GEOGRAPHIC INFORMATION SYSTEMS

Volume 25 No 8 2002
The Electronic Version ISSN 0742-468X Since 1978

Welcome to

The Harlow Report - GIS

Welcome to the eighth issue of 2002! This issue's lineup includes is full of useful information. Do not miss Confessions of a SCADA Hacker, even even if you never heard of supervisory control and data acquisition. Speaking of not missing things, Don't Miss the Summit is not to be missed either. Join me in Denver!:

- **Confessions of a SCADA** Hacker Read the congressional testimony by the Chief Hacking Officer of a well respected IT security firm, as he tells of the vulnerability of our infrastructure.

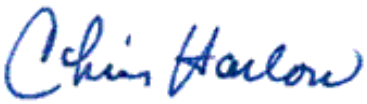
- **ESRI Helps You Plan for a GIS** It used to be that to develop a plan for your GIS, meant
- spending a ton of dough on a consultant (like me!), now ESRI will show you how to do it yourself.

- **Don't Miss the Summit** I've been spending my summer conducting a survey of the electric utility GIS and mobile computing market for the fine folks at InfoNetrix. On September 24th, 2002, I will be highlighting those findings. Check it out in this article.

- **Organizations for the IT Pro** Don't let the title scare you. Even if you don't consider yourself an IT pro (yea, that's why you sit in front of a PC all day long), there are plenty of professional organizations that need your skills.

- **What Really Kills You**! This one is just for fun, and need some in your life.
-
- **Results of Last Poll** This is a new recurring article that will display the results of the last poll.

As always, we provide you with the latest links to new topics, products, services and oddball ideas that either pertain to GIS, or seem like fun. You know that is located **in GIS Net Surfing.** If you just want the latest in GIS news, then click on over to **News to Use.**



Confessions of a SCADA Hacker

Editor's Note: The following testimony is provided to you as posted on eEye Digital Security's web site. It is the Congressional testimony of the company's Chief Hacking Officer, Marc Maiffret. He provides us with a chilling assessment of the security risks in our nation's SCADA systems. While some in the utility and public works industries will read this and attempt to poke holes into Maiffret's assertions, think again. As a member of InfraGard, a corporate IT security association, I assure you that Maiffret knows his stuff. At each monthly meeting of InfraGard, some of the smartest security people I know (including those of the FBI) are constantly surprised at the new security flaws that are discussed. Hackers spend their lives nit picking flaws in systems. So don't just assume that it cannot be done, because you can't do it. What may seem unlikely to you is a walk in the park for those who lurk in the shadows. Read this testimony carefully!

On the other hand, it makes you wonder about the balance between alerting us to the flaw and just plain bragging. Why not make our enemies work a little harder to find targets on their own? Why post it to a public web site? There is a debate in hacker circles about this type of disclosure. Hackers claim they do a necessary service by finding flaws, and it is their duty to tell the world about them so the holes can be closed. What do you think? Could this have been handled in a better way? Is he correct about our vulnerability? Am I guilty of doing the same thing? Send your comments to charlow@charter.net

The State of the Nation's Infrastructure Systems

Testimony of:
Marc Maiffret
Chief Hacking Officer
eEye Digital Security
Given to:
SUBCOMMITTEE ON GOVERNMENT EFFICIENCY,
FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS
Congressman Stephen Horn, R-CA Chairman

Everyday I wake up to find myself living in a world where the scientist is growing weaker and the pessimist is growing stronger. We are all too caught up in the moment of quick solutions, through finger pointing at weakness within each other, and the fragile systems that are slowly being placed as crucial foundations for our way of life.

With our lives becoming dependent on technology, there comes the need for increased security. Security is something that few technologists and scientists have been trained to think of when developing new ideas that make our lives easier and more convenient. With the lack of security forethought, we are building our future on systems that are insecure, and that will stay insecure until we are able to drastically change how technology is built, until security takes top priority.

The security of our nation's infrastructure is a complex problem that is affected by the inherent fallibility of the software it is built upon, and by the integrated nature of the systems. It is a problem that goes beyond technology to involve human weakness and trust. It is security meets business, meets usability, meets politics, meets everyone's opinion of how things should be. Albert Einstein once wrote: “If we have the courage to decide ourselves for peace, we will have peace.” I believe the same goes for security. Only when we, as a society, decide we truly wish to be secure, and follow through with that decision, shall we begin to start to attain security.

