PARA-PROTECT
Absolute state-of-the-hack.

# The Future of Internet Security

**By Mark G. Graff**
VP/Chief Scientist, Para-Protect, Inc.
markg@meer.net

Is the Internet ever going to be secure? Or will we always worry about doing business with our credit cards over the Net, and whether strangers can read our mail? I don't know, but I have been thinking it over. It seems to me that we need to have an idea of what the Net itself will look like in, say, fifteen or twenty years, before we can know much about how safe stuff on it is. So I'll speculate on that first, then tackle the question about security.

## The Elements of the Internet Itself

The online world has five elements we commonly lump together. There's the Internet proper—that is, the routers, firewalls, phone lines, switching gear and so forth. Let's think of that as the communications Medium. Then there's the World Wide Web, which is the best-known Application. We need also to consider the Content, like your medical records and my airline reservations and our income taxes. The fourth component of the Net is composed of Devices, like your PC. They are connected by the medium, and run the applications against the content. The fifth element? I think of it as Locality. I'll explain more about that later.

Our next step is to analyze near-future changes in each of these components. I don't think I have anything too startling for you, really. But we might well learn something when we weave all these threads back together again. Let's look first at the future of the Internet Medium.

## Future of the Internet Medium

What big changes should we expect in the transport mechanisms themselves? We'll start by talking about the Internet transport we are familiar with today.

One easy-to-predict progression is the growth of already familiar media, such as cable modems and DSL, which build upon our existing infrastructure. Fierce competition for the "last mile" of network connectivity will continue in coming years, but I imagine that two or three of today's technologies will survive at least two decades. Telephony, coaxial cable, and satellite dish systems all provide attractive foundations for winning approaches, in my view. Many experts predict roles for all three in the information infrastructure of the near future.

We can also sense today a revolution in the making: a tidal move to wireless devices. Already, I read, the number of new wireless connections to the Internet each year is roughly equal to the number of wired ones. And I think the shift away from copper will continue until we hit equilibrium in the neighborhood of, say, an 80/20 or 90/10 split in favor of wireless. Folks who need the fastest possible connection, or live and work in remote or mountainous regions, as I do, will be the last holdouts for copper-carried communications.

Another improvement we can predict with confidence is increased bandwidth. Of

course, Internet users of the future—that includes just about all of us—will still be chewing up all of the bandwidth technology can provide. We'll complain about the perceived deficit, too

An accompanying change will be improved latency. Response times, in other words, will be much crisper, because the devices at the ends of network connections will be better tuned for Net use, such as Web browsing.

**Future of Applications We Use on the Net**

Two Net applications most everyone is familiar with these days are (1) email and (2) the World Wide Web. How will these and other well-known applications evolve? What will the new key applications of the future look like? Let's try to imagine.

One obvious change hurtling towards us today is the ubiquitous use of voice command interfaces. Another technology not far down the pike is the use of gesture, and directed eye movements. So what we will be seeing here is that, as computers move out of their infancy, we will begin to be able communicate with them in ways similar to the means we use to communicate with each other. We'll use the information-rich output channel of human voice and gesture, and capitalize on the much richer input channel of vision.

The new interfaces will bring unique security challenges. How, for example, would you go about authenticating a gesture?

Speaking of new interfaces: do you see an implication here for email? Expect soon a guts-level merging of email and telephony.

Surfing the Web will soon emerge as a marriage of travel, reading, listening to or watching broadcasts, and enjoying recorded entertainment such as music or movies. Interactive broadcasts will be common. Navigation methods will encompass the fancy tools I discussed earlier.

As to new applications, note that as the Internet permeates our houses and cars as well as our work places, the distinction between the network "outside" and the network "inside" resolves into a difference in who is allowed access. When each room in your house has a flat touch-sensitive video panel playing a Web browser, as mine soon will, and you keep both your family recipes and the diagrams of the plumbing system online, the Web will be a personalized global encyclopedia as much as anything else.

You have probably also noticed, in the last year or two, the proliferation of services which offer to store your data for you, and help you share it with others. So long as people feel that their information and the use of it is secure, we will see more and more of the services folks buy or exchange in the world operated via the Internet. Far beyond commerce, we will see psychoanalysis, sexual satisfaction, voting, scheduling, testimony, and surgery online.

