Proving IEEE 802.11i Secure

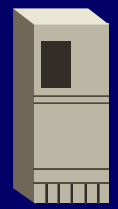
Mukund Sundararajan

Joint work with Changhua He, Arnab Roy,
Anupam Datta, Ante Derek, John Mitchell

802.11i Key Management

Laptop

Access Point



Auth Server

TLS: Uses Certificates, provides authentication

(Shared Secret-PMK)

4WAY Handshake:
Creates keys for data communication

Group key handshake:
Keys for broadcast communication

Data protection:
AES based

Properties of 802.11i Key Mgt.

- Roughly
  - Only authorized devices can join n/w
  - Devices do not join rogue n/w
  - Peer device is alive
  - Keys set up for data and group communication are fresh and secret

Proof of 802.11i security

A Formal Proof in Protocol Composition Logic (PCL) of :

- On execution of an 802.11i role, properties listed in the standard are satisfied.
- Attacker model (perfect crypto)
  - Intercept, read, reorder, delete any message on the n/w
  - Construct, send messages

Why a Proof?

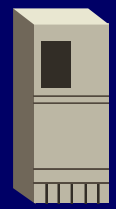
- [He Mitchell] analyzed 4Way Handshake using Murphi
  - Found a DoS attack
  - But did not find any security flaws
- [Mitchell Shmatikov] analyzed TLS

- 'Finite' state analysis does not guarantee security

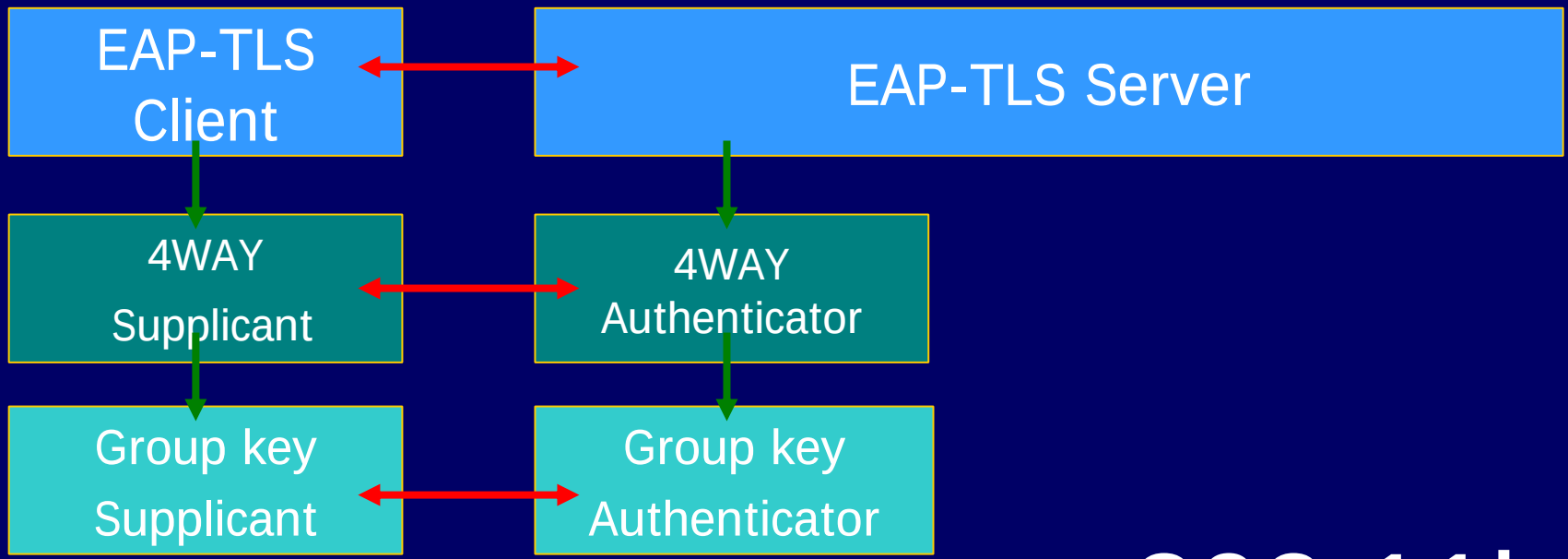
Model Checking does'nt Scale

Laptop

A.P.



A.S.



802.11i

TLS Server Role

receive C, S, n_c, $suite_C$ //Hello

new n_s

send S, C, n_s, $suite_S$ //Resp

receive C, S, $\{sec\}_{Ks}$, $SIG_C(hshk1)$ //Xfer

check $SIG_C(hshk1)$

decrypt $\{sec\}_{Ks}$

send S, C, $hash_{sec}(hshk2)$ //ServerView

Security Properties of TLS

- The client and the server agree on
  - Value of the *secret*
  - Version and crypto suite
  - Identities (mutual authentication)
  - Protocol completion status
- The *secret* term is not known to a principal who is not the client or the server (shared secret)

Matching Conversations

Honest(C) [TLS Server]$_S$ $\exists$ C.