Our Infrastructure is insecure

Advancements in technology are making it easier for businesses to cut costs and increase productivity. These benefits make it very appealing for companies to quickly update their legacy systems to be using the latest and greatest technology available to them. In many cases, however, the underlying technology is flawed, incorrectly managed, or incomplete.

The newer technology being deployed is mostly made up of COTS (Commercial Off the Shelf) software. This software is attractive because it is easy to use and to maintain, but like all other software it contains flaws that can put it at risk for exploitation. The fact that COTS software is so widely available allows it to easily fall into the hands of users with malicious intent. These

users have the potential to uncover security flaws, which then put the software and systems built on the software at risk for attack.

While newer technology is often more easily hacked into, we should not discount that older, legacy systems are just as vulnerable. Many times the only thing that keeps legacy systems secure is what is known as "security through obscurity". Since legacy systems are mostly proprietary, people believe criminal users will not have enough knowledge to manipulate and take control of these systems. The idea of security through obscurity, however, has long been proven to be ineffective.

One of the most common technologies in use within our infrastructure is SCADA (Supervisory Control and Data Acquisition). SCADA is the term that describes the majority of systems which have control over the physical aspects of our infrastructure. In its simplest form, SCADA allows software to manage various hardware aspects of our infrastructure, such as the ability to use software to control part of a power grid or a water treatment plant. Combined with other software that allows for remote control of SCADA software, companies have the capacity to manage their infrastructure with never-before-seen ease. For instance, fifteen field offices can be managed from one central location.

The remote management capability of SCADA systems is where some of the vulnerability of our infrastructure first arises. Most often, the remote management of SCADA systems is implemented using COTS software. Some COTS software applications provide dial-up solutions for remote access to SCADA systems. Others allow employees of infrastructure companies to remotely access and manage SCADA systems via encrypted "tunnels" through the Internet.

Most of these remote management systems attempt to put at least some access control on who is able to use them. This access control is usually implemented in the form of login passwords, and sometimes secure ID tokens. Unfortunately, no matter how strong the system to restrict access, we must remember that COTS software providing the access has been found time and time again to contain flaws. A weakness in the connecting software can be manipulated to bypass standard access control and provide direct access to the SCADA software itself.

Beyond the COTS software that provides "add-on" functionality to the SCADA software in the form of remote management, sometimes common software applications make up the backbone of SCADA systems. Technologies such as Microsoft Windows or Oracle databases have been proven insecure in the past, and thus compromise the security of the entire infrastructure system as a whole.

COTS software is not the only thing that can lead to attackers being able to gain access to SCADA systems; many times the software actually driving SCADA systems is flawed. I have been able to analyze a few SCADA software packages in a lab environment and have found that most of them actually contain possible vulnerabilities that can lead to SCADA systems being compromised.

With the use of backend database systems and network redundancy via common protocols, there exists a potentially attackable communication mechanism between some SCADA software. This communication mechanism is often flawed and vulnerable to common types of security vulnerabilities such as buffer overflow attacks and database injection attacks. In addition, SCADA software sometimes insecurely stores password information, which is a crucial component for any sort of final access control that may be in place. So, not only does an attacker have the ability to gain access to a SCADA network via COTS vulnerabilities, he then can elevate his access within SCADA control software via weak password storage mechanisms.

The vulnerability of our infrastructure to external attack does not only apply to networks where remote access to SCADA is in place. In fact, the infrastructure sites that do not employ any remote access capabilities are equally at risk. This usually exists because of improper segmentation of networks infrastructure sites do not have the right systems in place to separate their corporate networks from their critical infrastructure networks.

Many times two networks will exist at a single infrastructure site. One network is put in place to facilitate the control of the site via SCADA, and one network for supporting employees at the site not directly working with the SCADA systems. A security risk can arise when these two networks are not properly segmented. For instance, even though the SCADA system may not be directly connected to the Internet, an attacker coming through the Internet can compromise a computer within the non-SCADA side of the network and then jump to the SCADA part of the network. From their remote location, the attacker would be able to take advantage of the functionality that SCADA offers to seize control of a power plant, a water treatment plant, a dam, or even an amusement park.

A final, important weakness of SCADA software is the lack of auditing capabilities. Auditing functionality allows companies to keep an eye on what is happening within their computing environment. A consistent audit of the system provides a way for companies to trace the events that occur after a breach in security, which in turn provides crucial information required for quickly assessing and repairing any damage to the system. Also, auditing offers organizations a way to keep an eye on employees which could potentially be working for outside entities that wish to cause harm.

