Sjemenarstvo 17(2000)3-4

UDK: 378.663(045)=020
Izvorni znanstveni rad

NEW APPROACH TO THE INFORMATION SECURITY

V. GRBAVAC[1] and K. ANTOLIŠ[2]

[1] Agronomski fakultet Sveučilišta u Zagrebu
Faculty of Agriculture University of Zagreb

[2] Hrvatsko komunikološko društvo
Croatian Communication Association

SUMMARY

Overall, near-term prospects favor greater information security. True, closed systems are continuing to open up and the number of opportunities for waging computer warfare continues to rise. Yet, protection tools are becoming better, the Internet is likely to become more secure, the costs of backup and redundancy are likely to fall sharply, and cryptographic methods are likely to spread. The old model of information security is hard and closed: users, processes, and code are either licit or illicit. The new model of information security which is inaugurated in tihs paper is open and fuzzy.

INTRODUCTION

To illustrate the future of information security, imagine me giving you a piece of information, to wit, that the interests of your employers, the nation's security, and world peace would be greatly advanced if you were to, literally, take a long walk off a short pier. Few of you are likely to do that - even though I have conveyed a piece of information to a set of very complex information-processing systems, that is, you, the reader.

The basic reasons are obvious: I have no authority to make you do anything, the act suggested is something no sane person would do, and there is little if anything I can say that will make you insane. In a nutshell one can recognize the three primary methods by which, information systems are protected: authorization message filtration, and ensuring the integrity of core processes - or to put it more in terms of today's tools: good passwords, firewalls, and virus detectors.

However, imagine me as an internationally recognized expert in information warfare asserting that the threat of information warfare would be to the 21st century what the threat of nuclear warfare was to the latter half of the 20th century. To my mind this is still lunacy, albeit a more subtle one, but it is a proposition which some people would be more inclined to accept - indeed,

many act as though they do. This piece of information does not get blocked by the obvious filters. But, it too, is potentially dangerous.

There, in a nutshell is the message. As computers become smarter, more sophisticated, and more flexible, they will become more like us. That is, they will acquire the reliable information security provisions that all of us carry around as our basic make-up. Yet, as they become more like us, they will begin to ingest information at the semantic level from outside sources as we do (as in fact, you are doing now), and will thus be heir to more subtle but no less problematic forms of information warfare. Or, to put it simply: today's problems will pass and tomorrow's will rise - I just cannot say exactly when either will occur or how quickly. What I can try to do is lay out some indicators and warnings of each.

It is important to note that forecasts about information security are inevitably forecasts about information systems themselves. A large part of what makes information systems open to attack is that they contain bugs, often and pertinently referred to as undocumented features. The more experience one has with any one piece of software the more holes can be closed. Yet, even a perfect fix lasts only until the next innovation hits the system. To give an example: it used to be one could open up any E-mail without worrying about what it might do to your system. But, over time, E-mail has come to contain attachments; attachments often come with activatable macros, and macros, in turn, may carry viruses. This is a problem that simply did not exist several years ago. In years to come, one might make similar statements for objects over networks, ActiveX files, and others in that menagerie. As such, the art of forecasting tomorrow's troubles is intimately related with the art of forecasting tomorrow's pointless wonders.

KEY TRENDS

Let's start off by looking at some of the key factors that influence the current level of information security: legacy systems, the threat, consciousness of the threat, operating systems, security tools, the cost of storage, the Internet, and cryptographic methods. This examination is offered with the caveat, of course, the current state is a matter of serious dispute. Not every system fault is the result of a hacker; but some are. Many such faults go unnoticed. And, a record of what is, is an indicator, but only an indicator of what could be.

Legacy Systems

In the old days, information systems were relatively secure by virtue of being hosted on large proprietary machines and connected to very little. What makes systems vulnerable is the shift to smaller and far more open systems (not built with security in mind) coupled with the rise of networking. For many of us, small open networked systems are the here and now; for others, however,

they are still in the future. Sometimes it takes a situation like the Y2K bug to remind us that while the leading edge of technology races ahead, the lagging tail may be long and thick. As people move away from closed proprietary systems, they will expose themselves to more security risk, especially in the process control sectors. For this reason, but perhaps only for this reason, one may see a decline in the average level of information security over the next few years.

