Luminant

May 2001

Issue 3

AORTA

Adventures in Information Security

I am on my way back from a panel discussion at a press event on wireless security in San Francisco. On my way back, I am mesmerized and inspired by the beauty of the Cascades from 30,000 ft above sea level. This sets the stage to pen this month's column on information security.

Someone sane once said that there is no such thing as 100% security. This is nothing more than a myth. There are almost no networked systems in the world today which are hacker proof.

Did you know that 70% of the break-ins happen from within an enterprise, and all this time you were worried about attacks from outer space.

Traditionally, IT has thrown technologies like encryption, firewalls, PKI, VPN, IDs, scanners, biometrics, and authentication to solve security issues. You would think that things would get better and not worse with each advancement in the area of security. But this hasn't been the case. Why? Things get worse because the systems are getting much more complex and difficult to understand and operate. There is just too much to get your arms around, too many patches to apply, too many installations, and no such thing as plug-and-play in security.

So, what can you do?

Slow down; don't install new systems until the art of breaking into existing systems becomes so obscure that you are safe. Some folks actually do that. OR you can learn to live with the idea of insecurity on the web and embrace risk management, i.e. protect your assets by priority; put processes, policy, and procedures in place and enforce them. Also, be on a constant watch for patches and vulnerability updates to minimize your exposure window.

This brings us to the three commandments of securing information:

a) identify your valuable assets
b) have strict policies and procedures to protect them (along with monitoring and detection), and
c) have a plan to react to breach in security

If your most prized asset is your intellectual capital, protect it as if your life depended on it. If competitive snooping gets through, you might as well shut down the shop. But would configuring firewalls to limit access help matters? Certainly, but that's not the only thing that is going to help you. Most of the firewalls are configured incorrectly, changes overlooked. It's only by proactively implementing security policies and monitoring your network that you would be able to detect or resist break-ins. Most break-ins remain undetected, unless you know what you are looking for. As Tod Knight pointed out in his column *"Waves of Technologies—Expectations vs. Reality"* (AORTA Issue 2), newer waves create complex security challenges.

But, that shouldn't prevent you from adopting them. Be aware of them, and proactively update your policies and procedures.

Let's look at some security issues – some old, some new.

IEEE 802.11

IEEE 802.11 or Wi-Fi is a wireless LAN technology, which is getting attention from many enterprises. It's security mechanism works something like this. Wireless access points (AP) and units exchange management frames in order to associate with each other. A unique identifier for the basic service set (BSS) called service set identifier (SSID) is routinely transmitted by the access points.

Units also transmit probe frames to find access points. When a unit finds an access point, it initiates an association and proposes an authentication method. The default

Continued on Page 2

Inside this issue:

Adventures in Information Security	1
Waves of Technology—Expectation vs. Reality (2 of 2)	4
I dream of computers	5
Stat Focus	6
3G Perils	6
Corporate culture and Innovation—can we combine?	7
Bluetooth having an ache?	8

Continued from Page 1

method, Open System Authentication (OSA) provides no authentication at all. In OSA, any unit is permitted to join the BSS. If the unit proposes Shared Key Authentication, the AP generates a random 128-bit challenge. The station returns the challenge, encrypted with a secret shared key configured into both the unit and AP. The AP decrypts the challenge, using a cyclic redundancy check (CRC) (cyclic redundancy checking is a method of checking for errors in data that has been transmitted on a communications link) to verify its integrity. If the decrypted frame matches the original challenge, the unit is considered authentic. The challenge/response handshake is repeated in the opposite direction for mutual authentication. Unfortunately, an attacker who captures these frames possesses the plaintext, ciphertext, and the initialization vector used to turn the plaintext into ciphertext. Because wired equivalent privacy (WEP is an algorithm used to protect wireless communications in Wi-Fi from eavesdropping and to prevent unauthorized access to the network) uses RC4 (RC4 is a stream cipher designed by Rivest for RSA Security. It is a variable key-size stream cipher with byte-oriented operations. The algorithm is based on the use of a random permutation) encryption, this is enough information to derive the RC4 keystream—the stream of bits XORed with plaintext to generate ciphertext. Knowing a legitimate initilaization vector and keystream lets someone successfully respond to any future challenge, without actually knowing the actual shared key. You thus gain a permit to join the wireless LAN.

