CS378: Information Assurance and Security

IA in the Military

Dr. Bill Young
Department of Computer Science
University of Texas at Austin

Last updated: February 6, 2015 at 08:38

Why Study the Military

Why study IA in military contexts?

Why Study the Military

Why study IA in military contexts?

- Excellent case study for both defensive and offensive IA.
- Critically important protection domain that affects all of our lives.
- Historically, that's where IA has been developed.
- Most of the lessons of military IA can be adapted to other IA contexts.
- Others (?)

IA in the Military

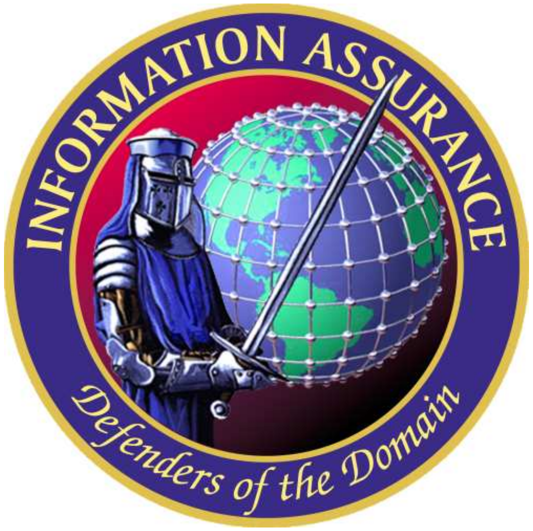
Historically, much of the work in Information Assurance has been contracted/subsidized by the military. Why do you think that is? Why does the government (particularly) care about IA?

IA in the Military

Historically, much of the work in Information Assurance has been contracted/subsidized by the military. Why do you think that is? Why does the government (particularly) care about IA?

- The stakes are high: national security, national prestige, international advantage.
- IA is part of an intelligent defensive/offensive posture.
- The government has deep pockets and can afford to support broader research than other entities.
- Govt. concern for the national welfare goes well beyond strictly military matters. E.g., Financial losses attributable to malicious hacking, online corporate espionage and other computer crimes have a huge impact on commercial activity in this country.
- Others?

U.S. DOD IA Emblem



McAfee Report Findings

McAfee's *Virtual Criminology Report 2009* was focused on cyber warfare. They reported three key findings:

1. Although there is no commonly accepted definition for cyber war today, we have seen nation-states involved in varying levels of cyber-conflict.
2. If a major cyber conflict between nation states were to erupt, it is very likely that the private sector would get caught in the crossfire.
3. Too much of the debate on policies related to cyber war is happening behind closed doors.

1940–1960: IA Prehistory

IA is an outgrowth of (predominately US) military thinking of the role of computers, and more generally, automated info processing in defense.
Initial military uses of computers were cryptography and mathematics

- Electromechanical "Bombe" deciphered Enigma messages.
- ENIAC and later computers were used for computing tables and trajectories.

Most security efforts at that time are focused on physical security and information security on paper and in transmission. Why do you think that's the case?

TEMPEST programs were begun to deal with emissions security, i.e., leaking information via electromagnetic emanations.

1960–1985: Multi-User Systems

Early systems were single-task, single-user machines. The 1960's saw the development of time-sharing and resource-sharing systems, and multi-processing.

What additional security challenges did this introduce?

1960–1985: Multi-User Systems

Military contexts have a specific protection model for document access control.

- Information containers (files) have associated classification levels (CONFIDENTIAL, SECRET, etc.)
- May have additional restrictions (NOFORN, EYES ONLY, etc.).
- Users assigned clearance according to their trustworthiness, job responsibilities.
- Information access may be further compartmented into "need-to-know" categories (CRYPTO, NUCLEAR, etc). Why?

Does this model translate well into the electronic world? Why or why not?

1960–1985: Multi-User Systems

Four models of operation were defined for computers handling classified information:

dedicated: all users cleared for all information on machine; no need for access control (MILS);

system-high: all users cleared, but must obey need-to-know compartments (discretionary access control).

compartmented: all users cleared, but must be need-to-know compartments (mandatory access control). System must handle requests across classifications.

multi-level: not all users cleared for all information; system enforces access control (MLS).