Wait—all of those we have already seen! How about in, say, twenty years? Truthfully, I don't know. (I bet Gutenberg's peers couldn't have predicted which books they'd be printing, either.) Better to ask what part of your life won't be migrating. I expect it will be a matter of taste. The technical restrictions, so far as I can see, don't amount to much.

Each activity will make its own demands on the Internet security of the day.

Add to all these toys and treats the promise of semi-autonomous, programmatic, partial-personality agents. They will act as receptionists and representatives, making the task of goading glass-and-silicon beasts into productive action that much easier.

Think again about how a communication application (the email of the future) might work. You will tell your messaging agent, "Let me talk to Pete," and it will look the situation over; ask, perhaps, whether you want to interrupt Pete's favorite narrowcast; then, one expects, give you a choice of media and accompanying art before making one or more appropriate connections.

Hand waving like this comes pretty easily, doesn't it? Let's stretch our luck and take a broader look at the future of Internet content.

**Future Content on the Net**

My first cut is: The Net will store all information about everybody. And that surely includes a bunch of things that members of my family might not want to throw into the Great Stew of Knowledge for everybody to slurp up.

Are we in for trouble? Are you? Consider that it will be very difficult, in many cases, to prevent the "networkization" of content such as:

- Report cards
- Love letters
- Arrest records
- Medical histories
- Itemized sales receipts

If you wonder what I mean by networkization, it's that the material is available to everyone in the world unless the all the security measures you rely on work extremely well.

Consider further the class of items that don't make you cringe until they can be crosschecked—say:

- Expense reports
- Credit card receipts
- Income tax reports
- Surveillance and traffic camera videos

Okay, now that I got you on the subject, stop thinking about what you'd like to hide from the rest of us and come back to the party. When you left, we were trying to decide what subset of "everything" would certainly not be online. Uh-oh. I'm drawing a blank.

Changing the subject a little, I'll point out that another singular attribute of the Net's information is—counter-intuitively—its permanence.

Sure, you've lost data because you didn't back up your hard disk. But the game has changed. Have you ever tried to truly extirpate a datum you once stored on the Internet? If so, you don't think you succeeded, do you? Then consider for a moment the backups performed on the intermediate mail servers that help transport your email; the browser caches of folks who have visited your web site; and the immutable records of all the Usenet news groups you've ever posted to.

Believe me, your dashed-off opinions, flirtations, inquiries, and disclosures are "out there" to stay. Plan your political future accordingly.

**Future Devices We Use to Connect to the Net**

We'll consider now what an Internet device of the near future might look like. (We're going through this procedure, remember, en route to an understanding of what security

threats and defenses will be needed. A rough understanding of the devices is a prerequisite, right?)

Sample devices you are probably familiar today are your email box (say, a PC); any palmtop or laptop you use which is networked some of the time; and of course all those truly special gimcracks, such as the San Diego Zoo's Panda-Cam.

How will network devices change? Here's my prediction: Net access in the near future will be insensibly fast, and will be built in—tiny and invisible—to a fantastic range of materials. A short list:

- Personal Data Assistants
- Personal Communication Devices
- Display devices—wall size, building size, tiny too
- Eyeglasses (used for both input and output)
- Microphones
- Telescopes
- Microscopes
- Temperature and weather sensors
- Medical scanners, such as X-ray machines and MRI's

Think for a moment about the decisions you and others will make based on the information returned from such devices, and you're tuning in again to the Internet security challenges that are heading our way. We'd better take awfully good care of them. Say, where will all these data sources and sinks be located?

**Future "Locality" of Internet Connections**

No longer restricted to business, communications, and, say, home entertainment, the Net will be imbedded into cars, everyday appliances, clothing, and even disposable packaging. It's going to be "everywhere".

OK, you caught me hand waving again. Let's try to be more precise. What will be the reach of the Internet? That, as I see it, is decided by the fifth, synthetic network element I call Locality.

