

Figure 1. A general outline of the security module's PIN verification. Data needed for the verification is encrypted, transformed, and compared to the PIN-verification value from the ATM card.

the PIN from the BankAsept part and then misuse the Visa/MasterCard part, and vice versa.

Here, we focus on the court case concerning the misuse of one of Mr. A's stolen cards. Because the court didn't consider Spain's ATM system during the trial, we'll focus solely on Norway's system. The stolen card was a MasterCard/BankAsept card issued by a particular Norwegian bank. Using this ATM card, unknown criminals withdrew more than 9,000 Norwegian kroner (NOK)—US\$1,000 at that time—about an hour after Mr. A's bags were stolen. The ATM card was misused four times within about six minutes. Each time, according to the verdict, the thieves entered the correct PIN on the first attempt.

Norway's Bankklagenemda is a national committee that solves disputes between Norwegian banks and their private customers. Bankklagenemda didn't believe that the unidentified criminals had obtained the correct PIN by looking over Mr. A's shoulder, because Mr. A had last used the card at the airport in Norway, prior to leaving for Spain. This argument is strengthened by the fact that one of his wife's stolen cards, which had a different PIN and wasn't used at the Norwegian airport, was also misused in Spain.

Although Mr. A claimed that the only written copy of his PIN was in a safe at home, Bankklagenemda ruled that he must have kept the PIN with the card in the stolen wallet. Referencing the relevant Norwegian law, Bankklagenemda therefore ruled that Mr. A was responsible for 8,000 NOK of the loss.

Mr. A rejected this ruling and took the case to court in 2004. The defendant was the bank responsible for issuing the ATM card. According to the scenario favored by the court, Mr. A's PIN was first encrypted

with DES, then stored on the card's magnetic strip during the card's production. The bank's two expert witnesses claimed that it would be impossible to use the magnetic strip's information to determine the PIN in the one-hour period between when the card was stolen and first misused.

In contrast, the plaintiff's expert witness explained how the thieves could do most of the cracking in advance if they had prior access to a small number of cards issued from the same bank. The judge chose to believe the bank's experts, concluding that the plaintiff most likely kept a copy of his PIN in the stolen wallet.

Both the court and Bankklagenemda decisions fall into a well-established pattern of rulings. These institutions have long assumed that the ATM system is very secure; they've therefore ruled in favor of banks in most cases involving the misuse of stolen ATM cards. Many of these decisions were clearly correct because the card owners wrote down their PINs in an unsafe manner. However, the plaintiff's expert witness in the cited case was also correct. As we now describe, it was indeed possible for a cracker to determine the PIN belonging to an ATM card without any involvement from the card's owner.

An ATM system model

Our study is of the Norwegian ATM system during the period it employed DES to verify PINs. To withdraw cash from the ATM, customers place their cards in the card reader and type the PIN on the keypad. Information on the card's magnetic strip—including the PIN-verification value—is first read, and then transmitted over a secure channel to the bank.

The bank employs a (hardware) security module⁵ to verify the PIN. Figure 1 shows the verification process. The security module uses DES encryption, with a 56-bit secret key protected within the module. The 64-bit block of input data to the DES encryption consists of the customer's PIN and data from the ATM card's magnetic strip. The card's PIN-verification value isn't encrypted; instead, the DES encryption's 64-bit output block is transformed and compared to the PIN-verification value. If the two values are equal, the bank accepts the PIN and lets the customer withdraw cash from the ATM.

This transformation (represented by the oval block in Figure 1) isn't the same in all real-world ATM systems, and the Norwegian system's exact function isn't publicly known. In our simplified model, we assume only that the transformation produces a 16-bit result. For simplicity, we assume that all possible 16-bit values are equally likely.

