figure 2. A3 algorithm [6]

In this procedure, two 128-bit input codes are calculated by A3 algorithm and then a 32-bit output code is generated. However, A3 algorithm does not refer to a particular algorithm; it is rather the algorithm the operator has chosen to be implemented for authentication. The most common implementations for A3 are COMP128. The authentication procedure can simply be described as: mobile phone provides the Ki to network and the latter could verify the Ki to prove the mobile phone is not the impersonated one. However, this is highly insecure because the Ki could be intercepted by an eavesdropper. If Ki is lost, the authentication will disappear because the eavesdropper will personate that subscriber by providing the same Ki.

In such situations, the GSM technology provides a better method to resolve such a problem. The network generates a 128-bit random number, RAND [10] which is 128-bit random challenge generated by the Home Location Register (HLR). It then uses the A3 algorithm (see figure 2) to generate an authentication sign, SRES [10] which is the 32-bit Signed Response generated by the MS and the Mobile Services Switching Center. After the generation of SRES, the network then sends the RAND to the phone. The phone in response then do the same, by generation of 32-bit SRES and the transmitting of the SRES back to the network for comparison. Authentication is complete and becomes successful only when the two values of SRES match, which enables the subscriber to then join the network. If authentication fails the first time, the network may choose to repeat the authentication with the IMSI. If that fails, the network releases the radio connection. The mobile then considers that SIM to be invalid. Therefore, the protection of Ki is provided. And in case an eavesdropper intercepts the RAND, no relevant information can be retrieve by listening to the channel because every time a new RAND number is generated.

## 2.2 Ciphering

It is highly important that providers keep user data and signaling data from interception by ciphering. The GSM system uses symmetric cryptography. And as we know, in symmetric cryptography, the data is encrypted using an algorithm and the ciphering key. In GSM systems, the ciphering key is named Kc. Kc is the 64-bit ciphering key [10] and used as a Session Key for encryption of the air channel. Kc is generated by the MS from the RAND presented by the GSM network and the Ki from the SIM utilizing the A8 algorithm. Like symmetric cryptography, this same Kc is needed by the decryption algorithm to decrypt the data. The idea is that the Kc should only be known by the phone and the network. If this is

the case, the data is meaningless to anyone intercepting it. AS I mentioned above, the A8 algorithm uses the RAND and Ki as input to generate a 64-bit ciphering key (see figure 3), Kc which is then stored in the SIM and readable by the phone [11]. Like the SRES, the network also generates the Kc and distributes it to the base station (BTS) handling the connection.

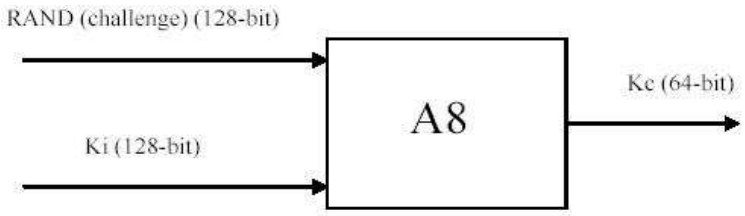


Figure 3. A8 algorithm [6]

Then, the A5 algorithm uses the 64-bit cipher key [12] derived from the 128-bit authentication key by the A8 algorithm in the SIM card to perform the encryption. The A5 algorithm is also 'seeded' by the value COUNT [6], which is sequentially applied to each 4.615ms GSM frame (see figure 4).

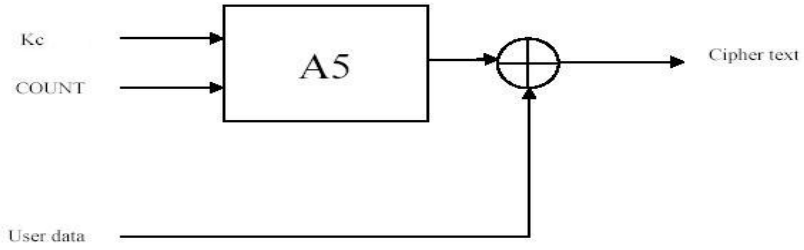


Figure 4. A5 algorithm [6]

Currently there are 3 algorithms defined for ciphering algorithms – A5/1, A5/2 and A5/3 [6]. A5/1 and A5/2 were the original algorithms defined by the GSM standard. A5/2 was a deliberate weakening of the algorithm for certain export regions, where A5/1 is used in countries like the US, UK and Australia. A5/3 was added in 2002 and is based on the open Kasumi algorithm defined by 3GPP. The output of A5 algorithm is the cipher text which is very secure and can not be easily decrypted by eavesdroppers.

