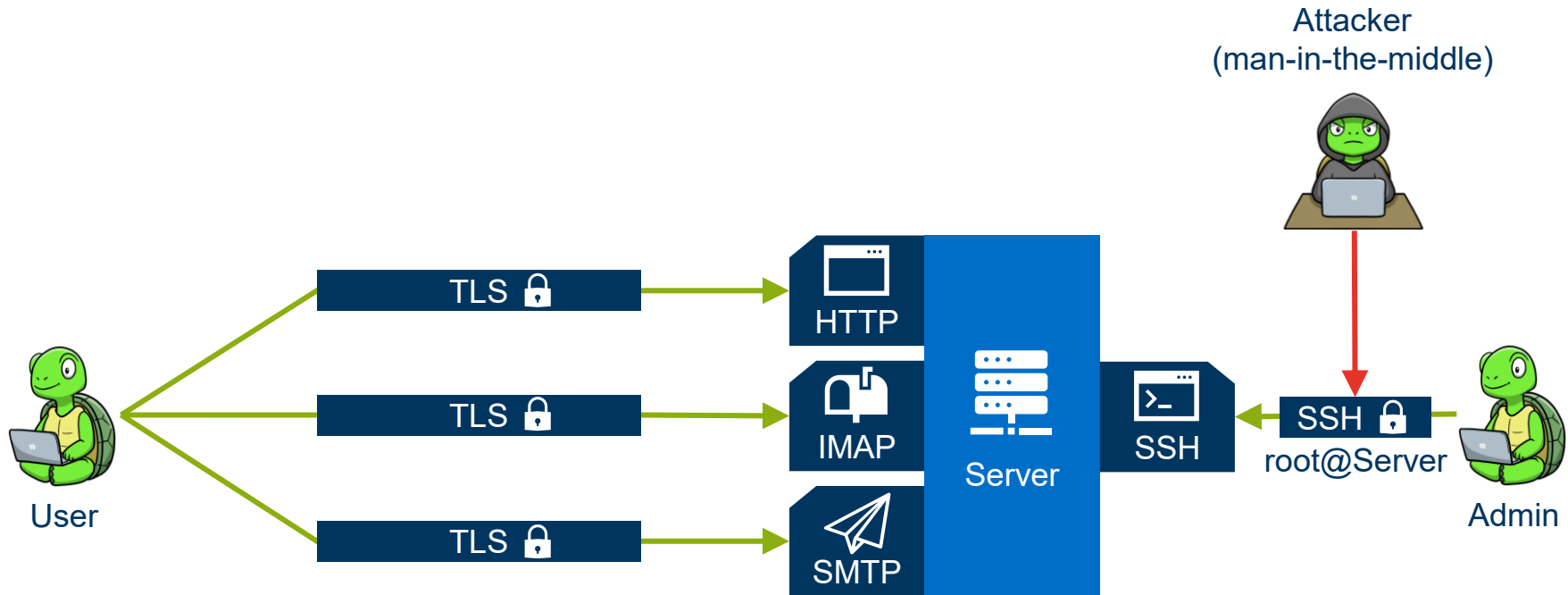


RUHR-UNIVERSITÄT BOCHUM

TERRAPIN ATTACK: BREAKING SSH CHANNEL INTEGRITY BY SEQUENCE NUMBER MANIPULATION

Fabian Bäumer, Marcus Brinkmann, Jörg Schwenk | 33rd USENIX Security Symposium

SSH Is Often Used for High Privilege Server Access



SSH Is Split Into Separate Layers



SSH Connection Protocol [RFC4254]



SSH Authentication Protocol [RFC4252]



SSH Transport Layer
Protocol (TLP) [RFC4253]

