Argonne NATIONAL LABORATORY | Nuclear Engineering Division

Sticky Bomb Detection

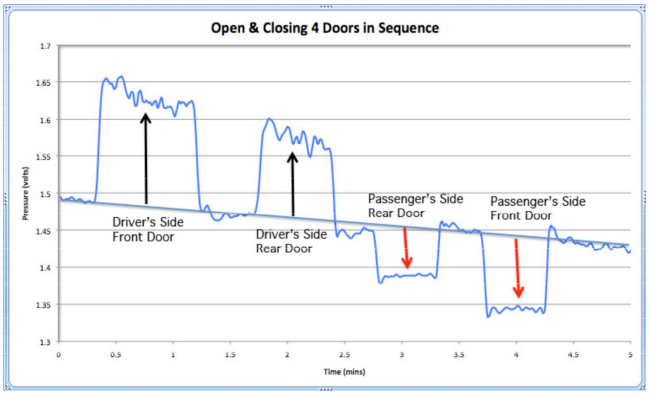
"Sticky bombs" are a type of improvised explosive device (IED), typically placed on a motor vehicle by a terrorist.

Tire Pressure

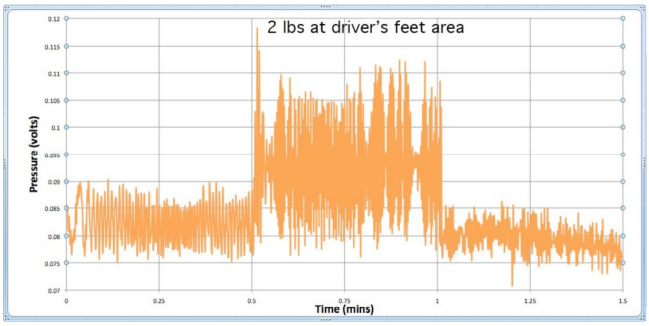
The Vulnerability Assessment Team (VAT) at Argonne National Laboratory has demonstrated that precisely monitoring the pressure in a tire makes it possible to detect a change of less than 5 ounces in the weight of a parked motor vehicle and its contents. This can be used to detect:

- placement of a sticky bomb
- placement of a surreptitious tracking device
- placement of a surreptitious eavesdropping device
- theft from the vehicle
- tampering with the vehicle
- intrusion into the vehicle
- which door was opened
- a person lurking or hiding in the vehicle

Even better sensitivity is possible with further work.



While monitoring the tire pressure on the front driver's side tire, each of the 4 car doors are opened, then closed in sequence. The magnitude and sign of the pressure change can be used to determine which door was opened. (Opening a passenger-side door causes a negative pressure change because the vehicle leans in the opposite direction compared to when a driver's-side door is opened.)



Relative tire pressure vs. time. A 2 lb weight is added to the parked vehicle at 0.5 minute, then removed at 1 minute.

Magnetic Detection

Sticky bombs or surreptitious electronic tracking devices are sometimes placed on vehicles using magnets. The VAT has demonstrated that inexpensive magnetic sensors can detect the magnets on parked vehicles.

Moving Vehicles

The magnetic technique should work well on moving vehicles. (AC magnetic fields and movement within the Earth's magnetic field do not cause problems.)

The tire pressure technique can potentially work on moving vehicles if an accelerometer and thermal measurements are used to correct for road vibration. The sensitivity, however, is likely to be less.

VAT Awards

The Argonne Vulnerability Assessment Team has won numerous awards. A partial list includes:

* 10 U.S. patents
* BECCA Honorary CCO Award for contributions to homeland security, 2009
* LANL Fellows Prize for Outstanding Research, 2004
* LANL Achievement Awards, 2007, 2004, 1999 & 1995
* Distinguished Performance Award from the CIA, 2002
* "Excellence in Performance Measure" Award, American Society for Industrial Security, 2002
* LANL Distinguished Performance Awards, 2001 & 1996
* Excellence in Technology Transfer Awards, 1997 & 1992
* R&D 100 National Awards, 1992 & 1994
* "Best of What's New Award", Popular Science, 1992

About Argonne National Laboratory

Argonne National Laboratory, the nation's first national laboratory, is one of the U.S. Department of Energy's largest national laboratories for science and engineering research. Argonne has approximately 3,000 employees, including 1,000 scientists and engineers, three-quarters of whom hold doctoral degrees. Argonne's annual operating budget exceeds $630 million. Since 1990, Argonne has worked with more than 600 companies, federal agencies, and other organizations.

Currently, 16% of Argonne's budget is for intelligence, defense, and homeland security projects (up from 6% before September 11, 2001). The long-term goal is to significantly increase this percentage.

Argonne is managed by UChicago, LLC, for the U.S. Department of Energy.

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov

Argonne NATIONAL LABORATORY | Nuclear Engineering Division

Detecting GPS Spoofing

It's easy to generate fake GPS time and location signals using widely available GPS satellite simulators. This spoofing can be detected with $15 of parts.

The Problem

Almost everybody (including most of DoD) must use the civilian Global Positioning System (GPS) signals. Unlike the military signals, these are not encrypted or authenticated, and were never intended for critical security applications. Yet civilian GPS is being used that way!

As we have demonstrated in the Vulnerability Assessment Team at Argonne National Laboratory, it is easy for an adversary to generate fake GPS signals using widely available (non-export controlled) GPS satellite signals.