Bluetooth

Bluetooth is a low-power, short-range wireless communications technology. Two engineers at Lucent discovered a flaw with the way encryption keys are exchanged and found, how easy it is to obtain address of another device. Also, the E22 algorithm, which is used for key generation, takes input of a PIN, the length of the PIN, and a random number. Most of the devices by default have 0000 (only 10^4 combinations) as their PIN, which sometimes doesn't get changed. Random number and length of PIN are sent out in the clear, and its pretty easy to figure out what happens next. It gets even more interesting - you could join a conversation between two devices without them knowing it and even masquerade as somebody else. This was explained in further detail in the research done by Juha Vainio of Helsinki University. There are some other similar issues with the protocol.

Bluetooth and similar technologies allow you to form peer-2-peer (P2P) wireless networks, which can be very fluid. However, their movement depends on the devices that are Bluetooth enabled – so how do you monitor that? If I can connect to your device without your knowledge, who is watching? What if this device is a Bluetooth enabled laptop, and while you are preparing the business plan for a hostile take over, I am downloading files from your computer and zipping them to your competitor. After all people have done that using Line of Sight (LOS) IR technology, Bluetooth doesn't even require LOS. What are your options – not give out Bluetooth enabled laptops? What if that's the default?

Wireless WAN

Many have considered Global Systems for Mobile Communication or GSM a secure standard for sometime, however it's A3/A5/A8 encryption and authentication algorithms have been available to the hacker community for a while. ETACS (enhanced total access communications system), which is a second-generation wireless technology available in some parts of Europe and Asia, has an encryption algorithm, which is essentially, security by obfuscation rather than an application of a true encryption scheme. What does this mean? For the algorithm, A is really H, and H really is T, and so on and so forth, so if this new language is leaked, transmissions are in the clear.

How many companies do you think have a policy on handhelds and cell phones? Not many, I am willing to bet. Why not? After all, they do have strict policies for desktops and laptops (although these not always strictly enforced). Isn't the information accessed via these devices equally important and sensitive? What if your phone or PDA gets stolen? What are the risks? I have long argued that, with the advent of M-commerce, fraud is going to increase. You will hardly find carriers acknowledging this or a conference presentation on the subject, but you know, it's happening as you read this. Information and systems are more interconnected than ever, compromise of one link leads to break-ins into others.

If your cell phone had gotten stolen or someone had opened an account under your identity five years ago, the worst that would have happened to you: you raking up $20,000 worth of airtime in dealing with drug lords of South America, getting unpleasant FBI inquiries, and on discovery, carrier and FBI apologizing profusely for mistaken identity. The carrier would have had to write-off the fraudulent charges.

If however, this theft happens today, by using a few keystrokes, one could be checking some of your email accounts, your stock portfolio, etc, without having to even worry about using any password or PIN. Things could get ugly very quickly. In addition to $40,000 (inflation) worth of airtime, you could be prone to potentially irreparable harm. So, should your usage of phones be banned?

Earlier this year, the CEO of an Internet firm was exchanging messages with his executive staff using Instant Messaging; discussing strategy, employees, and partners, with few reservations. Guess what happened? The messages were getting logged; somebody hacked into the servers, and published the logs on the Internet. It has done irreparable damage to the company; the majority of the senior staff has left, partners are distancing themselves from the company, and the CEO is trying to fight several lawsuits. Maybe his IT staff should have enforced encrypted logging or no logging at all. Oops!

Some companies go to an extreme by canceling or postponing some projects because of security reasons. Depending on the situation it doesn't always make sense to do that. You have a choice to make, to be an innovator, adopt, learn, innovate, and work around the issues or wait and be a laggard until all the security issues are ironed out. Being early obviously has its risks and should be carefully evaluated as such, but if the technology can offer you a business advantage, don't shut down the project just because you don't feel comfortable with it. In all the security flaws discussed above, there are ways to work around the loopholes.

Social engineering has been the time-tested art of breaking-IN since time immemorial. Until we turn into robots or something, I don't see the threat from SE going away (In wireless, the technical fraud (cloning, breaking algorithms, etc.) is going down, but subscription fraud is on the rise). So, how do you guard against that – not by encrypting every word that an employee utters or types, but by making sure, that utterance is only to trusted sources. This is in addition to all the infrastructural things you have to do to make things secure.

