ELECTRONIC PAYMENTS

Traceable e-cash

The widespread success and acceptability of electronic cash systems ultimately will involve striking a balance between anonymity and traceability

To be widely acceptable and therefore successful, electronic cash systems will ultimately have to strike a balance between anonymity and traceability. Traceable e-cash would make it harder to commit many crimes but would also threaten users' privacy. Completely untraceable digital cash would pose new difficulties for law enforcement agencies.

Although physical cash has certain properties of an anonymous medium, its anonymous use is significantly constrained by the following considerations:

- Bulk: large amounts of money take up a certain amount of space. The U.S. Bureau of Printing and Engraving, for example, no longer prints bills in denominations greater than $100, so a million dollars roughly fills up a large briefcase. This sort of bulk sometimes helps authorities track money.
- Transactional delays: the process of transferring, verifying, and counting bills takes at least a few seconds. For larger quantities, the times required are even less trivial.
- Palpability: physical cash cannot be transferred over a computer network, and transferring it securely to a remote payee takes time and resources that may render the process somewhat visible.
- Traceability: if law enforcement authorities know the serial numbers of bills being tracked, financial institutions may be able to help identify the next person who deposits them.

PETER S. GEMMELL
Sandia National Laboratories

0018-9235/97/$10 00©1997 IEEE

These properties can hamper certain types of criminal activity, including mugging, kidnapping, and other forms of extortion. One of the major challenges for a kidnapper, for example, is to get the payer to provide ransom in an anonymous form. With physical cash, the problem can be difficult: if the payer and the police cooperate, it can be hard to transfer a briefcase full of bills—despite even the coercive leverage of the kidnapper. Moreover, once the bills have been transferred, spending them without being identified is often troublesome because the serial numbers may well have been recorded. For muggers, too, it is not easy to remain anonymous after getting victims to hand over their loot. What's more, the mugger is limited to the anonymous money in the victim's pockets and perhaps to a few hundred dollars more obtained from a risky trip to an automatic teller machine and its camera.

E-cash and its problems

By contrast, with completely anonymous e-cash, the criminal's problem would be reduced to obtaining anonymous use of any one bank account. This might be achieved by setting it up under a false identity before an attempt at extortion began or by using a third party's account. Either way, once the account had been set up, the payer-victim would put the money in it, either directly or through the criminal, who would withdraw the money in a completely anonymous form.

