01 Jan 2004

An Overview of Security Issues in a Digital City

Bonnie Yates

An Overview of Security Issues in a Digital City

Bonnie Yates, Department of Information, Science and Technology, School of Management & Information Systems, University of Missouri – Rolla, Rolla, MO 65401, email: bjyrg7@umr.edu

Faculty Advisor: Dr. Bih-Ru Lea, School of Management & Information Systems, University of Missouri – Rolla, Rolla, MO 65401, email: leabi@umr.edu

Abstract

This paper addresses what a digital city is, the advantages a digital city provides and how security must be considered when developing and deploying a digital city. Digital cities provide a dynamic living space that cannot be founded on static technology. Instead it must have its foundation on dynamic technology. Included in dynamic technology is security, which is a common thread among digital cities. Without proper security, digital cities cannot expand to their full potential.

1. Introduction

Digital Cities are not just about globalizing businesses and earning companies more profit. It is also about creating rich information spaces for everyday life. Security is becoming a focal point for designing, developing, and deploying software security [10]. Security is the one common thread that runs through most of the articles available on digital cities. Security must be a high priority in order for Digital Cities to become fully functional and to be used as they are intended. While the Internet makes research and businesses global, life is inherently local. The Internet is no longer just for universities and businesses; but is now becoming a fixture in everyday life [3]. Each digital city has its own goal and uses different means in obtaining those goals.

This paper addresses what a digital city is, the advantages a digital city provides and how security must be considered when developing and deploying a digital city.

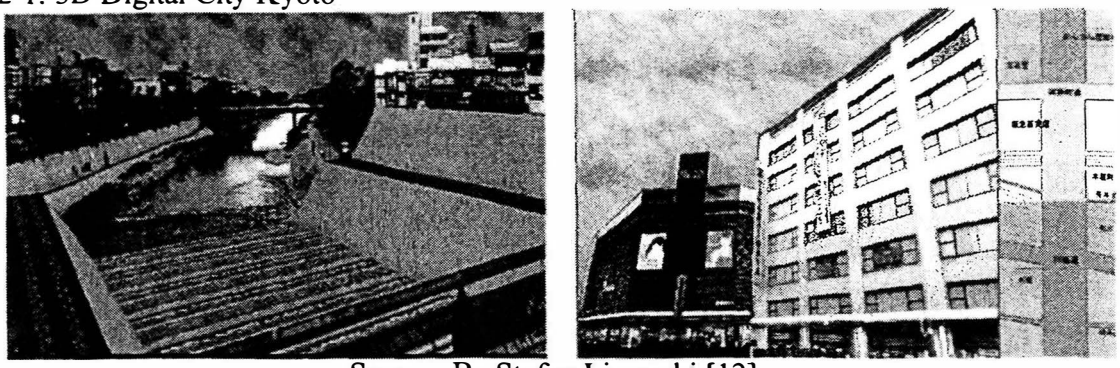
2. Digital City Overview

What is a digital city? A digital city is the virtual representation of a physical city, such as a real city, town or village, on the Internet through applications of advanced information and communication infrastructure [5]. For example, Digital City Kyoto establishes a strong connection and representation to physical Kyoto, as shown in Figure 2-1 [1].

Citizens of a digital city can share knowledge, experience and mutual interests [3]. Services offered by a digital city include all kinds of information about the real city [5], possibilities for communication and social interaction [5], access to social environments, community services, municipal information and e-commerce [4], and opportunities to engage in

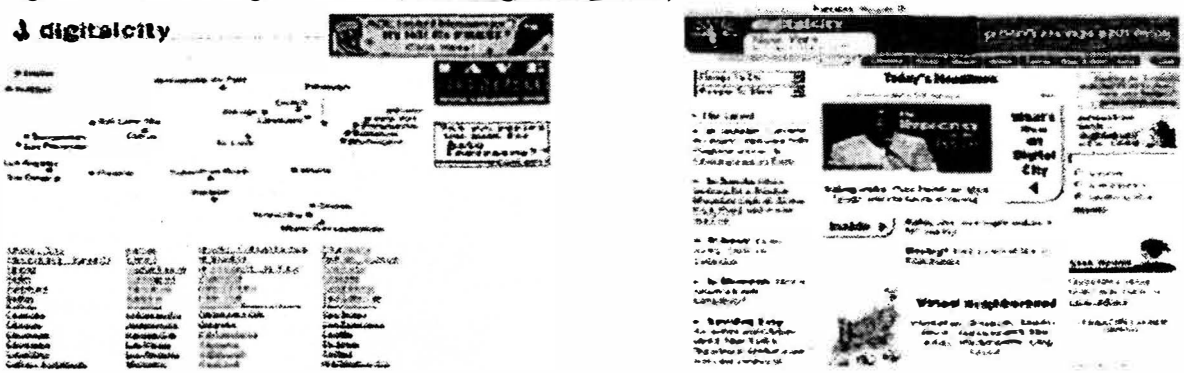
business transactions, personal ambition, and social activity [2]. AOL Digital City focuses on local information for each city it represents, as shown in Figure 2-2. If you want to visit a particular city, such as New York City, access AOL's digital cities home page at www.digitalcity.com and choose New York. From there you can locate local information such as shopping, commerce, hotels, the yellow pages, and the like.

