Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 5, No. 9. September, 2003

Cryptography in the News: GSM Voice Encryption Cracked

Greg Rose
QUALCOMM Australia

Israeli cryptanalysts Elad Barkan, Eli Biham and Nathan Keller of Technion in Haifa have shown how to launch efficient attacks on the GSM encryption algorithm designed for export (A5/2). They have also shown plausible, although far from instant, attacks on the more important voice encryption algorithm (A5/1). Their paper, "Instant Ciphertext-only Cryptanalysis of GSM Encrypted Communications," was presented at Crypto 2003 in Santa Barbara in August.

Background about GSM encryption

GSM calls are encrypted using a family of algorithms called A5. A5/0 provides no encryption. A5/1 is the "standard" encryption algorithm, while A5/2 is the "export" (weakened) algorithm. A5/3 is a new algorithm based on the UMTS/WCDMA algorithm, Kasumi. While one of the attacks below manages to "walk around" A5/3, there is no attack against it directly. For further information about the A5 algorithm family, review the **July 2002 issue** of *Wireless Security Perspectives*.

GPRS encryption is similarly implemented through a parallel family of algorithms: GEA0 (none), GEA1 (export), GEA2 (normal strength) and GEA3 (new, and effectively the same as A5/3). Note that the GEA1 and GEA2 algorithms do not have any relationship to the A5/1 and A5/2 algorithms, and they are not publicly known. No problems with any of these have been published.

All these algorithms use a 64-bit cryptographic key derived from a common mechanism: the mobile receives a random challenge, then the SIM (a smart card used to keep the subscriber's master key secret) calculates an authentication signature and an encryption key. The key calculated does *not* vary based on the algorithm with which it will be used.

Voice encryption is performed with a stream cipher. The encryption algorithm takes the secret key and a frame number, and generates a pseudo-random stream of bits (called the *keystream*). Half of them are XORed with the input (e.g, digitized voice) to encrypt it, and the remainder are XORed with the received bits to decrypt them. Thus, the transmit and receive bits are effectively encrypted independently of one another.

About Wireless Security Perspectives

Price

The basic subscription price for *Wireless Security Perspectives* is $350 for one year (12 issues) for delivery by emailed PDF file or by first class mail within the US or Canada. International subscriptions are US$400 per year. The basic subscription allows for distribution to up to 10 people within one organization. Contact us for license fees to allow more readers.

We provide discounts to educational institutions and small businesses (less than 10 employees).

Back issues are available individually, or in bulk at reduced prices.

Delivery is by first class mail or by email (Acrobat PDF file).

Complete pricing information for both publications is available at:

www.cnp-wireless.com/prices.html

To obtain a subscription, please contact us at:

cnpsales@cnp-wireless.com

Next Issue Due…

October 29th, 2003.

Future Topics

Wireless Flash Memory Security • Personal Area Network Security • Radius for Wireless • 3G Security • Public Keys & Wireless • 1XEV Security

Wireless Security Perspectives (ISSN 1492-806X (print) and 1492-8078 (email)) is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Cresc. NW, Calgary, Alberta T2N 3W1, Canada. **Phone**: 1-800-633-5514 (+1-403-274-4749) **Fax**: +1-403-289-6658 **Email**: cnpsales@cnp-wireless.com **Web**: www.cnp-wireless.com/wsp.html **Subscriptions**: $350 for delivery in the USA or Canada, US$400 elsewhere. **Payment**: accepted by cheque, bank transfer, American Express, Diners Club, MasterCard or Visa. **Delivery**: Email or 1st class mail. **Back Issues**: Available individually for $35 in the US and Canada and US$40 elsewhere, or in bulk at reduced rates. **Discounts**: Educational and small business discount: 25% off any order. **Copies**: Each subscriber is licensed to make up to 10 copies of each issue or back issue. Call for rates to allow more copies.

Technical Editor and Illustrator: Les Owens.

Article Sourcing: Tim Kridel.
Production: Doug Scofield.
Distribution: Debbie Brandelli.
Accounts: Evelyn Goreham.
Publisher: David Crowe.

Upcoming Wireless Security and Fraud Conferences & Events

The following are upcoming wireless, wireless security and general security conferences and events that may be of interest to our wireless security and network security practitioners.

Wireless Security
1st- 2nd October 2003
New York, NY
www.gocsi.com

PCIA Wireless Infrastructure Conference & Exhibition
1st- 3rd October 2003
Westin Diplomat Resort and Spa
Hollywood, FL
pcia.expoplanner.com

6th Information Security Conference
1st- 3rd October 2003
HP Laboratories
Bristol, UK
www.hpl.hp.com/conferences/isc03

MoMuc 2003 (8th International Workshop of Mobile Multimedia Communications)
6th- 8th October 2003
Munich University of Technology
Munich, Germany
www.momuc.org

RFID Journal University
7th October 2003
Westin San Francisco Airport
San Francisco, CA
www.rfidjournal-u.com

[Note: this event is being repeated in other locations during October]

Citrix iForum 2003
13th- 16th October 2003
Walt Disney World Dolphin
Orlando, FL
www.citrixiforum.com

SANS Research Triangle Park 2003
13th- 18th October 2003
Sheraton Raleigh Capital Center Hotel
Raleigh, NC
www.sans.org/trianglepark03

Mobile & Wireless RoadShow
14th October 2003
Westin Copley Center
Boston, MA
www.angelbeat.com/buildpage.cgi?file=home

[Note: this event is being repeated in other locations during October]

ACNS 2003 (Applied Cryptography and Network Security)
16th- 19th October 2003
Shibo Hotel
Kumming, China
www.onets.com.cn/dhe.htm

Gartner Symposium ITXPO 2003
19th- 24th October 2003
Walt Disney World Dolphin
Orlando, FL
www.gartner.com/2_events/symposium/2003/asset_46839.jsp