Locality is a combination of the physical location of the devices, the environmental context of that location, and the societal environ represented by that location. An example could be a scientific station in the Indian Ocean. It might be 1000 feet down, 100 miles off the island of Diego Garcia. That would be its location. The pressurized dome the aquanauts live in would be the environmental context of the network. The societal environ (in this case, the "use" the networked space was put to) would be as a laboratory, or living quarters, or perhaps an underwater trash dump.

Here are three sample sets of answers, then, to the question, "Where will the Internet be?" Here's a quick list, based on my projection of how all this technology (most already in existence) will be applied in the near future.

Locations:

- Most new buildings, many of the "old" (circa 2000) ones
- Most new electronic devices, many "old" ones
- Under the sea, including research facilities, mining operations, and residences
- In outer space, including satellites, space stations, transports, and colonies
- In inner space—inside our bodies, as well as those of our pets, working animals, and plant life genetically altered to facilitate Net access

Environmental contexts:

- Architectural elements: walls, floors, doors and windows
- Worldwide critical infrastructure elements such as communications, energy production and distribution, manufacturing, farming, and transportation
- Fabrics, paper products, sheet metal
- Foodstuffs and other ingestibles

Societal environs:

- Homes, offices, churches, gyms, schools, theaters, restaurants, stores, libraries, police stations, courtrooms, hospitals, bus stops, bus stop signs, bus stop benches, bus stop shelters, bus stop schedules
- Buses; taxis, trams, and trains; boats, private automobiles, trucks, forklifts, police cars, and ambulances
- Workplaces: most (or even "all", by legal mandate?)
- Appliances: refrigerators, ovens, lamps, light bulbs, television-telephone-computers, toilets, tools and utensils
- Containers
- Furniture
- Clothing
- Prosthetic devices, e.g., eyeglasses, hearing aids—and how about dental appliances?
- Medical treatment tools and instruments
- Medicines and ingestible medical treatments, diagnostic tools, and other devices

What did I leave out? A universe of materials, I'd wager.

**Summing up: The Internet Itself**

My case, briefly, is that, soon, the very fabric of our society will be suffused with Internet access. What we know and can know about the world will, to a large and increasing extent, combine into an informational cloud, a mist of facts. I call it (and Jeffrey Cooper of SAIC was there first) the InfoSphere.

I don't mean, of course, that these changes will be adopted all at once, and universally. Just as jet planes today scratch out contrails in the sky while "aborigine" tribes hunt and weave underneath, so do many ages and stages of technological achievement co-exist, the pace and degree of adoption varying according to location, wealth, need, custom, and tolerance for change. This "heterotechnochronicity" lives in our homes, too: in my family, we are as likely to stir the waffle batter with a wooden spoon as a microprocessor-controlled mixer. Still, wooden spoons notwithstanding, the InfoSphere will mist soon into our kitchen (and yours, too).

**The Internet Security Environment of the Future**

Now that I have taken my wild guesses about how the Net will grow, we can think about how it will be safeguarded (and violated) in the future.

How important then will security be? How might we achieve it, and what price will we have to pay—as a group, and as individuals—to get it? What attacks can we foresee against the Internet itself, and against its content, function, and applications? How will we defend against those threats, securing what is important to us and the people we love?

**Elements of Internet Security**

What are the elements of Internet security, as it is practiced and experienced today? To

my eye, there are five. I find it to be true that when I focus on any one of these elements, I convince myself for a moment that I have all of "security" in view. Each can seem a complete world. And understanding each is in fact necessary for our purpose. They are:

1. The Architectural
2. The Technological
3. The Procedural
4. The Psychsociological
5. The Existential element: Attacks and Attackers

By "Architectural elements", I mean the principles and goals that security architects use and pursue, e.g., authorization, authentication, access control and compartmentalization, and so forth. Architects use Technological means (such as firewalls, passwords, simple biometrics, public key encryption, checksums, and even log files) and Practical measures, like penetration tests and audits, to prevent and detect attacks. We rely, too, on Societal pressures and protections to deter and punish malefactors. Oh, and what do I mean by the Existential element of Internet security? Let's leave that for last.

