Monash Technology Report

The Future of Security Technology, Part 2

January 16, 2003

Introduction and Summary

In Part 1 of this report, published November 25, 2002, I made these predictions:

Over the next 2-4 years, most of what we now think of as information security technology will merge into five classes of products:

1. Integrated *security appliances.*
2. Centralized *network security management software.*
3. Real-time *identity management servers.*
4. DBMS and database-related software, which will take significantly increased responsibility for ensuring information security. The most important example is *office/collaboration applications, which will be ported to DBMS platforms.*
5. General client-side security products, whether software-only or hardware-based.

Part 1 went on to substantiate the first two points. This Part 2 covers the third point.

In particular, I expect:

- Demand in the AAA market, currently anemic, will eventually strengthen as mobile computing further shreds the network perimeter.
- The key technical and political challenge is *identity management* – which amounts to database integration.
- The most likely identity management winners are platform software vendors – Microsoft, IBM, Oracle, Computer Associates, BEA, et al. Acquisitions may play a role in determining the eventual winners.
- An important set of features that could determine who wins in identity management is represented by a currently separate category of product – *authentication brokers.*

The AAA mess – things have to change

The AAA* industry is a mess. Almost every major vendor has had a classic Internet bubble meltdown, and the closest thing to good financial news occurs is when results aren't quite as bad as were previously expected. Subsectors in varying degrees of distress include:

- PKI (Public Key Infrastructure), which is now seen as a product feature rather than an actual category, as all sorts of companies ship their own built-in certificate authorities;
- Biometrics, which has been a disappointment for two decades (I seem to recall that Fingermatrix was an old story when I was a rookie analyst in 1981);
- Single sign-on, where runaway leader Netegrity is struggling mightily to escape from its sluggish core market;
- Token-based authentication, where dominant vendor RSA is struggling to close a technology gap with Secure Computing, while Secure is making little headway itself, especially at large enterprises; and
- Smart cards, which are getting remarkably little traction for a technology that is being pushed by Microsoft, Sun, Cisco, the US Department of Defense, the credit card industry, and the national health services of many large countries.

**"AAA" stands for Authentication, Authorization, and any one of a number of choices for the third "A", such as Administration, Accounting, Accountability, Access control, and so on.*

I believe the AAA industry will recover, although it's hard to foresee when solid growth will return. Demand is weak for three reasons; while each will eventually abate, it is difficult to predict exactly when the improvement will happen.

1. *Unlike anti-virus and firewalls, AAA is acknowledged as necessary only by a small fraction of the overall user population. HOWEVER,* the network "perimeter" is dissolving due to, among other factors, advances in mobile and wireless computing. Eventually, this trend will make security impossible without strong authentication.
2. *End-users hate cumbersome security technology. HOWEVER,* when a genuine need is present they can be educated. Besides, smart cards will eventually be less cumbersome than most other authentication methods. Even more important, when "portable desktops" and/or "zero-footprint everything" finally work, so that

one can make effective use of any internet-connected computer anywhere, that will be a convenience benefit for which smart card authentication is a small price to pay.

3. *AAA administration is a nightmare. HOWEVER,* the emerging category of "identity management" will eventually tame the problem.

Indeed, that application of identity management is the best short-term opportunity in the AAA market, since it provides a genuine ROI (hot buzzonym #1) via reducing the TCO (hot buzzonym #2) of security applications enterprises already have. This buzzonym-friendliness provides reason to hope that the identity management business will be successful even in today's tough IT spending environment.

Authentication brokers

Every form of strong authentication, or even of not-ridiculously-weak authentication, imposes an unwelcome burden on users and/or administrators. Passwords that are at all difficult to guess are also difficult to remember. Not only does this annoy users, but when passwords are forgotten, they are a nuisance to reset. Hard tokens* are a pain for users to keep handy, and an even bigger pain to replace when lost. Other important forms of strong authentication – smart cards, biometrics – seemingly depend on there being a reader deployed at EVERY possible network access point. Soft tokens** present a similar deployment challenge. And cell-phone based systems (SMS or otherwise) are at best as reliable as – well, as cell-phone service.

**Hard tokens are small devices that generate one-time passwords, the magic being that the central server always knows which one-time password to expect. One-time passwords are more secure than the usual kind because they are useless to hackers if intercepted by, say, networking snooping or if guessed by a brute force "dictionary" attack. Equally important, they don't get written on little sticky notes and pasted to monitors for all to see.*

***Soft tokens are imitations of the same thing via software on a computer. Supposedly, the PIN number that protects a soft token is more secure than an ordinary password because the PIN number never goes across the network to be exposed to interception, and because it's short enough not to be written down on the aforementioned sticky note.*

If you accept that strong authentication is sometimes needed, and will be more widely necessary in the future, there should be a nice market for anything that makes it easier or

cheaper to deploy, administer, or use. And there is indeed a partial solution to the pain of authentication -- *authentication brokers.* The exemplary product in this category is Safeword PremierAccess (aka SPA), from Secure Computing, in a generalization of the server technology for their proprietary hard tokens. RSA has announced a similar strategy, combining most of its server products – market-leading token server, single sign-on, PKI/certificate authority. I find it difficult to predict whether and to what extent RSA will match or leapfrog Secure's offering.

The major aspects of an authentication broker are:

All applications that require authentication delegate authentication to the broker. This is a lot like single sign-on, and SSO is indeed an aspect of authentication broker products.

Multiple methods of authentication are supported. This is the key point – and the more flexible the associated policy server is in supporting different kinds of authentication for different contexts, the better. For example, users sitting at a terminal in an office might have relatively weak and easy forms of authentication – but only after their first six months on the job, and not when accessing particularly sensitive information. Mobile users, who are more at risk, may be asked to authenticate more stringently. Smart cards can be used wherever there is a reader, with an alternate form of authentication used otherwise. Or, in a system that basically relies on biometrics, exceptions can be made for those whose physical disabilities render them unable to use the biometric system.

So far, the authentication broker sector is floundering. The major product, SPA, is having dismal results at large enterprises, and only modest success (some dozens of units per quarter, at a five-figure price) at smaller ones. But there are reasons for this. First of all, Secure Computing is the wrong vendor – small, unfocused, and with a management team that is getting slapped around by shareholder lawsuits and even an outright SEC citation. More important, SPA's design effectively assumes the users' security information is neatly organized in one accurate LDAP directory. And most large enterprises are about as likely to have a global, all-encompassing LDAP directory as they are to have a single corporate-wide all-application integrated relational database.

Identity management

And that leads right into our next topic. Identity management is perceived as the great hope of the AAA and directory businesses. Netegrity, floundering in single sign-on, is refocusing on "identity management". Novell, floundering for years in directory

services, is refocusing on "identity management". IBM/Tivoli bought an "identity management" vendor. What's going on here?

The basic idea of identity management is to centralize and streamline the process of granting users access to applications (and other computing resources). The granting of initial access is generally called *provisioning*. Giving permission for a specific session is generally called *authorization*. But whatever you call it, identity management is really a big fat database integration and maintenance problem.

At a minimum, an identity management system probably needs to combine information from many copies of Microsoft Active Directory, plus a variety of applications and/or portals that each try to manage their own security. Also, to determine the roles and privileges of various users, human resources information has to be integrated in. (Indeed, the most obvious benefit to identity management is at the times of hiring and firing, when rapid granting or revocation of privileges is highly desirable). Mainframe security systems from Computer Associates or IBM – Top Secret, RACF, and/or ACF2 – are often involved too. Systems such as firewalls and VPNs tend to maintain their own user role/privilege directories. And of course any prior attempt at directory integration, enterprise directory, meta-directory, etc. needs to be factored in.

At a large enterprise, this kind of integration is a massive task. The worst issues are political and organizational: Which departments control which information? How can they trust those idiots in the other department to keep things accurate and secure? Who has to change the way they currently structure the data, so as to create interoperability or at least compatibility. This is all the same stuff we've been hearing about for years in data warehousing and enterprise application integration, and the companies most experienced at dealing with it are database and middleware platform software companies.

The purely technical challenges are formidable too, at both the front and back ends. The key interface concept for identity management is "delegated administration" – self-service where possible, departmental where possible, central only as absolutely needed. That doesn't sound so difficult, but somehow role/authorization policy servers always seem to be hard to get right (hence Check Point's long-standing lead in firewall management software).