10th Annual ISPCON Fall 2003
20th- 22nd October 2003
Santa Clara Westin & Convention Center
Santa Clara, CA
www.ispcon.com/fall2003

FIAC 2003 (Federal Information Assurance Conference)
21st- 22nd October 2003
University of Maryland
Adelphi, MD
www.fbcinc.com/fiac

CTIA Wireless IT & Entertainment 2003
21st- 23rd October 2003
Sands EXPO and Convention Center, Venetian Hotel
Las Vegas, NV
www.wirelessit.com/general/schedule.cfm

[Note: this is co-located with the Federal Wireless User's Forum (FWUF)]

Cyprus Infosec 2003 (3rd International Conference on Information Security & Workshops)
22nd- 25th October 2003
Hilton Park
Nicosia, Cyprus
www.cyprusinfosec.org

SecureGOV 2003
26th- 28th October 2003
Homestead Resort
Hot Springs, VA
www.securegov.info

PDC 2003 (Professional Developer's Conference)
26th- 30th October 2003
LA Convention Center
Los Angelos, CA
msdn.microsoft.com/events/pdc/agenda.aspx

10th Conference on Computer and Communications Security (CCS 2003)
27th- 31st October 2003
Wyndham City Center Hotel
Washington, DC
www.acm.org/sigs/sigsac/ccs/CCS2003

Nokia Mobile Internet Conference 2003
29th- 30th October 2003
Acropolis Conference & Exhibition Center
Nice, France
www.nokia.com/nmic

Compsec 2003 (20th World Conference on Computer Security, Audit & Control)
30th- 31st October 2003
Queen Elizabeth II Conference Center
London, UK
www.compsec2003.com/confoverview.htm

Can You See Me Now?

This year camera phones outsold digital cameras for the first time, according to a new report by Strategy Analytics. In the first half of 2003, 25 million phones with built-in cameras shipped worldwide, up from 4 million in the first half of 2002.

Some see this trend as both a problem and an opportunity: Iceberg Systems' Safe Haven technology claims to thwart everything from industrial espionage to peeping Toms by disabling nearby camera phones. The system works by periodically transmitting a signal that tells nearby camera phones and camera phone/PDAs to shut down only their camera functions. Once the device moves out of range the camera is cleared to resume operating.

Details on exactly how the technology works are limited, but based on Iceberg's description, it appears that the device would have to contain client software working in conjunction with the Safe Haven transmitter. The company says it is in talks with major handset manufacturers, whose endorsement will be key to the technology's future. Unless most handset vendors adopt Safe Haven, it will not be attractive to potential buyers – such as factories, gyms and offices – because it would protect against some devices but not others. Regulators also would have to approve Safe Haven, and so far, most countries have refused to allow similar technologies that disable phones or block signals.

In the meantime, some businesses have found an alternative, permanent solution. For example, the Bazooka's Showgirls strip club in Kansas City uses a sledge-hammer to disable camera phones used to photograph its dancers.

Encryption is done *after* coding for error correction. The error correction coding introduces known linear relationships between the bits to be encrypted; therefore, even though the attacker might not know the values of particular input bits, they know that certain groups of them XOR to 0. Taking the same groups of encrypted bits and XORing them reveals the corresponding XOR of the keystream bits. This is the fundamental deficiency that allows the attacks to work without any knowledge at all of what is being encrypted, which is what the authors mean by "ciphertext only" in the title of their paper. This is a very new result.

The Attacks:

There are effectively three different attacks discussed in the paper.

Passive Attack on A5/2

The fundamental attack is against A5/2. By performing a one-time pre-computation and storing the results on a decent-sized disk, you only need to intercept four frames of A5/2 encrypted voice (a few milliseconds worth) to obtain enough known linear relationships in the keystream to look up the key. The attack is, therefore, almost instantaneous. This is a "passive attack," requiring only eavesdropping. No one can tell that it has been done. Once the key has been recovered, it can be used to decrypt the actual frames in both directions.

Walking Around A5/1 and A5/3

The second attack interferes with the GSM protocol, relying on the quickness of the first attack. The attacker's ability to interfere with the communication makes it an "active attack." In theory, the attacker would only need equipment that could emulate some functions of a base station. This is more than just theory, however, since such attacks are known to have happened in the past. Commercially available test equipment can do it, as it is not much more than two cellphones back-to-back. Basically, this is how it works: Even though the real base station and the mobile would both prefer to use a stronger encryption algorithm than A5/2, the attacker (often called a "Man In The Middle") can convince the mobile to use A5/2 long enough to break it (for example, by pretending to be an Asian base station unable to perform A5/1), recover the key, and respond to the real base station with correctly encrypted data using the stronger algorithm. This works because the same key is used for both the weak (A5/2) and the stronger algorithms (A5/1 and A5/3). It happens so quickly that the real base station cannot be sure that there were not simply interference problems.

Attack on A5/1

The third attack is not as elegant as the ones above. This one would have been very alarming (and still publishable) all by itself, however. This attack uses the same trick as above, identifying linear relationships in the encrypted frames. This allows classification of the output keystream in a way that is amenable to searching using a technique called a "time-memory trade-off."

The attacker takes four consecutive encrypted frames, runs a processing phase on them, and checks if the output is in their database. If they are lucky, it is, and they can then very quickly determine the input key. If not, they try again with a different set of four frames. Eventually, they will get lucky. How long this takes depends on the size of the database, which in turn depends on how much time they have spent initially computing it.

Section 6 of the published paper shows that an A5/1 key can be recovered in real time (by which they mean it takes less CPU time than it takes to intercept the data) with:

- 5 minutes of intercepted frames (they do not have to all be from one call);
- 4.4 Terabytes of disk space (which is not that much these days);
- a lab full of PCs for a year's worth of one-time pre-computation.

This is just one point in the trade-off curve; I happen to think it is the 'sweet spot.' But security intelligence agencies with time and budgets on their hands, for example, could compute a bigger database and decrypt traffic with much shorter intercepted call durations.

Note that the key recovery success is probabilistic. If you have 2.5 minutes of call, you have a 50% chance of key recovery. If you listen to 10 calls at a time, you could get a key about every 30 seconds.

More about the active attacks

The important thing about the active attacks is that the attacker can confuse a mobile into doing what it wants it to do. At the limit, if the attacker has intercepted the random challenge sent to a particular mobile and has recorded all the traffic, whether it is GSM voice or GPRS data, they can later send the same random challenge to the mobile and tell it to use A5/2 to communicate. When the mobile responds, the attacker can recover the key, which is the same one that will decrypt the recorded traffic, regardless of which algorithm (presumably stronger) with which it was encrypted. What is more, the process with A5/2 is fast enough that it can be done between the time the real network sends a challenge to the mobile and when it would time out waiting for a valid response (about 12 seconds).

And what if the target is using A5/1 but the attacker did not get enough data to recover the key? They can simply call the target, ask for Bob, sound confused, verify that they called the right number, apologize, dither for a few seconds, and eventually the key will pop out. This currently works because the network usually uses the same key for multiple calls (to cut down on network traffic). This also gets around any problems with identifying the correct target in the first place; the attacker just needs to know their victim's phone number.

Once the attacker has the key, other types of active attacks can occur, such as originating calls (at the victim's expense), hijacking data sessions, or altering data messages (SMS). These will be undetectable (at least by cryptographic means) by the network, and exposure will continue until the network issues a new challenge.

Mitigation of the Attack

There are a number of proposals being discussed to address the attacks. Some are considered confidential, but two obvious approaches are:

1. Remove A5/2 from handsets and disallow its use in legitimate networks.
2. Challenge the mobile and invoke a new key for every new service.

Editor's Note

The removal of A5/2 from handsets will be problematic. Unless export controls over A5/1 are removed, this would create a class of phones that would be more secure within parts of the world using A5/1 (e.g, Europe) but unusable and unmarketable elsewhere. One of GSM's major benefits would be diminished: the economies of scale that come from being able to sell one device to many different markets.

About the Author

Greg Rose is a manager and cryptographer with QUALCOMM Australia, working on cryptography and authentication for CDMA cellular phone systems. He is an active participant in 3GPP2 and 3GPP security standardization groups. He acquired a B. Sc. degree in Computer Science from the University of New South Wales. He is an experienced teacher at university and in private courses, mostly involving cryptography and security, programming languages, operating systems, and implications of software and hardware technology.

Scalable, Extensible Security is Key to RFID Ubiquity

William Whyte
NTRU

From the gas station to the ski slopes, radio frequency identification (RFID) devices are changing how we pay for goods, control admittance and track inventory. Many companies are also looking beyond these single-function applications to multi-function RFID devices. Only one thing hinders the roll-out of mass-scale, multi-function RFID devices: the lack of cost-effective, scalable security.

Low-cost RFID tokens, packaged in contactless smart cards or key fobs, are gaining widespread adoption for use in a range of innovative and cost-sensitive applications including replacing transit tickets, access control, ticketing, loyalty programs and payments. Security on these applications, so far, has been limited to simple PIN-based and symmetric key cryptography based systems. However, the well-known security vulnerabilities of these systems have restricted these applications to small-scale, closed systems.

For many traditional RFID applications, such as supply chain management and transit passes, strong security has taken a back seat to cost, performance and usability. However, the demand for new functionality that allows for application expansion as well as business growth is putting security back in the spotlight. To compete, RFID manufacturers will need to find new, innovative security solutions … without increasing costs significantly.

Bound by Limitations

Today's popular single-function RFID devices such as SpeedPass have limited security options. Until recently, symmetric key cryptographic techniques have been the only option because of the cost and size constraints of the RFID environment. This approach binds all the devices together with a single "shared secret." Although this provides adequate fraud protection on a small-scale single-function device, it does not perform as well once a device is used for multiple applications involving multiple parties. The reason is simple: compromise of any trusted element of the system compromises the entire system. For many applications, the threat of a key being compromised is not acceptable. Many companies are unwilling to accept the risk of substantial losses due to fraud, brand corruption or compromised proprietary corporate information in the event of a successful attack.

Another drawback of symmetric-key cryptographic approaches is their inability to scale up from a field trial to full commercial implementation and their inability to provide extensible security to multiple applications that do not share a central controlling security organization. Security needs to provide the ability to scale up smoothly to support high-security financial applications and scale down smoothly for more inexpensive, single-application markets.

A Better Alternative – Use of Public-Key Cryptography (PKC)

A better option for RFID applications is public key cryptography which can be designed to ensure data confidentiality, user authentication and privacy of all exchanges. Without this, vendors wishing to deploy secure RFID applications have to choose between inexpensive, insecure tokens or expensive tokens that consume significant power and perform slowly. Today, PKC vendors can deliver payment capability on tokens for traditional RFID applications such as ticketing, access control and payment applications. Using the security provided by public-key cryptography, anti-passback and dynamic re-keying capabilities can be implemented using specific readers that can rewrite data to a token – the user's credentials, for example – on-the-fly.

Why are these PKC-enabled capabilities important?

Dynamic re-keying, or "key re-certification," lets integrators issue a new credential/signature on a token verifying its authenticity. This function is simple to implement using public-key cryptographic techniques, and it lets integrators implement a variety of new features, including the ability to reclassify divisions or employees as a result of mergers, acquisitions or spin-offs. In a symmetric-key model, the system has to maintain a synchronized database of keys or run the risk of an attacker cracking a reader and forging tokens.

Another major benefit of public-key-enabled readers is that they can provide strong authentication with the fast response time that enterprises, consumers and merchants demand, without being wired into a network. This feature enables low-cost terminals for micro-payments such as quick-service retail, vending and kiosks. Elimination of on-line requirements is a particularly important consideration where communications are expensive, unreliable or both.

For systems integrators, the value is clear: The additional functionality enabled by cryptographically secure storage on a token allows integrators to develop higher-value products and services to their customers, while lowering the cost and complexity of back-end systems infrastructure.

How does it work?

Public key security eliminates the risk of someone breaking an entire multi-vendor RFID system by ensuring that every entity involved in a secure transaction is uniquely keyed. In a public key system, two keys are involved: a private key, which can only be accessed by the entity; and a public key, which can be accessed by anyone. The two keys work together, so a message encrypted with the public key can be recovered only by the private key. If the keys do not match, the message cannot be decrypted. This architecture has several benefits:

- **Fraud Reduction** – Reduces the potential for use of counterfeit tags and readers and malicious attacks against applications and services.
- **Key Management and Distribution** – Reduces the cost of securing and managing centralized key storage, key distribution, and recovering from system compromises.
- **Privacy** – Meets consumer demands for less intrusion, protection against identity theft and limited distribution of personal data and/or behavioral information.

Transit systems are a good example for understanding these benefits. This low-end application may present an even greater risk than high-end applications because it involves huge numbers of transactions that are seldom checked for accuracy. Manufacturers of contactless cards, which do not have to be swiped, have been quick to promote the efficiencies of RFID technology over barcode-based systems for public rail

What is a public key cryptosystem?

A public key cryptography system provides a secure and trusted environment by meeting four major requirements of security:

- **Confidentiality** – assurance that nobody can listen in.
- **Authentication** – assurance that the parties you are doing business with are who they claim to be.
- **Integrity** – assurance that information you send or receive is not tampered with on its journey.
- **Non-Repudiation** – assurance that agreements are legally binding.

These systems use asymmetric encryption to ensure confidentiality, digital certificates for authentication, digital signatures to guarantee integrity and the combination of digital signatures and certificates for non-repudiation.

Each device or account in a public key cryptosystem is given a 'key pair' comprising a private key and a public key. The pair is linked mathematically and each pair is unique. The originator of a message or transaction digitally signs the message or transaction using the private key. The digital signature is proof of that user's identity, the equivalent of a handwritten signature. The recipient of the message uses the corresponding public key to verify the signature.

For a Good Chuckle...

www.cnp-wireless.com/acronyms.html

… has a collection of humorous definitions for common telecom and computer acronyms.

Some of these might be construed to belittle your favorite technology, but you may send us your favorite acronym barb. You'll help us spread the light-hearted spirit of the wireless world.

systems. In situations of high traveler throughput, the faster access is also very attractive to the traveler.

The current vulnerabilities of RFID symmetric-key-based cards are substantial. In order to meet the high throughput required in a transit system, for example, the readers contain an embedded system master key for authenticating each card. If just one of the many readers in the system is compromised, counterfeiters can easily manufacture fraudulent cards and sell them at discounted prices. The individual values might be low, but the overall size of the market is very large. For example, daily revenues of Hong Kong's Octopus transit card exceeds $7 million.

This risk is multiplied further when manufacturers and integrators extend the functionality and profitability of these transit cards to support multiple businesses within the transit system, such as shop owners and food stands.

This type of card also could be used in an airport, an amusement park or a shopping center. Access card applications include building access passes, city cards and fueling key fobs (e.g, Speedpass). However, these same vulnerabilities exist in all of them when they are based on symmetric keys.

In airports, where tags and tickets are essential, improved security could revolutionize RFID. Delta Airlines conducted trials using RFID labels to replace barcode-based baggage labels. Barcode-based labels had a read-rate of only 70%, while RFID labels had a better than 99% read-rate. In addition, RFID improves the ability to discover baggage not belonging to someone on the flight. This could avert the need for rigorous and time-consuming security checks for avoiding potential danger, which sometimes results in unloading of all baggage and disembarking of all passengers until the item is found. In the case of the 1988 bombing of Pan Am Flight 103, for example, the bomb was traced to a suitcase that did not belong to anyone on board.

These efficiency gains make a very persuasive business argument, but without addressing the security issues the risks are too high. If there is no way to authenticate the information on such tags or no way of proving that they have not been tampered with, what will stop the hacker from compromising the system and claiming any bag as his or her own or tampering with baggage after it has been checked in?

A Public Key Solution

With a cost-effective public key security solution for RFID devices, airlines could accelerate the flow of higher-value, lower-risk passengers through security checkpoints by encrypting the information on their frequent flyer cards or tickets to provide authentication of their identity. Such a system would be efficient and fraud-resistant, and it would improve the traveling experience of high value customers and the speed of security checks, thereby creating greater brand loyalty.

Ubiquity Within Reach

Although public key security reduces fraud and the potential for malicious attacks, the technology also needs to fit into tiny devices. Until now, the only public key solutions available required a large hardware footprint, which is inconvenient and cost prohibitive for low-end RFID transit cards and airline baggage labels.

In addition, a public key solution that can eliminate expensive co-processors on high-end RFID devices such as contactless smart cards will completely reshape the industry, where every fraction of a penny matters. A public key solution that eliminates the high price tag of strong, scalable security without compromising performance will help kick-start this nascent industry.

Strong security has emerged as the leading requirement for RFID manufacturers and integrators seeking to differentiate their products and applications. The combination of strong security provided by public key cryptography with very low price points will create opportunities for new applications and drive unit demand in price-sensitive RFID markets.

About the Author

William Whyte (wwhyte@ntru.com) is director of cryptographic R&D at NTRU. Before joining NTRU, he was senior cryptographer with Baltimore Technologies in Dublin, Ireland, where he spoke and lectured about cryptographic issues before audiences in many different countries and on television. He holds a B. A. from Trinity College, Dublin, and a D.Phil. from Oxford University.

About NTRU Cryptosystems

NTRU Cryptosystems, Inc. (www.ntru.com) provides security expertise to the embedded technology market. From system security analysis to optimized implementations on constrained platforms, NTRU provides practical security solutions tailored for specific application environments. NTRU's core competencies include development and evaluation of standards-based security architectures and protocols, cryptosystem design and implementations based on the NTRU algorithm suite and other major algorithms. NTRU provides services and solutions to a range of markets, including trusted computing, wireless networking, carrier-based wireless and RFID/contactless identification. Headquartered in Burlington, Massachusetts, NTRU's investors include TI, Sony, Macrovision, Lehman Brothers Venture Capital, Investor AB, Granite Ventures, Greylock and 3i.

Postscript: Unanswered Questions

WSP Staff

NTRU has made a case for the concept of using public key encryption to tighten the security on RFID tags. However, those interested in this technology must verify that RFID tags have sufficient computational horsepower. Detailed information flows from vendors of this technology must be examined to determine where credentials are stored and where computations are performed. It must show not only the real-time usage of the system, but also the key-generation and distribution system, and indicate which parts of the system belong to the manufacturer, integrator, merchant and consumer.

Addressing RFID Consumer Privacy Issues

Microwave "nuking" of an RFID tag may convince consumers that they are safe from its tattling (see the **July 2003 issue** of *Wireless Security Perspectives*), but a safer way to kill a tag employs a kill code such as the one being developed by the Auto-ID Center (For further details about RFID protocols, read Auto ID Center's TR016). Their device provides a means of terminating an RFID tag using a scanner which triggers a 'kill switch.' Anyone with such a scanner (a check-out clerk, a consumer, or an attacker) could disable any tag designed with this option allowing it to be killed. But what if the consumer wants both privacy as well as the tag's on-going benefits?

Several approaches can preserve the tag's value-added aspects while at the same time providing privacy.

- Public-key encryption – The RFID tag reader can either decrypt the ID data from the tag, or it can encrypt a new ID and issue it to the RFID tag to replace the tag's previous ID.
- Pseudonyms – An RFID tag may issue a different ID each time it is queried by a reader. The tag would issue these various pseudonyms in a given sequence. After reaching the end of its list of identities, it would begin again at the beginning of the list. A forced-delay mechanism in the tag's ability to repeat its entire identity helps prevent rapid querying by potential attackers attempting to determine the pattern.
- Faraday Cage – RFID-tagged objects placed in a cage made from metal foil or mesh cannot be read from outside. This approach is simple but inconvenient, in most situations.
- Jamming – Consumers could carry around a device that jammed signals to or from RFID devices. This may be illegal and would disrupt the legitimate use of RFID devices within stores.
- Blocker Tag – This is an auxiliary RFID tag which uses selective passive jamming to force a tag reader into the 'tree-walking' method for acquiring data from each tag. The Blocker Tag affects all susceptible tags within the range of any tag reader, making them more difficult to read only when in the presence of the Blocker Tag.

This article addresses only the Blocker Tag approach.

How the Blocker Tag works

The Blocker Tag forces the tag reader into a highly inefficient 'Singulation' protocol. It is targeted for RFID tag systems using the "tree-walking" protocol for singulation. Other protocols would require different types of blocker tag algorithms.

In this protocol, for the reader to identify any given RFID tag, it must query for each bit of tag identity, beginning with the lowest-valued bit and working through the tree of values presented by all nearby tags.

For each bit of an ID the reader asks for active devices to reply with the value of the bit, either a 0 or 1. By temporarily deactivating devices without a specific prefix (e.g, 011), it can determine whether all the remaining active devices have a 0 or a 1 as the next bit, or whether there is a mixture. It is also possible to determine if there is only a single device with that prefix.

A Blocker Tag will answer with both a 0 and a 1 to every query. This means that the reader has to search through the entire tree of possible identifiers rather than being able to search more efficiently by pruning branches of the search tree that bear no fruit.

A Blocker Tag can be designed to begin its combined 1 plus 0 response after a given number of bits of its identifier have been queried. Certain tags, therefore, can remain unblocked, while other tags will be blocked by the blocker tag. At the check-out counter, instead of killing the tag, the store employee could use the scanner (tag reader) to alter the RFID tag of a purchased item to a new tag ID that would fall into the subset of tag IDs affected by the Blocker Tag. An item not scanned at check-out would remain unblocked by the Blocker Tag, which means a tag reader at the exit could identify the item as unpaid-for, but the identities of purchased items would remain obscured.

A Blocker Tag used maliciously could become a problem, however, as it could be used as a Denial-of-Service attack tool. This cannot be prevented, but the presence of such a tag could be detected.

This Blocker Tag approach is being developed by RSA Labs. They plan to present it further at the Association for Computing Machinery's CCS2003 conference (included in the listing of **Upcoming Conferences**). A technical paper on the Blocker Tag is available at the RSA website:

www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker/blocker.pdf

GPS-less Tracking: RFID, WLAN and GSM-based

Hitachi plans to release a WLAN-based (802.11b) tracking/locating system using the Hitachi Direct Path Detection Method, developed as a spin-off from its recent work with their CDMA-based Hitachi Locating Systems approach. This product is expected to be released in the Japanese market during October, 2003. It can locate wireless devices to within 1 to 3 meters – as compared to over 10 meters with GPS locating systems. This makes the system useful for detecting WLAN intruders (e.g, WiFi war-drivers), similar to the LEN system presented in the **March 2003 issue** of *Wireless Security Perspectives*.

RFID tags are often used to assist with triangulation, and their accuracy is similar to Hitachi's WLAN locating system, but a system using RFID tags for tracking every square meter of a large area is much less practical. The tags are inexpensive enough, but to track all tagged devices within an area of 10,000 square meters, one RFID reader might be required for

Wireless Jammers and Scammers

In second quarter 2003, 110.9 million wireless phones were sold worldwide. That is almost the number of PCs sold in all of 2002. With that many phones in circulation, it is no surprise that another round of jamming technologies has hit the market.

The latest crop includes WolfPack, which is noteworthy for its price – $10,000 per node – and its developer: the U.S. Department of Defense. These are intended to replace the expensive air-based jamming systems currently in use. Each battery-powered node is a 6x4-inch, 4-lb. cylinder that can be dropped into enemy territory by plane or by truck. It jams cellular and 802.11 WiFi signals within one square kilometer, but does not affect commercial or friendly military wireless. A mass of these, dropped or launched strategically, gang up on the signals. A WolfPack prototype should be ready for testing by early 2005.

One advantage military jammers have over their commercial counterparts is that their users do not require regulatory approval. Authorities in most countries say jamming equipment requires licensing or is outright illegal, but lax enforcement only encourages people like Ronnie McGuire, a salesman whose main market is hotels and restaurants in Scotland. He imports GSM jammers from Taiwan and resells them for £75 apiece (equivalent to US$125 apiece). His pitch is straightforward: If patrons cannot use their cell phones, they will have to use the payphones, from which the establishment takes a cut of the proceeds.

"It comes up on their phone: 'no service' and people think there's no service in that area," McGuire told the London Daily Record. "A friend at [the Tower Hotel in Crieff] was annoyed by people in his dining room with the phone ringing all the time and he'd put in a new phone system and wanted some payback on it. A hairdresser bought two the other day because his staff are texting each other all the time."

10,000 square meters, one RFID reader might be required for each 9 meter square. Such a network of readers linked to a server could cost more than $200,000.

Hitachi's WLAN system does not come cheaply, either, however. For a cost likely exceeding $25,000, it could provide an intruder-device locating system to cover 40,000 square meters.

A recently developed GSM-based system may provide a low-cost approach to device locating. Using this system, for which trials were completed in June 2003, coverage of 100 square kilometers was achieved using a small number of servers and a multitude of GSM handsets software-enabled to communicate with them. Implementation costs were less than $1 per handset.

A word of caution, however. These systems are similar to E-OTD (Enhanced Observed Time Difference) that was trialed by major North American GSM carriers for locating emergency callers. It was eventually abandoned in favor of pure network-based triangulation (TDOA – Time Difference of Arrival).

Fraud and Security Patent News

US Patent: 6,622,050

Variable encryption scheme for data transfer between medical devices and related data management systems

An encryption apparatus, system, and method in which data from an Implantable Medical Device (IMD) and a data center could be transferred based on a differentiated encryption system. The encryption scheme allows for the differentiation, segregation, and classification of data at required or needed levels of security. Before transfer of the data, either from an IMD or any other part of a support network for the IMDs, the encryption device begins to distinguish the data. The variable data is then classified based on various levels of security having distinct encryption protocols. After classification, the data is encrypted based on the data's level of security. The data is then transmitted. Upon being received, the data is then segregated based on whether the data is encrypted. The encrypted data is then decrypted and interpreted.

Issued: September 15, 2003

Inventor: David Thompson
Assignee: Medtronic, Inc. (Minneapolis, MN)

US Patent: 6,622,015

Method and apparatus for using electronic documents within a smart phone

A method and apparatus for using electronic documents within a smart phone. A merchant, legal organization, or other entity provides an electronic document to a subscriber as proof of registration for a service or of legal entitlement. At the time of registration, the subscriber registers a phone number of a phone at which the subscriber desires to receive the issued electronic document. After the electronic document is created, the organization transmits the electronic document to the phone at the registered phone number. The receiving smart phone allows the subscriber to manage the electronic document within the smart phone.

Issued: September 16, 2003

Inventors: Maria Himmel and Herman Rodriguez
Assignee: International Business Machines (Armonk, NY)

US Patent: 6,622,014

Method for authorizing a communication between at least two devices

Known telecommunication systems like a DECT-system comprising a base-station and a handset or like, a Digital Home Network system comprising a controller and several devices or a car radio system comprising a car radio and a front. These are based upon an authorization process for introducing a new device or for coupling an already introduced but decoupled old device to said telecommunication system. Such authorization process, which often is user-unfriendly, can be partially or even completely avoided by either using the result of an old identification process or by using a new identification process for identifying a user, which can be done in a much more user-friendly way.

Issued: September 16, 2003

Inventor: Patrick Daniel
Assignee: Alcatel (Paris, FR)

US Patent: 6,621,854

Spread-spectrum electromagnetic signals

An assembly of simultaneously transmitted electrically generated signals, which contains a subset of binary spreading-code sequences that are members of a larger set of binary spreading-code sequences available to a particular node of a multi-node communication network. All sequences in the set of spreading-code sequences available to the particular node of the network can be generated by the same configuration of two linear-feedback binary shift registers, where feedback taps of the two shift registers correspond to primitive polynomials of the same degree over GF(2), the field of two elements.

Issued: September 16, 2003

Inventor: Bart Rice
Assignee: Lockheed Martin Corporation (Bethesda, MD)

Reference:

[1] Jones. *Physics for the Rest of Us, Ten Basic Ideas of Twentieth-Century Physics That Everyone Should Know . . . and How They Have Shaped Our Culture and Consciousness.*Contemporary Books, Inc., 1992, pp. 143-146.

US Patent: 6,618,763

Virtual private wireless network implementing message delivery preferences of the user

A virtual private wireless network in which wireless devices include at least one having a screen for displaying received text and an intelligent information interconnect device integrating voice messaging, email, and fax services into a single access point. The information interconnect device includes a centralized directory database storing identifying information regarding the wireless devices, and further storing delivery preference hierarchy information for delivering content to the wireless devices. A user interface is provided for specifying criteria used to select at least one device ID from the centralized database, and a message delivery system is provided for searching the centralized database using the specified criteria and transmitting information to the wireless device(s) using the delivery preference hierarchy information.

Issued: September 9, 2003

Inventor: David Steinberg
Assignee: InPhonic, Inc. (Washington, DC)

www.inphonic.com

InPhonic, Inc.
1010 Wisconsin Avenue, Suite 250
Washington, DC

Telephone: (202) 333-0001

InPhonic is a provider of wireless voice and data communication solutions to enterprises, online businesses, national retailers and end-users. InPhonic creates and manages online platforms for customers to enable their end-users, including employees, members and customers, to purchase wireless devices and services. They also sell communication software and services to enterprises.

US Patent: 6,618,584

Terminal authentication procedure timing for data calls

A subscriber terminal that initiates an authentication procedure with a supporting wireless communications system in response to either a timer expiration based trigger, a state change based trigger, or a combination timer/state based trigger. With respect to the timer expiration based trigger, a countdown timer is set by either the subscriber terminal or the supporting system and thereafter monitored for expiration to trigger authentication. For the state change based trigger, the subscriber terminal monitors for any transition from an operating state wherein use of an air interface connection with the supporting system has been suspended, which triggers authentication. Furthermore, for the combination timer/state based trigger, the subscriber terminal sets a countdown timer and monitors for an operating state transition that occurs subsequent to timer expiration to trigger authentication.

Issued: September 9, 2003

Inventors: Caisa Carneheim and Maria Moynihan
Assignee: Telefonaktiebolaget LM Ericsson (publ) (Stockholm, SE)

US Patent: 6,618,484

Steganographic techniques for securely delivering electronic digital rights management control information over insecure communication channels

Electronic steganographic techniques that can be used to encode a rights management control signal onto an information signal carried over an insecure communications channel. Steganographic techniques ensure that the digital control information is substantially invisibly and substantially indelibly carried by the information signal. These techniques can provide end-to-end rights management protection of an information signal, irrespective of transformations between analog and digital. An electronic appliance can recover the control information and use it for electronic rights management to provide compatibility with a Virtual Distribution Environment. In one example, the system encodes low data rate pointers within high bandwidth time periods of the content signal to improve overall control information read/seek times.

Issued: September 9, 2003

Inventors: David Van Wie and Robert Weber
Assignee: InterTrust Technologies Corporation (Santa Clara, CA)

About WSP Patent Listings

The US Patent and Trademark Office (USPTO) frequently grants fraud and security patents that will be of interest to some of our wireless security practitioners. Each patent includes the invention title – linked to the corresponding USPTO web page – a brief description, the inventor(s), and the assignee (owner). All of these patents were granted in August of 2003.

With the listing of patents provided each month, one can see who is doing what in the world of wireless inventions. Moreover, it is often instructive to read issued patents, since they include patent claims, specifications, illustrations, detailed descriptions and cited references. Patents often include other references, and these are sometimes useful to broaden one's perspective of wireless communications and security.

If the wording in these is difficult to understand, recognize that the patent abstracts are generally provided in their raw legal-jargon form,

References:

[1] Caruso, D. *Technology, Digital Commerce: 2 Plans for Watermarks, Which Can Bind Proof of Authorship to Electronic Works.* N.Y. Times, Aug. 7, 1995, p. D5.

[2] Choudhury, A.K. *et al. Copyright Protection for Electronic Publishing Over Computer Networks.* AT&T Bell Laboratories, Murray Hill, NJ, Jun. 1994. 17 pages.

[3] Cunningham, D. *et al. AT&T, VLSI Technology Join To Improve Info Highway Security.* News Release, Jan. 31, 1995. 3 pages.

[4] Dussee, S.R, *et al. A Cryptographic Library for the Motorola 56000.* Advances in Cryptology: Proceedings of Eurocrypt 90, I.M. Damgard, ed., Springer-Verlag, 1991, pp. 230-244.

[5] Low, S.H, *et al. Document Marking and Identification Using both Line and Word Shifting.* AT&T Bell Laboratories, Murray Hill, NJ, Jul. 29, 1994. 22 pages.

[6] Weber, R. *Digital Rights Management Technologies.* International Federation of Reproduction Rights Organization, Danvers, MA. Oct. 1995. 21 pages.

[7] Yee, B. *Using Secure Coprocessors.* CMU-CS-94-149, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, 1994. 94 pages.

US Patent: 6,618,483

Elliptic curve encryption systems

An elliptic curve encryption system that represents coordinates of a point on the curve as a vector of binary digits in a normal basis representation in F.sub.2.sub.sup.m. A key is generated from multiple additions of one or more points in a finite field. Inverses of values are computed using a finite field multiplier and successive exponentiations. A key is represented as the coordinates of a point on the curve and key transfer may be accomplished with the transmission of one coordinate only and the identifying information of the second. An encryption protocol using one of the coordinates and a further function of that coordinate is also described.

Issued: September 9, 2003

Inventor: Scott Vanstone, *et al*
Assignee: Certicom Corporation (Mississauga, CA)

US Patent: 6,616,035

Method and device for identification and authentication

A method and a device of identification and authentication of a holder of a mobile electronic transaction device in an electronic transaction process between a transaction service provider and a transaction terminal in communication via a computer network. A transceiver is adapted for transmitting an identity of the device to the transaction terminal and receiving a challenge transaction identifier from the service provider via the transaction terminal. A data processing device is adapted for determining an authenticity of a user identification input by comparison with a reference user identification, and for performing a cryptographic transformation of the transaction identifier using a secret key only on the identification input being determined as authentic. The transceiver is also adapted for transmitting a response result of the cryptographic transformation to the service provider via the transaction terminal for validating the transaction.

