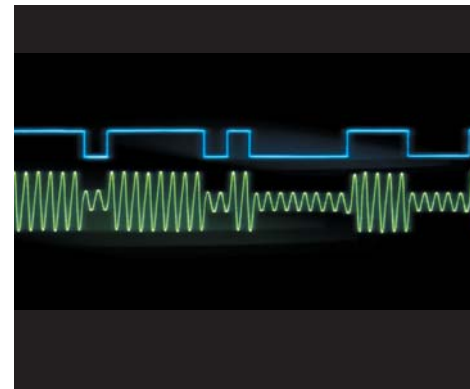


A black rectangular tag with rounded corners, hanging from a black string. The tag has white text that reads "Written by Randy Cronk" and "greatwriting.com".

Written by Randy Cronk
greatwriting.com

Time: the Currency of Computer Crime



WHITE PAPER

Definitions of what is computer crime matter less now that computers permeate everything. What does matter is how criminals and investigators use computer time.

Criminals, victims, and investigators all share one thing when it comes to crime involving computers. Everything that ever took place in a computer happened because a clock ticked. That means that both protection and recovery (technically, legally, and financially) fundamentally require timekeeping that is pervasively and demonstrably accurate.

Why? Because computers are the supreme example of something called “state machines” — i.e., they only change in response to clocks. Think of frames in a movie. Even though motion seems to be continuous, each action actually consists of a series of still shots, each of which synchronizes character action with music, animated effects, subtitles and so on. At any point in the show (or cyber crime) you can inspect a specific time slice and know exactly what happened in the theater (or computer) at that point in time. Email, financial statements, system logs — everything — can be revealed for any point (or series of points) in time. That’s why accurate time indexing has great potential both to deter crime and investigate it. Once events are accurately synchronized, you can essentially “rewind the tape” to see what occurred.

But it only works if the accuracy is both pervasive and demonstrable. Computers interoperate with other computers. What happens if their clocks don’t all agree? Who’s to say which clock is correct or whether time “indexes” — i.e., the time stamps contained in system logs, email, file directories and other items — were not altered after the fact? Only when the relation of events to a single time index can be proven will the potential of time-based computer forensics be realized — making the online world a far more secure place in which to live and work.

Why It Matters

CONSIDER THESE FACTS:

- 93% of all corporate documents re created electronically
- Printed documents comprise only .003% of information worldwide
- 610 billion email messages are sent each year worldwide
- Networked b2b transactions will reach \$2.4 trillion in 2003
- U.S. consumer spending over the Internet will reach \$95 billion in 2003

Digital assets — all of which are indexed by time — are both ubiquitous and valuable. They include everything from financial statements to patient records to proprietary formulas to conversations to online transactions. Moreover, a greater percentage of *all* asset value is now digital — comprising intellectual, as opposed to simply physical, capital. This is value that has not gone unnoticed by criminals. The FBI says that approximately 10,000 cyber crime complaints were filed in 2000 alone of which 273 organizations reported losses totaling over \$265 billion. But reported losses don’t begin to reveal the total picture. Most cyber crime goes unreported and undetected. Besides business interruption costs and system restoration costs there are also legal costs. Take evidentiary discovery. In a world where gigabytes of computer hard drives have replaced file cabinets, suing a perpetrator (or anyone else for that matter) can easily cost hundreds of thousands of dollars in discovery. Then there are the opportunity costs (measured in productivity losses) of keeping information *offline*. That’s one option apparently many hospitals favor in the face of two post-Enron laws imposing strict record keeping requirements: HIPAA (Health Information Portability and Accountability Act) and Sarbanes-Oxley. What many hospitals and other business people are learning is that you don’t have to break into systems to commit a

digital crime. *Not* protecting digital assets can be a crime too — an expensive one.

Here are some examples:

CRIME STORIES

In a pact that could change the face of Wall Street, 10 of the nation’s largest securities firms agreed to pay a record \$1.4 billion to settle government charges involving abuse of investors during the stock-market bubble of the late 1990s. . . . Regulators unveiled dozens of previously undisclosed examples of financial analysts tailoring their research reports and stock ratings to win investment-banking business. . . . The boss of one star analyst, Internet expert Mary Meeker of Morgan Stanley, praised her for being “highly involved” in the firm’s investment-banking business. An analyst at the UBS Warburg unit of UBS AG explained she soft-pedaled concerns against a drug because its developer was a “very important client.”

