Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 6, No. 7. July/August, 2004

Is Your Coke Can Eavesdropping? ... It's NOT the real thing, then!

Have a Coke and a smile? Not if you are worried about security, judging by the fuss over a Coca-Cola Company promotion that puts global positioning system (GPS) and GSM technology into more than 100 cans of Coke.

Randomly inserted into multi-can packages shipped May 17th – July 12th in the United States, the cans look like a standard Coke can, but with a button on the side. Press it, and the system goes into action: First, it uses GSM to call the Coke Unexpected Summer Search Team Headquarters. Once the user agrees to participate in the promotion, the can uses GPS to pinpoint the user's location, and a GSM link sends this data to Coca-Cola. Prizes such as plasma TVs and a Chevy Equinox SUV are then delivered to the user's location. A demo is available at www.unexpectedsummer.com.

> "This is all about thinking innovatively and figuring out new ways to reward and connect directly with consumers," said Steven Schiller, Group Director, Coca-Cola Brand Business Unit, Coca-Cola North America.

Not everyone thinks that is a great idea.

The U.S. Navy, for example, sees them as an eavesdropping threat in classified meetings. "We're asking people to open the cans and not bring it in if there's a GPS in it," said Master Sgt. Jerry Meredith, a Fort Knox spokesman. "It's not like we're examining cans at the store. It's a pretty commonsense thing."

This is not the first time Coca-Cola has dabbled in wireless. In the late 1990s, the company began work to equip 500,000 vending machines with wireless, initially to report inventory and jams, and eventually to allow customers to charge sodas to their cell phones. Soda machines rival water coolers for facilitating office scuttlebutt, but these so-called "intelligent vending machines" support only data, not voice, so they are apparently not perceived as an eavesdropping threat.

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...

September 15th 2004.

Future Topics

Light-weight Security Protocols • Security for UWB • MANET Security • Radius for Wireless • Handheld Device Security • 4G Security • Zigbee Security • PKE-enabled Wireless

Wireless Security Perspectives (ISSN 1492-806X (print) and 1492-8078 (email)) is published 11 times a year 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.

Crypto Question

Question: How do I secure my home wireless system so that other people cannot connect through my router?

Jess Faro, England

Answer: You should enable the built-in Wi-Fi authentication and encryption capabilities, at a minimum. These are likely WEP, although Wi-Fi Protected Access (WPA) is becoming increasingly available (and WPA is preferred, since it is somewhat more secure). For WEP this normally requires that you enter a keyword in your router (usually accessible via a web browser) and then enter the same keyword in each computer on your network. This keyword will be turned into a 40-bit or 128-bit key.

If entering the keyword does not seem to work, you may be able to enter the key numerically (through the use of hexadecimal digits, 0-9, A-F).

Some software will associate the key with a network so that if some of your computers are used on multiple wireless networks, they will pick the right one. In order to do this, the network name broadcast by the router (the SSID) should be distinct. Do not leave it as the default!

If you are truly paranoid or want to minimize the likelihood of compromise, consider a defense-in-depth strategy. NIST offers help in Chapter 3, Section 8 of SP 800-48, (available as a PDF file). Employ the mechanisms that are appropriate to your situation, choosing from what is suggested in Table 3-3 (security mitigation checklist) and Table 3-4.

The Bell Labs Privacy-Conscious Personalization Framework

Rick Hull, Peter Patel-Schneider, Bharat Kumar, Arnaud Sahuguet, Avinash Vyas, Sriram Varadarajan, and Daniel Lieuwen

Mobile, ubiquitous communication and computing devices enable a broad variety of new services and service combinations. They also have the ability to collect a wealth of data about subscribers and their activities. The upshot is that new freedom for users requires more responsibility from service providers.

Subscribers should have simple and natural access to the new services. This includes providing a seamless experience of the "converged" network, which spans combinations of wireline, wireless and the Web. That achievement would simplify the task of contacting other users via voice or data without needing to remember multiple phone numbers or e-mail addresses. It also would gradually give more decision-making power to the network in terms of, for example, call forwarding and blocking, message screening and revealing real-time context information to others. At the same time, however, service providers must safeguard subscriber data so that users can easily specify which information can be shared with whom and in which situations.

Existing approaches to supporting data privacy are largely focused on conventional data management environments and do not address a key issue stemming from mobility: They are not *context-aware*. In other words, they do not support the possibility that a user's willingness to share data may depend in part on factors such as the user's location and recent or current activities. This article introduces one of the key technologies that will give users personalized, context-aware controls over how their data is shared. This technology is embodied in the Privacy-Conscious Personalization (PCP) framework being developed at Bell Labs. It provides a policy-management infrastructure for personalizing telecom and converged services.

In an environment of mobile and ubiquitous computing, the network will have access to a wide variety of user profile data. One type is relatively "static" data, which is information that changes relatively infrequently. Examples include a user's address book, buddy lists, calendar and favorite restaurants. Another type is "dynamic" data, which typically includes user presence, user location and user device status (e.g., currently in a call and with whom). Dynamic data will come from diverse sources, including the mobile network infrastructure, the wire-line telephony network, and Internet access providers, especially including local and wide-area mobile networks.

Quote of the Month

"Better to remain silent and be thought a fool than to speak out and remove all doubt."

Abe Lincoln

Both static and dynamic user data should be shared only when the user desires it. Users will want to personalize sharing of their profile data in two fundamental ways: to block access in some cases, and to filter the information returned in other cases. Blocking, for example, might show presence to boss only on company-supplied devices, and show presence to family on all devices. Governments are mandating that such privacy protections be made available. For example, the European Union recently asked for changes to be made to Microsoft's Passport service. Many upcoming standards, including OMA, 3GPP and GUP, aimed at offering unified access to user profile data, include stringent privacy requirements.