**The Architectural Element of Security**

Consult any popular work on information security, and you are sure to find principles such as the following included. They are the pillars of any secure design. A popular few are:

- Authentication. Determining who really is trying to use a system.
- Identification. A method for separating the actions and permissions of one person from another, for example by the assignment of user names.
- Authorization. Deciding what each user is supposed to be able to do.
- Access control. Limiting what folks can do, based on authorization rules.
- Minimum useful access. Giving users only the access they really need.
- Compartmentalization. Not putting all your information eggs in one basket.
- Invisibility and Obfuscation. Hiding the baskets.

How will this aspect of Internet security change over the next twenty years? Frankly, I think this will be the element that changes the least. Good architecture will always be rewarded, and so far as I can see, the principles will largely remain the same. But I do see a few trends.

*Role-Based Authorization*. Today, most systems and networks make authorization decisions based on what a single user needs to do. So, Joe the sales clerk might be given access to a customer database, product and price information, and manufacturing schedules. But the increasing complexity and growth of networks, especially intranets, will make hierarchical, role-based authorization more popular. This means that access decisions will be based on a determination on what groups (e.g., citizenry, company, or national security clearance level) you belong to. Access rights will be granted to these sort of groups, and you will get to what you are supposed to by virtue of the groups or attributes that can reliably be ascribed to you.

*"Universal" Identifiers.* Today, it's not unusual for one person to have ten or twenty Internet user names. If you do a lot of online shopping, for example, you might well have found it impossible to obtain identical user names for all the stores. And do you have

several different email services, like I do? If you do, you will agree this has got to stop. Surely in the next few years we will agree on a scheme that lets us use a single identifier for the majority of our online work.

*Aggregated Access*. In the same vein, we are already seeing "screen-scraping" services that allow you to visit a single Web site and interact with, for example, an aggregation of all of your online financial services. This approach will certainly become the norm, don't you agree? Expect, too, the refinement of Web portals and shopping 'bots.

*Reduced Scope of Anonymity.* For commonplace Net transactions in the future I expect there to be a definite divide between the places you can act anonymously and the places where, if your identity becomes important at a later date, your identity (observing due process, of course) can be determined. Of course, it's hard to imagine a major medium of economic exchange where good old faceless, untraceable "cash" is not honored. And we will always need to protect whistle-blowers and bell-ringers. But as the Internet grows to dominate the world's marketplaces and communications, I predict that the need for exceptional reliability will create irresistible demand for a fair degree of certainty as to who is doing what to whom.

All of these changes, as you have probably already noticed, will require much better authentication techniques than we commonly use today.

**The Technological Element of Security**

Now for a look at current security technologies and how they will be changed and augmented.

Your service provider today almost certainly relies on a mix of the following techniques and technologies for their security. (Of course, this is not an exhaustive list.)

1. Re-usable passwords
2. Firewalls
3. Log file analysis
4. Virus checkers based on known attack "fingerprints"
5. Intrusion detection based on known attack "fingerprints"
6. Encryption, especially Public-Key Encryption
7. Adaptive load-shedding to limit the effect of Denial-of-Service attacks
8. Strong Checksums (for verifying contents of a file haven't changed)
9. One-time passwords, or token cards
10. Biometrics (e.g., real-time fingerprint checking)

While the use of techniques 1-4 is commonplace, my experience tells me that uniform use of 5-7 is still the exception rather than the rule today. And you will find that only the groups really dedicated to security are using all ten of the techniques I've listed.

I will describe first what I think is the fate of the old stand-bys. Then I'll try to describe what new variants or techniques I expect to emerge. And please remember the point I made in Part 1 about "heterotechnochronicity." Extant techniques (many dating from the 1950's, if not earlier) will co-exist with new technologies for as far into the future as I can see. (In fact, largely due to misplaced conservatism, critical systems often are the least secure on the network, getting security patches and improved procedures far later than less important systems.)

To start with, security geeks like me have been trying to kill off re-usable passwords for at least a decade. They are dodos, and will start dying off in droves when the stronger methods of authentication (like token cards) get cheap enough for universal use. Just too easy to guess and steal.

