INVITED PAPER

On the security of communication network: now and tomorrow

BOLDIZSÁR BENCSÁTH, LEVENTE BUTTYÁN, ISTVÁN VAJDA

Budapest University of Technology and Economic, Department of Telecommunications
Laboratory of Cryptography and System Security (CrySyS)

{bencsath, buttyan, vajda}@crysys.hu

Keywords: information security, privacy, Internet, wireless sensor networks, vehicular communications, RFID systems, network coding

In this paper, we first discuss some security issues in the Internet, and we sketch some future research directions in this field. Then, we discuss the security issues in wireless networked embedded systems through three examples: sensor networks, vehicular communications, and RFID systems. Finally, we give a brief introduction to the field of network coding, which is a new, promising research area in networking.

1. Introduction

In this paper, we give a brief overview of Internet security issues. First, we discuss the security problems of the current Internet as we know and use it today. Then, we introduce some future research directions in the field of Internet security. We continue by considering a broader interpretation of the Internet than it is usually meant today, where the network is not limited to PCs and servers, but it also includes various embedded computers. This broader interpretation is often referred to as the *Internet of Things*.

We describe the related security and privacy issues through three examples: wireless sensor networks, vehicle communication, and RFID systems. Finally, in the last part of the paper, we give a short overview on the security of network coding, which is a new promising research area that may have impact on the design of future networks.

Obviously, the general field of security and privacy in communication systems is a large area that cannot be fully covered in the context of this paper. Our selection of the topics discussed in this paper have been biased by our research activities in the Laboratory of Cryptography and Systems Security (CrySyS) of the Department of Telecommunications at the Budapest University of Technology and Economics. More information on our research and other activites is available on the web site of the laboratory at *www.crysys.hu*.

2. Security of the Internet

The security of the internet has evolved a lot in the last decades. Today, nobody can imagine the Internet without security mechanisms such as TLS, SSH, PGP, IPsec, or without advanced authentication techniques (smart cards, captchas, two factor authentication tools, etc.) However, lot of the security problems of the Internet remained unsolved.

Malware, badware, viruses and *worms* have been known for decades, however, the problem is getting worse and worse instead of finding proper solution for the problem. Malware infected hosts are not individual problematic points anymore, *botnets* have been created. These botnets might aggregate the resources of millions of computers. Even the estimation of the size of the botnets is a hard problem.

Using botnets, millions of *spam* e-mail messages can be sent out easily and rapidly. Although solutions are continuously proposed against spam, spam is still one of the biggest problems of the Internet. In June 2009, 88.9% of the full Internet e-mail traffic was spam.

Most of the Internet servers and services are prone to some kind of *Denial-of-Service problems (DoS)*. The basic architecture of the Internet was not designed to be resilient against such attacks, and therefore the number vulnerable services, servers, protocols is unknown and might very high, therefore, a significant increase might happen in both the number and the severity of the DoS attacks at any time.

Another unsolved problem on the Internet is *cracking and defacing web pages and servers*. Today, a number of tools and possibilities are available to make servers secure: automatic updates, intrusion detection systems, secure authentication, vulnerability scanners, etc., but still, the web sites are not secure and cracked frequently. There is multiple reasons behind that. Although tools are available, they are not used, for different reasons to make systems secure. Special web content cannot be updated automatically at all the time. Administrator do not have right to fulfill necessary operation without the owners' consent.

Grid-computing, cloud-computing also raise new security and reliability concerns. In such cases the legal situation is even more complicated. The cloud-based service might be free or very cheap, but there is no guarantee on the reliability, availability and security properties, therefore the end users might have no options to solve security problems.

2.1 Research directions

Not just the problems and solutions have been significantly changed during the last years, but even the methodology, the point of view on the problems changed a lot.

Future internet: A number of new research projects started to design the next generation of the Internet, including Global Environment for Network Innovations (GENI), a Future Internet Design (FIND), funded by the U.S. National Science Foundation (NFS), or projects in the Seventh Framework Programme of the European Union (FP7). The main goal of these projects is to redefine the basic architecture of the Internet. Traditionally the Internet provides best-effort services, it is a multi-layer unreliable network. Most of the services are based on TCP/IP where the main task of the routers just to forward simple packets. The reason behind many security problems is this approach: because of the architecture and protocols of the Internet, it is simply impossible or almost impossible to solve some security problems. By redesigning the basic blocks and the architecture, new solutions can be made for the security problems.