The core idea of the PCP framework is to put a mediating policy infrastructure on top of one or more legacy (profile) data stores, in order to provide the user both access control and data interpretation. Central to the system is the Vortex rules engine (also called "Houdini"), which can both filter and block access to user data. As suggested in **Figure 1**, when used in the PCP framework, the Vortex engine incorporates three kinds of information when deciding what to share:

a. The requester's context, including who is making the request and what device is being used;

b. The user's data, both static and dynamic;

c. The user's preferences.

Are You the Arcanist?

The question last month gave the series:
9, 45, 161, 405, 825, (N) ....
This is a polynomial series {for i: 1, 2, 3, 4 ,5} using the formula:

$$8(\mathbf{i})^3 - 8(\mathbf{i})^2 + 4\mathbf{i} + 5 = \mathbf{N}$$

For i = 6, N = 1469

The first person to answer correctly was Simon Arcand (Magma), followed quickly by David Ott (Qualcomm) and Chuck Magarian (AT&T Wireless). Cheers and congratulations to all three.

Next ...

Can you provide the next in the series:
49921, 49927, 49937, 49939, 49943, 49957, 49991, 49993, ?

Submit your answer to wsp@cnp-wireless.com and if you are the first (or maybe the second) to give the correct answer, we will send you our environmentally-friendly golf shirt, made from recycled cotton – free.

This information is used to determine which of the user's data should be revealed, to whom it will be revealed, and with which types of filtering or interpretation. More subtly, the preferences may include guidance on the user's view of the requester (e.g., is he a colleague, or a friend), the user's interest in the request and requester, and the user's current context (e.g., at work vs. with family, or in a high-priority meeting vs. doing background work).

> Note: The user, under the above circumstances, is the target of the requester (and some would say the user is then the 'requestee'). The requester seeks to establish a connection with the user's device.

One way to get a better sense of how the PCP framework works is to look at the Bell Labs iLocator system, which was policy-enabled to support rich personalization of data privacy. The iLocator system provides a variety of location-aware services, including the ability to display the locations of one's buddies, or a selected subset of them, on the mobile device. The iLocator system runs on top of the MiLife Intelligent Services Gateway (ISG). A key aspect with systems such as iLocator, that share personal context information, is how users are given control over who can see them and under what circumstances. In the PCP framework, the personalization infrastructure involves:

a. A Web Forms interface for gathering user preferences.

b. The Vortex engine and a ruleset for interpreting user context information and preferences.

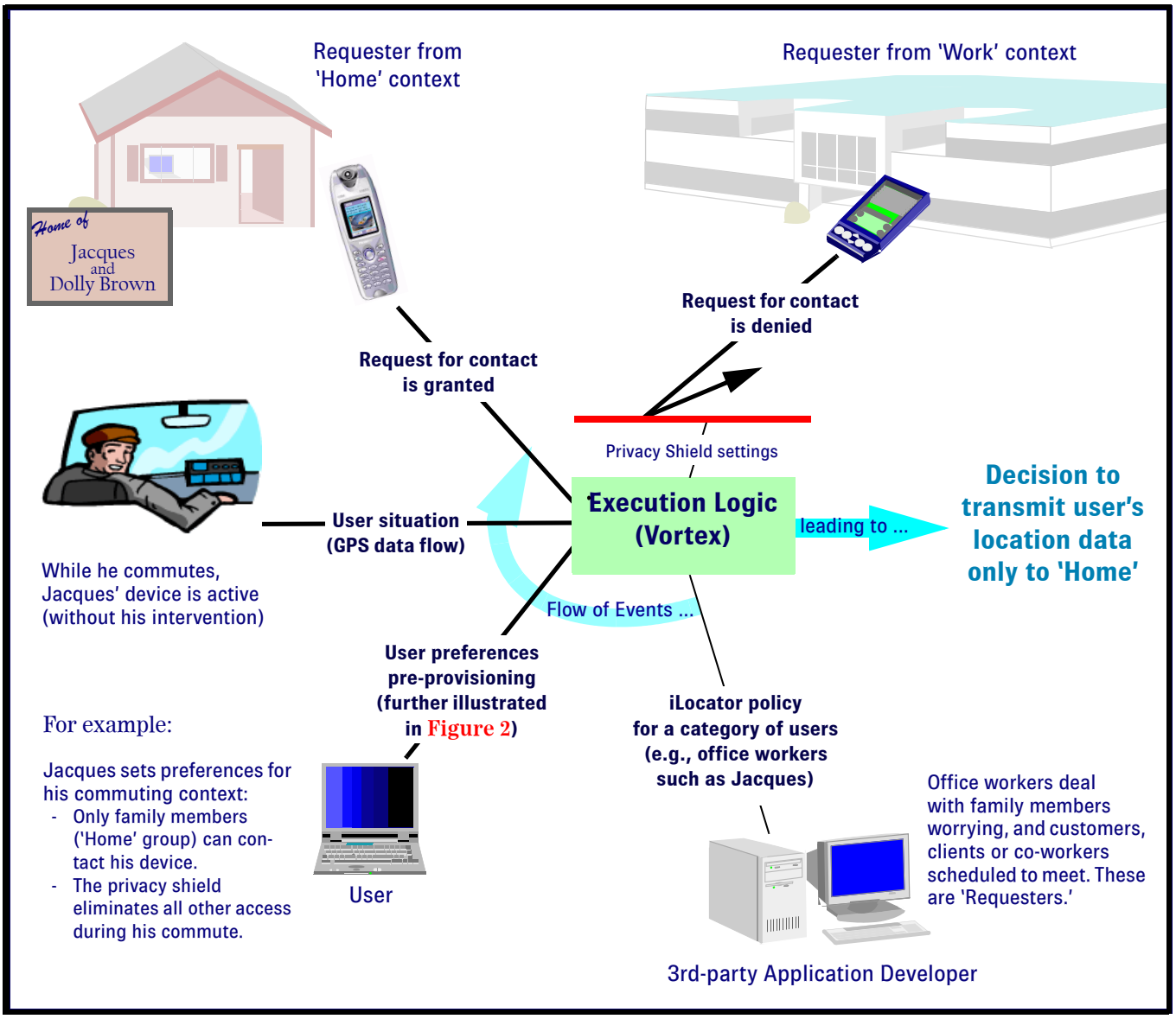
c. Hooks in the service, so that personalization decisions can be requested from the Vortex engine.