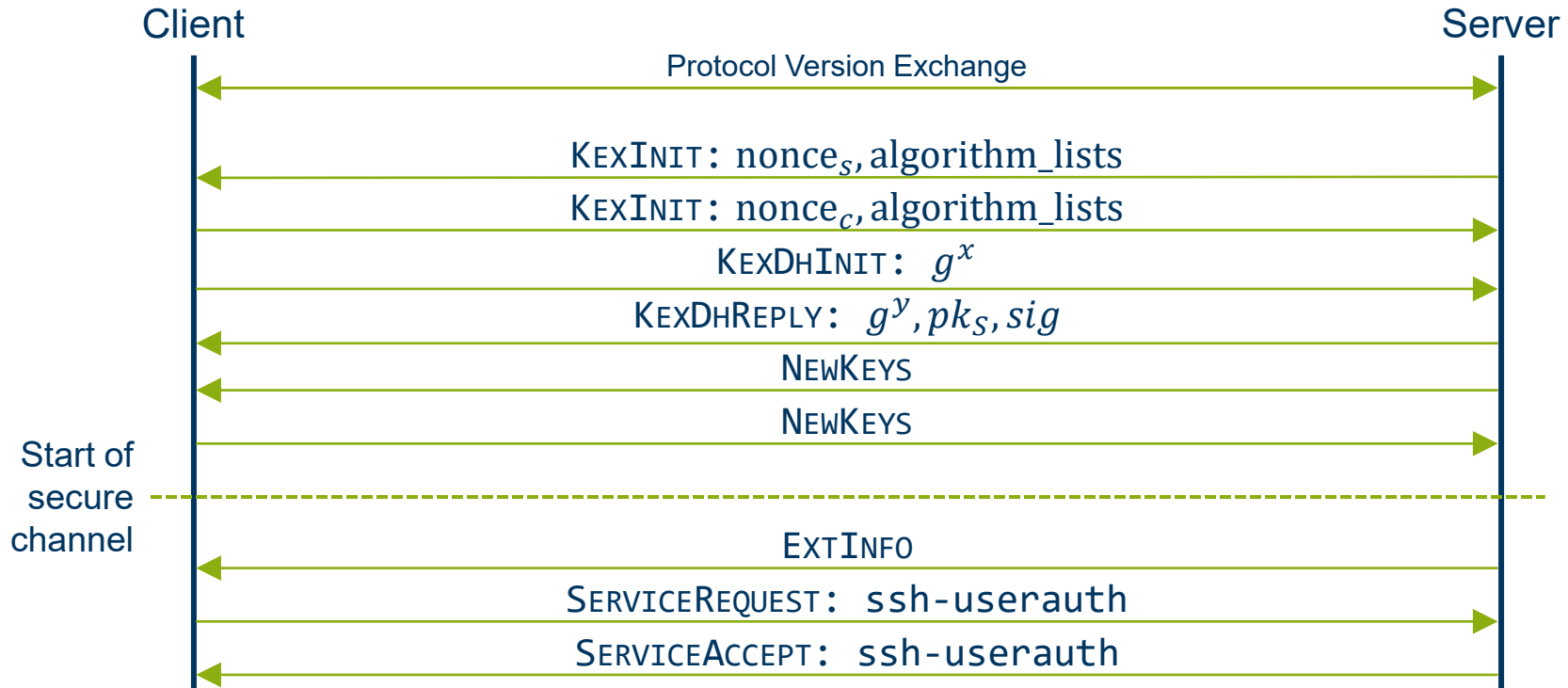
→ Binary Packet Protocol
→ SSH Handshake



