Talk for the 8th Security Seals Symposium
Charleston, SC, Jan 29-31, 2008

Argonne NATIONAL LABORATORY

… for a brighter future

Future Directions in Physical Security

Jon S. Warner, Ph.D.

Roger G. Johnston, Ph.D., CPP

Vulnerability Assessment Team

Argonne National Laboratory

jwarner@anl.gov *630-252-2114*

http://www.ne.anl.gov/capabilities/vat/index.html

“The best way to predict the future is to invent it. This is the century where you can be proactive about the future; you don’t have to be reactive .” -Alan C. Kay

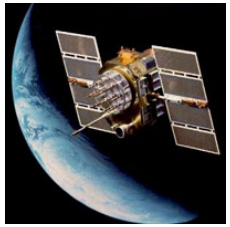
"We're driving faster and faster into the future, trying to steer by using only the rear-view mirror.” -Marshall McLuhan

Predictions

- More sophisticated policies will be employed to intelligently accommodate (instead of outright banning) new technology in order to remain globally competitive.
- It'll slowly be realized that current physical security methodologies aren't working. Physical security will become a legitimate scholarly subject.
- The Anti-Evidence approach to tamper detection will become common (because it is the best way to do it).

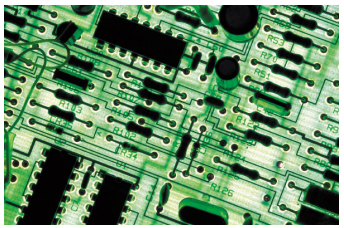
Predictions

- Wishful thinking about high-tech will only increase.
- As high-tech increases, careful thinking about security will decrease.
- At some point, a terrorist incident will shut down a major U.S. port/s with severe economic & geopolitical implications.
- The RFID allure will die out and will be replaced by true security devices, including RF devices.
- There will be serious GPS spoofing incidents.



Technology: Electronics

- Moletronics: Molecular scale electronics will replace current silicon based electronics thus saving space and power.
- Spintronics will also play a part in the future of electronics. Based on the spin degree of the electron, this would allow for significantly faster processing speeds, much lower power consumption, and much greater component densities.
- Photonics will replace electronics.



Technology: Electronics

- The battery problem will be solved due to smaller, more powerful batteries and more efficient, less power hungry electronics.
- Nanotechnology, while important, will have been over-hyped. Many useful devices will be built on the micron scale.
- Wearable electronics will become ubiquitous.

Technology: Microprocessors

- Microprocessors will be used everywhere in everything. A toaster of the not-too-distant future will have more computing power than the Apollo 13 mission.
- Multi-core microprocessors will be common place.
- Microprocessors will become “power-aware.”
  - Frequency and voltage scaling on the fly.
  - Will close unneeded processes to prolong battery lifetime.
- Will become: Self-optimizing (resource management), Self-Protecting (from unauthorized access), Self-Healing (problem finding and fixing), Self-Configuring (defines itself “on-the-fly), and “Self-Programming”.

Technology: Materials

- Bioactive coatings will be employed to react to the presence of a target biological.
- Self-repairing materials will be commonplace including self-repairing roads and walls.
- 3D printing and 3D milling machines will be available to the home hobbyist.
- New seal materials will be developed.
- Metamaterials will make invisibility devices practical and commercially available.
  - Devices that appear to be invisible to microwaves and acoustics have been demonstrated in the laboratory already.

Technology: Misc

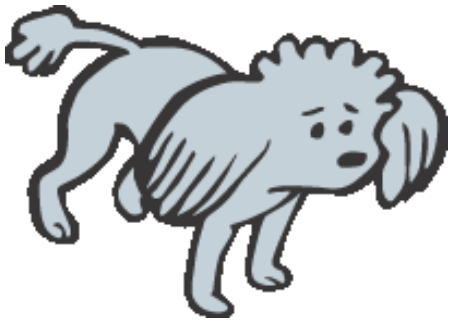
- New stealth bugs and cameras will be developed. These bugs will be undetectable and, due to the advance of new technologies, the buggers will be able to stay ahead of the scanners and bug sweepers.
- Poorer countries will build up significant air forces, navies, and armies using unmanned systems. This technology will not be purchased but stolen via information espionage.
- Polygraph tests will be replaced by brain scanning and mapping techniques to check human veracity.

