
By STEPHEN BONO, AVIEL RUBIN,
ADAM STUBBLEFIELD, *and* MATTHEW GREEN

SECURITY THROUGH LEGALITY

*The law alone won't prevent an unauthorized visit or even a deliberate attack.
Security depends on being able to think like an attacker.*

T

hat would work, but no attacker would try it,” said the chief designer of a wireless security system we had been contracted to evaluate. After several questions from across the table, we had determined why this particular security product would fail even against an adversary who was only modestly innovative. The security designers, along with a corporate manager and an electrical engineer, had made the common mistake of misunderstanding the potential adversary’s state of mind and unnecessarily bounded the scope of attacks that might be employed. We reminded them that the threat model for any system shouldn’t be based on what an attacker would probably do but on every possible thing an attacker could do.

MISUNDERSTANDING THE ADVERSARY AND RELYING ON THE LAW AS A CRUTCH HAS YIELDED INEFFECTIVE AND DAMAGING RESULTS.

Misunderstanding an adversary's mind-set and possible intentions has led numerous commercial security products to rely on the threat of legal action as a way to provide security, rather than on tried-and-true security measures. "Security through legality" has been a crutch, as well as a scapegoat, for justifying lax security provisions. As typically found with its better-known counterpart "security through obscurity," adopting this hopelessly flawed methodology can lead to systemwide compromise and cost exorbitant amounts in damages. Relying on legislation for protection has proved ineffective in the face of widespread abuse, illogical when incorporating a criminal's apathy toward the law, and to be a way to limit research by law-abiding professors and citizens who

seek to improve security rather than subvert it. This is not to say that criminal prosecution and the law don't play a significant role in providing a secure information landscape. But the unlawfulness of any action does not explicitly prevent it from occurring, suggesting only that it be avoided.

Treating the secrecy of a system's design as a security measure is commonly referred to by experts as security through obscurity. This faulty methodology is widely known among security experts for yielding insecure systems, as simple disclosure of the design can lead to catastrophic security failure. Still, many modern security devices and applications rely solely on a criminal's inability to figure out how a system works or obtain design documents rather than tried-and-true security methods.

In the same way security through obscurity has inspired insecure systems based on the fallacious assumption that an adversary probably wouldn't do something, we have noticed an unfortunate trend in commercial security system design of making faulty security assumptions based on what an adversary is legally allowed to do. Security through legality is the misconception that an adversary will not pursue some avenue of attack just because doing so is unlawful.

In lieu of developing preventive measures, designers occasionally argue that criminal prosecution is a sufficient deterrent to system compromise. On the contrary, criminals do not generally let laws stand in the way of breaking laws. A burglar intent on acquiring thousands of dollars in jewelry from a potential mark's master bedroom is well aware of the penalty if caught and is hardly concerned with the vandalism charge resulting from a broken window.

The U.S. Digital Millennium Copyright Act (DMCA) of 1998, as well as other copyright laws around the world, provide a more than adequate example of how criminalizing certain activities is not sufficient for preventing crimes from being perpetrated. During the past decade, the growing popularity of file-sharing networks has made piracy a major concern of the movie, music, and software industries. Though awareness of piracy as a crime and the fear of prosecution has attracted the public's attention, no significant evidence has emerged that the unlawfulness of piracy has actually slowed its spread. To be fair, no digital rights management (DRM) system has yet prevented the widespread piracy of movies or music, but preventive measures, rather than deterrents, must always take precedence when designing a security system.

The movie industry once relied on the DVD Content Scrambling System (CSS) to prevent piracy.

Between 1996 and 1999, DVD copy protection depended on the inability of pirates to copy DVD content in “raw,” or unencrypted, form. In October 1999, source code for circumventing this technology, known as deCSS, was released by a group of Norwegian hackers, giving DVD pirates an elegant work-around for defeating CSS. The movie industry asserted that the act of releasing, using, or sharing the deCSS source code was a violation of the DMCA, but doing so did little to prevent consumption of deCSS by the piracy community where recipients cared little that they were in violation of the DMCA, as they intended to break the law anyway. Since then the motion picture industry has funded development of stronger DRM products to directly prevent the unlawful copying of DVDs; examples include the Advanced Access Content System, which claims to allow authorized copies of digital media to be produced while preventing unauthorized copies, and Self-Protecting Digital Content, which offers renewable security as an alternative to revoking players when security vulnerabilities are discovered. This dramatic shift illustrates a budding awareness that concrete piracy-prevention methods are necessary where reliance on the law alone as a deterrent has proved itself ineffective.

Though the DMCA is the best-known legal pillar, circumventing anti-piracy measures is not the only area of law being used as a scapegoat. In 2005, students at The Johns Hopkins University showed that some vehicle immobilizers and the ExxonMobile Speedpass payment system utilizing cryptographically enabled RFID chips are susceptible to cloning attacks that allow thieves to make working copies of each device. A thief could, for example, duplicate car keys with little effort or make fraudulent purchases billed directly to a victim’s credit card. Both systems relied on a secret encryption algorithm developed by Texas Instruments that, once discovered, allows easy and inexpensive replication of these RFID devices.

Aside from committing the security of the entire system to the secrecy of the encryption algorithm (security through obscurity), upon its disclosure numerous arguments have been made suggesting it is still illegal to create or obtain key-cloning devices that use the Texas Instruments’ algorithm, and copyright and patent legislation make it cumbersome to develop commercially available equipment to do so. True as it may be that there are legal and cost hurdles to overcome before commercial cloning kits are available, these hurdles are orthogonal to the minimal legal and

economic barriers criminals face in producing such equipment on their own, as disregard for the law is already the norm.

In some cases, rules and regulations have the adverse effect of limiting public investigation and research into the security designs of some products. Massively deployed RFID-based toll-collection systems (such as EZ-Pass in North America) have enormous potential for security and privacy violations associated with tracking and correlating groups of people. These systems employ minimal (if any) security features; empirically exploring the depth of security and privacy concerns associated with them would benefit the industry, as well as the public. However, U.S. Federal Communications Commission regulations prevent the use of uncertified equipment operating in the appropriate frequency ranges at an acceptable power level. The cost of performing such a test is small, but the bureaucratic and cost hurdles of legally doing so make such experiments unreasonable for anyone wishing to operate within the law. However, it is likely that criminals would be able to design, build, and maintain the necessary equipment to launch attacks to an extent that is not yet known.

The law has always given the industrialized world the ability to prosecute criminals and in some cases yielded strong deterrents, but even the most aggressive ones cannot prevent a crime. System designers should never assume security through legality and instead take all necessary steps toward preventing any possible attack, legal or otherwise, against the system.

Misunderstanding the adversary and relying on the law as a crutch has yielded ineffective and damaging results. To avoid such mistakes in the future, today’s security system designers must be educated to think more like the adversary and understand the fault in assuming the adversary would be dissuaded by the unlawfulness of launching an attack. ■

STEPHEN BONO (sbono@securityevaluators.com) is a senior security analyst at Independent Security Evaluators, Baltimore, MD.

AVIEL RUBIN (rubin@securityevaluators.com) is president of Independent Security Evaluators and a professor of computer science at The Johns Hopkins University, Baltimore, MD.

ADAM STUBBLEFIELD (astubble@securityevaluators.com) is a senior security analyst at Independent Security Evaluators, Baltimore, MD.

MATTHEW GREEN (mgreen@securityevaluators.com) is a senior security analyst at Independent Security Evaluators, Baltimore, MD.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

© 2006 ACM 0001-0782/06/0600 \$5.00