Continued on Page 3

Continued from Page 2

Do you want to guess if there was a policy change at Qualcomm when Irvin Jacobs (CEO and Chairman) lost his laptop containing a ton of proprietary information at a conference? No using your spouse's name as your password, not that any body does that.

My point in all of this is that, no matter how well you prepare to guard your assets through technology solutions – encryption schemes and such, things don't work that way, and problems are not that easy to solve. Unless you identify your key assets and think clearly about what risks to them exist, then think through affordable and usable counter-measures and have strict policies, things are bound to fall apart at some point.

You also need to have a plan ready to act on in case something *does* go wrong – to minimize damage.

To grow your enterprise, you have to think out of the box, by constantly exploring and experimenting, staying ahead of the curve, and by informed risk taking.

Citibank did just that. An executive in charge of wireless program had a tough time convincing their internal IT about launching wireless initiatives. But after several discussions and negotiations, and by taking extra steps to secure transactions between carrier gateways and Citibank infrastructure, and by introducing extra checking and proactive monitoring, he was able to convince IT that this setup is similar to or better than their current Internet security.

Result: Citibank was one of the first banks to roll out wireless services worldwide, immediately reaping benefits of innovation, brand extension, and customer satisfaction. While the competition is still trying to figure out their wireless strategy, Citibank is moving on to the next generation of wireless applications and services.

Let's look at the consumer side for a minute.

Pop Quiz

Q. Do you want to guess how much fraud VISA and MasterCard wrote-off in 1999?
A. Thousands of dollars B. Millions of dollars C. Billions of dollars

Answer is C. A whopping $26.01 B to be precise.

Ouch!

We have entered into a world where players in the value chain need to look out for each other. What do I mean by this? If you are to buy a set of books from Amazon.com using your AT&T web-enabled cell-phone, your transaction is flowing through at least three different vendors – AT&T, Amazon, and the credit card company of your choice -- before your transaction is approved. What if the person used a fraudulent credit card, but it doesn't arouse enough suspicion to decline the transaction. What if Amazon felt the same about the user, but not enough to raise suspicion on the transaction? And, what if it was a real-fraudulent transaction. Oh! Nooo. The risk is shared; the consequences of any particular incident might fall on any one of the participating companies, and failure to provide for such situations as a matter of policy can damage or destroy companies' partnerships. The stakes are too high not to act.

As fraud becomes more rampant, vendors will be more willing to share information, and they really don't have to share user account and personal preferences, etc., but just info about the level of trust and confidence on any transaction. So, say AT&T processes the data call – applies 80% confidence level, Amazon.com says it's only 70% sure, and MasterCard only feels comfortable with 60% rating. You see where I am going with this. Simple math will yield overall confidence as 33.6%, which could be below a threshold agreed to by the players, so either the transaction can be stopped or further action is required. The parameters for allowing a transaction could be set independently or by using compounded information. With cooperation, there will be a much better chance to detect and prevent fraud – in REALTIME.

Now, you can add this to your business requirements.

I am pleased and excited to bring you three AORTA exclusives in this issue. Tod Knight, our CTO, concludes his two part series on *"Waves of Technology—Expectations and Reality"* and leaves us to ponder on the next wave.

David Quackenbush, our COO, who has experienced and lived through several waves, pens down a thought-provoking column: *"Corporate Culture and Innovation—Can we combine them?"*. Review and embrace the characteristics he outlines for an innovative corporate culture.

And finally, this month's guest column *"I dream of computers …"* comes from Dmitry Kaplan, my long time friend and mentor. He taught me how to think. His algorithms (for which he has been awarded many patents) help save lives (Defibrillator units), ward off wireless fraud (RF fingerprinting systems), and keep your kids away from unwanted content (X^3-filters).

Enjoy.

My sincere thanks to Tod, David, and Dmitry for their time and their respective columns.

Your comments are always welcome.

Best wishes,

Chetan Sharma

Have a cool idea, story to share or want to ask a question?
AORTA Submission Deadlines
10th of each month

Waves of Technology—Expectations and Reality (part 2 of 2) - *Tod Knight, CTO*

The first part of this article presented some of the trends I have seen as we have transitioned through several Waves of Technology (WOTs). In this installment, I will present some of the patterns I have observed in this chaos and see if we can use them to help us predict the future.