Issued: September 9, 2003

Inventor: Jakob Ehrensvard and Stina Grip
Assignee: Cypak AB (Taby, SE)

www.cypak.com

Cypak AB.
Box 2332
103 18 Stockholm, Sweden

Telephone: +46 (0) 8 545 00 835

Cypak developed a data carrier technology that allows objects to become “smart, secure and connected.” Each object has a unique and dependable identity, and it is small enough to be integrated into a range of products and items. Cypak focus and strength has been research and development.

US Patent: 6,611,913

Escrowed key distribution for over-the-air service provisioning in wireless communication networks

An escrowed key distribution system for over-the-air service provisioning of cellular telephones and other wireless communication devices provides a secure and efficient authentication key distribution method for wireless communications networks. To ensure security, an authentication key used to activate the wireless device is never transmitted over the air. In addition, mutual authentication is performed between the wireless communication device and the service provider using an embedded private-key algorithm to ensure proper authentication key transfer.

Issued: August 26, 2003

Inventors: Christopher Carroll and Yair Frankel
Assignee: Verizon Laboratories Inc. (Waltham, MA)

References:

[1] Reed, Michael G, *et al. Protocols using Anonymous Connections: Mobile Applications.* Naval Research Laboratory, 1998.

[2] C.P. Carroll, *et al. Efficient Key Distribution for Slow Computing Devices: Achieving Fast Over the Air Activation for Wireless Systems.* 1998 IEEE Symposium on Security and Privacy, Oakland, California, May 3-6, 1998.

[3] D. Denning, *et al. A Taxonomy for Key Escrow Encryption Systems.* Communications of the ACM, vol. 39, No. 3, Mar. 1996, pp. 34-40.

US Patent: 6,609,113

Method and system for processing internet payments using the electronic funds transfer network

A system and method for effectuating Electronic Funds Transfer credit messages. The main structural components of the system include a Payment Portal Processor (PPP), an Internet Pay Anyone (IPA) Account, a Virtual Private Lockbox (VPL) and an associated Account Reporter, the existing EFT networks, and a cash card for accessing a VPL or IP account. The PPP is a software application that provides a secure portal for accessing (linking to) either the user's Demand Deposit Account (DDA) or an IPA account, and it can be combined with the functionality of a traditional Digital Wallet. Consumers use a PPP-enhanced Wallet to fund their account, shop on the web, pay bills, pay anyone, store electronic receipts and transaction history, and check their recent PPP-enhanced Wallet activity. The IPA account is a special-purpose account with limited functionality for making electronic payments in the form of EFT credit messages. The VPL is a limited-function, receive-only account for receiving electronic payments through the EFT. The Account Reporter is a portal to view transaction history and balance of IPA and VPL accounts, provide online, real-time transaction reports, and to reconcile accounts receivable/purchase records against incoming EFT payment records. A physical card can be associated with either an IPA or VPL account in order to provide PIN debit capability.

Issued: August 19, 2003

Inventor: Denis O'Leary, *et al*
Assignee: The Chase Manhattan Bank (New York, NY)

References:

[1] O'Mahony, *et al. Electronic Payment Systems.* Artech House, 1997, Chapter 5, pp. 125-133.

[2] Yarden, *Evaluating the Performances of the Electronic Commerce Systems.* Proceedings of the Winter Simulation Conference, 1997.

[3] *Fedwire: How it works*. Last updated May 4, 2003.
www.fraudaid.com

[4] J. Weitzman. *Star Trek Promise Fulfilled: Wireless Cash Transfer.* American Banker.

[5] N. Deighton. *Bluetooth: The Missing Link in Mobile E-Commerce?*. The Gartner Group, Sep. 17, 1999.

[6] R. Egan. *CIO and CEO Alert: Wireless Access is a Growth Enable for E-Business*. The Gartner Group, Nov. 17, 1999.

US Patent: 6,607,136

Physical presence digital authentication system

An interactive authentication system allowing a consumer to interact with a base station, such as broadcast media (e.g, television and radio) or PC, to receive coupons, special sales offers, and other information, with the aid of an electronic card. The electronic card can also be used to transmit a signal that can be received by the base station to perform a wide variety of tasks. These tasks can include launching an application, authenticating a user at a website, and completing a sales transaction at a website (e.g, by filling out a form automatically). The interaction between the base station and the electronic card is accomplished by using the conventional sound system in the base station, so that special reader hardware need not be installed to interact with the electronic card. The user is equipped with an electronic card that can receive and transmit data via sound waves. In the various embodiments, the sound waves can be audible or ultrasonic (which can be slightly audible to some groups of people).

Issued: August 19, 2003

Inventor: Alon Atsmon, *et al*
Assignee: Beepcard, Inc. (Santa Monica, CA)
www.beepcard.com

Beepcard, Inc.
2644 30th, 2nd Floor East
Santa Monica, CA
Telephone: (310) 309-4819

Beepcard, Inc. is a developer and provider of miniaturized wireless authentication and verification systems for a variety of security and mass-market applications. Beepcard offers a reader-free smart card and self-powered digital devices that adhere to the international standards for bankcards. Beepcard, Inc is the maker of Comdot™ technology, a technology that enables a card or credit card to perform wireless communication with a PC, phone and cell phone, without requiring a card reader.

Further Patent Information

To obtain a complete copy of these patents, contact the US Patent and Trademark Office at the address or telephone numbers below:

General Information Services Division
U.S. Patent and Trademark Office
Crystal Plaza 3, Room 2C02
Washington, DC 20231

800-786-9199 or 703-308-4357