Beyond the obvious security needs at the software and network level, one cannot ignore the need for personal and physical security at infrastructure facilities. Even with the best computer security in place there will always be employees who must have access to the systems. While processes like auditing help keep tabs on employees potentially abusing infrastructure systems, more needs to be done on a social level to ensure the security of our infrastructure.

Know your enemy

At the human level, security must begin from the inside out. Not only should infrastructure companies keep watch for malicious employees, but all employees should be given proper training regarding proper security practices.

In order to start to attain security within the internal workings of a company you must establish a level of trust. This trust needs to be proven and enforced. We have become a society where nothing and no one is as it seems, and the strict enforcement of honesty and integrity on the operators of our nation's infrastructure is a necessity.

The threat of an attack from a person inside an organization must be considered, but not always are these internal attacks intentional. An outside attacker may often times target a social weakness within an infrastructure employee. By playing off of that weakness, it is possible that foreign persons can manipulate an employee to perform actions which ultimately lead to harm being brought against the network or the infrastructure. This type of social attack is something that has been used by the intelligence community for a long time, as it usually can lead to quicker and more significant turnaround on the effort expended for such tasks.

Although social attacks can be a useful method for getting into critical systems, not every enemy of ours posses the skills needed to perform such an attack. For those that cannot compromise our infrastructure via social or physical means, they could most likely do so via technology exploits as discussed earlier. The ability to penetrate our infrastructure through vulnerabilities in technology is a real threat that must be taken seriously, especially since it is likely to be the easiest and most appealing method of attack for many.

Attacking our infrastructure via technical means can be appealing because it can be done anonymously and without much money. The anonymous aspect stems from the way our communication systems have been built with the idea of access from anywhere, at anytime. It can be cumbersome to try and find the origin of an attack coming through a network, because of the ability to cover one's tracks without much effort. Also, with advancements in wireless technology and its widespread adoption, the ability to be invisible is easier than ever.

The second thing that makes hacking into infrastructure appealing is that computer hacking is the Wal-Mart of espionage and terrorism. It is a rather cheap endeavor, and the supply of trainable hackers is nearly endless. So far, however, I would guess that terrorists are only recently starting to realize the benefits of having people within their organizations that have real hacking skills.

It should be made clear that not every hacker is able to break into an infrastructure company and shut down a power grid. I have seen one too many news articles written that portray your average teenage computer hacker as having the ability to reach the most sensitive of systems - this is simply not true. It would be rare for the average hacker or script kiddie (so named because they rely upon existing pieces of hacking code - or scripts - that circulate around the Internet) to have the technical and social skills needed to break into something like a power grid. We shouldn't assume that script kiddies will never get access to SCADA networks - they have in the past - it is just very unlikely. Because of the complexity involved, only a small number of people in this country actually have the skills needed to perform such a targeted attack.

On the other hand, countries like China and Russia have been working hard to keep their hacking abilities on par with the United States. A country with the hacking ability of China should be considered a formidable foe and not be taken lightly. At the moment it could very well be that the only thing keeping our infrastructure safe from such countries is the simple fact that those countries have not wished to attack us. A race between the United States

and other countries to increase their technical hacking capabilities could be reminiscent of the nuclear arms race between the United States and Russia. Although, not nearly as potentially devastating.

Starting from zero

I think one of the things working to our advantage is the fact that we are essentially starting from nothing. The technology we are building upon is truly in its infancy, and the existing security is spotty at best. There is a lot that we can start to do to secure our infrastructure, which personally I believe is a good position to be in. We've yet to exhaust all possibilities of things we can do to protect ourselves from attack.

We must start small and build up. One of the first things we should be doing to protect our infrastructure is to enforce a set of requirements onthe security of sites and companies that we deem to be integral parts of our critical infrastructure. A lot of industries are slowly starting to move in the direction of forcing businesses to meet a certain level of security. The healthcare industry has begun to force hospital networks to come up to a standardized level of security. We should be doing the same with our infrastructure companies.

Infrastructure companies must be held accountable and forced to meet a set of security standards. We must also understand that infrastructure companies in many areas are struggling, and the increased costs of security must be taken into consideration. The financial aspect of such an endeavor, while an obviously important topic, must not overtake the importance of security. Once again, we must all agree to be secure, and follow through. Also, we should not simply let people write off their lackof security due to expenses - security at the most basic level does not need to be expensive.