Figure below illustrates the key patterns I have observed that can help us understand where we have been, and perhaps, where we might be going in the future.

Here are some comments and disclaimers to keep in mind while viewing this figure:

1. This is not meant to be all-inclusive of all technologies, but rather representative of large, important factors.

2. There are certainly smaller, albeit important, "mini-waves" within most of the major WOTs.

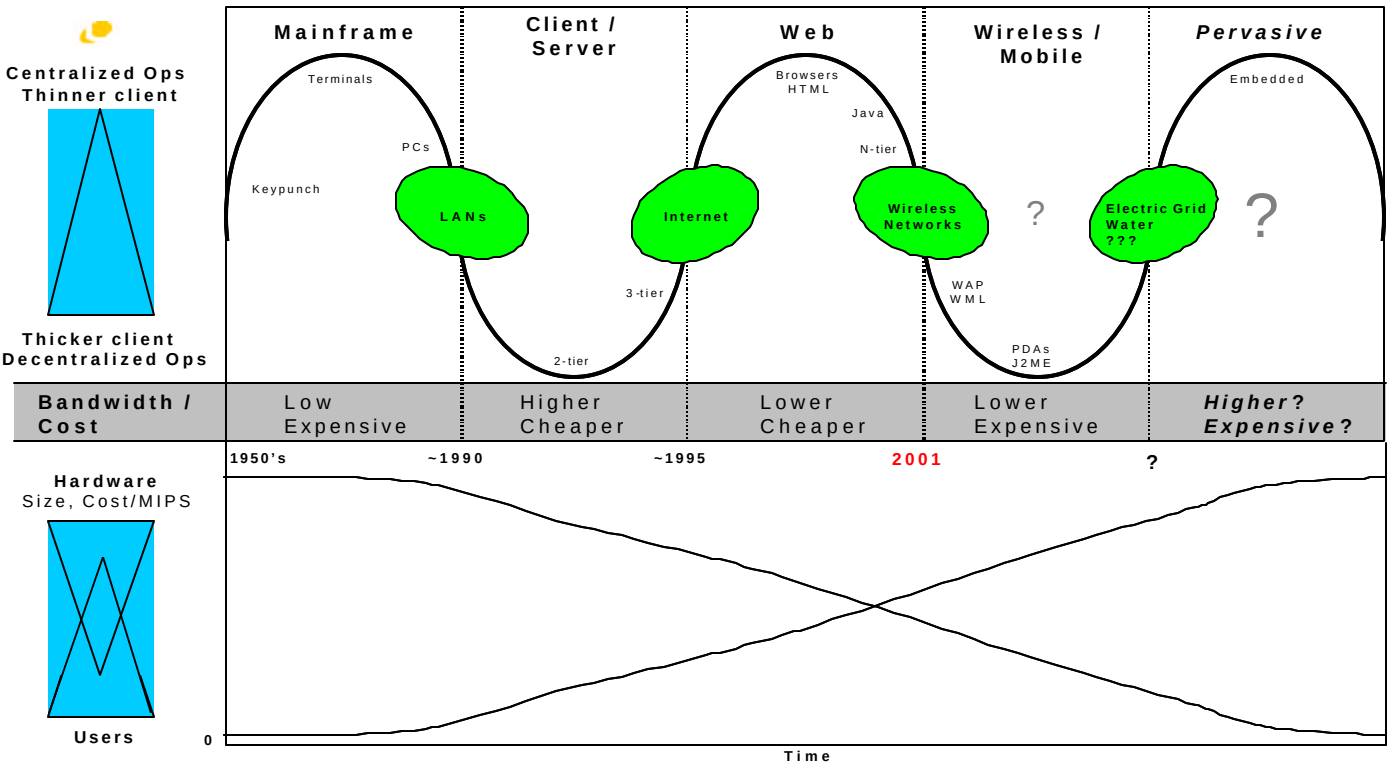
3. The timeframes attributed to the patterns relate to the mainstream adoption of a particular WOT, not the early adopters living on the bleeding edge.

4. We are only at the very beginning of the Wireless/Mobile WOT so things represented beyond today are based on two things: experienced opinion; and the exercise of applying the historical patterns represented by this graphic to the future.