## 2.3 Anonymity

Anonymity is a process set to make it difficult to track a mobile phone user of the system. According to Srinivas [13], when a new GSM subscriber switches on his/her phone for the first time, its International Mobile Subscriber Identity (IMSI), for example real identity, is used and a Temporary Mobile Subscriber Identity (TMSI) is issued to the subscriber, which from then on is always used. Once ciphering has commenced the initial TMSI is allocated. The VLR controlling the LA in which the TMSI is valid maintains a mapping between the TMSI and IMSI such as that the new VLR (if the MS moves into a new VLR area) can ask the old VLR who the TMSI (which is not valid in the new VLR) belonged to (See figure 5, 6) [6]. Use of this TMSI, prevents the recognition of a GSM user by the potential eavesdropper. To track a GSM user via the TMSI, an eavesdropper must intercept the GSM network communication where the TMSI is initially negotiated. In addition, because the TMSI is frequently changed, the eavesdropper must intercept each additional TMSI changing session.

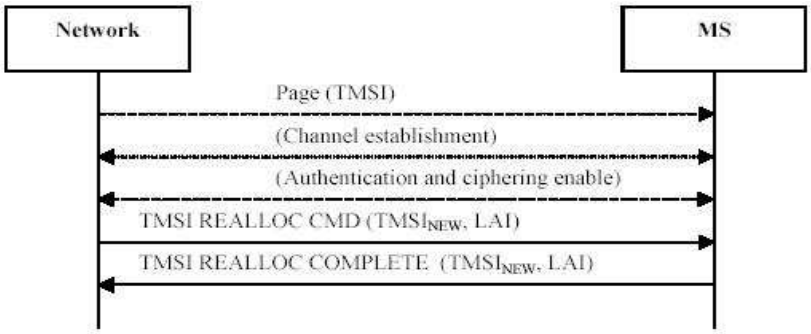


Figure 5. Allocating a new TMSI [6]

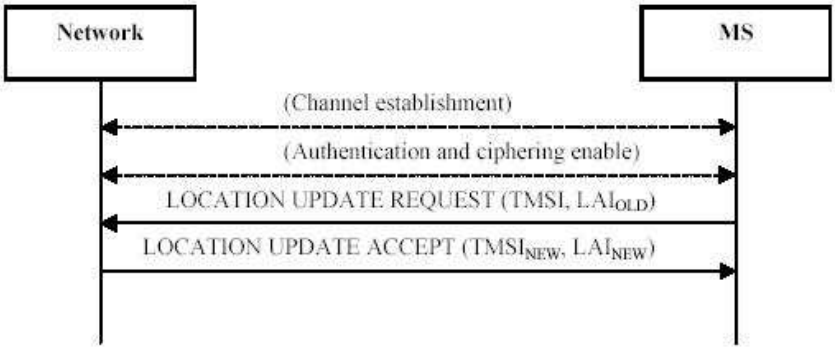


Figure 6. Allocating a new TMSI [6]

The TMSI is updated at least during every location update procedure such as when the phone changes LA or after a set period of time. The TMSI can also be changed at any time by the network. The new TMSI is sent in ciphered mode whenever possible so an attacker cannot maintain a mapping between an old TMSI and a new one [6]. The TMSI is valid in the location area in which it was issued. For communications outside the location area, the Location Area Identification (LAI) [14] is necessary in addition to the TMSI.

## 2.4 The transmitting of authentication vectors

As we know, the Authentication Centre (AuC), which is a part of Home Location Register (HLR), stores the SRES, Kc and RAND that I discussed above for every particular subscriber.
If the subscriber is roaming, the foreign GSM database known as VLR (Visitor Location Register) would learn the Ki from HLR [13]. So there is insecure that Ki transfers directly from HLR to VLR because of interception. However, the HLR distributes authentication vectors [6], including a valid SRES, Kc and RAND for the particular IMSI the VLR has specified. So the data which are transmitted are not Kis but other authentication and ciphering information so that the Ki is protected.

