NEXT GENERATION NETWORKS: HUMAN-AIDED AND PRIVACY-DRIVEN

*Raphael C.-W. Phan**

Loughborough University
LE11 3TU, UK
r.phan@lboro.ac.uk

Jean-Philippe Aumasson†

FHNW
5210 Windisch, Switzerland
jeanphilippe.aumasson@gmail.com

ABSTRACT

New generation networks (NGNs) deployed in the next five to ten years will integrate a myriad of underlying network technologies into a common internet protocol (IP) backbone. We put forward two theses on how NGNs will evolve based on recent trends in increasing ubiquity and the need for increased security. We assert that NGNs will be increasingly human-aided and privacy-driven. We discuss how these points are inter-related, and then we culminate this paper with a model that allows formal analysis of network privacy, including the tracing of entities.

Index Terms— NGN, evolution, cycle, human-aided, security, privacy, security model, standards

1. INTRODUCTION: MOVING TO A UBIQUITOUS PACKET-BASED NETWORK

A Next Generation Network (NGN) [1] refers in essence to the network architectural evolution over the next five to ten years. NGNs will be integrated, packet-based networks over phone, cable, satellite, or mobile networks that communicate converged multimedia information comprising voice, video, text, and other data.

The shift from communication over analog telephone lines to a converged internet protocol (IP) backbone comprised of diverse network types means a shift from circuit-based voice to packet-based (multimedia) data.

NGNs have support for generalized mobility and will provide for services including multimedia communication and messaging, video content distribution and streaming, interactive gaming, location-based services, mobile internet access and mobile TV.

One of the possibilities provided by this seamless integration is the effortless porting between offline and online access to the network to the extent that the user is in fact oblivious to when he is connected. The user's device connects or disconnects from a network transparently, whenever necessary, and without any initiation by the user. This gives an increased sense of ubiquity in terms of the user's connection to the network via his personal devices.

*Work done while the author was with the Security & Cryptography Lab (LASEC), Ecole Polytechnique Fédérale de Lausanne (EPFL), Switzerland.

†Supported by the Swiss National Science Foundation under project no. 113329.

1.1. NGNs: Human-aided and Privacy-driven

In this paper, we put forward two theses regarding the evolution of NGN in the future:

- **Human-aided**: NGNs will involve humans as separate entities, not just as end-users external to a network. This leads to the convergence of social science aspects into the technical design and analysis of future NGNs.
- **Privacy-driven**: NGNs will be privacy-driven as they become more seamlessly integrated among human societies. Every object (human or machine) that a person interacts with may potentially allow him to be tracked. This will require a privacy analysis model where a network protocol entity can be either a human or machine—basically anything that is connected to a network.

We culminate the paper by describing a formal model that allows us to analyze privacy in networks.

2. TRENDS FOR EMERGING NETWORKS

2.1. Towards Human-Aided Networks

Computers have taken over the many human tasks due to their higher efficiency, effectiveness and better suitability for mundane procedures. Yet, their interaction with humans has remained, mostly where humans are the end-users, because computers typically replaced humans that were used for information processing.

Clearly, this bears resemblance to the interaction between digital and analog counterparts. Indeed, as our physical world is analog and so no matter how much digital the information processing and communication becomes digital, at the other end the information needs to be converted back to analog signal form in order to be used in the "real world" again.

Our thesis here is that just as many of nature's processes go in cycles, so too does the information processing world. To elaborate, networks are moving towards having digital entities interact with human users not just at the terminal points but throughout the process at different intermediate points. The reason is not that humans are becoming more efficient, but that there are so-called *out-of-band* tasks for which only humans are capable.

The increasing involvement of humans at intermediate points is due to the development of two areas: ubiquity and security. While ubiquity is a matter of fact, security—as a process—remains a delicate trade-off between privacy, cost, and usability.