Send (C, Hello) < Receive (S, Hello) $\wedge$

Receive (S, Hello) < Send (S, Resp) $\wedge$

Send (S, Resp) < Receive(C, Resp) $\wedge$

Receive(C, Resp) < Send (C, KeyXfer) $\wedge$

Send (C, KeyXfer) < Receive (S, KeyXfer) $\wedge$

Receive (S, KeyXfer) < Send(S,ServerView)

Proof Sketch

1. S sees SIG_C(hshk1) concludes C constructed it
4. If honest C constructed SIG_C(hshk1), then it executed actions consistent with TLS Client role
5. Order actions based on freshness of nonces

Some Axioms Used in the Proof

AA4 $\top[a;\cdots;b]x\,\mathsf{a}\langle\mathsf{b}$

VER $\mathsf{Honest}(\hat{X}) \wedge \mathsf{Verify}(Y, SIG[\hat{X}](x)) \wedge \hat{X} \neq \hat{Y} \supset$
$\exists X.\mathsf{Send}(X, m) \wedge \mathsf{Contains}(m, SIG[\hat{X}](x))$

FS2 $\mathsf{FirstSend}(X, t, t') \wedge \mathsf{a}(Y, t'') \supset \mathsf{Send}(X, t')\langle\mathsf{a}(Y, t'')$
where $X \neq Y$ and $t \subseteq t''$.

Program Invariant used in Proof

$$\Gamma_{tls,1} \quad \mathsf{Honest}(\hat{X}) \wedge \mathsf{Sign}(X, sigterm) \supset$$
$$(\mathsf{Send}(X, tlsm1) < \mathsf{Receive}(X, tlsm2) < \mathsf{Send}(X, tlsm3))$$
$$\wedge \mathsf{FirstSend}(X, n_x, tlsm1) \wedge \mathsf{FirstSend}(X, secret, tlsm3))$$

Proof of TLS Authentication

$$\mathbf{AA1, P1, AA4} \quad [\mathbf{TLS : Server}]_Y \\ (\mathsf{Receive}(Y, tlsm1) < \mathsf{Send}(Y, tlsm2) \\ < \mathsf{Receive}(Y, tlsm3) < \mathsf{Send}(Y, tlsm4) \quad (1)$$

$$\mathbf{AA1, P1} \quad [\mathbf{TLS : Server}]_Y \mathsf{Verify}(Y, SIG_{\hat{X}}\{sigterm\}) \quad (2)$$

$$(-1),\ \mathbf{VER} \quad [\mathbf{TLS : Server}]_Y \mathsf{Honest}(\hat{X}) \wedge \hat{X} \neq \hat{Y} \supset \exists X.\mathsf{Sign}(X, sigterm) \quad (3)$$

$$(-1), \Gamma_{tls,1} \quad [\mathbf{TLS : Server}]_Y \mathsf{Honest}(\hat{X}) \wedge \hat{X} \neq \hat{Y} \supset \\ \text{and Inst } X \text{ to } X^o \quad (\mathsf{Send}(X^o, \hat{X}, \hat{Y}, m1) < \mathsf{Receive}(X^o, \hat{Y}, \hat{X}, m2) \\ < \mathsf{Send}(X^o, \hat{X}, \hat{Y}, m3)) \wedge \mathsf{New}(X^o, secret) \\ \wedge \mathsf{FirstSend}(X^o, n_x, tlsm1)) \wedge \mathsf{FirstSend}(X^o, secret, tlsm3)) \quad (4)$$

Matching Conversations!