The next generation Internet should give more than best-effort forwarding of packets. People need services instead of an unreliable transport network, the need quality of service (QoS) agreements. Today, Internet-wide secure authentication is not solved, especially for simple network protocols, and therefore, it is nearly impossible to track back the origin of an attack and punish attackers. This list of problems and new tools, features might be continued, but the most important message is that there is a need and also intention to modify even the foundations of the Internet.

Intelligent intrusion-detection: The intrusion detection (IDS, IPS, honeypot, etc.) tools have evolved a lot in the last years. From the basic event detection we arrived at complex systems which intelligently distinguish attacks from normal traffic and automatically carry out countermeasures. This change goes forward to make global intrusion detection systems (possibly with honeypot systems), to use modern network technologies, like P2P techniques in intrusion detection, or more intelligent reactions to security problems. To this last goal, to provide more dependable systems by automatic reconfiguration, an EU FP7 project, DESEREC *(www.deserec.eu)* has just been finished with the participation of BME's Laboratory of Cryptography and Systems Security (CrySyS).

In the area of trust, reputation and authentication, new methods give new tools to solve security problems and therefore there is a very intense research activity in this field. The work includes:

- Defining attack and defense incentives and providing new tools based on these properties.
- Using game theoretical methods to make such situations, where there is no use to attack, thus avoiding attacks.
- Providing new ways of authentication possibilities while retaining anonymity and civil rights.
- Dealing with trust on local level and on large scale.

Secure clients and secure, trusted platforms: Lot of the problems originate from the fact that the software elements and thus the whole client computer cannot be trusted. Trusted computing could provide a situation, where there are no malware programs, or, the can be easily removed at large scale. However, the concept of trusted platforms contradicts with the current philosophy of the Internet, e.g. the need of the users to install pirated software, downloading music illegally, etc. The typical research areas: secure software engineering; formal analysis and proving of protocols, rule sets, or even formally proven APIs; secure authenticaion in untrusted environment, etc.

This short introduction cannot provide a full picture of all the work that is currently in place to provide new solutions to security problem, we just tried to show the most interesting research areas in this field, that could have a great impact to the future of the Internet.

3. Security and privacy in wireless networked embedded systems

3.1 Security in wireless sensor networks

In the last decade, a considerable amount of research on wireless sensor networks has been carried out all over the world. This new wireless networking technology allows for a number of new and useful applications the monitoring of the parameters of our physical environment (such as temperature, pressure, humidity, vibration, acustic noise, etc.), and the automated collection and processing of all these monitored data. The potential applications include optimization of agricultural processes, making ecological observations on large scale or in environments that are difficult to access physically, forecasting natural disasters such as earthquakes, reducing cost in industrial process automation and control, prevention of accidents on the roads, remote monitoring of elderly or chronically ill people, and military tactical applications, just to mention a few.

Many of these applications have security requirements related to the protection of wireless communications on the one hand, and to the increased resistance of the networking mechanisms againts malicious attacks on the other hand. Although, security is a problem and has been addressed both in wired and in traditional wireless networks (e.g., in cellular and Wi-Fi networks), there are new security challanges in wireless sensor networks, and the solutions proposed for wired and traditional wireless networks can be used only with limited success, if at all. Such a challenge, for instance, is that the nodes in wireless sensor networks have severe resource constraints: the nodes are small, battery powered embedded computers designed for low energy consumption, and consequently, they have reduced computing, storage, and communication capabilities. Therefore, one needs new security mechanisms in wireless sensor networks that are computationally not so expensive, have small code size, and minimize energy consumption.

These requirements are usually not satisfied by the security mechanisms used in traditional networks.