Technology: Misc

- Room temperature super-conductors will be available.
- Photonics and quantum systems will become more commercially pervasive.
- New optical materials will be developed. These will generate dramatic visual changes when cut or attacked.
- The use of “smart cameras” will continue to increase. However, there are already studies that show such systems won’t prevent crime, but will be useful during the post crime investigation.

Technology: Sensors

- Electronic sniffers will outperform dogs in terms of accuracy, repeatability, maintenance, and ease of use.
- Smell will become the new biometric; it will be possible to go into a bank and smell if you were there yesterday.



Technology: Sensors

- Wireless sensor networks will be used extensively. These will communicate with each other as well as a central HQ.
- Some access control systems will communicate with HQ via the building electrical system.
- They will be able to reconfigure themselves for efficiency, and adapt to changing environments.
- Longer term, they will form a building security system that evolves itself to meet new challenges.

"Security is both a tradeoff and an arms race." -Bruce Schneier

Disposable Transportainers

- Only need to protect once.
- Will drive development of throw-away security devices.
- No need to return security devices to owners.
- Although the security device won't be proprietary, the data sent to and extracted from it will be. The security is in the data, not the device.

Technology: Communication

- Everything will radiate RF. Most devices will have IP addresses (toasters, picture frames, refrigerators, automobiles, small RFID parts, etc.).
- The security community will tire of having all their eggs in one RF basket. RF will fall out of favor in the security world because of interference issues, and other problems. IR, UV and acoustics/ultrasonics will become important alternatives.

"Security must pervade every aspect of system design." - Security in Wireless Sensors

Technology: Networks

- Network access will be ubiquitous.
- Users will demand continuous connectivity.
- Ubiquity of more powerful computing devices.
- Every device will have a routable IP address.
- Active content will increase.
- Peer to Peer usage will increase.
- Devices will require multiple management sources.
- Devices will always be “on.”

Technology: Networks

- Hacker interest in SCADA (Supervisory Control and Data Acquisition) network vulnerabilities will continue to grow.
- Physical security will be relied upon more than ever to protect computers and vice versa.
- Poor initial implementation of convergence will open up a whole new class of attack techniques.

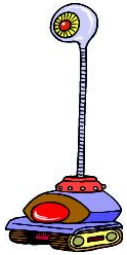
"Today's sloppiness' will become tomorrow's chaos." -Scott Berinato

Hacking

- The hacker community will continue to grow.
- Some of the current hacking conferences available now:
  Blackhat, DEFCON, SHmooCon, Hackers On Planet Earth, Hack-In-The-Box, Chaos Computer Club, PacSec, SysScAN, CanSecWest, ToorCon, PhreakNIC, etc.
- Hacking will become even a bigger problem:
  - The website “Lockpicking101.com” dedicated to lock picking enthusiasts has a registered membership of 57,522.
  - The website “Hackaday.com” and website dedicated to hacking hardware reported ~400,000 visits per week.

“Although hackers themselves aren’t necessarily malicious, one person’s sport can be another person’s training ground.” -Anonymous

Smart Guard



- Mindless applications will be replaced by technology.
- Technology will foster an appreciation of human beings and will emphasize the importance of the “super guard”: a roving expert in security, law, electronic troubleshooting, first aid, counseling, information security, etc.
- What we currently call a security manager will become the “super guard”.
- Physical security will become an honored profession instead of a job for high school drops outs which is the perception now.

Human factors

- The “best and brightest” will continue to avoid the field of physical security, until it becomes an honored profession.
- Students will be able to get a degree (including an advanced) degree in “Physical Security” from a major 4-year university.
- Just as inventory is confused for security, control will become confused with security.
- No matter what technology becomes available, no new crimes will be invented, only new ways to implement old crimes.

Legal

- There will be horrendous examples of the deficiencies of current vulnerability assessment schemes. Serious incidences will occur where current VA methods were used and very obvious security flaws were overlooked.
- Manufacturers and vendors of security products will start to face civil (and maybe even criminal) liabilities when the security products they provide are found to have poor security -- the current DHS attempt to mitigate terrorism liability notwithstanding.
- In the future, the theft or loss of a cargo shipment will cause far more harm than merely the replacement cost of the lost items. This will be due to increased JIT manufacturing, terrorism concerns, privacy & proprietary concerns, and the importance of good corporate reputations.