I believe a key pattern to note on figure below is that at each inflection point between WOTs there is a significant change in, and adoption of, networking capabilities. While I do not know if Andy Groves was necessarily referring to these specific inflection points when he said "every strategic inflection point [is] characterized by a '10X' change", I think it definitely applies here.

It is also interesting to note (although if you are reading this you have probably *experienced* it) that the duration of the waves we have already been through has become increasingly shorter. On top of that, I believe it is widely accepted that the progress and innovation in the latter (and shorter) waves were orders-of-magnitude larger and more important than the preceding WOT. As we look to the future and the Pervasive WOT it is probably hard to believe that it will be as short (or shorter) in duration than previous WOTs and that we may experience even more advances in that shorter period of time. If we use the patterns illustrated by Figure we might be able to make a project that it *will* be shorter, but not knowing what lies beyond makes this speculation pretty mind-boggling.

In a future article I will discuss the Pervasive WOT. In the meantime I will leave you with this: What lies *beyond* the Pervasive WOT? Robots and nano-technology? Artificial Intelligence? Molecular computing? Neural networks? Or is it *The Matrix*?



I dream of computers .. - *Dmitry Kaplan*

I am not a Luddite. Really. I often like the mechanical and silicon beasties that surround me. As proof of my dedication, I forewent more than a few years of my youth entreating with the wizards of the Ivory Towers to imbue my poor brain with the arcane trivia of Electronics and other dark arts. For my perseverance I was rewarded with letters after my name and the skill to sound important -- the right to call myself an engineer.

Every engineer lives through a few "revolutions" in their lifetime. The "REALLY BIG catapult" revolution, the "hot steam" revolution, the "fly horizontally" revolution (the "fly down" revolution was short-lived), etc. As the pace of engineering increased, the rate of revolution turnover increased as well; in a relatively short career, I can vouch for at least two: the "wireless" and the "personal computer". Today's lament is about the latter. I am going to argue that the current Personal Computer that attempts to perform a great variety of unrelated tasks has become a behemoth of complexity and the majority of computer users don't use more then a tiny iota of their machine's capabilities. But they are paying a terrible price for the feature creep in their software: more expensive and more fragile experience.

"You know you've achieved perfection in design, not when you have nothing more to add, but when you have nothing more to take away".

Consider yours truly.

1. I am perfectly capable of diagnosing and repairing a great majority of problems on my computers. I have four. Networked too. With real wires. And I am of a learned minority who actually know what goes over the wires. I can really dig into every grand mal e-seizure and administer a precise cure.
2. I don't. My daughter's computer still can't print over the network. I bought her a cheap printer because I didn't want to deal with it. That printer died the other day. I'll buy another one.
3. The main computer needs to be rebooted daily and Netscape needs to be re-installed every fortnight. Don't tell me about Linux. I am an old Unix devotee and work with Linux daily. Linux-only is simply not an option in a household with kids. If you don't understand why, you don't have school-age kids.
4. I fix computer problems for a few neighbors and friends. Perfectly intelligent people. A few doctors and PhD's. Tired of re-installing Windows. I am ashamed to suggest to them to re-install Windows. When is the last time you took your phone apart and tried cleaning the inside when it quit working? Did you try to re-arrange the buttons? Did you unplug it from the wall, waited for ten seconds, then plugged it back in? Did you clean the registry, har, har? You tossed it, didn't you?

Do you know why you tossed that broken phone? I know why!

1. It does one thing. It has two modes of operation: a) works well enough to hear charity volunteers and b) can't hear a damn thing. When the latter level is reached, either precipitously or by slow metastasis, you know it is not working.
2. Repairs available to you are few. A new battery. A carefully administered whack in the direction opposite to the direction of fatal fall (hey, we all do that, if only to hear the death rattle of dislodged innards). If phone is expensive and it's under warranty (now where would that warranty be?), you can try calling the offending PhonesRUs and beg. Because you have more than one phone, or can actually get another phone to make that call. Another device that does exactly what the broken device did. Convenient, isn't it? Don't even have to upgrade your phone wiring to 8.3.4 or later version to use the new phone.

