This is the supplementary file of the paper: Chenyu Wang, Ding Wang*, Yi Tu, Guoai Xu, Huaxiong Wang. Understanding Node Capture Attacks in User Authentication Schemes for Wireless Sensor Networks, IEEE Transactions on Dependable and Secure Computing 2020, Doi: 10.1109/TDSC.2020.2974220

Understanding Node Capture Attacks in User Authentication Schemes for Wireless Sensor Networks (Appendix File)

Chenyu Wang, Ding Wang, Yi Tu, Guoai Xu, Huaxiong Wang

Abstract—This appendix file consists of two parts. Appendix A takes Li et al.'s scheme as an example to show a viable way to follow our proposed suggestions in Section 5. Appendix B extends the discussion about the comparison results in Table 5, with a focus on node capture attacks.

Index Terms—Appendix file.

APPENDIX A: A CONCRETE EXAMPLE TO ILLUSTRATE A VIABLE WAY TO FOLLOW OUR PROPOSED SUGGESTIONS

Sensor nodes are often deployed in harsh environments or unattended locations, which makes it easy for adversaries to break them. Once the adversary compromises a sensor node, she is in a much better position to perform a series of subsequent attacks. Furthermore, the resource-constrained nature of sensor nodes drives designers to improve the performance and unconsciously degrad the security, which makes the situation worse. As such, understanding node capture attacks and exploring the countermeasure is significant to the design of a secure user authentication scheme for WSNs. Accordingly, we proposed some suggestions to node capture attacks in Section 5. In this section, we take Li et al.'s scheme [1] as an example to show a viable way to follow our proposed suggestions. Note that, we keep the original notations of Li et al.'s scheme [1]:

- **Unreasonable design intent.**
  As our suggested, their scheme does not expose users' information (such as user identities or unique secret parameters) to sensor nodes, thus their scheme is free from the issue of unreasonable design intent.
- **Insecure communication architecture.**
  As suggested, the secure model (a) of Fig.5 is chosen. Thus, their scheme is free from the attack Type VIII.
- **Inappropriate distribution of SN's private key.**
  As suggested, the private key of sensor node SN_j is distributed as $h(SN_{id}||w)$, where w is the long term secret key. Thus, the scheme is resistant to the attack Type II.
- **Insecure transmission of some parameters.**
  Their user identity, private key of SN_j and long term secret key are transmitted securely. As we suggest, user's identity ID_U is transmitted in a form of $ID_U \oplus h(D_2)$, where D_2 is U_i's $TUSP_{G/U}$ (it is constructed by a public-key technique). Their private key K_{gs} of SN_j is transmitted in a form of $K_{gs} \oplus r_G$ and $h(K_{gs}||D_8||r_G||SN_{id})$, where r_G is $TUSP_{G/SN}$. Their long term secret key w is transmitted in a form of $h(ID_U||w$ and $h(SN_{id}||w)$. Thus, the scheme is resistant to the attack Type VI and Type IX.
  However, their $FUSP_{G/U}$ (B_2) is transmitted with XOR, once the adversary compromises sensor node SN_j, then she can eavesdrop transcript M_1 which is sent to SN_j, and compute $DID_u \oplus D_3 \oplus SN_{id} \oplus ID_u$ to get $FUSP_{G/U}$ (B_2), then the attack Type III occurs.
  As we suggested, using $FUSP_{G/U}$ (B_2) in a form of $h(FUSP_{G/U}||TUSP_{G/U}||*)$ can settle the issue well, i.e. let $D_3 = SN_{id} \oplus h(B_2||D_2||ID_U)$. Note that D_2 is U_i's $TUSP_{G/U}$. In this way, $FUSP_{G/U}$ is protected in hash function.
- **Inefficient verification of SN or $CP_{SK/SN}$.**
  Li et al.'s scheme follows our suggestion partly: $Auth_3$ of Li et al.'s scheme D_9 contains $FUSP_{G/SN}$ (K_{gs}) and $TUSP_{G/SN}$ (r_G). Thus their GWN authenticate SN_j efficiently, the scheme is secure against attack Type VII.
  However, their $Auth_4$ D_{11} only contains $CP_{G/SN}$, which violates our suggestion, thus the adversary can conduct the attack Type X. Note that, from $Auth_4$ of Li et al.'s scheme, we should understand why we suggest $Auth_4$ contains at least $CP_{G/SN}$ and $TUSP_{G/U}$ rather than $CP_{G/SN}$ and $FUSP_{G/U}$. To avoid other distractions, we suppose that $FUSP_{G/U}$ (B_2) is securely transmitted, and $D_{11} = h(ID_u||D_1||D_8||B_2)$, then $\mathcal{A}$ can get D_1 and D_8 (i.e. $CP_{G/SN}$) with the capability of C1, and carry out an offline dictionary attack with the capability of C2 and C6. Therefore, to achieve users' verification of $CP_{G/SN}$ meanwhile not raising such an attack, we recommend to let $Auth_4$ at least contain $CP_{G/SN}$ and $TUSP_{G/U}$.
- **Forward secrecy.**
  Their scheme follows the principle to achieve forward

