

# **IT Security Architecture and Web 2.0: Brave New Worlds**

*A Case Study*

*Shay C. Colson*

*April 26, 2009  
IST 700 - Spring 2009  
Scott A. Bernard, Ph.D.*

<b>Introduction</b>	<b>3</b>
<b>What is Web 2.0?</b>	<b>3</b>
<i>The 2.0 Revolution</i>	3
<i>Web 2.0 Defined (?)</i>	4
<b>The Social Focus: Web 2.0 and Social Networking</b>	<b>5</b>
<i>Library 2.0</i>	6
<b>Web 2.0 and Business: “Enterprise 2.0”</b>	<b>7</b>
<i>S.L.A.T.E.S.</i>	8
<i>Web 2.0 Poster Child: The Mashup</i>	9
<b>Government 2.0</b>	<b>10</b>
<i>Three Part Formula</i>	10
<i>Stumbling Out Of The Blocks?</i>	11
<i>Learning Lessons</i>	12
<i>Intellipedia - Sharing Done Right</i>	13
<b>Security 2.0?</b>	<b>14</b>
<i>Inherently Open - Inherently Insecure?</i>	14

<b><i>Security: A People Problem</i></b>	<b>15</b>
<b><i>The Facebook Paradox</i></b>	<b>17</b>
<b>Web 2.0 for the IT Security Architect</b>	<b>18</b>
<b><i>Going Mobile</i></b>	<b>18</b>
<b><i>Business in the Cloud(s)</i></b>	<b>19</b>
<b>Leveraging Web 2.0 Securely for Enterprise Success</b>	<b>19</b>
<b><i>2.0 tools and beyond</i></b>	<b>20</b>
<b><i>Mobile Solutions</i></b>	<b>21</b>
<b><i>Lightning in a Bottle: Harnessing the Cloud</i></b>	<b>21</b>
<b><i>Self-Securing Data</i></b>	<b>22</b>
<b><i>Focus: People Problems</i></b>	<b>22</b>
<b>Conclusion</b>	<b>23</b>
<b>Sources Cited</b>	<b>24</b>

## **Introduction**

The stars of Web 2.0 have become household names: Facebook, MySpace, Flickr, and many others. Yet, what exactly is Web 2.0, and what does it mean for the way that people live, work, and connect? Perhaps more importantly, what kind of security implications come from an ultra-connected society, like the one that Web 2.0 is rapidly creating?

Before the security implications surrounding Web 2.0, collaboration, and user-created content can be discussed, it is important that the concept of Web 2.0 and the various implications that stem from it be carefully considered. As I will discuss, Web 2.0 is not easily defined in the traditional sense, but has come to symbolize a movement of participatory engagement in content creation.

After an exploration of what has become known as Web 2.0, including the technologies and methods that preceded the movement and are arguably responsible for its existence, I will discuss the social implications of these newly formed interaction platforms.

From there, I will look to various applications of this “2.0” attitude: Enterprise 2.0, Government 2.0, and finally “Security 2.0,” a necessary revisiting of established security norms and practices.

Finally, this paper will turn its attention to Web 2.0 in an IT Security Architecture framework. Since much of Web 2.0 is founded on openness - user accessible APIs, the ability to create “mashups,” etc., I will discuss what implications Web 2.0 has for the IT Security Architect as they look to both leverage the value in Web 2.0 tools and mentalities, and yet create a secure enterprise-level digital collaboration space.

## **What is Web 2.0?**

The term “Web 2.0” has become part of the accepted technology jargon, finding itself tossed around today as if everyone knows exactly what the phrase means. What’s more, the phrase has become so common in today’s tech dialogue that it has become assumed participants know what the implications of something being a “Web 2.0” product are. In reality, however, this is far from the truth. The phrase, and its definition, continue to evolve and change, much like Web 2.0 itself.

### **The 2.0 Revolution**

The phrase Web 2.0 is claimed to have originated “with a conference brainstorming session between O’Reilly and MediaLive International,” when the bust of the “dot com” bubble was first seen as leading to a new Internet revolution. (O’Reilly 2005) The exact definition, however, remains particularly elusive. Even today, “the Web 2.0 meme has become so widespread that companies are now pasting it on as a marketing buzzword, with no real understanding of just what it means.” (O’Reilly 2005)

Despite their best efforts, researchers have been unable to define Web 2.0 without using Web 1.0 as a reference point. As one pair of researchers put it, “methodologies which have grown up around the Web no longer apply” in a Web 2.0 setting. (Cormode and Krishnamurthy 2008) In fact, it is entirely likely that just as Web 2.0 could not exist without its Web 1.0 pedigree, the phenomenon itself cannot be defined but for in reference to the earlier iterations of the World Wide Web.

This circular definition can be understandably frustrating, much like trying to define a word while not using the word itself. In my opinion, however, this characteristic fits exactly within the concept of Web 2.0 in that it is highly inter-dependent and also relies on those things that have gone before it; Web 2.0 cannot (could not) exist as an independent entity. Indeed, many of the web services that exemplify Web 2.0 as a movement (technological, social, and otherwise) emphasize this interconnectivity and embody the idea that Web 2.0 would be a disastrous failure if it were to become a technological or social island.

### **Web 2.0 Defined (?)**

The difficulty of defining the term has not stopped people from trying, however. By exploiting the Web 1.0/Web 2.0 relationship, AT&T Labs researches recently offered the following analysis:

the essential difference between Web 1.0 and Web 2.0 is that content creators were few in Web 1.0 with the vast majority of users simply acting as consumers of content, while any participant can be a content creator in Web 2.0 and numerous technological aids have been created to maximize the potential for content creation. (Cormode and Krishnamurthy 2008)

IEEE’s *IT Pro* magazine also relies on Web 1.0 when attempting to define Web 2.0:

Web 2.0 is both a usage and a technology paradigm. It’s a collection of technologies, business strategies, and social trends. Web 2.0 is more dynamic and interactive than its predecessor, Web 1.0, letting users both access content from a Web site and contribute to it. Web 2.0 lets users keep up with a site’s latest content even without visiting the actual Web page. (Murugesan 2007)

Even Tim O’Reilly, the coiner of the phrase, cannot help himself from falling into the comparison trap, using Netscape vs. Google as the exemplary and defining dichotomy. “Netscape framed “the web as platform” in terms of the old software paradigm: their flagship product was the web browser, a desktop application, and their strategy was to use their dominance in the browser market to establish a market for high-priced server products,” O’Reilly writes. Their service was static, predicated on being installed on a user’s local machine. Google, on the other hand,

began its life as a native web application, never sold or packaged, but delivered as a service, with customers paying, directly or indirectly, for the use of that service. None of the trappings of the old software industry are present. No scheduled software releases, just continuous improvement. No licensing or sale, just usage. No porting to different platforms so that customers can run the software on their own equipment, just a massively scalable collection of commodity PCs running open source operating systems plus homegrown applications and utilities that no one outside the company ever gets to see. (O'Reilly 2005)

The difference here is the way in which the user experiences the data. Google “is not a server--though it is delivered by a massive collection of internet servers--nor a browser--though it is experienced by the user within the browser. Nor does its flagship search service even host the content that it enables users to find.” Rather, “Google happens in the space between browser and search engine and destination content server, as an enabler or middleman between the user and his or her online experience.” (O'Reilly 2005) This experience, the data gatherers, combiners, refiners, linker, presenters, creators, etc., are quintessentially “Web 2.0.”