In our model, the bank uses the same type of security module in both ATM card production and real-

time PIN verification. The part of Figure 1 starting with the input to the DES encryption and ending with the transformation's output defines how the module generates a 16-bit PIN-verification value. To ensure a match between the precalculated PIN-verification value and the value generated during a bank's real-time PIN-verification, both values must be based on the same DES key. In our model, this DES key is used to verify the PINs belonging to all cards issued by a given bank. Different banks have different DES keys.

For a given 64-bit input block to DES, many candidate keys result in the correct 16-bit PIN-verification value. Hence, the PIN-verification value partly determines the correct key—or, in more formal terms, the PIN-verification value constitutes a 16-bit condition on the secret key.

Attack strategy: **Description and analysis**

Using a two-step attack strategy, attackers can determine the PIN belonging to any ATM card issued by a given bank. It's therefore important to consider the possibility of successful attacks against the DES-based ATM system.

Step 1—Determining a DES key

Skilled attackers have been able to crack DES keys since the early '90s.⁶⁻⁹ Here, we describe how a fictitious attacker can learn the 56-bit DES key in Figure 1. We assume our attackers have the ability to read the information on any ATM card's magnetic strip. We further assume that they have an ATM card with a known PIN—one of their own cards, for example. Given these two things, attackers can determine the complete content of the 64-bit input block to the DES encryption in Figure 1. However, the attackers have a problem: They don't know the corresponding 64-bit output block; they know only the 16-bit PIN-verification value. So, the problem is that many keys cause the transformation in Figure 1 to produce a value equal to the PIN-verification value.

During the attack, the attackers must therefore try all 2^{56} keys and collect the 2^{40} keys that produce equalities in Figure 1. We derive the number 2^{40} from the observation that the crackers have a 16-bit condition on the key. Consequently, there are $2^{56}/2^{16} = 2^{40}$ keys that will give the correct PIN-verification value. However, only one key can correctly determine the PINs belonging to all ATM cards issued by the bank. That correct key is among the 2^{40} remaining keys. The attackers can reduce this set's size to 2^{24} keys by trying all 2^{40} keys together with a new ATM card that has a different PIN and PIN-verification value. To obtain the new card, the attackers might open another account, have another person open an account, or simply steal

the card and PIN from one of the bank's customers.

Using a third card, they can further reduce the set of 2^{24} keys to 2^8 keys. They can then determine the correct DES key using a fourth card. In the outlined attack, the attackers must store 2^{40} keys. If they have access to four different ATM cards with known PINs before the attack, they can test each of the 2^{56} keys against the four cards immediately and thus remove the need to store so many keys. This modification also reduces the number of candidate keys they must try to 2^{55} on average.

Step 2—Determining a PIN

Following step 1, the attackers know the DES key. To learn the PIN belonging to any ATM card issued by the bank owning the DES key, they connect a card reader to a computer to efficiently feed the data from a card's magnetic strip into a program mimicking the security module's operations. The program then tries different PINs until an encrypted PIN's transformed value is equal to the PIN-verification value (see Figure 1). This very simple technique gives the correct PIN because the PIN-verification value is available on the ATM card itself!

Analysis: The “key” points

Even today, calculating the key belonging to a DES-based security module takes time. Cracking a key also requires custom-built hardware or a large collection of PCs. The important point, however, is that crackers need only determine one DES key per bank. Once a DES key is known, the simple program described earlier can quickly ascertain the PIN belonging to any of the bank's ATM cards.

Because Norway's DES-based ATM system used four-digit PINs, the program had to try only 5,000 PIN values on average (assuming that all 10,000 possible PIN values were used equally often). In other words, once skilled attackers determined the DES key belonging to a particular bank's security module, any unskilled PC operator could use the program to establish the PIN belonging to any stolen ATM card from the bank in a matter of seconds.