- *Chenyu Wang and Guoai Xu are with the school of Cyber Security, Beijing University of Posts and Telecommunications, China; and with National Engineering Laboratory of Mobile Network Security.*
- *Ding Wang is with College of Cyber Science, Nankai University, China; and with State Key Laboratory of Cryptology, P.O. Box 5159, Beijing, 100878, China (Email: wangdingg@mail.nankai.edu.cn).*
- *Yi Tu and Huaxiong Wang are with School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore.*
- *Corresponding author is Ding Wang.*

Manuscript received 20 Dec. 2019; revised 18 Jan. 2020.

secrecy: conduct two exponential operations on sensor node's side [2]. Thus, the scheme is resistant to the attack Type I and Type II.

- **Offline dictionary attack.**
  Their scheme deploy public-key technology, and let Auth_1 (D_4) contain $\mathsf{FUSP}_{G/U}$ (B_2) and $\mathsf{TUSP}_{G/U}$ (D_2). Then with two unknown parameters ($\mathsf{B}_2, \mathsf{D}_2$), the adversary cannot conduct offline dictionary attack. Note that, in Section 4.4, we mention that once the adversary compromises a sensor node, she is in a better position to conduct such an attack via the parameters containing $\mathsf{FUSP}_{G/U}$ (B_2).
  In Li et al.'s scheme, besides Auth_1 (D_4), D_3 also contains B_2, once the adversary compromises sensor node SN_j, then she can eavesdrop the transcript M_1 that is sent to SN_j, and conduct an offline dictionary attack using $\mathsf{DID}_u \oplus \mathsf{D}_3 \oplus \mathsf{SN}_{id}$ as verification to test the correctness of guessed password and identity. Thus their scheme is not secure against the attack Type IV. The way to repair this weakness is not difficult and has been mentioned above: let $\mathsf{D}_3 = \mathsf{SN}_{id} \oplus h(\mathsf{B}_2||\mathsf{D}_2||\mathsf{ID}_U)$. Note that, D_2 ($\mathsf{TUSP}_{G/U}$) is an unknown parameter to the adversary $\mathcal{A}$, thus it can prevent $\mathcal{A}$ from constructing D_3 with the guessed password and identity to conduct offline dictionary attack.
- **The issue of temporary certificate technique.**
  Their scheme apply the public-key technique to achieve their security and functionality rather than the temporary certificate technique, thus their scheme is free from the issue of temporary certificate technique. Furthermore, combined with the analysis in "unreasonable design intent" and "insecure transmission of some parameters", their scheme can resist the attack Type V.

From Li et al.'s scheme, we can see that our proposed suggestions are practical and effective. Although the specific methods to achieve our suggestions are various and depend on protocol designers themselves, our suggestions do provide a good reference and guidance for designing a secure multi-factor user authentication schemes for WSNs that is resistant to node capture attacks .

APPENDIX B: COMPARISON RESULTS IN TABLE 5 ON NODE CAPTURE ATTACKS

As shown in Table 5, it is not difficult to find that regardless of whether the user authentication schemes for WSNs provide a formal proof, they are always found having this or that problems, which are caught in a circle of "break–fix–break–fix". As we mentioned in Section 6, "S6: resistance to node capture attacks" is one of the most popular criterion which cannot be achieve by most of multi-factor user authentication schemes for WSNs. Furthermore, it can be seen that each sub-criterion of S6 is met by more than 10 schemes, meanwhile unmet by at least 10 schemes. This implies the necessity of each of the ten sub-criteria of S6 and the rationality of our taxonomy of node capture attacks.

As shown in Table 5, in the years when node capture attacks were introduced into user authentication protocols, the proposed protocols were difficult to resist most types of node capture attacks. As time go by, the situation of the sub-criteria II and IX have a marked improvement, which indicates that designers have found a good way to securely distribute the private keys of sensor nodes and gateway. This changes is not surprised because the distribution of the private keys are the foundation issue to the security of authentication schemes, it should have been well settled after ten years intensive research. Since the distribution of the private keys of sensor nodes is also a factor causing the attack Type VI, it is not hard to understand why Type VI has the similar situation to Type II. Furthermore, most schemes can resist against the attack Type VII and VIII after 2018. This is because they use the secure communication model (a) of Fig.5 after Wang et al. [3] identified the inherent weaknesses in some of communication models and recommended model (a) for single-gateway settings in 2018.