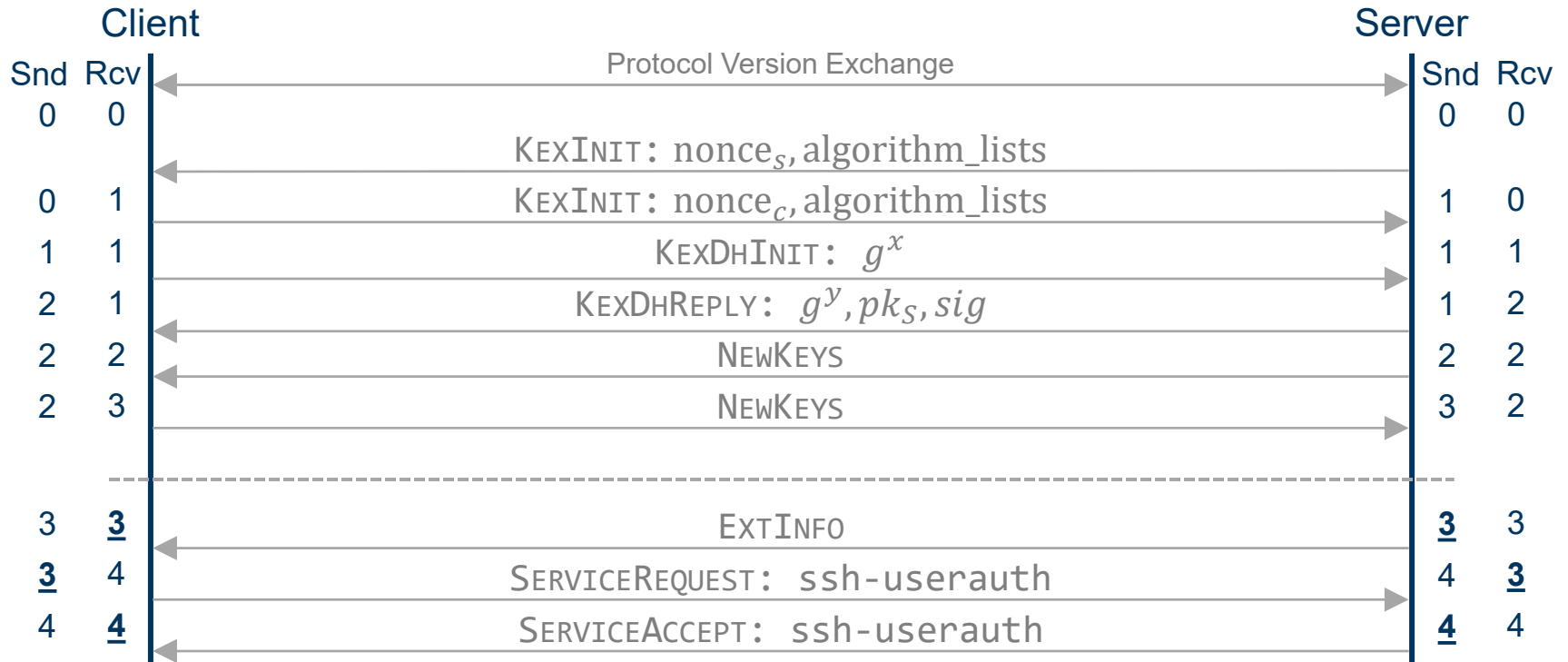
TCP / IP



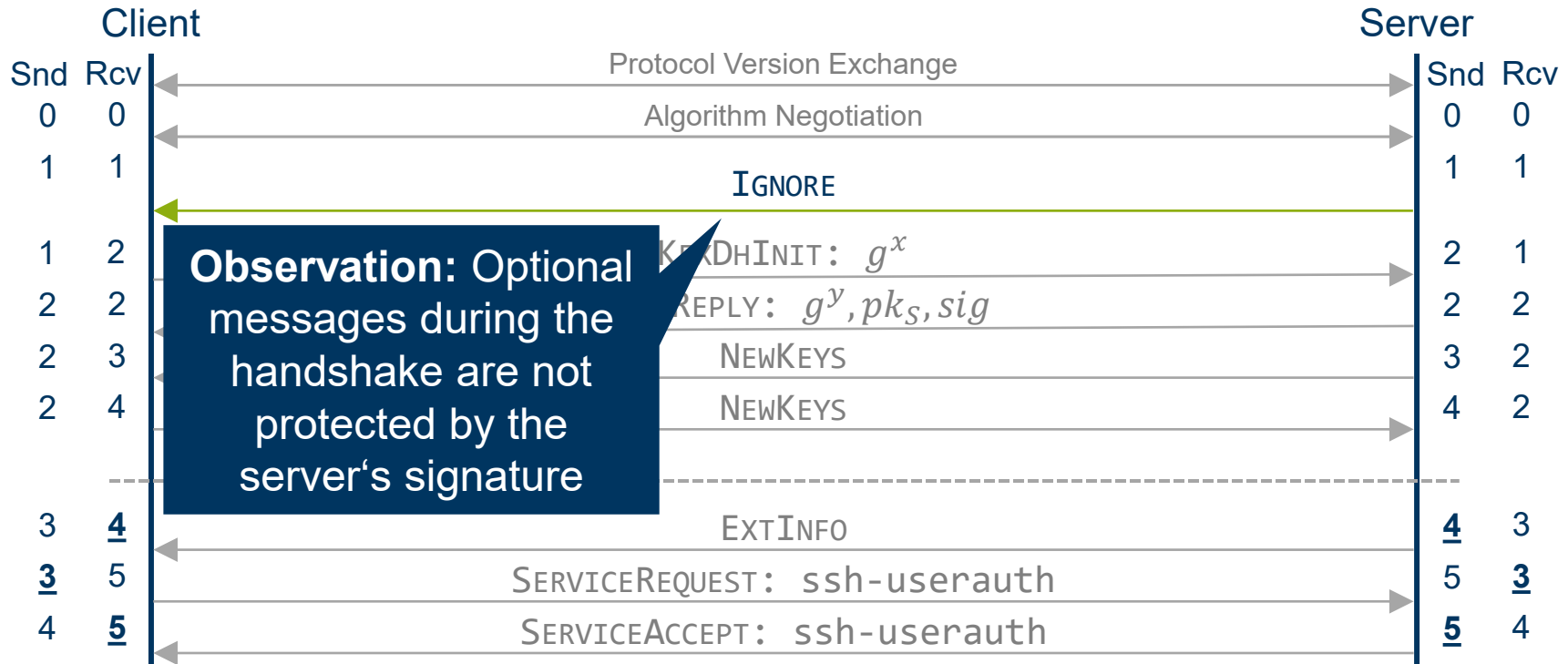