Threat

It is extremely difficult to know what the threat to information systems actually is, and thus all the harder to know in what direction it is going. In terms of actual day-to-day threat, information warfare has remained distinctly unimpressive. Most computer crimes are internal affairs, and most external computer crimes arise, not from systematic attack, but by small groups, or, more likely, random malevolence and even curiosity run amok. Is the relatively benign past a predicator of a relatively benign future? For example, when the United States had one big enemy, no one could cogently argue that the lack of a nuclear strike yesterday meant that the threat was gone. But today, the United States faces, not one dragon holding its fire until the right moment, but a profusion of snakes each with their own agenda and motivations. Thus, the question - why haven't we seen something big already - deserves an answer. That is, if somebody has not done something already, what makes one sure that anyone can do anything? Conversely, America was, by contrast to Europe, considered immune to the more conventional sorts of terrorism. After the World Trade Center bombing took place, that idea vanished.

In a sense, the threat by foreigners to U.S. information systems is a lagging indicator just as the conversion of legacy systems is. The Russians and the Chinese appear to be very interested in computer warfare - at least if their published writings are at all indicative. This makes sense; if one wishes to hold off the world's superpower, and if information systems lie at the core of what makes the superpower super, then that's the place to attack. That said, the Russians and Chinese seem to be more interested in the possibilities of unleashing destructive viruses then they are in the world of day-to-day computer intrusion. This bias may exist because they lack many open computer networks upon which to practice their intrusive arts - but a virus can be tested on a stand-alone machine.

Will others grow interested in computer warfare? FFor example, America is a trendy place and information warfare is a trendy subject. They, who are drenched in silicon, will spin therselves up on this threat well before others catch on - notably those others who live in lands unblessed by much computer equipment for instance Croatia and who thus lack an intuitive sense for their place in a modern world. True, all nations, even poor ones, have some hackers; but without a broad infusion of computer-consciousness within the top

leadership, the resources required to build hacker cadres and the wit required to put this approach on a list of serious attack options is unlikely. Most enemies of the country on high degree of development, live in places where systems are rare. That said, the entire world is becoming wired. If information warfare is a popular meme within the Department of Defense, the awe with which DOD is held worldwide cannot help but make it a popular meme everywhere else as well. Hollywood, is of course doing its part; more often than not the cinematic proof that someone is brilliant is provided by their being able to get into systems that they were otherwise barred from. Thus the option of information warfare is likely to rise on the agenda over time. Here too, the averages are affected as much by changes in the lagging edge as by changes in the leading edge.

Trends in lower-level threats such as crime or terrorism are harder to assess. In general, criminal enterprise tends to be responsive to opportunity with very little lag and thus a lurch upwards in the direction of computer crime seems unlikely; at worst, a gradually rising level can be expected. As for terrorism, the world's disaffected tend not to be the more computer-sophisticated and are likely to prefer violent means for the time being. Furthermore there is a great difference between five terrorist groups taking faux credit for an obvious act of terror (e.g., a car bomb) and the same folks taking credit for some glitch (e.g., a telephone outage) which may equally well be an act of nature, human error, design flaw, or the result of hostile activity.

Consciousness

The flip side of trying to gauge the changing threat is trying to gauge whether people are going to start taking computer security more seriously or not. The two are, of course, related; the greater the threat, the more likely people will take security seriousness; no threat, less response. What other indicators should one look at? One indicator may be how people respond to the Year 2000 problem. Assume the problem is as serious as people think, that many systems owners respond late, poorly, or not at all, that consequent damage results, and that lawsuits start to fly. What kind of echoes will this cause? Will systems owners be held liable for damages to third-parties due to software negligence? What standard for due diligence will result? Will users learn to be wary of anything a computer produces (thus reinforcing the need to keep wetware in the loop)? And, of course, will people take the same view of a system owner's inability to keep intruders out as they might for their fecklessness in dealing with the inevitable transition from the year 1999 to the year 2000? Wild cards may make a difference. Say a major earthquake hits California leading to the failure of institutions that have failed to back up their data several hundred miles away. Will people pay more attention to redundancy and back-ups as a result? Indeed, any publicized systems failure is likely to heighten people's awareness of unnatural risks as well.

Operating Systems

Most of the more serious weaknesses in computer systems lie with the operating system itself. It may be unfair but indicative that Unix assumed its current features at the University of California in the late 1970s, a time in its academic history that may be described by many adjectives, of which "security" is probably not one. In part because of its academic legacy people have been working on Unix security, in many ways, harder than they do for any other operating system. Over time, therefore, absent major changes, one might expect Unix to get more secure.