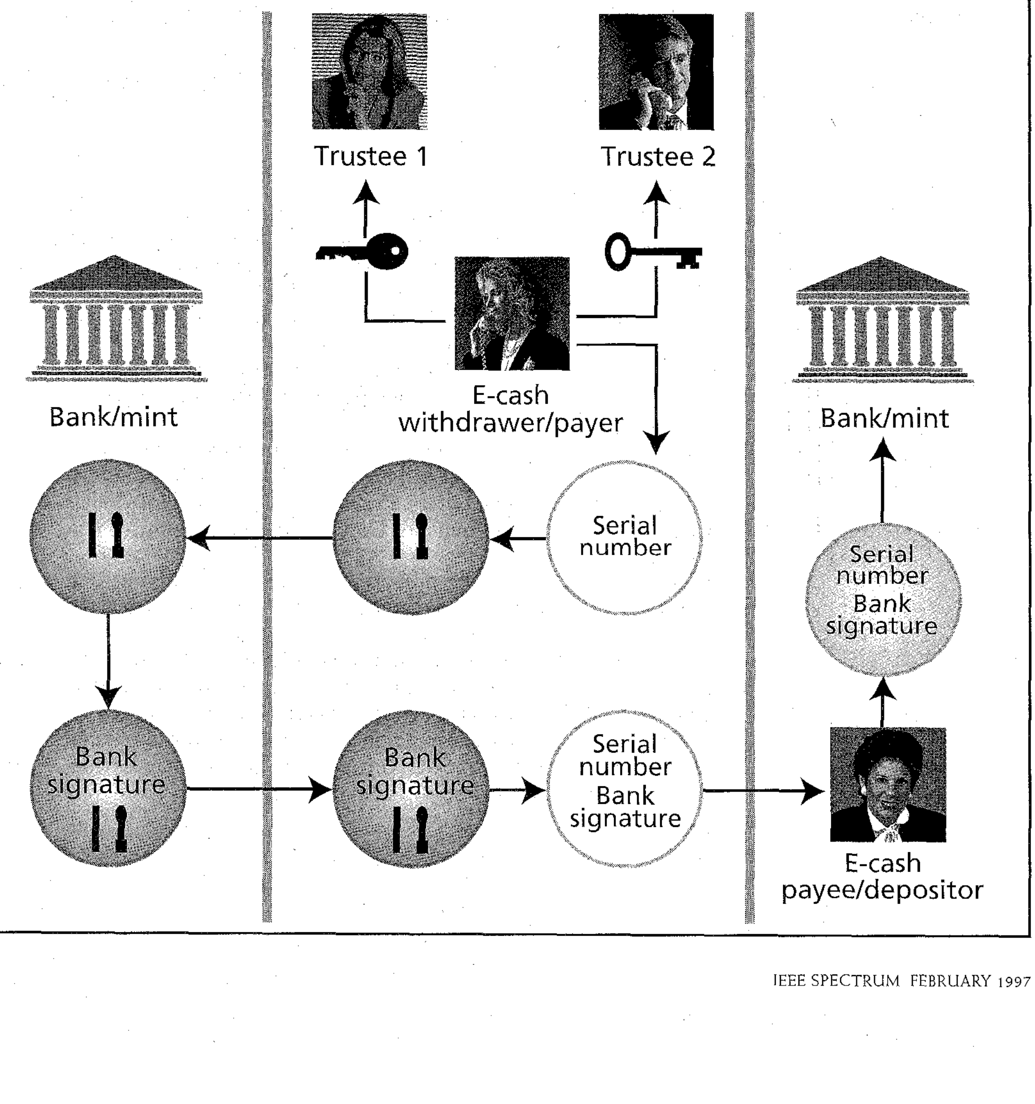
Money laundering, too, is hampered by physical cash and would be made easier by a completely anonymous electronic counterpart. Currently, if people suspect that the government is tracing physical cash, they may be forced to transport it to a foreign financial institution that will not continue the trace and there exchange it for different bills. This may be quite an inconvenience. With anonymous e-cash, money-laundering would be as simple as depositing one set of electronic "coins" in an account under an assumed name and withdrawing another set from the same account.

Moreover, it is now difficult for criminals to transport large amounts of money from one country to another; its sheer bulk makes it awkward to get past customs inspectors. With anonymous e-cash, however, it would be easy for a payer in one country to transfer funds to an overseas payee who would never have to explain where they came from.

Furthermore, consider the case of counterfeiting. With physical cash, even someone ambitious enough to acquire all the information, materials, and equipment needed to make apparently perfect counterfeit bills still has a problem: they would have serial numbers duplicating those of legitimate bills or made-up serial numbers that did not match those on any legitimate bill. In the former case, banks would eventually notice the existence of two or more bills with the same number and alert the proper authorities—in the United States, the Secret Service. In the latter, banks could in theory find out about the counterfeiting by comparing the numbers of bills they received with a database of legitimate numbers.

In completely anonymous e-cash systems, though, if a digital minting key used to create electronic coins were compromised, the result would be counterfeit cash indis-

To withdraw anonymous e-cash from a bank, a payer creates the shell of a coin at her computer and gives it a serial number. She then obscures the coin from her bank mathematically, although mathematical "keyholes" remain to allow trustees to reveal the coin (if necessary), and transmits it her bank. The bank signs it and returns it to the payer, who then uncovers the now-validated coin, which shows the original serial number and the bank's signature. The payer then transfers the signed coin to the payee, who can then redeem it at her bank.



tinguishable from the legally "minted" electronic variety. So long as the system managers were unaware that the digital minting key had been compromised, the counterfeiting could go on undetected. Of course, once system managers became aware of the crime, they could shut down the system temporarily, cash in the old money, and start up again with a new minting key. But there would be only one sure-fire way for them to find out that they had a problem: namely, observing that too much money had been deposited into accounts given the amount minted legitimately, together with the presumed amount of money currently in consumers' pockets and wallets.

Providing protection

Governments and financial institutions have been unwilling to support completely anonymous e-cash systems because of these threats. Yet until now, the only alternatives have been systems with little or no protection for the privacy of users. The challenge has been to develop a system that would provide such protection while also permitting law enforcement authorities to trace suspect transactions.