Human Involvement as a Consequence of Ubiquity

The *wireless revolution* and the *reduction in size* for devices has created a world of ubiquity where devices can be used anywhere with great mobility and ease. Because of the size reduction factor, embedded processor chips can be embedded into smart cards and radio frequency identification (RFID) tags, the smallest [2] of which was recently developed by Hitachi that just measures 0.05×0.05 square millimetres. Also, the concept of *wearable computer* emphasizes the progressive reconciliation between people and machines.

Ubiquity also warrants a single multiple-use device (also known as a smart device, e.g. iPhone) since a human user may not want to carry a different device for each separate application. This ubiquity leads to small devices interconnected with each other, and as an individual's collection of interconnected devices accumulates, this gives birth to personal area networks (PANs). The human user is in the middle of the PAN and is expected to interact with each device, sometimes even as simply as relaying information from one device to another. This is in contrast to the more conventional computer networks or the internet where no human intermediaries exist; the digital world is a becoming more of a heterogeneous metanetwork.

Increased Security Due to Human Intermediaries

As more devices are interconnected, more points of remote attack exist for human adversaries who do not have direct physical access. Present day deployed network technologies and protocols, such as Bluetooth [3] and certified wireless USB (wUSB) [4], now involve more human interaction and communication of authentication information via external human-aided channels that are harder to exploit without physical access; these are also so called out-of-band channels.

Recent security results have caused people to start realizing that humans are an inevitable part of any communication protocol. Interaction with humans affects security, and so concepts like "out-of-band channels" [3, 4] and "ceremonies" [5] are gaining popularity; humans now act as intermediaries or actively play a security-based role within networks. The idea is to formally analyze the security of an entire communication protocol or system by including humans as one of the entities, rather than analyzing non-human components only while leaving out the human interaction as out of scope of the network protocol design.

While humans are said to be the weakest link in a network, counter-intuitively we are returning to the humans to add extra factors for security, that is, having security based not just on public key infrastructure or passwords, but also on communicating information through real-world physical human-aided communication channels, such as voice, visual, etc.

From a security standpoint, human involvement in a network adds an extra factor of security and complicates attacks since it is harder to attack a human-based point remotely, and physical attacks are harder to execute.

Thus, we now cycle back through the network protocol evolution: starting with the state prior to the digital revolution where humans have major roles to play, through the decades of the digital era where human roles were replaced by machines, and now back to present day networks where we see again increasingly more human involvement as intermediaries.

More interestingly, the idea of having humans act as entities within a network security protocol by communicating with each other via an out-of-band channel was first initiated by Rivest and Shamir as early as 1984 [6], and yet it was only recently that this treatment was formally discussed e.g. the work of Vaudenay [7], sparking off several recent papers for formalizing this [8, 9, 10, 11]. The advantage of this approach is that entities can authenticate each other without requiring a central trusted authority or public-key infrastructure (PKI) to maintain a directory of public key certificates; something clearly infeasible to implement in practice for increasingly ubiquitous, mobile and ad hoc networks of present day. This is a clear example of the cycling back to human emphasis that is influenced by security issues.

2.2. Creating Privacy-Driven Networks

Security of information has always preceded privacy of the human throughout the ages, even in ancient times when encryption was used by Julius Caesar. As information became easier to access in the digital era, the urgent need was to protect the information secrecy or at least control access to the information. The points along the information communication channel were commonly non-human while humans only existed at the end points. Thus the only important entity to protect along a communication channel was the information itself that was being communicated.

Yet in this paper, we assert that the privacy requirement is catching up with, if not bypassing, its security counterpart, due to two major developments: increasing human involvement and ubiquity.

Increased Human Involvement Has Privacy Implications

Related to the previous subsection, increased human involvement at intermediate network points means that humans now also need to be protected against attacks.

While the more conventional notions of information secrecy, integrity, authenticity basically correspond to security properties, privacy is recently also increasingly a concern since humans are now present along the network, at times forming human-intuitive physically-perceptible out-of-band channels.

In particular, being involved at different points of a network should not cause the human to be traceable without his consent or knowledge. This leads to the issue of *untraceable privacy* (**Priv**), which will be treated in detail in Section 3.