Indeed, one might have imagined that Windows NT, which is based on Digital's VMS (a fairly secure system to begin with), plus another twenty years to reflect on information warfare, would be highly secure. Strangely enough, current versions are less secure than Unix and have bugs all their own. The computer industry seems, lately, to put more value on slick features than steady performance. At some point, economies of scale must set in, the n^{th} added feature will not be terribly exciting, and computer makers will settle down to engineering greater reliability into what they sell. But don't ask me when.

In the meantime, the Web has become the focus of the computer industry's developments. In some cases, especially electronic commerce, people are paying serious attention to security. But the glitzy end of the Web business - Java, ActiveX (which is worse), automatic software updates, and the various plug-ins - are all carriers of great mischief from the unscrupulous.

Security Tools

Current trends in information security treat it is a problem that can be solved by adding a patch here and there. Firewalls go on the outside of one's system and are meant to filter out certain types of messages by looking at each packet and making a determination based on their ostensible purpose (which can often be revealed by their port number). Intrusion detectors look for particular activities which are characteristic of known fault patterns and then take appropriate action (e.g., alert administrators, withdraw user privileges, note what systems or numbers the intruder is coming in from). Neither firewalls nor intrusion detectors are altogether reliable today, but they are getting better against a given level of threat. It is unclear whether they might go too far and make it possible for foes to instigate an anaphylactic attack, one which, using the immune system metaphor, works by overstimulating and thus setting a system's internal defensive mechanisms against itself.

The Cost of Storage

As the price of computer storage falls, the feasibility of archiving everything rises to the point where no one has a credible excuse for losing information

(although finding archived information after the crash will take work). To give an example, the 17-gigabyte DVD (digital versatile disk) of the year 2000 has enough capacity to store the complete billing records of a week's worth of long-distance calls made in the United States. In sensitive environments, very fast CD-ROMs (or any other non-volatile memory) may replace writable hard disks for storing operating systems – there by giving viruses nowhere to rest. CD-ROMs operating with zero buffer can also log everything that happens to a computer without some hacker going back and writing over the record.

The Internet

The evolution of the Internet, itself, will shape the near-term information security environment. The next version of the Internet Protocol, IPv6, has provisions for many security features such as encryption, key passing, and digital signatures. Eventually IPv6 will be universal, but deployment remains slow; the greatest penetration is occurring within specific circles of universities and other leading edge sites.

Several features of the Internet make it particularly attractive for hackers. What should only be a near-term problem is that the Domain Naming Service, which translates names (e.g., www.ndu.edu) into byte-addresses is poorly protected and has little authentication capacity. Chances are the former will be fixed, and, it may also be possible to authenticate the true source of any message coming into one's system in most cases.

A more permanent feature of the Internet is that it lacks a packet-level billing system. This makes broad flooding attacks possible and makes more focussed attacks very hard to trace back to their source. However, unless the free-packet structure of the Internet proves to be its undoing, the prospects for packet-level billing are modest.

Cryptographic Methods

Cryptographic methods remain the most obvious tool for information security. As hardware gets faster, the processing load for encryption and authenticating messages can be expected to decline. This is obviously true if the key length stays the same, and almost as certain if measured as the time it takes to encrypt a message which takes a fixed X hours decrypt (as supercomputers get better, the required key length rises). Thus, everything else being equal, cryptographic methods will see greater use, and information security will rise.

Needless to say, everything else is not equal in this field, and there are important policy and technology questions that must be factored in. The first policy question, of course, is when - not whether, but when – for instance, the U.S. federal government will give up trying to control encryption. One must admire the control effort both for its doggedness and cleverness, but in the end,

it can only delay the inevitability of technology. One may debate the merits of key escrow forever, but there is no denying that industry does not find the federal government helpful, and, indeed, is preparing to spend several million dollars saying as much in the public media. In the meantime, however, federal policy is confusing the market for encryption (perhaps deliberately so) and thus delaying its use as a way to defend information infrastructures.

The confusion in cryptography is not doing any favors for the digital signature market. The federal government built a digital signature standard around a technology, that has a non-trivial side-benefit; it cannot be reverse engineered into a public key encryption system. The market seems to prefer RSA's private standard. Compared to encryption, the level of federal resistance to digital signatures is far less and parts of the federal government are, in fact, working hard to encourage its use. The immediate requirement, particularly for electronic commerce, is greater, and thus digital signatures are likely to proliferate. A real spur to its use may come if and when people exploit digital signatures as a apply-once use-forever stamp to documents. For instance, college graduates may get a signed and dated bitstream of their grades that they could give to anyone; recipients could verify its authenticity by computer.

