CASINO$_{ng}$[*]— Towards Secure, Dynamic Group Management in Wireless Personal Area Networks

George Fankhauser, Nathalie Weiler, Germano Caronni
{gfa,weiler,gec}@acm.org
Sensaco Research,[†] Switzerland[‡]

Abstract

With the advent of more and more small devices with networking capabilities, the interest in their secure self organisation has grown. These devices – smartlets as we named them – may have multiple transient ownerships and the resulting trust environment can become quite complex. Our paper takes a look at a fictious next generation casino and some necessary hardware as an illustration, and examines what operations (such as cryptographically secure group management) could become relevant in solving the problems observed there.

1 Introduction

With new research initiatives such as the sixth framework programme it becomes necessary to review previously focused areas and observe trends for future development. For wireless personal area networks (WPANs), we give some examples of fields of recent interest. We will propose solutions and discuss how future work in WPANs could take shape and which issues must not be overlooked.

We name only a few fields that stirred considerable interest in the recent past: (a) *Sensor networks:* passive network nodes, recording data while being pushed around[1]; (b) *Smart dust:* millimeter-scale, mobile devices containing sensors, actors and communications capabilities [2]; (c) *Wearable networks* are emerging in our clothes; networks exist between nodes on one person (body area networks) and between persons that move around and meet; (d) *Smart tokens* such as tags, cards, dongles, jetons, etc. They will be used to enhance other devices (e.g. SIM), perform sensitive operations, help manage or remember complex configurations; (e) *Application specific, single-purpose smartlets,* such as fridge magnets that compile shopping lists and talk to your mobile phone whenever you walk by.

Other "small" digital gadgets such as mobile phones, media players, cameras, PDAs, etc. still tend to be managed directly by their owners. However, there is no distinct line between these classes of device and one could expect to see more devices that work together and share newly created services among each other. Generally, all these examples are part of pervasive computing and networking, or in its final consequence, they will form the ambient intelligence landscape.

When we look at these new fields of research, we recognize a focus on routing in ad-hoc networks, interconnection with fixed networks, physical layer/transmission issues and some transport problems is recognized. Besides, for special purpose demonstrators and prototypes innovative custom hardware has been built.

What has been neglected so far is the aspect of securing such a landscape that *will and has to* become increasingly self-organized. This will happen because of (a) the network nodes ("smartlets") sheer quantity; (b) their continuous shrinking and physical disappearance; and (c) the dedication of simple functions to single or groups of smartlets.

To keep up with managing all the digital stuff around oneself, group policies and tasks have to be defined, instead of trying to control the behaviour of single nodes. Network management in the classical sense is no longer possible and configuration of the network and nodes must be performed with no or only limited human interaction, starting from a very few trusted components.

In such environments, security is the next driver since we do not want arbitrary people to play around with our smartlets or even worse, we need some security services in place to prevent intentional misuse of the little helpers. Specifically we need:

- Authentication for source identification of new members in a group;
- An opaque channel to exchange sensitive data;
- Integrity in potentially hostile environments;
- Defense against malicious attacks and rogue users.

As those services are typically achieved by cryptographic primitives, keys will be used, and these keys should be distributed and maintained as we are considering groups of smartlets with frequently changing memberships.

Some of these systems can reliably perform group tasks under normal conditions and are resistant to failure of single group members because of their distributed structure. However, such built-in reliability is *not sufficient* when groups of network nodes are under specific attacks or when networks are denied of their regular services.

A promising approach to support secure self-organization goes beyond classical security services (i.e. PKI) by employing the services of dynamic trust and reputation management systems.

The next section gives a description of the *CASINO$_{ng}$* scenario with simple and advanced operations. Then it continues with the motivation for group operations and the protocols used to drive them; in Section 3 we assess the current state and future

[*] Name and scenario chosen for illustrative purposes only.

[†] http://www.sensaco.com

[‡] Research supported by the Swiss Federal Offi ce for Education and Science (BBW)

[1] e.g. the factoid project [3] tried to extend this to "remember every piece of information a person encounters during his entire life."