Ubiquity Increases the Privacy Threat

Because the wireless revolution has led to ubiquitous devices, the threat to user's privacy has increased; it is indeed now easier to track his location and activities by tracking his mobile connected devices.

Traditionally, devices like computers were non-mobile so that the most serious privacy issue was tied to the secrecy of the humans information processed by the computer. Yet, today privacy includes assuring that the human is not being tracked as he uses his mobile devices since these devices are with him wherever he physically goes. Due to ubiquity, the devices are further pervasively connected and interconnected, often in a manner seamless and transparent to the user. The ubiquity of network devices is also partially influenced by the deployment of wireless sensors deployed for national security reasons. The world now has more diverse types of devices connected to networks, each potentially leaking information that corresponds to a humans privacy [12, 13, 14, 15, 16]; of increasing concern are "Big Brother" issues.

Ubiquity is synonymous to omnipresence, thus the fact that connectivity is available anywhere at a certain point in time is in fact in direct contradiction to untraceable privacy. So, for NGNs where ubiquity is inherent, it is vital to analyze the impact on privacy and if possible, how it can still be offered in the face of ubiquity.

3. MODELLING PRIVACY FOR NETWORKS

We discuss here a general untraceable privacy (**Priv**) model that can be used to determine whether network protocols can safeguard protocol entities from being tracked.

The model defined herein can be seen as in the same vein as the Bellare et al. models [17] for authenticated key exchange (AKE) protocols, which can be regarded as one of the most commonly considered type of network security protocols.

In fact, this model defined specifically for radio frequency identification devices (RFIDs) was used recently in [18] to successfully analyse violations of privacy in recent RFID authentication schemes.

A protocol entity U interacts in protocol sessions as per the protocol specifications until the end of the session upon which each party outputs **Accept** if it feels the protocol has been normally executed with the correct entities.

Adversary A controls the communications between all protocol entities (U_0, U_1, etc.) by interacting with them as defined by the protocol, formally captured by A's ability to issue *queries* of the following form:

- **Execute**(U_0, U_1, i): This query models *passive* attacks, where adversary A gets access to an honest execution of the protocol session i between U_0 and U_1 by eavesdropping.
- **Send**(U_0, U_1, i, m): This query models *active* attacks by allowing the adversary A to impersonate some entity U_0 in some protocol session i and send a message m of its choice to an instance of some other entity U_1.
- **Corrupt**(U, K'): This query allows the adversary A to learn the stored secret K of an entity U, and which further sets the stored secret to K'. It captures the notion of *forward privacy* and the extent of the damage caused by the compromise of U's stored secret.
- **Test**$_{\text{Priv}}(U, i)$: This query is the only query that does not correspond to any of As abilities or any real-world event. This query allows to define the indistinguishability-based notion of *untraceable privacy* (**Priv**). If the party U has accepted and receives a **Test**$_{\text{Priv}}$ query, then depending on a randomly chosen bit $b \in \{0, 1\}$, A is given U_b from the set $\{U_0, U_1\}$. Informally, A succeeds if it can guess the bit b. In order for the notion to be meaningful, a **Test** session must be fresh in the sense of Definition 2.

Definition 1 (Partnership and Session Completion)
Two entity instances U_i and U_j are partners *if and only if both have output* **Accept**(U_j) *and* **Accept**(U_i) *respectively, signifying the* completion *of the protocol session.*

Definition 2 (Freshness)
An entity instance is fresh *at the end of execution if and only if (1) it has output* **Accept** *with or without a partner instance,and (2) both the instance and its partner instance (if such a partner exists) have not been sent a* **Corrupt** *query.*

Definition 3 (Untraceable Privacy)
Untraceable privacy *is defined using the game G played between a malicious adversary A and a collection of entity instances. Adversary A runs the game G whose setting is as follows:*

