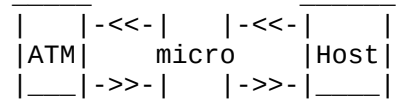
Jackpotting ATM Machines courtesy of the Jolly Roger

JACKPOTTING was done rather successfully a while back in (you guessed it) New York. What the culprits did was:
Sever (actually cross over) the line between the ATM and the host. insert a microcomputer between the ATM and the host. insert a fradulent card into the ATM. (card=cash card, not hardware)
What the ATM did was: send a signal to the host, saying "Hey! Can I give this guy money, or is he broke, or is his card invalid?"
What the microcomputer did was: intercept the signal from the host, discard it, send "there's no one using the ATM" signal.
What the host did was: get the "no one using" signal, send back "okay, then for God's sake don't spit out any money!" signal to ATM.
What the microcomputer did was:
intercept signal (again), throw it away (again), send "Wow! That guy is like TOO rich! Give him as much money as he wants. In fact, he's so loaded, give him ALL the cash we have! He is really a valued customer." signal.
What the ATM did:
what else? Obediently dispense cash till the cows came home (or very nearly so).
What the crooks got:
well in excess of $120,000 (for one weekend's work), and several years when they were caught.
This story was used at a CRYPTOGRAPHY conference I attended a while ago to demonstrate the need for better information security. The lines between ATM's & their hosts are usually 'weak' in the sense that the information transmitted on them is generally not encrypted in any way. One of the ways that JACKPOTTING can be defeated is to encrypt the information passing between the ATM and the host. As long as the key cannot be determined from the ciphertext, the transmission (and hence the transaction) is secure.
A more believable, technically accurate story might concern a person who uses a computer between the ATM and the host to determine the key before actually fooling the host. As everyone knows, people find cryptanalysis a very exciting and engrossing subject...don't they? (Hee-Hee)



The B of A ATM's are connected through dedicated lines to a host computer as the Bishop said. However, for maintenance purposes, there is at least one separate dial-up line also going to that same host computer. This guy basically bs'ed his way over the phone till he found someone stupid enough to give him th number. After finding that, he had has Apple hack at the code. Simple.
Step 2: He had a friend go to an ATM with any B of A ATM card. He stayed at home with the Apple connected to the host. When his friend inserted the card, the host displayed it. The guy with the Apple modified the status & number of the card directly in the host's memory. He turned the card into a security card, used for testing purposes. At that point, the ATM did whatever it's operator told it to do.
The next day, he went into the bank with the $2000 he received,

talked to the manager and told him every detail of what he'd done. The manager gave him his business card and told him that he had a job waiting for him when he got out of school.
Now, B of A has been warned, they might have changed the system. On the other hand, it'd be awful expensive to do that over the whole country when only a handful of people have the resources and even less have the intelligence to duplicate the feat. Who knows?