The Threat of Undetected GPS Spoofing

With GPS spoofing (not jamming), an adversary can:

- Crash national utility, financial, telecommunications & computer networks that rely on GPS for critical time synchronization
- Steal cargo or nuclear material being tracked by GPS
- Install false time stamps in security videos or financial transactions
- Send emergency response vehicles to the wrong location after a terrorist attack
- Interfere with military logistics (DoD uses civilian GPS for most cargo)
- Interfere with battlefield soldiers using civilian GPS (against DoD policy, but common)
- Spoof GPS ankle bracelets used by courts
- Spoof GPS data loggers used for law enforcement and counter-intelligence

The Solution

Signals from GPS satellite simulators have artificial characteristics allowing them to be recognized as fake. These include:

- wrong time
- suspiciously low noise
- excessive signal strength
- artificial spacing of signals
- all satellites have the same signal strength
- wrong or no time variation in signal strength
- reported accelerations don't pass a sanity check

For More Information

JS Warner & RG Johnston, *The Journal of Security Administration* 25, 19-28 (2002).

JS Warner & RG Johnston, *Homeland Security Journal*, December 12, 2003.

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov

Argonne NATIONAL LABORATORY | Nuclear Engineering Division

Vulnerability Assessments of Biometrics & Other Access Control Devices

The Vulnerability Assessment Team is probably the most impressive physical security research team in the world.

-- Prof. Ross Anderson of Cambridge University,
author of the classic textbook *Security Engineering*

Vulnerability Assessments

The Vulnerability Assessment Team (VAT) at Argonne National Laboratory (formally at Los Alamos from 1992-2007) has conducted vulnerability assessments on hundreds of different physical security devices, systems, and programs. This includes locks, tags, seals, RFIDs, GPS, microprocessor systems, contact memory buttons, electronic voting machines, and biometrics and other access control devices. The VAT has demonstrated how all these can be easily defeated using widely available tools, materials, and supplies, but has also devised and demonstrated simple and practical countermeasures.

In addition, the VAT has provided security consulting, training, R&D, reverse engineering, specialty field tools, and novel security devices/strategies for more than 40 different companies and government organizations, including DoD, DOE/NNSA, DHS, U.S. Department of State, the International Atomic Energy Agency (IAEA), Euratom, and the intelligence community.

Biometrics

The VAT has devised and demonstrated successful attacks and countermeasures for more than a dozen different biometric devices and systems, including those based on fingerprints, hand geometry, and iris patterns. The VAT did some of the earliest research on iris biometrics.

A multidisciplinary team of scientists, engineers, ethical hackers, and social scientists

VAT Resources & Capabilities

- Top Secret security clearances
- Access to 2 SCIFs + a new SCIF under construction
- 18+ years of experience with vulnerability assessments
- One-of-a-kind Vulnerability Assessment Laboratory
- 1200 square feet of classified VTR laboratory space
- 2000 square feet of other office & laboratory space
- Unique VAT microprocessor rapid prototyping shop
- Experience with the successful completion of $25 million of classified & unclassified projects since 1992
- Access to multidisciplinary, world-class science & engineering expertise at all the DOE national laboratories

Argonne NATIONAL LABORATORY | Nuclear Engineering Division

Tampering with Drug Tests

The Argonne Vulnerability Assessment Team:
Internationally recognized expertise in tags, seals, cargo security, & physical tamper/intrusion detection

The Problem

We've demonstrated that 23 of the most popular urine testing vials and kits are easy to tamper with, including those used by DOE, DoD, and sports authorities.

These results are presented in a paper in the *Journal of Drug Issues* (in press). The paper also calls into question the security protocols commonly used for urine drug testing by the federal government and national/international sports authorities. The paper warns that there has been insufficient concern about the risk of malicious false positive results.

Better Approaches

Given that drug test results are critical, affecting national security, public safety, and the careers, livelihood, and reputation of employees and athletes, much better security would seem warranted.

The Vulnerability Assessment Team (VAT) at Argonne National Laboratory has considerable expertise in developing better tamper-indicating seals and security protocols.

About Argonne National Laboratory

Argonne National Laboratory, the nation's first national laboratory, is one of the U.S. Department of Energy's largest national laboratories for science and engineering research. Argonne has approximately 3,000 employees, including 1,000 scientists and engineers, three-quarters of whom hold doctoral degrees. Argonne's annual operating budget exceeds $630 million. Since 1990, Argonne has worked with more than 600 companies, federal agencies, and other organizations.

Currently, 16% of Argonne's budget is for intelligence, defense, and homeland security projects (up from 6% before September 11, 2001). The long-term goal is to significantly increase this percentage.

Argonne is managed by UChicago, LLC, for the U.S. Department of Energy.

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov

Argonne NATIONAL LABORATORY | Nuclear Engineering Division

Better Tamper-Indicating Seals

Anti-Evidence Seals:
Fundamentally a better way to do tamper detection.

Tamper-Indicating Seals

The Vulnerability Assessment Team (VAT) at Argonne National Laboratory has devised and demonstrated easy defeats for hundreds of different tamper-indicating seals, including those used for high-level security applications and nuclear safeguards. As a result of this work, the VAT believes much better seals are possible, and has developed over 20 new kinds. Some have received U.S. patents.