The Bell Labs prototype allows users to name different "contexts," such as work, home, family, shopping, and tennis. They also can specify indicators about when they are *in* those contexts . These could be based on time of day, day of week, location, and calendar entries. Finally, users can specify: (1) preferences concerning what they see on their handset, based on current user context, and (2) who can see their location, based on the requestor and the current user context. Users can adjust their preferences at any time, through a browser window, and they can see the system-inferred context and explicitly override it if they wish.

The Policy Management Infrastructure

A fundamental choice in designing the PCP concerns which form of policy management to support. The customization infrastructure commonly used today, especially for most Web applications, is *value-based*: The core logic of an application or service is essentially static, but users (or sometimes the applications themselves using some data-mining and machine-learning techniques) can provision a collection of personalized values. These are interpreted to obtain customized behaviors. But looking forward, we expect vast richness and variability in anticipated composite

Figure 1: Typical Elements in a Personalized Decision



applications (e.g., Web services) and the richness of user status information stemming from mobile and ubiquitous computing.

If value-based policy is used for data sharing privacy in that context, then either the user will have very limited control over how personal private data is shared and interpreted, or application developers will have to create very expressive systems, where users will have to provision huge volumes of preferences. A better approach is to use rule-based policy management, where users can express their preferences at a higher, more generalized and more succinct manner than is possible with value-based customization.

With rule-based customization, the user preferences can be translated into rules that impact values used by the application, and in some cases, they compel changes to portions of the *core logic* of the application itself.

Bell Labs designed the Vortex rules engine to have the expressive power needed to support rules-based policy-enablement of telecom device user services and applications, while also providing high performance and scalability.

The Vortex engine follows the IETF and Parlay/OSA approach to policy enablement of applications, which includes a strict separation between the application and the policy-management infrastructure. This is analogous to the separation typically found between an application and a database server. The Vortex rules language is based on production-style rules. In particular, it supports variables of complex types built up from scalar, record, and list, and it supports forward rule chaining (but no recursion).

The Vortex engine has been productized by Lucent Technologies' Mobility IN business unit. The first product including Vortex is the MiLife ISG, a Parlay/OSA gateway. There are plans to incorporate Vortex into Lucent's SurePay billing system and to provide Vortex as a generic platform component that can be used by other Lucent applications.

Self-Provisioning of Preferences

It is clear that users cannot be expected to specify their preferences by creating rules in the Vortex rules language. Rather, they will be given a *preference palette*, which is a family of Web forms and cell-phone controls for creating, managing, and overriding their preferences.

Figure 2 illustrates some representative Web and cell-phone forms that might be used to gather preferences and overrides in the personalized iLocator system. In this example, users can define a variety of contexts (e.g., work, family, shopping) and specify rules so that the network can automatically infer the user's current context. For example, context is inferred from: "if between 9 AM and 5 PM on a weekday and if within one mile of my office, then I'm working." Additional forms can be used to specify, for each context, which buddies, groups of buddies, and enterprises should be displayed on the user's handset. Yet another form can be the "Privacy Shield," whereby users can specify who can see their location, depending on their current context.

A central premise of the PCP framework is that a "one-size-fits-all" approach to personalization will not always work. Different classes of users, such as students, salespeople, office workers, will base their privacy preferences on different factors. As suggested in **Figure 2**, the PCP framework supports the creation of different preference palettes for different classes of users.

How much development activity and time is needed in personalizing a new service for a given class of users? A design phase is needed to understand which data is relevant to how a user will want to control the service and how the users will want to organize their preferences. For example, in the preference palette of **Figure 2**, a key aspect was to infer "context" based on a variety of factors, and use context to infer when to share location. These factors are context building-blocks such as home, work, commute, shopping, day, hour, week, potential requesters (names of people or groups, and their respective devices types), and prioritizations, such as urgent, ordinary and low priority.

Using these data, Web forms must be created using software automation to harvest the user preferences, a database schema must be created to hold the preferences, a Vortex ruleset must be created for interpreting the preferences, and hooks must be incorporated into the service to request Vortex decisions.

In the PCP vision, essentially all of the specification will be at a high-level, and in particular, the logic for personalization is specified in the Vortex rules language rather than C++ or Java. Automatic code generation will be used to create the actual Web and cell-phone forms. This design will foster the creation of personalization infrastructure for a wide variety of services and classes of users.

Related Research Directions

The work at Bell Labs on data privacy describes part of a larger effort focused on enabling ease-of-use and personalization for the rich converged services that will be available in the future. Three additional components of that effort should be mentioned: machine learning of rulesets, policy management, and data consolidation.

Machine Learning

Self-provisioning of rulesets can be a significant burden on users, even when assisted by the sort of user interface described above. One option is to provide some sort of automatic methods for the generation of rulesets. We propose that machine-learning techniques could be usefully applied.