What is startling about this case is not so much the financial damages (many consider the \$1.4 billion inadequate) but the emails. For example, in his June 2000 email to Netscape founder Marc Andreessen, Joe Perella, head of worldwide investment banking for Morgan Stanley, promises Andreessen favorable analyst coverage in exchange for the IPO business of the company Andreessen was taking public. In another example, Joshua Williams, a Morgan Stanley analyst, tells Michael Blumstein, another Morgan Stanley analyst, not to commit to starting research coverage of Pilgrim’s Pride (the second largest chicken processor in the US) until Pilgrim’s Pride commits to a \$250 million high-yield debt offering that would generate \$3-\$5 million in fees for Morgan Stanley. Morgan Stanley should wait, Williams says, until “the money is in the bank.”

These and dozens of other incriminating emails are available for download from

investigators' and newspaper websites. They are blatant admissions of personal wrongdoing and disregard for investor trust. But these are more than just admissions; in many cases these email exchanges, performance reviews, and other digital artifacts were the actual instruments by which the alleged crimes and conspiracies were carried out. If the Wall Street firms hadn't settled, prosecutors could (and presumably victims' attorneys still can) establish clear timelines of actions and counter actions. There are so many emails with so many time stamps that repudiation of any individual act (or all of them as a whole) is extremely difficult. Had someone decided to backdate an email or two (say, to claim that a certain memo was written before a client became a client), there would have been massive counter evidence — including the time stamps on backup tapes.

Other types of computer crimes involve time more directly. Consider this example from the world of horseracing:

Leaders of thoroughbred racing scrambled yesterday to reassure fans shaken by allegations of tampering on last Saturday's Breeders' Cup wagering. The allegations — that a computer engineer working for a tote company may have electronically altered a bet after the race had been won — could devastate a sport increasingly dependent on fans betting from afar through computers. ... The \$3.1 million payoff to a Baltimore man has been frozen as investigators probe the circumstances of his wager.²

The basis of the scam was to enter — and backdate — bets on races already run. The erroneous bets were entered into computers at off-track locations — where bets were normally stored temporarily prior to upload to the more secure central server. Apparently the system was designed this way to prevent the main computer from being swamped.

Similar crimes have occurred at banks. In one case a programmer for the bank came to work at off-hours, reset the computer's clock to the preceding day, reran that day's transactions, added a credit to his girlfriend's account, debited that amount from dormant accounts belonging to other customers, and then

reset the clock to the correct time and date. The scheme worked for 18 months — until an elderly customer — out of state receiving medical care — came home and tried to make her first withdrawal in over a year.

The Wall Street example shows how time indexing computer events can help *prove* crime. The horse racing and bank examples show how (false) time indexing is a crime (or at least part of one). Then there are instances where the *absence* of time indexing can expose one to penalties, both criminal and civil, and substantial financial liabilities. Sarbanes-Oxley (2002), for example, says that:

- A corporation must maintain audit related records for seven years
- A CEO must attest to the effectiveness of internal controls for financial reporting
- Companies must report changes in their financial condition "in real time"

HIPAA (2002) says hospitals, doctor's offices, and other "covered entities":

... engaged in the electronic maintenance or transmission of health information pertaining to individuals assess potential risks and vulnerabilities to such information in its possession in electronic form, and develop, implement, and maintain appropriate security measures to protect that information. Importantly, these measures would be required to be documented and kept current.

Currency is a continuing theme in these laws. Companies must demonstrate currency (as in pervasively accurate time indexing) in the control of their digital assets.

While Sarbanes-Oxley and HIPAA do not spell out compliance measures in detail, experts like Lew Wagner, chief information security officer at the M.D. Anderson Cancer Center at the University of Texas in Houston, say that "any organization should be able to show who has access to its systems, what measures control and monitor that access, what accountability exists for actions within the systems — and how systems violations of unauthorized access are detected and responded to."³

What happens if an organization doesn't

do this? The consequences can be up to 20 years in jail, say information legal consultants Alan E. Brill and Kristin M. Nimsger.⁴ That's if you knowingly destroy files relating to a federal investigation or bankruptcy filing. If you delete emails and other documents related to other kinds of court actions, you could also face jail time and court sanctions in the thousands of dollars. Even if the mistakes were due to sloppy controls, you could still be found guilty — and the sloppier the record keeping, the more expensive the legal process will be, whether or not you end up also paying damages or fines.