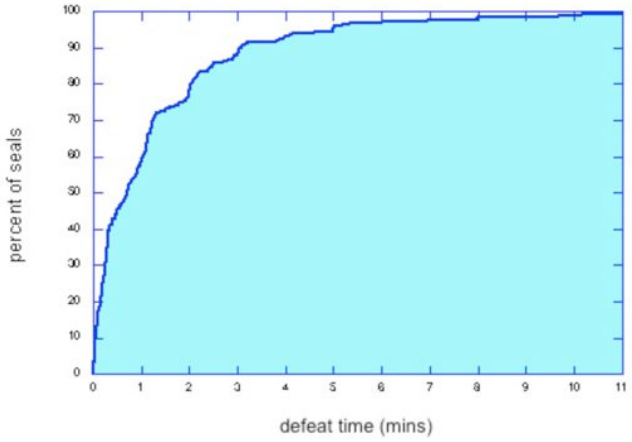
The Anti-Evidence Approach

Most of these new seals are based on the VAT's "anti-evidence" approach to tamper detection. In a conventional seal, the fact that the seal has been opened must be stored in or on the seal until such time as it can be inspected. But it is usually easy for an adversary to replace the original seal with a counterfeit, or else hide or erase this 'alarm condition' in the original seal.

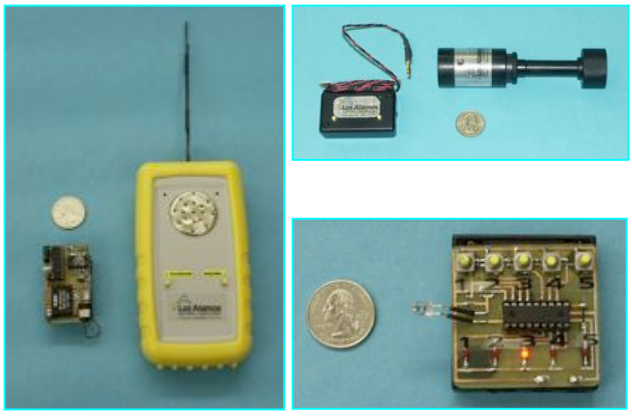
With an anti-evidence seal, in contrast, we store secret information (typically a byte) in or on the seal indicating that tampering has not yet occurred. When tampering is detected, this information gets instantly erased. As a result, counterfeiting is of no value to an adversary if he doesn't know what information to put in or on the seal.

Advantages

Advantages of the anti-evidence approach include better security, as well as simplicity & low cost, volumetric intrusion detection, no need for a hasp, and "anti-gundecking" features.



Percentage of 244 different conventional seals that can be spoofed (defeated) in less than a given amount of time by 1 person, working alone, using only low-tech tools, methods, and supplies. These 244 seals include high-tech seals and those used for nuclear safeguards.



Various VAT anti-evidence seal prototypes

VAT Resources & Capabilities

- Top Secret security clearances
- Access to 2 SCIFs + a new SCIF under construction
- 18+ years of experience with vulnerability assessments and tamper detection
- One-of-a-kind Vulnerability Assessment Laboratory
- 1200 square feet of classified VTR laboratory space
- 2000 square feet of other office & laboratory space
- Unique VAT microprocessor rapid prototyping shop
- Experience with the successful completion of $25 million of classified & unclassified projects since 1992
- Access to multidisciplinary, world-class science & engineering expertise at all the DOE national laboratories

VAT Awards

The Argonne Vulnerability Assessment Team has won numerous awards. A partial list includes:

* 10 U.S. patents
* BECCA Honorary CCO Award for contributions to homeland security, 2009
* LANL Fellows Prize for Outstanding Research, 2004
* LANL Achievement Awards, 2007, 2004, 1999 & 1995
* Distinguished Performance Award from the CIA, 2002
* "Excellence in Performance Measure" Award, American Society for Industrial Security, 2002
* LANL Distinguished Performance Awards, 2001 & 1996
* Excellence in Technology Transfer Awards, 1997 & 1992
* R&D 100 National Awards, 1992 & 1994
* "Best of What's New Award", Popular Science, 1992

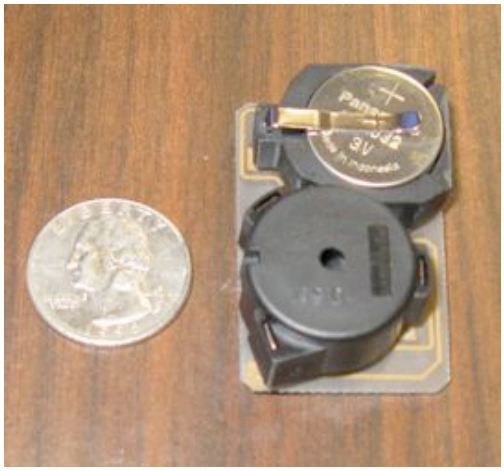
About Argonne National Laboratory

Argonne National Laboratory, the nation's first national laboratory, is one of the U.S. Department of Energy's largest national laboratories for science and engineering research. Argonne has approximately 3,000 employees, including 1,000 scientists and engineers, three-quarters of whom hold doctoral degrees. Argonne's annual operating budget exceeds $630 million. Since 1990, Argonne has worked with more than 600 companies, federal agencies, and other organizations.

Currently, 16% of Argonne's budget is for intelligence, defense, and homeland security projects (up from 6% before September 11, 2001). The long-term goal is to significantly increase this percentage.