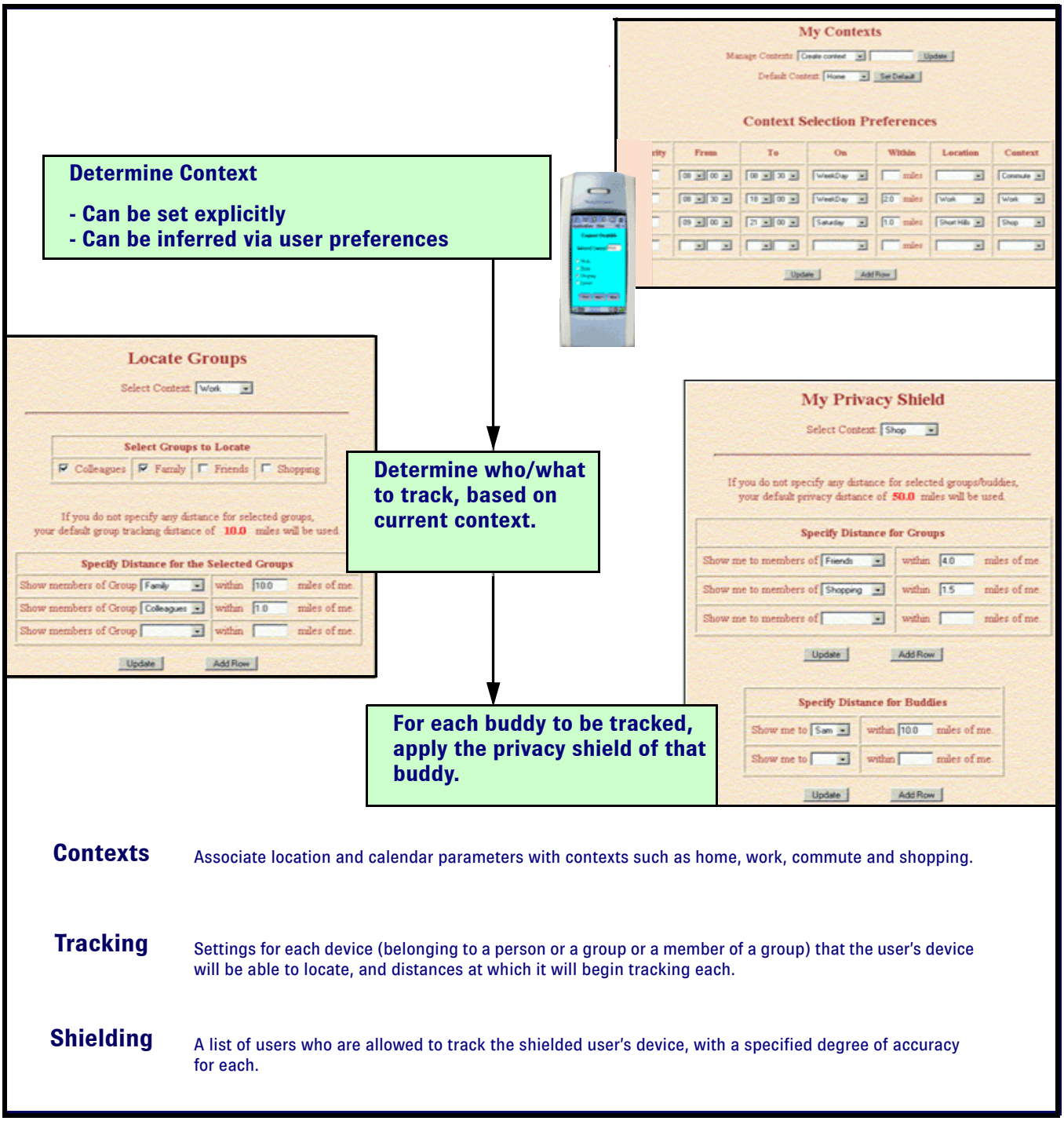
Although there has been considerable research on machine learning, the context of personalizing services and data privacy has unique requirements previously unaddressed. Chief among these is that the learned rules should be understandable by users, both so that they can have some confidence that the learned rules are reasonable and so that they can modify the learned rules as appropriate. For these reasons we envision using a learning algorithm similar to the Slipper system [5], which produces compact and comprehensible collections of rules.

Furthermore, we expect to be able to exploit the structure of the Vortex rulesets arising in the PCP. In particular, it is natural to view these rulesets as capturing a "decision flow" having the form of a directed acyclic graph, where the target parameters (e.g., should my location be shared?) are based on intermediate parameters (e.g., what is my current activity?, what is the relationship of the requester to me?), which in turn are based on other intermediate parameters or input parameters.

Managing the 'Norm'

Policy management will become increasingly widespread in telecom networks. This trend is indicated by the various standards groups developing policy management standards, including: OMA's privacy protocol PCP; and 3GPP's architectures for Location privacy, Presence privacy, and Generic User Profile privacy. As a result, it is useful to develop principled approaches to designing rulesets – for example, to develop "normal forms" for rulesets.

Figure 2: User Forms: Preferences Provisioning and the Logic That Uses It



It will also be useful to develop approaches for combining rulesets, perhaps in a manner reminiscent to federated databases. In particular, it would be desirable let users specify their preferences through a single, unified interface, even if the generated rules will be mapped to a number of different policy engines residing in scattered parts of the network. A preliminary investigation into this approach is discussed in an article published in an IEEE International Workshop proceedings [4].

Data Consolidation

The overall PCP framework is depicted in Figure 3. The PCP sits between the various network components and an application layer. A key component of the PCP, along with the policy engine, is data consolidation.