Still, in our example case, a key question remains: *Did an attack occur?* One viewpoint holds that it's un-

A very simple technique reveals the correct PIN because the PIN-verification value is on the ATM card itself!

likely, because if real attacks occurred, there would have been a massive number of unexplainable withdrawals from Norwegian bank accounts. Attack centers would have emerged that let any criminal de-

termine PINs belonging to stolen cards. Alternatively, criminals could have “rented out” laptops to run Step 2 of the PIN cracking for thieves who’d stolen cards from a particular bank.

However, real attacks might not have necessarily led to massive fraud. According to our model, a thief must physically steal each ATM card. Most card owners immediately report card theft to their banks, which in turn immediately close the account so that it’s impossible to withdraw cash. Given rapid account closings, thieves would have to quickly attempt ATM cash withdrawals, limiting the number of cards they could steal and abuse in a given time period.

As a result, a successful attack strategy would require a group of thieves to steal and successfully misuse, say, 500 cards per year. ATM systems limit the amount of cash a customer can withdraw within a single week, requiring the thieves to operate in different locations, both so they could steal enough cards to make the operation profitable and avoid detection. Attacks on different banks would thereby create a distributed geographical pattern of ATMs processing stolen cards—much like the pattern we’ve seen during the past decade.

The number of misused cards and the geographical pattern of abused ATMs depend on the number of criminal groups. Given the expertise and resources required to determine one DES key per targeted bank—as well as the actual number of stolen cards each year—it’s unlikely that more than a few groups can have existed in Norway.

Ultimately, it’s hard for both banks and outside experts to discover whether real attacks occurred because there’s no simple way to determine if a DES key has been cracked. In any case, uncertainty about a thief’s ability to obtain a PIN remains, making it debatable whether the plaintiff in the cited court case actually kept the PIN and the stolen ATM card together.

Too much secrecy is counterproductive

As we now illustrate, too much secrecy can cause PIN-based authentication’s strength to seriously weaken over time unless countermeasures are implemented. In addition, a bank’s refusal to share technical information can seriously threaten a customer’s right to legal protection during a conflict.

Implications of security analyses

The bank’s expert witnesses seemed to be unaware of our example attack scenario.² Their claim that it was impossible to determine a PIN belonging to a stolen ATM card in less than an hour showed a limited understanding of the security level in Norway’s DES-based ATM system. We observed a similar lack

of understanding when we analyzed customer authentication strength within the Norwegian Internet banking system. Several banks were completely unaware that they were vulnerable to distributed attacks against customer accounts during 2003 and 2004.⁴

In 2006, our investigation of Norway’s banking systems showed that banks continue to repeat well-known security mistakes. One experiment demonstrated how attackers could configure Internet browsers to connect to many Internet banking servers via SSL tunnels that use 40-bit key encryption—ignoring the fact that 40-bit keys can be cracked in a few seconds. Two banks also allowed browsers to use SSL with null encryption—that is, the data was unencrypted, and the banks relied solely on authentication and integrity checking. In addition, we found one mobile banking application that didn’t use SSL at all, due to a system misconfiguration. Although such SSL problems can easily be fixed, some banking systems also had architectural and design weaknesses that are far more challenging to address.

Our investigations of the ATM system, Internet banking systems, and mobile banking systems all indicate that Norwegian banks were not performing thorough, periodic risk analyses. In fact, according to its own records, the Financial Supervisory Authority of Norway—a government agency overseeing Norwegian banks—had not instructed any Norwegian banks to carry out IT systems risk analyses prior to August 2003.

DES cracking became a threat only as time passed and computer technologies improved. Similarly, the attack scenarios against the Norwegian Internet banking systems weren’t a problem when the systems were new and had few users. As the number of users increased, however, the systems became increasingly vulnerable. The acceptance of 40-bit encryption indicates that many banks don’t understand that secret-key length must increase as computers become more powerful. Indeed, it’s been many years since 40-bit encryption was safe.