To outline the requirements of what it takes to secure an infrastructure site is a bit beyond the scope of this paper. There definitely should be a meeting held to formalize an enforceable best-practice security policy for infrastructure companies. This should not simply be a meeting of management, but of employees as well, and of various knowledgeable people from the security community. Far too often we overlook the amazing insight of the people who “work in the trenches.” I have talked with many employees at infrastructure companies who know all too well what is wrong with their systems, and often know what needs to be done to fix it.

Listed below are a few high-level ideas that should be covered when setting security requirements for infrastructure companies:

- Background checks on all employees within critical infrastructure companies. In some cases background checks to the level of checking done to get some government clearances.
- Specifications to define a level of security for networked aspects of infrastructure companies.
- Specifications to define a level of security for SCADA control software.
- Specifications to define a level of physical security at infrastructure facilities.

Once again these ideas simply touch on the areas a security requirements policy would cover. These guidelines, once fully created, should be enforced by our government and companies need to be held accountable if they do not meet the requirements.

In the end

The doom and gloom that infrastructure critics have been peddling is not accurate for our current situation. Although weaknesses do exist that can currently be exploited, I believe we are in a fine position to create a thorough and strong security plan to come out on top. Time definitely is of the essence, however, and we should start proactively securing our infrastructure before it is too late.

I do not like hearing that there is no such thing as a secure system. We must believe that we can be secure. Maynard James Keenan once wrote: "The only way to fix it is to flush it all away. Time to bring it down again. Don't just call me pessimist. Try and read between the lines". I fear that if we do not begin to enforce security as a whole, and if we piece together security solutions only as they are needed, then we will be forced to thrust our infrastructure technology through a nihilistic rebirth, as the only means of becoming secure would be by starting over.

ESRI Helps You Plan for a GIS

Not that many years ago, planning for a GIS was a major undertaking. Consulting firms grew rich on feasibility studies, and planning studies. Back then, the technology was new, and was not readily accepted by budget conscious buyers. Today, the decision is not about if you should have a GIS, but rather when you will get one. Now, ESRI is trying to make the planning process a bit easier.

The ESRI Virtual Campus is offering a course Planning for a GIS. It is a 10-module course that explains how to successfully plan for a GIS implementation. Because ESRI cannot stand to leave anyone out, there is a mod that handles the fundamentals of GIS. No experience necessary at the ESRI Virtual Campus.

The smart people at ESRI recognized that there is a lot to know about GIS, and even those who consider themselves experts may still not get the benefits of some of the newer technology. ThatÕs one of the reason the Virtual Campus was created, and offers a number of courses.

Learning from the best

One of the first in the world to recognize the importance of GIS was Dr. Roger Tomlinson. He originated and directed the development of the Canada geographic information system, the first GIS in the world. Often dubbed the father of GIS, he is a long time friend of the uncle of GIS, Jack Dangermond, Tomlinson is the author of “Planning for a GIS,” a course he designed to help managers within their work environment. As Tomlinson said: "As a senior manager, or a present or future GIS manager, you have an important role to play in your organization to help it focus on what it needs to get out of your GIS,

According to ESRI’s Nikki Snowhite, the course has nine modules that describe the GIS planning process. A 10th module contains a detailed GIS lexicon - a software independent reference that aids students in their planning process. Just in case you are not sure if this is for you, Snowhite pointed out that the first module is free, so you can check it out. The course includes these modules.

- GIS Planning Basics
- Analysis of Business Needs: Taking the First Steps
- Describing Information Products
- Master Input Data List, System Scope, and Timing
- Conceptual System Design for Data
- Conceptual System Design for Technology
- Preparing for Implementation
- Benefit‹Cost, Migration, and Risk Analysis

- Procurement and Reporting Procedures
- Lexicon of GIS Functions

Is the price right?

To take the course, you will need Internet Explorer or Netscape 4.0 or higher, Adobe Acrobat Reader, and US$180.00. For further information or to enroll in the course, visit The ESRI Campus or call 1-800-447-9778.

Don't Miss the Summit!

As many of you know, I have been working with InfoNetrix, a leading utility IT and automation market research firm to conduct an important survey of the GIS and Mobile Computing Solutions for the North American electric utility industry.