Argonne is managed by UChicago, LLC, for the U.S. Department of Energy.

Time Trap: an anti-evidence tag & seal.



Prototype Chirping Tag & Seal

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov

Argonne NATIONAL LABORATORY | Nuclear Engineering Division

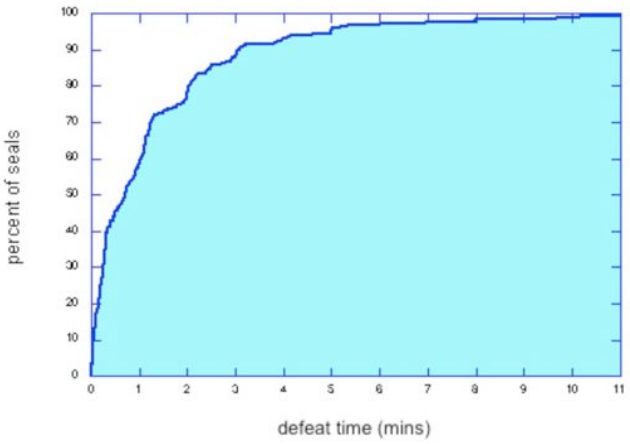
Countering Tampering & Counterfeiting

The Argonne Vulnerability Assessment Team:
Internationally recognized expertise in tags, seals, anti-counterfeiting, cargo security, nuclear safeguards, & physical tamper/intrusion detection.

Vulnerability Assessments

The Vulnerability Assessment Team (VAT) at Argonne National Laboratory (formally at Los Alamos from 1992-2007) has conducted vulnerability assessments on hundreds of different physical security devices, systems, and programs. This includes locks, tags, seals, RFIDs, GPS, microprocessor systems, contact memory buttons, electronic voting machines, and biometrics and other access control devices. The VAT has demonstrated how all these can be easily defeated using widely available tools, materials, and supplies, but has also devised and demonstrated simple and practical countermeasures.

In addition, the VAT has provided security consulting, training, R&D, reverse engineering, specialty field tools, and novel security devices/strategies for more than 40 different companies, NGOs, and government organizations, including DoD, DOE/NNSA, DHS, U.S. Department of State, the International Atomic Energy Agency (IAEA), Euratom, and the intelligence community.



Percentage of 244 different seals that can be spoofed (defeated) in less than a given amount of time by 1 person, working alone, using only low-tech tools, methods, and supplies. These 244 seals include high-tech seals and those used for nuclear safeguards.

Tamper-Indicating Seals

The VAT has devised and demonstrated successful attacks and countermeasures for hundreds of different tamper-indicating seals. As a result of this work, the VAT has developed improved training, seal use protocols, and novel kinds of seals. These new seals are based on the VAT's "anti-evidence" approach to tamper detection. Advantages include better security, simplicity & low cost, volumetric intrusion detection, no need for a hasp, and "anti-gundecking" features.

Some of these new seals are: the Talking Truck Cargo Seal, Tempered Glass Seal, Time Trap, Tie-Dye Seal, Chirping Seal, DTMF Watch Seal, Skunk Seal, MagTag, Magic Slate Seal, and the Triboluminescence Seal.

Novel Anti-Counterfeiting Approaches

The VAT has proposed and developed a number of new techniques for countering product (and other kinds) of counterfeiting, including:

Virtual Numeric Tokens [RG Johnston, "An Anti-Counterfeiting Strategy Using Numeric Tokens", International Journal of Pharmaceutical Medicine *19, 163-171 (2005)]*

Time Trap (authenticity & tamper detection with one device)

Wine Anti-Tampering and Anti-Counterfeiting Device

VAT Resources & Capabilities

- Top Secret security clearances
- Access to 2 SCIFs + a new SCIF under construction
- 18+ years of experience with vulnerability assessments
- One-of-a-kind Vulnerability Assessment Laboratory
- 1200 square feet of classified VTR laboratory space
- 2000 square feet of other office & laboratory space
- Unique VAT microprocessor rapid prototyping shop
- Experience with the successful completion of $25 million of classified & unclassified projects since 1992
- Access to multidisciplinary, world-class science & engineering expertise at all the DOE national laboratories

The Time Trap anti-evidence tag & seal.

A new cap invented by the VAT can detect counterfeit or tampered wine. By plugging the cap into a computer through a USB cable, a wine buyer or auctioneer can check if the wine inside is genuine and undisturbed.

VAT Awards & Recognition

The Argonne Vulnerability Assessment Team has won numerous awards and received widespread recognition. A partial list includes:

* 10 U.S. patents
* Interviewed by the Wall Street Journal (front page), NPR, CSO, RFID Journal, Homeland Security Alert, IOMA Security Director's Report, Mechanical Engineering, Business Travel Executive, Pharma Manufacturing, etc.
* BECCA Honorary CCO Award for contributions to homeland security, 2009
* LANL Fellows Prize for Outstanding Research, 2004
* LANL Achievement Awards, 2007, 2004, 1999 & 1995
* Distinguished Performance Award from the CIA, 2002
* "Excellence in Performance Measure" Award, American Society for Industrial Security, 2002
* LANL Distinguished Performance Awards, 2001 & 1996
* Excellence in Technology Transfer Awards, 1997 & 1992
* R&D 100 National Awards, 1992 & 1994
* "Best of What's New Award", Popular Science, 1992

Sample Publications

RG Johnston, EC Michaud, and JS Warner, "The Security of Urine Drug Testing", Journal of Drug Issues*, (in press).*

RG Johnston, "Layered Security: Self-Defense or Self-Delusion?", *Security Management* (in press).