Another distinct security problem in sensor networks is that the nodes are usually physically accessible and they are not tamper resistant. Thus, they can be relatively easily compromised, meaning that an attacker can obtain secrets stored in the node and install rogue software on the node such that it continues to behave arbitrarily. Node compromise may happen in traditional networks too, however, as the nodes of traditional networks are usually located in locked rooms, the attacker is essentially restricted to remote logical attacks. In wireless sensor networks, node compromise is easier to carry out due to the easy physical access to the nodes, and we must always assume that some nodes may have indeed been compromised.

In our CrySyS laboratory, we have been working on the problem of securing wireless sensor networks in the context of two projects, UbiSec&Sens *(www.ist-ubisecsens.org)* and WSAN4CIP *(www.wsan4cip.eu)*, both funded by the European Commission. In the former project, we participated in the development of a security toolbox for sensor networks inlcuding a random number generator, new encryption algorithms, new key establishment protocols, and security enhancements for routing, clustering, data aggregation, and distributed data storage schemes.

In particular, we developed the Secure-TinyLUNAR secure routing protocol, the RANBAR and CORA resilient data aggregation algorithms, and the PANEL robust aggregator node election protocol. In the latter project, we are currently working on dependable networking mechanisms for wireless sensors in the context of critical infrastructure protection applications.

3.2 Security and privacy in vehicle communication systems

Unfortunately, more than 40.000 people die in road accidents in Europe, and the statistics in the US are similar. In addition, another problem is the ever increasing amount of road traffic in large cities that leads to traffic jams and vaste of tremendous amount of time and fuel. In both cases, the situation could be improved if the right information would be available at the right place at the right time (i.e., if drivers would be informed about hazardous situations and receive up-to-date information about the traffic conditions). This could be achieved by letting vehicles to communicate with each other and with roadside equipments. Such communications must obviosly be wireless due to the nature of the application.

Most of the large car manufacturers around the world are seriously considering the idea of vehicle-to-vehicle and vehicle-to-infrastructure communications, and they investigate the related technical problems in national and international projects (e.g., NoW, CVIS, Safespot and Coopers projects). Among those technical problems, they are also looking at security issues. Indeed, it must be clear that vehicle communications can only be adopted if it cannot be easily misused, or its operation cannot be easliy disabled. One thing to absolutely avoid is that someone sitting at the roadside injects fabricated messages in the system, and in this way, provokes accidents. A security hole in the system can easily translate into fatalities in this case. Therefore, it is indispensable that messages are aunthenticated and their contents are validated, for instance, through consistency checking and correlation with other similar messages.

Most safety applications require that the vehicles continuously inform nearby vehicles about their current location, direction of movement, and speed. For this reason, the vehicles send so called heart beat messages, with a rate of several hundred messages per second, which contain these data. This, however, raises privacy problems, as it becomes rather easy to track the whereabouts of the vehicles by sniffing the wireless channel. Note that, although tracking vehicles is possible by means of video surveillance technologies, tracking by eavesdropping is less expensive, more precise, and can be carried out at larger scale. We, and fortunately many others, believe that, in modern societies, new technologies should be introduced only if they are designed in such a way that they do not make privacy violations easier than they are today. Therefore, the protection of location privacy in vehicle communication systems is an important design requirement.

In our CrySyS laboratory, we have been working on the problem of securing vehicle communications and location privacy enhancing techniques in the context of the SeVeCom project *(www.sevecom.org)* that received funding from the European Commission. In particular, we have investigated various pseudonym schemes and their effectiveness in preventing location tracking in vehicle networks.

3.3 RFID privacy

Similarly to the problem of location tracking of vehicles, individuals can be tracked by sniffing the wireless transmissions generated by various devices that they carry with or on them. In particular, it is expected that in the future many objects will be tagged with RFID tags that emit unique identifiers each time they are queried by a nearby reader. Hence individuals could be identified and tracked by observing the identifiers of their RFID tags. Unfortunately, RFID tags are even more constrained in terms of resources than the previously described sensor nodes; hence, it is very challenging to design protocols for them that would prevent this kind of tracking.

In our CrySyS laboratory, we have been working on efficient private identification schemes for low-cost RFID tags that ensure that external eavesdroppers cannot obtain the identifier of the tag from the transactions between the tag and a valid readers.