“The term ‘Web 2.0’ really only refers to the fact that there’s been a dramatic increase in functionality for the web. Maturing Internet users have become more savvy as online tools have become more challenging and complex.” (Knights 2007) Web 2.0 defies a widely agreed-upon, concise definition - perhaps because the underlying phenomenon is huge. (Murugesan 2007)

Indeed, in drawing upon the creative talents, energies, and ideas of users world-wide, Web 2.0 continues to break new ground and truly defies even the traditional concept of a definition. As one blogger put it, “Web 2.0 is an attitude not a technology.” (Davis 2005) This perhaps best embodies Web 2.0: an attitude more than a technology. The various technological implications will come and go (like the social network Friendster, for example) but the attitude behind these iterations will remain. Moving forward, the 2.0 attitude becomes increasingly important, especially when using 2.0 tools in the enterprise or government arenas.

## **The Social Focus: Web 2.0 and Social Networking**

Many of the Web 2.0 superstars are focused on one thing: social networking. These sites have quickly become household names. Facebook, MySpace, YouTube, etc. seem to have mastered the formula for driving enormous volumes of users to their site, engaging the users on their own level, and retaining the users to come back again and again. What is the draw? Why does social networking lend itself so well to the ‘attitude’ of Web 2.0? What implications does this have for the enterprise, in professional settings, and from a security perspective?

First, we must determine whether it is social networking itself that is driving these changes, or something much larger than that.

Social networking is defined as the act of building one's social network. People rely heavily on these relationships to help them with everyday tasks, such as making decisions, forming opinions, and/or finding information. As a result, one of the many uses of a social network is in conjunction with, and as a precursor to, collaboration. Leveraging one's social network vastly improves the ability to collect the right people and information upon which to collaborate toward a common goal. (Deans 2008)

Collaboration, as we have already seen, is probably the major driving force behind the phenomenon that is Web 2.0. So, the fact that social networking, Web 2.0 poster-boy, is driven also by collaboration should come as no surprise. In fact, social collaboration is likely the main reason for the existence of many of the Web's most popular sites. "With Web 2.0, the community's contributions are foremost: the site exists only to create and serve those contributions; the result of user-generated content is 'collective intelligence'. YouTube would not exist without the videos contributed by community members." (Warr 2008) The same could be said about Facebook, MySpace, or any other of the dozens of social networking sites that make up significant chunks of Internet traffic.

## Library 2.0

One of the professional communities that has raced to embrace the 2.0 revolution is libraries. In his 2006 paper "Library 2.0 Theory: Web 2.0 and Its Implications for Libraries," University of Colorado Professor Jack Maness describes the idea of "Library 2.0":

Library 2.0 could be understood to have these four essential elements:

- It is user-centered. Users participate in the creation of the content and services they view within the library's web-presence, OPAC, etc. *The consumption and creation of content is dynamic, and thus the roles of librarian and user are not always clear.* [emphasis mine]
- It provides a multi-media experience . Both the collections and services of Library 2.0 contain video and audio components. While this is not often cited as a function of Library 2.0, it is here suggested that it should be.
- It is socially rich . The library's web-presence includes users' presences. There are both synchronous (e.g. IM) and asynchronous (e.g. wikis) ways for users to communicate with one another and with librarians.
- It is communally innovative. This is perhaps the single most important aspect of Library 2.0. It rests on the foundation of libraries as a community service, but understands that as communities change, libraries must not only change with them, they must allow users to change the library. It seeks to continually change

its services, to find new ways to allow communities, not just individuals to seek, find, and utilize information. (Maness 2006)

Maness manages to capture the 2.0 ideology well with his four points, and provides a springboard from which others have applied the 2.0 mentality to their own industry. [See **Enterprise 2.0** below] Of particular note is Maness' suggestion, italicized above, that "The consumption and creation of content is dynamic, and thus the roles of librarian and user are not always clear." This perhaps best epitomizes the soul of "2.0" and is arguably the reason for its social networking appeal: the dynamic relationship between creation, consumption, and content allows users to participate in their own new or existing communities in ways that were never before possible.

For libraries, Maness argues that 2.0 "will constitute a meaningful and substantive change in the history of libraries." (Maness 2006) Will these Web 2.0 tools fundamentally change the way that humans are interacting, working, collaborating, etc.? Can this collaboration be harnessed for professional gain? In an enterprise level? What about at the government level? In short, yes. The details will be explored in the coming chapters of this essay.

### **Web 2.0 and Business: "Enterprise 2.0"**

The phrase Enterprise 2.0 was coined by Andrew McAfee, an Associate Professor with the Technology and Operations Management Unit at Harvard Business School. In a 2006 *MIT Sloan Management Review* article, McAfee described how Web 2.0 technologies "can potentially knit together an enterprise and facilitate knowledge work in ways that were simply not possible previously." (McAfee 2006) And so began Enterprise 2.0.

Before the concept of Enterprise 2.0, a much different technological paradigm had taken hold of the modern knowledge worker. Then, technology bound "business executives to follow itineraries that place them on global, round-the-clock time schedules, subject to laptops, modems, mobile phones, faxes, email and other messaging at any time of the day." (Thorne and Kouzmin 2008) This created a distinct struggle between life and technology.

Knowledge workers and knowledge communities connected to the Internet are kept in a constant "emergency time" or in a permanent state of tension about how to survive in the seemingly elusive, but ever threatening, technocratic brave new world - an "existentialism" as to how to frame and utilize physical and non-physical arena's of visibility and invisibility, and how to act or not act in everyday life. (Thorne and Kouzmin 2008)

Lacking smooth integration prior to Web 2.0, information technologies for communication amongst knowledge workers fell into the following two categories:

*-Channels.* This encompasses technologies such as e-mail and person-to-person instant messaging — where digital information can be created and distributed by anyone, but the degree of commonality of this information is low (even if everyone’s e-mail sits on the same server, it’s only viewable by the few people who are part of the thread).