Firewalls are dated, too, in my opinion, though still today a requirement for a diligent design. What's wrong with them? In my experience, any firewall that stays in place long enough tends to devolve into a router. Getting in the way of two people or companies or software entities that really want to communicate, and staying in the way, is not a good long-term survival strategy. I do expect the firewall to survive, however, as a form of "valve" which can be opened or closed to damp or regulate gross traffic, and prevent floods.

Log file analysis has its place, but, like fingerprint-based detection, will not be able to survive a massive scaling-up without re-engineering. So I expect that for many years we will still see the use of log files, virus checkers, and intrusion detection systems; but they will be much smarter.

How big can a log file be today, before it becomes too ponderous for use? Some number of gigabytes, I expect. Many people already find that this is too big to process algorithmically. What happens when we need to keep information on a scale, say, three or four or five orders of magnitude larger?

The same argument sinks fingerprint-based virus and intrusion checks. Worse yet, in these cases, we can also expect that the attack mutation rate will increase as the Internet reaches most of the world's population, so that we will have, say, hundreds of new variants a day. Such a pace would overwhelm any current update scheme, even if the total size of the thing-to-check database didn't.

The rise of executable content, exhibited today in Java and ActiveX applications, is an obvious additional complication.

The only way I can see these techniques surviving as useful tools is if they are made intelligent enough to "understand" the sort of things that are permissible, and flag or disallow every other activity. This should be cheaper and faster than checking for activities that are disallowed, as they (generally) do today.

The last few Technologies I mentioned above are newer and stronger than the others, and are likely to be in the mix of protective measures in use twenty years from now.

- Encryption, especially Public-Key Encryption
- Adaptive load-shedding to limit the effect of Denial-of-Service attacks
- Strong Checksums (for verifying contents of a file haven't changed)
- One-time passwords, or token cards
- Biometrics (e.g., real-time fingerprint checking)

Of these, I expect encryption and biometrics (smaller, cheaper, and passive) to be ubiquitous and transparent. Token cards, in their present form factor, I see a limited future for, because of the need to carry them around and the resulting risk of loss. But there's always that empty space right behind our ears, ideally placed for a token chip, bone-conduction microphone, and middle-ear speaker. Are you ready for that? The next generation might be.

As I will discuss in detail in the section on the Existential element, the most promising technology I can see is the use of independent, stochastically operating, software agents which perform access control and check for anomalies. While I can imagine both stateless and "state-full" varieties, I think the latter could be much more powerful, if we can solve the additional security challenges that goes with preserving state information.

**The Procedural Element of Security**

Technology aside, there is today many current procedures which are key to defense. How will they change, and what will survive the next two decades?

Most sites practice some mix of the following protective measures.

1. Detecting and fixing software bugs and vulnerabilities
2. Installing software upgrades and patches
3. Configuration and change control
4. Checking for change (i.e., file contamination, Trojan horses)
5. Penetration tests and security audits
6. Honey pots and other pest control measures
7. General administrative policies and procedures, such as account handling, authorization policies, and information classification

Now, how will each of those methods of assurance evolve? What new methods of assurance will we see?

The first four of these practices will gradually diminish in usefulness, for the same reasons that fingerprint- or pattern-based virus and intrusion checkers will decline. The pace of change, mutation, failure-and-fix of the networks of the future will defeat these largely manual practices. The trend will have to be towards true automation, using largely autonomous, non-determinative (i.e., stochastic) agents.

On the other hand, I think these other Practices will stand the test of time:

- Penetration tests and security audits
- Honey pots and other pest control measures
- General administrative policies and procedures

All three will need to adapt in precision and cleverness, of course, and automation will again be key. But all will be essential to information security for the foreseeable future, largely unchanged except for detail.

Interesting to note, isn't it, that the practices we've listed here are prophylactic and defensive? When we think about it, shouldn't we expect information protection to become more "offense-based"? How long can it be before we hear some huge world-wide enterprise announce that, subject to the laws in force at a particular point in their networks, they will "shoot first and ask questions later" when they see suspicious activity? As I first pointed out almost twenty years ago, if all the big companies who are being attacked by teenagers turned their computers and aimed them back at the kitchen table hackers, we could comprise a formidable deterrent.