A Typical SSH TLP Protocol Flow



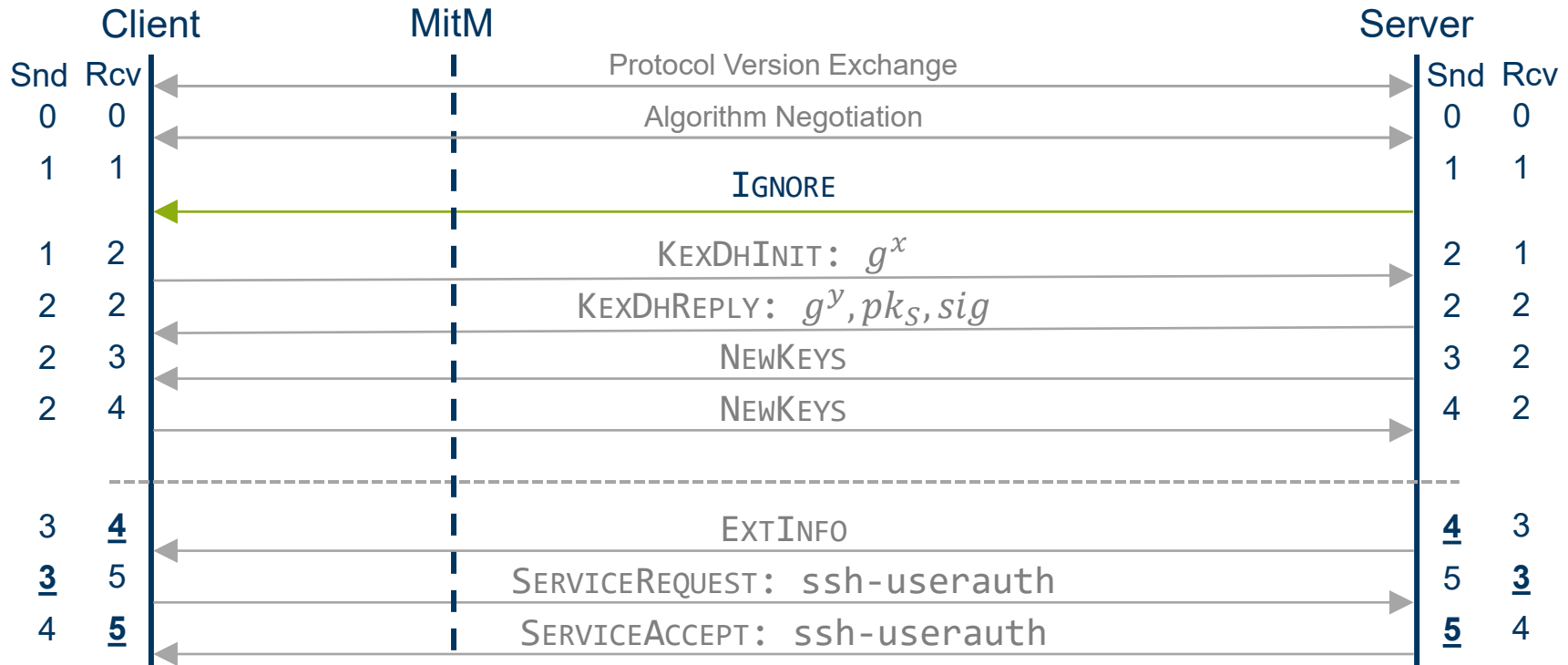
SSH Uses Implicit Sequence Numbers