EG Bitzer, PY Chen, and RG Johnston, "Security in Organizations: Expanding the Frontiers of Industrial-Organizational Psychology", International Review of Industrial and Organizational Psychology *24, 131-150 (2009).*

RG Johnston, "Tamper-Indicating Seals", *American Scientist* 94, 515-523 (2006).

RG Johnston, "New Research on Tamper-Indicating Seals", International Utilities Revenue Protection Association News, 16, 17-18 (2006).

RG Johnston and JS Warner, "The Dr. Who Conundrum: Why Placing Too Much Faith in Technology Leads to Failure", *Security Management* 49, 112-121 (2005).

RG Johnston, "The 'Anti-Evidence' Approach to Tamper-Detection", *Packaging, Transport, Storage & Security of Radioactive Material* 16(2), 135-143 (2005).

JS Warner and RG Johnston, "A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing", *The Journal of Security Administration* 25, 19-28 (2002).

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov

Sample Invited Talks

"Security Against Theft, Tampering, and Counterfeiting", General Assembly of the Pharmaceutical Security Institute, Mclean, VA, October 28, 2009.

(Keynote Address) "The Importance of Not Being Earnest", SecureWorld Expo, San Francisco, CA, September 19-20, 2007.

"Pharmaceutical Security & Authenticity", Pharamaceutical Supply Chain Integrity Conference, Baltimore, MD, April 25-27, 2007.

"Vulnerabilities & Limitations of RFID and Contact Memory Devices", IAEA Technical Meeting on Sealing Systems and Containment Verification Methods, Vienna, Austria, February 12-16, 2007.

"Countermeasures to Wishful Thinking", ASIS International Middle East Security Conference, Manama, Bahrain, December 4-6, 2006.

Vulnerability Assessments on Tamper-Indicating Seals", Joint US-Russia TID Working Group, Moscow, Russia, September 13-14, 2006.

"Research on Improving Cargo Security", 5th North American Cargo Security Forum, Washington, D.C., September 6-7, 2006.

About Argonne National Laboratory

Argonne National Laboratory, the nation's first national laboratory, is one of the U.S. Department of Energy's largest national laboratories for science and engineering research. Argonne has approximately 3,000 employees, including 1,000 scientists and engineers, three-quarters of whom hold doctoral degrees. Argonne's annual operating budget exceeds $630 million. Since 1990, Argonne has worked with more than 600 companies, federal agencies, and other organizations.

Currently, 16% of Argonne's budget is for intelligence, defense, and homeland security projects (up from 6% before September 11, 2001). The long-term goal is to significantly increase this percentage.

Argonne is managed by UChicago, LLC, for the U.S. Department of Energy.

Argonne NATIONAL LABORATORY

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov

Argonne NATIONAL LABORATORY | Nuclear Engineering Division

Handbook of Security Blunders

By Roger G. Johnston, Ph.D, CPP and Jon S. Warner, Ph.D.
(the editors of the *Journal of Physical Security)*
Available February 2010

The Weakest Link

There's an old adage that your security is only as good as the weakest link. This makes sense because adversaries typically attack where there are problems, not at random.

Thus, when conventional security books focus on how to have effective security, they often overlook the fact that what you get right about security is often less important than what you get wrong.

Security Mistakes

The Vulnerability Assessment Team (VAT) at Argonne National Laboratory (formerly at Los Alamos from 1992-2007) has conducted vulnerability assessments on hundreds of different security systems, devices, and programs. We keep seeing the same kinds of mistakes.

The Handbook of Security Blunders lists and discusses over 1,000 serious security mistakes that the VAT has seen repeatedly.

Topic areas include Security Strategy, Security Culture & Climate, Organizational Security, Security Management & Supervision, Cyber Security, The Insider Threat, Social Engineering, Building Security, Access Control & Biometrics, Locks, Seals, Tags, Cargo Security, Product Counterfeiting, Choosing Security Products, Vulnerability Assessments, Risk Management, Nuclear Safeguards, Security Device & System Design, Business/Financial Security, and Personal Security.

The book concludes with a glossary of over 800 security terms that every security professional should know.

VAT Awards & Recognition

The Argonne Vulnerability Assessment Team has won numerous awards and received widespread recognition. A partial list includes:

- 10 U.S. patents
- Over 60 invited talks at national and international conferences, including Keynote Addresses
- Interviewed by the *Wall Street Journal* (front page), NPR, *CSO, RFID Journal, Homeland Security Alert, IOMA Security Director's Report, Mechanical Engineering, Business Travel Executive, Pharma Manufacturing*, etc.
- BECCA Honorary CCO Award for contributions to homeland security, 2009
- LANL Fellows Prize for Outstanding Research, 2004
- LANL Achievement Awards, 2007, 2004, 1999 & 1995
- Distinguished Performance Award from the CIA, 2002
- "Excellence in Performance Measure" Award, American
- Society for Industrial Security, 2002
- LANL Distinguished Performance Awards, 2001 & 1996
- Excellence in Technology Transfer Awards, 1997 & 1992
- R&D 100 National Awards, 1992 & 1994
- "Best of What's New Award", Popular Science, 1992

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov

Argonne NATIONAL LABORATORY | Nuclear Engineering Division

Key Keepaway

Securing a secret key by keeping its fragments in motion.