Figure 2-1. 3D Digital City Kyoto



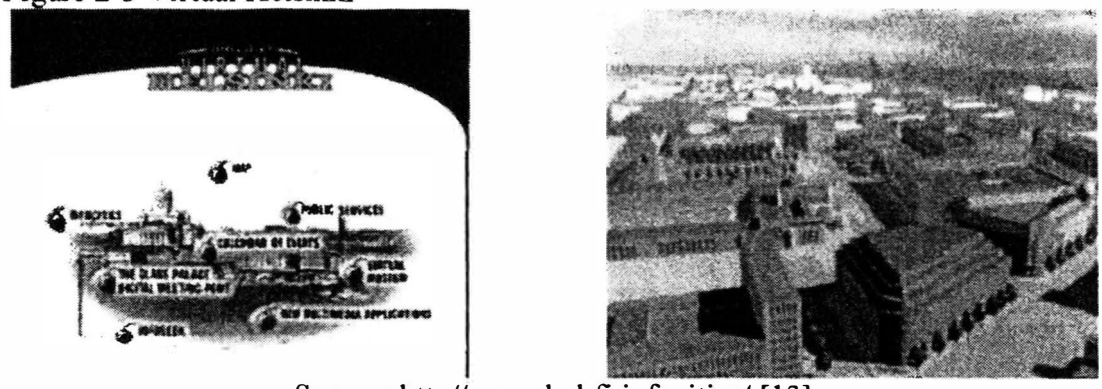
Source: By Stefan Lisowski [12]

Figure 2-2. AOL Digital Cities (www.digitalcity.com)



Digital city is a virtual place where people can go to meet other people, not just from their geographical area but from around the world. They are able to develop relationships, share mutual interests, offer advice, and exchange solutions to problems. Therefore, citizens of a digital city are able to participate in social interaction, economic and commerce activities and have the opportunity to improve their everyday life. The Virtual Helsinki project (http://www.hel.fi/infocities/) is one of these examples [13]. The project was named Helsinki Arena 2000 and was a four year project which began in 1996. An example of Virtual Helsinki is depicted in figure 2-3. Virtual Helsinki was an attempt to put all the municipality's public services online. It gave the citizens of physical Helsinki the ability to view public areas in real time, access online services, make purchases and place video phone calls through their personal computers [11].

Figure 2-3 Virtual Helsinki



Source: http//www.hel.fi.infocities/ [13]

The advantages of a digital city encompass several aspects. The digital city provides social interaction, economic and commerce activities, and the ability to improve the efficiency of daily life.

With social interaction people are able to share experiences and knowledge with each other, to make recommendations, and to discuss a wide range of topics. It also enables people to get to know other people and to seek out affiliation, companionship, and support [24]. Digital cities can also strengthen family ties by providing a means of communication. A site with local everyday life eventually becomes a nexus linking residents to visitors from overseas [12]. Digital City Kyoto, Virtual Helsinki, and AOL's digital cities are just a few of the well-known examples in existence. Each digital city has something different to offer depending on what they want to accomplish. For example, Digital City Kyoto was developed as a social information infrastructure; AOL collects both tourist and shopping information of a corresponding city and provides for local advertising opportunities for vertical markets; and Virtual Helsinki was developed so that their residents could do anything in the virtual city that can be accomplished in the physical city, which not only encompasses social interaction but also provides opportunities to improve the efficiency of everyday life.

The success of these cities indicates that people need these services for their everyday life. Residents of Helsinki are able to access their municipal public information services online [11]. In this virtual city, if you forget your friend's phone number, all you have to do is logon to your computer, take a stroll down the 3D version of the street in which they live on, and ring the virtual doorbell. AOL makes information retrieval convenient and easy so those who either live in the area or perhaps those wanting to visit the area can get access to hotels, entertainment, restaurants, and so on.