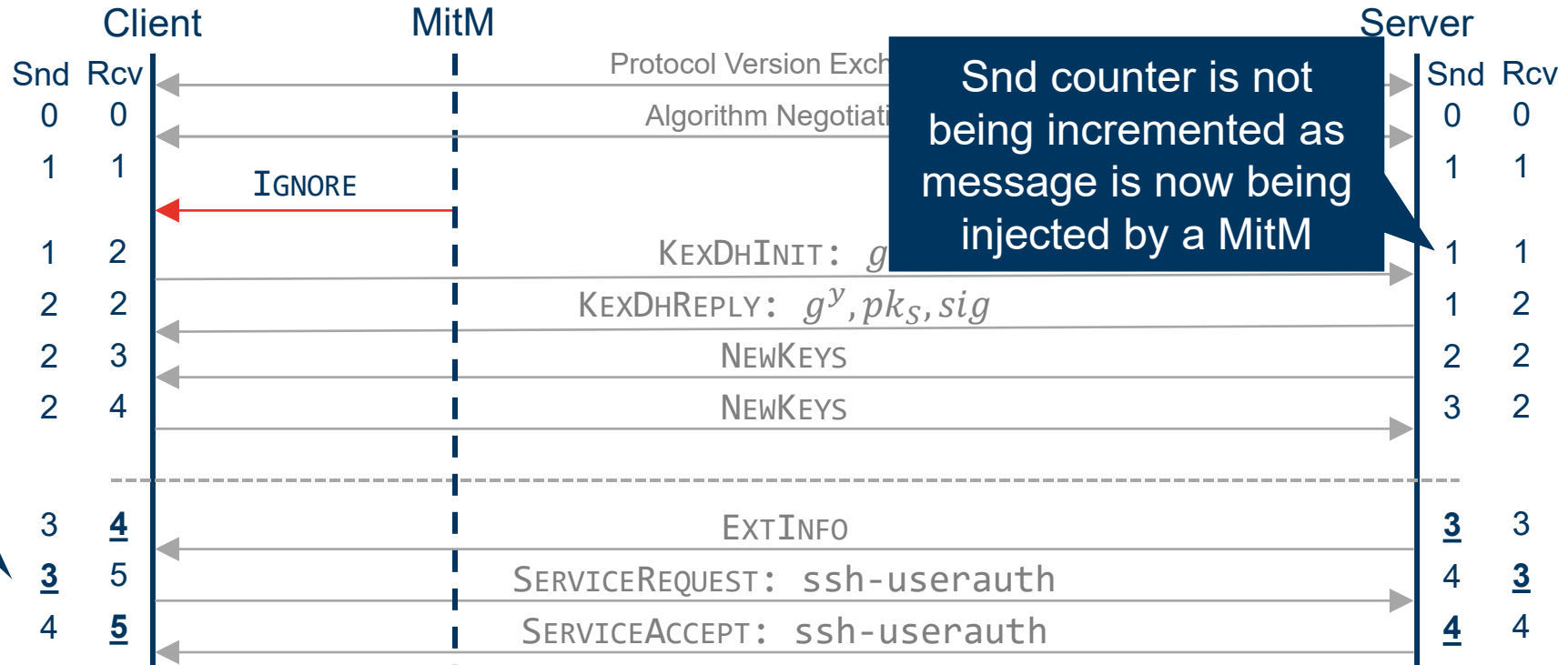
SSH Allows for Optional Messages in Handshakes