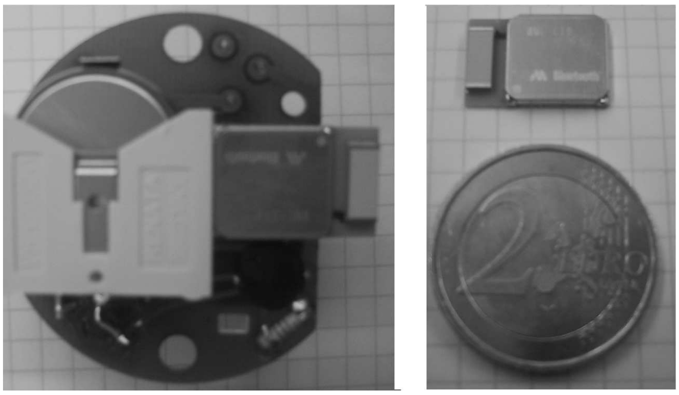

Figure 1: Prototype jeton with network node and radio interface (left); commercial radio module compared to a 2 Euro coin (right).

developments of cryptographic support in very small devices, network technologies and group protocols. Finally, conclusions and future work are discussed in Section 4.

2 Smart Jeton Scenario

We introduce a scenario that is not science-fiction-like in terms of physical requirements but one that introduces all basic problems occurring in dynamic groups of small, mobile network nodes in unfriendly environments. It is a (physical) casino that is run by traditional rules but has smart jetons that feature full wireless networking capabilities. In a more generic formulation it is the idea of combined physical/virtual cash[2]. Such a combination has all the advantages of tangible currency and allows for new applications such as reloading, tracing, counting, and theft prevention.

Although this scenario might not yet seem commercially viable it can be developed as a prototype with components available today. The hardware system shown in Figure 1 measures about 40 mm in diameter and includes everything from the battery to the small custom application processor that implements simple networking functionality. In addition, the application processor features digital and analog signals that are used to connect a simple display and sensors for on-table positioning.

It has to be noted that traditional jetons with security printing (UV, holograms, inlays, microprinting etc.) and serialized numbering have proven to be highly counterfeit resistant. Nevertheless, the gaming industry wants more flexibility and is exploring advances with *passive* jetons that allow for some limited storage of information[3].

2.1 Operations in the $CASINO_{ng}$

The requirements on this jeton software are manifold and are described below by its behaviour. In the casino scenario we distinguish two categories of operations:

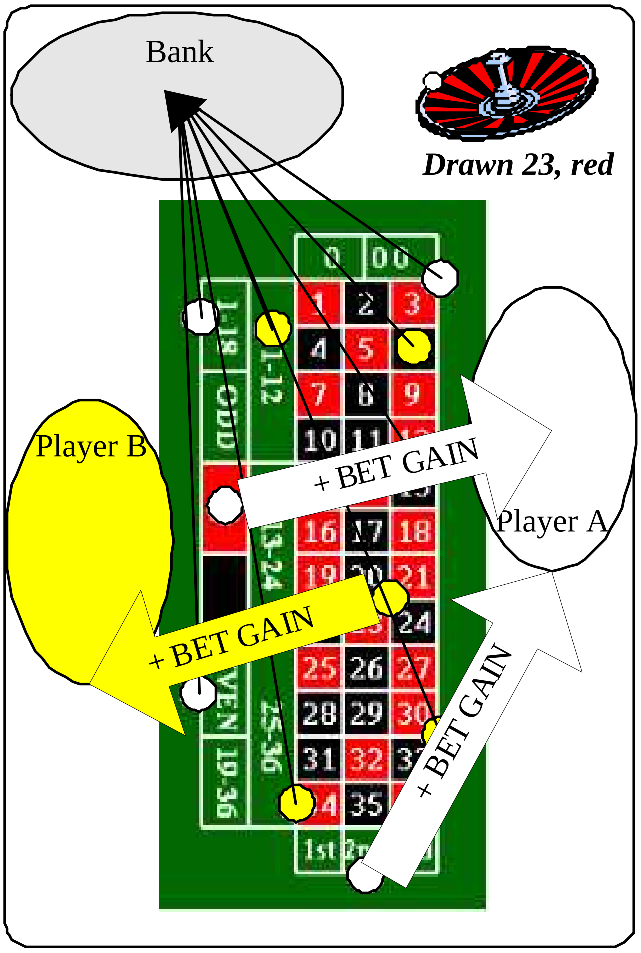

Figure 2: Example of a Roulette Table.