Sandia National Laboratories, Albuquerque, N.M., has attempted to develop computer protocols that strike a balance between these needs by giving the government and financial institutions the ability to control crime while maintaining privacy in other respects. A number of trustees, or key-escrow agents, would share the power to trace electronic transactions. Trustee-based tracing would be undertaken through cryptology. In this system, a tracing key or keys with a number of bits specific to a particular user and a particular withdrawal would be employed, and the operation would resemble the opening of a combination lock: to identify anyone who received money, it would be necessary to know the correct bits in the correct sequence.

Once a trace had been authorized, the tracing keys of a previously determined subset of trustees (for example, three out of five) would have to be combined for a search to be effective. Thus, if too few trustees revealed their shares of the tracing key, users' spending would be completely unlinkable to their withdrawals.

Such unlinkability protects users from the possibility that one or two trustees might be corrupt and is provable in the same sense that unlinkability is provable for completely anonymous protocols. Trustees could be individuals or organizations appointed by businesses operating e-cash systems or by a consensus of all parties involved. At the national level, trustees could be appointed to enforce national e-cash security.

Trustee-based tracing might resemble the current U.S. system for obtaining search warrants: if a law enforcement agency believed that it had a legitimate reason to trace an individual's spending patterns, it would seek permission from the courts. Should a judge deem the request legitimate, the trustees could be authorized to conduct a search and then make the information from it available to law enforcement authorities. Such a system would guarantee users that their spending patterns could not be detected by anyone or for any reason. At the same time, it would also give governments and other legitimate entities the ability to trace a user's spending with certainty but would otherwise be completely anonymous.

In a different trustee-based e-cash system, the users' "wallet" software would require them to supply the authorities from time to time with transaction records stored in their electronic wallets and encrypted with their tracing keys. These records could be decrypted only if the trustees used their shares of the tracing keys.

Another possible way of solving the anonymity problem might be to allow individuals to withdraw a modest amount of completely untraceable electronic cash a day—say US $100—remotely, that is, from their homes; there might be higher limits for withdrawals made in person at the bank. Any remote withdrawal above that sum would be traceable through the trustee-based system.

A number of variations on the trustee-tracing theme are possible. In some systems, users change their money with a number of electronic cash-issuing servers. In another, pseudonyms would be acquired from servers. Both ideas involve the creation of a trail that would have to be followed with the servers' cooperation for a trace to be conducted.

Electronic change

Anonymous electronic change is another important area. In a totally traceable e-cash world, anonymous change would not be an issue. But in a trustee-tracing or completely anonymous environment, it is a necessity. For older e-cash systems, including those aiming at total anonymity, it would be hard to make anonymous electronic change. If a consumer purchased a $5 item with $10 in electronic coins, for example, the $5 change could take the form of traceable electronic coins.

A simple approach to change might be for users to withdraw all their anonymous money in electronic "pennies" (that is, the smallest possible denomination), so that they would always have correct electronic change. Unfortunately, each electronic coin would require at least several thousand bits, so this approach is hardly feasible in most situations.

In early attempts to create anonymous electronic change, it might have been impossible for someone illegally tracing user spending to link a purchase directly with a user, but the tracer could easily tell when a user had made two different purchases. In this sense, a user's purchases would be linked to one another, and if the user were somehow to be identified in just one purchase, all the others would be linked indirectly to that user.

Anonymous electronic change remains potentially troublesome in off-line scenarios, in which only the payer and the payee need be active at the time of payment. However, Sandia National Labs has developed on-line anonymous change concepts that would let users and a bank anonymously exchange a set of electronic coins for another set with equal value but different denominations. The bank would not learn the user's identity, and the system would be protected from multiple spending of electronic coins. Without multiple spending or the help of trustees, it would be impossible to link the old coins to one another or to the user. Such anonymous change could be used in either trustee-tracing or completely anonymous environments. ◆

About the author

Peter S. Gemmell has been a senior member of the technical staff at Sandia National Laboratories in Albuquerque, N.M., since May 1995. His research interests include the design and cryptanalysis of cryptographic algorithms and protocols for such purposes as distributed cryptography and e-cash. He has also undertaken extensive work on formal techniques for establishing the reliability of software. This article reflects inventions made at Sandia by Ernie Brickell, David Kravitz, and the author.