Talk for the 7th Security Seals Symposium,
February 28-March 2, 2006, Santa Barbara, CA

LAUR 06-0516

Limitations & Vulnerabilities of RFID and Contact Memory Devices

Jon Warner, Ph.D. and Roger Johnston, Ph.D., CPP

Vulnerability Assessment Team
Los Alamos National Laboratory

505-665-9987
jwarner@lanl.gov
http://pearl1.lanl.gov/seals/default.htm

Los Alamos NATIONAL LABORATORY EST.1943

Not everything that can be counted counts, and not everything that counts can be counted.
-- attributed to Albert Einstein (1879-1955)

Problem: Too often, inventory is confused with security.

"The computer allows you to make mistakes faster than any other invention, with the possible exception of handguns and tequila." -- *Mitch Ratcliffe*.

Los Alamos NATIONAL LABORATORY EST.1943

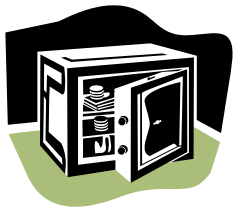
Inventory

- Counting and locating our stuff.
- No nefarious adversary.
- Will detect innocent errors by insiders, but not surreptitious attacks by insiders or outsiders.

Los Alamos NATIONAL LABORATORY EST.1943

Security

- Meant to counter nefarious adversaries, typically both insiders & outsiders.
- Watch out for mission creep: inventory systems that come to be viewed as security systems!

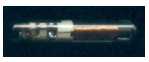


Los Alamos NATIONAL LABORATORY EST.1943

Classic examples of confusing Inventory & Security

- bar codes

- rf transponders (RFIDs)



- contact memory buttons

Usually easy to:

lift, counterfeit, & spoof the reader

The more sophisticated the technology, the more vulnerable it is to primitive attack. People often overlook the obvious.
-- Dr. Who in *The Pirate Planet* (1978)

Los Alamos NATIONAL LABORATORY EST.1943

Contact Memory Button (CMB):

- Requires direct contact for communications.
- Most devices are passive (do not use batteries). However, some devices are active (do use batteries).
- Passive devices draw power from the “reader.”
- Extremely rugged metal enclosure protects circuitry.
- A variety of different devices available (ID only, memory based, cryptographic devices, real time clocks, and temperature sensors).

Contact memory buttons are an excellent technology for inventory purposes!

Los Alamos NATIONAL LABORATORY EST.1943

Some CMB applications:

- Animal tracking
- Medical bracelets
- Chain of custody
- Portable database
- Property tags
- Beer keg dispenser
- Utility pole tracking
- Waste profile storage
- Maintenance records
- Security guard tracking
- Time & attendance tracking

A few worrisome applications:

- Electronic locks
- Electronic ballots
- Deposit boxes
- Electronic safes
- Extra security for tamper-indicating seals

Los Alamos NATIONAL LABORATORY EST.1943

Of particular concern:

Contact Memory Buttons are being used for Nuclear Safeguard applications.

While it is claimed that they are used only for nuclear "material inventory processes" it is clear from the literature that they are also being used for security (to monitor for theft, for example).

Los Alamos NATIONAL LABORATORY EST.1943

Example of Mission Creep!

CMB: problematic for security

- Easy to lift.
- Easy to counterfeit. All needed information, software, & parts are readily available.
- Easy to tamper with the reader. No access to the tag itself is needed.

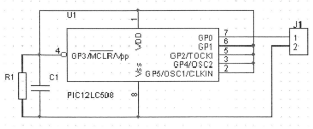
Our first attempt at counterfeiting: Starting with zero knowledge, a working counterfeit was developed in 2 hours. (The first hour was for reading about how the device worked.) The counterfeit costs less & worked better than the original!

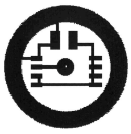
Los Alamos NATIONAL LABORATORY EST.1943

Others know how to do this too:

Имитатор ключей iButton (продолжение)

Схема имитатора проста - сравните с имитатором, описанным в разделе "Проекты" зеленоградской фирмы "Телесистемы". В минимальном варианте содержит только две детали - контроллер PIC12C508 и танталовый конденсатор емкостью 6,8 мкФ . Резистор в несколько сотен кОм нарисован карандашом на плате. Microchip'овские контроллеры имеют бесподобно надежный сброс, тем не менее резистор необходим для разряда емкости и определяет время, через которое имитатор будет снова работоспособен. При указанном значении время составляет десятки миллисекунд и для пользователя неразличимо (кажется, что срабатывает сразу). Контроллер работает в режиме внутреннего сброса без внешних элементов, и с внутренним генератором частотой около 4 МГц.





Коротко об алгоритме работы
При касании имитатором контактного устройства конденсатор заряжается от него до рабочего напряжения, после чего происходит инициализация контроллера, а затем он переходит в режим SLEEP с малым потреблением энергии в ожидании запроса от контроллера замка, по приходу которого включается и анализирует команду запроса. Если это команда "Read ROM" - 33H, имитатор в соответствии с алгоритмом шины 1-Wire, передает серийный номер и контрольную сумму, после чего опять впадает в спячку с подзарядом конденсатора, ожидаючи прихода очередного запроса.

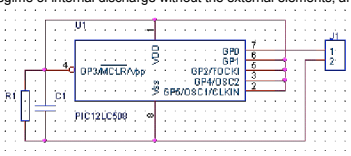
Конструкция
А это печатная плата. Наружный диаметр 17 мм. При изготовлении придерживайтесь размеров, указанных для DS1990A (или просто замерьте ключик). Танталовый конденсатор типоразмера A или B, а рядом с ним еще есть место для установки SMD-резистора, хотя, как я уже сказал, можно …

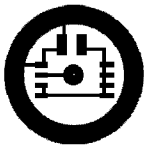
Los Alamos NATIONAL LABORATORY EST.1943

Translation:

Imitator of keys iButton (continuation)

The diagram of imitator is simple - you will compare with the imitator, described in the division the "projects" of zelenogradskoy firm "teles-system". In the minimum version contains only two details - controller PIC12C508 and the tantalum capacitor with a capacity of 6,8 F. Resistor into several hundred k is drawn by pencil on the pay. Microchip'ovskie controllers have excellently reliable discharge, nevertheless resistor is necessary for the discharge of capacity and determines the time, in which the imitator will be again operational. With the value indicated the time composes tens of milliseconds and it is not distinguished for the user (it seems that it operates immediately). Controller works in the regime of internal discharge without the external elements, and with the internal generator with a frequency of about 4 MHz.





Briefly about the algorithm of the work

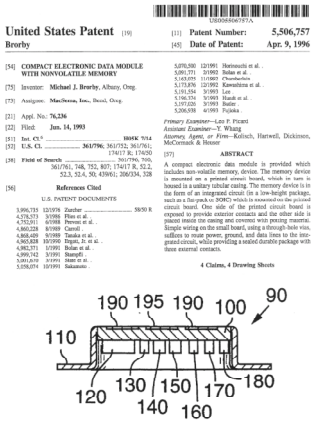
With the contact by the imitator of contact device the capacitor is charged from it to the operating stress, after which the initialization of controller occurs, and then it passes into regime SLEEP with the small energy consumption in the expectation of demand from the controller of the lock, on arrival of which it is included and analyzes the command of demand. If these are command "Read ROM" - 33H, imitator in accordance with the algorithm of tire y-.Shire, it transfers series number and check sum, after which again it falls into the hibernation with the booster charge of capacitor, ozhidayuchi of the arrival of sequential demand.

Construction

But this is printed-circuit board. The outer diameter of 17 mm. with the production adhere to the sizes, indicated for DS1990A (or simply measure small key). The tantalum capacitor of standard size A or B, and next to it still is a place for installation SMD- resistor, although, as 4 already he said, it is possible…

Los Alamos NATIONAL LABORATORY EST.1943

Full details of some devices are disclosed in patents…



United States Patent [19]
Brorby

[11] Patent Number: 5,506,757
[45] Date of Patent: Apr. 9, 1996

[54] COMPACT ELECTRONIC DATA MODULE WITH NONVOLATILE MEMORY

[75] Inventor: Michael J. Brorby, Albany, Oreg.