Finally, Norwegian banks continue to keep all system information secret and don’t allow independent experts to analyze their systems. As a result, few security experts have an intimate understanding of the Norwegian banking systems. Over time, the banks’ own experts tend to start thinking alike—particularly because they can’t freely discuss their systems with outside experts. As a result, they have a propensity to overlook slowly developing system vulnerabilities.

The role of Bankklagenemda

During the past decade, the Bankklagenemda committee has considered numerous cases involving stolen

ATM cards. As mentioned, the committee has almost always concluded that the card owner must have stored the PIN together with the card—a conclusion the card owners typically dispute. This state of affairs continues even today.

Throughout its proceedings, Bankklagenemda has based its decisions on the assumption that the ATM system has had, and still has, a high degree of security. As evidence, they initially referred to a 1993 note from the Norwegian Central Bank, which stated that it was impossible to crack the PIN using the information on the magnetic strip. Our fictitious attack scenario shows the opposite; in the 1990s, at least, it was indeed possible to crack PINs in this way.

More recently, Bankklagenemda has begun citing a 2002 letter from the Financial Supervisory Authority of Norway. This letter cites a security report—completed in 1997, and then reevaluated in late 2001—written by representatives from the Norwegian bank community. The report isn't available to the public.

Even after the ATM system in Norway and many other countries began using triple DES, there were strong indications that the security level might be lower than the banks have advertised. Ross Anderson and colleagues described numerous physical and logical attacks on security modules, including powerful remote attacks on a module's API.⁵ Mike Bond and Richard Clayton describe a clever insider attack that determined triple-DES keys.⁹ Omer Berkman and Odellia Moshe Ostrovsky reported severe attacks on the API of security modules used in both network switches and banks.¹⁰ These attacks exposed customer PINs by executing one or two API calls per PIN.

Some card owners undoubtedly forget that they've written down their PIN, and others might knowingly lie about doing so. Still, it's unfortunate that Bankklagenemda has, over many years, branded numerous bank customers as liars without ever thoroughly reviewing the ATM system's security. Unlike the earlier secret self-evaluations from the Norwegian bank community, independent security experts should carry out a new review of the ATM system and make the findings publicly available.

Court case update

As long as the true security level is hidden from the Norwegian courts, it's very difficult for bank customers to win cases against the banks. The case we describe here illustrates this problem. The international research community had known that DES was unsafe for many years. Still, it was difficult for the plaintiff's lawyer to refute bank's expert assertions because the bank didn't have to provide the lawyer with any information about the ATM system.

The plaintiff appealed the verdict to a higher court.

According to the judge's ruling during the first trial, the ATM system used DES to verify a PIN when the card was stolen. During the appeal process, the defendant's lawyer tried to show that the ATM system had actually used triple DES, not DES, to verify PINs. The fact that this key information wasn't established during the first trial only underscores how important it is to have access to correct technical information.

During the appeal process, the plaintiff's lawyer asked for more information from the bank, but very little was given. In particular, they argued that it must keep secret an encryption algorithm developed to do PIN-verifications for MasterCard transactions. According to established security thinking, there's no need to keep cryptographic algorithms secret. In fact, it's considered very bad practice. Unfortunately, the plaintiff had to withdraw the case for economic and personal reasons before the higher court could consider it.

Discussion

As we see it, neither Bankklagenemda nor the judge wrongly interpreted the laws pertaining to the case. Rather, the real problem was that both the committee and the court accepted the banks' claims that their systems were very secure. Given this premise, the conclusions that both parties drew were unavoidable.

Norwegian banks can make strong security claims without having to provide any adequate documentation for at least two important reasons. First, the many cases that both Bankklagenemda and the court must hear force them to allocate limited time to cases involving ATM card misuse. During the restricted time available, the Bankklagenemda lawyers and the court's judges might find it difficult to make sense of security experts' conflicting technical claims. This is particularly likely given that most lawyers and judges have a limited understanding of large networked computer systems in general, and perhaps an even weaker understanding of the systems' security aspects. Bankklagenemda and the court therefore rely on "conventional wisdom"—that is, that the ATM system is very secure—rather than believing opposite claims made by independent security experts with limited access to the ATM system's technical information.