In a slightly more civilized vein, I expect to see proactive/offensive activity like

- Profiling of likely attackers, perhaps making it harder for folks to fit the "hacker profile" to get access
- Grading of ISP's or other connection sources, such as universities—some enterprises might establish a quota

(or surcharge) for "risky" connections
- Automated, policy-driven, doomsday can't-stop-it eye-for-an-eye counter-attacks (with associated problems of misidentification and impersonation)

Of course, the "profiling" and "quota" activities I describe are quintessentially anti-democratic, making them clearly unsuitable for some environments (and no doubt open to caustic criticism in others).

OK, that's it. Enough technology. We're moving on to some social issues.

**The Societal and Psychological Element of Security**

The more tightly the Internet is woven into the fabric of our society, the more closely interwoven it will become with other institutions and constructs. I discuss here a few examples.

One trend to consider is that, as we bring the Internet into our homes, families, and bodies, security becomes much more personal. An attack could then threaten not only our livelihood and our life, but also our sense of bodily integrity. Anyone who has ever come home from a vacation to find their home burglarized can easily imagine being still more disturbed by an attack on, say, molecular medical devices operating in the intestines.

Way before we reach that point, however, our reliance on the Internet for the correct operation of the hydroelectric and communications grids, as well as fire, police, and other essential social services, will engender an irresistible demand for greater reliability of all networked components. The "phone company" achieved in years past, and we expect today as a matter of course, "four nines" reliability. (That's 99.99% uptime.) We will come soon to expect at least that level of performance for the Internet.

A demand for such superb reliability will engender social change with respect to the way we as a society perceive and react to attack activities.

Who will "manage" the security of the Internet, connected devices, and all that data? I guess big companies will tend their pastures, as now, certainly in some cases under more regulation. But what about all the little imbedded devices, mobile phones, and so forth? One thing is for sure: it won't be the end consumer, scanning the Web for security alerts and applying software patches to his refrigerator (checking first for compatibility with the stovetop). In the United States, I can see the FTC issuing warnings. I can see recalls from manufacturers, and insurance policies, a little like health coverage that protects consumers against failures.

Mostly, I see liability suits against computer vendors and other manufacturers for selling insecure products, and government watchdogs helping to develop, coordinate, and enforce quality standards. The safety standards governing flameproof sleepwear for infants is a good example here. A second: seatbelt laws.

Beyond regulation, expect a burgeoning of criminal law as the Internet weaves around us. Today's prank is tomorrow's crime. Surely it is only a matter of time before we hear, say, the first tale of an elder or toddler fatally being denied medical help at a critical time because of a denial-of-service attack.

We should see, too, an increasingly responsible attitude from major news media as regards the reporting of hacker attacks.

Still, let us not expect the extermination of popular support for the hacker/attacker. To quote the old chant, "Trickster makes this world", and sympathy for the light-footed, crafty and resourceful anti-establishment figure will never die. In the near future not only will security attacks be a common medium for social protest, but we should expect a slate of wildly out-of-the mainstream, mildly sub-cultural celebrities as well.

In twenty years, international treaties facilitating cooperation amongst nation-states (and, one imagines, corporation-states) in Internet security matters will have been in place for many years. The first ones are being negotiated now.

That said, we should expect to see a mix of events similar to other treaty areas. We will have rogue states, safe harbors, asylum, and the eternal dilemma of the rational/democratic when yoked to the irrational/repressive: do we turn over those who have furthered what we see as social good while breaking the laws of their own country?

Oh, sorry, forgot to clear something up. I mean to include activity taking place in cyber-space, not just the surface of a medium-sized planet. We will help pursue software agents who have committed criminal acts, across the boundaries of cyber-states. Can you arrest and prosecute a program? Execute one? We are going to find out. By 2020 or so we should know.

With that idea as prologue, we are ready to tackle the Existential element.

**The Existential Element of Security: Attacks and Attackers**

The most significant incipient change I can foresee in Internet security relates to a state of being—what the Greeks might call *Ousios.*

We'll get to the metaphysics soon. First, let's look at today's attacks.