SSH Allows for Optional Messages in Handshakes

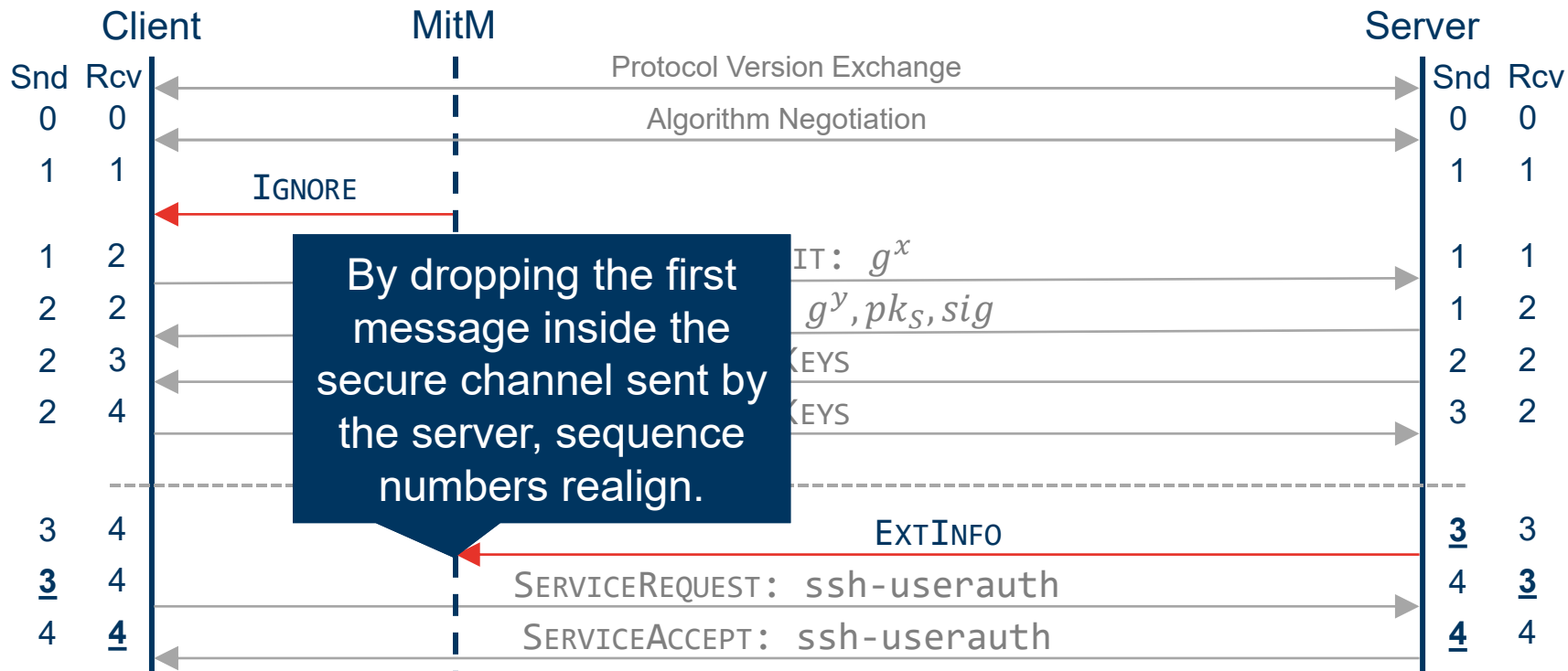


MitM Attackers Can Inject Messages Into Handshake...



... And Drop Messages Inside The Secure Channel

CVE-2023-48795
(CVE-2024-41909)



The EXTINFO Message Contains Extensions as Key-Value Pairs

