Smart Cards Aren't Always the Smart Choice

David Chadwick, University of Salford

Generally speaking, the more you pay for security, the more you get. However, security services also suffer from the law of diminishing returns. At some point, the costs of using the next feature-rich component outweigh the benefits you gain. The transition from worthwhile benefit to mere financial sink occurs at different points on the security continuum depending on the particular environment and application.

In environments where security is paramount, such as banking or military applications, the cost scales can be more heavily loaded before they tip the balance. In contrast, public administrations usually have more limited cash reserves, and they may have to forego most of the nice-to-have security bells and whistles.

The public healthcare sector presents an interesting dichotomy that emphasizes this dilemma. The security of patient-specific data is paramount, yet the public healthcare sector is chronically short of cash. Concerns about security have contributed to the healthcare sector's great reluctance to transfer patient-specific data between primary and secondary caregivers across the Internet.

The X.509-based public-key infrastructure may finally provide a safe, cost-effective way of transferring this confidential data. PKIs have a huge potential for reducing healthcare operating costs and waiting lists as well as having a positive impact on the quality of care. For example, PKIs facilitate the electronic transfer of confidential information such as referral letters, patient records, prescriptions, and high-resolution digital images of skin or eye disease.

In some scenarios, smart cards are not the security panacea that some people believe them to be.

Traditionally, Internet clients have stored users' private keys in software files encrypted with a user-chosen password. However, TrustHealth 2—a research and development project that has been implementing PKIs in various healthcare applications throughout Europe for nearly two years—chose to store users' private keys in smart cards. Using a password or PIN number protects smart cards, which are generally regarded as being more secure than encrypted software files.

SMART CARD ADVANTAGES

The benefits of using a smart card as opposed to a software token include

- increased security,
- potential user mobility, and
- sequential access to one machine by multiple users.

Two factors contribute to the increased security of smart cards. First, there is a decreased possibility of copying the smart card's private key because it never leaves the card. The smart card uses its on-board CPU to compute the transmitted data's digital signature. In contrast, with a software-based token, the computer decrypts the private key and holds it in memory while the CPU processes it.

Second, it's easier to copy a software-based token and to try to break the password at leisure without the user's knowledge. Fraudulent use of the smart card's private key is less likely because the attacker has to both steal the card and know the user's password or PIN. Guessing a card's password is usually fruitless because most cards use their on-board CPU to lock up after several wrong guesses.

Using a strong password to protect the software-based token significantly diminishes this second threat. It's almost impossible to break a 16-character password. For example, a short eight-character mixed-case and alphanumeric nonsense word or phrase gives 62^8 combinations (2.2×10^{14}), which is equivalent to 48-bit encryption. A 16-character password is equivalent to 95-bit encryption.

SMART CARD DISADVANTAGES

A smart card-based system doesn't automatically allow user mobility. User mobility is only possible if every machine that the user accesses has a smart card reader attached. The machine must support the same standard smart card reader interfaces or use the same proprietary smart card reader. Similarly, to use the same machine sequentially, multiple users must all use the same smart card technology.

In addition, smart card technology can be expensive. For example, the base price for a simple smart card reader is $25 (and significantly more if it has built-in security features such as key-

Editor: Ron Vetter, University of North Carolina at Wilmington, Department of Computer Science, 601 South College Rd., Wilmington, NC 28403; voice +1 910 962 3667, fax +1 910 962 7107; vetterr@uncwil.edu

pads), a PCMCIA-reader can cost up to $250, and the interface software requires an additional expenditure. The cards themselves cost between $10 and $30 each. Our supplier charges more than $100 for the software license fee for each smart card. While these costs should decrease with time, the initial investment in smart card technology can still cost more than $100,000 for an organization such as a hospital that has several thousand employees. This kind of expense can be prohibitive for healthcare organizations that are already dealing with scarce financial resources.

Some smart card implementations have slower performance than software-based tokens in current Pentium-based PCs, both during initial loading when a user logs on and during message signing and encryption. We found that cards were typically 5 to 100 percent slower during message signing and encryption, but they were up to an order of magnitude slower in the worst cases.

Because card implementations are relatively new, they are more buggy and rough around the edges than most other software. For example, the PKI smart card interface we use doesn't recognize a PCMCIA smart card reader if you dynamically remove and reinsert it (even after releasing the port). Instead, you have to reboot the laptop each time. It isn't always possible to freely move smart cards between machines unless the configurations are identical, and even then it can be a complex operation.

The equipment's physical limitations can include a shortage of slots (either PCMCIA or IRQs) for attaching the card to the PC. In addition, smart cards have a limited storage capacity. One smart card that we tried would only allow a single key update before its memory was used up, and then we had to use another card. In contrast, software-based tokens allow an unlimited number of key updates.

WHEN THE DISADVANTAGES OUTWEIGH THE BENEFITS

If users work primarily from their own PCs, there are few (if any) benefits to using a smart card instead of a software-based token, while there are still all of the disadvantages. Because the PC only contains the one software token, there is no possibility of mixing it up with another token or of someone inadvertently taking the wrong token. The PC remains fairly secure unless an attacker gains physical access and steals a copy of the token before trying to break the password—assuming, of course, that this PC isn't permanently connected to a network. In the healthcare sector, practice nurses, consultants, and general practitioners often have their own PCs.

Even if you use several PCs—for example, a home PC, a laptop, and an office PC—using a smart card has fewer benefits than you might at first expect. You can easily copy the software token for use on any one of the PCs. The only minor inconvenience occurs if you update the software token for some reason. Then you must remember to manually copy the updated token to each machine to synchronize them.

If users who can be trusted not to tamper with each other's tokens share an office PC, there is no significant additional benefit to using smart cards. Several users, for example in a general surgery practice, can share a PC that holds all their software tokens, and each user can select his or her own token prior to logging on to the security application.

Smart cards are beneficial in some scenarios, but they are not the security panacea that some people believe them to be. In some user environments, the costs and inconveniences clearly outweigh the potential benefits of using smart cards. ❖

David Chadwick *is a senior lecturer in the Information Systems Institute at the University of Salford, Manchester, England.* *This research was funded by the European Commission IV Framework Programme TrustHealth 2 Project (Contract No. HC 4023), the UK EPSRC Distributed Diabetic Dietician project under grant number GR/L60548, and Entrust Technologies.* *Contact Chadwick at D.W.Chadwick@ salford.ac.uk.*

Resources

URLs

- Information about the TrustHealth 2 project: http://www.spri.se/th2/default.htm
- Web site for Entrust Technologies Inc.: http://www.entrust.com
- An overview of ICE-CAR, a European project that promotes the use of public key infrastructures (PKIs): http://ice-car.darmstadt.gmd.de/
- ITU-T X.509: http://www-library.itsi.disa.mil/org/ituccitt/x_509.html
- The basic concepts of the Public Key Authentication Framework: http://www.ozemail.com.au/~firstpr/crypto/pkaftute.htm

Smart card information

- Answers to FAQs about medical smart cards from Health Card Technologies: http://www.hct.com/faq.htm
- A list of smart card resources from the Center for Instructional Technology: http://www.unc.edu/cit/guides/irg-35.html
- Smart card market statistics: http://www.cardshow.com/statistics/uk/philips.html
- An overview of the potential for using smart cards in the US: "Smart cards: The ultimate plastic"; http://www.businessweek.com/1997/20/b3527107.htm