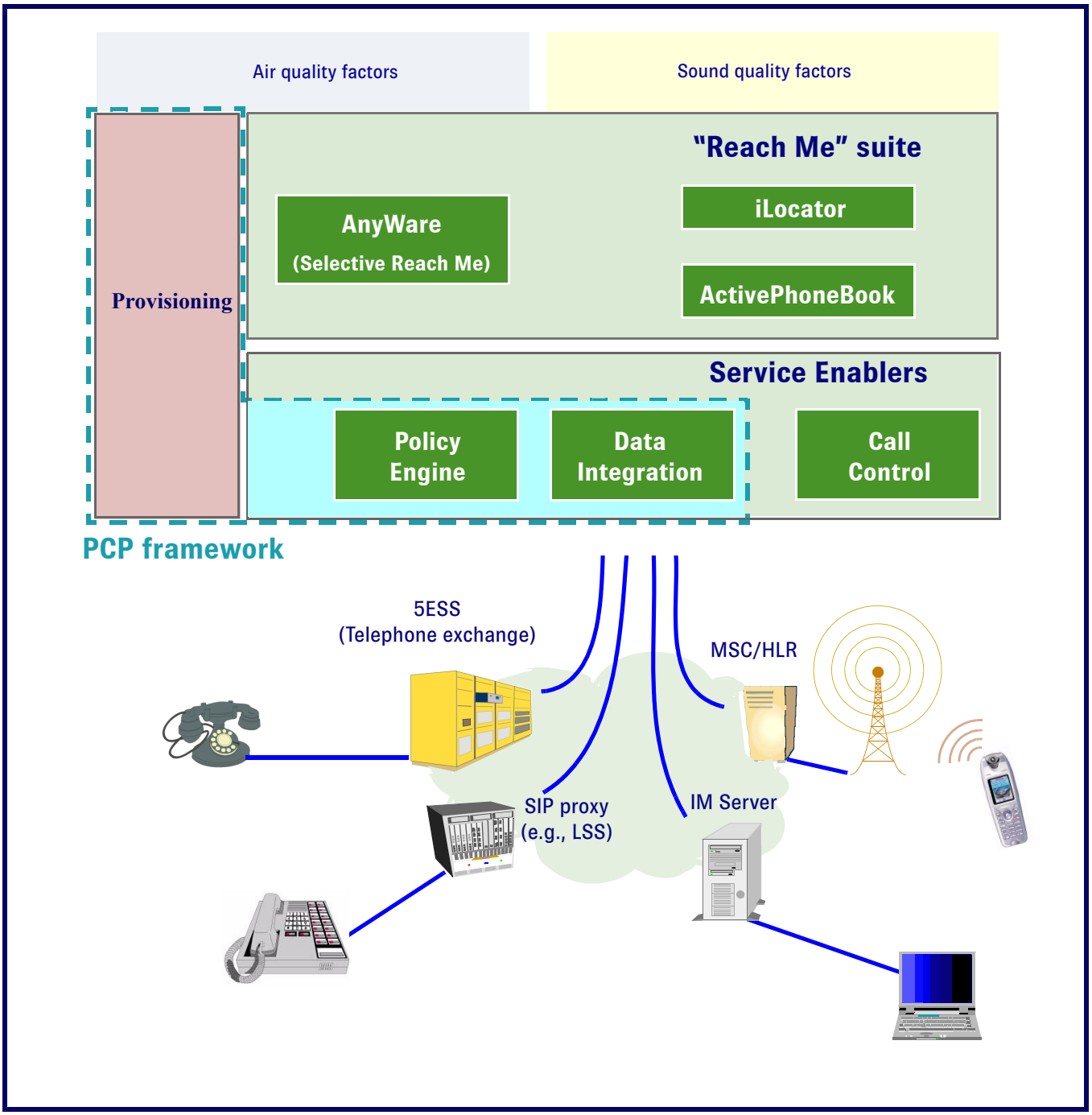
Today there is a plethora of subscriber-relevant data residing in a vast array of heterogeneous components. Many of these are within the network, including the

core communications components (e.g., HLRs, MSCs, AAA servers, and push-to-talk servers), in subscriber provisioning databases and portals, and in targeted services (e.g., location services, presence services and notification services).

Bell Labs is developing a high speed data consolidation platform that will provide applications within the network a single-point-of-access for the data. That platform will use a combination of federated (virtual) and warehousing (materialized) technologies to enable a variety of performance trade-offs.

Note: Data sources outside the network are also relevant to services personalization. These include such things as address books and calendars, which may be on handheld devices, behind corporate firewalls, or on ISP portals. A complementary data consolidation project [3] is focused on sharing profile data *across network boundaries*, in a manner that will comply with the emerging 3GPP Generic User Profile (GUP) standards.

Figure 3: The PCP Framework and its Surrounding Environment



Further Reading

[1]. R. Hull, B. Kumar, D. Lieuwen, P. F. Patel-Schneider, A. Sahuguet, S. Varadarajan, and A. Vyas. *Everything Personal, Not Just Business: Improving User Experience Through Rule-based Service Customization*. Proc. of Int'l. Conf. on Services Oriented Computing (ICSOC), Trente, Italy. December, 2003.

[2]. R. Hull, B. Kumar, D. Lieuwen, P. F. Patel-Schneider, A. Sahuguet, S. Varadarajan, and A. Vyas. *Enabling Context-Aware and Privacy-Conscious User Data Sharing*. Proc. of Int'l. Conf. on Mobile Data Management (MDM), Berkeley, CA. January, 2004.

[3]. A. Sahuguet, R. Hull, D. Lieuwen, and M. Xiong. *Enter Once, Share Everywhere: User Profile Management in Converged Networks*. Proc. of the Conf. on Innovative Database Research (CIDR), Asilomar, CA. January, 2003.

[4]. R. Hull, B. Kumar, and D. Lieuwen. *Towards Federated Policy Management*. IEEE 4th Int'l. Workshop on Policies for Distributed Systems and Networks (Policy2003), Lake Como, Italy. June, 2003.

[5]. W. W. Cohen and Y. Singer. *A simple, fast, and effective rule learner*. Proc. of the Nat'l. Conf. on Artificial Intelligence. AAAI Press, 1999.

About the Authors

The work described in this article was performed by several members of the Network Data and Services Research Department at Bell Labs, a division of Lucent Technologies. This department performs research and technology transfer activities in the areas of data management, policy management, and converged services (including both telecommunications and Web services).

Rick Hull, the group leader, received his Ph.D. from the University of California, Berkeley, in 1979. He co-authored the text *Foundations of Databases* and has published extensively in the areas of database theory, data management, workflow and Web services.

Peter Patel-Schneider received his Ph.D. from the University of Toronto in 1987. He is widely published in the areas of description logics and automated reasoning, and has been a primary contributor to W3C's OWL standard.

Bharat Kumar received his Ph.D. from The Ohio State University in 1995. He has published in the areas of Web technologies, workflow, and policy management, and serves as the chief research architect for the Vortex rules engine.