server-sig-algs

- List of public key algorithms for user authentication
- Enables RSA-SHA2 support

ping@openssh.com

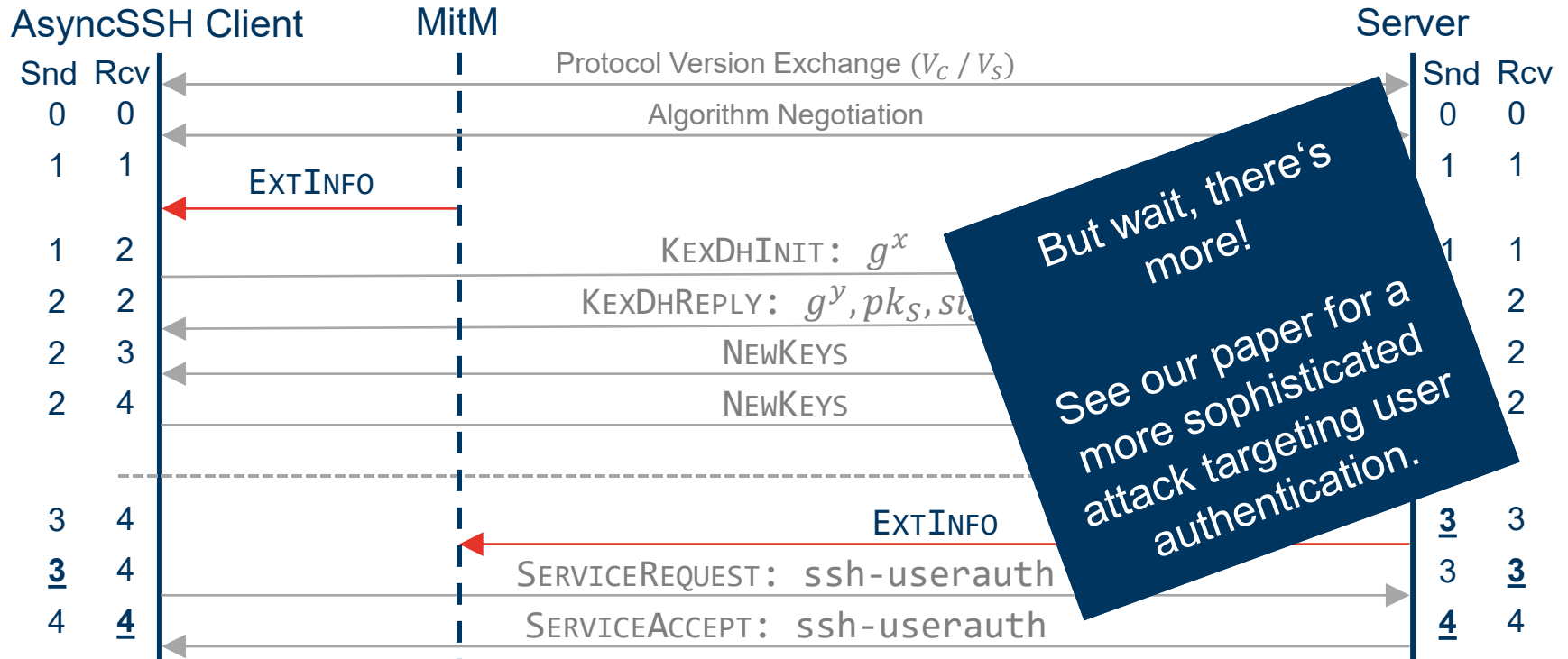
- Like Heartbeat extension in TLS
- Can be used to obscure keystroke timings