The Problem

When physical or electronic intrusion is detected, a secret, electronic key often needs to be erased. It is difficult to do this quickly enough & reliably (given data remanence), especially for large (256 byte) keys needed for high security encryption & equipment.

The Solution

Portions of the secret key bounce around in a microprocessor circuit or microprocessor wheel in a complex, unpredictable manner.

Quantum noise is used (or else a chaotic, non-linear, recursive equation) to direct where portions of the key go. Neither the central microprocessor nor the designer/programmer knows where the key fragments are at any given time.

To reassemble the key, the CPU issues a reassemble command and waits for the key portions to show up randomly, typically 0.5 seconds later vs. << 1 microsecond to destroy the key.

Key storage is dynamic so information is lost mid-transfer when erasure is called for. The microprocessor also has a non-graceful shutdown behavior on power loss.

Data remanence is much less of a risk with this dynamic, chaotic approach.

The Vulnerability Assessment Team

The award-winning Vulnerability Assessment Team (VAT) at Argonne National Laboratory (formerly at Los Alamos from 1992-2007) provides security consulting, training, vulnerability assessments, and R&D to a wide range of sponsors. Examples include DoD, DOE/NNSA, U.S. Department of State, IAEA, Euratom, intelligence agencies, NGOs, and private companies.

The VAT resources include top secret security clearances, a unique Vulnerability Assessment Laboratory, 3200 square feet of laboratories and office space including 2000 square feet of VTR laboratories for classified work, a rapid prototyping microprocessor shop, and access to 2 SCIFs (with a third one under construction). The VAT has successfully completed $25 million of classified and unclassified projects since 1992.

Argonne NATIONAL LABORATORY

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov

Argonne NATIONAL LABORATORY | Nuclear Engineering Division

Assuring the Veracity of Monitoring Data

See RG Johnston, MJ Timmons, and JS Warner, *Science & Global Security* 15, 185-189 (2007).

Conventional Techniques Are Not Secure

When data is logged in the field, such as with GPStrackers or nuclear safeguards monitoring equipment, it is not safe from tampering because:

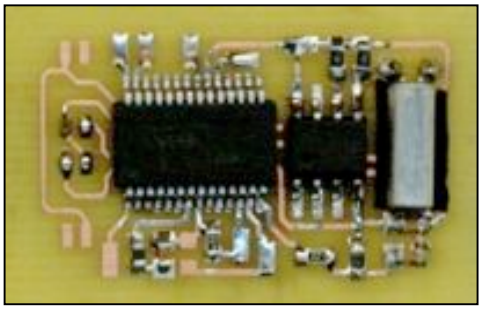
1. Conventional physical/electronic tamper and intrusion detection techniques are too easy to defeat (as shown by the Argonne Vulnerability Assessment Team and others).
2. The encryption or data authentication key cannot be erased quickly enough, even if intrusion is detected.
3. The encryption or data authentication key cannot be erased reliably enough, even if intrusion is detected, because of data remanence problems.
4. A sophisticated adversary can break the cipher even without knowing the key because he has knowledge of the algorithm and all or some of the plaintext.

OPODS: A Better Approach

OPODS stands for "Onetime Pad of Digit Substitutions". It is a stream cipher based on the only unbreakable cipher—the one time keypad.

Advantages include:

- Much better security than conventional ciphers or MACs when physical security & tamper detection is poor (as is usually the case).
- Data recorded prior to trespassing cannot be modified; data after trespassing is not as secure but is difficult to fake.
- The data is quite secure even if the trespassing or tampering goes undetected.



- It's a fast algorithm (not computationally intensive).
- Cheap & easy to implement on low-cost microprocessors.
- Only 1-2 bytes need to be quickly and reliably erased once intrusion is detected, not 256 bytes or more as is the case with a conventional high-security key.
- The technique has been demonstrated on notebook computers and small microprocessor circuits.
- Works with analog or digital data.

Applications

- courier bags
- safe & vault logs
- audio recordings
- GPS data logging
- tamper detection
- nuclear safeguards
- counter-intelligence
- weapons use logging
- financial transactions
- biometrics & access control devices

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov

Argonne NATIONAL LABORATORY | Nuclear Engineering Division

Human Factors in Security

What's wrong with this quote from a high-level government official after a major security incident?

"While serious, the incident in question was the result of human error, not a failure of securitysystems. We have a robust system in place to report and investigate potential violations. In my opinion, this is a circumstance where those systems worked well."

Human Factors

The term "human factors in security" has been hijacked somewhat from its original meaning. Nowadays, the term is often taken to mean computer modeling of human threats, but the term originally entailed a kind of ergonomics, i.e., understanding human psychology and organizational behavior so as to optimize security.

In the Vulnerability Assessment Team (VAT) at Argonne National Laboratory, we believe "human factors" in the original meaning of the term has been under-studied and insufficiently exploited. Our technical personnel engage in collaborations with industrial/organizational psychologists and other social scientists to try to improve the efficacy of security.