Multi-level is the most difficult so was not widely deployed. RAND Report R-609-1, "Security Controls for Computer Systems," (1970) summarizes best practice.

1985–1990: TCSEC

In 1985, the *Trusted Computer Systems Evaluation Criteria* (Orange Book) established a set of criteria by which the government could evaluate secure computer systems.

- Evaluation criteria for DoD purchase of COTS computer products.
- Criteria had four divisions: D (minimal protection) to A (verified protection), with several classes in most divisions (C1, C2, B1, B2).
- Most commercially viable systems did not seek certification. Why do you think that was?
- Only special purpose network products sought the highest certification levels (A1).

TCSEC was specifically for operating systems. No provisions for evaluating other security-related products.

TCSEC (2)

TCSEC was superceded by Common Criteria, which we'll discuss later in the semester.

"Rainbow series" of books attempted to apply TCSEC across a wider class of products. (see "Rainbow series" on Wikipedia)

Windows NT Workstation and many Unix-based operating systems achieved C2 rating (very weak, and often used configurations only generally of interest to the military).

Only Trusted XENIX and Multics operating systems obtained B2 rating. No general purpose operating system obtained A1 rating, only special purpose network products (Boeing MLS/LAN, Gemini Trusted Network Processor).

1960–1990: Military Networking

Early wide-area networks were based on person-to-person telegram messages, such as AUTODIN, begun in 1962.

ARPANET, for real-time data exchange, establishes first connection in 1969 between two researchers.

Computers on the early ARPANET network at many universities were accessible via dial-up, and these were not particularly secure. (ARPANET's password system was once compromised by two high school students.)

But some threats, such as viruses, were not yet known.

1980–present: Networking

Defense networks began to switch to TCP/IP in 1983. ARPANET was terminated in 1990 and replaced for military purposes by:

NSFNET: (1985–1995) for research, which became the backbone of the Internet.

SIPRNET: network for SECRET communication, has no connection to Internet. (Secret Internet Protocol Router NETwork)

NIPRNET: DoD network for unclassified, but sensitive communication, from which user can access Internet. (Non-classified IPR network)

Highly secure military applications may not be connected to any external network. Example: U.S. Navy submarines connect to SIPRNET only when surfaced and in a non-CSI mission phase.

Nature of the Threat

Cyber war is not occurring right now but nation-states are definitely in competition. Cyber weapons exist, and we should expect that adversaries might use them. –McAfee Virtual Criminology Report 2009, p. 13

America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration that will take office in January 2009. ... It is a battle we are losing. Losing this struggle will wreak serious damage on the economic health and national security of the United States. –CSIS report on Securing Cyberspace for the 44th Presidency, Dec. 2008

Information Warfare

In recent years, conventional combat has been augmented (or replaced) by information warfare—attacking the cyber-infrastructure of the adversary.

> *In the very near future many conflicts will not take place on the open field of battle, but rather in spaces on the Internet, fought with the aid of information soldiers, that is hackers. This means that a small force of hackers is stronger than the multi-thousand force of the current armed forces. –Nikolai Kuryanovich, Russian Deputy of the State Duma, March 2006*

Thus, a large sponsor/consumer of IA activity is the military establishment.

Cyber Warfare

The 2009 Virtual Criminology Report from McAfee says that cyber strikes could have a devastating impact on national infrastructure with power grids, water supplies and financial markets all at risk.

In their 2007 report, McAfee reported that approximately 120 countries have been developing ways to use the Internet as a weapon and target financial markets, government computer systems and utilities.

> *Beijing is increasingly devoting itself to cyberwarfare. This is a cheap way to counter American dominance in traditional military fields. If the U.S. and China ever jostle with force, Beijing may hit us not with missiles but with cyberinfiltrations that shut down the electric grid, disrupt communications and tinker with the floodgates of dams. –Nicholas Kristof, The New York Times, January 18, 2010*

Information Operations

Information Operations actions implement Information Warfare.