## 2.5 The security in the SIM

Every body knows that the SIM itself is protected by an optional PIN. It looks like an ATM PIN can keep the ATM card secure. After inputted by the phone's keypad, the PIN is passed to the SIM for

verification. If the code inputted by certain user does not match with the PIN which is stored by the SIM, then it claims that the code was invalid and fails to perform authentication functions [8] unless the correct PIN is entered. Furthermore, after user inputs the wrong PIN number three (3) times, the PIN will be locked out. A pin Unlock named PUK is required to be entered and if the PUK is correct, then the PIN will be unlocked. But if the PUK is entered incorrectly a 10 times, it is terrible that the SIM refuses local access to privileged information permanently, making the SIM useless.

# 3. Flaws and Remedies to the GSM security

Some of the security algorithms discussed above tend to provide the GSM system with some security, and it may seem that such a GSM system is protected absolutely. However, when reality comes into play, and technologies become commonly available, the systems also becomes even more vulnerable and complicated, as more people begin to find flaws in the GSM security. From developmental point of view, these flaws could be resolved by specialists as the GSM specifications have gradually improved. Other new technologies such as GSM 1800, HSCSD, GPRS and EDGE have been added to enhance GSM system [3]. And, the 3rd generation (3G) technologies such as UMTS [6] have also been used to improve the security in GSM. This section will explore some of the network security issues.

## 3.1 Using UMTS technology.

In the GSM network systems, it is unbelievable that the authentication procedure does not require the network to prove its knowledge of the Ki or any other authentication context to the mobile phone. Therefore, it is possible for an attacker to set up an impersonated mobile base station with the same Mobile Network Code as the user's network. And with this, all calls or text messages sent by the subscriber could easily be intercepted. The Universal Mobile Telecommunications System (UMTS) is the world's choice for 3rd Generation wireless service delivery [15], as defined by the International Telecommunications Union (ITU). With the UMTS technology, it is near impossible for an attacker to mimic or imitate the network in terms of a 2-way authentication procedure. The procedure for which the mobile authenticates itself to the network is almost the same as GSM. But in UMTS, the network also sends an Authentication Token known as AUTN along with the RAND. The AUTN contains the MAC code, which works much like the GSM SRES but in the opposite direction. Therefore, if the MAC sent by the network does not match the MAC calculated by the SIM, the phone respond by sending an authentication reject message to the network and the connection is then terminated.

## 3.2 Enhancement of Common implementation of A3/A8 Algorithms

As earlier discussed, the common implementation of the A3 and A8 algorithms is concerned with a single algorithm - COMP128; which generates the 64-bit Kc and the 32-bit SRES from the 128-bit RAND and the 128-bit Ki input. This algorithm has been found to be insecure, because as it is, the RANDs will provide enough information for an attacker to determine the Ki in significantly less than the ideal number of attempts. Earlier attacks based on repeated 2R attacks [6] could typically crack a SIM in approximately 217 RANDs. Increasingly too, some users have found it useful to 'clone' several of their SIMs [16] onto a single programmable smartcard. The common implementation of A3/A8, COMP128 has another flaw. This is almost certainly a deliberate weakening in that, when generating

the 64-bit Kc, it always sets the least significant 10 bits of the Kc to 0 [3]. This effectively reduces the strength of the data ciphering algorithm to 54 bits, regardless of which ciphering algorithm is used. Therefore, faced with the above insecurity, the newer implementations of A3/A8 have been introduced such as COMP128-2 and COMP128-3 [6] to help alleviate the problems. So far these algorithms have held up reasonably well, however, they are still a mystery as they are developed in secret. COMP128-2 still has the deliberate 10-bit weakening of the ciphering Kc however. COMP128-3 is the same basic algorithm without this weakening such as a truly 64-bit Kc. In fact, the new algorithms of COMP128-2 and COMP128-3 have managed to stop SIM cloning and have also made the serious over the air Ki extraction difficult and unfeasible, even if they do not approach the ideal strength of 2128.