VAT Human Factors Research Areas

- Security Culture & Security Climate
- Countermeasures to perceptual blindness
- Reducing security guard turnover
- The psychology of seal inspection
- Human factors in nuclear safeguards inspections
- The Insider Threat in nuclear safeguards
- Applying security vulnerability assessment techniques to safety
- Correlations between employee attitudes & the rate of security incidents
- Hosting *the Journal of Physical Security* (technical and social sciences)

Recent VAT Papers on Human Factors

EG Bitzer, PY Chen, and RG Johnston, "Security in Organizations: Expanding the Frontiers of Industrial-Organizational Psychology", *International Review of Industrial and Organizational Psychology 24, 131-150 (2009).*

EG Bitzer, "An Exploratory Investigation of Organizational Security Climate in a Highly Regulated Environment", Ph.D. Thesis, Colorado State University (2008).

EG Bitzer and A Hoffman, "Psychology in the Study of Physical Security", *J Physical Security* 2, 1-18 (2007).

EG Bitzer, "Strategies for Cutting Turnover", *Security Management* 50, 88-94 (2006).

EG Bitzer and RG Johnston, "Turnkey Turnaround Solutions: Exploiting the Powerful Tools of I/O Psychology", Los Alamos National Laboratory Report LAUR-05-1130, (2005).

RG Johnston, JS Warner, ARE Garcia, et al., "Nuclear Safeguards and Security: We Can Do Better", Paper 1009, *Proceedings of the 10th International Conference on Environmental Remediation and Radioactive Waste Management*, September 4-8, 2005, Glasgow, Scotland.

RG Johnston, "Adversarial Safety Analysis: Borrowing the Methods of Security Vulnerability Assessments", *Journal of Safety Research* 35, 245-248 (2004).

EG Bitzer and RG Johnston, "A Taxonomy for Security Assignments", *J Security Administration* 26, 1-11 (2003).

VAT Awards

The Argonne Vulnerability Assessment Team has won numerous awards. A partial list includes:

* 10 U.S. patents
* BECCA Honorary CCO Award for contributions to homeland security, 2009
* LANL Fellows Prize for Outstanding Research, 2004
* LANL Achievement Awards, 2007, 2004, 1999 & 1995
* Distinguished Performance Award from the CIA, 2002
* "Excellence in Performance Measure" Award, American Society for Industrial Security, 2002
* LANL Distinguished Performance Awards, 2001 & 1996
* Excellence in Technology Transfer Awards, 1997 & 1992
* R&D 100 National Awards, 1992 & 1994
* "Best of What's New Award", Popular Science, 1992

About Argonne National Laboratory

Argonne National Laboratory, the nation's first national laboratory, is one of the U.S. Department of Energy's largest national laboratories for science and engineering research. Argonne has approximately 3,000 employees, including 1,000 scientists and engineers, three-quarters of whom hold doctoral degrees. Argonne's annual operating budget exceeds $630 million. Since 1990, Argonne has worked with more than 600 companies, federal agencies, and other organizations.

Currently, 16% of Argonne's budget is for intelligence, defense, and homeland security projects (up from 6% before September 11, 2001). The long-term goal is to significantly increase this percentage.

Argonne is managed by UChicago, LLC, for the U.S. Department of Energy.

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov

Argonne NATIONAL LABORATORY | Nuclear Engineering Division

Effective Video Monitoring for Nuclear Safeguards

Non-scary, but believable video monitoring.
See *Science & Global Security* 9, 113-141 (2001).

The Problem

Video monitoring is a powerful technique for international nuclear safeguards, nonproliferation, and dismantlement monitoring, but how do the inspectors know the video is not being faked—especially given that physical and electronic tamper detection to protect cameras is not currently very reliable?

Local Verify

We use the intrinsic high-bandwidth of video and the finite speed of electronic signals to show that the live video images originate locally—not, for example, in some distant Hollywood-like studio designed to fake the video images.

Live Verify

We use off-site video analysis, combined with on-site illumination techniques, chaotic but smoothly varying props (toys & displays), and inspector and facility personnel actions to show that the video images are real-time, and not pre-recorded.

Advantages

- Simple & low-cost
- High levels of confidence in the veracity of the live video.
- Full transparency: No cryptography or secrets.
- Minimizes need for inspectors to be inside facilities.
- Few safety or espionage concerns by the inspected facility and nation.

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov

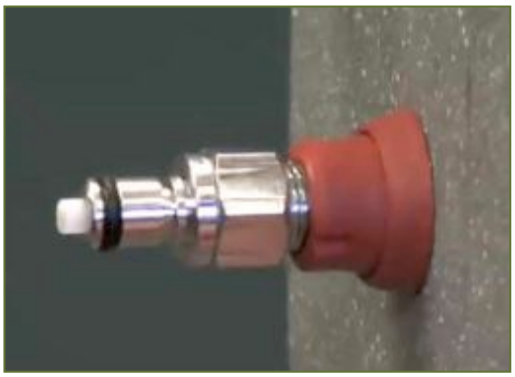
Argonne NATIONAL LABORATORY | Nuclear Engineering Division

Rapid Sampling Tools

Sampling gases, liquids, or flowable powders from inside a container without opening the container, or becoming exposed to its contents.