1998 *Joint Doctrine for Information Operations* defines IO as: "actions taken to affect adversary information and information systems while defending one's own information and information systems."

Offensive Information Operations

- Target adversary decision makers and control systems
- "May have the greatest impact in peace and the initial stages of a crisis"
- Operations include "hacker brigades" that attempt to infiltrate and compromise adversary's network-accessible systems

Information Operations (2)

Defensive Information Operations:

- Integrates and coordinates policies and procedures, operations, personnel, and technology
- Types of operations include:
  - typical information assurance measures
  - operations security (OPSEC)—a process for protecting information that denies an adversary the ability to compromise it
  - physical security–protection of or with physical assets (e.g. perimeters, mechanical defenses)
  - counterdeception—negating an attacker's deception attempt
  - counterpropoganda—exposing attacker's propoganda

Information Operations Roadmap

In October, 2003, then-Secretary of Defense Donald Rumsfeld issued the *Information Operations Roadmap*, which was initially secret but subsequently released.

Google “Information Operations Roadmap 2003” to see a copy. You’ll note that it’s marked **SECRET/NOFORN**.

The release embarrassed the U.S. government because the document suggested that the U.S. was involved in significant PSYOPS activity, but didn’t distinguish external adversaries from the American public.

The Smith-Mundt Act (1948, amended 1972 and 1998) expressly prohibits the government from propogandizing the American public with information and psychological operations directed at foreign audiences.

Information in War

Information Warfare (IW) is a key scenario for military IA. What does an attack look like? How do I prepare? How do I respond?

Information in War

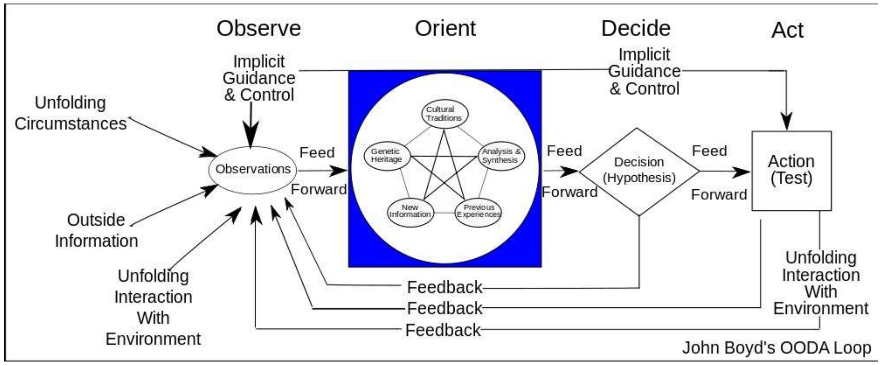
Information Warfare (IW) is a key scenario for military IA. What does an attack look like? How do I prepare? How do I respond?

Military strategist John Boyd came up with a characterization of stategic response to threat called the *OODA Loop.*

- Observe: sensors transmit information about the attack to the commander.
- Orient: the information is interpreted by the commander.
- Decide: the commander forms a plan of operation.
- Act: the plan is carried out.

What do you think are the primary goals of the OODA loop?

OODA Loop



From the Wikipedia page on OODA Loop.

OODA Loop

The OODA Loop was originally applied to the combat operations process, but has been adapted for commercial operations and learning processes.

Ideally, an individual or an organization that can process the cycle quickly, observing and responding to unfolding events can gain a strategic advantage by “getting inside” the opponent’s decision cycle.

Aside: Boyd’s thinking was instrumental in moving the US Air Force from heavy, powerful jet fighters such as the F-4 Phantom to lighter and more responsive jets such as the F-16 Falcon. What is the relationship between OODA and jet fighters?

The OODA Loop

The OODA Loop provides a framework for formulating/evaluating a response, but must take into account whether one can/will respond.

If A launches an attack on B, what factors are likely to influence B’s response?

