

Commentary

It's Time to Get Smart About Smart Cards

Everyone complains about passwords, but no one does anything about them. We believe the gain from using strong authentication has increased and the pain of implementation has decreased enough to make smart cards the way to go.

Gartner has a very active security, privacy and risk research community. Its analysts from across the world share research and debate the critical issues facing enterprises trying to secure their networks and information systems. We recently posed this question to the Gartner security analyst community: "If you had \$100 per user to spend on one thing to increase the level of information security at your company, what would you spend it on?" To focus the discussion, we limited the choices to one area and only counted the initial year's expenditure. A 10,000-user enterprise would have \$1 million to spend, one with 75,000 employees would have \$7.5 million, and so on. Although most corporate security groups despair of ever getting such a bonanza, many enterprises routinely increase their desktop computing spending by similar amounts when they standardize on PCs that include sound cards and speakers, for example.

Gartner security analysts were evenly split, with half believing stronger authentication (primarily smart cards) would be the most effective expenditure, while the other half believed spending the funds on user awareness and education would bring the most "bang for the buck." Here, we focus on the argument that smart cards to provide strong authentication for all enterprise users will provide a dramatic increase in security and a reduction in fraud.

Why Smart Cards Now?

In "Authentication: Who's That Knocking on the Door?" (TU-12-9616), Gartner compared the pros and cons of various authentication techniques. Strong authentication has a twofold effect on increasing security: It makes it harder for "bad guys" to do bad things, and it provides a strong audit trail to determine if trusted people do bad things.

In "Building Trust in Online Identities" (COM-12-9321), we explored the barriers enterprises face in trying to move from passwords to stronger forms of authentication. We concluded that smart cards would be the first technology to see widespread use, but that infrastructure barriers would prevent widespread adoption of smart cards before 2003. After all, industry pundits have been proclaiming every next year as the year of the smart cards since 1996. Yet, in late 2001, we still see no standard PC configurations containing smart card readers. Without readers as standard equipment, the costs and complexity of adding them will always doom smart cards to niche use. Mainstream enterprises will forego stronger

Gartner

authentication or resort to stopgap measures, such as USB dongles or password generator tokens that users resent.

If smart card readers were in every corporate laptop and desktop PC, the cost of using smart cards for network login would be negligible, especially for enterprises already using smart-card-based employee badges. The cost of deploying smart cards where readers are already ubiquitous would be in the \$10 per user range for large enterprises, and the incremental cost would be roughly half that when the smart card is already used as an employee badge or building access card. By combining a simple PIN number with the smart card, enterprises can have increased security with reduced password reset calls. If the smart card is combined with the employee badge, lost card rates will be no higher than lost badge rates are today, and employees will be less likely to share the smart cards with coworkers.

Where, oh Where Can My Readers Be?

However, smart card readers are not standard equipment in corporate PCs. If we budget \$10 per user for the cards, the remaining \$90 per user will need to go to smart card readers, installation costs and server-side set-up. A phased strategy would be to require all new PCs to be ordered with smart card readers as standard equipment and migrate users to stronger authentication as their corporate computer is upgraded. Gartner estimates that ordering desktops in keyboards or laptops with installed smart card readers will add approximately \$60 to \$80 to the cost of the typical enterprise PC configuration — less than 3 percent. This number would drop below \$50 if manufacturers believe including such capability will be required to win corporate competitions for PC procurement.

Therein lies the rub. The leading laptop and desktop computer vendors have been taking baby steps toward offering smart card readers as standard equipment for several years, but haven't seen enterprises demanding them as required equipment in requests for proposals. With margins shrinking, PC manufacturers have been offered incentives to compete on price and remove cost from computers, not increase cost. The "if we build it, they will come" philosophy doesn't work in times of commoditization, as hardware manufacturers are quickly punished by Wall Street if their profit margins drop below their competitors. This aversion to risk leads to lemming-like behavior by PC manufacturers, where no one jumps until they all jump. Gartner believes that if a few large global customers begin to require smart card readers as a standard feature, PC makers will make the jump.

Is Gartner Saying (Gasp) That 2002 Is the Year of the Smart Card?

Gartner has projected that by YE03, 30 percent of the installed base of corporate Windows 2000 users will use a smart card for network log-on (0.6 probability). Based on the current buying patterns of enterprises, that projection is still realistic. However, increasing that percentage or moving up the time frame would result in a significant increase in corporate security. If large enterprises with meaningful buying power changed those buying patterns to require smart card readers, the effect would be a forceful shove to the lemmings on the edge of the cliff. After all, a few years ago, most enterprises began requiring sound cards to be standard equipment, and today most employees can replace the standard Windows beep with all kinds of silly sounds. Taking a similar position on requiring smart cards can provide at least as much corporate benefit as hearing Homer Simpson say "Doh!" when new e-mail arrives.

Bottom Line: Current economic conditions don't make us optimistic that many enterprises will be motivated to increase per-desktop security spending, nor will manufacturers be willing to take risks without seeing evidence of such largesse by corporate PC buyers. However, given the design cycles of the most popular form of corporate computer — the laptop — large enterprises should move to begin pressuring their suppliers to include smart card capabilities as low-cost options in corporate PCs.