Arnaud Sahuguet received his Ph.D. from the University of Pennsylvania in 2001. He has published in the areas of database management and XML, and is a key contributor to the 3GPP Generic User Profile (GUP) activity.

Avinash Vyas received his M.S. degree from the Indian Institute of Technology, Kanpur, India, in 2001 and is working on XML technologies and services personalization.

Sriram Varadarajan received his M.S. degree from the Indian Institute of Technology, Kanpur, in 2001, and is working on policy and data management infrastructure for services personalization.

Daniel Lieuwen received his Ph.D. from the University of Wisconsin in 1992. He has published in the areas of database management, optical networking and Web technologies. He is currently working on personalization technologies and data integration.

About Bell Labs and Lucent

db.bell-labs.com

Lucent, headquartered in Murray Hill, NJ, offers products for the largest communications service providers. Bell Labs supports Lucent with its research and development efforts to develop next-generation software, services and equipment for mobile, optical and data/voice networks.

U-R-Linked: WiFi Phones ... and More

wirelessbandit.nerdsunderglass.com

WiFi users are organized – or getting there, at least. Many of them converge at Wireless Bandits to offer amusing and interesting blog postings. At the top of their discussion recently is WiFi phone service.

WiFi phone (or WiFi VoIP) is an emerging technology. Initial testing occurred in New Jersey earlier this year, and a limited area of Michigan recently became its first debut in the U.S. It is available as an alternative to standard and specialized wireline phone services, and with its exceptional bandwidth performance, chances for its commercial viability are likely.

Particular advantages include: (1) Boaters 20 miles offshore could have the same wireless services offered to residences or businesses and; (2) tourists may sign up for access while within the broadcast range, and only their computer is needed to do so – no need to download special software, and no need to call a customer support representative.

Introduction of dual mode phones (WiFi/cellular) can be expected to accent its chances. Meanwhile, local-loop phone services may eventually find themselves choking on the dust of antiquity.

Upcoming Mobile & Wireless and Wireless Security Events

The following are mobile & wireless and wireless security events for August that may be of interest. The name, dates and venue of the event, plus URL, are provided.

SANS Cyber Warrior 2004
1st- 2nd August
JW Marriott Hotel
Washington, DC
www.sans.org/cyberwarrior_dc04

HP Wireless and Mobility Roadshow 2004
3rd August
Hyatt Regency Austin
Austin, TX
www.winnetmag.com/roadshows/mobilewireless/index.cfm

ESAS 2004 (1st European Workshop on Security in Ad-Hoc and Sensor Networks)
5th– 6th August
Eurescom Conference Center
Heidelberg, Germany
www.netlab.nec.de/esas/esas2004.html

11th Annual Workshop on Selected Areas in Cryptography
9th- 10th August
University of Waterloo
Waterloo, Ontario, Canada
vlsi.uwaterloo.ca/~sac04

Information Technology Exposition (Department of Veterans Affairs)
9th- 12th August
Hilton Austin
Austin, TX
www.technologyforums.com/vaitc/index.asp

13th USENIX Security Symposium
9th- 13th August
Town & Country Resort and Conference Center
San Diego, CA
www.usenix.org/events/sec04

CHES 2004 (Workshop on Cryptographic Hardware and Embedded Systems)
11th- 13th August
Boston Marriott Cambridge
Cambridge, MA
security.ece.orst.edu/ches/ches2004

MWN 2004 (Internaitonal Workshop on Mobile and Wireless Networking)
15th- 18th August
Hotel Omni Mont-Royal
Montreal, Quebec, Canada
cs.ua.edu/mwn

[Note: This event is held in co-location with The 2004 International Conference on Parallel Processing – ICPP-04]

Crypto 2004 (24th Annual International Cryptology Conference)
15th- 19th August
University of California, Santa Barbara Campus
Santa Barbara, CA
www.iacr.org/conferences/crypto2004

Asia/Pacific Ubiquitous Mobility Conference
17th August
Star City Hotel Pyrmont
Sydney, Australia
www.idc.com.sg/Mobility2004/agenda.asp

[Note: This 1-day IDC event is held in several other Asia/Pacific locations during August]

Information Security World Australia 2004
23rd- 24th August
Sydney Convention and Exhibition Center
Sydney, Australia
www.isecworldwide.com/2004/isw_AU

WISA 2004 (Workshop on Information Security Applications)
23rd- 25th August
Ramada Plaza Jeju Hotel
Jeju Island, Korea
dasan.sejong.ac.kr/~wisa04

ICETE 2004 (International Conference on E-Business and Telecommunication Networks)
25th- 28th August
Polytechnic Institute of Setúbal
Setúbal, Portugal
www.icete.org

SIGCOMM 2004 (Special Interest Group on Data Communication)
30th August – 3rd September
Hilton Portland and Executive Tower
Portland, OR
www.acm.org/sigs/sigcomm/sigcomm2004

P2P2004 (The 4th IEEE International Conference on Peer-to-Peer Computing)
25th- 27th August
IFW Building
Zürich, Switzerland
femto.org/p2p2004

Fraud and Security Patent News

US Patent: 6,763,366

Method for calculating arithmetic inverse over finite fields for use in cryptography

The present invention is a method for calculating greatest common divisors (GCD) and modular inverses using the extended Jebelean GCD algorithm, which keeps track of the number of times that U3 and V3 have been divided by two in the process of calculating the greatest common divisor and corrects the modular inverse for these divisions. The shifting of the binary values representing U3, that occurs during the calculation of the GCD, is accomplished by changing the position of respective pointers to bit positions in the binary values rather than implementing a shifting operation.