If you are a GIS and Mobile Computing (GMC) solution provider, you need to have information that will help maintain and sharpen your competitive edge. As a long-term participant in the GMC market space, I readily recognize this need. This is a major reason why I teamed with InfoNetrix on their upcoming GMC Executive Market Summit.

Scheduled for Tuesday, September 24th at the Denver Marriott City Center, this unique one-day forum promises to be time well spent. The Summit is designed as an intimate gathering of industry leaders. This provides ample opportunities for learning about the latest developments from the GMC market's leading thinkers. Also, it allows for openly exchanging ideas and exploring new ways of delivering your solutions to the marketplace.

Who'll be speaking?

MORNING SESSION (8:00AM - 11:30AM)

- **David DiSera**, Managing Partner, EMA; (President, GITA-2002): "Real World Drivers for GIS & Mobile Computing Applications"
- **Jeb Bolding**, Analyst, Mobius Venture Capital; "Electronic Clipboards: Wireless Tools for 21st Century Enterprises"
- **Peter Gomez**, Xcel Energy: "OMS & Mobile Technology: How it Works for Xcel Energy - South"

AFTERNOON SESSION (1:30PM - 4:00 PM)

- **Ron Burdis**, Principal, RDB Consulting: "GIS & Mobile Computing - New Frontiers in Utility Automation"
- **Mike Smith**, Principal; InfoNetrix: "Business Opportunities in the GIS & Mobile Computing Marketplace" (Project Outlook Summary)
- **Chris Harlow**, Senior Research Analyst; InfoNetrix: "Issues & Trends in the GIS & Mobile Computing Marketplace" (Market Outlook Summary)

For details about the InfoNetrix Summits, and a registration form, visit the InfoNetrix site at http://www.infonetrix.com

The InfoNetrix staff and I also partnered on the upcoming Electric Utility GMC Strategic Market Intelligence Report, - an in depth analysis and forecast of the GMC market through 2006. The report will be available shortly after the Summit on September 24th, 2002

If you have any additional questions about the Summit, please feel free to contact Mike Smith, Principal, at 916 984 7430, or mfs@InfoNetrix.com.

Conclusion

If you are, or want to be involved in the GIS and mobile computing solutions for the electric utility industry, sign up for the Summit today! (And, be sure to ask for the special $139/night InfoNetrix Summit rate at the Denver Marriott!)

See you in Denver

Organizations for the IT Pro

Editor's Note: Richard Lowe provided us with some solid recommendations for organizations that IT professionals should know. I realize that in the GIS industry, many believe that somehow GIS is above the riff raff of IT. Think again. In many ways, you are leading the industry. So take Lowe's advice and look into some of his recommendations. Richard Lowe Jr. is the webmaster of Internet Tips And Secrets at http://www.internet-tips.net - Visit the website any time to read over 1,000 complete FREE articles about how to improve your internet profits, enjoyment and knowledge.

Some Good Organizations To Join

by
Richard Lowe, Jr

There are many organizations all over the internet which are useful to webmasters and other people on the internet. This is a list of some of the ones which I find useful.

* **Americans For Computer Privacy** - This is the organization to take a look at if you are interested in privacy matters.
http://www.computerprivacy.org

* **Association of Computing Machinery (ACM)** - One of the oldest organization of all. This group is huge and has so many benefits that it's impossible to list them here. It can be highly technical, and tends towards the theory and practice of computing. They have dozens of publications and for about a hundred bucks you get access to a huge online library of white papers and technical works.
http://www.acm.org

* **Better Ethics Online (BEO)** - A great group all about the ethics of the online world. They have several lists of known spamming email addresses which can be used in filtering software.
http://actionsites.com/beo/index.html

* **Coalition Against Unsolicited Commercial Email** - Want to learn about spam and how to prevent it? This is a great organization to join and join the fight.
http://www.cauce.org

* **Cyber Crew** - A group of volunteers who cover just about everything on the internet. More of a users group than anything else.
http://www.cyber-crew.com

* **HTML Writer's Guide** - This organization has lots of good web-based courses and a certification program (Certified Web Professional). This group (which has merged with the International Webmasters association) has many other great features. Yearly members is about fifty bucks, and this gets you the courses at half price.
http://www.iwanet.org

* **IEEE** - One of the very largest and oldest computer societies. In fact, computers are only a portion of what this organization offers. Thousands of papers are available online to members, and dozens of publications are published. This group tends to be highly technical and very in-depth.
http://www.ieee.org/portal/index.jsp