Other Extensions

- Not considered because no security impact

Implementation Bugs Can Escalate Impact

CVE-2023-46445
 CVE-2023-46446



ChaCha20-Poly1305 And Encrypt-then-MAC (EtM) Are Affected

Perfectly Exploitable

Exploitation Unlikely

Limited Exploitability

Success rate
between 0.0003 –
0.8383

AE Mode	Preferred		Supported	
ChaCha20-Poly1305	8,739k	57.64%	10,247k	67.58%
CTR-EaM	3,964k	26.14%	4,200k	27.70%
GCM	1,219k	8.04%	10,450k	68.92%
CTR-EtM	828k	5.46%	10,685k	70.46%
CBC-EaM	359k	2.37%	1,585k	10.46%
CBC-EtM	14k	0.09%	2,614k	17.24%
Other	2k	0.01%	-	-
Unknown / No KEXINIT	36k	0.24%	-	-
Total	15,164k	100%		

Mitigating Our Attack Is Difficult

Countermeasure	Our Suggestion	“Strict KEX” (OpenSSH)
Reset sequence numbers at key installation	✓	✓
Authenticate the entire handshake transcript (hash)	✓	
Harden handshake to disallow unexpected messages		✓



> 30 unique implementations support “strict kex”



~ 11 million servers offer “strict kex”




Lessons Learned

- **Terrapin is a novel cryptographic attack targeting SSH channel integrity**
 - Can be exploited in practice to downgrade the connection's security
 - May lead to more severe vulnerabilities if combined with state machine flaws
- **Affected modes of encryption (% Supported):**
 - ChaCha20-Poly1305 (67.58%)
 - CBC-EtM (17.24%)
 - CTR-EtM (70.46%)
- All these modes have been proven secure in previous works
 - Proofs hold when “strict kex” countermeasure applied

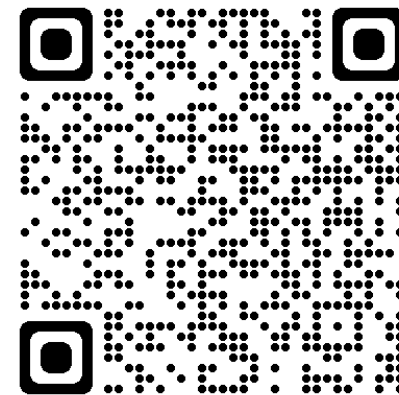


Thanks! Questions?



Terrapin Attack

Paper	Vulnerability Scanner
Q&A	Patches



<https://terrapiin-attack.com/>

E-Mail: fabian.baeumer@rub.de
X (formerly Twitter): [@TrueSkrillor](https://twitter.com/TrueSkrillor)
Mastodon: [@Skrillor@infosec.exchange](https://mastodon.social/@Skrillor)