Implants

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University, Northfield VT

"Daddy, why is there a Yinghui poster floating in front of the holovision display?"

Six-year-old Mei seemed puzzled but not alarmed.

"What do you mean, a poster?" asked her dad through his neural link, eyes opening wide in concern as he switched his receiver into high-volume mode.

"It says, 'U r .." she paused and spelled out the next word, "… p-w-n-e-d."

Xiayue Dien was an implant engineer at DienhuaKwai Corporation, makers of the real-time-access implants he and his daughter were using to watch the live HV feed from the lunar volleyball tournament. He accessed his daughter's sensory feed and the hair on his neck tickled as he felt the blood drain from his face.

"Um, sweetie, don't worry about it. The message is some sort of joke, I'm sure."

Actually, Dien was far more worried than he let on. The fact that the message was inserted at all was alarming enough, but having "English" inserted into an implant's output was terrifying. The criminal hacker gangs from Bei Mei had been trying to crack the dynamic encryption routines on the RTAs for years, but until recently, they'd never managed to penetrate the cyclic asymmetric algorithm that ensured that the data streams couldn't be corrupted.

"Pwned" was an ancient word dating from the late 20th century that meant roughly "owned" or "controlled." It had been popular until about a hundred years ago, in the mid-21st century but had died away – until last year, when reports surfaced on the internal networks that a few users of the latest three models of the RTA units were noticing intrusions into their data streams.

The first report he had seen referred to a relatively young woman of 62 in Fuzhou who experienced inexplicable movements of her prosthetic left hand; the first three fingers were waggling back and forth for 30 seconds at what seemed at first to be random intervals. Luckily, the other four fingers on the hand seem to be working OK, so she hadn't dropped anything. As the tech support team got involved, they invoked the logging function on the RTA and shot the data stream to their central pod in Harbin. Careful analysis and a good deal of creativity revealed that the episodes were occurring at exactly 01:00, 02:00, 03:00, 05:00, 07:00, 11:00, 13:00, 17:00, 19:00 and 23:00 – California time! It was obvious that these were prime numbers imposed on a 24-hour clock, and the use of California time strongly suggested that one of the resistance cells left in the old "USA" (now Meiguo) might be involved. Some of those troublemakers simply couldn't get over the change of administration and language that had occurred over three generations ago when the old People's Republic had finally won control of the entire "North American" (Bei Mei) continent (now the provinces of Tsianada, Meiguo, and Wusike) using effective asymmetric warfare and established the People's Empire. The barrage of cyberattacks launched against the critical infrastructure of those countries had effectively shut down their entire civil and governmental rule, leaving the continent easy pickings for the People's Liberation Army invasion.

Dien connected to his office network within a few seconds and accessed the cyber-situational awareness tools that constantly monitored all systems in the empire for possible intrusion or corruption – in addition, of course, to the perpetual scan for disloyal information flows. That side of the dashboard he was visualizing with the input from the network showed the usual sporadic outbreaks of unapproved anti-government propaganda. "Propaganda" was defined as revealing personal enrichment of protected officials, documenting sexual peccadillos by various high-ranking members of the Politburo, and reporting occasional excesses by the PLA leading to excessive deaths (excessive only from the point of view of friends and families of the survivors) in their zealous suppression of treason and revolt at home and in the new provinces.

The dashboard did show, however, that there was a flood of intrusions throughout the Empire that was contaminating the RTAs and causing operational and visual distortions. Most of the reports indicated that the monitors had classified the intrusions as propaganda: people all over the Empire were receiving full access to the private records of the highest-placed officials in the Empire – and there were side-bar reports of growing anti-Empire activity. If the anti-revolutionaries' access to the RTAs were not shut down immediately, there could be riots comparable to those of the early 21st century, when failures in the Great Firewall had allowed foreign agitators to foment counter-revolutionary revolts that had led to the death of over 49 million citizens at the hands of the People's Liberation Army. The problem had been that later analysis showed that many of the victims had in fact had nothing to do with any counter-revolutionary activities at all: the PLA had based its actions on flawed information in its databases. Apparently a programmer had been granted access to the databases maintained by the PLA and had accidentally toggled the flag for counter-revolutionary status in some 40 million records without noticing it. The PLA had used the altered records in their house-to-house searches and had executed the corresponding number of innocents as part of their standard operating procedure.

The problem now was that shutting down access to the implants was not easy. Implants were as widespread as the old mobile phones had been in the old days – and everyone depended on immediate access to information that was authorized for distribution by the Empire. Children had their implants installed by the age of two; schooling centered on effective mastery of the devices using neural feedback techniques. In the rare cases where implants had to be shut down or removed, the users found themselves completely isolated from normal interactions. Most people no longer "talked" using their vocal cords once they had their implants; it was so much more effective using the artificial telepathy of the devices for direct contact. The Empire had worked hard to establish the firewalls that prevented the proletariat from accessing leaders' channels so that no inappropriate information would be leaked downwards – and now it looked like those efforts were crumbling.

Dien would have to conference with his colleagues on a high-priority channel to exchange information about the growing crisis. Open access to information was the most dangerous threat to the power structure and the continuation of peace, order and good government in the Empire.

Dien felt the foundations of his world trembling.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *