In Proceedings MADNES 2005, Singapore, September 20-22, 2005, Revised Selected Papers, 2006, pp. 186-191

Panel: Authentication in Constrained Environments

Panelists: Mike Burmester[1], Virgil Gligor[2], Evangelos Kranakis[3], Doug Tygar[4] and Yuliang Zheng[5]

Transcriber: Breno de Medeiros[1]

[1] Dept. of Computer Science, Florida State University
Tallahassee, Florida 32306
{burmester, breno}@cs.fsu.edu
[2] Dept. of Electrical and Computer Engineering, University of Maryland
College Park, MD 20742
gligor@eng.umd.edu
[3] Sch. of Computer Science, Carleton University
Ontario, K1S 5B6 Canada
kranakis@scs.carleton.ca
[4] Dept. of Electrical Engineering and Computer Science, University of California
Berkeley, CA 94720-1776
doug.tygar@gmail.com
[5] Dept. of Software and Information Systems, University of North Carolina
Charlotte, NC 28223
yzhenguncc.edu

Abstract. This paper contains the summary of a panel on authentication in constrained environments held during the Secure MADNES'05 Workshop. These were transcribed from hand-written notes.

Mike Burmester (M. B.): We are having a talk here, on the topic of *authentication on constrained environments*. The panelists could take it into any direction they find interesting. I chose this topic because it is almost impossible to achieve authentication in ad-hoc settings. (After this opening, M. B. introduces the speakers to the audience filling the room.)

Virgil Gligor (V. G.): So, I will try to be respectful to the topic. I will mention several topics that are related to the main topic.

First primitive: *Authenticated encryption.* Involves 1-pass through data, requiring block cipher computation plus redundancy check. No extra work is required, only the block cipher. This is the most efficient approach. If authentication fails, then encryption fails with high probability. Note that 1-pass authenticated encryption is what you want. Alternative: Kerberos authentication (using hashes) and a second pass with block cipher. Another alternative: use block cipher and authentication (using block cipher to implement both primitives). Again, two passes over the data. The 1-pass authenticated encryption is clearly most efficient.

M. Burmester and A. Yasinsac (Eds.): MADNES 2005, LNCS 4074, pp. 186–191, 2006.

Second primitive: Another form of authentication that is needed is to authenticate based on *threshold voting:* Suppose there are m neighbors in a location. One should be able to figure out if t-out-of-m vote to take some action (sensing event). Any t messages out of m authenticate in a neighborhood. How to do this? Various primitives are available: I have described a technique using *random polynomials*, where the degree should be approximately equal to the threshold. May have to use *Merkle trees*. In summary, it is possible to implement t-out-of-m authentication efficiently using one of Merkle trees, hash trees, or random polynomials.

Other form of authentication: Base station based as opposed to fully distributed. Not so interesting, and [I am] not convinced it is needed [for] more sophisticated forms of authentication.

Doug Tygar (D. T.): About base-station to node not being interesting: It hurts, I wrote a book on the topic! I do not think authentication will be a problem, at least machine-to-machine or message authentication. I believe our model is wrong. I will give an example with dual-core devices: a low-power one that runs all the time, and a high-power crypto device that works infrequently. What about tamper-resistance? I believe that trends coming in the next few years (Playstation DRM technology, trusted computing base (TCB)) will make tamper-resistance available. Important question: Will we have any anonymity in this type of environment?

Yuliang Zheng (Y. Z.): My interest is efficient cryptographic solutions to problems. I take a different approach. How keys get distributed, updated? How to design efficient/better algorithms? How to design authenticated encryption? For that, a solution is available. So, first issue: Key distribution. second issue: If we look to far ahead, we may loose perspective. Why not look at novel techniques for authentication if you want to anticipate MADNES 2010? Before then quantum devices may be available, so why not look at novel approaches?

M. B.: Take another angle. MANETS are short-term networks, but also useful as support for fixed networks. Attackers of fixed-line networks exploit particular weaknesses of the network. I wish to set-up wireless overlay networks to set-up new networks quickly and compensate on attacks on wire-based networks.