Purpose

- a field tool that can sample from many different kinds of containers in seconds, with zero release of contents
- small, light-weight, inexpensive, easy to use
- works with any battery-powered hand drill
- can sample gas, liquid, or free-flowing powders
- for containers up to 0.5” wall thickness & 8 atm pressure



Applications

- ✓ firefighters
- ✓ hazmat response
- ✓ counter-terrorism
- ✓ nuclear safeguards
- ✓ customs inspection
- ✓ waste management
- ✓ drug & environmental raids
- ✓ industrial process monitoring
- ✓ verifying the contents of labeled containers
- ✓ identifying the contents of unlabeled containers
- ✓ venting, flushing, monitoring, & transferring liquids
- ✓ archiving samples prior to incineration or shipment

Other Notes

- Covered by 3 U.S. patents.
- Currently in use by U.S. Special Forces and U.S. Border Control.
- Can be made covert.
- It takes < 15 seconds to sample from a 55-gallon drum.
- If the tool is left in the container wall, additional samples can be taken many months later.

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov

Argonne NATIONAL LABORATORY | Nuclear Engineering Division

Better Real-Time Monitoring of Cargo

The 'Town Crier' Method

The Town Crier Method

The 'Town Crier' method for monitoring moving cargo (or stationary valuable assets) in real-time is based on the following concepts:

1. Avoid conventional 2-way, high-bandwidth communications and state-of-health checks. These are too complicated, expensive, and impractical; exhibit too many vulnerabilities; and draw too much attention to the valuable cargo.

2. Don't sound an alarm when intrusion is detected and don't use complex encryption. The alarm can be blocked and the encryption greatly increases complexity without significantly improving security.

3. Instead, send an occasional "All-OK" bit or byte, the correct value of each at any given instant known only to the good guys.

4. The absence of the "All-OK" signal means intrusion.

5. Intrusion into the monitoring system causes instant erasure of the information needed to generate future "All-OK" signals.

6. The adversary gains nothing by blocking the signal and doesn't know how to counterfeit the "All-OK" sequence to hide his intrusion; the necessary information is gone.

Advantages

- Simple & low-cost
- One-way, ultra-low bandwidth communications (~ few bits/min)
- Very tolerant of communication glitches
- Thousands of containers or vehicles can use the same channel
- Very high levels of security
- Surreptitious real-time cargo monitoring is possible
- Allows for an *ad hoc* "Vault Type Volume": we wheel in a small amount of hardware on a cart, and in 5 minutes we have unattended, high-security monitoring of any given volume. Useful for tents in the field, customs inspections, emergencies, or to protect a conference room after a bug sweep.
- Already demonstrated on notebook computers, microprocessors, and in a field demonstration.
  (See *International Journal of Radioactive Material Transport 13, 117-126 (2002) and*
  "Improved Security Via 'Town Crier' Monitoring",
  Proceedings Waste Management '03, Feb 23-27, 2003, Tucson, AZ.)

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov

Argonne NATIONAL LABORATORY | Nuclear Engineering Division

Chirping Tag & Seal

A better approach than RFIDs!

The Problems with Conventional Approaches

RFIDs and conventional radio frequency (rf) tags, seals, and real-time monitors suffer from most or all of the following negative attributes:

- flakey
- power hogs
- prone to interference
- still relatively expensive
- easy to eavesdrop on
- easy to "lift"
- easy to tamper with the reader
- easy to spoof the reader at a distance
- easy to counterfeit (even by hobbyists)
- work poorly around corners
- work poorly in or near liquids & metals
- there's mish-mash of international standards & regulations
- create safety & security concerns in nuclear facilities

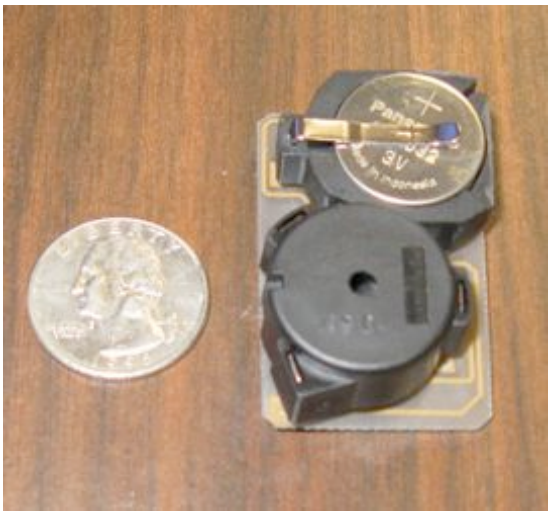
An Alternative

• Don't use RFIDs or rf! Use sound (or ultra-sound for shorter range). It has few of the problems of rf.

• Don't bother modulating the signal or sounding an alarm. For simplicity & low-cost, each tag/seal 'chirps' at a random, unpredictable, constantly changing time (every minute or so on average) known only to the good guys.

• The chirping from any one tag/seal will cease if the item is stolen or has been tampered with. The future pattern of chirps is then instantly erased inside the microprocessor.

• We use a microphone and inexpensive DSP chips to analyze the chirps & ignore background noise.



A prototype Chirping Tag/Seal. This devices uses less than $4 of parts (retail quantities of 1) to provide high-levels of security for critical assets. The device can detect tampering or theft in real-time. Chirping can be detected 300 feet away.

Advantages of the Chirping Tag/Seal

- Cheap, simple, & small
- Low power requirements
- Works well around corners and inside containers.
- Not bothered by proximity to liquids or metals.
- Many chirping tags/seals can be in the same volume. (The chirps are so short that they rarely overlap, though the overlaps that do occur are known in advance to the good guys.)

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov