一种FPGA上防重放攻击的远程比特流更新协议的分析改进

李 磊 陈 静 张志鸿
(郑州大学信息工程学院 郑州 450001)

摘 要 Devic等提出的防重放攻击的远程比特流更新协议在密钥分发、密钥更新和存储方面具有较低的效率。提出了一种改进协议,它利用密钥链取得请求密钥和确认密钥。改进协议可有效提高密钥管理的效率,降低协议参与方的存储负担。分析表明,改进协议满足机密性和完整性,且能够防止重放攻击。

关键词 安全协议,比特流更新,FPGA,重放攻击,密钥链
中图法分类号 TN918.1 **文献标识码** A

Analysis and Improvement of Remote Bitstream Update Protocol Preventing Replay Attacks on FPGA

LI Lei CHEN Jing ZHANG Zhi-hong
(School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China)

Abstract The remote bitstream update protocol preventing replay attacks on FPGA proposed by Devic et al has a lower efficiency in the key distribution, updating and storage. We proposed an improved protocol which utilizes key chains to obtain keys for request and acknowledgement. The improved protocol can improve the efficiency of key management, and reduce the storage requirements of participants. Technical discussions show that the improved protocol ensures confidentiality, integrity, and prevents replay attacks.

Keywords Security protocol, Bitstream update, FPGA, Replay attacks, Key chains

1 引言

高性能计算能够提供强大的计算能力,具有计算领域清晰、计算作业可控、计算过程明确等特点。但实际应用问题在计算模型、处理过程以及对处理器、存储器和通信的要求上存在巨大的差异。这造成了高性能计算中心虽然在Linpack上效率高于60%,但实际运行效率一般低于10%,并带来了"高耗能"的问题。计算效能低下的主要原因是单一物理计算结构难以适应差异巨大的应用。因而,采用可重构的计算体系结构,可以提高计算的效能。在可重构计算研究领域,基于FPGA的动态可重构计算是当前的研究热点。

基于FPGA的动态可重构实现方法主要有:off-chip重构[1]、基于模块化电路设计的重构[2,3]和基于比特流技术的重构。其中,基于比特流技术的动态可重构是当前的主要研究方向,而比特流协议是实现配置动态更新、FPGA可重构的重要手段。

利用比特流更新协议进行FPGA系统的远程配置和动态更新,对信息的机密性、完整性等带来了一些安全问题。主要安全问题有:

1)窃听:攻击者可以通过网络监听等手段,盗取FPGA系统设计。

2)篡改:攻击者篡改经由网络传输的数据,欺骗FPGA系统。

3)重放:攻击者重放监听到的早期信息,获取FPGA的信任或将FPGA系统配置降级。

因此,比特流更新协议的设计需要综合采用签名、加密、Hash等安全手段保证信息的机密性和完整性等,同时需要保证协议运行的高效性。

本文分析了Devic等[4]提出的防重放攻击的比特流更新更新协议(后文简称Devic协议),将密钥链引入到协议中,使协议具有更好的安全性,并能有效减轻协议参与方的密钥管理和存储负担。

2 相关研究

在比特流更新协议的相关研究中,机密性保证比特流更新协议的信息只能被密钥拥有者读取,机密性的保证主要依赖对称密码体制,如AES或3-DES等。完整性保证比特流更新协议的信息不被非法篡改,完整性的保证主要依赖消息认证码(MAC:Message Authentication Code)。协议的防重放攻击主要依赖加密的随机数或版本号来保证信息的新鲜性。

文献[5-7]提出了采用上述方法在FPGA重配置过程中的保证机密性和完整性的方案;文献[6]提出了在比特流更新协议中使用随机数防止重放攻击的方案;文献[4,6]提出了利用版本机制防止重放攻击的方案;文献[4]指出在批量对FPGA进行更新的过程中,使用随机数防止重放攻击效率较低,但其提出的方案要求版本更新的请求和确认采用独立的密钥

到稿日期:2012-10-28 返修日期:2013-01-25 本文受国家863计划重点项目(2009AA012201)资助。
李 磊(1974-),男,博士,主要研究方向为网络与信息安全,E-mail:ielilei@zzu.edu.cn;陈 静(1977-),女,讲师,主要研究方向为P2P、移动信息安全;张志鸿(1965-),男,博士后,教授,主要研究方向为服务计算、移动信息安全。

进行加密。

密钥链机制[8]是一种在多方协议或双方协议的多轮信息交换中降低密钥存储负担和提高协议效率的有效手段。文献[9,10]分别把密钥链应用在双方和多方非否认协议的设计中，显著降低了 TTP 的存储负担并提高了协议的效率。

3 Devic 协议分析

Device 协议是一个防重放攻击的比特流更新协议。在其攻击模型中，不考虑旁路攻击、破坏或关机攻击，但考虑远程 DoS 攻击。其攻击模型假定攻击者能够通过网络读取、修改和重放比特流，系统设计者(SD：System Designer)可信且 FPGA 平台已安全初始化。攻击模型还假定攻击者位于 SD 和 FPGA 之间，能够窃听和修改所有经由网络的信息。

Devic 协议忽略身份认证过程，仅考虑比特流更新的过程。协议运行期间，采用对称密钥对信息进行加密，SD 和 FPGA 各保存 4 个对称密钥 K_{req}，K_{ack1}，K_{ack2} 和 K_B。其中，K_{req} 用来加解密更新请求，K_{ack1} 和 K_{ack2} 分别用来加解密两次确认信息，K_B 用来加解密新版本的比特流信息。K_B 采用 AES 算法，保存在静态逻辑中；而 K_{req}，K_{ack1} 和 K_{ack2} 都采用 3-DES 算法，保存在 NVM(非易失性存储器)中。

Devic 协议进行比特流更新的交互过程如图 1 所示。

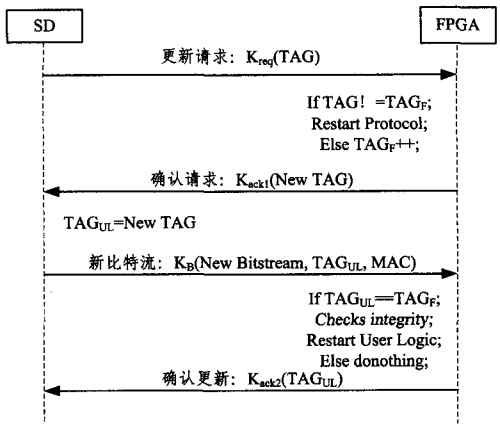

图 1 比特流更新协议

协议中 TAG 表示比特流版本号，TAG_F 是保存在 NVM 中的版本号，TAG_{UL} 是保存在用户逻辑的比特流中的版本号。

SD 首先用 K_{req} 加密 TAG 发送给 FPGA，请求更新比特流，FPGA 验证收到的 TAG 与本地的 TAG_F 是否一致，若一致，则将 TAG_F 增 1，用 K_{ack1} 加密新的 TAG 返回给 SD，确认更新请求。然后，SD 计算新的 TAG_{UL} 和 MAC，用 K_B 加密新比特流、TAG_{UL} 和 MAC，将其发送给 FPGA。FPGA 收到后，计算 MAC 验证比特流的完整性并检查 TAG_{UL} 值和本地的 TAG_F 值是否相同，以防止重放攻击，之后用新的比特流重启用户逻辑，最后用 K_{ack2} 加密 TAG_{UL}，发送给 SD，确认更新完成。

Devic 协议依赖 3 个不同的密钥对版本号进行加密，保证消息的新鲜性，防止重放攻击。在多 FPGA 组成的系统中，由于版本号是一样的，为保证对多个 FPGA 进行安全的动态更新，Devic 协议要求每个 FPGA 都拥有不同的 K_{req}，K_{ack1} 和 K_{ack2}。

考虑一个 SD 管理大量 FPGA 的情况，SD 需要保存和每个 FPGA 对应的 3 个密钥，这会给 SD 带来较大的存储负担。此外，基于安全考虑，通常密钥需要定期更换，SD 需要运行密钥更新协议，与每个 FPGA 进行 3 次密钥更新，这也会使得 SD 和 FPGA 的密钥管理效率较低。

基于以上考虑，本文将利用密钥链取代 K_{req}，K_{ack1} 和 K_{ack2}，改进 Devic 协议。

4 Devic 协议改进

4.1 双密钥链结构

改进协议采用如图 2 所示的双密钥链结构。

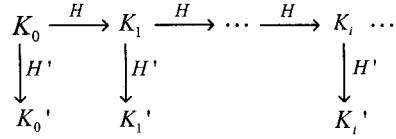

图 2 双密钥链

其中，K_0 为密钥链种子，$K_{i+1}=H(K_i)$，$K_i'=H'(K_i)$，H 和 H' 是两个不可交换的安全 Hash 函数。采用 K_0'，K_1'…作为加密密钥替代原协议的 K_{req}，K_{ack1} 和 K_{ack2}。

在双密钥链结构下，即使使用过的 K_i' 已经泄露，攻击者仍然不能计算出后续的加密密钥 K_{i+n}'。因此无需逆向使用密钥链，就可避免协议初始化时就协商密钥链的长度。

4.2 改进的比特流更新协议

改进的协议仍然使用不同的密钥对版本号进行加密，保证消息的新鲜性，防止重放攻击。但每次比特流更新，版本号不再是加 1，而改为加 3，以便利用版本号计算本次更新使用的密钥。将比特流的版本号由 i 更新为 $i+3$ 的一轮协议，将采用 K_i' 加解密更新请求，采用 K_{i+1}' 和 K_{i+2}' 分别加解密两次确认信息。由于 K_B 位于静态逻辑中，并且采用的是不同的加密算法，因此不将 K_B 纳入密钥链中。

改进后的协议运行时，首先 SD 用 K_{TAG}' 加密 TAG 发送给 FPGA，请求更新比特流，FPGA 验证收到的 TAG 与本地保存的 TAG_F 是否一致，若一致，则计算 $i=TAG$，$TAG_F=TAG_F+3$，然后用 K_{i+1}' 加密新的 TAG_F 返回给 SD，确认更新请求。SD 收到确认后，令 $TAG_{UL}=$ 新 TAG_F，并计算 MAC，用 K_B 加密新比特流、TAG_{UL} 和 MAC，将其发送给 FPGA，FPGA 收到后，计算 MAC 验证完整性并检查 TAG_{UL} 值和本地的 TAG_F 值是否相同，若相同，则用新的比特流重启用户逻辑，最后用 K_{i+2}' 加密 TAG_{UL}，发送给 SD，确认更新完成。

5 安全分析和性能比较

5.1 安全分析

改进协议采用与 Devic 协议相同的方法保证机密性和完整性，由文献[4]的安全分析可知，改进的协议仍满足机密性和完整性。

关于防重放攻击，Devic 协议依靠不同的 Key-Tag 对和封装在消息内的 Tag 值进行区分，改进协议虽然引入了密钥链，但协议中仍然使用不同的 Key-Tag 对，因而不改变原协议的防重放攻击特性。

Devic 协议允许多轮比特流更新使用相同的密钥 K_{req}，

(下转第 195 页)

[6] Bouguila N, ElGuebaly W. Discrete data clustering using finite mixture models[J]. Pattern Recognition, 2009(1): 33-42

[7] Figueiredo M A T, Jain A K. Unsupervised learning of finite Mixture models[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2002(24): 381-396

[8] Lin T I. Robust mixture modeling using multivaritate skew t distribution[J]. Statistics and Computing, 2010(20): 343-356

[9] 余成文,郭雷. 基于有限混合多变量 t 分布的鲁棒聚类算法[J]. 计算机科学, 2007(5): 190-193

[10] Bouguila N, Ziou D, Vaillancourt J. Unsupervised learning of a finite mixture model based on the Dirichlet distribution and its application[J]. IEEE Transactions on Image Processing, 2004 (11): 1533-1543

[11] Biernacki C, Celeux G, Govaert G. Choosing starting values for the EM algorithm for getting the highest likelihood inmultivariate Gaussian mixture models[J]. Computational Statistic&Data Analysis, 2003(41): 561-575

[12] Reddy K, Chiang H D, Rajaratnam B. TRUST-TECH-based expectation maximization for learning finite mixture models[J]. IEEE Transactionson Pattern Analysis and Machine Intelligence, 2008(30): 1146-1157