[73] Assignee: MacDermid, Inc., Bend, Oreg.

[21] Appl. No.: 76,236

[22] Filed: Jun. 14, 1993

[51] Int. Cl.[5] H04K 7/14

[52] U.S. Cl. ..... 361/796; 361/732; 361/761; 174/17 R; 174/50

[58] Field of Search ..... 361/796, 760, 361/761, 748, 752, 807; 174/17 R, 52.2, 52.3, 52.4, 50, 439/61; 206/334, 328

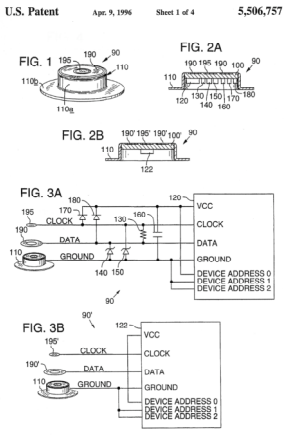
[56] References Cited

U.S. PATENT DOCUMENTS

[57] ABSTRACT

A compact electronic data module is provided which includes non-volatile memory, device. The memory device is mounted on a printed circuit board, which in turn is housed in a unitary tubular casing. The memory device is in the form of an integrated circuit (in a low-height package, such as a flat-pack or SOIC) which is connected to the printed circuit board. One side of the printed circuit board is exposed to provide exterior contacts and the other side is placed inside the casing and covered with potting material. Simple wiring on the small board, using a through-hole vias, suffices to route power, ground, and data lines to the integrated circuit, while providing a sealed durable package with those external contacts.

4 Claims, 4 Drawing Sheets



Los Alamos NATIONAL LABORATORY EST.1943

What about Cryptographic Buttons?

- From our observations, these lack effective physical tamper detection capabilities.
- Others have demonstrated that defeating the DS1991 using a dictionary based attack is not terribly difficult.
  - "DS1991 Multikey Ibutton Dictionary Attack Vulnerability," http://www.grandideastudio.com/files/security/tokens/ds1991_ibutton_advisory.txt
- The DS1991 contains three 48-byte data blocks.
  Each data block is protected by a separate 64-bit password.
- Used for some cashless transactions and access control applications

"We make the chip itself. We don't know the implications of use afterwards by companies that buy the technology."
--Dennis Jarret, iButton Product Manager*

Los Alamos NATIONAL LABORATORY EST.1943

*April, 1999 Recharger Magazine

RFID: Radiofrequency Identification tags

- RFID devices transmit data using radio waves.
- Come in three flavors: Read Only, Read/Write, Cryptographic.
- Most RFID devices are passive (do not use batteries).
  However, some are active (uses batteries).
  Some are even "semi-passive."
- Passive RFID devices draw power from a "reader" generated field.
- The most common frequencies used are:
  Low : (~125 KHz) High : (~13.56 MHz)
  Ultra-High : (~850-900 MHz) Microwave : (2.45-5.8 GHz)

RFID devices are an excellent technology for inventory purposes!

Los Alamos NATIONAL LABORATORY EST.1943

RFID (con't) :

