sie flas f	Diffie-Hellman based	AKE:	
01		Back	
Africe x & Zo	8×	Bank y ^{er} Z p	
· .	at conten (k' (mot	\rightarrow	
•	g, C Encar (K, Can Bank, O	$\underline{r}) k,k' \leftarrow H(g,g^{*},g^{*},g^{*},g^{*})$	
		$\sigma \leftarrow \text{Sign}(\text{sk}_{\text{Buck}}, (g, g^2, g^3, p))$	k _{Bank}))
derive k,k'	← H(q, g ^x , g ⁸ , g ^x ⁸)	session key k	
check o is	5 signature on (g, g ^x , g ^y)	PkBank) (intui	tion: CertBank identifies server as Barik (with pkBank)
	pheant is the public key		σ binds the session parameters (g, g^{x}, g^{y}) to
			the public key identified by cert Bank
d at actua	J: Alice knows she is	talking to Book (but not vice	verse ()
in or protoc	NOC RIGGS DIE 15	talking to Boark (but not vice	
	THE HE LAND	\sim 1007 common modul on 1004	e web E TLS 1.3 - Don't innent your own AKE postoco)!
		("ONE-Sided HRE) ALWAYD US	E 125 1.3 Don't invent your own MAC protocol.
client	<u>server</u>		- older systems / foreign systems
	Client Hello DH Key-Share	<u>ClientHell</u> o: List of supported ci	phersuites older systems / foreign systems
		(e.g., AES-GCM	- 120, 1125 (Cur 236) Optors
	ServerHello DH Key-Share	Possible TLS extens	to snotener versions of
	Certificate	Server Hello: Chosen ciphersuite	TLS vulnerable to
	(encrypted)		cipher downgrade attacks
	-Finished	Application layer secured using u	
	- Application >	Application layer secured using u kA->B and	k _B ⇒ _A
)	20
otecting S	igning keys is extre	enely important for a (2A
ommon a	pproach: threshold	l signatures	
Recall F	SA signatures :	5 = H(m) ^d (mod N)	
	0		
Idea:	Split signing ke	y d'into many "she	"
		/ /	
	Sample de da	R Turn such the	$d_1 + d_2 + \cdots + d_n = d$
	eunipic official official		
		a and a la a la	What is not the fill set I is a short
	Ubserve - given a	in subjet of shares (.	that is not the full set), d is perfect
	hidden		
	Suppose we give	one share di to each	server
	di	H(m)	given signature shares of = H(m)di,
	HC	mili	let o = Mierry oz
	d2 .	H(m) dient	let $\sigma = \pi_{iecn} \sigma_i$ = $\pi_{iecn} H(m)^{d_i}$
		H(m)d2 -7/	
	dr l	H(m) ⁴²	= H(m):ed; = H(m) which is a signature on m

TLS supports session setup using a "pre-shared key" (so full handshake not needed): <u>client</u> <u>full</u> handshake <u>server</u> <u>New Session Tickat (none, id)</u> I <u>Client</u> server \Longrightarrow preshared key olerived from session secrets, nonce, and id fresh key KA->B, KB>A derived for rest of session (based on : aitial mesoages) hegotisted identity of peer Output of AKE protocol: (key, id) Authenticity: Only party that knows key is id (i.e., the party identified by id) Secrecy: 'All parties other than client and id cannot distinguish key form random (i.e., key is hidden) Consistency: If id also completes protocol, then it outputs (key, id client) C if we do not have client authentication, then idetent is empty Often also require forward secrecy: compromise of server in the future cannot affect secrecy of sessions in the past > In TLS, server secret is a signing key - fresh Diffie-Hellman secret used for each session is fresh ("ephenarcal") Compromising signing key allows impersonation of server, but does not break secrecy of point sessions has we will see, not all AKE protocols provide forward secrecy Very tricky to get right as we will see ... Just use TLS! <u>AKE from PKE</u>: suppose server has certificate authenticating a public key for a PKE scheme (CCA-secure): $k \stackrel{R}{\leftarrow} K \xrightarrow{Alice} \underbrace{\frac{r}{\leftarrow} r}_{k} \stackrel{cert_{Bank}}{\leftarrow} \underbrace{\frac{r}{\leftarrow} ert_{Bank}}_{k} \xrightarrow{Bank} \underbrace{\frac{sk_{Bank}}{cert_{Bank}}}_{k} \xrightarrow{cert_{Bank}} \underbrace{\frac{sk_{Bank}}{cert_{Bank}}}_{k}$ Yields statically-secure AKE (no forward secrecy) Compromise of SkBank compromises all past Sessions $\begin{array}{c} \downarrow & (r'_{k}) \leftarrow Decrypt(sk_{bank}, c) \\ k, Bank & k, L & check that r' > r \end{array}$ no client authentication If we do not encrypt the nonce r: replay attack possible (adversary replays messages from past session - e.g., "send Eve \$10") C nonce ensures <u>freshness</u>