*-Platforms.* Technologies like intranets, corporate Web sites, and information portals. These are, in a way, the opposite of channels in that their content is generated, or at least approved, by a small group, but then is widely visible — production is centralized, and commonality is high. (McAfee 2006)

The distinct separation between both the information contained and distributed in the above-named categories, and the users who were able to create information for distribution, characterize the slow, static silo mentality that was so pervasive in Web 1.0. By moving into the Web 2.0 mindset, McAfee’s Enterprise 2.0 revolutionized the 2.0 tool by working “to focus only on those platforms that companies can buy or build in order to make visible the practices and outputs of their knowledge workers.” (McAfee 2006) In doing so, the knowledge worker was gradually freed from their unenviable position of being tied to their data in ways they did not choose.

### **S.L.A.T.E.S.**

McAfee uses the acronym S.L.A.T.E.S. to describe the Enterprise 2.0 processes and their relationship to the information:

- **Search** (information must be searchable)
- **Linking** (links must connect and cross-reference blog posts, wikis etc. into an interactive and interdependent community)
- **Authoring** (simple tools must be provided to allow everyone to contribute and edit content)
- **Tagging** (users must be able to assign their own terms and descriptions, which allows content to be structured in a way that is meaningful for users)
- **Extensions** (applications should include a suggestion and recommendation system such as that found on Amazon or StumbleUpon – ‘if you liked X, you’ll like Y’)
- **Signals** (technology, such as RSS, that tells users when new content of interest appears).” (McAfee 2006)(Warr 2008)

Upon examination, it becomes clear that McAfee’s S.L.A.T.E.S characteristics are quite similar to those of Maness’ “Library 2.0.” This similarity is especially insightful when one considers the diametrically opposing reasons for existence between these two types of organizations: Enterprises exist solely to earn a profit, while Libraries are built on the concept of free access. This speaks to the dynamic range of the 2.0 tool and mindset - McAfee and Maness suggest that 2.0 is capable of driving the world’s largest organizations in a very bottom-line focused environment, yet those same tools can enhance and enrich the services of a community organization just as well.

This begs the question: it is easy to see where 2.0 tools would appeal to libraries and similar organizations: tools and contributions are free, and freely contributed. But how can Enterprises monetize the 2.0 mentality?

Returning to O'Reilly's Google vs. Netscape example, he posits that "the value of the software is proportional to the scale and dynamism of the data it helps to manage." (O'Reilly 2005) Therefore, in the 2.0 world, the more dynamic a software application can become, that is to say the more ways it can accept input and produce meaningful output, the more value potential exists. These dynamic interactions also create a host of new security implications. By exploring these dynamic data transformations in a common setting, perhaps the enterprise can better understand where the strengths lie and also where the risks lie.

### **Web 2.0 Poster Child: The Mashup**

One particularly poignant example of this is dynamic content existence is the "mashup." 'Mashups' are a phenomenon unique to Web 2.0, defined as "hybrid applications, where two or more technologies or services are conflated into a completely new, novel, service." (Maness 2006)

At first, it seems like enterprises and mashups are two things that cannot be reconciled. On the one hand, the enterprise places an enormously high value on its data, and on protecting its data. On the other hand, a mashup requires full and open access to large data sets to create anything of value. How can these two viewpoints be reconciled? One recent article suggests that

an enterprise can use mashups internally to collect information from different sources and combine it in intelligent ways to help people make smarter decisions. For example, executives can use mashups to gain a deeper understanding of customers and sales, and thus to make better decisions. Mashups also find application in areas such as payroll, customer relationship management, logistics, procurement, marketing, and e-commerce. By opening up data and services that mashup creators can use, enterprises can gain strategic advantages. For example, the mashed-up applications can divert new users to their sites, or mashup creators could develop a new Web site that provides better interfaces to an enterprise's existing Web site, which in turn could bring more visitors to the enterprise's site. (Murugesan 2007)

Murugesan suggest that the true value of the mashup lies not "in the data or service itself, but in a better user interface for the data, or in its ability to combine data from several sources in interesting or significant ways." (Murugesan 2007) Increasingly, data is becoming the most valuable asset for any given Enterprise. This fact, combined with the break-neck speed of 2.0 evolution, creates a very serious Catch-22: do Enterprises open up their data in the hopes that they can harness it in new ways through mashups? Or is the data too valuable to allow free access and manipulation? Is there a way to split

the difference? I would argue that there is, in fact, a way to both harness the value in the 2.0 ways of interacting with data, and also preserve the inherent value of the data. [See **Security 2.0?** for suggestions on achieving this]

In an interesting twist on the fate of Enterprise 2.0, Harvard's Andrew McAfee suggests that it may very well end up being self-directed, in a true 2.0 fashion: "The technologists of Enterprise 2.0 are trying not to impose preconceived notions about how work should be categorized or structured. Instead, they're building tools that let these aspects emerge." Web 2.0 tools are easy to use: "authoring, linking and tagging all can be done with nothing more than a Web browser, a few clicks and some typing." (McAfee 2006) This way, everyone can participate, contribute, create, distribute, and hopefully, succeed.

Technologists in other arenas are also adopting the evolutionary 2.0 mindset when trying to build a better tool. One area, in particular, is seeing a boom of growth in 2.0 tool adoption and utilization: government.

## Government 2.0

### Three Part Formula

According to Dan Mintz, former Chief Information Officer at the United States Department of Transportation (DOT), Government 2.0 represents the newest generation of participatory government. Government 2.0 is characterized by three distinct characteristics: it is participatory, pervasive, and integrated:

- Participatory*. The original passive Internet - where a provider placed information on a Web page and a user read it-has changed. Users make their own content and, in the case of artificial worlds, become part of the Internet experience directly.
- Pervasive*. Internet access has grown beyond the computer on a desk - to cell phones, cars, and even kitchen appliances. Hotels and coffee shops - and a growing number of other public and private spaces almost anywhere - feature wireless [internet] access.
- Integrated*. More and more "things" are being connected to the Internet, from security access devices transmitting their status, to home security systems, to data devices implanted in a highway sending signals on the status of the road. We are entering a world where everything is connected to everything else. (Mintz 2007)

We have seen examples of each of these things in recent months, especially visible throughout the last presidential election cycle. Participatory interaction was highlighted by the CNN/YouTube presidential debate, where tens of thousands of Americans contributed questions over the video sharing service, and millions viewed both the

questions and their responses from the candidates on CNN, YouTube, and many other platforms and devices (again, a function of the “openness” that characterizes the 2.0 movement).