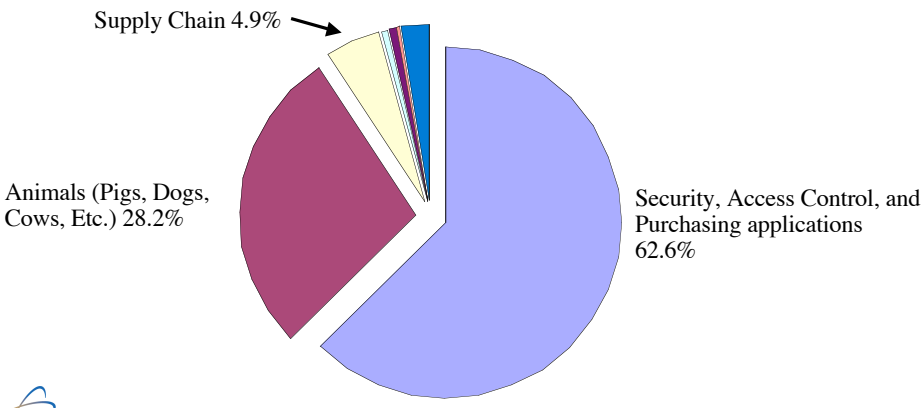
- Sales revenues of $300 - $503 Million in 2004.
- Estimated sales revenues of $2.8 Billion by 2009.
- RFID tag prices range from $0.15 to > $100.
- Many systems are governed by public standards (ISO) to make them more "Universal."
- Some examples include: ISO14443 (passports, proximity cards), ISO10374 (freight containers), ISO15693 (unique ID, vicinity cards), ISO18000 (RFID item management), etc.

"There is a huge danger to customers using this (RFID) technology, if they don't think about security."
-Lukas Grunwald (creator of RFDump)

Los Alamos NATIONAL LABORATORY EST.1943

Where the RFID money went in 2004:

RFID market sectors by % of total sales revenue, 2004



Source: In-Stat

Los Alamos NATIONAL LABORATORY EST.1943

Some RFID applications

- Animal ID
- Fleet tracking
- Parcel & Post
- Library scanners
- Inventory control
- Baggage handling
- Personnel tracking
- Car inventory tracking
- Food production control
- Supply chain management
- Manufacturing line tracking
- Pallet tagging
- Child tracking
- Automobile Immobilization
- Parking lot access control
- Automatic toll booths
- Payment Systems
- Gasoline stations
- Passports
- Banknotes
- Access control
- Tamper-Indicating Seals
- Pharmaceutical anti-counterfeiting (track & trace)

Los Alamos NATIONAL LABORATORY EST.1943

RFID: Not good for security

- Easy to Lift.
- Easy to counterfeit. All needed information, software, & parts are readily available.
- Easy to spoof or modify the reader. No access to the tag itself is required.

Starting with zero knowledge, it took 2 weeks, and < $20 in parts to demonstrate 5 different successful defeats

Los Alamos NATIONAL LABORATORY EST.1943

Some types of attacks:

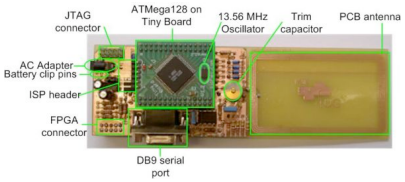
- Communication Based:
  - Skimming: reading data off of someone else's transponder without their knowledge with a reader (home built or commercial).
  - Sniffing: "listening in" to a tag/reader communication stream.
  - Denial of Service: DoS prevents communication from occurring.
  - Spoof tag/reader communication: The act of sending a false (but correctly formatted) communication stream to the tag or reader.
- Tag Based:
  - Clone: impersonate a tag (legitimate/home built) with stolen data.
  - Reprogramming: change data on a tag, works on select tags.
- Reader Based:
  - Reader Modification: attack the reader electronics.

Los Alamos NATIONAL LABORATORY EST.1943

RFID Cloning Devices

Commercial: Used for "faking RFID tags", "reader development."

Commercial: $20 retail, Cloner.



Hobbyist: RFID Skimmer, Sniffer, Spoofer, Cloner.

Los Alamos NATIONAL LABORATORY EST.1943

What about cryptographic RFID?

- Others have defeated the challenge/response format of the Digital Signal Transponder (DST) in early 2005.
  - "Security Analysis of a Cryptographically enabled RFID Device," http://rfidanalysis.org/DSTbreak.pdf, http://rfidanalysis.org/#signifigance
- These transponders are used in Vehicle Immobilizer, Electronic Payment, and other high importance systems.
- The DST contains a secret, proprietary, cipher based on a 40-bit cryptographic key.
- The result is that now ~130 Million RFID transponders currently in use are vulnerable to cloning or spoofing.