- *Classical operations* encompass basic verification and validation of jetons. Reading the values is used for counting and sorting. Writing “ear-marks” to the jetons allows for more advanced applications such as checking the validity date, adding a group’s or client’s name or even bet tracking. Last but not least, basic verification is used for secure exchange of cash into jetons and vice versa. A part of the operations is depicted in Figure 2 for the example of one roulette game table. The table hosts two players A and B and the bank through the croupier. The players place their bets and the roulette wheel draws Red 23. The largest part of the jetons goes to the bank. Only the numeric bet on “20-24” and the bets on “2nd place” and “red” are winners for player B and A, respectively. They are paid together with the bet gain issued by the bank. In this process, the jetons must be able to communicate their bet to the table and must be verifiable as legitimate jetons. Finally, they must support ownership transfer from the bank to a player and vice-versa.
- *Advanced operations* allow for jetons to interact with other jetons, the games and the environment. Some of the smart jetons can then exchange information about the games and the environment, e.g. statistics, information on rules that may change dynamically, fairness observed, software upgrades, etc. Such information is always signed and forms the basis of the reputation system. This dynamic trust re-

[2] Also proposed for legal tender with high denomination by the European Central Bank .

[3] For example, Philips is producing a ”Vegas”-version of the Hitag RF-ID transponder for gaming applications. It is operating at 125 kHz and comes with a memory size of 256 bytes.

lationships stand in contrast to the initial, static trust relationships given by players, employees of the casino, and other smart jetons that blend into the background (see Section 2.3). The concepts needed to implement these advanced operations will be explained below in Section 2.2.

2.2 Smart Jetons in Groups

For most of the advanced operation described in Section 2.1, the smart jetons should act in a group manner, i.e. not each individual jeton on the same bet should interact with the casino system, but all jetons of the same player on the same bet should be addressed as the smallest single entity – the *bet group* as we call it.

Additional groups are also formed for ease of use in the casino: All jetons in the same game regardless of the bet are grouped in the *table group*[4]. All jetons of the same player are inside the *player group*[5]. And finally all jetons active in the casino games are in the *casino group*.

Thereby, we introduce the concept of *multi-ownership*: a smart jeton may belong to different groups, i.e. it is owned by different groups. We illustrate this concept by describing the group memberships in an example $CASINO_{ng}$ as depicted in Figure 3:

- The *player group* of player A at the roulette table depicted on the left-hand side consists of all greyish jetons on the table and in his pocket. The black one belong to the player group of player B. Typical operations in these groups include ear marking and counting of values.
- The *bet groups* on the table play an important role after the draw. In our example of a roulette table, the bank must determine in a fast manner the *winning and loosing groups*[6] respectively after a draw. The bet groups belong as members to either one of the two. The loosing group is moved to the bank, i.e. they leave the player group and become members of the bank group. The members of the winner group are added the gain according to the parameters of the bet and return to the respective player. their bet. The bet group forms an easier manageable entity for the player: Instead of issuing an order to each one of the smart jetons, this order must only be sent to the bet group. E.g. 6 jetons on bet “red 16” should be moved to “red 19” or the value of this bet should be increased from 20 Euros to 60 Euros, table limit permitting, etc.
- The *table group* is important for the correct and fair play assuring that no jetons are moved after “les jeux sont faits”. The other operations on this group after the draw process were discussed above.
- The *casino group* assures the administration of the $CASINO_{ng}$: On one hand, the performed operations in this group allow for statistics and planning (which games are popular at what time, which bet behaviour exists in which games). On the other hand, through tracking operations the organisational security is ensured, i.e. fraud and theft prevention is implemented through operations in this group.

The groups described require methods supporting rather dynamic and potentially very fast membership changes. To be operational in the $CASINO_{ng}$, the operations and the membership changes require security services: authentication, confidentiality and integrity to name just the basic ones. So, finally, in order to become operational, we need a secure, dynamic group key management scheme suited for multiple, interconnected groups and for low end devices – the smart jetons.

