Point of View

Trust Clouds

An Emerging, Horizontal Information-sharing Service for Governments

Authors
Jeff Frazier, Cisco Internet Business Solutions Group
Charles Jennings, CEO, Swan Island Networks

January 2009

Cisco Internet Business Solutions Group (IBSG)

Trust Clouds

An Emerging, Horizontal Information-sharing Service for Governments

By Jeff Frazier, Cisco Internet Business Solutions Group, and
Charles Jennings, CEO, Swan Island Networks

Introduction

Our view is that government leaders should :

- *Harness the dynamism of social networking and Web 2.0 technologies, quickly but carefully.*
- *Assume a leading role to enable Web.2.0 mediums that are significantly more trustworthy—in particular, through highly secure, rules-driven, virtualized computing networks known as "Trust Clouds."*

Our argument has its beginnings in the New Mexico desert . . . .

At the foot of the Rocky Mountains, near Santa Fe, Guy Theraulaz changed the life of Eric Bonabeau. Guy, a French scientist studying division of labor and nest construction among social wasps, introduced Eric, a France Telecom R&D engineer, to the amazing world of swarm intelligence: The collective cleverness of insect colonies, flocks of birds, and other animal groups.

Individually, one insect isn't capable of much, but collectively, social insects can build palaces of dirt, fill stores of food for winter, raise young broods together—even construct complex bridges and chains. Solutions to problems are emergent rather than predefined and preprogrammed. Ants, for example, do not use blueprints to discover the shortest path to a food source. To solve this optimization problem, they employ constant, simple interactions, guided by a few simple rules. They connect, stay in tune with their environment, and adapt. The results can be amazing.

Listening to Guy's story was an epiphany for Eric. Back at France Telecom, he started applying the ant metaphor to computer information routing, a recurrent telecommunications network problem. Routing is needed because, for cost effectiveness, most large-scale communications networks are not fully connected. Thus, messages have to be guided through the network to reach their destination. Eric found that by allowing virtual ants to leave virtual pheromone at the network's nodes or routers, he could optimize the routes that messages take. The technique worked wonders.

Eric used an approach scientists call emergent computing: essentially, building systems that can self-organize and continually adapt to changing conditions—in other words, modeling the approach of social insects and animals. The key to this model is to create highly distributed systems, with many simple nodes communicating continually and operating under a few simple rules.[1] This is the essence of social media today.

[1] *Swarm Intelligence: An Interview with Eric Bonabeau,* Dick Story, O'Reilly Network, 2003.

Network routing is just one of the complex human problems to which the principles of emergent, self-organizing behavior can be applied. We examine its potential role in the deployment of a highly secure government network system for the sharing of critical information. We will discuss both what the concept of emergent computing can offer in this scenario and how best to combat the challenges that it presents.

A Top-down Problem: Connecting the Dots

In the aftermath of the terrorist attacks on America, the 9/11 and Weapons of Mass Destruction (WMD) Commissions, various U.S. congressional committees, U.S. Government Accountability Office reports, and popular media commentary all agreed: The U.S. needed better information sharing for intelligence. No clear pattern emerged that could have predicted 9/11, and no action was taken to question the potential terrorists—because the conspiratorial dots were not connected in time.

And yet, seven years later, broad "connect the dots" information sharing in America has yet to emerge, and the problem may even be getting worse. As noted in H.R. 6193, the Improving Public Access to Documents Act of 2008, which passed in the U.S. House of Representatives recently:

> The control markings problem, which has worsened since the 9/11 attacks, causes considerable confusion about what information can be shared with whom both internally at the Department of Homeland Security and with its external partners. This problem negatively impacts the dissemination of homeland security information to the Department's state, local, tribal, and territorial homeland security and law enforcement partners, private sector customers, and the public.

> "Our goal now is not to build walled gardens or fortresses .... We have competitive asymmetric advantage in our open society and the free flow of ideas; we achieve strategic asymmetric advantage on the battlefield by moving ideas to action quickly—and that means taking advantage of tools like the social web. Manage its risks, yes; but slam the brakes on the social web, and we risk fighting with one hand behind our backs in the asymmetric battlespaces of the future."
>
> Zachary Tumin
> "Twitter Jitters," October 28, 2008, Leadership for a Networked World
> blog, http://www.lnwprogram.org/blog/archive/2008/10/

Barriers on the road to a government network of networks have been many. Issues of culture, turf, and policy have proven significant, often appearing insurmountable. Technical issues related to identity stores, public key infrastructure (PKI) schemes, and competing data models have added to the difficulty—though we would argue that this is largely the result of a "the great is the enemy of the good" dilemma.

Recently, though, there has been some good news on the policy front. The U.S. federal government has settled on a new policy for sensitive information sharing. Known as CUI, for Controlled Unclassified Information, it rationalizes well over 100 government-sensitive information policies down to a simple framework with a few distribution rules, built-in security, and access-control safeguards. On May 9, 2008, a U.S. presidential executive order was enacted. This begins to address the mandate that CUI immediately replace the antiquated Sensitive But Unclassified (SBU) standard, and that government agencies deploy it gradually and within five years.