- Phase 1 (Learning)*: A is able to send any* **Execute**, **Send**, *and* **Corrupt** *queries at will.*
- Phase 2 (Challenge)*:*
  1. *At some point during G, adversary A will choose a fresh session on which to be tested and send a* **Test**$_{Priv}$ *query corresponding to the test session. Note that the test session chosen must be fresh in the sense of Definition 2. Depending on a randomly chosen bit $b \in \{0, 1\}$, A is given a challenge ID denoted U_b from the set $\{U_0, U_1\}$.*
  2. *Adversary A continues making any* **Execute**, **Send**, *and* **Corrupt** *queries at will, subjected to the restrictions that the definition of freshness described in Definition 2 is not violated.*

- Phase 3 (Guess)*: Eventually, A terminates the game simulation and outputs a bit b', which is its guess of the value of b.*

The success of A in winning G (and thus in breaking **Priv***) is quantified in terms of his advantage in distinguishing whether it received U_0 or U_1, i.e. it correctly guessing b, compared to randomly guessing it. This is denoted by* $\mathbf{Succ}_A^{Priv}(k)$ *where k is the security parameter.*

Thus, once it is shown that $\mathbf{Succ}_A^{\text{Priv}}(k)$ for a particular network security protocol, then we can know that the protocol achieves untraceable privacy.

A formal model is however not a panacea: the strongest security argument with respect to a formal model will never "prove" the concrete security of a scheme, especially with regard to attacks based on social engineering or side-channels.

The formalized notion of untraceable privacy discussed here is in fact the strongest kind of privacy that can be offered. This is because if it is shown that **Priv** can be achieved, then clearly privacy in the sense of anonymity of an entity is achieved as well. This can be seen from a standard reduction argument well used in provable security [17, 19]. In more detail, consider an adversary A that breaks anonymity of an entity, i.e. he can obtain the identity of the entity. Then clearly we can transform A into an adversary B that can trace the entity, thus breaking **Priv**. Hence, if a network protocol is shown to offer **Priv**, i.e. no such adversary B exists, then by implication adversary A would not exist either, thus anonymity is achieved.

Additionally, we remark that a network protocol where entities have uniquely identifiable IDs need not violate untraceable privacy. One example is where human entities use pseudonymous IDs while machine entities can use normal uniquely identifiable IDs, yet no machine entity should be linked to any human entity's ID. Counterintuitively, it appears that the ad hoc and mobile nature of ubiquitous NGNs do aid in avoiding this linkability.

4. CONCLUSION

Sensors and monitoring devices in strategic locations seem inevitable in view of public safety concerns about crime and terrorist threats. Yet, violation of privacy can be brought to a controllable—if not acceptable—level by ensuring that the individual is at least aware that online devices are in his vicinity; and when desired, that he knows where they are so that private information, such as behavioural patterns related to his personal life, will not be leaked out without his knowledge. The issue whether privacy and security are contradictory is however disputed [20].

Privacy has only been recently treated for RFIDs, and appears yet to be treated for other new network technologies such as Bluetooth, certified wireless USB, etc. It will be worth exploring how privacy can be offered for these new technologies.

With the fast evolving ICT scene, "the only thing constant is change", and network architecture designs should not be technology-driven but rather socio-economically driven. For instance, the trend now is towards ubiquity and PANs, and while it is important to improve existing networks to best exploit the latest technology, it is more important that networks maintain or increase existing security and privacy since new technologies are often double-edged swords. A new technology knows no owner and benefits both honest legitimate users as well as potential attackers. The ease with which the new technology allows for communication is also the ease with which the attacker can make use of the same technology to mount his attacks. Just as the average human is never satisfied with existing knowledge, individuals always exist that wish to acquire more than they can legitimately access, and thus security and privacy will always be a concern. So, even though technologies and their supported networks will constantly change, the importance of security and privacy will not.

As a final remark, a new network technology becomes the de facto standard due more to its ease of use rather than the security or privacy it offers; even cost is not so much a factor since it decreases over time as technology advances and becomes more widespread. An example of this is wireless devices, where security and privacy lag behind widespread deployment. This phenomenon adds to the difficulty of the security researcher in designing mechanisms to secure information and individuals as networks evolve.

Acknowledgement

The first author thanks Jonathan J. Little for editorial comments that improved how this paper turned out. We thank God for His blessings; and for all that was, is, and is to come [Rev 1:8].