Also, it can see that node capture attacks have big adverse effect on users: the attack Type III, Type IV and Type V all are popular. The attack Type IV is the outcome of not applying public-key technique or the lack of deep understanding on node capture attacks (so do the attack Type III and Type V). For example, in Jiang et al.'s scheme [4], as we shown in Section 4.4, the adversary with the private key of SN_j can use the guessed value to compute M_8, then conduct the attack, where $\mathsf{M}_8 = h(\mathsf{SK}||\mathsf{ID}_i||\mathsf{d}_i||\mathsf{K}_j)$. The reason why Jiang et al.'s scheme [4] suffers from this attack, is an issue of consciousness rather than technique. Because if they do not assume that the adversary can compromise sensor nodes, they cannot find this attack. Therefore, if we have a well understanding on node capture attacks, this attack can be found and avoid easily. Similarly, if we have realized the adversary has the same capability as a legitimate sensor node, then we will not let the sensor node know user's identity and transmit important parameters relying on the parameters that can be computed by sensor nodes. In this way, the schemes' performance on resisting the attack Type IV and V could be better. Accordingly, our comprehensive research on node capture attacks will help to design a scheme that is resistant to the three attacks.

Furthermore, among the ten types of node capture attacks, Type I is the most popular, then Type X and Type V. Type I is essentially an issue of forward secrecy. Since the resource-constrained nature of sensor nodes, it is not easy to design a user authentication scheme for WSNs that provides forward secrecy efficiently. As mentioned in Section 5, it is not difficult to avoid the attack Type X and Type V. However, due to the lack of research on node capture attacks, the adversary's capabilities are not well understand (i.e. the protocol designers are not very clear about what actually the adversary can do after getting the private key of sensor nodes), thus the protocol designers usually give the sensor node too much authority (such as computing user's identity) or do not verify $\mathsf{CP}_{\mathsf{SN}_j}$. Under this situation, the attack Type V and Type X become popular.

From Table 5, we can see that the lack of node capture attacks is one of the critical factor resulting in the circle of "break–fix–break–fix". Naturally, one of the way to break the circle is: proposing a set of comprehensive evaluation criteria, and then exploring the challenges and solutions for achieving each criterion. Evaluation criteria are the cornerstone for the design of protocols. Without a set of complete and reasonable criteria, it is difficult for designers to fully

consider the security goals of their schemes. If everyone uses their customized criteria to assess their schemes, they may ignore some important security requirements. That will undoubtedly hinder the progress of this area seriously.

However, the lack of understanding on node capture attacks makes this attack related criterion not getting a proper position in the widely-accepted criteria [3]. Before our work, the criterion "resistance to node capture attacks" is included in the criterion "resistance to known attacks". As such, when designing or analyzing a user authentication scheme for WSNs, this attack naturally is regarded as a normal attack as other simple attacks in the criterion "resistance to known attacks", thus is overlooked. Furthermore, since the adversary in the criterion "resistance to known attacks" is not allowed to get the victim's smart card, the attack scenarios where the adversary simultaneous compromises a sensor node SN_j and a user U_i's smart card cannot be captured. These two aspects greatly hinder the design of a secure user authentication for WSNs. Without a proper position in the evaluation criteria, let alone the solution to various security threats. In addition, without effective solution to be followed, designers are also helpless to node capture attacks.

Therefore, our work on node capture attacks not only improves the current evaluation criteria, but also provides a guidance to design a secure user authentication scheme for WSNs that is resistant to node capture attacks. Our larger-scale comparative measurement of 61 representative user authentication schemes for WSNs shows that only two schemes are resistant to node capture attacks, which well indicates the unsatisfactory situation, and also highlights the necessity of our work on node capture attacks.

REFERENCES

[1] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ecc based provable secure authentication protocol with privacy preserving for industrial internet of things," *IEEE Trans. Ind. Inform.*, vol. 14, no. 8, pp. 3599–3609, 2018.

[2] C. Ma, D. Wang, and S. Zhao, "Security flaws in two improved remote user authentication schemes using smart cards," *Int. J. Commun. Syst.*, vol. 27, no. 10, pp. 2215–2227, 2012.

[3] D. Wang, W. Li, and P. Wang, "Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks," *IEEE Trans. Ind. Inform.*, vol. 14, no. 9, pp. 4081–4092, 2018.

[4] Q. Jiang, S. Zeadally, J. Ma, and D. He, "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks," *IEEE Access*, vol. 5, pp. 3376–3392, 2017.