President Obama, then candidate Senator Obama, proved the pervasiveness of the Internet, raising more money than any candidate in any election in the history of the country. In fact, his economic success was nearly entirely predicated on the pervasiveness of Internet access: “Obama’s machine attracts large and small donors alike, those who want to give money and those who want to raise it, veteran activists and first-time contributors, and—especially—anyone who is wired to anything: computer, cell phone, PDA.” (Green 2008)

Finally, integration is becoming a reality as more and more devices become network enabled. Korean electronics company LG has offered a web-enabled refrigerator since 2000, and an Internet-connected washing machine/dryer combination since 2002. (LG 2002) As Mintz mentions, devices everywhere are becoming networked with technology such as Radio Frequency Identification (RFID) and other methods, allowing new levels of interaction. One product, recently released for Apple’s iPhone, allows the presence of a local RFID tag to trigger a set of actions on the iPhone (opening a website, displaying a picture, playing a movie, etc.). This opens an entirely new realm of possibilities, such as targeted locational advertising, customized television service, and even dynamic pricing models in stores.

### **Stumbling Out Of The Blocks?**

We have witnessed a phenomenal rise in the use of 2.0 tools by those in and those related to government. Yet - is Government 2.0 an achievable, sustainable goal? Have we reached the now-famous “tipping point,” where 2.0 adoption is inevitable, or is it still too soon? Are there still some kinks that need to be worked out? As of today, there are many large hurdles that must be overcome before Government 2.0 reaches a fully functioning status.

Mintz suggests the most prominent roadblocks are “that any material a federal employee publishes can be taken as establishing or implying the establishment of formal policy. As anyone who has had their name appear in the press or has had to testify before the Congress will tell you, even offhand remarks and e-mails can be used in unexpected ways.” Moreover, “when the creation and maintenance of these sites crosses organizational boundaries - including federal, state, and local governments, as well as private stakeholders - responsibilities for the level of accuracy can become complex and unclear.” (Mintz 2007) This, again, comes with the 2.0 territory of allowing users to be content creators and contributors as well. In the world of social networking, this is the path to success. In the world of government, this is more likely than not the road to disaster.

One of the most interesting, and perhaps also most complexing issues surrounding any 2.0 movement is those questions surrounding leadership roles and responsibilities. As I

have discussed, much of what makes Web 2.0 so successful is the community-based decision making, where there is a very loose (if any) leadership structure. How can we reconcile this existence with the governmental structure of the United States, and yet retain the benefits inherent in 2.0? Mintz offers this cautious advice:

By its varied nature, these new Internet-enabled technologies allow unpredictable interactions between unexpected stakeholders producing unplanned results, none of which offer comfort to the typical government agency. To participate, government agencies will need to define small pilot projects and give the staff flexibility to experiment. In our current “blame first, ask questions later” environment, it will take strong leadership for this to occur. (Mintz 2007)

With the election of the Obama administration in 2008, the 2.0 revolution took center stage. Whether through campaigning, fundraising, debating, or even “tweeting,” there was a 2.0 facet of every part of the Obama campaign. This mentality has continued to the newly revised Whitehouse.gov, which went live the instant Obama was sworn in. (Gaudin 2009) Whitehouse.gov has continued to serve as an information clearinghouse in true Web 2.0 fashion, having been updated every single day since taking office in January and even featuring its own channel on YouTube.

Perhaps Government 2.0 will usher in a sea change, revolutionizing the processes that create, enforce, and support governmental functions. As a recent *Economist* special on e-Government pointed out, “Citizens are not only the state’s customers; they are also its owners.” (2008) Instead of the term “Government 2.0,” the Economist uses the term “eDemocracy,” which perhaps better captures the truly participatory nature of the synergy between government and 2.0.

*The Economist* suggests that the greater impact of Government 2.0 will be felt in countries that are just now establishing their democratic processes, allowing them to build the 2.0 mentality into the system. Attempting to retrofit an existing system with new methods, roles, and rules - especially in a governmental context - is often difficult, if not impossible. One clear example of this “new paradigm, old rules” can be seen in the United States through the lack of criminal law regarding computer crimes. Often times hackers are charged with violation of 18 USC 1030 - or “unauthorized access,” because that is all the US legal framework can offer to accommodate the barrage of new crimes being committed with computers and the Internet..

## **Learning Lessons**

Despite their track record of massive success, even Obama’s crack team of web experts has had their share of bumps along the road, especially now operating under a strict governmental framework. (Vargas 2009) There are several pitfalls to be aware of when looking towards Government 2.0. The two challenges posing the greatest danger were illuminated by Spanish researcher David Osimo in a report to the European Union’s Institute for Prospective Technological Studies:

- *Adopting only the technology, but not the values.* (Osimo 2008) As we have seen from its inception, Web 2.0 has been embodied by a driving mentality, a shared set of values that include open sharing, access, manipulability, and correlation. For government to adopt only the technology (say, for example, a community-driven blog or wiki) but not the corresponding mentality, the project will surely fail. There must be a mentality, ideally already having reached critical mass, behind any 2.0 technical implementation. Motivations vary widely by organization, but with the incoming members of the workforce being vastly more familiar with the 2.0 mentality, garnering internal support for 2.0 initiatives should become significantly easier in the next 3-5 years.
- *Focusing on developing a proprietary Web 2.0 application.* (Osimo 2008) I would argue that proprietary is almost the antithesis of “2.0.” The heart of 2.0 is interoperability, typically through a web browser. By choosing to develop a proprietary set of software, a governmental agency has already put themselves behind before the project even leaves the planning stage. That said, there’s absolutely nothing wrong with customizing an existing open-source implementation of a particular software. One wildly successful example of this is the US Intelligence community’s “*Intellipedia*,” a customized implementation of a wiki based entirely on same the community-driven platform as *Wikipedia*.

### **Intellipedia - Sharing Done Right**

Intellipedia is a particularly excellent example of successful Government 2.0, both because of the content contained within the project and because of the traditional roles and beliefs of the content creators. Headed by the Office of the Director of National Intelligence, the Intellipedia project attempts to overcome the very distinct and silo-like nature of the intelligence community. According to one report, Intellipedia’s Top Secret area, after only 16 months of operation, contains nearly 30,000 articles with more than 100 being added every day, and nearly 5,000 edits by participating intelligence analysts. The same report indicates that nearly two-thirds of all US intelligence analysts are actively participating in this system. (Osimo 2008) How did this system find such success, especially in a culture that is prone to information hoarding, not information sharing?