How Can Organizations Protect Themselves?

Clock ticks make events happen in computers. It is therefore impossible to create, alter, steal, or destroy a digital asset without leaving a time trail somewhere. No other method of asset tagging (whether for control or forensics) is potentially so universal or absolute. The only questions are whether the tag is accessible and whether it can be trusted. As recent events have shown, sometimes people alter time to commit crimes or to cover them up. Another issue: time indexes rarely agree. Creating an accurate timeline reflecting a sequence of events occurring on multiple systems is harder if clocks don't agree — effectively creating multiple time indexes, even though at any instant there can only be one correct time.

Organizations can use time at two levels to solve control and forensics issues:

- The accurate time stamping of events (**Requirement #1**)
- The synchronizing of events to an accurate clock (**Requirement #2**)

Requirement #1 is satisfied if events *in the past* actually happened at the instant they are alleged to have happened. A *trusted time stamp* on a digital asset (an email, a contract, a log file, or whatever) reflects three qualities: *accuracy* — the time stamp can be shown to be correct at the time of application; *integrity* — that the copy of the asset containing the time stamp hasn't been altered after the fact, and *binding* — that the asset and time stamp are inextricably linked. In

other words, a trusted time stamp is irrefutable proof as to the state of the asset at a point in time. You can, for example, prove the content of an email when it was sent, the event captured by a specific system log entry, the content of an online order, the timely filing of a financial statement, when a tape backup was made — or the *content* and *time* of any digital event. The forensic and legal value of such proof is obvious. Any digital asset can be identified with an irrefutable evidence tag at any stage in its lifecycle.

Requirement #2 is satisfied if events happen at the instant they are *intended* to happen — i.e., they are *synchronized* to an accurate time index. This means events will occur in the proper sequence and at the proper intervals in relation to other events, even if those occur in multiple locations. Satisfy Requirement #2 and the tasks for which you employ computers (including the task of safeguarding digital assets) will likely occur as planned. Backups will happen on schedule; financial notices will be emailed on time; erroneous system log entries will be harder to accomplish and easier to spot; and protective measures involving networked systems — like security monitors and firewalls — will more likely operate properly. Moreover — for purposes of Sarbanes-Oxley and HIPAA — it will be easier to demonstrate that adequate security measures are in place.

Technically, trusted time stamping and synchronization also have different requirements — even though both ultimately depend on access to an accurate and secure time source.

For trusted time stamping, that access is over a PKI (public key infrastructure). The PKI connects a *time stamp server* to atomic clocks audited and certified by national time authorities (like NIST in the US). The time stamp server signs the time directly into digital assets (for example, email), which it receives from applications (such as email servers). The signing is done with an encryption key. If either the time stamp or the asset to which the time stamp was applied is altered, the signature will not decrypt.

For synchronization, a *secure timeserver* receives time from NIST via public carriers instead of over a dedicated PKI. Public carriers include GPS satellites, which are considered to be highly reliable sources of time. Not only are the satellites located in outer space, making physical tampering virtually impossible, their timing signals are the basis for tracking virtually all modern commerce, whether by sea or land. The secure timeserver then distributes this time via an encrypted channel to computers on its network — so that all clocks on the network are synchronized to the correct time and therefore to each other.

Crime Stoppers

Where crime is concerned, trusted time stamping and secure synchronization each confer benefits that complement the other. Trusted time stamping is obviously a great forensic tool. However, proving an event happened at a point in time may not be enough, *if the event happened at the wrong time* (and damage is already done). Moreover, secure synchronization also has significant forensic value in its own right. It is not practical to time stamp every digital event or asset in a trusted manner (i.e., with demonstrable accuracy, integrity and binding). Where time stamps are missing, network synchronization can nevertheless substantially speed up criminal investigations. In a synchronized environment, for example, investigators might not have to go through the preparatory chore of manually synchronizing multiple computer clocks in order to timeline a crime.

By the same token, trusted time stamping also provides value in crime prevention, even in the absence of synchronization. One reason is simple deterrence. If time stamping practices are widely communicated, then potential criminals will think twice before they attempt a cyber break-in, backdate a document, or reset a system clock. Another reason is that time stamping can authenticate the fact that other security systems are working properly (or were at the time of a crime). Take digital signatures. Time stamping certificates in digital signature systems ensures that the certificates used to val-

idate these signatures have not expired (hence, the signatures themselves are not suspect). A similar case can be made for firewalls, facility access control systems, video surveillance monitors, and any other system that relies on accurate time indexes. Records from these systems can be time stamped to show the systems are operating and that security events are being detected.

Ideally, most organizations would want both — trusted time stamping *and* secure synchronization. It's not just that more is better (although that is often the case when confronting criminals). Different kinds of cyber crimes lend themselves to different security and investigative techniques — and often to mixed approaches. Consider recovery of digital evidence. The US Department of Justice says that:

Although every computer search is unique, search strategies often depend on the role of the hardware in the offense. If the hardware is itself evidence, an instrumentality, contraband, or a fruit of a crime, agents will usually plan to seize the hardware and search its contents off-site. If the hardware is merely a storage device for evidence, agents generally will only seize the hardware if less disruptive alternatives are not feasible.⁵

In deciding on evidence recovery measures, the DOJ says the relevant distinction is between two types of crime:

Type 1: "Regular" crime where digital technology is incidental to the crime; and

Type 2: "Cyber" crime where digital technology is part of what the crime is about

In the first category belong the new white-collar criminals, like those who use computers to mislead investors — crooks who probably don't think of themselves as criminals and certainly not cyber criminals. Thanks to laws like Sarbanes-Oxley, many of them will now join the ranks of crooks that use computers to do the kinds of things criminals have always done:

The mafia uses computers for extortion. Drug dealers enlist an encrypted fax machine to send orders for narcotics to their suppliers in Columbia. Prostitution

*rings maintain their customer payments and client lists through computer software applications. Burglary rings [use computers to] track break-ins and then inventory their winnings from each job.*⁴

In the second category belongs the conventional cyber hacker — the techies who steal money from unsuspecting bank customers, change the bets on horse races already run, or commit industrial espionage via the Internet.

Time-Active Versus Time-Passive

So how does time play into the DOJ distinction? More importantly, is time a useful basis on which to create crime prevention and investigation strategies? Let's start with trusted time stamps. In "regular" crime, investigators might rely on trusted time stamps on incriminating documents — they wouldn't necessarily confiscate the physical hard drive to prove a case. Time stamps might be downloaded from the criminal's computer — say, if he or she worked for an organization that used trusted time stamping as a crime deterrent. Those time stamps might also be available on computers wherever the criminal sent the documents — making a physical examination of the criminal's computer even less necessary. Thirdly, an investigator might apply time stamps during evidence gathering — for example, to prove that such-and-such a file existed at a certain time, thus establishing a chain of custody.

But what about "cyber" crimes, for which the crook's computer is considered the "instrumentality of the crime"? Could time stamps help here too? Probably, depending on circumstances. Suppose criminals surreptitiously alter financial transaction records (say, to remove money from bank accounts or place wagers on races already run) — and then rewrite time stamps and reset system clocks to cover their tracks. If those were trusted time stamps, then by definition they could not be altered. So investigators could make a case *without* confiscating the computer — even though the computer was very much part of the crime.

Crimes in which confiscation would be more likely would those where time stamps could not be relied on. Financial transaction records and emails may be time stamped — but what about system logs, firewall intrusion histories, and web server event logs — and dozens of time-indexes (logs and clocks) that might reveal crime? Here, investigators would more likely rely upon the time tracking mechanisms of the computer itself. They would need detailed forensics to establish a crime timeline and to establish a chain of custody once forensics were in hand. Investigators might want to look at:

- System logs (e.g., file creation/modification dates)
- Time keeping and time tracking mechanisms (i.e., how the computer tells time)
- Application repositories (e.g., email exchange servers)
- Security monitors (e.g., firewall history logs)

When looking at evidence, investigators would want to know:

- How accurate were the clocks?
- How consistent were clocks to each other and to external time sources?
- How reliable were the time sources for these clocks?
- How secure were the time sources from tampering?

The environment in which this type of close physical examination would be most effective is clear. Secure synchronization would offer, by definition, time that is the most *pervasively* accurate, consistent, reliable and secure. To succeed in that environment, a criminal would have to know: a) every single place a record might be kept that could reveal surreptitious access or tampering, and b) how to alter each of those records so as not to create inconsistencies with other records, all of which are consistent with each other and with a known good time source. In that environment, criminal activity is both easier to investigate and prevent.