Notice that with a phone, there is never an issue of it basically working but not doing what it used to do. You also know that if the phone's turned to the dark side, your microwave will not be affected. Your cat will not throw up. This is very important. Not the cat's health, but the idea that our world is made up of relatively simple, independent and uncorrelated events and machines. In fact, the rare causal relationships make good stories: "I was hanging a picture and nailed right through the water pipe and flooded the first floor pantry". See, it's a good story because it is highly unlikely that failure to hang a picture will result in a plumber's paradise. Now think of your computer experience. How many times have you really, really regretted ever installing a new cool software? All of us experience that dreaded feeling of wanting to simply go back in time, before the fateful double-click. Because it broke something else and you can't figure out why and how. You've just entered the death spiral of upgrade-and-reinstall-everything-in-sight, just hoping to get back where you were, never mind the game.

So where am I going with that? I don't believe that the do-everything box that the current PC has become is maintainable by an average person. The number of incompatibilities grows geometrically with the number of tasks any machine is required to do.

Continued on Page 6

Continued from Page 5

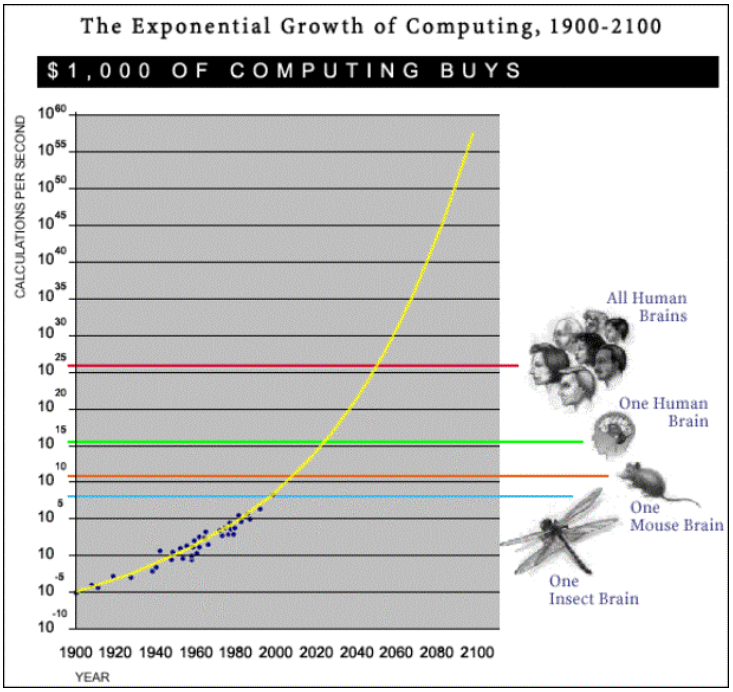
This creates a web of interlinked failures that are unobvious and insidious. Failures that come and go depending on factors beyond your ability to track easily – when's the last time you kept track of the number of page swaps per second? Right. A PC is also devoid of separable chunks, rendering the basic car repair technique of "keep replacing pieces until it works" completely useless. You can't replace software or even hardware piece in a PC without multiplying your problems. Parts are not interchangeable. What's a user to do?

Right now, there is nothing but hope for the future. It is my firm belief that the cure will arrive slowly in a form of a PC becoming a control center for a collection of interlinked but independently operating pieces. I admit it's harder with software, but consider a computer consisting of a CD-burner, a DVD drive, a hard disk, a floppy, a CPU, a camcorder, a display module, a keyboard, a mouse, etc. all connected with in a self-configuring network (Firewire, wireless, tachyon waves, whatever). The point is, I can watch a DVD and burn a CD when my mouse dies. I simply plug in another pointing device and it figures out what it's supposed to do and the rest of the devices are not affected. If I want to use a word processor, I plug in a word processor software box into the network. When I don't, I unplug it. Each software module is a self-contained device (or a memory chip, or an icon, or an optical quantum memory bubble – use your imagination) that can be unplugged and plugged in and is free to fail on its own accord but is not allowed to break other things. You don't have to reboot the computer, fer-goodnessakes to continue working.

When a device fails, you can plug in another functionally similar device and continue with your work. That's because functionally similar devices share interface definition. We will have to give up such perversions as mouses with built-in radios and keyboards with calculators. No-one uses that junk anyway (after the first ooh-aah day, that is). One device, one (or a few) simple functions. Life's good! But hey, if you want a radio in your mouse, go right ahead. But when your radio dies, don't be surprised when the mouse quits working.

