

SPECIAL SUPPLEMENT TO DEFENSE SYSTEMS

NOVEMBER / DECEMBER 2006

UNCHANGED INTRUSION RISKS

Threats to modern cryptography generally fall into the same two risk categories as previous generations of the technology, according to Chris Fedde, senior vice president and general manager of SafeNet Inc. of Belcamp, Md.

The first is decryption of the traffic itself, which depends on the enemy having the computing horsepower to crack the algorithms, says John Pescatore, vice president of security research at Gartner Inc. of Stamford, Conn. "That's why they're swapping everything out. Today's standard, the Digital Encryption Standard, goes back 25 years to when I worked signals crypto at NSA," he adds.

The second threat is the sideways attack or workaround. That is the enemy obtaining a key or password to crack a device. Faulty passwords continue to be a major failure point. In August, Trusted Strategies, a Pleasanton, Calif., IT security consulting group, identified password lapses as the number one cause of data loss and damage based on analysis of Justice Department prosecutions between 1999 and 2006.

For this, and other reasons, key management is vital to the security of encrypted communications. An example is what happened after the United States lost an AWAC spy plane over China in 2000.

"One could easily assume that the Air Force re-keyed very quickly after that AWAC went down. And you can imagine that wasn't easy, given the shortcomings in previous key manageability," says Peiter "Mudge" Zatkó, division scientist and technical director of decision and security technologies for BBN Technologies Inc. Zatkó, a cryptography expert, co-developed l0phtcrack (still the most common tool used to crack encrypted passwords).

Device tampering is another example of a sideways attack, says Benjamin Jun, vice president of technology for Cryptography Research Inc. of San Francisco. Protective measures should center on the key, which should never be extractable from the device, he says. Anti-tampering measures today include ways to turn a lost or stolen device off, erase its contents or otherwise make it unusable.

"Gooping up" chip components inside the box so the enemy can't distinguish them protects against chip tampering. But protections should also cover power output readability at the transistor level, say Jun and other experts who know how to read transistor energy to extract keys and passwords.

"You've got transistors humming on a chip while the computation is being done, which uses power," explains Jun, who specializes in transistor-level cracking and

protection technology. “Instead of cracking the crypto, the enemy just listens for it.”

These power currents coming off the transistors act like signals that properly placed spying devices can pick up, he says. The sniffing devices must be within a foot of the system or within it for this to work, Jun acknowledges. But if the desire to obtain the data is strong enough, such attacks mustn't be overlooked because they are not improbable or impossible, he adds.

“Apply this to smaller devices that are mobile and can be dropped in the battlefield, lost, stolen or borrowed,” he says. “With the miniaturization of command and control devices, we must rely more on the technology for built-in protections.”

Cryptography Research, says Jun, has been working with Raytheon Co. and other defense contractors on cryptographic enhancements that would protect against tampering with mobile devices. —*Heather B. Hayes*