The decision to confiscate is only one of many that can be based on the type of crime — depending on how *time* is used

— and not just when investigating crime, but also when preventing it. In that light, the DOJ guidelines might be restated as follows: *Although every computer crime is unique, protective and forensic strategies depend on the role of time in the offense.*

The more aggressive the criminal with respect to time — e.g., by backdating emails or resetting systems clocks — the more active the counter measures required to block or investigate the crime. This time-passive versus time-active distinction is a better litmus test of how to respond than the "regular" versus "cyber" distinction. How, for example, should the defendants involved in the SEC settlement of April 2003 be classified?

Even though these people weren't hackers, their computers were nonetheless used for more than just storing information *about* their alleged crime. According to the SEC, the emails *were* the crime. Does that mean the Wall Street types would be investigated with the same techniques as, say, a cyber bank robber? Probably not. Both crimes involved putting false information into computers. In one case that false information included time; in the other it did not. Were active time manipulation involved, the more aggressive "hands on" approach of physical confiscation would no doubt be employed. •

What makes most "regular" crimes regular is that they tend to be time-passive. Most Wall Street felons, for example, do not intentionally manipulate time to commit their crimes or mislead investigators. (It is one of the qualities they typically share with the mafia, the drug cartels, and the prostitution rings.) Nor is the time-active nature of many "cyber" crimes apparent. Take identity theft. Not all perpetrators of that crime bother to rewrite system log files or compromise timekeeping mechanisms to gain system entry (although many do). Nevertheless, time plays a very active role in the crime — because the perpetrator must overcome several time-based tripwires to do the crime and avoid exposure risk. Those tripwires include security-monitoring systems, firewalls, and system event logs (like

those that show when assets were accessed or modified). That's why preventing and investigating identity theft (and other time-active crimes) usually involves a heavy dose of both trusted time stamp technology *and* secure synchronization.

Wanted: A Comprehensive Computer Time Policy

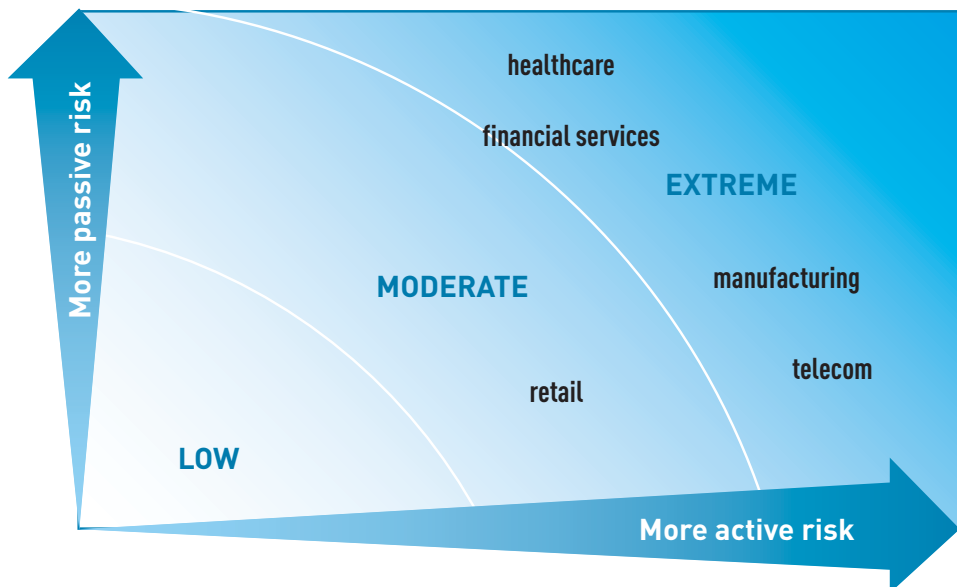
Prevention and investigation of computer crime are two sides of the same coin — and policy. An environment in which trusted time stamping is in place will both deter crime and help solve crime once it occurs. The same applies for secure synchronization. Having defensive tripwires tied to secure, accurate and reliable time sources means that those tripwires will more likely operate when called upon to do so — which means they are more likely to catch criminals either in the act or shortly afterwards.

Monitoring systems are ideal against time-active criminals — for example, to track hacker probes preceding a denial of service attack on a web server. And trusted time stamps are ideal against the time-passive crimes — for example to deter fraudulent or sloppy record keeping. The key is recognizing that different organizations face a different mix of threat levels from a different mix of criminals (and civil liabilities). Those risks carry high costs. Each organization therefore needs to assess its own potential and likelihood of exposure and invest accordingly.