- Issue: Key revocation. How to revoke keys? How to decide with mobile devices are not behaving as required, how to revoke them? There is scope for ad-hoc networks that are not only sensors, not short-lived, but needed for long-term survivability (using threshold-based encryption).

Evangelos Kranakis (E. K.): These guys have left nothing for me. Let me see, authentication in constrained devices. One word at a time.

- Authentication: Verify that something is genuine. How much authentication is satisfactory to us? How much do we want? How may we afford it? Each application has its own risks, constraints, so focus on what is important.

- Constrained devices: Which part is constrained? Do we mean bandwidth limitations, resource limitations? Authentication is best for short periods of time. Authentication is short-lived.
- Environment: Assuming an ad-hoc environment, not previously thought-out. Out-of-blue authentication needed. What is involved: Servers, a wi-fi network? Environment is not well defined. Within this context, think differently, new approaches.
  - Use directional antenna in some clever way.
  - Use location in some clever way.
  - Use radio-frequency fingerprint, at least study for what aspects they may work.
  - What is possible? Measure it.

History of wired networks: As V. G. mentioned, we have experience transferring solutions from other contexts to see what can be better: Take wireless out, put wire-line back in, go back 30 years (old devices were constrained). Think differently, not just transfer solutions.

M. B.: It occurs to me, we started this workshop with V. G. with talk about how to do things in a different way. Then E. K. talked about new technologies, using non-cryptographic authentication for identification. It is an emerging technology to deal with new types of properties referring to wireless technologies.

Y. Z.: We talked about constrained devices. My watch is powered by light. Perhaps the battery issue will go away.

E. K.: I do not think battery issues will go away, it will not because of Moore's law.

Member of Audience: New technologies (TOSHIBA) increase battery capacity 3 times, then double the capacity again. Batteries improve, but many interests require power. Are we making mistakes to use crypto that is secure by going back in time 30 years?

D. T.: I do not think that we go back in time, some issues are revisited, but new issues appear. Batteries have Moore's law, everything has Moore's laws except human intelligence. Batteries could use temperature differentials, liquid fuel, could burn fuel for decades. I think these issues will be addressed. Think about the motivation: More than a third of the weight that American soldiers carry is batteries.

V. G.: Batteries are nice targets of attacks. Authentication protocols are not designed to protect against battery depletion attacks, especially public-key authentication. The problem is not really public-key if you use only once. But where to stop authentication? For example, vehicular protocols, authenticating distances. What do you mean? Feet, yards? I am talking about revealing positions. Can A reveal his position to B, then B to A? What primitives, batteries need to be used?

E. K.: There are examples of environments that are not constrained. E.g.: Internet. We try to run BGP, notoriously insecure. Cannot do anything very well. How can we be secure when we cannot do anything right?

D. T.: We cannot defend BGP. May be people will do something right next time.

V. G.: More than BGP, look at DNS. We know DNSSEC for 10 years, but it is nowhere to be seen. How to reconcile competing economic interests that are difficult to change? We know how to do Internet authentication, but other issues come in the picture. I hope in MANETs we should not box ourselves in. Back to D. T., we are interested in privacy. What is the impact of authentication on privacy? When are we for authentication? When for privacy?

D. T.: Example: My house is burglarized. I can cancel my credit cards w/o authentication. There are clear DoS issues in this picture. I want to digress. Legacy of Internet: Remember TCP/IP were experimental protocols. Do it over again, and we could make better choices. I fell negative about IPv6, its a patch instead of an evolution. In MANETs there is an opportunity not to build upon previous mistakes. What stops us from making new mistakes? Make new protocols modular so that we can address these.

Member of Audience: Regarding anonymity. Any possibility of achieving privacy-preserving authentication? Any hope?

D. T.: I do not know.

V. G.: Skeptical.

E. K.: Product of anonymity and authentication equals 1.

Y. Z.: I think devices that, for devices that are not associated with human beings, like sensors in a forest, this is not an issue. But for cell phones, this is an important issue.

Member of Audience: Some networks have hundreds of nodes. If a small number of nodes is compromised, how much damage takes place?

E. K.: A containment issue. I do not know the answer.

M. B.: Hard issue in fixed-line networks. Different, much harder in MANETs. Nearly impossible in general, but maybe local containment is achievable. Depends on the application. If it is a military application, you can use sophisticated techniques. Varies with context.

