cheaper than a Powerball ticket.

Another approach, related to cracking the RSA-2048 bit key, is to modify an existing, signed Xbox executable in a useful manner without changing its cryptographic hash value. Such a constructive hash collision would make the modified executable look identical to the original as far as the digital signature check is concerned. The hash used in the Xbox's digital signature algorithm is SHA-1. SHA-1 is a 160-bit hash with no publicly known algorithmic weaknesses; since the source of the hash is fixed, about 2^{160} random variations would have to be tried to discover a collision. As a side note, you can't use a birthday attack to reduce the difficulty of the attack to 2^{80} random variations because we are not trying to find two messages that hash to the same arbitrary value. The goal is to generate a specific target hash, or perhaps one of a very limited set of target hashes harvested from the set of all published Xbox game titles. Hence, this approach also falls into the category of "Very Difficult Problems".

An alternative approach to Project B is to find security holes in Xbox softwares and use the holes to seize control of the CPU's instruction pointer. To see how this is helpful, consider this example. Suppose a network-based buffer overrun exploit was discovered in a game that can lead to arbitrary code execution. A program running on a PC connected to the Xbox via the network could then use this exploit to send packets to the

Figure 11-1:

The Xbox-Linux core team at the 19th annual Chaos Computer Conference, held in Berlin, Germany. In the back, Michael Steil; in the front, from left to right: Andy Green, Milosch Meriac, and Franz Lehner.

Photograph courtesy of Gerhard Farfeleder.

Xbox that has the effect of installing a simple bootloader for Xbox-Linux. This bootloader could be something as simple as a program that runs code at a designated location on the Xbox's hard drive or on the DVD drive. Note that any port where the Xbox can accept data is a vector for this kind of attack. This includes the USB and network port as well as the hard drive and the DVD-ROM drive. Corrupted save games or file structures can be imaged onto the hard drive or DVD-ROM drive that cause the Xbox to run user-developed code. To Microsoft's credit, all of the network interactions and save game protocols use fairly strong and well-tested security techniques. In addition, I heard at a presentation about the Xbox by Microsoft at MIT that all game code is inspected by a buffer overrun checker and that Microsoft has contractual remedies against game developers that are found guilty of putting deliberate back doors into their game code. This points to the Xbox code base being more secure than a typical Microsoft product, which makes it all the more of an interesting problem for hackers to work on. If you are interested in participating in hacking on the Xbox as a part of "Project B", I encourage you to first check out the Project B Prize Rules web page at `http://xbox-linux.sourceforge.net/articles.php?aid=20030023081956`.

Recently, a buffer overrun exploit was discovered in the way saved games are handled by Electronic Arts' "007: Agent Under Fire" game. The exploit was first divulged by a hacker known simply as "habibi_xbox" on March 29, 2003 through a posting on the XboxHacker.net BBS. Significantly, the

Profile: Milosch Meriac

Can you tell us a little bit about yourself?

My general history is fairly simple. I was born 1976 in Czechoslovakia. My parents (mother teacher, father civil engineer) escaped during cold war to western germany because of repressions by the communist regime. I was about three years old when we arrived in Germany. In German kindergarden I immediately learned the German language. From this point it was really simple - being ten years old, I got my first computer after some months of whining. Things started to roll.

After school leaving exams and a weird intermezzo at German Federal Armed Forces Military Duty i started studying cybernetics and computer science, but i decided after three years to quit university and to concentrate as a long-term objective on my own company. During my studies i established some valuable business connections, so it was easy to work as a freelancer for various companies in Germany. I did some reverse engineering projects, developed realtime embedded linux systems with small footprint, did some lowlevel programming like realtime extensions for windows systems and developed a software based harddisk safeguard for a famous German company. I now live with my Girlfriend in Berlin and we are having a great time there.

continued...