The OODA Loop

The OODA Loop provides a framework for formulating/evaluating a response, but must take into account whether one can/will respond.

If A launches an attack on B, what factors are likely to influence B’s response?

- *B’s perception of the situation:* based on data and resources available and many other factors.
- *B’s capacity to act:* resources available to B to make a response.
- *B’s will to act:* human factor hardest for A to quantify or affect.

This suggests that an offensive strategy should take these factors into account and attempt to influence them, if possible.

Influencing the OODA Loop

What types of attack are possible?

Influencing the OODA Loop

What types of attack are possible?

- *Physical attack:* destruction intended to reduce B's capacity to respond. (Example: D-Day 1944—massive shelling followed by invasion at Normandy beaches)
- *Deception:* reduces B's effectiveness in responding through distortion, concealment and false indications. (D-Day: fake invasion plans and exercises targeting Pas-de-Calais instead of Normandy)
- *Psychological attack:* cause B to become disoriented. (D-Day: dummy paratroopers dropped behind enemy lines)
- *Information attack:* explicitly target B's sensors and information infrastructure. (D-Day: French resistance and special ops teams cut telephone lines)

Remote access need not include physical force or even physical presence. Can warfare exist primarily at the information level?

Some Information Attacks

First Persian Gulf War (1991): Iraq's command and control infrastructure is targeted. Radar and missile control network is fragmented and sections of radar coverage are taken offline without central control being aware of the outage.

Estonia (2007): Cyberattacks disabled the websites of government ministries, political parties, newspapers, banks, and companies. Russia was suspected of launching the attack in retaliation for the removal of the Bronze Soldier Soviet war memorial in central Tallinn.

Georgia (2008): Russian attacked the nation of Georgia in a dispute over the province of South Ossetia. In addition to the military attack, a concerted cyber DoS attack shut down much of Georgia's ability to communicate with the external world.

Some Information Attacks (2)

Is the U.S. at risk from cyber attack? Do you think that the U.S. has already been attacked?

Some Information Attacks (2)

Is the U.S. at risk from cyber attack? Do you think that the U.S. has already been attacked?
Titan Rain: series of coordinated attacks on American computer systems since 2003. The attacks were labeled as Chinese in origin, although their precise nature (i.e., state-sponsored espionage, corporate espionage, or random hacker attacks) and their real identities are unknown.

Moonlight Maze: series of alleged coordinated attacks on American computer systems in 1999. The attacks were traced to a computer in Moscow but it is not known if that is where they originated. It was claimed, though not certain, that these hackers had obtained large stores of data that might include classified naval codes and information on missile guidance systems.

Credible U.S. security experts suggest that a successful widespread attack on U.S. computing infrastructure could largely shut down the U.S. economy for up to 6 months.

Objectives of Information Warfare

Information dominance: (typically at national level) obtain strategic and battlefield superiority, denying the enemy information or the systems on which to process it.

Information protection: (defensive) protect information systems from attack, and recover when attacks occur.

Information attack: (offensive)

- *Disruption (denial of service):* cause loss of or delay in accessing services
  - Attacks include jamming, physical destruction
  - Targets the *availability* of the information
- *Corruption:* change information or services; targets the *integrity* of the information
- *Exploitation:* gain access to protected information; targets the *confidentiality* of the information.

Examples of Information Attacks

- **International context:** information wars between nations (or proxies)
- **Corporate context:** industrial espionage and sabotage
- **Interpersonal context:** impersonation and identity theft
- **Asymmetric contexts:** terrorism and hacking

CyberWarfare Tactics

According to the Wikipedia article on CyberWarfare, these are the “methods of attack in cyberwarfare,” *ranked from mildest to most severe*.

1. *Cyber espionage:* the act or practice of obtaining secrets from individuals, competitors, rivals, groups, governments and enemies also for military, political, or economic advantage using illegal exploitation methods on internet, networks, software and or computers.
2. *Web vandalism:* attacks that deface web pages, or denial-of-service attacks. This is normally swiftly combated and of little harm.
3. *Propaganda:* political messages can be spread through or to anyone with access to the internet or any device that receives digital transmissions from the Internet to include cell phones, PDAs, etc.