V. G.: If devices can be captured, all authentication protocols will fail. Authentication is designed to protect against man-in-the-middle attacks. If one end is compromised, what will happen to them? If adversary captures node. We will develop and deploy these technologies, introducing new vulnerabilities on old security protocols. What worries me is mismatch: That spells trouble.

D. T.: To be controversial, if [adversary] captures nodes, and re-uses them, ok. What if cloning? Need to develop cloning-proof technology.

V. G.: We have examples of protocols that can solve such problems, but they are few and far between.

D. T.: Give me 18 months. One solution: tamper-resistance. Substantial work has been achieved on this from PODC. We can learn from them. We have different applications in mind. I look at ubiquitous devices (not hundreds, but tens of thousands). Instead of looking at one sensor, pool many sensors to find answer. One question is how to design protocols to achieve security this way.

M. B.: We can handle faults, but not malicious faults. If one looks at military applications, look at the cost of attacks. Malicious faults would include cloning millions of devices, flooding. Will it happen? Who is the adversary?
V. G.: Comment about device capture: Tamper-proof not withstanding, if you have control (capture) you win (modify inputs). In World War II, spies were captured, and provided with modified information, and the Brits had poor intelligence for 2 years. This is a problem with device capture.
Member of Audience: Should remote sensing be used instead of sensors?
V. G.: Deployment has not been looked at, it is an important issue.
Y. Z.: Authentication itself is not alone the solution. Self-destruction is the answer.
V. G.: What about changing inputs? It is a fundamental problem.
Member of Audience: What about scalar authentication?
E. K.: How to mathematize this problem?
Y. Z.: Crypto technology is one of many aspects. Usability, practicability are important.
D. T.: What it means to authenticate w/ some probability? For instance, Zero-Knowledge. But not sure what that means otherwise. Once a vulnerability is discovered, authentication problems spread like wild-fire.
V. G.: People at Ericsson have looked at fairly weak authentication. It depends on the purpose. Could be that what you need if you have ways to confuse.
Member of Audience: What do you mean by weak?
V. G.: Other means of authentication: Fingerprinting, biometrics, weak for a variety of reasons. However, sufficient.
D. T.: Question for the audience: If we have a student that wants to work on this issue? What should we give him as a topic?
V. G.: Characterize your problem: Novel, formulatable, 3–4 years. E.g.: Study of emergent properties. Emergent algorithms and protocols. What is the big security problem? The big ubiquitous device is the mobile phone.
Member of Audience: People are using mobile phones as wallets, credit-cards, everything.
V. G.: Japan had an experiment with mobile phones as wallets, not very promising.
Member of Audience: If authentication is there, what about misconfiguration?
M. B.: This is like an insider attack.
V. G.: Excellent topic: Intruder attacks. We look at intrusion detection in wired networks. What to do to protect network against malicious security administrators? Right now, nothing. How to make it robust? Nothing so far.
E. K.: Some previous work exists.
Member of Audience: I think using cell phones will be secure in the future. For the moment, not feasible. But with IPv6, there will be ways to place your info somewhere in cyberspace. Currently not feasible, but with unified protocol with WLAN. IP is common protocol for all these. If we put security on IP, all these networks will be protected. Future of business is cross-protocol. I hope that in the future putting secrets on cell phones will be useful, but not now.

V. G.: Unification is good. Good research topic: Design human interfaces for security. E.g.: security interface for setting PIN/password. Did not work on my phone after switching off. I failed, and needed to look up the manual. Nice to have intuitive interface.

Member of Audience: At the moment, all in cell phones relates to 3GPP. All implementations, so it is fundamental to secure the 3GPP protocol.

V. G.: Problems: administrators fully trusted, problems with misconfiguration, bad user interfaces. It will stay like this for a while. We will get it wrong, even if protocols are good, even with tamper-resistance.

E. K.: We want to use cell phone like a wallet, but want it to be more like a pet-device–recognizing you all the time. (Human-computer authentication.) Move Ph.D. students to do some practical work.

(Panel adjourns)