Figure-1 illustrates the two dimensions of time-passive versus time-active threats. One point stands out immediately: an extreme time-passive threat is still an extreme threat — nor is it exclusive of time-active threats. Just because it is time-passive doesn't reduce the threat level; it just makes it very different from a higher time-active threat.

hold hospitals criminally accountable for the integrity and security of patient records. As previously mentioned, HIPAA also holds hospitals accountable for monitoring system incursions. Even so, few hospitals face the type of time-active attacks that telecom providers do, many of which face almost daily hacker assaults to their servers. Telecoms are cited in the high-active/low-passive region. Like hospitals, telecom providers also care about the integrity of their customers' records — it's just that no customer will likely ever die from a telecom record keeping mistake.

What matters is that different organizations formulate different time policies reflecting their different risk profiles. The healthcare provider might want to implement more intensive secure time stamping of patient charts, MRI scans, diagnostic results, and emails. The telecom provider might wish to more thoroughly synchronize time indexing throughout its infrastructure of server farms, routers, firewalls, and customer service applications.



Passive risk = using computers to commit crimes without deliberately manipulating time (e.g., computer clocks or e-mail dates). Examples: securities fraud, inventorying stolen merchandise.

Active risk = manipulating time to commit or hide a crime. Examples: identity theft, network sabotage.

Figure 1: Different organizations face different levels and kinds of risk from crime. Wanted: a computer time policy that applies the right mix of counter strategies.

That said, it's nevertheless true that different threats require a different mix of responses. Securely synchronized moni-

Healthcare, for example, is cited in the high-passive/moderately-active region. That corresponds to HIPAA rules that

Conclusion — Do the Time

Distinctions between what does and does not count as computer crime probably make little sense in modern life, where computers are part of everything. Laws like HIPAA and Sarbanes-Oxley, and recent securities fraud cases underline this fact. Actions that once would have passed under the radar are now vigorously prosecuted. Without computers these acts would not have been considered criminal, they could not have been detected, or they could not have been done in the first place. Not only have computers become part of society's fabric — they've become part of the legal fabric as well, with impact on discovery, chain of custody, and timely disclosure. In fact, it has become almost impossible to contemplate crime outside the realm of information technology in some form.

What makes more sense is recognizing that computers — like movies — time index everything — including crime. Law enforcement and potential crime victims might therefore wish to consider how to employ time to their best advantage.

One distinction that is valid is how criminals themselves employ time. A crime that involves the manipulation of time is usually different from one that does not. When it does, the criminal artifacts are usually the resources needed to run the IT infrastructure itself. When it does not, the criminal artifacts are usually the files intended for consumption by users of that infrastructure. In the first case, the emphasis for protection and investigation is secure synchronization of IT resources. In the second case, the emphasis is on the trusted time stamping of files.

Ultimately, computer crime is not about either computers or files. It's about the organization's reputation, potential criminal and civil liabilities, and the costs of the legal process itself. For victims, it's also about the cost of recovery, where recovery is even possible. Organizations should protect themselves from crime the best way they can. They should implement a comprehensive policy that reflects the reality of their risks and the absolute reliability of time.

¹ "Wall Street Firms Settle Charges Over Research in \$1.4 Billion Pact," *The Wall Street Journal*, April 29, 2003.

² "Avoiding spill of faith is goal in bet scandal," *Baltimore Sun*, 11/2/02.

³ "Data security measures failing to match legal expectations," Jaikumar Vijayan, *Computerworld*, 4/28/03

⁴ "Data destruction: What they can't find can get you 20 years," Alan E. Brill and Kristin M. Nimsger, *Computerworld*, 2/5/03.

⁵ Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice, 7/02.

⁶ "Investigators Focus on Foiling Cybercriminals," *Illena Armstrong*, SC Magazine, 4/00.



SYMMETRICOM, INC.
2300 Orchard Parkway
San Jose, California
95131-1017
tel: 408.433.0910
fax: 408.428.7896
info@symmetricom.com
www.symmetricom.com

©2003 Symmetricom. Symmetricom and the Symmetricom logo are registered trademarks of Symmetricom, Inc. All specifications subject to change without notice. DS/CS4000/D/0703/500