CyberWarfare Tactics (2)

4. *Gathering data:* classified information that is not handled securely can be intercepted and even modified, making espionage possible from the other side of the world. (Titan Rain and Moonlight Maze)
5. *Distributed Denial-of-Service Attacks:* large numbers of computers controlled by one person launch a DoS attack against systems
6. *Equipment disruption:* Military activities that use computers and satellites for coordination are at risk from this type of attack. Orders and communications can be intercepted or replaced, putting soldiers at risk.

CyberWarfare Tactics (3)

7. *Attacking critical infrastructure:* Power, water, fuel, communications, commercial and transportation are all vulnerable to a cyber attack.
8. *Compromised/Counterfeit Hardware:* Common hardware used in computers and networks that have malicious software hidden inside the software, firmware or even the microprocessors.

CyberWarfare Tactics (4)

The Wikipedia article on CyberWarfare ranks these *from mildest to most severe*.

1. Cyber espionage
2. Web vandalism
3. Propoganda
4. Gathering data
5. Distributed denial-of-service attacks
6. Equipment disruption
7. Attacking critical infrastructure
8. Compromised/counterfeit hardware

Do you agree with this ordering? Could it possibly be that compromised/counterfeit hardware is more of a threat than attacking critical infrastructure?

CyberWarfare Tactics (5)

According to the Wikipedia article, the most severe attack strategy in CyberWarfare is: Compromised/Counterfeit Hardware. Is that really a problem? Does it even happen?

CyberWarfare Tactics (5)

According to the Wikipedia article, the most severe attack strategy in CyberWarfare is: Compromised/Counterfeit Hardware. Is that really a problem? Does it even happen?

December 2009: “A federal grand jury has indicted four people accused of selling counterfeit Cisco Systems Inc. computer hardware through their Colorado-based company.”

How is this relevant to CyberWarfare?

2008 DefenseTech Article

From: `defensetech.org/2008/04/01`:

> *Recent events have raised the concerns about hidden backdoors and malicious code inside of counterfeit hardware all the way down to the integrated circuit level. In fact, a 2005 report by the Pentagon's Defense Science Board addresses this issue. While this report assessed the problem, recent events have now raised the anxiety over cyber sabotage in bogus hardware. In fact, many consider the use of compromised counterfeit hardware as a strategic tactic in cyber warfare. In January of 2008, a joint task force seized $78 million of counterfeit Cisco networking hardware. This international effort resulted in over 400 seizures of counterfeit networking hardware that was shipped between China, Canada and the United States.*

The Acquisition Problem

In addition to direct attacks on the national cyberstructure, the U.S. military is a consumer of vast amounts of commercial hardware/software. This is called *acquisition*, *procurement* or *supply chain*. Where do these products come from? How do we know they're reliable? Can we even tell? Is this just a problem for the military?

The Acquisition Problem

In addition to direct attacks on the national cyberstructure, the U.S. military is a consumer of vast amounts of commercial hardware/software. This is called *acquisition*, *procurement* or *supply chain*. Where do these products come from? How do we know they're reliable? Can we even tell? Is this just a problem for the military?

The trend in government acquisition is toward commercial-off-the-shelf (COTS) products and services.

- (1991) Sec. of Defense Perry announces DoD Strategic Acquisition Initiative mandating a preference for COTS products.
- (1997) Sec. of Defense Cohen launches Defense Acquisition Reform Initiative that accelerated the preference for COTS in defense acquisition.

What do you think motivated this preference for COTS over GOTS or contract developments?

Advantages of COTS Products

Preference for COTS products aims to obtain the latest technology at reduced cost, with shorter development and refresh cycles, and to leverage commercial investment and commercial best practices. Do you think this is an an effective strategy?

Advantages of COTS Products

Preference for COTS products aims to obtain the latest technology at reduced cost, with shorter development and refresh cycles, and to leverage commercial investment and commercial best practices. Do you think this is an an effective strategy?

