



安全协议设计与分析

第十二讲：课程总结

李晖 网络空间安全学院

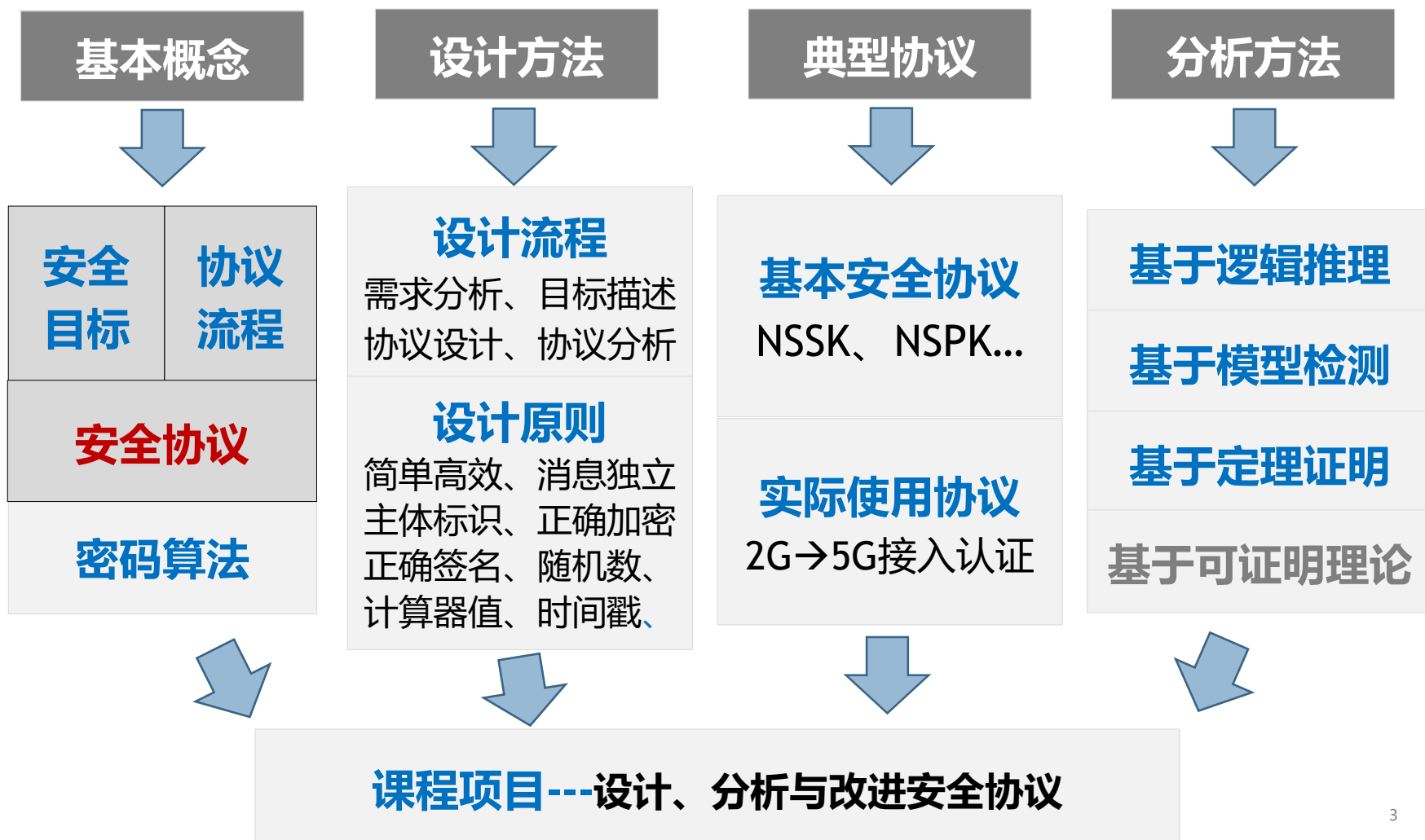


本讲内容



1. 课程内容
2. 安全协议的生命周期
3. 形式化分析方法
4. 常用的形式化分析工具
5. 未来研究方向

课程内容

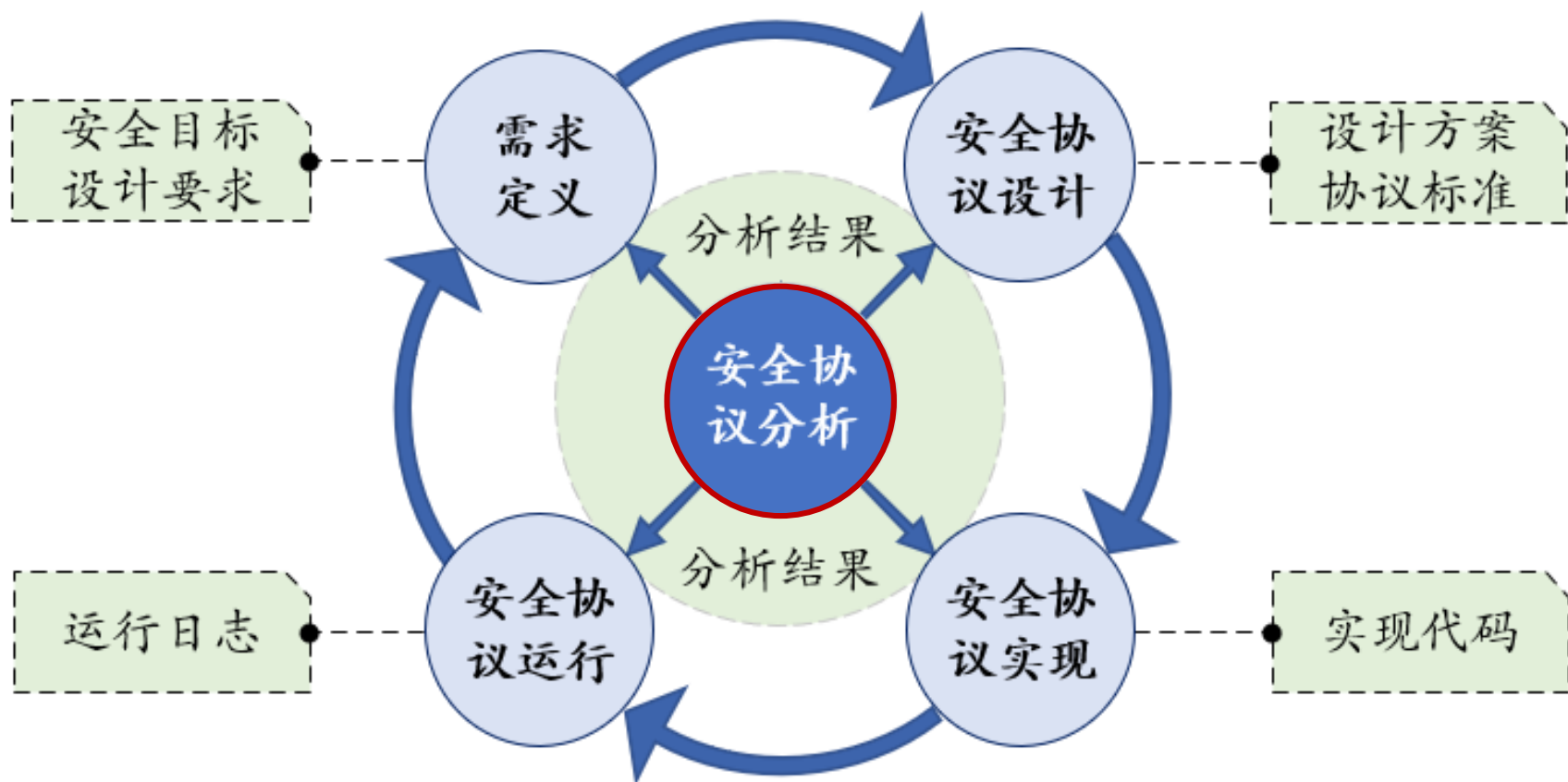


本讲内容



1. 课程内容
2. 安全协议的生命周期
3. 形式化分析方法
4. 常用的形式化分析工具
5. 未来研究方向

安全协议的生命周期



本讲内容



1. 课程内容
2. 安全协议的生命周期
3. 形式化分析方法
4. 常用的形式化分析工具
5. 未来研究方向

形式化分析方法



1983

Dolev-Yao模型

- 形式化系统模型
- 形式化分析基础

1989

BAN逻辑

- 推理规则
- 证明安全目标

1996

CSP+FDR

- 模型检测
- 发现未知漏洞

1997

Paulson归纳法

- 定理证明
- 无限并发运行

2001-现在

自动化分析工具

- ProVerif(2001)
- Scyther (2010)
- Tamarin(2012)

证明了协议的安全性

Kerberos
1980年末

NSPK
1978年

“中间人攻击”

LOWE改进协议

NSL
1996年

拓展为

5G-AKA
BlueToot
hTLS
FIDO
TESLA
.....