[13] Richardson P, Green J. On Bayesian analysis of mixtures with an unknown number of components[J]. Journal of the Royal Statistical Society-SeriesB, 1997(30): 731-758

[14] Reaven G M, Miller R G. An attempt to define the nature of chemical diabetes using a multidimensional analysis[J]. Diabetologia, 1979(16): 17-24

(上接第 150 页)

K_{ack1}和K_{ack2}，改进后的协议根据比特流版本号确定密钥K_{TAG}'，K_{TAG+1}'和K_{TAG+2}'，每轮比特流更新的密钥均不相同，这种一次一密的加密方式具有更强的安全性。

5.2 性能比较

由于改进后的协议在每轮比特流更新时均使用新的请求和确认密钥，密钥管理中对这 3 个密钥的定期更新就不再需要，仅需对 K_B 进行定期更新，与 Devic 协议相比，减轻了协议密钥管理的负担。

在多 FPGA 系统中，Devic 协议要求每个 FPGA 都存储 3 个请求和确认密钥，且各 FPGA 的密钥均不同，若 SD 管理 n 个 FPGA，则 SD 需要存储 $3n$ 个密钥。改进后的协议中 FPGA 只需要存储一个密钥链种子 K_0，SD 中也仅需保存与 n 个 FPGA 对应的 n 个 K_0。比特流的版本号和密钥 K_B 在两个协议中均须保存，不改变协议参与方的存储负担。因此，与 Devic 协议相比，改进后的协议减轻了协议参与方的存储负担。

表 1 给出了在具有 n 个 FPGA 的系统中，经过 m 次密钥定期更新后，Devic 协议与改进协议在密钥存储空间、密钥分发次数、密钥更新次数等方面的比较。

表 1 协议性能比较表

	Devic 协议	改进协议
SD 密钥存储空间	4n	2n
FPGA 密钥存储空间	4	2
初始化密钥分发次数	4	2
密钥更新次数	4m	m

结束语 本文首先分析了 Devic 提出的防重放攻击的远程比特流更新协议，发现 Devic 协议在密钥存储和管理方面效率不高，然后，基于双密钥链结构，对协议进行改进。改进协议在不改变原协议具有的机密性、完整性和防重放攻击特性的前提下，采用一次一密的方式加密 TAG，具有更好的安全性。此外，改进协议能提高协议密钥管理的效率，并降低协议参与各方的存储负担。

进一步的研究中，我们将考虑将群加密策略引入多 FPGA 系统的比特流更新协议，以期提高协议的运行效率。

参 考 文 献

[1] Lysaght P, Stockwood J. A simulation tool for dynamically reconfigurable field programmable gate arrays[J]. IEEE Transactions on Very Large Scale Integration(VLSI)Systems, 1996, 4(3): 381-390

[2] Upegui A, Peña-Reyes C A, Sanchez E. An FPGA platform for on-line topology exploration of spiking neural networks[J]. Microprocessors and microsystems, 2005, 29(5): 211-223

[3] Upegui A, Peña-Reyes C A, Sanchez E. A methodology for evolving spiking neural-network topologies on line using partial dynamic reconfiguration[C]// International Conference on Computational Intelligenc. Medellin, Colombia, 2003

[4] Devic F, Torres L, Badrignans B. Secure protocol implementation for remote bitstream update preventing replay attacks on FPGA[C]// 2010 International Conference on Field Programmable Logic and Applications(FPL). IEEE, 2010: 179-182

[5] Actel. ProASIC®3 Handbook. 2008[OL]. www. actel. com/documents/PA3_HB. pdf

[6] Badrignans B, Elbaz R, Torres L. Secure FPGA configuration technique preventing system downgrade[C]// Proceedings of the 18th International Conference on Field Programmable Logic and Applications(FPL'08). 2008

[7] Drimer S. Volatile FPGA design security-a survey [M]. IEEE Computer Society Annual Volume, 2008: 292-297

[8] Lamport L. Password authentication with insecure communication[J]. Communications of the ACM, 1981, 24(11): 770-772

[9] Cederquist J, Dashti M T, Mauw S. A certified email protocol using key chains[C]// Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on. IEEE, 2007: 525-530

[10] 李磊,谭新莲,王育民. 密钥链多方非否认协议[J]. 计算机科学, 2009, 36(010): 89-90