The key to Intellipedia’s success, as with all successful 2.0 projects, is community buy-in and active participation. Leadership encourages active participation amongst contributors by rewarding analysts whose judgements most often turn out to be correct. Also, there are awards for “exemplary contributions,” and each entry is attributed to the particular agency, office, and individual analyst - encouraging strong contributions through the idea of representation. (Osimo 2008) This final component - tagging contributions by name, office, and agency - is perhaps the most interesting component of the Intellipedia system.

Especially in the context of a large bureaucracy such as the US Federal government, it is easy for employees to take on the all too common stereotype of the faceless “drone,”

whose actions matter little and where consequences are minimal. By attaching a name, office, and agency to every contribution made in a system viewed, analyzed, and used by peers, Intellipedia effectively counters this mindset much in the way that a peer-reviewed academic journal does. In a context where you know that others whom you respect will be critically examining your work, the work that is produced and submitted is naturally of a much higher quality. Harnessing this peer-based motivation, in combination with the strengths of a Web 2.0 platform, has led to a break-out success for the Intellipedia project.

The other success of Intellipedia is its ability to operate “openly” while containing classified, secret, and top secret information. Issues surrounding the new paradigms of data and information security in a 2.0 world are explored in the next section.

## **Security 2.0?**

### **Inherently Open - Inherently Insecure?**

“Ultimately, it is the social and interactive nature of Web 2.0 technologies that make them inherently difficult to secure. Couple that with the speed with which new applications and widgets are created and launched, and you have a potential disaster in the making for the unprepared.” (Short 2008) This realistic view of security in the 2.0 world appeared in the October 2008 edition of *Risk Management* magazine. When the concept driving new project centers on the idea that things can be created quickly and easily, deployed widely, and contributions made by anyone, where do security professionals even begin?

As with other areas impacted by the 2.0 revolution (social networking, enterprise, government, etc.) it is likely time to revisit the concept of security, working towards something loosely called “Security 2.0.” Corporate security providers have already jumped on this phrase as a marketing tool - Symantec hosts an annual conference by the same name, including the tag-line “Connected. Protected.” “It’s about integrating software, services and partnerships to protect customers’ most important assets: their information and their interactions.” (Evers 2006) This sounds like a good start, but for some reason, I get the feeling that this is likely still more marketing hype than security substance.

Security 2.0 is about much more than “integrating software, services, and partnerships.” Security 2.0 must become about the integration of the digital selves that today’s knowledge workers and organizations are becoming. As we have seen, people are connected 24/7, Internet access and devices are pervasive, prevalent, and only getting more-so. The new concepts of Security 2.0 must reconcile this “always on” connectivity in ways that go far beyond the bounds of today’s security conceptions.

Security risks are everywhere in the 2.0 world. The heavy use of AJAX, Ruby on Rails, and other 2.0 programming languages, software tools, and databases create a wealth of ‘attack surfaces’ from which attackers can potentially gain access to sensitive data. With

the ability to post photos, video and audio recordings to sites, employees can inadvertently “leak” confidential company information and post inappropriate personal information that puts both the employee and the business at risk of everything from a reputational black-eye to multi-million dollar litigation.

It has been suggested that success in Security 2.0 will be found through the ability to adapt. “The key to Security 2.0 is finding an adaptive security model that will facilitate collaboration without making it the fatally weak link in the security chain.” (Davidson and Yoran 2007) This advice clearly falls under the category of “easier said than done.” The simple fact of the pace at which 2.0 technologies develop, gain popularity, and fade make any type of meaningful technological security analysis extremely difficult.

With that said, I perceive the key to Security 2.0 will come down to one main concept: authenticity. As our digital selves merge with our “traditional selves,” it will become increasingly important to ensure that comments, contributions, actions, and authorship are accurately attributed. Already, we are facing issues of “brand-jacking,” asserting that you are a representative of a company or organization where in reality you have no connection to the group in question but are instead using their existing reputation to drive traffic and profit to your 2.0 product (see the user “Janet at ExxonMobilCorp” on Twitter for an example). (Short 2008) This same concept can be applied to individuals, as well. It is easy to see how maliciously placing libelous, slanderous, or otherwise inappropriate contributions (blog posts, emails, tweets, etc.) could ruin a person’s reputation, career, or even an entire organization.

### **Security: A People Problem**

Security 2.0 is not a technology problem. It is a people problem. The types of technologies that are behind the 2.0 revolution are so revolutionary exactly because they place their power at the fingertips of the human users. These are not the types of technologies that previously revolutionized our world by cutting the human out of the equation. Rather, these are technologies that exponentially increase a user’s ability to influence and shape their world. Defeating security threats in this new paradigm will require a new definition of security, especially considering that employees account for 61-81% of Information Systems breaches. (Spears 2006)

One of the most common means of expressing this idea, though often not in a Web 2.0 context, is the concept of “non-repudiation.” (King, Dalton et al. 2001) The primary goal of non-repudiation is to “prevent an individual from being able to deny receipt or transmission of a message.” Non-repudiation controls are used when authentication controls are incomplete, and there is a need to “uniquely identify an entity without question.” (Bernard and Ho 2009) Previously, non-repudiation had typically been used in situations of extremely high sensitivity. Non-repudiation often requires a much larger amount of processing overhead, and can create excess work for network administrators. In the future, however, non-repudiation will be able to be leveraged into a 2.0 security system (likely with some form of single sign-on) allowing employees to contribute to and consume enterprise-level 2.0 resources, while simultaneously

enabling management to ensure that any problems are quickly identified, properly attributed, and appropriately resolved.

The idea behind non-repudiation is much of what drives the contributory success of Intellipedia, the open-source intelligence analysis tool that I have already discussed. When community members are aware that their actions, for better or worse, are going to be attributed to them, they are more likely to make positive, consistent contributions. An analog example of this idea can be found in any small town in America. As a product of one such town, I can assure you that a similar social dynamic is created - it seems as though one cannot go anywhere or do anything without someone else noticing. This does wonders for encouraging positive social behavior, and arguably produces a stronger community while requiring little conscious effort.