形式化分析方法



- 学到什么？有什么启发？
- 如何解决复杂问题？
- **降维 ---→ 把复杂问题变为简单问题**
- **表示 ---→ 如果准确描述问题**
- **分析 ---→ 如果自动寻找答案**

本讲内容



1. 课程内容
2. 安全协议的生命周期
3. 形式化分析方法
4. 常用的形式化分析工具
5. 未来研究方向

常用的形式化分析工具



	ProVerif	CryptoVerif	Tamarin
模型构建	应用Pi演算 Horn子句	比特串	迹
分析方法	进程等价观察 支持非迹属性	基于计算模型、Spi演算、Game序列	搜索树、启发式算法、支持迹属性
证明结果	给出攻击流程或证明	攻破概率	给出攻击流程或证明
适用协议	很难处理各种状态性协议，如各种密码学API。支持电子投票类协议。	使用高级密码学原语的协议	适合分析各种状态系统，如密码API，具备特定安全属性的密钥交换协议
分析的典型协议	JFK、FIDO	NSSK、NSPK、Kerberos5、Yahalom	TESLA、YubiKey、5G-AKA

常用的形式化分析工具

	AVISPA	Maude-NPA	DEEPSEC
模型构建	形式化语言HLPSL	NRL 工具升级版	应用Pi演算
分析方法	OFMC、CL-AtSe、SATMC 和 TA4SP	模型检测	等价性判定方法
证明结果	给出攻击流程	给出攻击流程或证明	html格式输出结果，可以按步跟踪
适用协议	可以发现协议攻击和漏洞，还可以对有限和无限数量会话的协议进行验证.	不仅可以实现攻击和漏洞搜索，还可以实现安全性证明	测试过经典认证协议，增加并行协议会话数量，支持复杂协议
分析的典型协议	ISO-PK 协议、IKEv2-DS 协议以及H.530 协议	IKE协议	匿名认证协议，欧洲护照协议，3G AKA协议等

重要分析结果



Protocol	Year	Published in	Tool	Main Findings
TLS	2017 2017	INRIA CCS '17	ProVerif Tamarin	TLS 1.3 Candidate, led to discover an unknown key share attack ; Uncover applications that assume TLS 1.3 provides strong authentication guarantees may lead to security problems
5G-AKA	2018	CCS '18	Tamarin	UE and SN only holds weak agreement; traceability attack, impersonate attack
LoRaWAN	2019	Computer Networks(J)	Scyther	Jamming and replay attacks exists in versions 1.0 (2015), and 1.1 (2017) is secure
ZigBee	2020	HotSoS '20	Tamarin	Leak network key and link key in ZigBee 1.0, and Zigbee 3.0 holds secure properties
WPA2.0	2020	USENIX'20	Tamarin	Capture key-reinstallation attacks and their variants of WPA2
FIDO	2021	NDSS'21	ProVerif	Capture authenticator rebinding attack, parallel session attack, privacy leakage, DoS attack
BlueTooth	2022	S&P '22	ProVerif	Capture 5 known vulnerabilities and discovering 2 new security issues.
UTX protocol	2023	CCS '23	ProVerif	UTX protocol – an enhanced payment protocol satisfying privacy requirements
SPDM 1.2	2023	CCS '23	Tamarin	SPDMthe current design still has some design pitfalls

本讲内容



1. 课程内容
2. 安全协议的生命周期
3. 形式化分析方法
4. 常用的形式化分析工具
5. 未来研究方向

未来研究方向



➤ 安全协议描述

- ✓ 规范安全协议的描述方法

➤ 安全协议分析

- ✓ 安全协议实现与标准的一致性分析及证明方法、实现正确性的分析与证明方法
- ✓ 安全协议形式化分析新方法（新的安全目标、提高分析效率的方法、自动构建攻击的方法、提高分析自动化的方法）
- ✓ 各种前端工具（通过代码直接生成形式化模型、自动分析多场景安全、依据标准自动建模安全属性和协议流程等）

➤ 安全协议设计

- ✓ 设计新应用场景下满足特殊安全需求的多种安全协议
- ✓ 自动化的安全协议设计方法

➤ 安全协议运行

- ✓ 研究保障安全协议的配置正确方法



谢谢大家！ 欢迎提问！