Modular simplicity. It's the key to future PC sanity. I will now stop pontificating and leave you with some of the wisest words ever spoken on the subject of multiple functionality and feature creep: Antoine de Saint-Exupery: *"You know you've achieved perfection in design, not when you have nothing more to add, but when you have nothing more to take away".*

Dmitry Kaplan has spent a better part of a decade late last century collecting letters after his name at the University of Washington. Since then he's bounced from industry to industry, playing with electronics and math, hoping to maintain his record of being right more often than wrong. He owns a typewriter and a mechanical calculator... just in case.… He can be spammed at dmitryjoy@yahoo.com



Stat Focus

From Ray Kurzweil's forthcoming book *"The Singularity is Near"*

AORTA Challenge

You just received $200 million in venture funds to work on an *idea* you always felt passionate about. You can hire the best people in the world. What will you use the funds to work on and why? Send me your thoughts. Summary in next issue.

Best entry gets a nice gift.

3G Perils

Remember the fourth point in the column "Deconstructing 3G Mythology" (AORTA Issue 2) about the pain phase of technology evolution?

Even mythical DoCoMo is not immune to that. They delayed their much publicized launch this month. British Telecom also announced the delay in it's 3G launch.

What does the delay mean to DoCoMo, BT, and more importantly to the 3G fan club? As I was telling a journalist covering the story, for DoCoMo and BT, the fight is still on for bragging rights to be out there first.

As for the rest, it gives them some breathing space to sit down, relax, and revise their aggressive rollout schedules.

Corporate Culture and Innovation – Can we combine them? – *David Quackenbush, COO*

It's amazing how many books have been written on the subjects of Culture and Innovation. So far, I have not seen many that focus too much on combining the topics. Sure, there are chapters devoted to creating cultures and environments that spur innovation, but very little talk about building an innovative culture. There are many questions that must be answered regarding these subjects. The questions addressed in this article are:

1. Can we build an "innovative culture"?
2. Have we made the concept of innovation too mysterious?
3. What are key characteristics of an "innovative culture"?

"The best way to get a good idea is get a lot of ideas"

Can we build an "innovative culture"? The answer depends on who "we" are and how we define innovative. First, it is hard for any group to build a culture. Instead, I think a culture evolves based on the collective interactions of a group over time. In our case, we have tried to establish a set of basic values for Luminant that are shared across the company. Using these values as a foundation, we can start to assemble some common cultural characteristics. But the job of creating the real culture rests with each geographical group within the company. I believe with a company like ours, it is impossible to define a culture that fits every group in our company, and instead we should use our values and core cultural themes to build geographic specific versions of our culture based on the personality of each geography. Let's use the second question to explore the definition of innovative.

Innovation, as a word in a statement, can be very intimidating for some. We use innovation like we use re-engineering. It has become a word that is used so much to describe "how" we should be, and what successful companies should be, that its meaning has become more of a mystery to some. I would like to propose that innovation begins just to the right of common sense. Some of the best innovations are improvements to things that have been around for a long time. In many cases, these "innovations" are really just the natural evolution and recognition of process improvement. Take the concept of eBusiness. Is eBusiness a radical new innovation that just appeared on the scene a couple years ago? Or is it something has been evolving since the advent of the modern computing age? Everything you read indicates a radical innovation. I believe it is just part of the natural evolution and convergence of two powerful innovations, the computer and the network.

The other side of innovation is opportunity. Many innovations are the result of seizing an opportunity and taking action. Take Enron, for example. Enron has been voted the most innovative company by Fortune Magazine 6 years in a row. Their main innovation occurred many years ago when they created the first financial markets for trading natural gas. They saw an opportunity that was created due to the de-regulation of the natural gas transportation business and were able to take advantage of that opportunity. And most importantly they took bold action to create and capture this market. That was an innovation. Since that time, most of their "innovations" have come from extending and improving on that concept.

So as you can see, being innovative does not mean you need to have the next "great idea", it can be an incremental improvement in something that already exists. This of course presents a great opportunity for us as we get exposed to the many different business processes and models of our clients. We are in the unique position of looking at these from a different perspective and should therefore be in a position to offer innovative (read incremental improvement) solutions to their business. Now that the definitions are clear, what characteristics should we be looking for in building an innovative culture?