Despite a relatively clear path, cultivating a positive, engaged, and secure community in the 2.0 world has proved to be very difficult. Perhaps this is a result of human nature, or perhaps current security mentalities have not yet accepted the human aspect of the 2.0 revolution. One security researcher suggests that

a growing number of companies are considering or developing policy guidelines or codes of practice governing safe and appropriate conduct, as a way to limit the risk of inadvertent disclosure of company secrets and risk to the company's reputation. We have all read of instances where an overzealous employee posted a derogatory comment about a competitor on a blog, forcing senior executives to apologize and backtrack. Thus, most companies that are blogging today moderate all corporate posts prior to publication. They also append language to their blog's comment area, dictating the tone of the blog and warning that inappropriate comments will be removed. (Short 2008)

To me, this seems entirely backward. As an enterprise, if you do not want a person representing your company, do not hire that person. If you are afraid that a person may pose a liability risk through their actions, confront the issue (preferably *in person*) or terminate the employee. A bad employee is one thing. A bad employee with access to the internal network, business cards, and an email address at your .com is entirely another.

This is not to say, however, that there are no technological solutions to 2.0 problems. These solutions will be explored in depth in the next section, **Web 2.0 for the IT Security Architect**. But these technologies are only going to augment or supplement the true security solution: a savvy, well-trained workforce who understands the risks and rewards of using 2.0 tools in an enterprise. Young people entering the workforce today will be far better versed on 2.0 technologies, so much so that their use of them may be able to dictate whether or not they get hired. This could actually prove to be an enormous benefit to hiring managers in organizations across the world - something I have deemed "The Facebook Paradox."

## **The Facebook Paradox**

From a social point of view, Facebook is an incredibly powerful tool, allowing new connections to form and thrive, and lost connections to be re-established. Facebook is, and always has been, a Web 2.0 application. It is leading the way for many of the new methods of interaction, both on and offline. The monetary value of the tool, user-base, and functionality is almost incalculable, surely reaching well into the billions of dollars. Yet, from an organizational security point of view, there remain drawbacks and opportunities for exploitation.

Companies are looking for employees who know how to use these 2.0 tools, and use them effectively. Moreover, companies are looking to hire employees who can make good decisions about what should be shared in a 2.0 environment, and what type of activities are perhaps best left as lore, or at least a story with plausible deniability. Examining a potential hire's Facebook page is an almost ideal test for examining both the potential hire's ability to thrive in a 2.0 world, and their ability to present themselves well in this new social arena.

There are certainly those who feel that employers should not be able to "check up on them" through their Facebook accounts, or that what they do when they are off the clock is up to them, but as I have already said, the reality of the modern workplace is that the digital self and the analog self are merging. Blackberries and iPhones keep employees connected (and often working) 24/7, meaning that there is no more "off the clock." Sites like Facebook often list users' places of employment, opening the organization up to the aforementioned "reputational black-eye." Successful "Employees 2.0" must learn to balance their participation with professionalism if they are to succeed. Gone are the days of uploading every embarrassing photo of a compromising situation, knowing that only your closest friends will be able to see you in such a state.

Yet, there also exists another extreme: those who eschew tools like Facebook for fear that they may not be able to control every aspect of their experience (as is common with community driven tools) and as such avoid them entirely. This can raise questions for potential employers as well - not the least of which include questioning an employee's 2.0 skills, or even perhaps their social abilities. A balance must be struck. In the immediate future, it is easy to envision a situation in which lack of a Facebook account may pose a red flag - just as it has become commonplace for every company or product to have a website. Not having a website, anymore, is the surest way to failure. Will we see a time when not having a Facebook account can be the same fatal blow?

Thus exists The Facebook Paradox. People with aspirations of entering the modern workforce must now cultivate an online presence, much in the same way that they look for volunteer opportunities or other resume builders. They must show the world, and potential employers, not only that they can use Web 2.0 tools, but that they can do so successfully and responsibly. Not having a 2.0 presence, or having a poorly maintained one in terms of acceptable content, can spell disaster on the job market.

## **Web 2.0 for the IT Security Architect**

As we have already explored, the 2.0 revolution is well underway, and it seems inevitable that 2.0 data practices will become the norm for the modern enterprise. Knowing this, and also knowing the value that can be had through successful utilization of 2.0 concepts and techniques, how can an IT Security Architect juggle the freedom required for a full Web 2.0 experience, yet maintain the levels of security necessary when dealing with sensitive enterprise data?

A project between Oracle and security consultants Security Growth Partners concludes that

Security 2.0 must adapt to reflect the new reality: Data is no longer locked up behind multiple portcullises and moats. Rather, it strolls out of the gates of a fortified castle and camps with other data in “mashup tents” that fold or are rolled out elsewhere with apparent ease. (Davidson and Yoran 2007)

Moreover, the technologies behind 2.0 software solutions are moving to a more distributed model, with the mobile platform quickly rising to the primary position, both for personal use and in the enterprise. Highly-capable mobile devices (PDAs, smart phones, systems that can be accessed via SMS text message) are something relatively new to the IT Security Architect, and can be even more problematic when these devices begin to gain access to business-critical data in real-time.

### **Going Mobile**

One proposed method for dealing with the rise of mobile devices is to resort to a security model in which “the devices themselves must be secured, including encryption of basic voice communications.” (Davidson and Yoran 2007) Davidson and Yoran suggest that there may be advantages in segmenting the data on the actual device, disallowing portions of the phone (say, “Personal”) from accessing other data areas (like “Big Client Data”). Unfortunately, I think this approach is rather near-sighted and will have limited, if any, positive impact on an enterprise-level. This security solution may actually prove to be a hindering addition to these powerful mobile devices, and is a product of the old security paradigm, not taking into account the human factor.

Instead of segregating data (the silo model which the entire world seems to be moving away from as quickly as possible), empower users to be able to blend their data as needed, creating a sort of “mobile mashup.” The reality of the enterprise is that business and personal lives often overlap, with connections, conversations, and business deals taking place in “personal” situations with alarming regularity. These sorts of interactions need to be cultivated, not segregated, if an industry is looking to succeed in the 2.0 world.

Rather than a strict segregation of data, perhaps a better model is one based on the permissions model of the Unix/Linux operating system. In a mobile context, this may

resemble something more along the lines of the ability to access potentially sensitive data only after entering an administrator-level password. This way, there can be no “accidental” accessing of potentially sensitive data, and malicious software (worms, viruses, etc.) would be unable to access the data as well. This permission model has already been introduced on the newest personal smart-phones (Apple’s iPhone and Google’s G1), but an enterprise level equivalent has yet to reach the market.

### **Business in the Cloud(s)**

Another facet of the 2.0 revolution that will have enormous implications for the IT Security Architect is the concept of “cloud computing” and “cloud storage.” Instead of the traditional models of server-farms or giant data centers with massive RAID-arrays to process and store data, the concept of the “cloud” has emerged.

In this new model, “cloud” computing builds on decades of research in virtualization, distributed computing, utility computing, and, more recently, networking, web and software services. (Vouk 2008) It allows for storage, retrieval, and manipulation of data by widely distributed networks of processors and storage devices, which the user often has no control over other than their own data.