2.3 Trust Relationships

In the $CASINO_{ng}$, one has several competing entities. The casino, its croupiers, and the customers have conflicting economic interests, and the existence of the groups outlined in Section 2.2 illustrate this nicely. However, each jeton is under partial control of each of the competing entities at the same time, and both the patterns of control and the controlling entities change. This makes for interesting trust relationships.

From an economic perspective, the casino’s business model relies on accountability, i.e. its goal is to maximize the jetons’ utility to the casino while minimizing the threats by both stupid and malicious users. It will trust its customers to buy the jetons and thus obtain the right to participate in games (and win or loose jetons). It may also allow one customer to hand his jetons to another customer directly, and it will want to allow both its customers and its croupiers to verify the validity of a jeton. The customer trusts the casino to honor his jetons when he collects his gains (if any) later on, and he trusts the croupiers to run the game fairly, accounting for the placed bets, and compensating them by the right amount.

From a different perspective, the jeton itself trusts all parties known to it sufficiently to prove its identity and authenticity to them. It trusts peer jetons owned by the same customer sufficiently to re-negotiate its face value with them if the customer so wishes, and it trusts the table (and thus its croupier) to handle ownership transfers to and from the bank, and between customers.

In the classic casino, most of these relationships are realized by contractual agreement, trust, and belief. They are enforced by control, monitoring and auditing. In the $CASINO_{ng}$, we can replace some of those with explicit cryptographic mechanisms. Thereby trust by implicit belief or contractual agreement can be made explicitly dependent on the security of e.g. group management protocols and cryptographic primitives.

This could even be taken as far as making the jetons an agent of the customer in tracking the compliance of the casino to agreed-upon rules. While the casino will track jeton movements to understand customer behaviour and protect against fraud, the customer may want to have jetons to keep track of table behaviour, and thus ensure that casino and croupier are both running a straight game. One customer may even certify this to others via his jetons (or an out-of-band channel), thereby giving rise to a reputation system which evaluates casino behaviour.

The typical threats that our $CASINO_{ng}$ environment faces are impersonation (e.g. the introduction of fraudulent jetons, or the ursurping of a customers jetons by another customer), denial of service (by disrupting communication networks in the casino), and the breach of confidentiality (e.g. one customer figuring out the amount of chips that another customer owns).

[4] This group eases the game operation.

[5] Thereby, the player can better control his possessions. On the other hand, the interaction with the cashier is made more efficient (no counting of individual jetons, the group performs this counting in a counterfeit resistant manner).

[6] These groups form together the *table group* explained below.

