PARA-PROTECT

Sleepless in 2020: The Future of Internet Security

By

Mark G. Graff

VP/Chief Scientist, Para-Protect, Inc.

Markg@meer.net

When I Have Explained All Of This I Will Stop Talking

- Five Elements of the Internet Itself: Medium, Applications, Content, Devices, Locality
- The Future of These Internet Elements
- Five Elements of Internet Security: Architectural, Technological, Procedural, Psychosociological, Existential
- The Future of the Five Elements of Security
- Three Net Nightmares for the Future
- Summing Up

Future of the Internet Medium Itself

- Existing media (especially telephony, coaxial cable, and satellite dishes) to grow
- Wireless will dominate work, travel, home environments
- Bandwidth will skyrocket; we'll still kvetch
- Latency will grow markedly crisper for major sites

Future Applications We Will Use On the Net

- User interfaces: voice and gesture, wall-sized screens, wireless everything
- New combinations: telephony+email, travel+reading+watching+listening
- New applications: encyclopedia, courtship, voting, surgery—all (at least) we can imagine
- Quasi-intelligent agents will handle most routine interactions, initiate and monitor everyday tasks, digest+summarize+advise

Future Content on the Net

- Scope="everything": report cards, love letters, arrest records, medical histories, itemized sales receipts. What's the limit?
- Synthesis, too: cross-correlating expense reports, credit card receipts, income tax reports, surveillance and traffic cameras
- Permanence of records is counter-intuitive
- Plan your political career (and love life?) accordingly

Future Devices We Will Use to Connect to the Net

- Personal Data Assistants, phones, etc.
- Display devices (building size to bug-sized)
- Microscopes, telescopes, microphones
- Eyeglasses, hearing aids, other prostheses
- Cameras and other recorders
- Thermometers and other sensors
- X-ray machines, MRI's, other medical scanners, sensors, and samplers

PARA-PROTECT

Future "Locality" of Internet Connections

- Locations: most buildings, most devices, under the sea, outer space, inner space (including pets, working animals, plants)
- Environmental contexts: wall, floors, doors, windows, worldwide infrastructure, fabrics, paper products, sheet metals, foodstuffs, drugs
- Societal environs: homes, offices, churches, jails, schools, public places and transport, appliances, containers, furniture, clothing, prostheses, medical diagnostic tools and treatments, medicines and ingestible medical treatments

Summing Up: The Internet Itself

- The fabric of our society—and, for some of us, our bodies themselves—will be suffused with Internet access
- Most of us will live to see the instantiation of the InfoSphere
- Old and new styles, artifacts, and even life forms will co-exist due to the phenomenon of “heterotechnochronicity”

PARA-PROTECT

Five Elements of Future Internet Security

- The Architectural
- The Technological
- The Procedural
- The Psychosociological
- The Existential

The Architectural Element of Future Internet Security

- Likely to persist: principles of authentication, identification, authorization, access control, minimum useful access, compartmentalization, simplicity, obfuscation
- Increased use expected of: role-based authentication, universal identifiers, aggregated access (e.g., “screen-scraping”), reduced scope of anonymity
- Key to most improvements will be progress in authentication techniques

The Technological Element of Future Internet Security

- Dead technologies: re-usable passwords, firewalls (still useful as valves), log-file analysis
- Technologies which must adapt or die: fingerprint-based virus-checkers, classical intrusion detection
- Technology paradigms which will persist: encryption, adaptive load-shedding, strong checksums, biometrics
- Dominant new form factor will be tiny and endemic or implanted. Input and authentication will be via voice, gesture, eye tracks and facial expression, maybe brain waves—and that empty space right behind our ears

PARA-PROTECT

The Procedural Element of Future Internet Security

- Headed for the trash heap: detect-and-fix bugs, customer-pulled upgrades and patches, configuration and change control, checking for unexpected changes
- Likely to survive: penetration tests and security audits, honey pots, administrative policies, practices and procedures
- Why be passive? Somebody soon is going to strike back. We may see “doomsday” devices built and used as deterrents

The Psychosociological Future of Internet Security

- More personal when it's a matter of bodily or mental integrity
- Concomitant demand for greater reliability, especially as infrastructure becomes completely dependent
- Crime and punishment, civil liability will soon be routine
- The Trickster will never die
- The international scene: we'll see treaties, conundrums, controversy

The Existential Future of Internet Security

- Yesterday: core wars
- Today: denial of service, vandalism, thefts which are motivated, rational, commensurable and comprehensible
- Tomorrow: Attacks will be of a different state of being—fulfilling no purpose; associated with no human mind; having no beginning or end; not controllable; alive; perhaps effectively immortal
- New models become weather, gang warfare, and especially disease. What latent cycles will we find?
- When looking back we will likely see that all this has already been initiated

Nightmare #1: Contagion

- Fantasy rooted in mg's own experience
- Imagine a quiet back door generator placed in a major vendor's software—say, o.s.-level helper utilities, like backup or Web stuff
- Ideal vehicle is probably a data file, not a piece of software *per se*; the file should not be in a format easily readable by humans, and not often changed
- The plan would be to let the files permeate the Internet for a decade or so, then reap whatever rewards are desired

Nightmare #2: Gangland

- Imagine a set of gangs occupying “turf” on the Internet, attacking those who threaten their hegemony (as well as their chosen “enemies”). Why not, for starters, claim a particular set of IP numbers as “ours”?
- To think of their location as being cohesive geographically is old hat; instead, think socioeconomic clusters, “true believers”
- Expect an “ISP-agile” existence: these are Net Nomads, wisps
- A Robin Hood-like persona, for example, might be popular enough to survive
- Can a Net religion be far off?

Nightmare #3: Doomsday

- Tired of being attacked and taken offline? What's the best way to make it stop?
- If you were desperate enough, couldn't you figure out a way to take the Net down, and keep it down, for a long time?
- Would it be hard to establish thousands of stand-by attack cells, keyed to attack if a certain entity was off the Net for a specified time?
- Won't we soon be able to build an agile enough worm to maneuver around the net and elude capture indefinitely?
- Might as well call it the doctrine of "Mutual Assured Downtime"

Summing Up: The Future of Internet Security

- The Internet will be invisible everywhere
- No “clean” networks; no “data centers”
- The struggle will promote the survival of the fittest network element--and attacks
- Networks must “heal” in order to survive
- We must decide: what rights do cybernetic entities—“programs”—have?
- Remember: “If we knew what we were doing all of the time…”