Issued: July 13, 2004

Inventors: Lazlo Hars and Gregory Perkins

Assignee: Matsushita Electric Industrial Co., Ltd. (Osaka, Japan)

US Patent: 6,763,315

Method of securing access to a user having an enhanced security proximity token

The present invention provides a method to determine the proximity of a user having a first electronic device to a second electronic device for allowing the user access to the second electronic device. The method includes the steps of transmuting data in a plurality of signals at different frequencies to establish communication between the first electronic device and the second electronic device. The method further includes detecting the plurality of signals at the different frequencies with the first electronic device. The method is characterized by determining an overall signal strength from the predetermined number of measured signals strengths, and comparing the overall signals strength to a predetermined threshold for enabling the second electronic device in response to the overall signal strength being above the predetermined threshold. The subject invention allows for increased security for systems that communicate via frequency hopping spread spectrum by determining the overall signal strength from the measuring of multiple signals detected at different frequencies.

Issued: July 13, 2004

Inventor: Thomas Xydis

Assignee: Ensure Technologies, Inc. (Ann Arbor, MI)

www.ensuretech.com

Ensure Technologies
3526 W. Liberty Road
Suite 100
Ann Arbor, Michigan 48103

Telephone: (734) 668-8800
Fax: (734) 668-1242

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. We brief ly describe it and provide, at minimum, its inventor(s) and assignee (owner).

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, straight from an attorney's word-processor. Sometimes we edit the abstracts for readability when the legalese is too impenetrable.

US Patent: 6,763,250

Rapidly-deployable fixed wireless communication system and method of switching during operation of same

The present invention describes a fixed wireless communication system that comprises a wireless subsystem and a backbone network. The wireless subsystem includes at least one base transceiver site and at least one stationary remote unit. The stationary remote unit communicates with the base transceiver site via a wireless communication resource. The wireless subsystem resides in a first geographic area served by a first public switched telephone network (PSTN) access switch. The backbone network includes at least one point of presence (POP) and a switch. The switch serves to at least route voice communications between the stationary remote unit and a PSTN subscriber unit residing in a second geographic area served by a second PSTN access switch. The POPs couple the switch to at least the wireless subsystem, the first PSTN access switch, and the second PSTN access switch. The switch employs a method to facilitate communication between a wireless subsystem subscriber and either a PSTN subscriber or another wireless subsystem subscriber, wherein a switching path is established to include a PSTN access switch only in the event that received call set-up information indicates that the communication involves a PSTN subscriber.

Issued: July 13, 2004

Inventor and Assignee: Joseph Forbes, Jr.

US Patent: 6,763,112

Security procedure in universal mobile telephone service

This invention discloses a security procedure for a Universal Mobile Telephone Service (UMTS) mobile communication system that includes detecting a communication failure between a Radio Network Controller (RNC) which controls radio coverage within a prescribed geographical area and a Mobile Station (MS) in the geographic area, authenticating the MS and setting a new security parameter in response to the communication failure. The security parameter to be changed may be a ciphering key CK or an integrity key IK. Moreover, the steps of authenticating and setting a new security parameter may be performed separately or simultaneously.

Issued: July 13, 2004

Inventor: Serge Haumont
Assignee: Nokia Networks Oy (Keilalahdentie, Finland)

US Patent: 6,763,014

Intelligent communication node object beacon framework (ICBF) with temporal transition network protocol (TTNP) in a mobile ad hoc network

The present invention describes a method for managing and controlling the discovery and maintenance of routes in a mobile ad hoc network that includes transmitting beacon signals from each mobile node, determining a node or group condition at each mobile node, and varying the beacon signals based upon the determined node/group condition. The mobile ad hoc network includes a plurality of wireless mobile nodes and a plurality of wireless communication links connecting the nodes together. Route tables are built and updated at each mobile node, with a first one of proactive and reactive route discovery processes to define routes in the network. The beacon signals are received and node/group condition information is stored at each node. Route stability over time is predicted based upon the node/group condition information, and when predicted route stability reaches a first transition parameter, the method switches to a second one of the proactive and reactive route discovery processes.

Issued: July 13, 2004

Inventor: Robert Kennedy
Assignee: Harris Corporation (Melbourne, FL)

Notable References:

[1] Van Dyck, et al. *Distributed Sensor Processing Over an Ad-Hoc Wireless Network: Simulation Framework and Performance Criteria.* Proceedings IEEE Milcom, Oct. 2001.

[2] Zhu, *Medium Access Control and Quality-of-Service for Mobile Ad Hoc Networks.* Ph.D. thesis, Department of Computer Engineering, University of Maryland, College Park, MD, 2001.

[3] Park, et al. *Temporally-Ordered Routing Algorithm (TORA) Version 1 Functional Specification.* Internet Engineering Task Force (IETF) MANET Working Group, Internet Draft, Jul. 20, 2001.

[4] Ogier, et al. *Topology Broadcast Based on Reserve-Path Forwarding (TBRPF)*, Internet Engineering Task Force (IETF) MANET Working Group, Internet Draft, Jan. 10, 2002.

US Patent: 6,760,843

Maintaining a soft-token private key store in a distributed environment

The present invention includes methods, systems, and devices for securely updating private keys, key pairs, passwords, and other confidential information in a distributed environment. A transaction is created including appropriate encrypted soft-token content, and then transmitted to a new location. Comparisons are made to determine whether the new soft-token content should be recognized as authentic and entered at the new location. Updates are accomplished without ever sending the plain text form of a key or a password across the wire between the distributed locations.

Issued: July 6, 2004

Inventor: Stephen Carter
Assignee: Novell, Inc. (Provo, UT)

Notable References:

[1] Wilson, Stephen: *Certificates and Trust in Electronic Commerce*; 1997 MCB UP Limited, vol. 5, issue 5, p. 175-181.

[2] Bellare, et al. *Provably Secure Key Distribution – The Three Party Case.* 1995.

[3] Bird, et al. *The KryptoKnight Family of Light-Weight Protocols for Authentication and Key Distribution.* Feb. 1995.