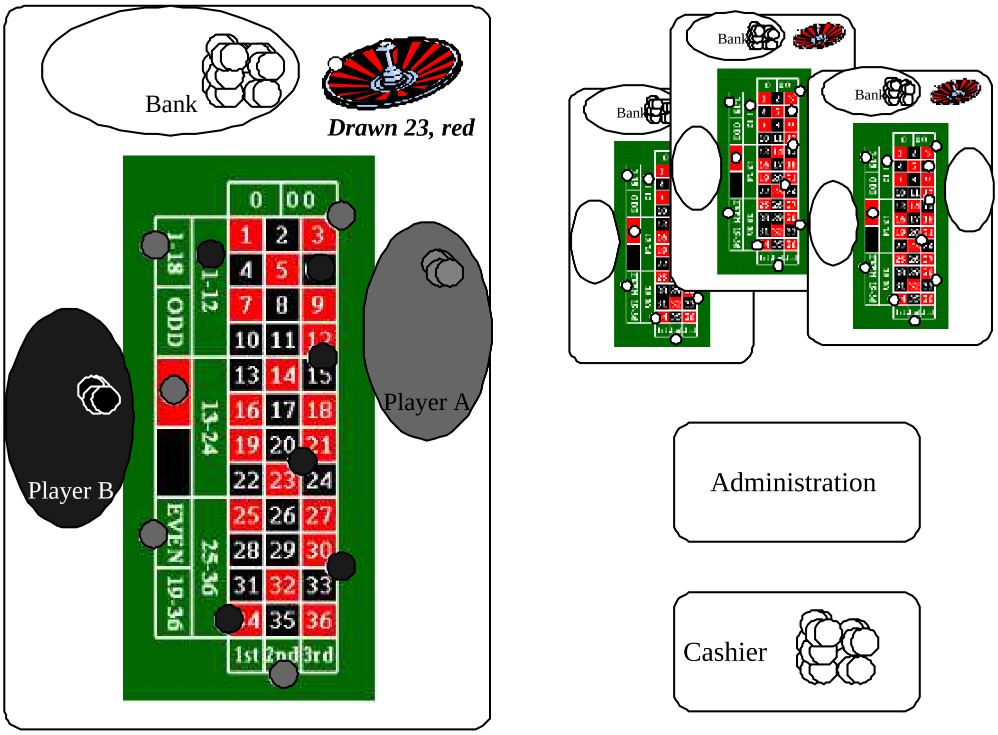

Figure 3: Groups in *CASINO*$_{ng}$.

3 Implementation Issues

Although we chose *CASINO*$_{ng}$ as a scenario that can be built as a prototype system today, it is worthwhile to review the basic technology components for groups of secure smartlets with respect to cryptographic requirements, networking technology and group protocols.

3.1 Platforms and Cryptographic Systems

One of the basic ideas of *CASINO*$_{ng}$ is to replace a jeton's physical security features with the secure network identity of the smartlet. The cost of both approaches are expected to be about equal in 2-3 years. The advantage of the secure network solution is to allow more, new and flexible applications.

It is important that the smartlets are still secured by basic physical properties that are hard to forge or copy. Fortunately, *tamper resistance* is fairly advanced in smart card chip technology and can be reused in this context. In addition, read-only hardware with long, unique serial numbers for identification and true hardware random generators should be present. For basic platform support, *low power consumption* when performing complex calculations is required and memories and bandwidth have to scale to the number of group memberships that applications require.

Basic *cryptographic operations* are needed in smartlets to support fast group operations. When we consider the example of a winner group which forms after announcing the result and disappears a few seconds later, we recognize the need for low-latency encryption and authentication functions. In group communications this means that at least symmetric key generation and encryption, DH key-exchanges, PK signatures (e.g. DSA) and message digest algorithms must be provided with a turn-around time in the milliseconds range. Considering the "expensive" operations such as signing messages, accelerators must be used. Hardware implementations of these functions not only speed up calculations but may also help save energy when smartlets have no external power source available. Chip real estate and power can be further saved by providing small-scale versions of e.g. public key operations. Such a system wouldn't protect one from an agency attack on one's secret files but could be sufficient for a players' group bet statistics that becomes invalid after some seconds or minutes.

Commercially available systems, such as smart cards, iButtons, or next generation RF-IDs, already provide some of those features. More flexible systems, e.g. based on configurable logic, will enter the scene in the next few years and will allow for a more fine-grained control over the functions needed. In addition, combined communications/controller platforms will start adding crypto functionality to their systems.

3.2 Network Technologies

With the investigation of smart dust and other extremely constraint applications, fundamental discussions on physical layer communication arise. Basically, there are two ways: (1) Optical, line of sight communications was proposed for its low power requirements but the technique leaves other points like addressing and communication with hidden devices completely open. (2) Radio frequency (RF) communications with groups of network nodes within radio cells. This is well known and suited model for group communications but it requires considerable peak power for the smartlets.

However, in the *CASINO*$_{ng}$ and similar scenarios, small batteries, inductive or other alternative power sources are possible solutions. The RF approach is clearly favored because of environmental requirements and the need to communicate efficiently as a group even at the physical layer. The following gives an overview of existing and future WPAN technologies:

- WPANs for cable replacement (Bluetooth),
- Multimedia capable WPANs based on future 802.15.3 high rate and Ultra-Wide-Band standards,
- WPANs for low-rate control applications (Zigbee) such as sensors, interactive toys, smart badges, remote controls, and home automation,
- Various RF Systems such as Wireless USB[7] with similarities to cable replacement and control applications.

Now, what is really needed from the network to support secure, dynamic group applications?

