



Using research to determine product attributes and stratification for the design and marketing of user authentication.

[Study 4:
**Contextual inquiry of security
and technology professionals**]

By Mark Schraad

April 24, 2006

Experiment 4: The purpose of this study was to delve deeper into the needs of those professionals in small and medium size businesses responsible for security, information technology and user authentication.

In recent years the incidents of information theft or at the very least information loss, seem to be on the rise. At least the reporting of those losses in trade magazines and newspapers appears to be increasing. Reports of laptops, digital media and hacking into corporate infrastructures pose a more serious threat to data integrity and safe keeping than ever before.

In the case of financial services firms and healthcare professionals, the federal government has become proactive by passing legislations in the form of the Gramm-Leach-Bliley Act Safeguards Rule and HIPPA provide guidelines for the safe keeping and safeguarding of this data. This sort of legislation is aimed at putting the responsibility of safeguarding customer information firmly in the hands of the company storing the data. The tactical execution of these safe guards falls onto professions within various departments and holding a number of different job titles.

Method

Participants

The persons involved with this study ranged from technical personnel responsible for maintaining as few as two servers to IT personnel that oversee hundreds of workstations. Contextual inquiry or respondent directed conversations with 27 different professionals were conducted over a 15-month period ending in the spring of 2006.

Design and Procedure

Conversations ranged from informal interviews on trade show floors at both MacWorld in San Francisco and Networld-InterOp in Las Vegas with a range of professionals seeking security solutions, to technical support calls regarding the shortcoming of existing solutions, sales calls with potential buyers of an enterprise wide authentications system, as well as more formal phone conversations with professionals researching authentication systems are included in this study.

Discussion

Security and Information technology managers range greatly in both responsibility and in motivation for their search for information regarding authentication strategies and methods. The respondents I spoke to ranged from a pair of 'techies' in charge of a couple of servers and a dozen workstations, to an upper level information executive responsible for securing thousands of workstation with direct access to sensitive customer information. This range also represents a

difference in motivations from protecting data to lowering the time involved maintaining and administering these workstations and network systems.

At MacWorld, I had several conversations with “techies” who oddly enough came to the booth in pairs. Their primary motivation was to restrict access to Windows or Macintosh Servers. In two cases all they needed was the SecuriKey Professional product. This is not the target market for the product, but will effectively fulfill their requirements. In addition two of these groups were looking to secure the preference settings in computer labs – both Macintosh and Windows computers that were either used by students in an educational environment, or in a Kinko’s like shop that sold access to computer use to customers. They explained that the users often change settings critical to the operation of the software, network or printing functions, without knowledge of the problematic effects. Their goal was to keep these changeable preferences out of reach of the customer. Preventing such access is a benefit of the product and these administrators hoped to save as much as 50% of the time they spend fixing these preferences. Another person within this group was in charge of a public library’s computers that are frequently used for Email and Internet access. He expressed some interest in restricting access to specific web sites or specific types of web site, primarily those of questionable content. This is a capability of the ControlKey product, but is not currently an applicable component of the SecuriKey product, either Profession or Enterprise versions. The effectiveness of Griffin Technologies approach to this control is not considered the best on the market.

When speaking to these individuals the subject of an enterprise version of the SecuriKey product was mentioned and they were asked if this was a more desirable solution. All of the participants in these conversations were excited about the capabilities of this yet to be released version of the product. They realized that centralized administration, particularly in mixed environments would be a huge time saver. One respondent said flat out, “you mean I could control access to all of the workstations in my domain while sitting at my workstation, that would be awesome.” There was overwhelming confirmation that there was a need and demand for the enterprise product. Then came the downside. For those in educational or library environments there was great concern regarding the cost of such a system. These individuals do not have the authority to spend thousands of dollars on the enterprise product, they do have the authority to make purchases in the \$200 – 500 range, well below the cost of the enterprise solution, but a range that could afford at least one and possibly three copies of the Professional version. It appeared that in the educational and public libraries, they would have to deal with some level of inconvenience, in spite of their recognition of the value of the enterprise version.

Several of these individuals were concerned specifically with controlling access to Windows or Mac servers. Those servers were being used to control the network, Email, web access, file serving and print serving. Additionally some were hosting client server applications. Locking control to those servers was well within the capability of the professional product as long as the access was consistent and limited to a few individuals.

The inclusion of cross platform client functionality to the enterprise product was a very exciting component to Mac environment administrators. There was considerable enthusiasm and encouragement for this feature. We found the divide between Macintosh and Windows users that existed years ago has eroded. The restriction of the administration functionality to Windows was not deemed a problem. Most were very familiar with the use of Windows servers in a Macintosh environment. I am pretty sure that there are Macintosh only networks in existence, but I did not speak to or hear of a single instance.

One common question from this group was the possibility of booting a workstation from another drive, or taking the hard drive out of the computer and accessing from another computer. Our initial fear was that this would be a drawback as it compromises to some extent the security of the data on the hard drive. Instead what we found was this was seen as a convenience. These administrators saw this potential break in security as a process that the typical user would deem as "too much trouble" or outside of their capabilities. The ability to boot a computer from another hard drive was seen as a quick method for them to fix problems.

Specifically with the educational domain, I did speak with one IT individual from a small private research based institution that was very concerned about protecting intellectual property. They had recently experienced the loss of a laptop while traveling that contained a post-doctoral research project. The Professor had not backed up or archived his most recent draft. The situation presented a case of lost data, a problem that SecuriKey could not have prevented or resolved, and that of his research out in the public domain prior its being ready for publication and without an copy write or publishing protection. SecuriKey could have helped to alleviate this problem.