Technology remains the wild-card behind any forecasts of encryption's use. Innovations such as elliptical methods or cryptographic analysis will affect the time required to generate or break codes. Yet, very little in the last fifteen years has broken the fundamental fact that increases in key length have a modest affect on the cost of making codes and a major affect on the cost of breaking them. The one joker in the deck is the prospect of quantum computing which can break the back of the prime factoring problem thereby rendering both public key encryption and digital signatures obsolete. But no one knows whether quantum computers will work.

POTENTIAL BENDS

At this point, I want to explore the second half of the future: the prospect that while the long-term information security environment is likely to become better in obvious ways, it is likely to worsen in subtle ways. The key to understanding this phenomenon lies with how tomorrow's information systems are going to be used.

As noted earlier, the increasing power of hardware and the growing sophistication of software suggests a future in which silicon starts to act more like carbon: that is, computers take on more characteristics of humans while networks take on more characteristics of human organizations.

Tomorrow's information systems are likely to make, or at least set the table for, more judgements than today's do. What is more, the feedstock for these judgements are likely to be information harvested from the world out there. Such applications are likely to appear among institutions that depend on

reacting to an outside environment: e.g., politico-military intelligence, business sales-and-marketing, environmental control, or broad-scale social service functions such as law enforcement, traffic regulation, or public health. Institutions that do not react with the outside directly but may learn from external experience may develop some links with the outside world. Process control applications may never have these links, at least not directly. Yet, even process control applications may not be immune to influence. For instance, a toy company may have its agents cruise the Web in search of data to help them predict the hot trend for next Christmas. The results of its search will change what it makes, thus its production mix, and thus how it schedules and supplies its production lines - a classic process control application.

Today, computers process information using tight algorithmic logic from a carefully controlled set of inputs - the way they are supposed to. Tomorrow, computers may use techniques of logic processing, or neural network technologies to sift through a trusted set of material and bring things up to human attention. The day after, so to speak, computers may reach and present conclusions based on material of widely varying reliability. Thus a military intelligence system may evaluate the relative security of a village through a combination of authenticated overhead imagery, an analysis of potentially spoofable telephone switch activity and overnight police reports, and the collective detritus of written gossip from electronic community bulletin boards. A traffic controller may set stop-lights based on monitored traffic flows, plus a forecast of the kind of traffic loads selected large events may generate based on what their organizers predict. A drug company may put out usage advisories to doctors based on combing through data-bases on hospital treatments and outcomes. Individuals may plan their evenings out based on the suggestions of their agents trolling web sites that list entertainment offerings cross-correlated by less formally established "what's-hot" lists.

Needless to add, there will be people who find it worthwhile to corrupt such systems. They may not all be criminals; indeed, many of them would classify themselves as basically honest gamesmen eager to put the best face on the world's data-stream in order to influence the judgements of Web users. Some Web sites are crafted so that their URL appears at the top of search lists generated by automatic tools (e.g., Altavista). It would not be surprising to see the less scrupulous engage in many of the same fraudulent techniques of misrepresentation and lying that today's con artists do. Indeed, for a long time to come, computers will be easier to con than people will. Thus, a flow of false information on patient histories that reflect the efficacy of a licensed drug may subtly shift a system's recommendations to another one (bad reports of which are buried). A series of reports on the flow of loans to an otherwise suspect lender may convince rating agencies to boost its reputation and permit it to garner loans that it otherwise would not deserve (and has no intention of paying back).

Once you have this picture of the future, it does not take much imagination to forecast what else may go wrong. So here goes:

Learning Systems and Neural Net Computing

For the most part, one can determine why a system does what it does by examining its source code to learn what and querying coders to learn why. Tomorrow, that process may not be so easy. Computers may learn from experience. If they use traditional AI, they will build and refine a data base of rules that will govern the logic by which they draw conclusions. If they use neural nets, they will steadily tune their association matrices by using real-world test sets and backward propagation.

All this is well and good - until something goes wrong. If the experience base upon which learning systems or neural nets have been corrupted then their conclusions will be similarly corrupted. Fixing them will be costly. Corruption must be detected, and that may be possible only by observing poor decisions. What if the corrupter alters the input so that the system makes a bad decision only when it encounters a very specific input set? Unless one knows the input set, corruption may be completely masked. Even if the nature of the corruption is determined, when the system was corrupted has to be estimated. Then the system can be reset to its last known uncorrupted state, if one has archived such parameters. Otherwise, the system has to be returned to its original settings, which means losing all the learning that has taken place since it was turned on.