Second, banks have argued that they can't provide the court or the plaintiff with any technical information about their systems because doing so would make the systems less secure. Because lawyers and judges, like the rest of the Norwegian population, depend on these systems, they're unlikely to do anything to reduce their security. The counter-argument here—that too much secrecy decreases security over time—is unknown to most of the public, including lawyers and judges. As long as only a few university

and industry security experts partake in the public debate in Norway about these issues, there's no real pressure on the banks to change their security-by-secrecy policy.

We believe that the refusal to share information indicates a very limited understanding of real security among the banks' senior management and the lawyers they employ. In the long run, more openness around security questions, better security education, and more applied security research could make the banks change their security-by-secrecy policy. It could also convince Bankklagenemda and the court to ask the banks to provide thorough documentation of their security claims. Until this happens, Norwegian bank customers are at a disadvantage during conflicts with their banks.

Finally, in the future, Bankklagenemda and the court should seriously consider the possibility that an outside cracker or a rogue insider was able to determine the PIN belonging to an ATM card; this will lead to a more balanced evaluation of disputes concerning ATM card misuse.

Our analysis and discussion of the court case involving a previous version of the Norwegian ATM system is motivated by three goals:

- To show that at least one Norwegian bank didn't know about a relatively simple attack on the DES-based ATM system, which led to it providing a Norwegian judge with incorrect information.
- To argue convincingly that the lack of insight into ATM system security was, in large part, caused by the strong belief that secrecy leads to good security. Unfortunately, in reality, too much secrecy leads to "groupthink" and reduces the ability of experts to evaluate a system's true security.
- To illustrate that secrecy makes it very difficult for a customer to win a case against a bank. As things stand today, a Norwegian bank has an unfair advantage during a conflict because it can simply state that its security level is very high without having to provide any evidence to support the claim.

We don't claim that the attack we discussed was the most likely scenario at the time the plaintiff's ATM card was misused. We analyzed the scenario because it was discussed in the judge's written ruling. In fact, we believe that the court should have considered additional—and perhaps more likely—attack scenarios. In particular, the court should have investigated the ATM system in Spain.

Many international banks believe that secrecy is a prerequisite for good security, and many have systems

that are similar to those in Norwegian banks. We therefore have some recommendations of general interest.

First, banks need better development processes. Our analysis of

- the older ATM system featured in the case,
- newer Internet banking systems,⁴ and
- a new national security infrastructure for online banking

all indicate that better processes are needed to develop banking systems that remain secure over time. Our discussions with bank experts have led us to conclude that a bank's development team must collaborate more closely with outside lawyers, security experts, and customers. Such collaborations are hampered when a bank's policy dictates that the development team must keep all system information secret.

In particular, banks need improved architectural and design processes that better incorporate security aspects. These processes must produce architectural and design documents understandable not only to system developers, but also to external security experts. The lack of adequate documentation makes it difficult to carry out periodic security reviews of the architecture and design, reducing the likelihood that slowly developing security problems will be discovered before they become serious.

Second, customers need better legal protections. Future banking systems' architectural and design documents should be publicly available. The ability to use independent security experts to evaluate a banking system's security during a conflict significantly increases a customer's legal protection.

Finally, in Norway, the true role of Bankklagenemda in attempting to resolve conflicts between customers and their banks is unclear. Many of its decisions are based on security evaluations produced by the Norwegian banking community. These documents are unavailable to banking customers and, as far as we know, have not been evaluated by independent security experts. To make fair decisions, Bankklagenemda and other, similar committees should use independent experts to evaluate a bank's security claims. □

Acknowledgment

We are grateful to the reviewers for many useful comments and suggestions that significantly improved this article.