"Significant psychological damage is needed before there will be changes in security." -Anonymous

Authentication

- Biometrics will become commonplace. Biometrics will be increasingly used to the point that biometric identity theft is the same level as other identity theft is today. Consequently, biometrics will not be used much in high security applications in the future.
- Passwords will go away altogether and be replaced by something more user friendly (not biometrics). Algorithmic passwords are currently possible and will play a large role in the future.

Information

- Physical security will become even more important in the protection of information.
- The paradigm today is “protect the data in place.” The paradigm of tomorrow will be “share the data with those authorized but protect it as it travels.”
- Biometric data theft will become the preferred identity theft method.

Privacy

- All your data and personal applications will follow you around (on your person or via internet). They will be available to whatever computer station you are working at.
- Real time satellite imagery will become commonplace and inexpensive for the average person.
- Individual's habits will be tracked through mapping techniques. This will be achieved through satellite surveillance and article tracking (RFID, credit card purchases, etc.).

Privacy

- Consumers, politicians, and CEOs will demand that the security manager protect privacy. The job title will become “Security and Privacy Professional.”
- Security and privacy will be major issues in the 2012 presidential election.
- Privacy will become the ultimate luxury of the future.

“In the future, everyone will be seeking their 15 minutes of anonymity.” -Anonymous

A little farther out:

- In the far future, sea & cargo shipping will become too slow and inefficient, which will lead to the building of a (floating or submerged) trans Atlantic/Pacific rail/tube system. This will lead to a huge increase in cargo speeds (>200 mph). We can then exploit the old adage that “cargo that is moving is safe.”

- Newborns and the general population will be able to have the criminal, violence, and other “anti-social” genes removed via gene replacement therapy.

Other Changes

- China will undergo social chaos with severe economic, security, and geopolitical implications.
- We may see the emergence of "criminal states" that are not merely safe havens for international criminal activities, but support them as a matter of course.
- The criminal world in 2010 may be populated by large interactive networks of smaller, independent organizations who cooperate on the basis of comparative advantage.
- Criminal groups will take advantage of scientific and manufacturing advances to produce new synthetic drugs or more high-quality counterfeit products.
- International criminal groups will keep pace with changes in technology and globalization to enhance their capability in traditional organized crime activities and to move into new criminal business areas.

See: http://www.fas.org/irp/threat/pub45270chap5.html

Argonne
NATIONAL
LABORATORY

... for a brighter future

U.S. Department
of Energy

UChicago ▶
Argonne LLC

A U.S. Department of Energy laboratory
managed by UChicago Argonne, LLC

Things remaining the same:

- High-tech features will continue to fail to address the critical vulnerability issues.
- Users still won't understand the device, this will only get worse as high-tech increases.
- Developers & users will continue to have the wrong expertise and focus on the wrong issues.
- Managers will continue to be over-confident about the difficulty of counterfeiting security devices!
- The "Titanic Effect": high-tech arrogance will continue.

Things remaining the same:

- There will continue to be huge data leaks.
- People will continue to be temped by the latest, greatest high technology.
- Human beings won't change just because the technology does.
- Society will continue to tolerate a small percentage of bad guys and incidents. ~2% levels
- Inventory devices will continue to be foolishly used in security applications (RFID, GPS current examples).

Things remaining the same:

- The Insider Threat will continue to be ignored or underestimated.
- The traditional performance measure for security will remain pathological: success is often defined as nothing happening.
- Objectives will remain often remarkably vague.
- It will still be true that adversaries can attack at one point, but security managers may need to protect extended assets.
- Adversaries will be able to exploit only one or a small number of vulnerabilities, but security mangers will have to identify, prioritize, & manage many vulnerabilities, including unknown ones.

Regulatory; Remains the same

- Bureaucrats will continue to dominate security.
- Policy makers will continue to be reactionary and will continue to ignore human factors in setting security policy and strategies.
- Regulations will continue to follow major security incidences:
  (Prior examples include:)
  - Radio Act 1912 (Titanic): Federal legislation of wireless communications.
  - Glass-Steagall Act (Market Crash 1929): Separation of commercial banks.

    This was repealed by the Gramm-Leach-Bliley Act in 1999.
  - Patriot Act (911): Expanded authority of law enforcement to combat terrorism.
  - Sarbanes-Oxley Act (Enron, Tyco Int., WorldCom): New and enhanced standards for public company boards, management, and public accounting firms.