Defining the characteristics of an innovative culture is a more difficult task, for the simple reason that many of these characteristics are intangibles that do not lend themselves to simple statements. However, some characteristics include:

1. Having a new idea funnel that allows people to provide new ideas (solutions) for how we should deliver services to the market. As Linus Pauling said, "The best way to get a good idea is get a ***lot*** of ideas."
2. Recognizing innovative results with both clients and internal improvements
3. Evaluating people based on their ability to provide new ideas to clients
4. Establish the expectation that part of your time here should be dedicated to creating new concepts/ideas/solutions.
5. Encourage and reward calculated risk taking.

There are companies that embrace many of these characteristics today. Enron and 3M are among the most visible.

Continued on Page 8

Book Recommendation

TechVenture
Mohan Sawhney and Co.

Drawn from the popular TechVenture program at the Kellogg School of Management, this book provides a deep understanding of the key finance and business trends in e-commerce. Viewing Silicon Valley as a test lab for e-commerce strategies, this book delivers the latest financial and business models shaping the e-commerce industry. TechVenture focuses on the Silicon Valley phenomenon, the new financial strategies, and evolving e-business.

Continued from Page 7

Another, which was founded on these concepts, is IDEO whose business is creating products, services, and environments for companies pioneering new ways to provide value for their customers. This is an area where we are improving our focus as well. Clearly, we have room for improvement, but we are heading in the right direction.

So, where are we at building an "innovative culture" at Luminant? This is not something that can happen overnight. If you look at the companies that possess an "innovative culture" they have done so over a long period of time by constantly recognizing and rewarding the behaviors that generate innovative thought and action. In order for Luminant to build an "innovative culture" we must all take responsibility for making innovation part of our culture. This is not the domain of a few, but a responsibility for us all. And we must continue to look for creative ways to recognize and reward this behavior.

Finally, we should not be intimidated by the word "innovate". Instead, we should all have the confidence to bring new thinking to the forefront of this company no matter how simple that new thinking appears. We should all remember three things regarding this point. *First*, ideas that seem simple and pedestrian to us may actually be very powerful to the right audience and situation. *Second*, something you may regard as common sense may not be "common" to everyone else. *Third*, the more we share our ideas with each other, the more and better ideas we will generate together.

Bluetooth having an ache?

Two Ericsson engineers started work on Bluetooth in the mid-nineties. For the past two years, it has competed well with WAP and 3G to capture the headlines for all things hyped. Things were going pretty well for it until 2001. We always knew that interoperability and interference were going to be the two biggest issues to plague Bluetooth. So far, there hasn't been any let down. But in all honesty, let's cut Bluetooth some slack. After all it's new standard and we are still making progress. However, it's time for another reality check.

There is no doubt that the world needs a low power, small range, high bandwidth protocol, but 3 of them? It still remains to be seen which ones will survive. HomeRF, IEEE802.11a/b/I or Wi-Fi (I wish engineers came up with better names than these), and Bluetooth are vying to be on a device near you. One of the clear benefits is cable replacement, but there are other applications as well, like creating your own P2P piconet to exchange data at high bit rates.

Recently, Microsoft pulled support for Bluetooth in its upcoming OS version, a big blow to the supporters of the standard. Microsoft's support would have meant instantaneous worldwide support. Microsoft is a big proponent of IEEE802.11 and has been using it internally quite extensively. Intel is also backing away from some Bluetooth projects (Intel also announced they will stop making HomeRF products). Security issues with both Wi-Fi and Bluetooth are well documented (we discussed some of them in our security column).

One of the biggest problems with Bluetooth is also going to be shipment of devices. This is one of the issue that turned the tide (downwards) for WAP, and if the situation doesn't improve anytime soon, Bluetooth will meet the same fate. Proponents of Bluetooth should move quickly to address:

a) interference with Wi-Fi and HomeRF,
b) interoperability amongst vendors, and
c) shipment of devices,

to prevent a fatal trip to the dentist.

So far the only people who have made money on Bluetooth are the analysts who have been predicting Bluetooth world domination in their >$5000 reports.