Experience has shown that COTS products are often more:

- flexible
- scalable
- configurable
- maintainable

than products produced solely for the government

These benefits are exemplified by a reported *ten-fold reduction in price for U.S. Navy submarine sonar and combat systems over a ten year period*, with significantly enhanced capabilities. (Stevens)

So What's the Downside

How could compromised hardware/software cause problems?

So What's the Downside

How could compromised hardware/software cause problems?

An adversary intent on damaging U.S. national interests might insert unauthorized or damaging functionality which could be:

active: code that

- alters the behavior of critical systems,
- exfiltrates sensitive information,
- modifies programs or data,
- crashes a machine or network

passive: e.g., a backdoor to allow a future intruder to bypass the security protections of the system.

Role of Acquisitions Policy

One of the CSIS recommendations "to make a noticeable improvement in the nations cybersecurity" is:

> *Use acquisitions policy to improve security. The federal government is the largest single consumer of information technology products. We recommend that the United States buy only secure products and services; standards and guidelines for secure products should be developed in partnership with industry. (CSIS report, p. 2)*

Well, isn't that the solution to the acquisition problem? Just buy only secure products. So, what's the problem?

Product Evaluation

> *Trust, but verify. – Ronald Reagan*

Question: Isn't that what vulnerability scanners are for? Can't we just implement methods to ensure that acquired systems do not contain exploitable vulnerabilities?

Product Evaluation

Trust, but verify. – Ronald Reagan

Question: Isn't that what vulnerability scanners are for? Can't we just implement methods to ensure that acquired systems do not contain exploitable vulnerabilities?

Answer: Not completely. The problem of detecting arbitrary malicious functionality is *undecidable*—there is no algorithm that can reliably distinguish between malicious and benign code.

Malicious Software

Ken Thompson (1984 Turing Award lecture) noted that even complete control over source code is not sufficient to ensure the absence of malicious functionality, which can be introduced by the compiler, linker, loader, assembler, microcode, and even hardware.

> *You can't trust code that you did not completely create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code. [...] As the level of program gets lower, these bugs will be harder and harder to detect. A well-installed microcode bug will be almost impossible to detect. –Ken Thompson*

But We Can Try

Example: The U.S. Army requires that all systems receive a "certificate of networthiness" (CoN) before being deployed on Army networks.

According to the Army's *Networthiness Certification Program for Information Systems*, networthiness encompasses:

> *network security, network impact, compatibility with the total infrastructure, infrastructure requirements, spectrum support, security policy compliance, Foreign Ownership and Influence (FOCI), Joint Technical Architecture-Army (JTA-A) standards compliance, communications and information manpower, training, logistics support, schedule, and funding.*

The Army currently has a backlog of several thousand applications awaiting CoN evaluation by the 3 or so guys working for the Certification Program.

Some Sobering Facts

- A recent study of 32,000 Websites found that *nearly 97% of sites carry a severe vulnerability*. –Web Application Security Consortium, Sept 2008
- "NSA found that inappropriate or incorrect software security configurations (most often caused by configuration errors at the local base level) were responsible for 80 percent of Air Force vulnerabilities." –CSIS report on *Securing Cyberspace for the 44th Presidency*, Dec. 2008, p. 55.
- "Some U.S. government computer systems have shown significant security lapses." –Bagchi, et al., Summer 2005

But the fact that these statistics are available at all implies that significant classes of vulnerabilities can be detected.

There is Some Hope

The fact that a problem is undecidable *doesn't mean that there aren't useful steps that can be taken.*

Most vulnerabilities in software systems were introduced inadvertantly rather than maliciously. In many cases, it is impossible to distinguish the two.

> *Sufficiently advanced incompetence is indistinguishable from malice. –Prof. Hovav Shachem*

Historically, most vulnerabilities have not been recognized as such until someone discovered a way to exploit them.