Software Agents

One of the ways integrated open systems work is by letting clients place software agents on servers. These software agents, in effect, query servers, in some cases periodically. Sometimes results go back to the client. In other cases, one agent or a part of an agent may be sent forward to other sites. For instance, a travel agent, so to speak, interested in putting together a meals-lodging-entertainment-and-transportation package may be split into four sub-agents (each of whom then go out looking for the best deals in their area, return candidates, so that the master agent can fit them together).

In theory anything an agent can do may be done by successive queries, but the use of agents saves on message traffic (especially for "tell-me-when" requests) and permits in-server consolidation. Badly designed agents, whether by not-so-benign neglect or malign intent, may cause some servers to cycle forever for an answer, set up a mutually destructive server-to-server harmonic, or may replicate without bounds and clog entire networks. Malevolent agents may look for certain outgoing mail, and then work their way into systems from which it originated. If mischievous enough, such agents could have a chilling effect on free network speech. Indeed, network administrators are already

beginning to understand that bringing a network to its knees does not take many automatic E-mail responders (All it takes is one message sent to at least three individuals on vacation that echo an "I am on vacation" message to everyone on the original mailing list).

Hijacked agents or agents forwarded to successively less trustworthy servers ("a friend of a friend of a friend ...") may relay misleading or dangerous information back. In a sufficiently rich network, replicating agents may be carriers of replicating viruses whose eradication may be fiendishly difficult if there are niches in the network ecosystem that cannot be identified or do not cooperate.

Ecologies

The reference to ecosystems was deliberate. Systems, beyond some point of complexity, and many seemed to have reached that point, become extremely difficult to control in the sense that one can predict the performance of the whole by understanding the performance of each part. Even perfect understanding of components cannot predict all fault modes in a succinct way. Although today's hacking requires active intruders, much of the risk and tedium associated with malicious hacking can be transferred to bots - pieces of code that wander the Net looking for a computer to roost in. A single hacker unleashing a flood of junk to clog a system can be traced and stopped; perhaps even caught. Similar effects, however, may be generated by implanting a virus in thousands of systems. Turning on one or two (e.g., including a key word in otherwise innocent text) can simulate a chain letter on steroids, as each infected system turns on another, with thousands of sites flooding the system, well before their owners know what is going on.

Mother Nature has long ago given up trying to govern complex systems by imposing behaviors on each component. Instead, ecologies carry on from one year to the next through a mix of competition, diverse niches, predator-prey relationships, and, above all, a facility for adaptation and evolution. Tomorrow's networks may need some way to maintain homeostasis by populating themselves with analogous instruments. Needless to add, of course, no one will get the proper combination and distribution of instruments right the first time. It is not much of a leap to see how such instruments may be used by evildoers to bring systems down to the silicon version of extinction, at least temporarily.

New Approach

All this suggests a completely different approach to information security. Consider how complex humans are compared to computers and how they, like computers, network themselves in order to exchange knowledge. Yet, for the most part, it is difficult for humans to pass disabling bitstreams among each other. Few word combinations can cause a rational person to seize up, spin

cycles endlessly, or flood friends and acquaintances with pointless communications. Why? As noted earlier, humans accept inputs at the semantic rather than syntactic level; messages are converted into specific meanings and then processed as such. Information and commands are screened for harmful nonsense.

Yet, as any observer of human affairs can attest, cognition does not prevent certain messages from achieving widespread and deleterious affects. Ideas grip the imagination and spread. Some induce "extraordinarily popular delusions and the madness of crowds" (indeed, "information warfare" is, itself, such a meme). This is where education, notably classical education, comes in. People are trained to externalize and objectivize information and view it as something separate from the self; to examine information critically and thereby avoid the twin hazards of excessive naivety or total cynicism. Rhetoric deals with the proper inference of intentions from statements. Logic deals with generating correct implication therefrom. Language is taught as a precision tool so that information could be passed and understood with clarity. Etiquette governs what people say (and how intrusively) and inculcates propriety so that people keep private information private. Thus can humans interact with others, even strangers, to form functioning organizations and other relationships.