Los Alamos NATIONAL LABORATORY EST.1943

> "*It's basically a bar code that barks.*" --Robin Koh, director of applications research at the Auto-ID Labs of the Massachusetts Institute of Technology, on RFID tags used to track prescription drugs.

Lifting:

- Contact memory and RFID devices are typically affixed to a surface using adhesives, epoxies, brazing or fasteners.
- There are many techniques to remove these devices from a container.
- After the tag is removed, unharmed, the adversary is then free to:
  - Place a false tag on a legitimate container.
  - Take legitimate tag home to clone/counterfeit.
  - Steal the container without setting off any alarms.
  - Place the legitimate tag on a counterfeit container.
  - Swap legitimate tags on legitimate containers to cause confusion.
  - Do whatever the adversary can dream up.

Los Alamos NATIONAL LABORATORY EST.1943

Counterfeiting is…

Often overlooked: Counterfeiting is easy (more so than developers, vendors, & manufacturers claim).

Counterfeiters usually only need to counterfeit the superficial appearance & apparent performance, not the actual tag/seal or its real performance.

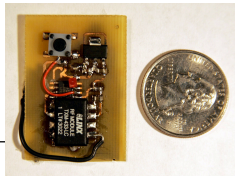
Los Alamos NATIONAL LABORATORY EST.1943

> Sincerity is everything. If you can fake that, you've got it made.
> -- Comedian George Burns (1896-1996)

Remote attack on reader:

- The adversary needs access to a legitimate reader for a short period of time (3 – 30 seconds).
- The adversary places a pre-built RF circuit into the legitimate reader. The pre-built circuit is powered by the reader.
- When the adversary presses a button on his/her transmitter the:
  - Reader database can be modified/erased.
  - Tag registers as legitimate even if there is no tag.
  - Reader behaves normally/abnormally if adversary desires.
  - Reader displays to the user whatever the adversary wishes.
  - Entire reader database can be downloaded from reader to adversary.
  - Outcome of tampering is limited only by the imagination of the adversary.

Los Alamos NATIONAL LABORATORY EST.1943



Why it's not surprising that RFIDs and CMBs are vulnerable

- The tags and readers are inexpensive & readily available for cannibalizing. (High-tech cuts both ways).
- Manufacturers are eager to provide technical support, free samples, and cheap evaluation kits.
- Developers & users have the wrong expertise and focus on the wrong issues.
- These devices have little or no security built in.
- Many more legs to attack.

Los Alamos NATIONAL LABORATORY EST.1943

Myths:

- Myth 1: Seals need a unique identifier (true). RFIDs and CMBs provide one (true). Therefore, they are good for seals (false).
- Fact 1: A seal's unique ID must usually be damaged, destroyed, or otherwise modified during tampering. RFID and CMBs are robust and do not satisfy this requirement.
- Myth 2: RFID and CMBs provide good security.
- Fact 2: RFID and CMBs are not generally designed with security in mind. And security does not happen by accident.
- Myth 3: RFIDs and CMBs are high-technology devices, which makes them effective for high security.
- Fact 3: High-technology is often less secure. Hardware is not magic. The more complicated a device (system) is, the more legs of attack an adversary has to work with.

Los Alamos NATIONAL LABORATORY EST.1943

Some thoughts…

- Design engineers will only use electronic components they have documentation (datasheets) for. This is the same information the attacker needs to defeat the device.

- The more involved a technology becomes with cash, the more interest hackers will have to defeat (exploit) that technology.

Los Alamos NATIONAL LABORATORY EST.1943

The Bottom Line…

- RFID and Contact Memory Devices are great for inventory applications.
- These devices should not be used for critical security applications.
- If using either of these technologies, periodic reassessments should be conducted to ensure mission creep is not occurring.

> IT security managers openly expressed worries with maintaining and protecting the digital files these (RFID) tags will produce. Not to mention black-hat tools already exist to thwart tags' effectiveness. -- Search Windows Security.com

Los Alamos NATIONAL LABORATORY EST.1943

THE END

Questions?

If you are satisfied with your security program you can be sure your adversaries are as well.
--Vulnerability Assessment Team

Los Alamos NATIONAL LABORATORY EST.1943