* **Internet Engineering Task Force** - Interested in helping the internet as a whole? This group helps maintain the structure and operation of the entire internet. This group is perhaps second in importance (and it could be classified as first according to some) to the W3C. They also archive and maintain RFC's, which are the documents which describe the protocols and standards of all of the internet.
http://www.ietf.org

* **Internet Society** - Another huge organization dedicated to helping internet professionals. A large number of benefits are available.
http://www.isoc.org

* **Internet Engineering Task Force** - Interested in helping the internet as a whole? This group helps maintain the structure and operation of the entire internet. This group is perhaps second in importance (and it could be classified as first according to some) to the W3C. They also archive and maintain RFC's, which are the documents which describe the protocols and standards of all of the internet.
http://www.ietf.org

* **Paint Shop Pro Users Group (PSPUG)** - If you use Paint Shop Pro (one of the best graphics editors around), then this group is essential.
http://www.pspug.org

* **Web Master World** - Want to learn about the web from professionals who actually know what they are doing, with a strong emphasis on promotion (especially using search

engines)? If so, visit this forum, lurk for a while, then start posting your own opinions, experiences and questions.
http://www.webmasterworld.com

* **World Of Webrings** - A group dedicated to promoting all of the webring systems. If you want to find out about webrings, this is one of the best places to start.
http://www.worldofwebrings.org

* **World Wide Web Consortium (W3C)** - One of the heavyweight groups of the web. These people define many of the standards, including HTTP, HTML and XHTML. This is the best place to begin looking for information about web related specifications and documents.
http://www.w3.org

Some Good Organizations To Join

GIS Net Surfing

NIMA
http://www.nima.mil/

The National Imagery and Mapping Agency (NIMA) provides timely, relevant and accurate geospatial intelligence in support of national security. NIMA was formed through the consolidation of the following: the Defense Mapping Agency (DMA), the Central Imagery Office (CIO), the Defense Dissemination Program Office (DDPO) and the National Photographic Interpretation Center (NPIC) as well as the imagery exploitation and dissemination elements of the Defense Intelligence Agency (DIA), the National Reconnaissance Office (NRO),the Defense Airborne Reconnaissance Office (DARO) and the Central Intelligence Agency.

Intergraph GeoSpatial Users Community
http://www.intergraph.com/gis/community/geoforum.asp

The mission of the Intergraph GeoSpatial Users Community is to further knowledge, product use, and interaction with Intergraph and users worldwide. The IGUC has members from 91 countries and continues to grow. Members can participate in the IGUC Networks, which are forums for users to provide direct comment and feedback about Intergraph's product planning, development, priority, and direction.

Tiger Map Engine
http://tiger.census.gov/cgi-bin/mapbrowse-tbl

US Bureau of Census Tiger Mapping Engine. If you don’t know about this site, shame on you. It is full of useful maps based on 1998 Tiger/LINE© data and 1990 Decennial Census data. The map engine is a breeze to use. Try it now!

The Arkansas Interactive Mapper
http://www.cast.uark.edu/products/MAPPER/

The Arkansas Interactive Mapper is a Web-based program which allows any user to generate maps of any area in Arkansas. This project is sponsored by NASA
nearest nuclear waste route. Ironically, the ESRI HQ building is a mere .3 miles from the nearest nuclear waste route.

MapPublisher Winners

http://www.mapscience.org/

This site honors the winners of the 2002 2002 MAPublisher Map Competition - a competition that showcases the quality and diversity of maps that can be produced with MAPublisher. MAPublisher 5.0 is a suite plug-ins for Adobe Illustrator that bridges the gap between GIS and high-end graphic design for high quality creation, high resolution printing and electronic publishing of maps.

World Site Atlas

http://www.sitesatlas.com/index.htm

World Site Atlas. Oh, what a site! Plan to spend the rest of the day clicking around the world for maps of every conceivable country, including road maps, physical maps, political maps, and more! Oh, what a site! Plan to spend the rest of the day clicking around the world for maps of every conceivable country, including road maps, physical maps, political maps, and more!

Pixxures

http://www.pixxures.com/

Pixxures offers a comprehensive array of high-resolution aerial mapping products, including ortho imagery and derived products, an expansive online library of imagery from multiple sources, and a family of data hosting and Internet portal products and services.

What Really Kills You!

Editor's Note: Here is one of those anonymous bits of wisdom floating around the Internet. This makes sense!