> *A good attack is one that the engineers never thought of. –security guru Bruce Schneier*

There is Some Hope

The most common approach is *vulnerability scanning*, which seems to be the main approach of the Army currently. Several automated scanners are used by the CoN certifiers:

- **Nessus**: proprietary network scan tool, easily configured with plugins, available for Windows and Unix platforms.
- **Retina**: commercial network monitoring tool (Windows, Unix, others).
- **DISA Gold**: detect, report and remediate vulnerabilities in Windows.

There are many other tools out there. How could you decide what tools are the most appropriate? What factors enter into the decision?

The Problem

> *As we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns—the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones. –Donald Rumsfeld, Secy of Defense*

Scanners are excellent tools for discovering *known vulnerabilities*, but a sophisticated adversary will craft the attack until it defeats the scanners. Explain.

Example: In tests of 36 commercial anti-virus products, fewer than half of the newest malicious software programs were identified. (research by Stuart Staniford of FireEye, Nov. 2008) What's the lesson here?

Vulnerability Scanners

Vulnerability scanning has the following weaknesses:

- Scanners only test for known vulnerabilities; may not be effective against zero-day attacks.
- Only applicable to testable vulnerabilities; some may trigger on specific environmental conditions.
- Report presence/absence of vulnerabilities not potential for damage; e.g., foothold scenarios.
- May be limited to vulnerabilities on individual machines; some require a network of machines to exploit.

Explain zero-day attacks and foothold scenarios. How would you go about countering zero-day attacks?

Dimensions of the Analysis

There are multiple dimensions in which to evaluate an analysis methodology.

Objects of analysis: What artifacts are available to the analyst—code (source, intermediate or object), an executable system, test vectors, etc.?

Depth of analysis: How thorough is the analysis carried out with any given tool?

Required skillset: What expertise is required to use a given tool effectively?

Precision and accuracy: Are specific methods likely to find all and/or only genuine vulnerabilities?

Depth of Analysis

Another key dimension is how deep is the analysis.

Black box methods: take a purely external perspective on the object of analysis without knowledge of the internal details.

Gray box methods: apply limited knowledge of the internal working of the object to guide the analysis.

White box methods: relies on internal knowledge of the software to guide the analysis.

These categories are typically applied to generation of test cases, but can be applied to any analysis methods. Why would you ever use a more shallow analysis if a deeper analysis is possible?

Depth of Analysis

Another key dimension is how deep is the analysis.

Black box methods: take a purely external perspective on the object of analysis without knowledge of the internal details.

Gray box methods: apply limited knowledge of the internal working of the object to guide the analysis.

White box methods: relies on internal knowledge of the software to guide the analysis.

These categories are typically applied to generation of test cases, but can be applied to any analysis methods. Why would you ever use a more shallow analysis if a deeper analysis is possible?

Which to use depends crucially on the available time and resources, toolset, artifacts for analysis, etc.

Precision vs. Accuracy

We say that a vulnerability detection scheme is

Precise: if it never reports legitimate functionality as harmful, i.e., *no false positives*;

Accurate: if it detects all genuine vulnerabilities, i.e., *no false negatives*.

It is easy to build a scheme that is either accurate or precise; it's hard to do both simultaneously. Why?

Which is worse: false positives or false negatives? How would you go about estimating the rate of false positives/negatives in your system?

Base-Rate Fallacy

When searching for events that are relatively rare in a population, even a moderately accurate detection scheme will return a high proportion of false positives.

Example: Suppose that only 1% of traffic is attacks and the detection accuracy is 90%. What percentage of raised alarms do you think will be false alarms?

Base-Rate Fallacy

When searching for events that are relatively rare in a population, even a moderately accurate detection scheme will return a high proportion of false positives.

Example: Suppose that only 1% of traffic is attacks and the detection accuracy is 90%. What percentage of raised alarms do you think will be false alarms?

Approximately 92% of raised alarms will be false alarms.

What conclusions can you draw from this analysis?

Useful systems often have parameters that can be tuned to adjust the levels of false positives and false negatives depending on the environment and threat profile.