- A low-latency physical layer and flexible MAC level addressing is needed.
- Multicast support at MAC level to reduce complexity at higher layers
- Mobility support across different cells using (hierarchical) mobile IP
- Micro mobility WPAN features such as scatter nets or meshes to support fast, local movements
- Groups at the network layer must result as a common interface for applications, even for systems using different WPAN technologies
- Low power operation must be supported while smartlets are in active groups.

Early experiments, e.g. using Bluetooth as an underlying technology, have shown that limited multicast support and high latency network access prevent the use of dynamic groups at all. Even for more static secure groups, low latency is important because it adds to the time needed to authenticate new groups members.

Generally, systems with a simple, contention-based MAC layer and native multicast support are expected to fit the bill much better than systems that are built around unicast addressing, connections and enumeration schemes that exceed some tens of milliseconds.

Finally, the cost of such a solution should be comparable to a smart card when considering prices for casino jetons that range from some tens of Eurocents to very few Euros.

3.3 Group Management Protocols

One crucial element for small devices is the creation and dismantling of groups that mirror the actually valid trust relationships. While it is perfectly feasible to make each device have its own identity, and provide it with a public/private key pair in a tamper resistant environment, public key cryptography is a very expensive way to insure communication security from a computational perspective, and it is not always necessary. One way to reduce overhead would be to introduce computation proxies for the smartlets, another way is to use more lightweight cryptographic operations wherever possible. Grouping devices according to trust relations (creating trust domains), and then performing operations within these groups allows us to exploit recent advances providing such lightweight protocols.

The following example shows that asymmetric cryptography can still play a significant role, when used carefully in the small device. Consider the problem that the smartlet and the casino may want to talk to each other securely when the customer hands the smartlets back to the croupier, or when the customer passes the door to exit the casino. Casino and smartlet can simply use a shared symmetric key to communicate – if a way can be found to convey such a key to the smartlet beforehand. One way would be to seed the smartlet with the public key of the casino. Since (e.g. in RSA) signature verification is much less expensive than signature computation, the casino can establish and refresh the shared secret between itself and the smartlet by conveying it over a secure link (i.e. physical contacts on the smartlet, or in an electromagnetically shielded room such as the vault). This key is signed by the casino, thus making it impossible for anybody to impersonate the casino towards the jeton.

Once a customer acquires a smartlet, the casino can introduce that owner to the smartlet by giving it the owner's public key, or signing the owner's credentials. Should the owner now want to talk to many smartlets (or the table to all smartlets that are being put on it, or smartlets among themselves, to re-distribute their face values), protocols such as [1], or [4] can be used. With or without infrastructure support, they offer mechanisms whereby one group member can talk to all others in a group-wise authentic and confidential fashion efficiently, and where the change of group membership can be made known to all relevant parties with one or two messages and minimal computational overhead.

4 Conclusions

This paper illustrated the use of known concepts such as secure dynamic group management and WPANs in a realistic but futuristic scenario, the $CASINO_{ng}$. The proposed smartlets are one of many possible implementations of objects sharing an important characteristic in self-organizing networks: for a certain lifespan, they follow the same path, and can therefore be grouped and managed together. The benefits of this approach, besides the added security functionality, are obvious: less management overhead and better control while self-organizing. While most of the technology to build the $CASINO_{ng}$ is available today, the software to run on this technology must be "fitted" to fulfill the security and dynamics requirements. Therefore, we plan to use a simulator with support for level-of-detail operation and plugins to compare different WPANs in secure group applications. An advanced prototype should become available inside a relatively short timeframe (1-2 years).

References

[1] G. CARONNI ET AL. Efficient Security for Large and Dynamic Multicast Groups. In *IEEE 7th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE '98)* (1998).

[2] J. M. KAHN ET AL. Next Century Challenges: Mobile Networking for "Smart Dust". ACM MobiCom, 1999.

[3] MAYO, R. N. The Factoid Project. `ftp://gatekeeper.research.compaq.com/pub/DEC/WRL/research-reports/WRL-TN-60.pdf`.

[4] WEILER, N. SEMSOMM - A Scalable Multiple Encryption Scheme for One-To-Many Multicast. In *IEEE 10th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE'01)* (2001).

[7] This proprietary system is a 2.4 GHz frequency hopping radio with a CDMA MAC layer. The technology is *not* standardized.