Promising enormous storage and computing potential, combined with low overhead, maintenance, and fees, cloud computing almost seems too good to be true. And yet, the 2.0 technologies of today are conditioning users to become comfortable with the cloud experience. Facebook, YouTube, and every other 2.0 tool maintain their own cloud - and users live and thrive on these platforms. Think, for a moment, about the data that you may have uploaded to a 2.0 site (perhaps even your own blog or online email account). Where is that data, physically? What kind of security controls are on that device? What kind of redundancy plans are in place? Who is in charge of my data? Can I retrieve it? Can I delete it? These questions, and more, must be answered before cloud computing or storage becomes a viable enterprise solution. The security risks are simply far too great for any self-respecting IT Security Architect to place their trust, and their organization’s data, in the cloud.

### **Leveraging Web 2.0 Securely for Enterprise Success**

The modern enterprise will face many challenges in the quest to incorporate and exploit the newly formed Web 2.0 tools, users, and potential. The crucial intersection will be keeping data nimble while also keeping it secure. Enterprises will look to be able to do things like Wikis, Mashups, and other data-centric processes, but the worry of losing sensitive data will be ever-present. Below are several suggestions for ways in which organizations, both governmental and private enterprise, can make the most of the 2.0 revolution.

## 2.0 tools and beyond

There are several simple guidelines that will allow companies and organizations to get the most from an implementation of 2.0 tools in their IT toolset:

- *Adhere to open standards.* By using widely available tools, organizations can often save themselves quite a bit of money and headache. Not only is developing an in-house tool expensive initially, but maintaining and upgrading the product is often outside the scope of most organization's IT departments. Selecting a pre-existing standard and tool allows the organization to harness the power of the distributed development network that currently creates and maintains the software product. As a bonus, many of these tools are "open-source," allowing security professionals to review the source code for any potential holes prior to rolling out the product. If, on the off chance the product becomes unsupported or the organization needs to upgrade, choosing an open data standard (XML, etc.) allows for easy portability to another platform. Proprietary data standards are a thing of the past, especially when looking to cultivate a collaboration mindset with the software and data.

- *When in doubt, take it internal.* The selection of an open-source tool and open data standard does not mean that a company's data must also be open to the world. Many security conscious organizations have successfully implemented the open tools on a heavily secured intranet, even adding more accountability through non-repudiation tools (see *Intellipedia - Sharing Done Right* above). An intranet implementation of these tools allows an organization to benefit from the other security measures that have become commonplace: firewalls, VPNs, VLANs, and other network focused security tools. Internally hosted tools also allow for access controls that enable mobile users to participate while not compromising existing security protocols.

- *Lead by example.* As we have seen, the success of any particular Web 2.0 tool is driven by a committed and active user community. In an enterprise level, this culture must be driven from the top down. This could be as simple as the CEO or President starting a blog, and updating it regularly. Or, allowing for community participation in decision making through other Web 2.0 tools. If there is support and actual buy-in from organizational leaders, a 2.0 tool is much more likely to be successful. The one caveat about leadership in the 2.0 world it that it is much better to "pull" participation than it is to "push." Microsoft has attempted to launch several 2.0 tools and has failed because of their attempts to push users to the products, rather than pull them in through peer participation or quality of product (see Microsoft Live Search and Microsoft Passport as two examples). Intellipedia encourages this sort of participation in the pull model by rewarding the most accurate and well-respected users. Each organization can create their own "pull" model based on the existing corporate culture - as with many 2.0 tools, what worked for someone else may not be the best solution for you.

## **Mobile Solutions**

Heavy reliance on the mobile platform is inevitable in the modern business environment. To succeed on any sort of large scale, organizations need to provide secure methods of data access on mobile devices. Largely, these abilities will be provided by vendors, and likely through proprietary technologies - entirely counter to the driving factors of the 2.0 revolution. One possibility, however, is that with the rapid “civilian” adoption of powerful smart-phones (the iPhone, in particular) is that these platforms will become appealing targets for open-source development.

In this case, integration to enterprise-wide 2.0 platforms is much more reasonable. Modern phones are beginning to offer VPN capability, allowing them to take advantage of the other network protections yet still access sensitive data. Many of the other challenges for successful mobile device deployments are decidedly low-tech: their small size and easy portability, combined with the fact that they communicate “over the air,” make them easy targets for criminals, hackers, and industrial espionage.

To counter these problems, mobile devices must incorporate an additional security layer before allowing access to the device. This may be cumbersome at first, such as requiring a password or PIN to be entered, but modern methods and capabilities will soon eliminate this problem. One example, already available in Google's G1 smart-phone, allows the user to define a preset motion (almost like drawing on the screen) that unlocks the phone and allows access. These sorts of access control methods, combined with rapidly advancing capabilities in the arena of biometrics, will mean secure mobile device deployments are much closer to reality than other 2.0 possibilities.

Heavy reliance on mobile devices will require additional overhead in the form of training, policy and procedure review, and data allocation (ensuring that data which must be accessed by mobile devices is capable of such access, and also that data which must not be accessed by mobile devices is not capable of such access). The potential, however, for success is enormous. The mobile platform is poised to be the platform of the future, and can offer a significant competitive advantage to organizations who successfully implement a mobile 2.0 platform.

## **Lightning in a Bottle: Harnessing the Cloud**

Cloud computing, though not still in its infancy, may not be ready for prime-time deployment in an enterprise setting. Until cloud computing reaches the same open standards as other Web 2.0 tools, my recommendation would be to avoid it. By same open standards, I mean that there is one access protocol (API) that allows for uploading, downloading, and manipulating data, no matter what vendor or platform the hardware is running. Until this point is reached, the amount of legwork required for a smoothly functioning cloud computing experience, much less a secure cloud computing experience, far outweighs any potential gains.

That said, cloud-like applications are rapidly approaching maturation. If an enterprise does choose to use such a service (Amazon Web Services, GoogleApps, etc.), they should be careful to ensure that they are able to extricate their data should the need arise (changing vendors, changing enterprise needs, etc.). Security of data in the cloud is a primary concern, with some industry professionals suggesting that “the most viable solution appears to be the creation a “government cloud.” This would allow the owners of the data to leverage the benefits of a cloud approach, but still control the environment. If you own/control the cloud, you can ensure that privacy/security policies are adequately addressed and implemented.” (Sellow 2009) Yet having to create your own “cloud” may defeat any sort of cost and infrastructure savings that the cloud stands to offer. For now, the potential risks and drawbacks associated with cloud computing far outweigh any advantages.