US Patent: 6,760,841

Methods and apparatus for securely conducting and authenticating transactions over unsecured communication channels

The subject invention describes a transaction processing system that employs an authentication device which receives identifying and authentication information from a token such as a credit or debit card. The authentication device forms an information block comprising the identifying and authentication information, and encrypts the information block using a preprogrammed key. The information block is transferred to a transaction terminal such as a merchant terminal or customer computer, and it is subsequently transferred to an authorizing server. The authorizing server transfers the information block to an authenticating server, which decrypts the information block, extracts the identifying and authentication information and compares the identifying and authentication information against similar information accessible to the authenticating server. The authenticating server instructs the authorizing

server to accept or reject the transaction based on the result of the comparison. Alternatively, a self-authenticating token may be employed in which authentication information characteristic of the token is converted to a numerical format, encrypted and stored on the token. The authentication device decrypts the numerical representation of the authentication information and compares it against the actual authentication information. The authentication device accepts or rejects the transaction based on the result of the comparison.

Issued: July 6, 2004

Inventor: Alberto Fernandez
Assignee: XTec, Incorporated (Miami, FL)

www.xtec.com

XTec Incorporated
5775 Blue Lagoon Drive
Suite 280
Miami, Florida 33126

Telephone: (305) 265-1565
Fax: (305) 265-1569

US Patent: 6,760,804

Apparatus and method for providing an interface between legacy applications and a wireless communication network

This invention discloses an apparatus and method for interfacing legacy applications with a wireless communication network. Specifically, the present invention discloses an integrated hardware device that creates and manages a virtual serial communication port. The virtual port is presented, to legacy applications and an operating system in a computer system, as a serial communication port having a UART device. An interface application ensures legacy application compatibility with the wireless communication standard, including a Bluetooth communication standard.

The interface application converts outgoing data from the legacy application into a format associated with the Bluetooth communication standard. The interface application converts incoming data from a format compatible with the wireless communication standard to a format compatible with a bus and the legacy application located on the computer system. The virtual serial communication port and the integrated hardware device have device stacks compliant with a Windows™ driver model (WDM).

Issued: July 6, 2004

Inventor: Elwin Hunt, *et al*
Assignee: 3Com Corporation (Santa Clara, CA)

Notable Reference:

[1] Hwa Jong Kim and J.P. Linnartz. *Virtual cellular network: a new wireless communications architecture with multiple access ports.*

US Patent: 6,760,444

Mobile IP Authentication

Methods and apparatus for authenticating a mobile node. A server is configured to provide a plurality of security associations associated with a plurality of mobile nodes. A packet identifying a mobile node may then be sent to the server from a network device such as a Home Agent. A security association for the mobile node identified in the packet may then be obtained from the server. The security association may be sent to the network device to permit authentication of the mobile node. Alternatively, authentication of the mobile node may be performed at the server by applying the security association.

Issued: July 6, 2004

Inventor: Kent Leung
Assignee: Cisco Technology, Inc. (San Jose, CA)

Notable References:

[1] Uyless Black. 1992. *TCP/IP and Related Protocols.* McGraw-Hill, Inc., pp. 226-249.

[2] G. Montenegro. May 1998. *Reverse Tunneling for Mobile IP*. RFC 2344, Sun Microsystems, Inc., pp. 1-19.

US Patent: 6,760,441

Generating a key hierarchy for use in an isolated execution environment

The present invention is a method, apparatus, and system to generate a key hierarchy for use in an isolated execution environment of a protected platform. In order to bind secrets to particular code operating in isolated execution, the method uses a key hierarchy comprising a series of symmetric keys for a standard symmetric cipher. The protected platform includes a processor that is configured in one of a normal execution mode and an isolated execution mode. A key storage stores an initial key that is unique for the platform. A cipher key creator located in the protected platform creates the hierarchy of keys based upon the initial key. The cipher key creator creates a series of symmetric cipher keys to protect the secrets of loaded software code.

July 6, 2004

Inventor: Carl Ellison, *et al*

Assignee: Intel Corporation (Santa Clara, CA)

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

US Patent: 6,760,438

System and method for Viterbi decoding on encrypted data

This invention discloses a system and method for performing Viterbi decoding on encrypted data. At the receiver, maximum likelihood decoding is performed based on received input in the encryption domain. When selecting a path from one stage of a Viterbi decoding trellis to the next, a local metric may be associated with each of the possible paths based on Euclidean distance between a received symbol and a path state. The path state is determined by encrypting the binary path state. An overall metric is associated with each state equivalent to a sum of local path metrics along a survivor path of selected paths. At the end of the Viterbi decoding trellis, a decoded and decrypted bit sequence is obtained by tracing back in a conventional manner.

Issued: July 6, 2004

Inventors: Yan Kui and Karl Mann
Assignee: Nortel Networks Limited (St. Laurent, CA)

US Patent: 6,760,325

Processing of mobile originated calls in packet switched protocol based communication networks

A method is disclosed for processing a mobile originating telephone call in a packet switched protocol-based communication network comprising a packet switched protocol-based cellular telephone network having a first layer for transferring signaling information assigned to the telephone call being processed by the communication network, a second layer for transferring payload information assigned to the telephone call, and an interface for coupling the cellular telephone network to a further network.

Issued: July 6, 2004

Inventor: Heino Hameleers, *et al*
Assignee: Telefonaktiebolaget LM Ericsson (publ) (Stockholm, Sweden)

Corporate WiFi Security Survey

*iGillot*Research has found that most enterprise wireless LANs are secured. Only 2% have no security.

In about half the cases, though, it is not the built-in security that is being used, but a VPN. This security mechanism allows virtually any external link to be secured, but requires that the wireless LAN be outside the corporate firewall. This makes the use of the wireless LAN less convenient to corporate users ... and may allow people outside the company to access the internet via the wireless LAN, reducing the performance of the network to legitimate users.

Of the survey respondents that had WLANs, 16% used WPA (WiFi Protected Access), while 45% were using a form of the less secure WEP (Wired Equivalent Privacy).

Numbers add up to more than 100% because some companies were using more than one security method. The **graph** sketches the survey's results.

For more information on WEP and WPA, consult our **November 2003, November 2002, January 2002, December 2001** and **February 2001** issues of *Wireless Security Perspectives*.