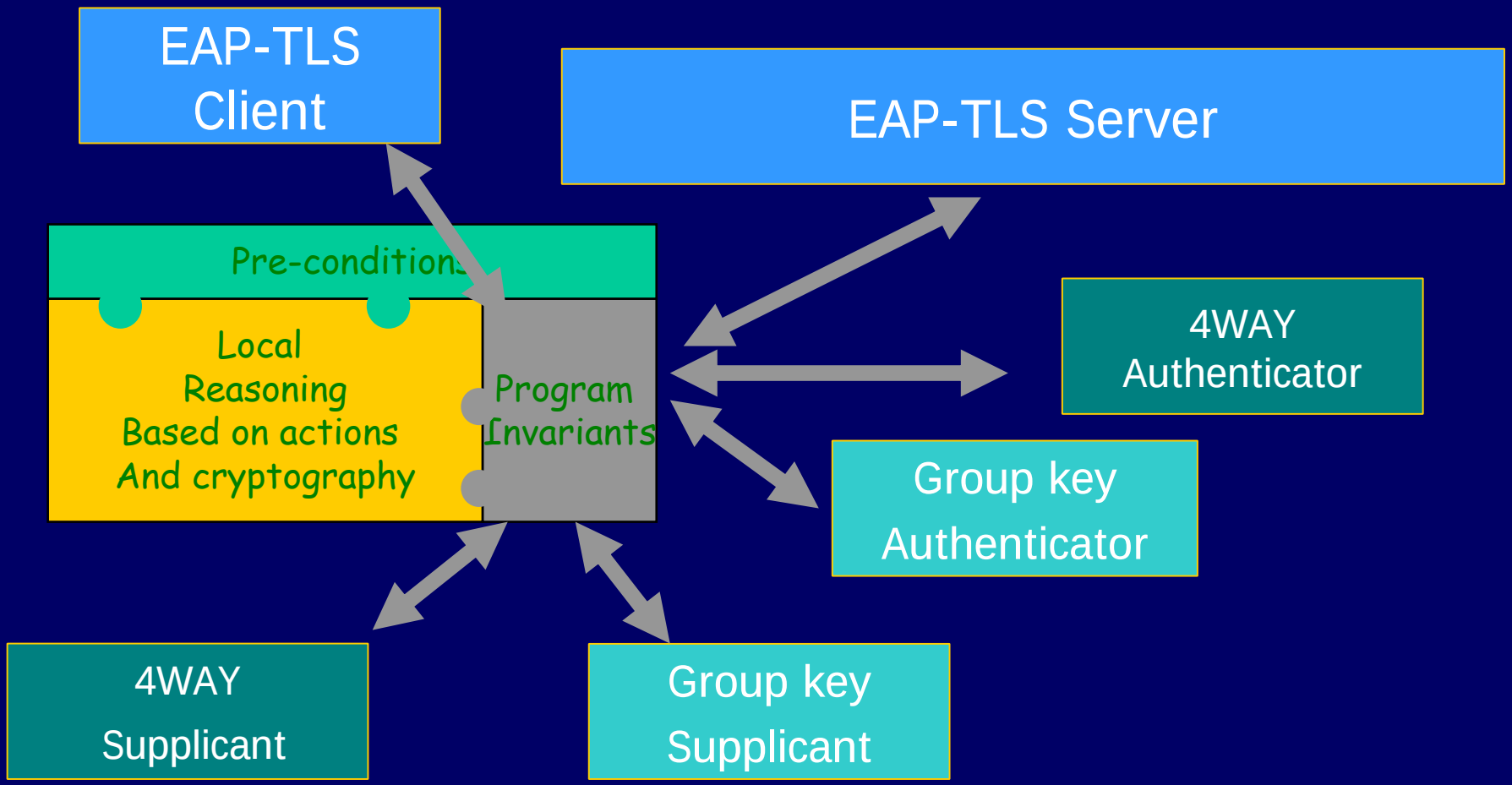
$$\mathbf{AN3, FS1, P1} \quad [\mathbf{TLS : Server}]_Y \mathsf{FirstSend}(Y, n_y, tlsm2)) \tag{5}$$

$$(-1), (4), \mathbf{FS2} \quad [\mathbf{TLS : Server}]_Y \mathsf{Honest}(\hat{X}) \wedge \hat{X} \neq \hat{Y} \supset \mathsf{Send}(Y, tlsm2) < \mathsf{Receive}(X^o, tlsm2) \tag{6}$$

$$(4), (1), \mathbf{FS2} \quad [\mathbf{TLS : Server}]_Y \mathsf{Honest}(\hat{X}) \wedge \hat{X} \neq \hat{Y} \supset (\mathsf{Send}(X^o, tlsm1) < \mathsf{Receive}(Y, tlsm1)) \wedge (\mathsf{Send}(X^o, tlsm3) < \mathsf{Receive}(Y, tlsm3)) \tag{7}$$

$$(1), (4), (6), (7), \mathbf{ORIG} \quad [\mathbf{TLS : Server}]_Y \mathsf{Honest}(\hat{X}) \wedge \hat{X} \neq \hat{Y} \supset \exists X.(\mathsf{Send}(X, tlsm1) < \mathsf{Receive}(Y, tlsm1)) \wedge (\mathsf{Receive}(Y, tlsm1) < \mathsf{Send}(Y, tlsm2)) \wedge (\mathsf{Send}(Y, tlsm2) < \mathsf{Receive}(X, tlsm2)) \wedge (\mathsf{Receive}(X, tlsm2) < \mathsf{Send}(X, tlsm3)) \wedge (\mathsf{Send}(X, tlsm3) < \mathsf{Receive}(Y, tlsm3)) \wedge (\mathsf{Receive}(Y, tlsm3) < \mathsf{Send}(Y, tlsm4)) \wedge \mathsf{Has}(X, secret) \tag{8}$$