Digital cities also provide opportunities for economic and commerce activities. According to the Census Bureau of the Department of Commerce, the fourth quarter U.S. retail e-commerce was $18.4 billion (adjusted) and $21.4 billion (unadjusted) [25]. These figures indicate that digital cities, such as AOL's Digital Cities, are providing site visitors with the opportunity for economic activities. More and more people are doing their shopping online

through digital cities rather than trying to run "all over town" trying to find what they are looking for.

3. Important Issues involved in a Digital City

In addition to technological problems, non-technical problems have also been encountered. A dynamic living space cannot be founded on static technology [12]. It must be founded on dynamic technology, constantly moving and changing. The research gaps identified are currently based on dynamic technology and include international focus, government involvement and security.

3.1 International Focus

Digital cities give us the ability to overcome the geographical limitations. In these environments, we can meet people who have different cultural backgrounds and living in different geographical areas. Since digital cities create regional information spaces in the Internet, cross-cultural communication becomes an essential issue [7]. Intercultural interactions in daily life become necessary if digital cities are to thrive.

There are two essential reasons for discussing cross-cultural and intercultural communication in the context of digital cities. First, almost all cities are becoming 'melting pots,' meaning that citizens are becoming more diverse. A digital city can play a major part in building a bridge to cross the cultures. Second, a digital city will represent a real city on the Internet. Millions of people are using the Internet to visit different cities and countries; therefore, cross-cultural and intercultural communication must be supported, even though the main purpose of digital cities is to support the everyday life of local residents [12].

Two major issues to resolve are copyright infringement and mistranslations. For example, both the United States and England speak English. However, some of our words, even though they are spelled the same, have a different meaning.

3.2 Government Involvement

The main question is: should government be responsible for providing Internet security measures or should it be a combination of government, those who are developing the digital cities, or someone in between. The growth of computer-based crime has led to criminalization of certain behavior on the Internet: throughout the 1990s there was growing law enforcement attention and legislation relating to abuses of computers in both private and public sectors [14].

The public's concern over privacy and security is growing as the Internet grows. The evidence is mounting and the necessary remedy just might be a protective framework that includes legislative provisions. In the information society and economy, law, like location, will still matter [9].

3.3 Security

There are several types of security measures available today. Will it be adequate as technology changes? Practically speaking, the security of most sites on the Internet today rests on four key pieces [18]:

1. Firewalls that partly insulate servers (and a company's intranet systems) from the public Internet
2. Secure Sockets Layer (SSL) for encrypting sensitive data, such as credit card numbers and other billing information
3. Passwords to authenticate individuals
4. System hardening, to decrease the likelihood of a break-in.

Enterprises today can no longer afford to consider security only after the application has been constructed: irreparable security compromises may have already been exposed, and fixing such problems requires tremendous effort and resources [10]. Users rely on a digital city to provide the security they require. Just as we have social laws in physical cities such as peeping-tom laws, digital cities should introduce social guidelines that provide the security people need to feel comfortable about joining the information space [13]. A range of technologies is going to be needed in order to keep up with the Internet which is dynamic and changing everyday. Some of the ranges may include encryption, authentication, password controls, and firewalls. Since the Internet is dynamic, threats change, business needs change and technologies change. Ongoing research and analysis are needed to keep up to date with potential attackers [13].

A single-dimensional security approach is no longer sufficient. A multi-dimensional approach is now required to discourage the ever-more-sophisticated threats that a digital city can face [6]. A multi-dimensional security approach uses a range of security measures to ensure a comprehensive security system.

Security generally falls into three categories: prevention, detection, and response. Prevention comes in the form of a firewall. A firewall helps to prevent unwanted and unauthorized communication into or out of the network, and to allow an organization to enforce a network security policy on traffic flowing between its network and the Internet [15]. A firewall enables employees who need to access the Internet to perform their job, do so with confidence. Firewalls are like a fence around a house, they are a necessary part of the overall security, alone however, it is insufficient to provide the necessary security for a digital city. Another problem with using firewalls only is that this setup does not provide protection from the people the FBI says are responsible for most computer and network crime: employees already on the inside of the network [6].

One form of detection is a server scanner. Like door alarms and motion detectors in a building, intrusion and misuse detection devices add an important dimension to Internet security [6]. Response can include the shutting down of log-in accounts or sending an e-mail message to the appropriate administrators. A response is like alarms on a building that sound off and also call the police and building manager. In addition to sounding an alarm, sending an e-mail message, or transmitting a message pager, misuse and anomaly detector systems can take

defensive actions such as shutting down a log-in account, shunning connections from an attacker's Internet address, and replacing damaged files [6]. Unfortunately, there is no one program that can provide all three layers of the multi-dimensional security system. Usually one program will cover only one or two aspects of security.