5. REFERENCES

[1] ITU, "ITU-T's "Innovations in NGN" Kaleidoscope academic conference, paper proposal submission instructions," June 2007.

[2] Hitachi, "Operation verified on world's smallest 0.05 mm x 0.05 mm "contactless powder IC chip"," News Release, 13 February 2007.

[3] Bluetooth SIG, "Bluetooth specification v2.1 + EDR," July 2007.

[4] USB Implementers Forum (USB-IF), "Wireless USB specification, revision 1.0," May 2005.

[5] Carl Ellison, "Ceremony design and analysis," Cryptology ePrint Archive, Report 2007/399, 2007, `http://eprint.iacr.org/`.

[6] Ronald L. Rivest and Adi Shamir, "How to expose an eavesdropper," *Commun. ACM*, vol. 27, no. 4, pp. 393–395, 1984.

[7] Serge Vaudenay, "Secure communications over insecure channels based on short authenticated strings," in *CRYPTO*, Victor Shoup, Ed. 2005, vol. 3621 of *LNCS*, pp. 309–326, Springer.

[8] Sylvain Pasini and Serge Vaudenay, "An optimal non-interactive message authentication protocol," in *CT-RSA*, David Pointcheval, Ed. 2006, vol. 3860 of *LNCS*, pp. 280–294, Springer.

[9] Sylvain Pasini and Serge Vaudenay, "SAS-based authenticated key agreement," in *Public Key Cryptography*, Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin, Eds. 2006, vol. 3958 of *LNCS*, pp. 395–409, Springer.

[10] Sven Laur and Kaisa Nyberg, "Efficient mutual data authentication using manually authenticated strings," in *CANS*, David Pointcheval, Yi Mu, and Kefei Chen, Eds. 2006, vol. 4301 of *LNCS*, pp. 90–107, Springer.

[11] Moni Naor, Gil Segev, and Adam Smith, "Tight bounds for unconditional authentication protocols in the manual channel and shared key models," in *CRYPTO*, Cynthia Dwork, Ed. 2006, vol. 4117 of *LNCS*, pp. 214–231, Springer.

[12] CASPIAN, "`http://www.boycottbenetton.com/`," Accessed 19 September 2007.

[13] Jaap-Henk Hoepman, Engelbert Hubbers, Bart Jacobs, Martijn Oostdijk, and Ronny Wichers Schreur, "Crossing borders: Security and privacy issues of the european e-passport," in *IWSEC*, Hiroshi Yoshiura, Kouichi Sakurai, Kai Rannenberg, Yuko Murayama, and Shin ichi Kawamura, Eds. 2006, vol. 4266 of *LNCS*, pp. 152–167, Springer.

[14] Ari Juels, David Molnar, and David Wagner, "Security and privacy issues in e-passports," in *Securecomm*. 2005, pp. 74–88, IEEE Press.

[15] Ari Juels and Stephen A. Weis, "Defining strong privacy for RFID," in *PerCom Workshops*. 2007, pp. 342–347, IEEE Computer Society.

[16] Eleni Kosta, Martin Meints, Marit Hansen, and Mark Gasson, "An analysis of security and privacy issues relating to RFID enabled epassports," in *New Approaches for Security, Privacy and Trust in Complex Environments*. 2007, pp. 467–472, Springer.

[17] Mihir Bellare, David Pointcheval, and Phillip Rogaway, "Authenticated key exchange secure against dictionary attacks," in *EUROCRYPT*, Bart Preneel, Ed. 2000, vol. 1807 of *LNCS*, pp. 139–155, Springer.

[18] Khaled Ouafi and Raphael C.-W. Phan, "On the privacy of recent RFID authentication protocols," in *Information Security Practice and Experience (ISPEC '08)*, 2008.

[19] Jacques Stern, "Why provable security matters?," in *EUROCRYPT*, Eli Biham, Ed. 2003, vol. 2656 of *LNCS*, pp. 449–461, Springer.

[20] Bruce Schneier, "Security vs. privacy," Blog "Schneier on Security", 29 January 2008.