Building such sophistication into silicon will not be easy, both technically and socially. To exchange information requires conformance to shared norms at several levels: of meaning, of intention, of context, and of behavior (e.g., what constitutes a legitimate piece of information). Without shared norms - standards as it were - there is no meaning but only programmed reactions. As long as that is true, it will be difficult to defend information systems from a potentially polluted environment except through mechanisms antithetical to the way we would like to see ourselves be. That is, we will have erected castles, moats, gates, and sympathetic brigands to defend ourselves against cyber highwaymen.

Computers cannot be made consistently more powerful and remain safe if they are not endowed with the power not only to input and output bytes but understand them. But, having taught them to listen and speak we must simultaneously teach them proper manners.

CONCLUSION

The moral to the story will be, if not familiar, then at least recognizable. The old model of information security is hard and closed: users, processes, and code are either licit or illicit. There is no grey area. The trick is to differentiate between the two, give the former just enough liberty to do their job, and close the system off to the rest. This model is not entirely bad; indeed, one ought not to run a military C2 net, nuclear power plant, air traffic control system, telephone switch, or funds transfer system any other way. The new model of

information security is open and fuzzy. It is necessarily that way because the systems that we want to both exploit and protect must be open to the outside world and learn from it. One therefore needs a security model that recognizes that fact and makes continual judgements over the validity and reliability of information it ingests. All of this presumes, of course, that the core functions are lock-tight, and that, in turn, requires that the architecture of what must be protected is both simple and transparent. Ironically, that is key to letting systems deal with ambient complexity and opacity. The first challenge ought to be simple; regretfully we have made it complicated, but, one hopes, not too complicated, thereby leaving us with the really fun complex security problems of the future.

NOVI PRISTUP INFORMACIJSKOJ SIGURNOSTI

SAŽETAK

U bliskoj budućnosti očekuje nas veća sigurnost na području informacija. Istina je da se dosad zatvoreni sustavi otvaraju i da se prilike za "upade" i sukobe na informatičkoj razini povećavaju. Međutim, zaštitni programi postaju sve učinkovitiji. Internet će vjerojatno postati sigurniji, troškovi za pohranu i potporne sustave će vjerojatno pasti, dok će se kriptografija proširiti i razviti. Stari model zaštite informacija je tvrd i zatvoren: korisnici, procesi i programi su istodobno legalni i ilegalni. Novi model zaštite informacija koji je inauguriran ovim radom je otvoren i neizrazit.

REFERENCES

1. Alvin Toffler and Heidi Toffler, War and Anti-War (Boston: Little Brown, 1993).
2. Late in 1994, the two directorates negotiated a formal division of labor. How well that division holds up as the roles and missions of information warfare come up for decision remains to be seen.
3. Readers are also pointed to Julie Ryan, "Offensive Information War, a paper presented to the Naval Studies Board of the National Research Council (Washington, DC), 8 Sept. 1993.
4. Seminal works plural on information warfare include: George Stein, "Information War - Cyberwar - - Netwar," Air War College, 1993, and John Arquilla and David Ronfeldt, "Cyberwar Is Coming!" Comparative Strategy, 12 (1993), 141-165. The definitions used there differ from those used here. Netwar for those authors is akin to psychological warfare against both national will and national culture; cyberwar is command-and-control warfare, which broadly includes psychological operations against opposing commanders. A tenth of the latter is devoted to Genghis Khan's use of such techniques.
5. Anne Wells Branscomb, Who Owns Information? From Privacy to Public Access (N.Y.: Basic Books, 1994), 1.
6. An extended period of material deprivation coupled with continuous carpet bombing prior to the ground offensive has also been cited.

7. Physical (weak) and virtual (strong) decentralization are different: physical decentralization retains a centralized information architecture but protects the system by dispersing and replicating memory and processing; virtual decentralization makes subunits capable of operating on their own but uses coordination with the center to strengthen the quality of their decisions.
8. Whiteboarding is a network application that permits what is put on one person's screen to come up on another's.
9. Part of the Southern strategy in the Civil War was to conduct raids against railroads and telegraph lines used by Union forces; by 1864, nearly half the Union strength was devoted to occupation duties and protecting its lines of communication.

Adresa autora - Authors' address:
Prof.dr.sc. Vitomir Grbavac
Agronomski fakultet Sveučilišta u Zagrebu
Svetošimunska 25 HR - 10000 Zagreb

Doc. dr. sc. Krunoslav Antoliš
Hrvatsko komunikološko društvo

Primljeno - Received:
17. 11. 2000.