4. Security and the Digital City

In the U.S., alone, nearly 300 virtual cities, representing their counterpart physical cities, have emerged over the past five years. They provide a range of services to city inhabitants and plenty of others, including those wishing to do business over the Internet [2]. With the addition of new Internet users on a daily basis, the number and variety of information that is transmitted on computer networks has increased. At the same time, the number of security attacks and aggressors has also increased. This incipient number of threats over the information systems forces us to make an effort to improve information systems security and its communication [17]. Users must feel confident that their personal information is kept secure, if not; they are less likely to use the Internet.

Webster's Dictionary defines security as a safeguard, protection, feeling secure, freedom from fear, doubt, and the like [8]. However, it is most commonly defined as "keeping the wrong people out, while letting the right people in" according to Avolio [1998]. Initially, the Internet was used primarily by both the government and academic community. Today, it is an indispensable business tool involving millions of users in nearly every country on the planet [6]. Security, particularly Internet security, is vague terms that may mean various things to different people [15].

The impact of not having proper security can be devastating. For example, the Federal Bureau of Investigation was forced to take down its Internet site after hackers began an attack against it. It remained inaccessible for several days, along with the site for its National Infrastructure Protection Center, which helps investigate computer crimes [22]. Another example is a series of distributed denial-of service attacks interrupted service at many high-profile sites, including Yahoo!, CNN, and eBay. These attacks have disrupted businesses with direct costs for cleanup, indirect costs through lost productivity, and, in some cases, lost revenue [18]. There seems to be no end to these types of stories. Complex attacks are not only performed by hackers but also because of simple mistakes. For example, a programmer at Northwest Airlines turned their encryption program off to make changes in the code. The programmer forgot to turn the encryption program back on and gave access to thousands of credit card numbers to anyone who logged onto their Web site. Security must be provided well if digital cities are to be used to their full potential. In addition to security, privacy and trust must be addressed.

Another issue related to security is the privacy concern. Privacy is usually interpreted as the unauthorized collection, disclosure, or other use of personal information as a direct result of electronic commerce transactions [21]. Privacy is better thought of as a personal space that is free from impedance by other people and businesses. If individuals feel that their personal information is not kept private, they are unlikely to visit, and do business, in digital cities. Therefore, free flow of information should equal the benefits that citizens receive from that free flow of information. In order for privacy to be protected, several aspects must be aggregated.

Some people believe that the government should be responsible for protecting their security. On the flip side of the same coin, others believe that if digital cities are regulated by the government they will not be able to grow and expand. A balanced approach to regulation may gain majority support within a country, but we question whether regulation can be established internationally, at least in the near future [22]. Therefore, Wang, et. al, propose that the government, business and individuals are the three main parties should be involved in dealing with security issue [21]. Government should promote strong privacy laws for both the public and private sectors; establishing independent privacy commissions to oversee the implementation of these laws; educating the public about privacy issues; encouraging business self-regulation. On the other hand, businesses need to promote self-regulation for fair information practices. Finally, individual should adopt privacy enhancing technologies, such as network and information security tools.

5. Conclusion

Each digital city has its own goal. AOL's digital cities aim at growing their business in so-called vertical markets. Helsinki is planning the next generation metropolitan network. In Kyoto, a social information infrastructure for urban life is being tested [1]. In all of these cities, security must be addressed in order to build digital cities that are reliable. It is often stated that one of the most obvious characteristics of virtual communities is that they are restricted by geographic or time "borders."

Security not only affects whether users will participate in a digital city but also to what extent they participate in it. If a user feels that proper security measures are not available, the likelihood they will participate in the digital city is slim. A secured digital city would therefore enhance the advantages of participating in it. For example, if a consumer feels confident in the security measures available in a digital city, they are more likely to participate in various activities.

One area of debate concerning security measures is who should be responsible for providing those measures. There are those who feel that the government should be responsible for providing the laws for security measure while others do not want the government involved. They believe that the government would stifle the expansion of the digital city. However, the author feels that the security should be a shared responsibility among the participants, business or the digital city providers, and the government in order to fully realize the anticipated advantages of participating in a digital city.

6. Acknowledgement

I gratefully acknowledge OURE for providing the opportunity to expand my horizons through research. I would like to thank Dr. Bih-Ru Lea, my faculty advisor and mentor, for her support, encouragement and guidance.