A Bottom-up Problem: Trust and Social Media Systems

So, a new, greatly simplified, high-assurance approach to government-to-government exchange of sensitive information has now been codified into law. And though there's still much room for improvement, "new media" technologies of collaboration are now more than ready. In fact, they're being used every day, even in emergencies:

- In the recent wildfires in California, a Second Life mashup operated by young teen boys routinely provided better, faster, more reliable evacuation notices than the local reverse 9-1-1 system (according to a local Department of Homeland Security official).
- When cellular communications failed during the Los Angeles–area earthquake of July 2008, Twitter was the emergency communications platform of choice. The Red Cross is also using Twitter—to replace emergency phone banks. And during recent hurricane disasters, individuals came together via the Tsunami Help Blog and Katrina Help Wiki.
- In Europe, the Swedish Emergency Management Agency is operating its own mashup, complete with internetworked communities of trust that stretch from the prime minister's office to local ambulance dispatch.

The "new media" has been harnessed to enable citizen participation at very little cost. This captures the full promise of collaboration technologies—simply stated, it is about keeping the lines of communication horizontal, with simple rules, as the least common denominator. This is the power of "Spontaneous Order."

We're not suggesting that the solution to the complex problem of sharing emergency and intelligence information is to put it all on Facebook and comment with Twitter tweets. But we do believe that a new breed of Web 2.0 technologies can be used to foster much greater and more agile connectivity among government workers and their collaboration tools—and that, if applied broadly and horizontally across agencies and jurisdictional domains, such tools can help government self-organize and create agile, new information services that will help its workers respond more effectively to critical problems, especially emergencies.

Increasing use of social media technologies by ordinary citizens in emergencies, however, presents a different, but no less pressing, information-sharing problem. With familiar social networking systems, there is no trustworthy way to authenticate either the information or those with access to it—or to ensure that it does, in fact, reach those who need it. Government needs to act to provide not just collaboration, but also information integrity, linked to real sources of expertise and authorization. And the action needs to take place soon—before free-for-all social networking swarms completely dominate government information-sharing environments.

> "The Leadership for a Networked World (LNW) program…of the John F. Kennedy School of Government at Harvard University…taps into the diverse knowledge and talent of the Harvard community…. Current efforts are focused on the 'cross-boundary' challenge of transformations operating across traditional organizational boundaries, such as departments, jurisdictions, branches of government, sectors of the economy, and national borders. We believe that cross-boundary reforms represent the next wave of the enormous opportunities and challenges opened up by information technology and networked organizational models."
>
> "About LNW," Leadership for a Networked World blog,
> http://www.lnwprogram.org/about_overview

The Trust Cloud

So how can trusted source information in government systems emerge? The first step is to start experimenting with commercial social networking technologies/services. Start simply, but *start*. This is as simple as beginning with personal use authentication of weather information, Google terrain maps, or information inputs by known and pre-authorized communities.

Fortunately, new, interconnected commercial IT resources, collectively known as "The Cloud" or "Cloud Computing," make starting easy. Cloud Computing mimics the behavior of social insects, massively connecting simple nodes and operating under a few basic rules to achieve complex, adaptive behaviors. The essence of the Cloud is this massive, anytime, anywhere, standards-based connectivity. It is a growing network of physical and logical data centers that is rapidly changing IT and business models across the planet.

The Cloud, like the Internet itself, does have a dark side populated by cyber attack threats and rogue users. But, the U.S. government, by using both its large IT footprint, and its innovative, new CUI policy framework, could substantially increase information assurance and protection in information-sharing systems by layering new levels of policy and technology trust into the Cloud. It could, in fact, launch a whole series of new Trust Clouds—trusted computing services accessible across agencies and jurisdictions by authenticated users.

Recommendations

Our recommendation to governments and their partners: start trying new services delivered out of the Cloud. Demand that CUI be built as an information-protection standard, and apply it in situations where no better standard currently exists. Then begin connecting—and sharing resources and information out of new, trusted cloud environments—using Web 2.0 technologies.

All that's needed, really, is the bureaucratic equivalent of a snap of the fingers. Launching information sharing as a service can be accomplished within in matter of weeks, in a form that can be supported by multiple government agencies, and made available to various, trusted partners:

- Align information-dissemination rules as closely as possible to CUI, without making the service officially CUI-compliant.

- Adhere to an "opt-in" model that allows each organization participate at whatever "start small" level it deems appropriate. There should be no top-down, forced rules.
- Start with open, nonsensitive information only.
- Dub this new information-sharing arena a "failure-tolerant" environment where a lean-forward attitude is accepted as the norm.
- Designate it as a commercial service, operating not unlike a traditional telecom provider or a third-party subscription service. This includes inherent liability protection.
- Openly solicit the participation of nonfederal partners, including those from state, local, tribal, international, and private sectors.
- Use only available, off-the-shelf technology. Government should build requirements, not systems.
- Capture feedback, collect lessons, iterate, and scale quickly.

The U.S. government has lost control of information flow during emergencies in part due to the proliferation of available information on personal, connected devices. Now, government has the opportunity and responsibility to capture and harness human intelligence through a simple rules strategy that uses Web 2.0 to its advantage. Plenty of Web 2.0 veterans, citizens, and government information providers are poised to "opt in." Once these services become available, the behavior of government early adopters across the country will work together to help new systems emerge—just as has occurred with "new media" continuously over the public Internet.

Acknowledgements

Cisco IBSG would like to acknowledge the significant contributions of Charles Jennings, founder and CEO of Swan Island Networks, Inc., to the development of this paper.

More Information

The Cisco Internet Business Solutions Group (IBSG), the global strategic consulting arm of Cisco, helps CXOs and public sector leaders transform their organizations—first by designing innovative business processes, and then by integrating advanced technologies into visionary roadmaps that address key CXO concerns.

For further information about IBSG, visit http://www.cisco.com/go/ibsg.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.