### 3.3 Exploiting the A5/3, A5/1 and A5/2 algorithms

The A5/1 output is based on the modulo-2 which is performed using an exclusive OR known as xor operation summed output of 3 LFSRs whose clock inputs are controlled by a majority function of certain bits in each LFSR. However, the attack exploits flaws [15] in the algorithm and A5/1 could be cracked in less than 1 second on a typical PC. A5/2 is a deliberately weakened version of A5/1, which has been demonstrated to be also flawed. A5/2 can be cracked on the order of about 216, and thus is even weaker than A5/1. GSM supports up to 7 different algorithms for A5 ciphering. Until recently, only the A5/1 and A5/2 algorithms were used. In 2002, GSM added a much stronger algorithm A5/3 which is based on the Kasumi core which is the core encryption algorithm for UMTS [6]. However, only few networks and handsets support this algorithm currently.

## 4. Conclusion

In this paper, many algorithms have been implored to demonstrate that the mechanisms of security in the GSM specification maintain some level of security in the cellular telecommunications system. The measures used in the GSM such as authentication, ciphering and anonymity give the mobile phone users some privacy and anonymity, in addition to protecting the system from the fraudulent use. However, we have also seen some weaknesses in the security of GSM. There are flaws such as in COMP128, A5/1 and so on. These vulnerabilities could be used by attacker to intercept the contents of conversations or text messages. Some measures have also been explored to prevent these flaws to an extent and imploring new technologies and algorithm to take care of the weaknesses in GSM security. Although new measures by which the security of GSM is protected are introduced, it could be said that, with the increase of time, attackers may find out other vulnerabilities of these and handle them like the relation between virus and anti-virus. In fact, there is no silver bullet to curb GSM vulnerabilities and also no perfect product that can be said to be very secure. Having said all these, GSM is the most secure, readily available and globally accepted wireless system with public standard to date. It could be made more secured by implementing appropriate security measures in certain areas. Furthermore, with the expanding developments in the GSM technology, it is believed that, more secured methods will come into play and used in the system to give it appropriately better security.

**Reference:**

[1] GSM Tutorial, International Engineering Consortium, 2004, http://www.iec.org/online/tutorials/gsm/topic02.html

[2] Today's GSM, 2005, http://www.gsmworld.com/technology/gsm.shtml

[3] Priyanka Agarwal, Security of GSM System, Jan. 2005, Distribution Source: Article Warehouse.

[4] Chengyuan Peng, GSM and GPRS security, (24th Oct. 2004) http://www.tml.hut.fi/Opinnot/Tik-110.501/2000/papers/peng.pdf

[5] Charles Brookson, Can you clone a GSM Smart Card (SIM)? July 2002, http://www.brookson.com/gsm/clone.pdf

[6] Jeremy Quirke, Security in the GSM system, May 2004

[7] How is encryption utilized in GSM? 2004, http://www.gsm-security.net/faq/gsm-encryption.shtml

[8] SIM card, GSM system, Chapter 7, http://www.mc21st.com/techfield/systech/gsm/g7-4.htm

[9] What is an IMEI? 2004, http://www.gsm-security.net/faq/imei-international-mobile-equipment-identity-gsm.shtml

[10] What are Ki, Kc, RAND, and SRES? http://www.gsm-security.net/faq/gsm-ki-kc-rand-sres.shtml

[11] Secure Mobile Communication, Oct. 2003, http://www.dcs.warwick.ac.uk/~esvvv/docs/specification_10-10-03.pdf

[12] Comparison of Airlink Encryptions, 2003, http://www.qualcomm.com/technology/1xev-do/webpapers/wp_Airlink_Encryption.pdf

[13] Srinivas, The GSM Standard (An overview of its security), Oct. 2004, http://www.sans.org/rr/papers/index.php?id=317

[14] Yong LI, Yin CHEN, Tie-Jun MA, Security in GSM, 2003, http://www.gsm-security.net/papers/securityingsm.pdf

[15] Biryukov, Shamir, Wagner, Real Time Cryptanalysis of A5/1 on a PC, http://www.cs.berkeley.edu/~daw/papers/a51-fse00.ps

[16] Have the A3 and A8 algorithms been broken? http://www.gsm-security.net/faq/gsm-a3-a8-comp128-broken-security.shtml

[17] International Telecommunication Union (ITU) (2004), African Telecommunication Indicators 2004. http://www.itu.int/ITU-D/ict/publications/africa/2004.

[18] Arreymbi, J. (2002), Issues in Delivering Multimedia Content to Mobile devices, In Proceedings of the 6th International Conference on Information Visualization. IEEE, Computer Society, London 2002.