Here's the final word on nutrition and health. It's a relief to know the truth after all those conflicting medical studies.

* The Japanese eat very little fat and suffer fewer heart attacks than the British or Americans or Canadians.
* The French eat a lot of fat and also suffer fewer heart attacks than the British or Americans or Canadians.
* The Japanese drink very little red wine and suffer fewer heart attacks than the British or Americans or Canadians.
* The Italians drink excessive amounts of red wine and also suffer fewer heart attacks than the British or Americans or Canadians.

CONCLUSION

Eat and drink what you like. Speaking English is apparently what kills you.

News to Use

City of Winnebago, (www.winnebago-mn.com/) Water and Waste Department successfully implemented a water and wastewater geospatial infrastructure management system. They used Intergraph Mapping and GIS Solutions GeoMedia technology. The department uses GeoMedia, GeoMedia Professional, GeoMedia WebMap Professional, and GeoMedia PublicWorks Manager to improve access to the city's asset information. The city database serves 178 square miles and contains over 200,000 pipe segments and more than 1,000,000 additional features. Winnipeg uses Oracle and Oracle Spatial for its enterprisewide database for use with the GeoMedia-based geospatial infrastructure management system..

ESEA http://www.esea.com MapMerge, from ESEA, was awarded the distinction of second place in the category of Best Productivity Enhancement in the ESRI ArcGIS Challenge Contest. The contest was designed to highlight ESRI business partners who have developed solution products based on ArcGIS. MapMerge brings conflation tools to ArcGIS as an extension product. Conflation is the process of enhancing data quality by merging multiple data sources. When you have one data source with rich attribution and another with accurate locations, MapMerge allows you to create a single data set containing the best data from both sources.

GE Network Solutions
http://www.gepower.com/dhtml/network_solutions/en_us/index.jsp
GE Network Solutions, announced that Telkom SA Ltd (Telkom), South Africa's leading communications company based in Pretoria, has selected its Smallworld Network Inventory system. The new system will replace numerous existing, disparate applications currently being used for network planning within Telkom's seven regional offices. The creation of a single, fully integrated network planning system will enable Telkom to streamline its business processes and provide immediate, nationwide access to up-to-date network information.

Also, GE Power System said that **Warren Ferguson** will head up Software and Customer Initiatives for its Energy Management Services business. Warren previously led GE Network Solutions. **Henry Stueber** will replace Ferguson as president and general manager of GE Network Solutions.

The Omega Group http://www.theomegagroup.com/
The Omega Group won two awards in the 2001 ESRI ArcGIS Challenge Contest. CrimeView_ 2002 was distinguished with The People's Choice award and placed second in the category of Best Integrated Solution. CrimeView 2002 is the next generation in crime analysis software, based on ESRI's new ArcGIS 8.x platform, and the first release of the new Omega GIS family of products. CrimeView 2002 offers the same ease of use that made previous versions of this crime analysis mapping application so popular, and also includes many enhancements based on the new technology. CrimeView can now be used as part of an enterprise solution for law

enforcement and public safety agencies by integrating it with CrimeView Internet, CrimeView Community, and FireView™

Applied Geographics, Inc. http://www.appgeo.com

The Commonwealth of Massachusetts has contracted with Applied Geographics, Inc. (AGI) to provide geographic database design and support services for the Boston Preparedness Pilot Project. Funding and project participation was provided through the Executive Office of Administration & Finance (EOAF) and the Executive Office of Environmental Affairs (EOEA) MassGIS program and a variety of Federal agencies. The Pilot was initiated in response to the National Imagery and Mapping Agency (NIMA) 120 Cities Project, an effort to engage state and local agencies to gather and maintain important geospatial data in support of homeland defense and emergency preparedness.

Voice Insight http://www.voice-insight.com/

Voice-Insight released Voice Assistant for ArcPad, a new application built on top of ESRI's ArcPad 6 software. Voice-Insight's Voice Assistant for ArcPad lets users in the field complete their common ArcPad applications using their voice. Users can perform basic tasks such as zoom in, zoom out, and pan as well as more complex tasks, such as retrieve and update forms, query data, and edit features, all with the sound of their voice. Voice Assistant for ArcPad uses Voice-Insight's, Voice Query Language (VQL), a technology that allows database applications to be queried with voice and language.

If you change your

Email address,

tell us!

Mailto:Charlow@charter.net