Goal of current attacks seem to center around:

- Denial of Service
- Thefts of Intellectual Property
- Fraud
- Diminished data integrity
- Door-Rattling/Experimentation

Attackers tend to fall into one of these categories.

- "Thrill Seekers"
- Competitors
- Criminals
- Terrorists
- Warriors

The means of attack tend to be:

- Social engineering
- Exploitation of technical defects
- Resource depletion

That's all fairly straightforward. Now, take a look at the list of common characteristics of today's attacks. The hair on the nape of your neck might just begin to stand up. Generally, Internet-based attacks today:

- Are initiated purposefully
- Are directed at a specific target or small set of or targets
- Can be traced to a single source
- Are launched and coordinated by a single person or small group
- Can be stopped or controlled by the attacker

- Have a beginning and an end
- Last hours, days, or (rarely) weeks

Will this state of affairs last?

Simple Internet-based attacks in the future will, I believe, often resemble those of the present in terms of goals and attackers. These are determined by the nature of people and their societies. Many attackers, also, will continue to use "traditional" means of attack.

But there is a new kind of security storm brewing. If we listen attentively, we can hear the wind blowing our way now. All of the "common characteristics" I listed above will be transcended by tomorrow's attacks, many of which will:

- Be untraceable, having taken on a life of their own
- Survive and persist on the Net as self-reproducing software entities
- Fulfill no purpose discernible to the human mind
- Be directed at no discernible target, the set of affected hosts or services not sharing a common attribute we can fathom
- Not be stoppable or controllable, except perhaps by the launch of a counteracting entity
- May well have no discrete beginning or end (i.e., birth or death), but rather be best viewed as an evolutionary stage
- Persist for years, even decades, in a longitudinal attack

In the future, while we will still talk of individual attacks, it will be in the way we speak of an especially severe squall, on the periphery of a hurricane. We will rank security "seasons", too, and bad years; and someday we may also discover latent cycles, like the 11-year period of sunspots. In this way, remarkably, a cloud of artifacts—attacks—that began as an abstract dance of the intellect may well take on the aspect of a force of nature.

What I foresee (to swap metaphors) is an Internet suffused with a pathogenic mist. Cleansing agents will act like antibiotics. Agents acting against the interest of our networks will subject them to a constant bombardment, which suites of defensive agents will counter, also in a stochastic, non-deterministic steady state.

The picture resembles nothing so much as a human body and its internal organs, wrapped in skin, warding off germs. (A nod of the head here goes to Fred Cohen and Len Adleman, generally credited with coining the term "computer virus" in 1983.) The human body, properly considered, is a battleground, and our clearest exemplar of future networks. We are already close to this state of affairs. I submit that, looking back from the future, we may well determine that such neobiological attacks have already begun.

It is interesting, too, to consider the coming reduction in network latency (which I alluded to earlier) as a parameter of the Net's distributed "nervous system". I wonder, what will the effect be of this "quickening" transformation of the Internet feedback loop?

**Summing Up: The Future Internet Security Environment**

My answer, then, to the question, "How will we defend against those threats, securing what is important to us and the people we love?" is that we will develop and deploy immune systems for our networks. Active research (for example, at IBM) has already begun. After a while, if we build them well,

the networks themselves may help to improve their own immune systems. We may expect an appropriately Darwinian contest.

The outcome, of course, will include the survival of the fittest attacks, as well as the fittest networks, as the arms race escalates. Fairly considered, attacking entities are individuals themselves. What rights will they be accorded? We must wait to see.



PARA-PROTECT

**About the Author**

Mark Graff, Chief Scientist at Para-Protect Services, is a frequent speaker at industry workshops and conferences and a Congressional expert witness on Internet security. He has also appeared before the Presidential Commission on Infrastructure Survivability, anchors Para-Protect's founding membership in the Partnership for Critical Infrastructure Security, and has lectured on network security topics at the Pentagon, other key U.S. government facilities, and the American Academy for the Advance of the Sciences.

Mr. Graff was Security Architect for Sun Microsystems for several years. He holds a Bachelor's Degree in Computer Science from the University of Southern Mississippi, and is the author of a modest set of books and articles on a variety of computer-related subjects. The working title of his current book project is "Software Vulnerabilities".