Reference

[1] Ishida, Toru; 2002; "Digital City Kyoto," Communications of the ACM, Vol. 45 (7), pages 76 – 81.

[2] Sairamesh, Jakka; Lee, Allison; Anania, Loretta; 2004, "Information Cities," Communications of the ACM, Vol. 47 (2), pages 29 – 31.

[3] Akahani, Jun-ichi; Isbister, Katherine; Ishida, Toru; 2000, "Digital City Project: NTT Open Laboratory," CHI 2000, pages 227 – 228.

[4] Ferguson, Donald; Sairamesh, Jakka; Feldman, Stuart; 2004, "Open Frameworks for Information Cities," Communications of the ACM, Vol. 47 (2), pages 45 – 49.

[5] Van den Besselaar, Peter; Tanabe, Makoto; Ishida, Toru; 2002, "Introduction: Digital Cities Research and Open Issues," Digital Cities II, Springer-Verlag Lecture Notes in Computer Science.

[6] Avolio, Frederick M.; 1998, "A Multi-Dimensional Approach to Internet Security," Putting it Together, pages 15 – 22.

[7] Ishida, Toru; Akahani, Jun-ichi; Hiramatsu, Kaoru; Isbister, Katherine; Lisowski, Stefan; Nakanishi, Hideyuki; Okamoto, Masayuki; Miyazaki, Yasuhiko; Tsutsuguchi, Ken; 1999, "Digital City Kyoto: Towards A Social Information Infrastructure," Cooperative Information Agents III, pages 34 – 46.

[8] Guralnik, David (Ed.); 1971, Webster's New World Dictionary of the American Language, page 539.

[9] Clarke, Roger; 1999, "Internet Privacy Concerns Confirm the Case for Intervention," Communications of the ACM, Vol. 42 (2), pages 60 – 67.

[10] Wang, Huaiqing; Wang, Chen; 2003, "Taxonomy of Security Considerations and Software Quality," Communications of the ACM, Vol. 46 (6), pages 75 – 78.

[11] Geary, James; 1998, "Digital Cities," Time.com, Vol. 151 (26).

[12] Ishida, Toru; 2004, "Activities and Technologies in Digital City Kyoto," www.digitalcity.gr.jp/DigitalCityKyoto20040601.pdf.

[13] Ishida, Toru, Isbister, Katherine; 2000, "Understanding Digital Cities," Digital Cities: Technologies, Experiences and Future Perspectives, Springer-Verlag Lecture Notes in Computer Science, Vol. 1765.

[14] Blumenthal, Marjory; Clark, David; 2001, "Rethinking the Design of the Internet: The End-to-End Arguments vs. the Brave New World," ACM Transactions on Internet Technology, Vol. 1 (1), pages 70–109.

[15] Oppliger, Rolf; 1997, "Internet Security: Firewalls and Beyond," Communications of the ACM, Vol. 40 (5), pages 92-102.

[16] Cranor, Lorrie Faith; 1999, "Internet Privacy," Communications of the ACM, Vol. 42 (2), pages 29-31.

[17] Sierra, J.M.; Ribagorda, A; Munoz, A, Jayaram, N.; 1999, "Security Protocols in the Internet New Framework," IEEE, 0-7803-5247, pages 311-317.

[18] Treese, Win; 2000, "Living on the Internet Plateau," Putting It Together, Vol. 4 (3), pages 9-11.

[19] Xiao, Lu; 2002, "Digital City Examples," http://filebox.vt.edu/users/lxiao1/Digital%20City%20Examples1.ppt

[20] Stotlterman, Erik; 1999; "Technology Matters in Virtual Communities," SIGGroup Bulletin, Vol. 20 (2), pages 7-9.

[21] Wang, Huaiqing; Lee, Matthew; Wang, Chen; 1998, "Consumer Privacy Concerns about Internet Marketing," Communications of the ACM, Vol. 41 (3), pages 63-70.
[22] Dekleva, Sasa; 2000, "Electronic Commerce: A Half-Empty Glass?" Communications of AIS Vol. 3, (18), pages 1-99.
[23] Sproull, Lee; Patterson, John F.; 2004, "Making Information Cities Livable," Communications of the ACM, Vol. 47 (2), pages 33 – 37.
[24] Girgensohn, Andreas; Lee, Allison; 2002, "Making Web Sites Be Places for Social Interaction," Communications of the ACM, pages 136 – 145.
[25] Scheleur, Scott; King, Carol; Shimberg, Michael; 2005, "Quarterly Retail E-Commerce Sales 4th Quarter 2004," United States Department of Commerce News, http://www.census.gov/mrts/www/ecomm.html