4. Network Coding

The idea of network coding was born at the beginning of our new millenium, an important development in the theory and practice of infocommunication. 60 years ago

Shannon in his famous publication gave the information theoretical foundation for point-to-point communication (channel capacity, existence of optimal channel codes). From the beginning of the 1960's till the end of 1980's capacity calculations were extended to small/special networks and channels (e.g. broadcast channels, multiple-access channels, feedback channels).

For practical applications many important results were found in the field of random access channels and code division multiple access channels (CDMA). Then more than a decade spent without new ideas in the field of information theory of networks when, finally, in the year of 2000 the network coding was innovated [7].

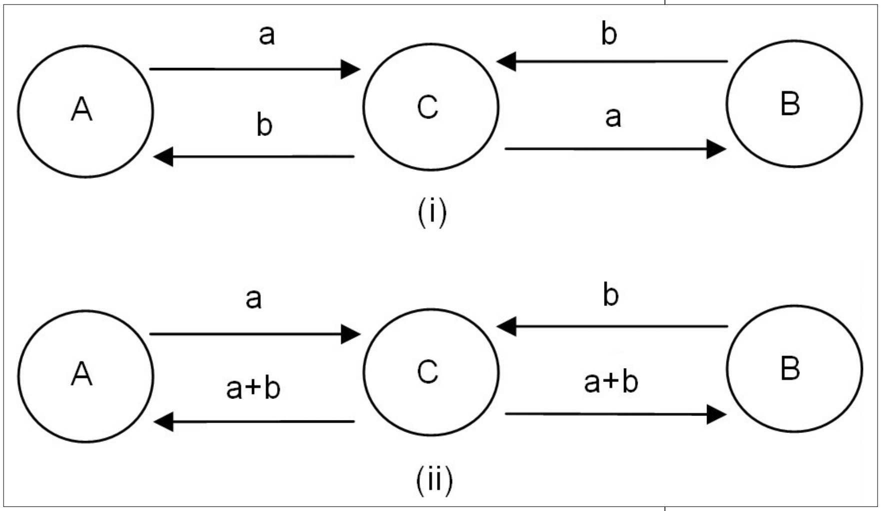

Figure 1. An illustration of the idea of network coding

One the simplest example for the strengh of network coding is given in *Fig.1.* Wireless communication nodes *A* and *B* want to exhange their messages *a* and *b*, respectively Obviously, they can solve this task in four steps of communication, as shown by version (i). However, they can also do it by sending only three messages in total: node *A* and *B* send their messages to node *C*, which linearly combines the messages by XOR addition *(a+b)* and broadcasts the sum in one step. It easy to see that network coding, i.e. allowing linear combination of messages by communication nodes, improves the communication efficiency compared to the classical store-and-forward solution: the store-and-forward solution is the trivial network coding, when no combination is done at nodes.

The principle of network coding can be extended to non-binary cases by straighforward generalization. In retrospect, the network coding in the case of the scenario of Fig.1 is trivial. But, how can we find appropriate combinations for large, general networks? Fortunately, it turns out that nodes can independently choose random linear combinations to achieve, essentially, optimal coding.

If a source (or a set of sources) wants to transmit a time flow of messages to destination nodes through the network, then the flow is partitioned into units of fixed number of messages (called generations) and network coding combines messages within the same generation. A destination node is able to decode messages of a generation, when it has collected a set of linearly independent combinations (so called innovative combinations) with set size equals to the size of a generation.

Network coding has important advantages for a diversity of practical application: for example, improvement of network throughput, improved robustness of communication in case of link/node failure, decrease of the number of communication steps in case of energy critical application (battery powered nodes).

Now, we shortly summarize the possible positioning of network coding in the protocol stack. Network coding can be placed in each layer, resulting in different potential applications. If we implement it in the application layer, it has the advantage that routing and MAC layers remain intact, and extension is needed only in the software of the source and destination nodes. A typical application is the case of overlay communication topologies, e.g. P2P file distribution systems.

When the network coding is implemented in the transport layer, a destination node does not send back an ACK for a received packet, but the node sends back information about possible combinations which were innovative for it. A source node according to received needs for innovative information selects combination which is innovative for largest possible set of destination nodes.