The back-end issues are definitely tough. Some identity information is stored in relational databases; but much is stored hierarchically, in LDAP formats. (I'm not even going to get into X.500). Integrating hierarchical and relational data is notoriously

difficult. Indeed, it's probably impractical in full generality. Some of you may remember IBM's "Eagle" project 20 years ago to integrate the hierarchical IMS with the then new-fangled relational systems; to the best of my knowledge, Eagle still hasn't landed.

That said, relational/LDAP integration is doable, because of the limited complexity of LDAP directories. Indeed, this integration has been achieved to various levels of flexibility and scalability in a variety of offerings, especially metadirectories such as the one from Critical Path/Isocor. And while the metadirectory market has never amounted to much, such sales as there are have typically been to telecom service providers, sometimes with millions of users supported.

Again, the companies best equipped to meet these challenges are probably platform software vendors. A robust identity management system will need to support a variety of different architectures, such as:

- Update user information in a hodge-podge of different systems and do federated queries real-time for authorization (not likely to be the most scalable).
- Update user information in a hodge-podge of different systems, then copy it to a central directory for real-time authorization (as in the case of data warehousing, the most likely solution).
- Copy parts of the central directory to many locations as needed (think data marts for an analogy).
- Update all information centrally and synchronize the other systems to it (ideal, and therefore probably a marketing necessity, but not likely to be 100% implemented at most large organizations).

And there will need to be high-quality interfaces to a broad range of existing directories, RDBMS, enterprise applications, and security systems. This is the kind of development and consulting challenge best met by large platform software companies, and so I expect the market to be won by a subset of the usual suspects: IBM, Oracle, BEA, et al.

Conclusion: Yes, it's a real business

Every enterprise has some level of password, directory, and authorization technology and investment. A concentrated group of enterprises have further spent billions of dollars on more serious AAA. Identity management promises to reduce costs associated with current levels of security. That's an attractive business proposition.

What's more, strong(er) authentication will at some point become necessary, to secure computing topologies in which there's no effective perimeter defense. Thus, there's real growth ahead in the AAA area.

I think the AAA market will condense into a single class of servers. The technical challenges in identity management are much greater than those in authentication brokers, and anyhow the two categories are ready to overlap (e.g., both subsume SSO). I think authentication brokering will just become a necessary feature of identity management, and there will be a round of acquisitions to accelerate this.

Netegrity and RSA are two leading acquisition prospects. They both having trouble prospering as standalone companies; they both have high market share; they both have technology that would be useful to an acquirer. But other independents – Vasco? Oblix? – are reasonable acquisition candidates as well.

A few notes on specific players

Of all existing companies, *IBM* has the most pieces of a future AAA business. It acquired a "leading" identity management startup. It is a leader in database and other platform software, with a focus on integration; it is also a leader in security software. And via Lotus it has access to one of the two large installed bases of email/messaging users; messaging is one of the key applications storing identity information.

Computer Associates, in many ways, is right behind IBM. It's a powerhouse in security software, probably well ahead of IBM/Tivoli, and with the broadest product line of anybody. It's a second-tier player at best in database and data warehousing technologies, but that still amounts to a lot of expertise.

Microsoft has Active Directory and Exchange. And there are plenty of smaller enterprises that are pure Microsoft shops. But for most large enterprises, I think Microsoft will not be seen as a provider of security solutions; instead, Microsoft will long be seen as a causer of security problems.

Oracle hasn't yet decided whether it's serious about either security or database integration. But at least for pure Oracle shops, it's likely to roll out a fine identity management solution. A lot of pieces are still missing, but they'll get there in time.

BEA, as the only major platform software company without a DBMS, is trying to become the dominant provider of data integration software. What's more, RSA is building its authentication broker on the BEA platform. Don't rule BEA out.

With SecureID, *RSA* is the dominant authentication provider. Hopefully, one of the big players will at some point buy it and put RSA out of its standalone misery. Whoever does will have an instant lead in the authentication part of AAA. But if RSA stays independent, it's going to have a hard time prospering with its authentication broker strategy once the hardware token business finally begins to fade.

As the SSO leader, *Netegrity* is by some measures the most accomplished integration technology provider in the AAA space. It too is a natural acquisition candidate.