References

1. S.T. Kent and L.I. Millett, eds., *Who Goes There?* National Academies Press, 2003.
2. *Verdict from Trondheim Tingrett*, 24 Sept. 2005, case number 04-016794TVI-TRON (in Norwegian).
3. US Nat'l Inst. Standards and Technology, DES (Data

- Encryption Standard), US Commerce Dept., Oct. 1999; <http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>.
4. K.J. Hole, V. Moen, and T. Tjøstheim, "Case Study: Online Banking Security," *IEEE Security and Privacy*, vol. 4, no. 2, 2006, pp. 14–20.
 5. R. Anderson et al., "Cryptographic Processors—A Survey," tech. report 641, Computer Lab., Univ. of Cambridge, 2005; www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-641.pdf.
 6. R. Anderson, "Why Cryptosystems Fail," *Proc. 1st ACM Conf. Computer and Comm. Security*, ACM Press, 1993, pp. 215–227.
 7. Electronic Frontier Foundation, *Cracking DES*, 1998; www.eff.org/Privacy/Crypto/Crypto_misc/DES_Crackerr.
 8. RSA Laboratories, *RSA DES Challenge III*, 1999; www.rsa.com/rsalabs/node.asp?id=2108.
 9. M. Bond and R. Clayton, *Extracting a 3DES Key from an IBM 4758*, Computer Lab, Univ. of Cambridge, 2001; www.cl.cam.ac.uk/~rnc1/descrack.
 10. O. Berkman and O.M. Ostrovsky, "The Unbearable Lightness of PIN Cracking," Algorithmic Research Ltd., 2006; www.arx.com/documents/The_Unbearable/_Lightness_of_PIN_Cracking.pdf.

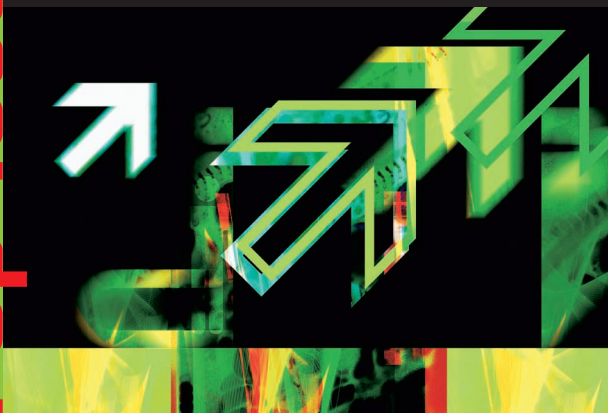
Kjell J. Hole is a professor in the Department of Informatics, University of Bergen, Norway. His research interests include risk management and application security. Hole has a PhD in computer science from the University of Bergen. He is a member of the IEEE and the IEEE Computer Society. Contact him at kjell.hole@ii.uib.no.

Vebjørn Moen is a governance and security analyst at GE Money Bank, Norway. He contributed to this article as a student at the Department of Informatics, University of Bergen, from which he has a PhD in computer science. Contact him at moen@ii.uib.no.

André N. Klingsheim is a PhD student in the Department of Informatics, University of Bergen. His research interests include network and application security. Klingsheim received an MS in computer science from the University of Bergen. He is a member of the IEEE Computer Society. Contact him at klings@ii.uib.no.

Knut M. Tande is an associate professor at the Faculty of Law, University of Bergen, Norway. His research interests include legal methodology and copyright. Tande has a higher doctorate (dr. juris) in legal science from the University of Bergen. Contact him at knut.tande@jur.uib.no.

Sign Up Today



For the
IEEE
Computer Society
Digital Library
E-Mail Newsletter

- Monthly updates highlight the latest additions to the digital library from all 23 peer-reviewed Computer Society periodicals.
- New links access recent Computer Society conference publications.
- Sponsors offer readers special deals on products and events.

Available for FREE to members, students, and computing professionals.

Visit http://www.computer.org/services/csdl_subscribe