In the network layer during the discovery of network topology – which typically some kind of flooding technique – application of network coding is very appropriate. The so called opportunistic network coding in wireless networks is an excellent example for the usage of network coding in the data link layer. Network nodes are set into promiscuous mode and overhear the wireless communication in their neighborhood, according to which they can optimize the next network coding step they do. Network coding can also be implemented even in the physical layer, which is called analogic network coding.

A serious disadvantage of the network coding is its sensitivity to the so called pollution attack. This means that network coding does not check the integrity of the received packets, and if a – illegally – modified packet (polluted packet) is used in a combination it also becomes modified and will be combined into several further combinations accross the network, resulting in spreading of the pollution, which finally deteriorates the network communication. This attack can be stopped by detecting and dropping polluted packets.

For detection cryptographic techniques (MAC, digital signature or hash techniques in case of available authentic channels) can be used. This cryptography must fit to network coding by having special algebraic property (homomorphic mapping). However, in case of resource constrained environments (e.g. sensor networks) cryptographic techniques with high computational complexity are excluded.

We can derive the conclusion that the theory and practice of network coding is developing fast in recent years. There are many important, potential applications, however, it is an open question yet, when will network coding be an ubiquitous option for networking protocols.

5. Conclusions

Communication systems play a fundamental role in today's society, and therefore, their dependability is crucial. Dependability includes also security, which means resistance against intentional attacks. In this paper, we reviewed some of the security issues pertaining in the current Internet, and those expected in future emerging wireless networks and communication systems.

As we could see, there are important challanges ahead of us that must be properly addressed by researchers and designers of future communication systems, such that we can live in a safer cyber world than we do today.

Authors

BOLDIZSÁR BENCSÁTH received his MSc diploma in Computer Science in 2000 from the Budapest University of Technology and Economics (BME), and his MSc diploma in Economics in 2001 the Corvinus University of Budapest. He has been working in BME's Laboratory of Cryptography and System Security since 2000, first as a PhD student and then as a researcher. His research interests are in practical Internet security, protection against spam and distributed denial-of-service attacks.

LEVENTE BUTTYÁN received the M.Sc. degree in Computer Science from the Budapest University of Technology and Economics (BME) in 1995, and earned the Ph.D. degree from the Swiss Federal Institute of Technology – Lausanne (EPFL) in 2002. In 2003, he joined the Department of Telecommunications at BME, where he currently holds a position as an Associate Professor and works in the Laboratory of Cryptography and Systems Security (CrySyS). His research interests are in the design and analysis of security protocols and privacy enhancing mechanisms for wireless networked embedded systems (including wireless sensor networks, mesh networks, vehicular communications, and RFID systems), and the application of formal methods in security engineering.

ISTVÁN VAJDA obtained his MSc degree in Electrical Engineering in 1977, and a diploma in Telecommunications Engineering in 1979 at the Budapest University of Technology and Economics (BME). He received his CSc degree (equivalent to PhD) in 1984, and his Doctor of Sciences (DSc) degree in 1997. Currently, he is a full professor at the Budapest University of Technology and Economics, and he is the head of the Laboratory of Cryptography and System Security at the Department of Telecommunications. His research interests include coding theory and cryptography.

References

[1] MessageLabs Intelligence Reports, Symantec, July 2009. http://www.messagelabs.com/mlireport/MLIReport_2009.07_July_FINAL.pdf

[2] Rajab, M.A., Zarfoss, J., Monrose, F., Terzis, A., "My botnet is bigger than yours (maybe, better than yours): Why size estimates remain challenging," Proceedings of 1st Workshop on Hot Topics in Understanding Botnets (HotBots'07), 2007.

[3] Global Environment for Network Innovations (GENI); http://www.geni.net/

[4] NFS NeTS FIND Initiative, http://www.nets-find.net/

[5] Seventh Framework Program, http://cordis-europa.eu/fp7/ http://www.future-internet.eu/activities/fp7-projects.html

[6] The Honeynet project, http://www.honeynet.org/

[7] Ahlswede, R. et al, "Network information flow." IEEE Transactions on Information Theory, July 2000, Vol. 46, No. 4, pp.1204–1216.