### **Self-Securing Data**

Not yet a reality, self-securing data has the potential to revolutionize the way that organizations conceive of secure data storage and transport. Several competing models exist, but most indications point to some sort of “permissions” model, as discussed above. (Strunk, Goodson et al. 2000) This system would allow each piece of data to “log” any access and changes, as well as supporting a file-by-file encryption system that can be customized an organization’s needs. Once this sort of extremely granular control is available at an affordable price-point, options of cloud computing, distributed storage, etc. become much more appealing.

### **Focus: People Problems**

Above all, security in the 2.0 world will come down to an organization’s people. As 2.0 tools place more power in the hands of the user, and as organization look to squeeze more and more out of their most valuable (and expensive) resource, IT Security Architects must ensure that their focus includes the human component. Top priorities will soon be things like usability, dynamic data access, portability, and

Technological security solutions, of course, will remain important. But IT Security Architecture must expand and adapt to meet the changing needs of the modern enterprise. The significant challenge will be the fact that 2.0 technologies change too quickly to address any one particular technology. Rather, training, policies, and tools should focus on creating smarter employees. A great training program will not only create end users who can avoid common pitfalls of the 2.0 world (phishing scams, posting personal or sensitive information, etc.) but also create more valuable contributions to the enterprise. This is truly a win-win situation for any IT Security implementation.

Furthermore, the capability and makeup of the workforce will change drastically in the next 10-15 years. Employees will be vastly more technologically savvy, allowing for these training programs to expand their scope from the remedial and intermediate topics to the advanced and even expert arenas. This will inevitably lead to a data-rich

2.0 operating environment where user contributions exceed even the visions of today's 2.0 leaders.

## **Conclusion**

Web 2.0 is much more of a mentality than a toolset. This mentality, based on community participation, sharing, and dynamic content creation, is poised to revolutionize the way that we socialize, conduct business, and even govern ourselves. Done successfully, and combined with the rapid proliferation of networked devices, the 2.0 revolution is poised to literally change the world and the way that humans live.

For an IT Security Architect, these new 2.0 tools demand a revision of the traditional concept of security. The new challenges will focus on keeping data secure in transit, in storage, and when placed into new situations never before experienced by either the user or the security professional. To be successful, a dynamic balance must be reached, but remain centered on the user.

Today's enterprise is data-centric. The pace of rapid development will move the focus away from any one particular technology and onto the end user. The enterprise of the future will become user-centric, where that user - often an employee of the enterprise - will control tools far more powerful than even today's custom-built analytic applications. For these reasons, the next wave of IT Security Architecture must work to ensure that users are better educated, more knowledgeable, and more capable of successful operations in the 2.0 realm. Fortunately, the workforce of the future will come well-prepared to accept this challenge, having grown up in the 2.0 world.

The modern IT Security Architect must both incorporate the dynamic and more open data needs of a 2.0 world, combined with an ever increasing level of ability amongst users to create a new dynamic security paradigm in which collaboration and creation can take place in real-time, without sacrificing controls and including systems for non-repudiation and appropriate attribution. Those who can do all of this will lead the next generation of security professionals and foster growth in ways that - even today - seem impossible.

## **Sources Cited**

- (2008). "The electronic bureaucrat." The Economist **386**(8567): 3-3.
- Bernard, S. and M. Ho (2009). Introduction to SA.ppt. Syracuse.
- Cormode, G. and B. Krishnamurthy (2008). Key Differences between Web 1.0 and Web 2.0.
- Davidson, M. A. and E. Yoran (2007). "Enterprise Security for Web 2.0." Computer **40**(11): 117-119.
- Davis, I. (2005). "Internet Alchemy » Talis, Web 2.0 and All That." from <http://iandavis.com/blog/2005/07/talis-web-20-and-all-that>.
- Deans, P. C. (2008). Social Software and Web 2.0 Technology Trends.
- Evers, J. (2006). Symantec touts 'Security 2.0'. CNET News.
- Gaudin, S. (2009). Obama makes quick move to update whitehouse.gov. Computerworld.
- Green, J. (2008). The Amazing Money Machine. The Atlantic. **301**.
- King, C. M., C. E. Dalton, et al. (2001). Security Architecture.
- Knights, M. (2007). "Web 2.0." Communications Engineer **5**(1): 30-35.
- LG. (2002). "LG R&D News - LG Global Site." from [http://www.lge.com/about/rnd\\_news/detail/2275\\_8.jhtml](http://www.lge.com/about/rnd_news/detail/2275_8.jhtml).
- Maness, J. M. (2006). "Library 2.0 Theory: Web 2.0 and its Implications for Libraries." Webology **3**(2).
- McAfee, A. (2006). "Enterprise 2.0: The Dawn of Emergent Collaboration." MIT Sloan Management Review **47**(3).
- Mintz, D. (2007). "Government 2.0-Fact or Fiction?" Public Manager **36**(4): 21-21.

- Murugesan, S. (2007). "Understanding Web 2.0." IT Professional **9**(4): 34-41.
- O'Reilly, T. (2005). "What Is Web 2.0 | O'Reilly Media." from <http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html>.
- Osimo, D. (2008). *Web 2.0 in Government: Why and How?* Seville, European Commission Joint Research Centre, Institute for Prospective Technological Studies.
- Sellow, M. (2009). *Re: Relation of Physical Security & EA*. S. Colson. Syracuse.
- Short, J. (2008). "RISKS IN A WEB 2.0 WORLD." Risk Management **55**(10): 28-28.
- Spears, J. (2006). *Defining Information Security*. 5th Security Conference 2006. Las Vegas, Nevada.
- Strunk, J., G. Goodson, et al. (2000). "Self-Securing Storage: Protecting Data in Compromised Systems." SYMPOSIUM ON OPERATING SYSTEMS DESIGN AND IMPLEMENTATION: 165--180-165--180.
- Thorne, K. and A. Kouzmin (2008). "CYBERPUNK-WEB 1.0 "EGOISM" GREETINGS GROUP-WEB 2.0 "NARCISSISM": CONVERGENCE, CONSUMPTION, AND SURVEILLANCE IN THE DIGITAL DIVIDE." Administrative Theory & Praxis **30**(3): 299-299.
- Vargas, J. A. (2009). *Obama Team Finds It Hard to Adapt Its Web Savvy to Government*. The Washington Post.
- Vouk, M. A. (2008). "Cloud Computing - Issues, Research and Implementations." Journal of Computing and Information Technology **16**(4): 11.

Warr, W. A. (2008). "Social software: fun and games, or business tools?" Journal of Information Science **34**(4): 591-591.