The second group of IT professionals I spoke to had considerably more technical acumen and at times I found it a challenge to finish a conversation or completely answer queries about the product. I was however, able to draw on additional expertise from within the company and glean valuable insight by listening to the remainder of the conversation.

Most of these individuals were charged with protecting relatively large numbers of workstations, often as many as several thousand. They fall in between current offerings in the market and have very specific concerns. There are vendors, RSA, Alladin and others that offer either smart card or other enterprise authentication solutions but are geared towards a network of 100,000

or so workstations. As a result the deployment is an extensive effort and very expensive. Further, we learned that once installed the company was heavily reliant upon the vendor for updates, problem resolution and maintenance, all at a premium cost. The installation for a couple thousand workstations pushes SecuriKey Enterprise to its limits, but it was well within the technical capabilities and cost structure of these types of firms.

Most every case of corporate concern was as a result of a problem already encountered, either by them or a close competitor. The most frequent incident was that of a lost laptop containing critical data, either for corporate planning, sales data or client information. The issue is not the return of the laptop or the data, as these types of professional have insurance to cover the cost of the hardware and back up systems for data recovery. The issue was, not knowing who had access to this critical information.

In a dozen of these conversations we confirmed that the price range of SecuriKey Enterprise was not an issue. In fact in three cases the feedback was a surprise in its low cost. In two of those cases the response lead to some hesitation. There seemed to be a notion of "it can't possibly be an effective solution at that price point." This lead to some very serious reconsideration of pricing some weeks late and a strategic move to increase the price of the product.

There were a couple of product features missing from the product offering that seemed to be either 'deal killers' or would greatly enhance the prospects of purchase. One of those was the issue of data encryption. Most of the technical professionals I spoke to had determined that the optimal balance between security and ease of use was to install some form of two-factor authentication with a reliable encryption tool. In these technology camps there was universal agreement that Microsoft Windows EFS encryption security was not only sub par and unacceptable, but also was problematic. They were looking for AES 128 bit encryption at a minimum and would like an even more robust solution. This further resounded with technical support calls and inquiries with currently installed systems. Encryption at the corporate IT level was a critical element. Our assumptions that there was concern for reliable data recovery and the performance hit that encryption might cause were not issues. The level of technical skill paired with a tendency to purchase high performance hardware negated those worries.

A second feature that was nearly always asked about was the use of the product on the Linux Operating System. In these corporate environment Linux presents a very flexible, robust, reliable and inexpensive platform for servers of all kinds. We were surprised at the market penetration in these small and medium size companies. SecuriKey does not currently have a solution for the Linux or Unix platform.

Another issue that we spoke to in these conversations was that of end-point security. With the larger enterprise solutions, being attached or tethered to the network is a requirement of the security measures. This leaves remote access by way of laptops and home computers as a huge whole in most enterprise security solutions. In these circumstances they were relying on Password protection alone. This gives potential access to everything back at the main server network to anyone capable of hacking a password or finding that “sticky note under the keyboard.” This issue met with mixed interest. In each case where the IT professional recognized this situation has a real threat, they had an example where it had been a problem. The acceptance of this issue was clearly a reactive one. Currently, SecuriKey is the only solution providing unlimited end-point security for laptops and other isolated workstations. Most recently, Alladin has taken steps to fill this need by offering timed or limited duration security. This means if the laptop is not reconnected to the network within a specifically set time parameter, it is not accessible. This is a shrewd stopgap solution. It is clear they recognize this limitation in their system.

The final feature that we were concerned about was that of Biometrics. The most commonly utilized form of this is that of fingerprint scanning. Most of the IT professional we talked to were rather matter of fact and unimpressed with this technology. They deemed it as “either too expensive or ineffective.” The most common problem being false negatives in which the cheaper solutions did not recognize an authorized fingerprint, preventing access for an authorized user. The extremely rational nature of these individuals was never more obvious. One interviewee commented, “we get requests for that all the time, mostly as a substitute for passwords from the executive, but they are mostly annoyed with our password policies and dig the cool factor.”

We did find that most all of these technicians in search of two-factor authentication currently used a policy of regularly forcing users to change passwords.

One last grouping of potential customers that we encountered included consultants. These were predominantly individuals that consult as technical administrators for all things computer-ish. Though three of those we talked to worked for consulting groups. All were trying to be pro-active in offering security evaluations and recommendation to their clients. Some were reacting to policies being enforced at the corporate level, but there seemed to be considerable interest at the professional office level as well. The offices of attorneys, financial planners, banks, credit unions and medical offices were top most of concern. Obviously the recent legislation in the medical and financial industries was starting to cause concern for the liability of storing private and customer data. One particular objection to two-factor authentication was in the case of a medical office. A security consultant had come across a nurse that asked, “In an emergency, will it slow or deny me

access to patient information.” The unfortunate answer to that is yes. But that is true of any technical solution measure that meets HIPPA guidelines.

From these conversations I can make some pretty solid conclusions. First there is unmet demand in the small to medium business or organization for an effective two-factor authentication solution. Second, the inclusion of credible encryption is a necessary component for most professional IT technicians. And third, the addition of Macintosh and Linux client capabilities opens the product to a considerably more expansive market and should be a top priority.

This is a component of research done in part as a thesis project in graduate school and initiated during my role as Vice President of Marketing. It is highly topical to Griffin Technologies without which this project would not have been necessary or possible. My thanks to all of those individuals for their help and support.

Tables, figures and some of the conclusionary content have been omitted from the versions published on the web site. Some of that content is available by request.

For further information please contact me at mschraad@markschraad.com.