Proof Structure



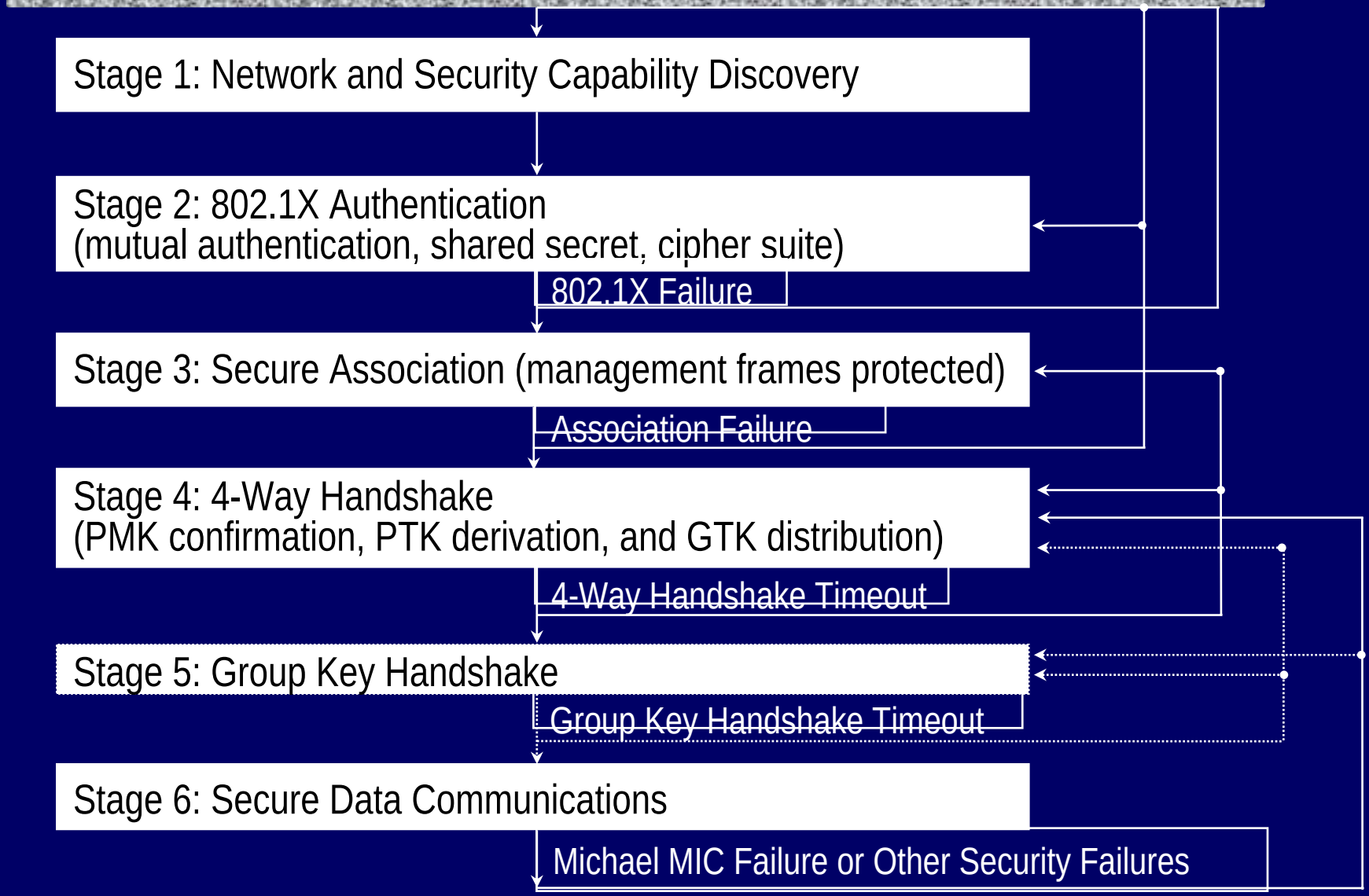
Protocol Insights

- 802.11i is secure
- Other modes are safe
  - Using Cached PMKs and Pre-shared Keys is safe
  - Safe under error handling
- Protocols can share certificates with TLS as long as conditions listed in paper are satisfied

Evolution of WLAN Security

- Wired Equivalent Privacy
  - Incorrect use of cryptography
  - WEP lacks key mgt
- 802.11i is designed to fix these issues (June 2004)
- [He Mitchell] uncovers DoS attacks
- Fix adopted by standards committee
- Security Proof of 802.11i

Error Handling [HM05]



Interactions can cause Flaws

- Exercise: Construct two protocols. Each does something reasonable. Each is secure in isolation.
- But, if any principal executes both protocols, one of the two protocols is insecure.
  - Chosen protocol attack (Wagner et.al.)

Thanks!